SAFETY4RAILS

Investment assessment model for cost-benefit evaluation of risk mitigation and recovery

Deliverable 7.1

Lead Author: RMIT

Contributors: UREAD

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.

D7.1 Investment assessment model for cost-benefit evaluation of risk mitigation and recovery		
Deliverable number:	D7.1	
Version:	V1.2	
Delivery date:	26/08/2022	
Dissemination level:	PU – Public	
Nature:	Report	
Main author(s)	Sujeeva Setunge Mojtaba Mahmoodian, Nader Naderpajouh, Huu Tran, Kanishka Atapattu, Mohsen Moshrefzadeh	RMIT
	Atta Badii	UREAD
Internal reviewer(s)	Atta Badii Stephen Crabbe Malte von Ramin Antonio De Santiago Laporte Ibrahim Ulucinar Marina Trentin	UREAD Fraunhofer Fraunhofer, SAB member – Security Assessment MDM TCDD CDM
External reviewer(s)	*Process not yet completed - feedback input to future work*	

Document control			
Version	Date	Author(s)	Change(s)
0.1	31/05/2022	RMIT	ToC
0.2	11/06/2022	RMIT	PC Feedback
0.3	23/06/2022	RMIT UREAD	Requirements overview, UREADcontributions
0.4	07/07/2022	RMIT	Further Refinements
0.5	22/07/2022	RMIT	2nd draft for review, considering PC further feedback
0.6	28/07/2022	RMIT UREAD	Creation of v0.5 from 1.5 after internal Review
0.7	30/07/2022	RMIT	Final Formatting
0.8	01/08/2022	RMIT	Considering comments
1.0	01/08/2022	RMIT	Creation of 1.0 from V0.8 (1.6), after PC comments
1.1	07/08/2022	RMIT	Creation of V1.1 after PC comments
1.2	26/08/2022	Fraunhofer	Creation of V1_2 with updated version of V1_1 provided by RMIT following further internal review by TCDD, CDM MDM. Potentially sensitive data in Table 11 redacted.

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 onrush 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, for example, 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 novel emerging risks, it will facilitate continuous adaptation of the SAFETY4RAILS solution; this will be validated by two rail transport operators and the results will support the re-design of the final prototype.

TABLE OF CONTENTS

List of tables

List of figures

Executive summary

This document, Deliverable D7.1, has established a guided analysis of Purposes and Contexts underpinning the proposed SAFETY4RAILS Investment assessment model for cost-benefit evaluation of risk mitigation and recovery, and, accordingly set out the implicated stakeholder and data types. According to the preliminary investment assessment, the deliverable identified three types of data types as part of the current investment plan for processing critical response budgetary planning and de-identification strategies for asset data. The essential data have been identified, including historical data processing by the CAMS software in SAFETY4RAILS. Therefore, the requisite compliance measures have been budgeted, deployed, and monitored at each stage of the project lifecycle. Other partners and end-users can use this information to update their cost-benefit analysis and generate a justified budget plan together with all the necessary information prior to data acquisition. The deliverable 7.5 defines a localised Investment Assessment model for end-user decision makers so that mitigation and recovery phases can be cost-benefit evaluated, as well as risk-aversive measures to reduce delays in planning specific investment assessments, since it will collect and describe cyber-physical threats and systems incorporated into the asset assessment. This deliverable is devoted to asset management in the wake of railway infrastructure and network incidents - in other words, incidents (such as combined cyber-physical incidents) that, in the event of failure, would cause the most severe damage to infrastructure and/or the system, and/or lead to the need for recovery, albeit despite some infrastructure damages. CAMS analyses the costs of cyber-physical threats and their impact on infrastructure components. For railway infrastructure assets, they are divided into several categories, including: (Track, Station, Information System, Rolling Stock, Railway signalling system, IT networks, operational systems, etc.) and each asset has an identification code assigned to it for easier referencing.

In this process, assets have been grouped by type, taking into consideration their nature as well as potential sources of incidents, by using the following criteria:

- Physical attacks (deliberate/ intentional) e.g., sabotage, vandalism, theft;
- Cyber Incidents (human error) e.g., leaks of data via mobile applications, increasing recovery time; increased time to recovery post-incident
- Cyber-attacks (deliberate/ intentional) e.g., Abuse of resources, Worms/ Trojans;
- Cyber Incidents (Failures/ Malfunction) e.g., Hardware failure, Failure of cable networks;
- Natural Hazards e.g., Heavy wind, Thunder stroke, Fire, Floods;
- Outages e.g., power outage, wireless network is down;
- Physical incidents e.g., Tunnel collapse, Fire in rolling stock, Individual hit by a train.

This deliverable is output of the first task of work package 7. The work package is called Policy planning and investment measures for prevention, detection, and response mitigation, for which RMIT is the lead participant under the SAFETY4RAILS project. Additionally, in this context this deliverable extends the analysis base by introducing a framework for cyber-physical Threats Severity Ranking and Combinatorial Countermeasures Prioritisation (TSR-CCP) by UREAD. This supports an evolutionary iterative re-prioritisation of steps to be undertaken by an enterprise to ensure optimal preparedness, business continuity and mitigation strategies to remain responsive to the inevitable evolution of the threat space. This incorporates an ontologically committed and methodologically guided framework to support combined threats-driven and risks-based Resilience Agility Optimisation for any risk types in any domain as demonstrated for the privacy and security threats in Railway Systems.

1. Introduction

1.1 Overview

The Central Asset Management System (CAMS) provides deterioration modelling, risk assessment, rehabilitation cost forecasting, and an integrated mobile solution for data collection.

Budget policies will also affect resilience, as different recovery plans, associated with mean different budget allocations, will lead to different recovery times and resilience factors.

CAMS software forecasts asset ageing damage. An effective maintenance plan and budget allocation requires insight into the deterioration process of each asset. Variations in conditions over time are represented by curves derived based on historical data.

Based on the predicted damage conditions, the model will forecast future maintenance and repair expenditures. Using this data, asset managers can maximise impact and reduce risk by choosing the most suitable time and place to invest. This module determines the final damage condition after a disruptive event. An intensity measure of the disruptive event is used to determine fragility functions that express the probability of reaching or exceeding a level of damage. The response of an asset to a certain event depends also on its current infrastructure state. Deterioration also affects fragility analysis. Defining the extreme event is the first step in performing this analysis.

By defining level-of-service criteria for the given elements and suggesting rehabilitation strategies, risk cost mitigation and expenditure projection can be achieved.

CAMS can include inflation's effect based on inflation rates. Based on the forecasting of damage and maintenance costs, the backlog estimation provides the asset manager with valuable decision-making information. CAMS informs the asset manager about the most effective financial strategy to enhance resilience against different threats, taking into account other asset management activities such as maintenance, repair, and rehabilitation. CAMS can be applied to IT assets as a budgeting tool as described in the previous requirements. By integrating physical and digital elements, budgetary and financial strategies will be more effective.

CAMS provides analysis of different budgetary scenarios based on different maintenance, repair, rehabilitation, and enhancement strategies. CAMS optimises resilience enhancement strategies within regular asset management plans. It will therefore utilise the modules for optimisation and budgeting. In order to evaluate all possible strategies, CAMS could define normal and accelerated response times as well as cost.

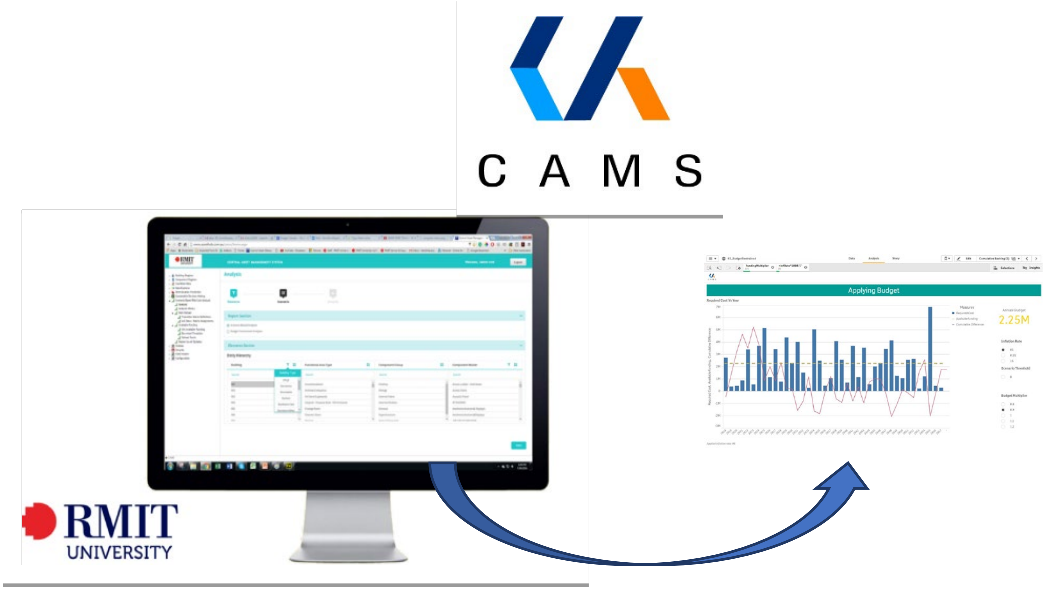


FIGURE 1: CAMS - CENTRAL ASSET MANAGEMENT SYSTEM [56]

CAMS is responsible for ensuring an accurate recovery budget for assets affected by sudden events. The final asset damage is calculated based on the initial condition of the assets before the incident, as well as the condition of the asset after the incident.

In the S4RIS platform architecture the CAMS GUI is available through the S4RIS GUI and CAMS also has the ability to publish and subscribe to the Distributed Messaging System (DMS).

When incidents occur, managing investment and critical response budgeting is essential for mitigation and recovery, since disasters or extreme events are usually excluded from operation and maintenance budgets. As part of SAFETY4RAILS, CAMS enable decision makers to integrate financial and budgetary elements related to these types of unexpected events.

Specifically, CAMS is responsible for providing accurate recovery costs for assets involved in the event based on the assessment of the damaged assets. Damage is assessed using the initial condition before the incident and the impact the incident has on the assets, using an onsite inspection to determine the conditions after the incident.

As part of the specific investment management, end-users can recalculate their budget plans for restoring services based on the output of CAMS, and the railway maintenance and repair budget can also be calculated in parallel with normal deterioration of the railway.

1.2 Structure of the deliverable

In work package 7, the tools focus on policy planning and investment measures for prevention, detection, response, mitigation, and recovery phases, but in CAMS the focus is on the cost and time of reopening facilities during recovery phases.

- Chapter 1: Introduction

In this section, we introduce CAMS and its involvement in the SAFETY4RAILS project.

- Chapter 2: CAMS (Central Asset Management System)

In this section, the overall purpose is to consider the CAMS requirements with the CAMS's Graphical User Interface (GUI), consistent with the requirements that are outlined in the SAFETY4RAILS project Grant Agreement.

- Chapter 3: Asset Management and budgeting strategies

This section discusses Asset Management and Budgeting strategies under ageing and extreme events.

- Chapter 4: CAMS FRAME WORK

This chapter presents a CAMS framework for asset management adapted for the S4RIS platform as part of the CAMS budget planning.

- Chapter 5: Prevention, Detection, Response and Mitigation

CAMS output can be used to generate asset management for all above-mentioned phases affected by the ageing of railway infrastructure. Additionally, CAMS output allows railway end users to update their budget planning after incidents in the recovery phases.

- Chapter 6: Case-Studies Addressed

The purpose of this chapter is to give a brief overview of some of the S4RIS case studies that have been conducted using the platform.

- Chapter 7: Future extensions

The effective budgeting for investments as targeted for resilience enhancement in cyber-physical incidents is dependent on the categorisation and prototyping of the various incidents. Therefore, digitising cyber-physical events can generate additional vulnerabilities information for the tool, which can make budget charts and predictive investment models more accurate. Accordingly, this section, establishes a detailed list of the various cyber-physical privacy and security threats that could possibly lead to cyber-attacks and/or data privacy violations within an IoT-enabled railway system. The analysis then sets out a comprehensive explanation of the responsive countermeasures and introduces a use-context-aware Threats Severity Ranking and Combinatorial Countermeasures Prioritisation Framework (TSR-CCP). This is implemented by means of a hierarchy of decision tables with an intuitively explainable ranking calculus which determines the highest priority safeguarding measures to be prescribed for cyber-physical resilience.

- Chapter 8: Summary and Conclusion

An overview of CAMS output relating to asset management by budget plan is provided in this chapter. RMIT presents a short summary of what was delivered and what can be inferred from the CMAS process when it comes to integration and testing with other tools in the S4RIS platform.

2. CAMS (Central Asset Management System)

The main objective of WP7 within SAFETY4RAILS is to establish an analysis of the current asset management practices followed by the development of a tool to assist organisations in making informed decisions about budget and investment policies facing extreme events, such as terrorist physical, cyber or combined attacks as well as normal operations.

Utilising CAMS provides a great opportunity for exploring the combined effects of physical and cyber disruptions on assets. In other words, how, when and where to spend money to enhance resilience under cyber-physical incidents can be summarised as follows.

- Definition of Framework
- Defining the concept of Fragility module
- Defining the concept of Budget module
- Defining the concept of Resilience module
- Defining the concept of Normal Degradation module
- Implementation of transition matrices for future damage
- Drafting specifications of the new features
- Building the case study

2.1 Background

Initially, the Central Asset Management System (CAMS) developed by RMIT University as an online platform for deterioration modelling, risk assessment, and rehabilitation cost assessment.

CAMS incorporates stochastic deterioration models developed based on validated and calibrated discrete condition data for components of an infrastructure.

The sustainability indicators are sourced from over one hundred end users. An infrastructure maintenance, refurbishment and other operating costs module is included in the software. Assets can be analysed based on scenarios cost and risk forecasts for the infrastructure portfolio are generated using the discrete condition data gathered from inspections or end-user historical databases.

CAMS also integrates mobile applications to collect data on assets.

2.2 Functionalities

Assets from existing infrastructures represent decades-long investments that are worth several hundred billion dollars.

For the long-term management and design of public infrastructure such as buildings, drainage systems, bridges and roads, it is imperative to understand the deterioration process. CAMS supports data-driven decision making in relation to infrastructure life cycle management based on a variety of factors.

By using CAMS, an asset manager can capture asset data and obtain various analysis reports, such as asset deterioration, recovery time and budget forecasting, so that end-users can make informed decisions about maintenance and budget allocations even during incidents.

Domains of actions		Needs expressed by internal end-users
Risk Management cycle	Forecast	**Turning Big Data into added-value information**, to be used as a basis to forecast events or attacks.
	Prevent	**Anticipation of cascading effects** due to interdependencies between different segments & stakeholders to prevent those effects.
	Detect	**Improve detection of weak signals** to early detect crisis, with an enhanced calibration of algorithms - Reducing the number of false positive alerts
Threat (or crisis) Management cycle	Respond &Mitigate	**Real-time observation and analysis** of crowd movements during a crisis to determine the nature of the crisis and adapt response accordingly
	Recover Phase CAMS contribution for Cost & Time of recovery	**Methodologies for managing cyber-physical events** and foster the recovery
	RETEX (Return of experience)	**Lessons learnt from cyber-physical events to** update procedures, approaches and tools

TABLE 1: SHOWS WORK CIRCULATION ACCORDING TO END-USER NEEDS [2]

2.3 Current framework

The current framework of CAMS is based on the concept of resilience and system of components for rail assets.

In the literature of infrastructure asset management, resilience is often viewed as the capacity of an asset to recover quickly to an acceptable level after a damage event. This concept of resilience is considered well suited for this project on safety for rails. The resilience concept has three main items, namely, damage level, time and cost to recover as shown in the FIGURE 2.

Damage level can be caused by time-based deterioration processes (e.g. corrosion of steel, fatigue) and/or random extreme damage events by natural hazards (e.g. flooding, earthquake) and man-made incidents (e.g. terrorist attack, human error). The time-based deterioration processes and random extreme damage events can be dependent on each other. For example, a minor earthquake event can cause concrete cracks, which enable accelerated corrosion of reinforcing steel of concrete if the cracks are not filled. On the other hand, the time-based deterioration can reduce the strength of rail assets, which can be failed under a normal operating load and/or a random damage event.

The time to recover often refers to time required to bring the assets back to an acceptable level of service capacity after the occurrence of an extreme damage event. The time to recover is dependent on the damage level and other factors including the budget, the constraints of resources and the priority level.

The cost of recovery often refers to the cost required to achieve the planned recovery time. It is dependent on the damage level and the required time to recover.

The resilience index of a rail asset can be defined as the area of the triangle between damage level and recovery time (if recovery cost is excluded under unlimited budget and resources) or the volume of 3D triangle or pyramid (if the recovery cost is considered). The smaller the area/volume, the higher the resilience index and vice versa.

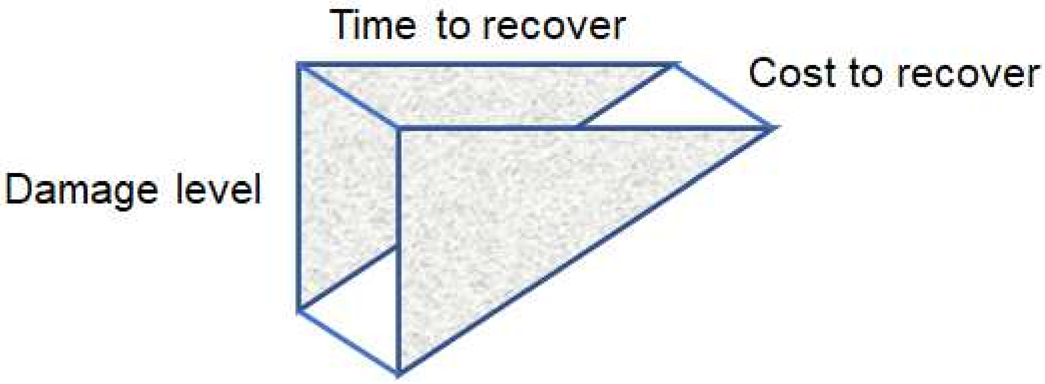


FIGURE 2: CONCEPT OF TRIANGULAR RESILIENCE

For the concept of system of components, the current CAMS framework treats individual rail assets (e.g. IT components, rail tracks) as components of a rail system since train station and similar assets (e.g. bridge and bus) are just a name for a group of interconnected components that serve a purpose. For example, components of a train station can include platform, stairs, roof, office, ticket machines and so on. The main features of these components are:

- They are made of various materials such as steel, concrete, plastic and so on.
- They have different deterioration mechanisms and rates of deterioration
- They are subjected to different forms of hazards and damages.

Therefore, when the condition state or deterioration rate or service life or reliability of a train station is referred to, the simple answer could be the average of its components or the worst components because the 'train station' is not a single physical asset but is a group. With the above definition, it is better to look at train station and the like as a system of components.

2.3.1 Component hierarchy of a train station

Components of a train station can be arranged in a hierarchy structure. FIGURE 3 shows a simple train station, which has only five main components: concrete platform, rail track, ticket gate, fence and time display.

These components are divided into 2 classes, called A-components and B-components, with the assumption that the failure of any A-component can cause closure of the train station and the failure of B-components do not cause closure of the train station but affect the serviceability of the train station. For example, if the platform is badly damaged or the railway track is destroyed, and then train station is closed. On the other hand, if time display is failure, train station is still in service but customers might be inconvenienced. The purpose of dividing rail assets into different levels of importance is in order to determine the condition of train station as a combined asset and for prioritised preventive and recovery rehabilitation planning.

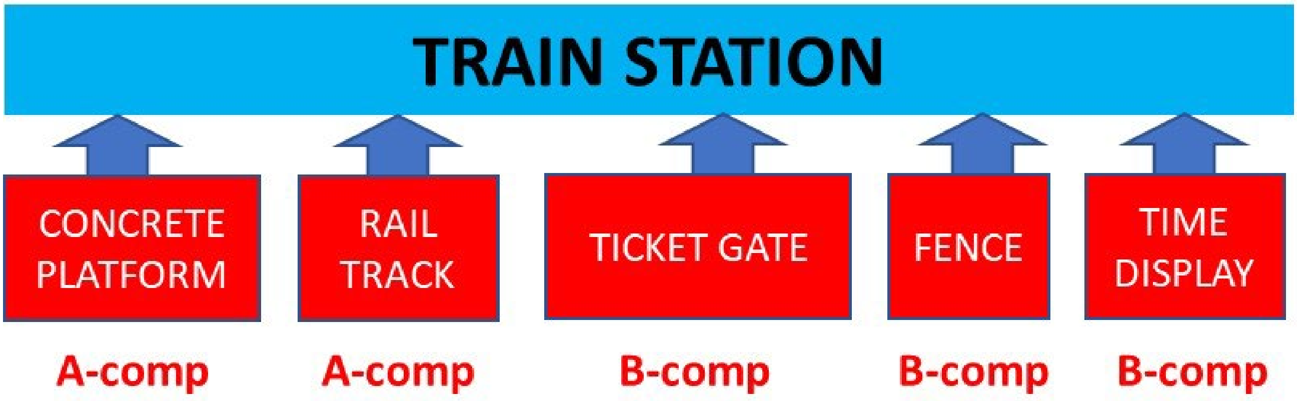


FIGURE 3: HIERARCHY STRUCTURE OF A SIMPLE TRAIN STATION

2.3.2 Performance indicators of a train station

There are numerous performance indicators for a train station in the literature. The two basic performance indicators are structural safety and customer satisfaction; and these can be used as the key performance indicators to be assessed in the evaluation of any proposed solution to support operational safety and efficacy to the satisfaction of the stakeholders.

2.3.3 Asset management of a train station

The asset management of a train station is a process to ensure asset management objectives over the service life. Asset management objectives include:

- Acceptable performance of train station
- Lowest lifecycle cost and least adverse impacts on society and environment
- Others

The asset management objectives can be achieved by asset management tasks:

- Monitoring of condition of components
- Conducting risk assessment
- Performing optimal maintenance and rehabilitation program
- Predicting future deterioration and maintenance budget
- Other

2.3.4 Condition of components

The task 'Monitoring of condition of components' is crucial to ensure the performance of a train station. Despite the advancement of condition monitoring techniques such as Structural Health Monitoring (SHM) and non-destructive test (NDT), visual inspection is still commonly used for components of a station. From visual inspection, visual damage can be recorded and then are scored to provide condition rating of the component with regards to one or several performance indicators. For example, a hole in a platform could not be regarded as serious damage as to the structural capacity of the station platform but may be a serious hazard to customers.

The typical condition rating of component can be from 1 to 5, with one being brand-new like and five being failure or failure imminent. The condition rating can be based on combined damage found from visual inspection. A condition inspection and rating manual is required to cover all the components of train station.

2.3.5 Condition of a train station

Condition of a train station can be rated between 1-5 with linguistic meaning similar to condition rating of its components as explained in Section 5. The condition of the train station can be used for at least two purposes:

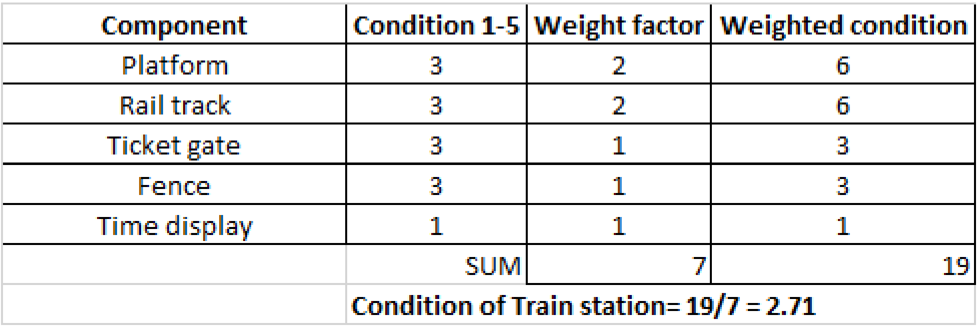
- To report condition of a train station and a network of train station since reporting of components is too detailed
- To prioritise funding and maintenance planning between train stations.

As explained in Sections 2.3.3 and 2.3.4, a train station is a group of components. Therefore, condition of a train station can be derived from condition of its components by several methods.

i- Weighted average method

This method determines the condition of a train station by using 'weighted average' on condition of its components. The term 'weighted' refers to the importance or contribution of individual components the condition of the train station can be different and can be expressed through weighting factors. Table 2

For example, the platform can be considered more important than the time display and their weight factors can be 2 and 1 respectively. The 'average' means that the conditions of components with their weight factors are averaged for decision making.

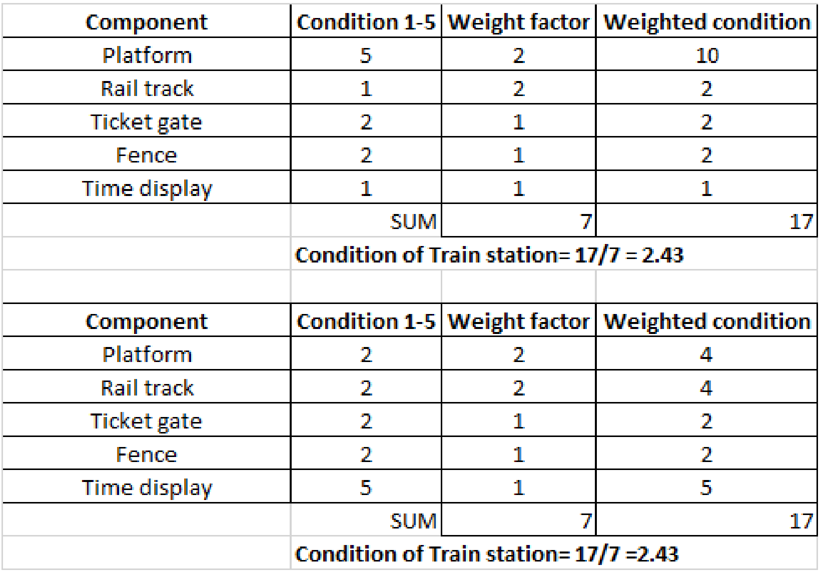


Component	Condition 1-5	Weight factor	Weighted condition
Platform	3	2	6
Rail track	3	2	6
Ticket gate	3	1	3
Fence	3	1	3
Time display	1	1	1
	SUM	7	19
	Condition of Train station= 19/7 = 2.71		

.

TABLE 2: SHOWS AN EXAMPLE OF CALCULATING THE CONDITION OF A TRAIN STATION

However, this method can be misleading as shown in Table 3 and 4, which shows that the condition of train station is 2.43[3] (i.e. fair condition), while its platform is in failure condition 5. Similarly, Table 4 shows the time display is in failure condition while the train station has the same condition with a failed platform in Table 3.



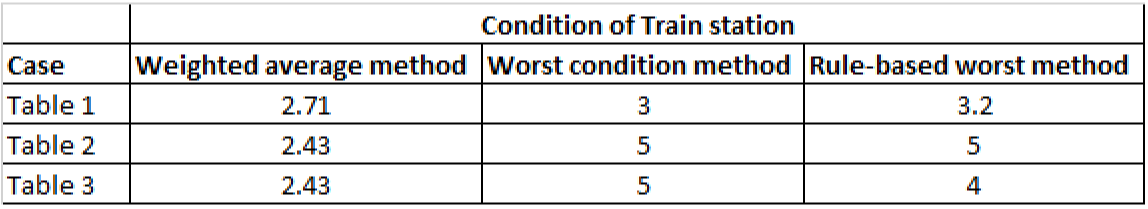
Component	Condition 1-5	Weight factor	Weighted condition
Platform	5	2	10
Rail track	1	2	2
Ticket gate	2	1	2
Fence	2	1	2
Time display	1	1	1
	SUM	7	17
	Condition of Train station= 17/7 = 2.43		

Component	Condition 1-5	Weight factor	Weighted condition
Platform	2	2	4
Rail track	2	2	4
Ticket gate	2	1	2
Fence	2	1	2
Time display	5	1	5
	SUM	7	17
	Condition of Train station= 17/7 =2.43		

TABLE 3: (UPPER) AND TABLE 4: (LOWER) CONDITION OF A TRAIN STATION.

ii- Rule-base worst method

This determines the condition of a train station by using a combination of the rule-based method and the worst condition method. Table 5 compares the rule-based worst method with the weighted average method and worst condition method. The weighted average method is already explained in Section (i). The worst condition method simply assigns the worst condition of components as the condition of train station. This worst condition method is unable to different Table 3 and 4. The rule-based worst method augments the worst condition method with the rule-based scores to differentiate between various conditions of components and their weight factors.



	Condition of Train station		
Case	Weighted average method	Worst condition method	Rule-based worst method
Table 1	2.71	3	3.2
Table 2	2.43	5	5
Table 3	2.43	5	4

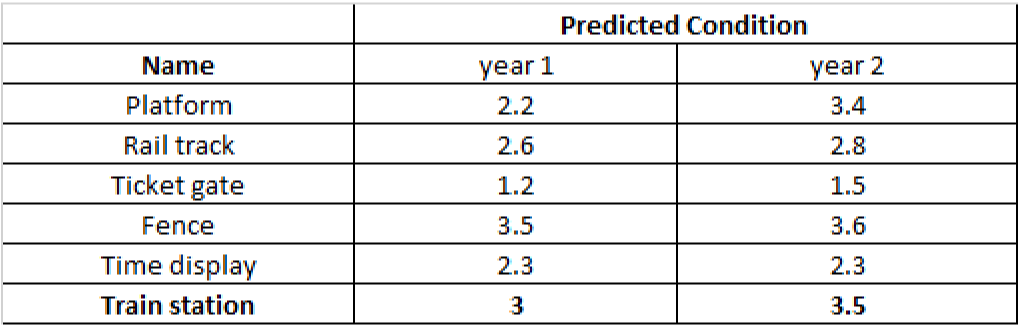
TABLE 5: COMPARISON OF DIFFERENT METHODS

2.3.6 Deterioration prediction of train station

The deterioration prediction of a train station can be derived from the predicted condition of its components and the rule-based worst method as explained in Section ii.

The predicted condition of components can be based on the Markov model[1] or other models such as linear and exponential model depending on data and model fitness. Table 6 shows predicted condition for components and the train station over period of 2 years as an example.

[1] Deterioration prediction of community buildings in Australia, HESSAM MOHSENI, 2012.



	Predicted Condition	
Name	year 1	year 2
Platform	2.2	3.4
Rail track	2.6	2.8
Ticket gate	1.2	1.5
Fence	3.5	3.6
Time display	2.3	2.3
Train station	**3**	**3.5**

TABLE 6: PREDICTED FUTURE CONDITION

2.3.7 Budget forecasts of maintenance

Budget forecast for maintenance of train station can be based on the predicted condition of its components as follows:

Budget of Train Station (year 1) = ∑ *Component qty * unit cost * predicted component condition*

2.4 Budget forecast and asset monitoring

The investment model needs to address IT assets as well as physical assets. The assets were classified according to the type of railway component in D3.1[57]. Accordingly, the classified asset list has been categorized and prioritized for input based on CAMS's needs[2]. The main goal is to keep the framework as general as possible, being able to work with both physical and cyber systems in the same way. This could include, but not be limited to, the following.

- Make sure that critical infrastructure data is kept secure by enforcing cyber security
- Guidelines and other methods to determine the severity of extreme events, hazards, and attacks on infrastructure.
- IoT sensors and live monitoring to ensure safety.
- Integration of large IT systems into various projects.
- Interdependency between infrastructure assets: e.g.: when an asset fails, others are affected.

The investment model needs to address IT assets as well as physical assets. The main goal is to keep the framework as general as possible, being able to work with both physical and cyber systems in the same way.

In the first place a definition on the condition rating for IT systems is needed. Condition ratings for physical assets are defined as having different levels of damage, the required repairs and the possible losses on their performance. In the case of IT systems the definitions of the different conditions for the rating scale have to be related to their level of update and security. As for physical assets, passing from one condition to the next will depend on time and on the maintenance activities. The establishment of the definitions of this condition for IT assets enable the use of the same normal degradation module as used for physical elements. A Markov-chain model can be trained to forecast the future conditions of the IT systems based on previous monitoring data of these elements. The main difference between physical and IT assets will be that the former losses performance over time and that the later only becomes more vulnerable to future attacks.

Further a state-dependent-fragility or vulnerability assessment is made on physical elements, in order to establish the damage condition after a disruptive event taking into account its previous condition. This type of analysis enables the calculation of the initial drop in the resilience curve and enables the analysis of different

[2] As an example, in Table 12, assets of CdM SE were categorised and prioritised according to asset classification guide on section 3.3 of Deliverable 3.1[57].

strategies to enhance resilience by improving maintenance. A similar type of analysis has to be made for IT assets, in order to do so definitions of the limit states are required. Limit states are boundaries between each damage condition defined in the rating scale. In addition, this type of analysis would require the description of cyber-attacks by means of an intensity measure (IM). This could be defined in a qualitative or quantitative way. Ideally this definition has to be related to the probability of occurrence.

This deliverable explores the different definitions required to treat physical and IT assets in a similar way, so they can be incorporated to the framework developed in WP7.

2.4.1 Budget forecasts of maintenance

Several condition rating systems exists for physical assets. Most of them are related to their damage condition, to the maintenance requirements or to the residual life (remaining life). Assessing the condition of an asset is crucial for taking decisions on maintenance, rehabilitation or replacement. Further, the forecast of the asset condition enables a better planning of resources and expenditures. Table 7 shows an example of condition rating for physical and IT assets. Visual inspection is commonly used to assess the condition of these assets through their visual defects such as cracking and corrosion for physical assets and noise and high core temperature for IT assets. With IT assets, percentage of useful life remaining can be used to estimate their condition if visual defects are not shown or difficult to be detected

Physical Assets			IT or Digital Assets		
Condition Rating	Asset Condition	Description	Condition Rating	Asset Condition	Description
C1	Very good	The element is as new, no damage or maintenance required. The performance is 100%.	C1	Very good	Completely updated; the asset is new. No maintenance required.
C2	Good	The element is sound; minor damage, minor maintenance required	C2	Good	Sign of deterioration such as fan noise, higher core temperature
C3	Moderate	Moderate damage; moderate maintenance required	C3	Moderate	Moderate deterioration signs or passing of mid service life point
C4	Poor	Major damage; major maintenance required	C4	Poor	Performance and reliability significantly reduced or nearing of end service life
C5	Very poor	Serious damage; the element should be replaced. 0% performance.	C5	Very poor	Failure or completely out-of-date; the asset is. Decommissioned and implementation of a new asset.

TABLE 7: PHYSICAL AND DIGITAL ASSETS

2.4.2 Condition monitoring

In the case of physical assets, the condition can be achieved in different ways. The typical way is by the visual inspections of technicians which are then formalised into preformatted reports. These take place regularly, and the time between inspections depends on the regulations and on the asset nature. For example, in the case of buildings these inspections can take place once every 5 or 10 years or, in case of rails conditions, it can take place every few weeks.

In the case of IT assets the condition monitoring can be carried out by remote scanning of the elements, and the time between inspections is shorter and depends on how fast these assets can change between conditions. TBC, basically how it is carried out in IT asset management.

3. Asset management and budgeting strategies

In most established asset management frameworks, operation and maintenance budgeting exclude disasters or extreme events and ageing. The focus of CAMS is to determine the budgeting strategies to assist asset management of rail assets in terms of increasing resilience index of rail assets and time and cost-effective recovery after an event which caused the damage including ageing issues. To derive budget strategies, CAMS require data and information on regular inspection and condition rating of rail assets, which are often carried out in most infrastructure asset management practices.

3.1 Resilience index before extreme-damage events (ageing)

To mitigate the impacts of extreme damage events, the resilience index (as defined in Section 2, 3) of rail assets should be above a threshold level to ensure normal operation and minimal impacts under damage events. To achieve the acceptable level of resilience index, rehabilitation budget should be derived to cover maintenance needs due to time-based deterioration processes and to cover strengthening of rail assets based under various scenarios of extreme damage events. In this study, CAMS is focused on determining the maintenance needs due to time-based deterioration. The strengthening option requires reliability assessment of rail assets under various extreme damage event scenarios, which might be carried out by other research teams. However, the strengthening budget can be easily imported into CAMS based on end-user-demand.

3.2 Time and cost-effective recovery after extreme-damage events

After an extreme damage event has occurred, inspection of damage is often carried out to identify asset conditions and recovery options, including do-nothing, minor repair, major repair and replacement. In this case, CAMS can produce estimated recovery time and cost in a prioritised planning based on inspection report and repair decisions by structural engineers.

3.3 Taxonomy of rail assets

Taxonomies for the assets and railway components have been classified[3] in SAFETY4RAILS to provide a preliminary overview of the elements that will interact during the asset assessment CAMS has capability to import and export and use data from other tools such as SecuRail which are connected to DMS. CAMS also allows project participants to input their data and edit or update it according to possible incidents.

CAMS input algorithms calculate both value and recovery time by categorising each element based on several attributes .

In the creation of taxonomies, the goal is to describe railroad infrastructure elements, potential attacks/incidents that could occur within them, and how to avert or limit their impact during the recovery phase .The framework, while designed for asset management, can be used in other tools and adopted as a reference for SAFETY4RAILS .

RMIT used asset taxonomies classified in D3.1 with specific categorization and prioritization prepared for CMAS input.

[3] See Asset list (ANNEX II) and Asset condition (ANNEX III), which were divided for CAMS input preparation in accordance with D3.1's asset classification guidelines[57].

Railway assets are considered as potential targets of certain incidents. Indeed, each asset can be hit by a threat which will cause an impact on the asset itself and on other connected assets and services.

Defining attributes of each asset is essential to implement a reliable estimation of the impact of each risk scenario. In CAMS, the end-user can create a predefined database of railway infrastructure assets or budget planning purposes. These can be derived by the end users from historical data on similar incidents or simulation tools.

4. CAMS framework

End-users are able to forecast budgets for maintenance and rehabilitation of normal degradation, strengthening of assets, and recovery after extreme damage events by using CAMS.

4.1 Normal degradation module

The normal degradation module of CAMS produces a budget forecast for routine maintenance of normal degradation of individual rail assets.

The normal degradation refers to time-based deterioration such as corrosion and fatigue of steel, carbonation and chloride attack on concrete and damage caused by truck overloading and other damage events that are not considered to be extreme events. CAMS requires the normal degradation of individual rail assets to be inspected regularly and then rated using 4 or 5 condition states.

The Markov chain model is used by CAMS to derive deterioration curves for individual rail assets based on inspection and condition rating data. A component of the condition rating is the progress on routine maintenance options including monitoring, minor repair that can escalate to major repair and replacement based on the inspection report. A failure condition may be associated with a replacement action.

The budget for routine maintenance can be determined based on the deterioration prediction by the Markov model and the cost of corresponding maintenance options over any selected planning horizon of typically 5-20 years. It should be noted that a Markov prediction for longer planning horizon is possible but is not accurate due to the constant improvement in repair technology and material.

4.1.1 Condition rating and inspection methods

It is recommended that individual rail assets should be inspected regularly to ensure service performance and structural safety. The inspection frequency depends on the current condition and the type and material of assets. As described in earlier sections, visual inspection is still commonly used within infrastructure asset management. Based on inspection reports, individual rail assets can be rated using four or five condition states, which represent the level of deterioration and damage and corresponding maintenance options. The Table 8 below presents an example of a rating of 5 condition states.

Condition	Description	Corresponding maintenance action
1	Brand-new like or Good	Do-nothing
2	Fair: show minor signs of deterioration that should be monitored.	Monitoring
3	Poor: show signs of deterioration that should require a minor repair to avoid escalation.	Minor repair

4	Very Poor: shows significant deterioration that should be a major repair or replacement.	Major repair
5	Failure: needs to be replaced immediately	Replacement

TABLE 8: AN EXAMPLE OF CONDITION RATING OF RAIL ASSETS WITH 5 CONDITION STATES

4.1.2 Markov-chain model

Among the deterioration models in the current research literature, the stochastic Markov chain model is found to be suitable for modelling the deterioration process of infrastructure assets with a random element coming from the local variation of the surrounding environment and uncertainty of construction. The suitability of the Markov chain model includes:

- The ability to directly model the discrete condition data using ordinal numbers (*e.g. condition 1 is very good and condition 2 is fair and so on*) currently used by industry to rate the overall condition of infrastructure assets. The rated condition in a particular year is expressed by condition 1 for that year;
- The ability to capture the stochastic process of a time-based deterioration mechanism and the random damage events as observed with the discrete condition data. For example, visual inspection and condition rating might show that condition 1 (*very good*) of an asset is unchanged over a period of 10 years, which is an indication of slow deterioration. It might show that condition 1 moves to condition 4 (*very poor*) over a period of 2 years, which indicates an occurrence of a random damage event such as flooding or earthquake or a very fast corrosion process. This is expressed by the transition probability *Pij* to move from condition i to condition *j>=i* over a unit time by the discrete state Markov model. For example, *P11* of 0.98 means a relatively slow deterioration process with less chance of a random damage event while P14 of 0.2 means a reasonably high likelihood of random damage event;
- The ability to predict an average rate of network deterioration for a large network of assets such as bridges or culverts. Such predictive information can be useful for maintenance budget planning and an accounting report of asset depreciation. For example, the probability in various condition states of a network at any future year can be predicted by the Markov model such as [80% 10% 5% 5% 0%] for condition [1 2 3 4 5] respectively. This means that at that particular year in the future, 80% of network can be in condition 1 and 10% in condition 2 and so on.

The Markov model (*Ross, 2000*)[10]can simulate the deterioration process by using a discrete condition state (captured during the deterioration process through inspection) and transition probabilities between the deteriorated states.

The model is based on the assumption that the future condition state of an asset is dependent on the current condition (*i.e. memory-less*) and is expressed as a probability *Pij* that an asset can move from condition i at year t to condition *j* at year *t + 1*. Since condition data of culverts have 5 condition states, a 5x5 transition probability matrix M can be established as shown in Equation (1). The Markov model can capture a gradual deterioration process through transition probabilities *Pij* when *j=i* or *j=i+1* (*e.g. P11 and P12*) and mild to extreme damage events through transition probabilities *Pij* when *j>i+1*(*e.g. P13, P14 and P15*). Furthermore, the probability *Pij* is zero when *j<i* meaning that the deterioration process is not reversed nor maintenance applied. Equation 2 shows the *Kolmogorov* equation (*Ross, 2000*) for predicting the future condition given the current known condition (shown in Equation 3) and transition matrix M.

$$\boldsymbol{M} = \begin{bmatrix} P_{11} & P_{12} & P_{13} & P_{14} & P_{15} \\ 0 & P_{22} & P_{23} & P_{24} & P_{25} \\ 0 & 0 & P_{33} & P_{34} & P_{35} \\ 0 & 0 & 0 & P_{44} & P_{45} \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \qquad (1)$$

$$\boldsymbol{P}^{t+1} = \boldsymbol{P}^{t} * \boldsymbol{M} \qquad (2)$$

$$\boldsymbol{P}^t = [p_1^t, p_2^t,\ p_3^t,\ p_4^t,\ p_5^t] \quad (3)$$

where p_i^t is probability in condition *i* at time *t* and *i*=1 to 5.

4.1.3 Transition matrix determination

The transition matrix M can be calibrated using the simple frequency method or the sophisticated optimisation method.

- The simple frequency method is based on the frequency equation:
- *Pij = Nij / Ni*

Where *Nij* is the number of assets that shift from state i to state j during one step and *Ni* is the total number of sections that were in state i before the transition. Let us suppose the following case:

- Category/Condition class 1: 10 assets
- Category/Condition class 2: 20 assets

After one cycle, for example one year, from the 10 assets in condition 1, 6 remained in the same category and 4 shifted to a worse condition, class 2. Hence, the elements of the TPM would be: *p11 = 0.6, p12 = 0.4*. This is the way to develop TPMs. Obviously, as seen, it is necessary to have assets in all the classes to see how they shift after a cycle. If not, it is possible to observe some section during more cycles to observe the deterioration of the section in worst conditions.

The sophisticated optimisation method is based on Equations 1-3 that search for *Pij* that can minimise the error between observed and predicted number of assets in each condition rating class. The validation of Markov model is based on Chi-square test by separating sample data into calibration data (80%) and validation data (20%) (*Micevski, et al., 2002[9]; Tran, 2007[8]*). The validation dataset is not used in the calibration process. The test hypothesis, with the test statistics being the Chi-square value, is that the observed frequency is consistent with the predicted frequency for a particular condition rating at a particular observed age. The Chi-square value   for the Markov model can be calculated using Equation 4 (*Micevski, et al., 2002*)[9]:

$$\chi_M^2 = \sum_{i=1}^{5} \frac{(O_i - E_i)^2}{E_i} \quad (4)$$

Where *Oi* is observed number of elements in condition i and Ei is predicted number of elements in condition i. If the test statistic   is larger than the critical value of Chi-square distribution at 95% confidence level and a specified degree of freedom, the hypothesis is rejected. The degree of freedom is calculated as (row number-1) multiplying with (column number -1) where row number is number of observed ages and column number is number of observed condition states at an observed age.

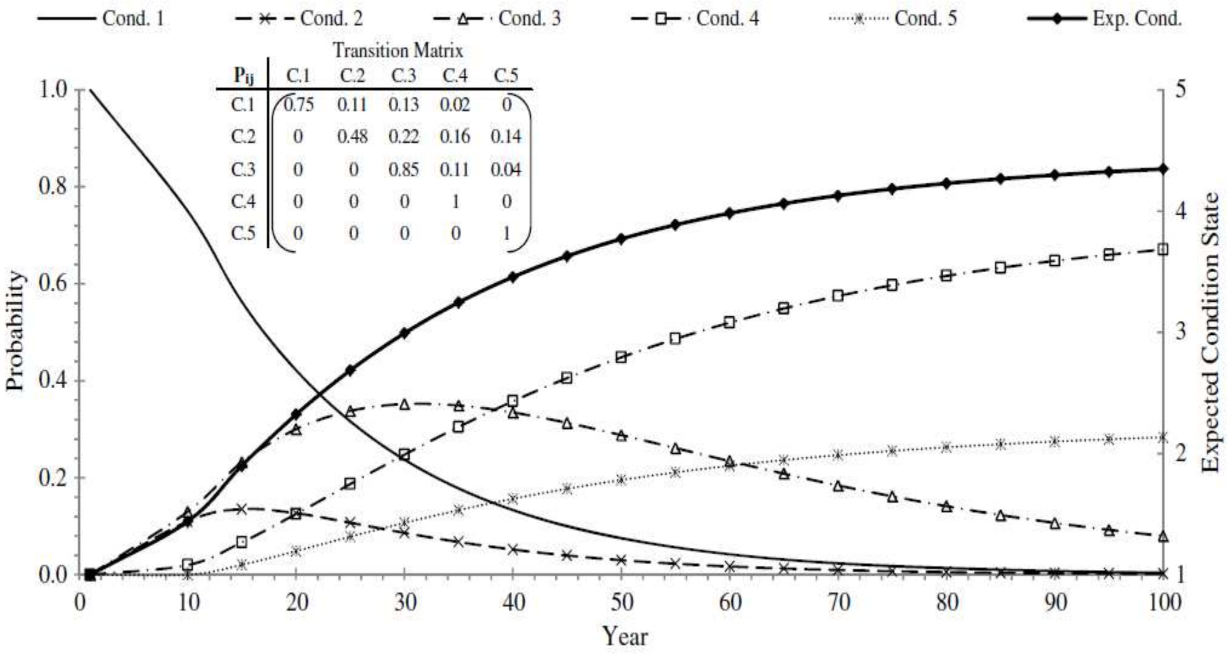
4.1.4 Deterioration prediction module

CAMS has a Markov deterioration model for each rail asset (e.g. rail track, door), but other deterioration models such as linear and non-linear models can also be considered. **Figure 4** shows the prediction of deterioration by the Markov model for an asset, which has 5 condition states with one being brand-new like and 5 being the worst or failure state. The left vertical axis shows probability value while the vertical axis on the right-hand side shows the expected condition similar to the 5 condition states of the asset.

For the left vertical axis, there are 5 deterioration curves for 5 condition states and corresponding probability values over time in year. The curve of condition 1 starts at 100% probability at year 0, meaning the asset is assumed to be 100% in condition 1 at the start of its service life (i.e. age zero). As the age of the asset increases over time, the asset deteriorates with the decreasing probability in condition 1 and increasing probability in the poorer conditions. The focus is on deterioration curve of the worst condition 5, which shows mild slope for this particular example in FIGURE 4, meaning slow deterioration.

For the right vertical axis, the expected condition is the weighted average of 5 condition states of the asset over time, which is shown in the thick continuous line. For example, at year 50, the probabilities in 5 conditions states can be read from the curve as [0.05 0.1 0.3 0.4 0.15] and the expected condition is calculated as 3.9 out of 5. The expected condition is used to make it easier to understand the deterioration curve of the asset as compared to the 5 probability curves.

The probability curves for 5 condition states can also be used for a cohort of assets that have similar attributes such as rail tracks or concrete floor. For example, taking again the year 50 and rail tracks of 1000 linear meters, the probabilities [0.05 0.1 0.3 0.4 0.15] in 5 condition states can imply that there are [5% 10% 30% 40% 15%] or [50 100 300 400 150] meters of rail tracks in 5 condition states respectively. This information can be used for forecasting of maintenance budget. It should be noted that the Markov model can not predict which particular assets are in which conditions. This shortfall can be addressed through regular inspection.



Transition Matrix

P_{ij}	C.1	C.2	C.3	C.4	C.5
C.1	0.75	0.11	0.13	0.02	0
C.2	0	0.48	0.22	0.16	0.14
C.3	0	0	0.85	0.11	0.04
C.4	0	0	0	1	0
C.5	0	0	0	0	1

FIGURE 4: TRANSITION MATRICES – MARKOV PROCESS

Mohseni, H.; Setunge, S.; Zhang, G.; Wakefield, R. Markov Process for Deterioration Modelling and Asset Management of Community Buildings. J. Contra Eng. Manag. 2017, 143, 04017003[6].

4.2 Fragility module

The investment assessment model developed in the context of the SAFETY4RAILS project, relies on the accurate calculation of the damage (or performance loss) suffered after a disruptive event. The nature of this event may be a natural hazard or a terrorist attack which can be cyber, physical or a combined attack. In addition, the damage assessment has to take into account the initial damage due to the normal ageing of the elements.

Depending on the element, when it is degraded in different years after its creation (disruptive event origination) and depending on the type of disruption event (threat) CAMS make a fragility analysis for different intensities of the event. FIGURE 5 shows the example of fragility curves of a physical asset for three scenarios of its aging at 30 years, 60 years and 90 years. The figure shows that with aging, the probability of exceeding the damage level for 5 condition states is increased under same intensity level of damage events

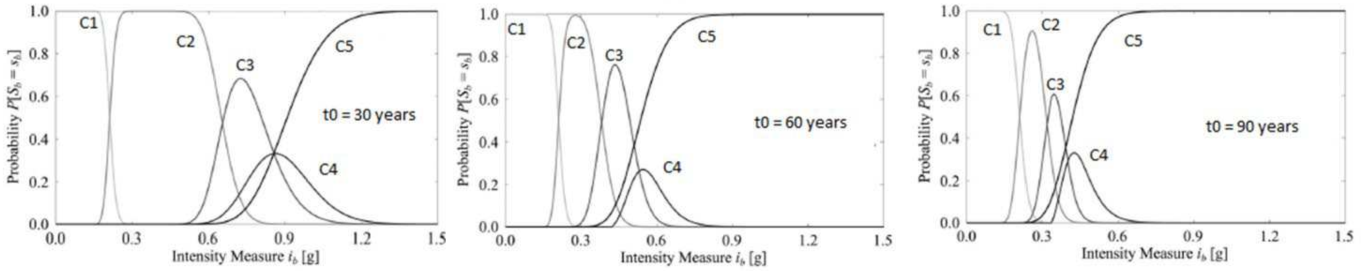


FIGURE 5: FRAGILITY CURVES [6]

Furthermore, the impacted components might be of different type, for example it can be a physical element such as bridges, rails, rolling stock, or it can be a soft element such as the information and control systems.

The fragility module has to be integrated into the framework after the normal degradation module Mohseni[6] et al. (2017). The input of this module is going to be the initial damage condition and the type and intensity of the disruptive event as shown in FIGURE 6. The outcome is the final damage condition after the incident.

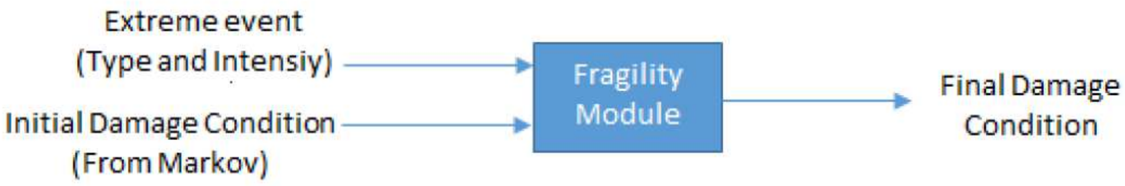


FIGURE 6: FRAGILITY MODULE

4.2.1 Fragility analysis

In order to determine the damage after a disruptive element a fragility analysis is needed. Fragility analysis are common practice in earthquake engineering *Capacci* and *Biondini(2020)*[5], it consists of the determination of fragility functions that express the probability of reaching or exceeding a level of damage at a given intensity measure of the disruptive event. This approach has been recently extended to other types of loads or natural hazards such as wind or wave loads *Qeshta et al. (2019)*[7].

For an intact element, four fragility functions are required each one for a different limit state (slight, moderate, extensive and complete). Each one of these limit states represents the boundary between the damage conditions considered in the Markov model for normal degradation. Thus, once the limit states fragility functions are obtained, the probability of being in certain condition is straight forwardly calculated. See FIGURE 7

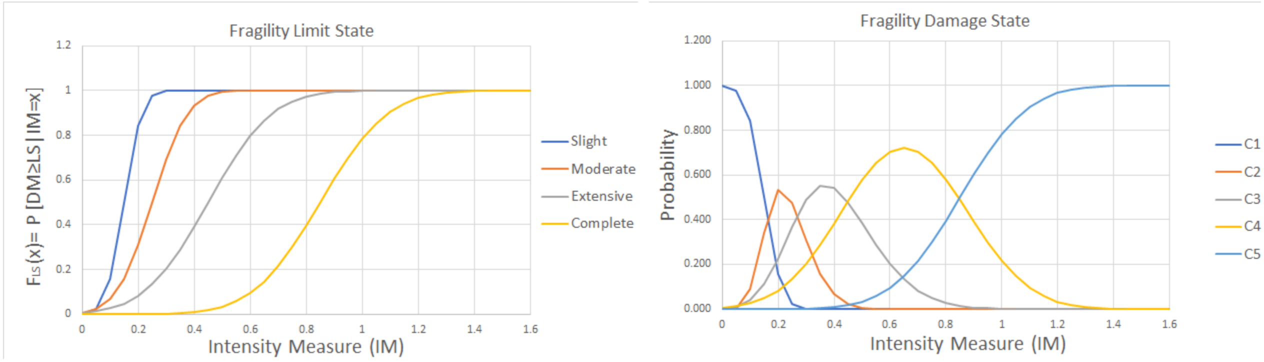


FIGURE 7: FRAGILITY ANALYSIS

To take into account the normal ageing of the elements, the same analysis has to be repeated for each incident of damage in its initial condition. The fragility analysis can be made by different methods: experimental fragility functions based on experimental data; empirical fragility curves based on survey data; judgmental functions based on expert's judgment; numerical simulations or analytical models. The last of this type of analysis is the most used in earthquake engineering where a finite element model of the structure is submitted to different levels of the earthquake motion measuring the damage. This approach might be impractical for our purposes due to the extensive number of elements considered the different nature of the hazards and the different nature of the elements (physical or digital).

Another aspect to be analysed is uncertainty. Fragility analysis can be made taking into account uncertainties at two stages, from the event itself and from the response of the element. Otherwise, a deterministic and simpler approach can be followed. In this way the fragility functions became simply a step function. Intermediate options can be followed using semi-probabilistic approaches (See FIGURE 8).

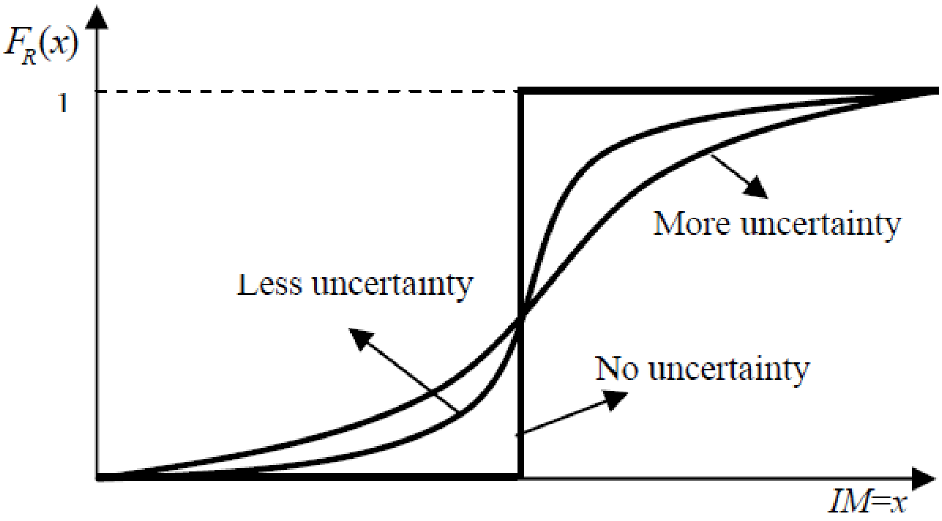


FIGURE 8: UNCERTAINTY

Finally, the interaction between cyber events and physical elements must be addressed. A first idea is to treat physical and soft elements in the same way. Also the different threats have to be considered similarly. Thus a cyber-attack has to be measured in some way in order to have an intensity measure. The cyber-attack will have an impact on soft elements but also it may produce damage to physical assets. For instance, a cyber-attack of a certain level impacting on the control system will affect not only the control system itself but also the rolling stock as it may cause a derailment.

From the previous analysis it follows that for a given element of the system; a fragility analysis has to be made for each one of the possible disruptive events. Further, each fragility analysis has to be repeated four times, taking into account the previous damage due to normal ageing. It can be seen that the number of elements makes it impractical to perform an analytical analysis for each one of the elements. Nevertheless, as the framework aims to be as general as possible, for some elements and types of events a simplified analysis will be enough and leaving open the possibility to carry out closer studies for particular elements and events.

4.2.2 Proposed approach

As was previously stated, fragility analysis has to be as simple as possible in order to be feasible but without losing generality. In that way a deterministic or a semi-probabilistic approach has to be taken.

The scale of terrorist attacks as cyber, physical or combined attacks can be divided into intensity levels. Natural hazards might be characterised by means of specific intensity measures such as peak ground acceleration for the case of earthquakes.

The simplified fragility functions for an intact element can be seen in the FIGURE 9.

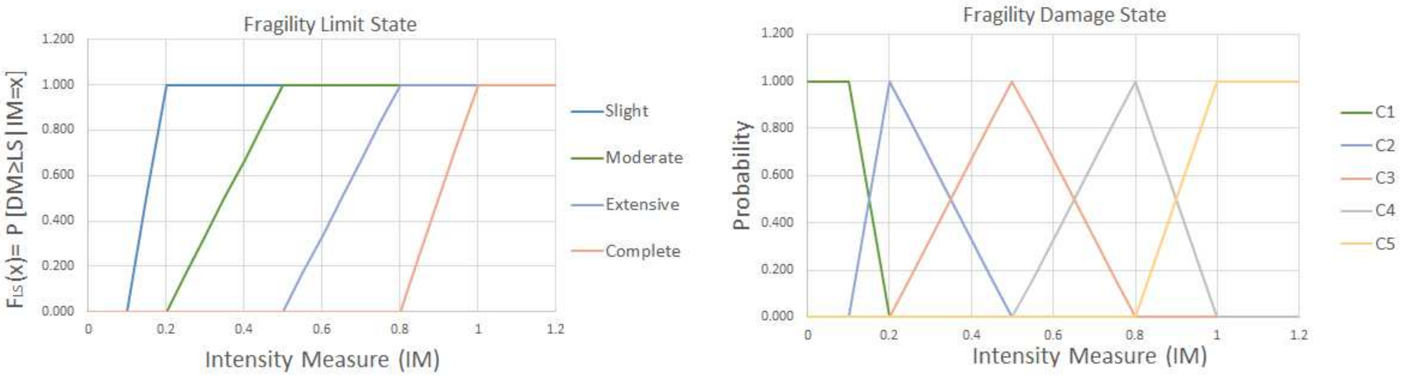


FIGURE 9: SIMPLIFIED FRAGILITY ANALYSIS

Fragility analysis consists of the determination of fragility functions that express the probability of reaching or exceeding a level at damage at a given intensity measure of the disruptive event. For an intact element (C1 damage condition), four fragility functions are required, each one for a different limit state (slight, moderate, extensive and complete), see FIGURE 9(right). These curves represent the probability of reaching a defined limit state for a given level of the disruptive event. Each one of these limit states represents the boundary between the five damage conditions considered in the condition rate. Thus, the probability of actually being in a certain damage condition after the event can be obtained by simple operation of the previous curves, see FIGURE 9(left). Afterwards, the combination of the probabilities will give the most probable condition after an event, FIGURE 10.

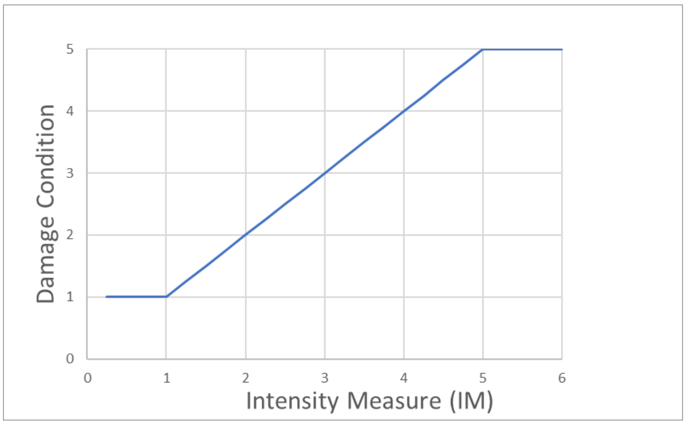


FIGURE 10: DAMAGE CONDITION

The previously described analysis has to be repeated for each initial damage condition. In this way the effect of previous damage and the responsive mitigational capability of an asset would be effectively considered. The outcome, would be five curves of expected damage condition after the event, see FIGURE 11.

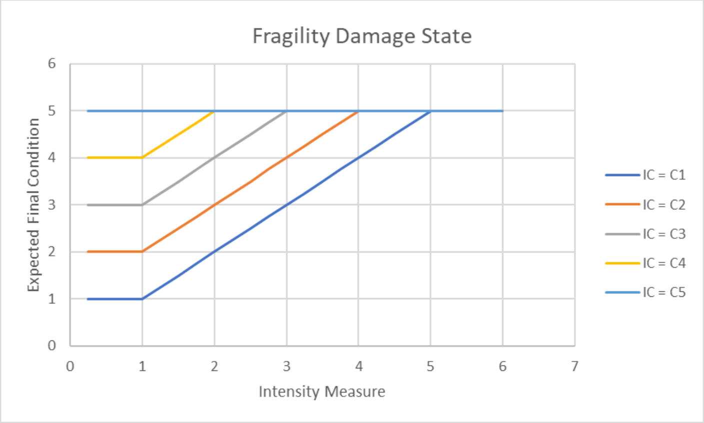


FIGURE 11: STATE-DEPENDENT FRAGILITY ANALYSIS

In the case of physical assets, this analysis first concerns the definition of the limit states which comes directly from the definition of the damage conditions. Then, the disruptive event must be defined by means of intensity measures. In the case of natural hazards, such as earthquakes, tsunamis, storms, this intensity measure is a physical variable which may be peak ground acceleration (*in the case of earthquakes*) or the maximum wave height (*in tsunamis*). These variables are also characterised in a probabilistic way, so each intensity is related to a probability of occurrence in a given context.

In the case of IT asset and cyber-attacks, a definition of the limit states and the intensity of cyber-attacks must be made. The intensity measure of the cyber-attacks cannot be carried out in a quantitative way; the qualitative definition of different events must be made. A possible approach is to define five different intensities (from very low to very high) related to the probability of occurrence during the lifetime of the asset (See Table 9).

An alternative is to obtain curves by means of expert judgement, which involves expert opinion of a certain asset to assess the probability of being damaged after an event. This approach even if less accurate is generally applicable and can be applied to a large number of assets.

Attack	**Very Low**	**Low**	**Medium**	**High**	**Very High**
	Prob. [95%]	**Prob. [75%]**	**Prob. [50%]**	**Prob. [25%]**	**Prob. [5%]**
Cyber					

TABLE 9: ATTACK PROBABILITY

The open point for the IT assets would be if this fragility analysis can be implemented and be the most efficient. The solution in CAMS development is to categorise IT assets and physical assets based on different priority levels.

The effect of previous damage will have an impact on the fragility functions; first some fragility curves will disappear or become trivial. For example, if the element is already in damage condition 2, it means that the first limit state has been reached. Then the other effect will be a shift of the curves towards the left. This means that the same event will produce greater damage to those elements that are in the worst initial conditions. Table 10 shows the 5 levels of impact on the asset due to a cyber-attack event.

	Impact on the asset
0	*- Not Affected*
1	*- Aesthetic*
2	*- Compromised - still works*
3	*- Compromised - doesn´t work - need small reparation -substitution of pieces*
4	*- Compromised - doesn´t work - need severe reparation -substitution of element*

TABLE 10: INTENSITY MEASURES / IMPACT ON THE ASSETS

4.3 Budget and investment module

CAMS has developed a model for analysing risk mitigation and recovery investments. As mentioned in D7.5, the investment assessment model analyses the cost-benefit of risk mitigation and recovery, and the current deliverable and resilience assessment model was used to generate budget planning results in D7.4.In order to improve investment management, 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. The following are some of the major objectives of the CAMS tool. This prediction is based on the normal deterioration of railway assets due to age and the unpredictability of cyber-physical incidents. CAMS calculates maintenance/repair Time and Budgets Scenario (as shown in FIGURE 12) for railway/subway components in case of a cyber-physical attack or ageing. Aspects of deterioration were also considered by CAMS during any incidents (which took into consideration ageing issues) and after incidents (discussed in D7.3).

In case of a cyber-physical event, CAMS through the S4RIS enables end-users to identify weak and strong points in their infrastructure. CAMS is then 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.

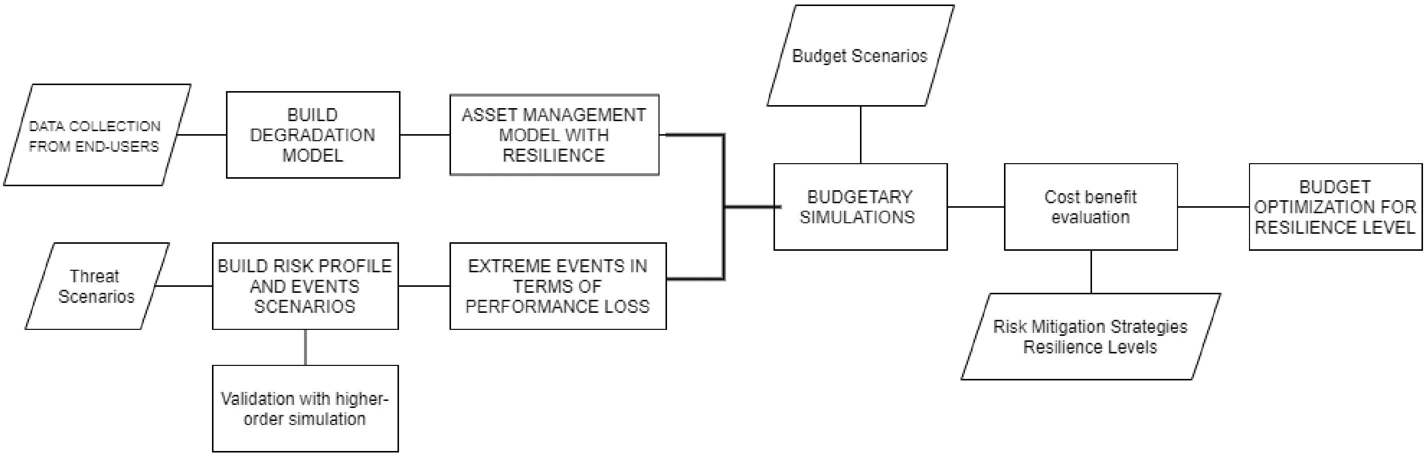

Budget Scenarios
DATA COLLECTION FROM END-USERS
BUILD DEGRADATION MODEL
ASSET MANAGEMENT MODEL WITH RESILIENCE
BUDGETARY SIMULATIONS
Cost benefit evaluation
BUDGET OPTIMIZATION FOR RESILIENCE LEVEL
Threat Scenarios
BUILD RISK PROFILE AND EVENTS SCENARIOS
EXTREME EVENTS IN TERMS OF PERFORMANCE LOSS
Risk Mitigation Strategies Resilience Levels
Validation with higher-order simulation

FIGURE 12: INVESTMENT ASSESSMENT MODE [58]

4.3.1 Budget module

Budget policies will affect the process in a different way, and in accordance with maintenance plans, the normal deterioration of the building will also be affected in a different way as well. Performance of each of the fundamental components (the leaves in the graph model) indirectly depends on natural conditions and disaster effects caused by potential hazards. This cost model reflects the number of resources needed to fully restore each component. This is outlined in Work Package 7 and is formalised in FIGURE 13[7].

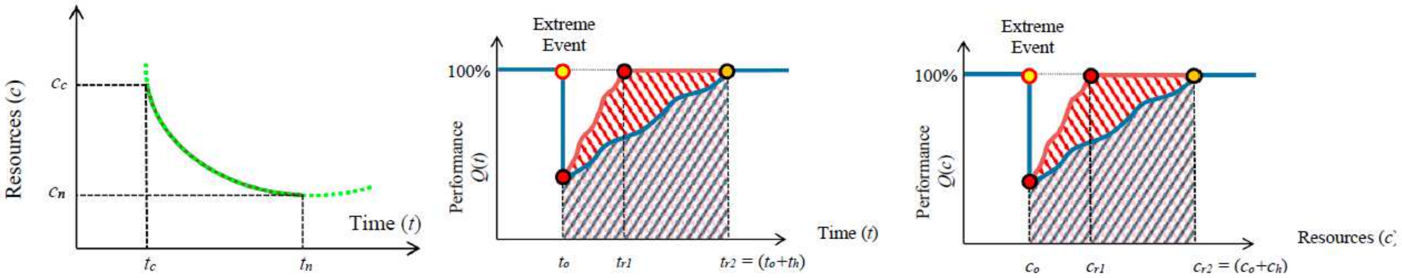


FIGURE 13: PERFORMANCE IN TERMS TO COST CONSUMPTION

FIGURE 14 shows an example of probabilistic deterioration curves that can be used in budget module. The left vertical axis shows probabilities in 5 condition states at any time point in the assets' service life. The right vertical axis shows the expected condition, which is often a weighted average of the probabilities of 5 condition states. The expected condition is a deterministic value that can be used for reports and financial valuation. This will influence the fragility module, as the event will occur under different initial conditions, therefore the reaction plans will have an impact on the performance curve.

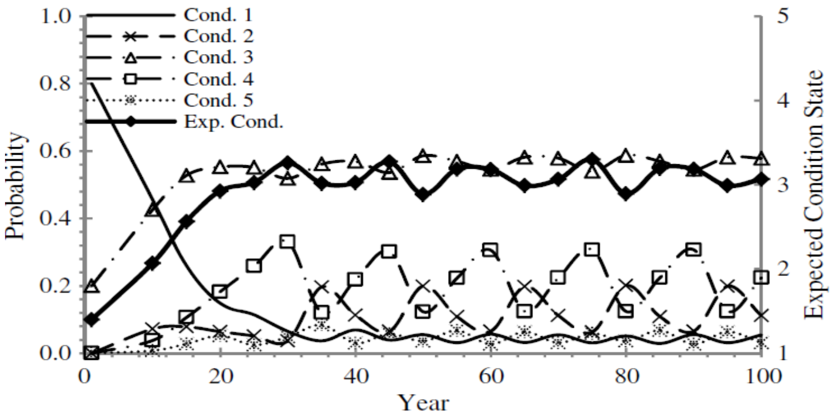


FIGURE 14: COMPONENT EXPECTED CONDITION STATE

CAMS output covers maintenance and repairs, rehabilitation and refurbishment, retro-fitting and replacing affected components as well as the overall budget.

4.3.2 Predictive cost

CAMS can provide cost prediction for maintenance against normal deterioration, strengthening of assets for improving resilience index and recovery cost after extreme damage events.

The cost prediction for maintenance against normal deterioration is based on deterioration prediction by Markov model. For example, the Markov deterioration prediction can be [60% 20% 10% 5% 5%] in conditions 1, 2, 3, 4,5respectivelyin a future year T.

For a cohort of assets, the percentage prediction means the percentage of assets in these conditions. For a particular asset, the percentage means probabilities in these conditions.

If the required parameter is the costs to repair these conditions are known as Cst1, Cst2, Cst3, Cst4 and Cst5 with Cst1=0 for do-nothing, then expected cost can be calculated as the total expected cost:

*Cost = Number of assets N * (Cst1*60%+Cst2*20%+Cst3*10%+Cst4*5%+Csts5*5%)*

The cost prediction for strengthening of asset for improving resilience index can be calculated as:

∑ *(strengthening asset(i) * cost(i)).*

The prediction of recovery cost after extreme damage events can be calculated as follows. Suppose that conditions of assets before the extreme event is [60% 20% 10% 5% 5%] for conditions 1, 2,3,4,5 respectively at a current year (by inspection) or a future year T (by prediction).

In the extreme event of bombing, the damage rule is that if assets are in condition 1, the after event, asset condition are changed to condition 4 and all other conditions would move to condition 5.

Then condition after the extreme event becomes [0% 0% 0% 60% 40%], the recovery cost can be calculated as *Recovery cost = N * (Cst4*40% + Cst5*60%)*

The results will include a comparison between:

- Before: all assets go to C5 regardless the impact on the asset
- New feature after “fragility analysis”: not all the assets go to C5 so not all of them will need renewal
- More accurate predictive cost

4.3.3 Maintenance, Repair and Rehabilitation Cost

Once all required information including condition before and after incident, cost of repair/replacement etc. is uploaded an output in FIGURE 15 below can be produced. The life cycle model includes the replacement/repair cost of the asset due to incident as well as cost resultant of replacing assets due to natural deterioration. As can be seen from the figure, the resultant profile includes a cost spike for the year of incident occurring (e.g. 2022, 2032 and 2042) and repetitive costs due to natural deterioration in the years after that. These costs are accelerated due to the incident that occurred. It is also possible to include a budget that is available for the disaster recovery phase. With this budget a backlog calculation can be carried out to see if that available budget is enough to support bringing the station to a working condition.

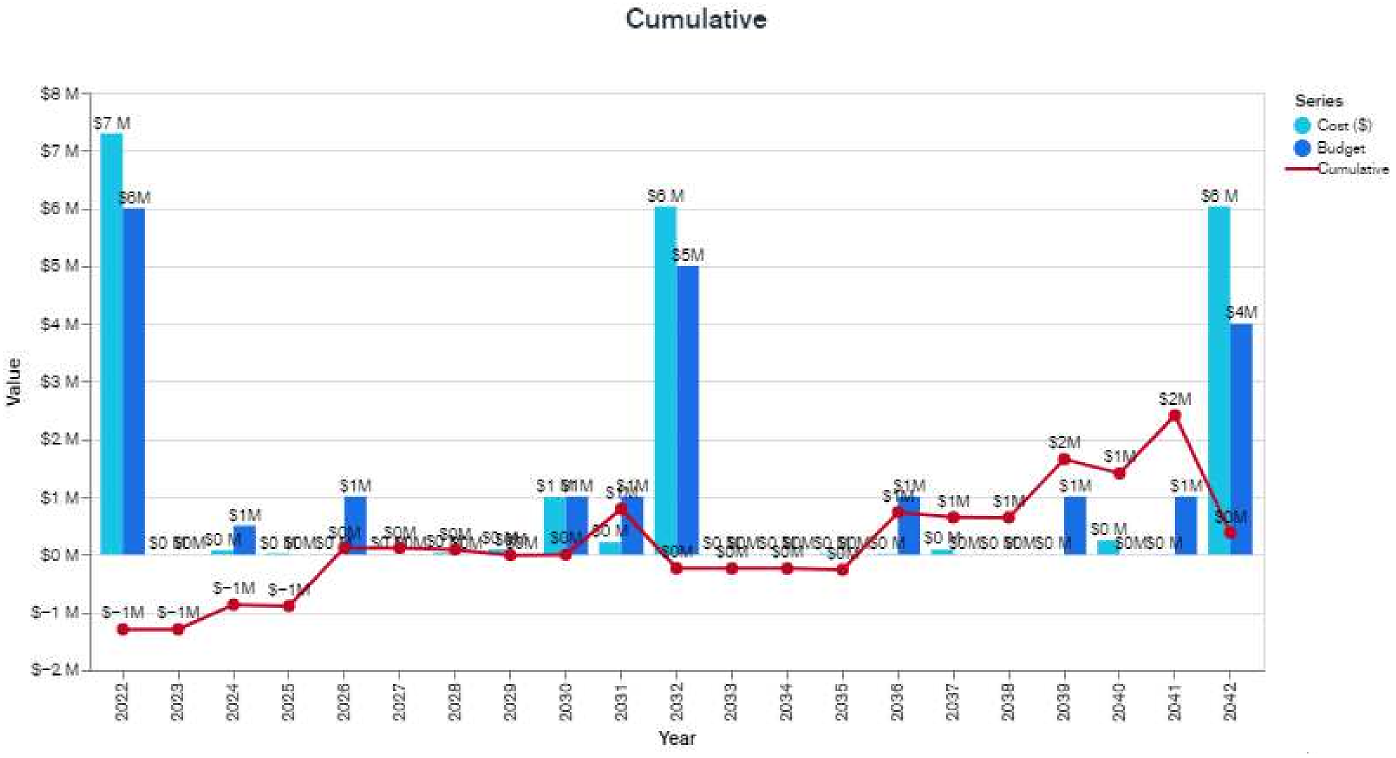


FIGURE 15: COST PREDICTIONS WITH CUMULATIVE BACKLOG

In the cumulative budget graph, the backlog due to the incident is explored. The above image shows the planned budget as well as the cost that is required after the incident. The cumulative difference between these two figures provides the back log curve in red. In an ideal scenario the backlog graph needs to be on the positive side if the station is to recover fully over time.

4.4 Resilience module

Conceptually, the resilience index is the area ABC as shown in the FIGURE 16, where A is the point of condition just before the occurrence of the extreme event, B is condition after the extreme event completed and C is the recovery point after repair action. Based on the concept of resilience, the resilience index can be calculated using the equation below.

$$R_1 = \frac{1}{t_h} \int_{t_o}^{t_o+t_h} Q(t)dt$$

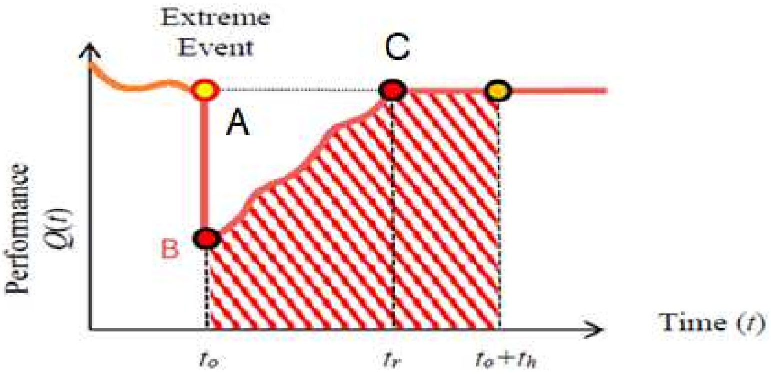


FIGURE 16: DAMAGE-PERFORMANCE CURVE [7]

CAMS resilience module calculates the resilience index of a rail asset by using its rated condition because the asset condition is related to time and cost of recovery. For example, the failure condition requires more time and cost to replace than the repair for poor condition. Other factors such as size, material, cost and function of the asset also affects the resilience index of the asset. To account for such contributing factors, the resilience index of a rail asset can be calculated as:

*RI = 100/(Cond*Dt*Dc)*

Where *Cond* is the asset condition rated between 1-5, *Dt* is the time factor with values of 1,2 and 4 for increasing recovery time, *Dc* is cost factor with values of 1,2 and 4 for increasing recovery cost and *RI* is resilience index between 1-100.

The resilience index for a train station, which is a system of many components, can be calculated based on the resilience index of its components and the rule-based worst method as described in Section 2. The FIGURE 17[7] shows the diagram for resilience index of a system.[4]

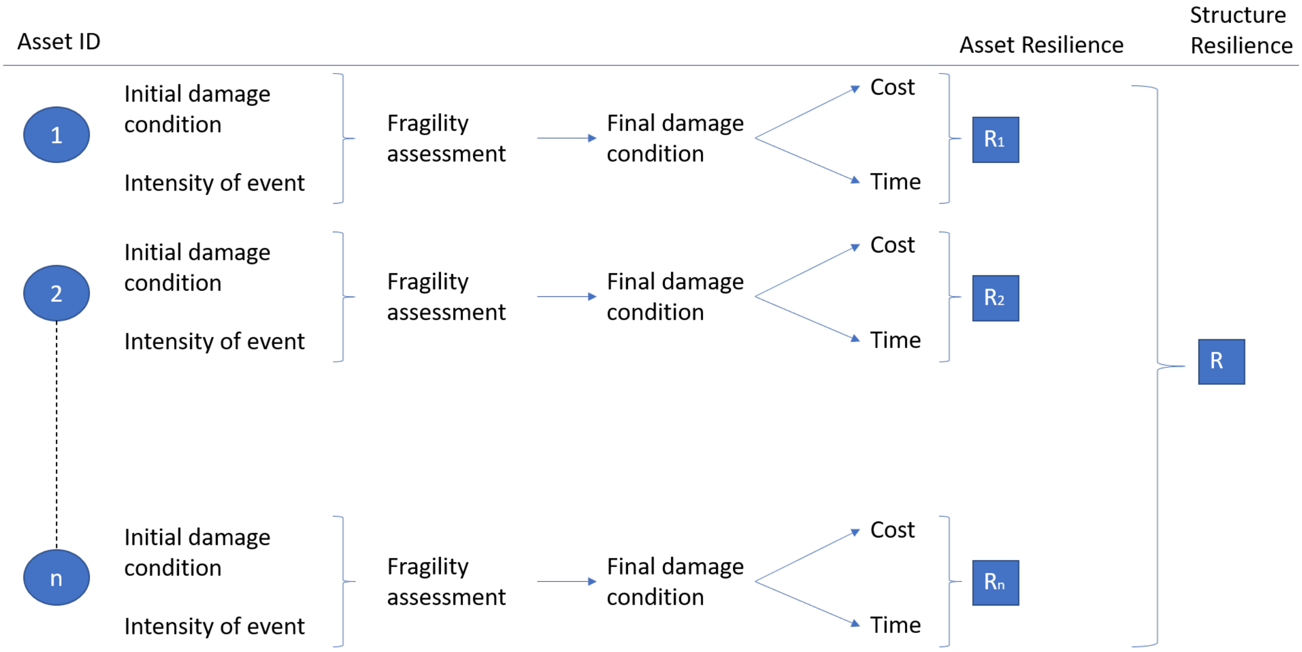


FIGURE 17: ASSET RESILIENCE DIAGRAM

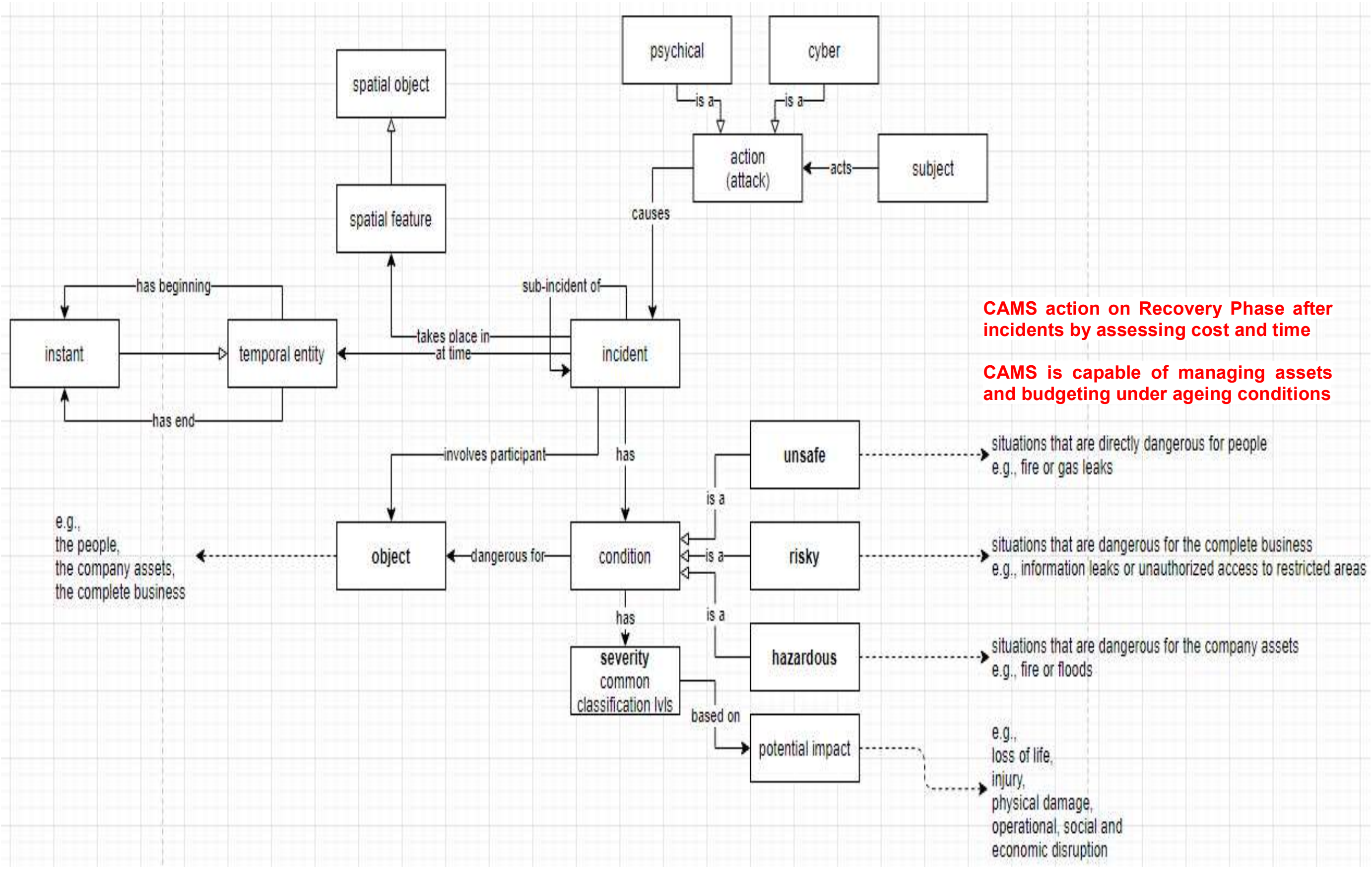
To align the unit of measurements, time can also be assessed as $ lost per each hour of out of service.

[4] Qeshta, I. M., Hashemi, M. J., Gravina, R., & Setunge, S. (2019). Review of resilience assessment of coastal bridges to extreme wave-induced loads. Engineering Structures, 185, 332-352.

5.Prevention, Detection, Response and Mitigation

The decision provided by a Whole of Life Asset Management System (eg: CAMS) is based on the resilience of infrastructure in a particular region, which is gathered using historical data and event data. CAMS enables managers to evaluate various analysis reports related to asset deterioration, risk, and budget forecasting. Thus, they enable making informed decisions regarding maintenance and budget allocations.

CAMS combines intelligent inspections with data analytics to offer an optimised life cycle management system that also includes budget planning. CAMS is able to work on infrastructure such as buildings, drainage assets, bridges, and railways. SAFETY4RAILS expanded the concept to include railway assets, digital assets, and planned assets. A further improvement to the current system is its resilience to extreme incidents, such as combined terrorist attacks. FIGURE 18 shows the working diagram of CAMS, which covers both normal deterioration and extreme attack events.



CAMS action on Recovery Phase after incidents by assessing cost and time

CAMS is capable of managing assets and budgeting under ageing conditions

FIGURE 18: CAMS ROLE IN DATA MODEL INCIDENT [61]

Through S4RIS's DMS platform, the data collected by the tool providers can be exchanged. Secondary data can be collected from past studies and historical events whenever possible. Various components of the S4RIS, notably the monitoring, simulation, and risk assessment tools, can specify and define the exact nature of the data to be gathered.

Regarding the SAFETY4RAILS project, the outcome also includes the cost of replacing assets during ageing issues or a threat situation were classified on D3.1 (shown in FIGURE 19) as well as the repercussions it has on the existing lifecycle model.

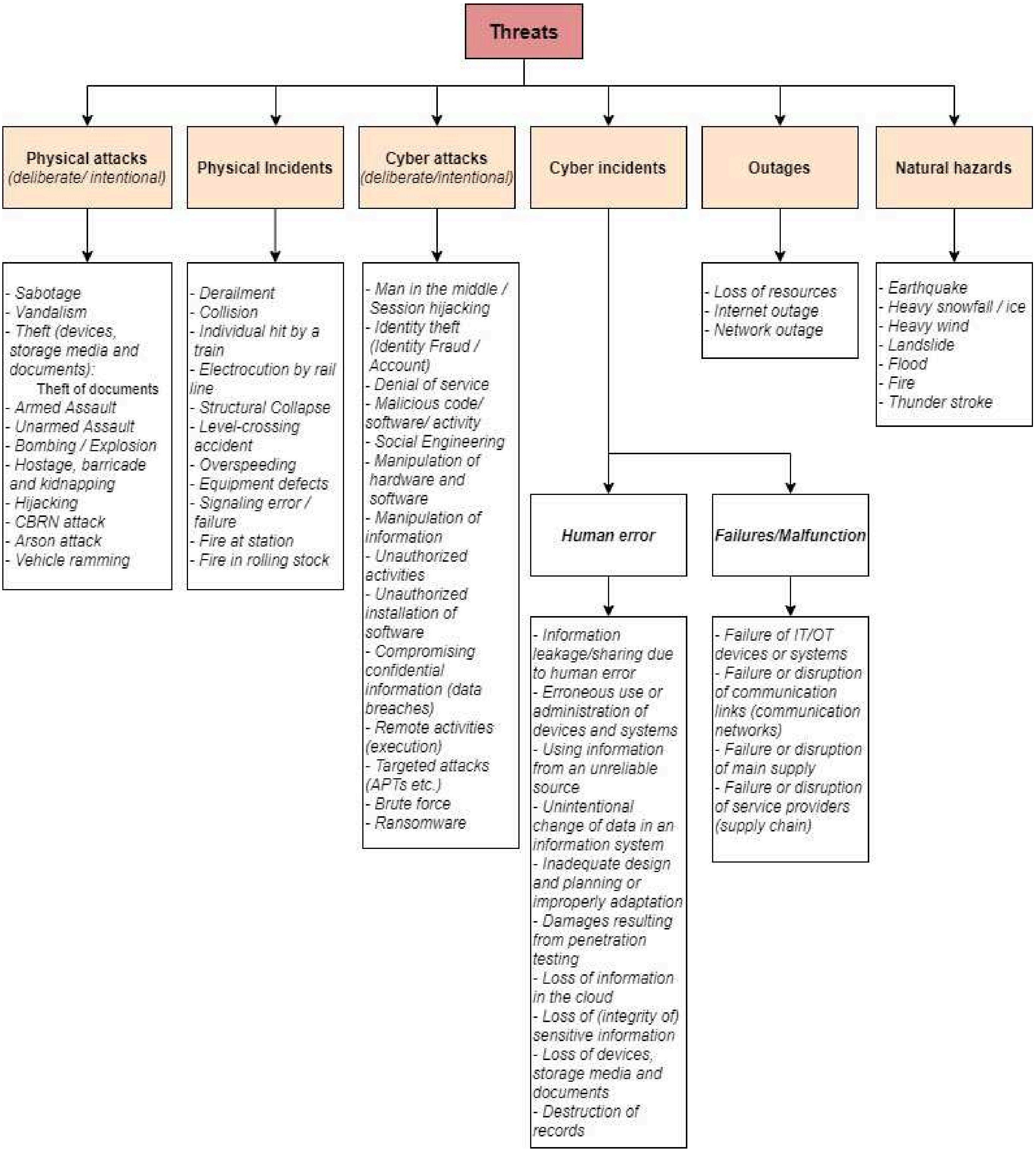

Threats
Physical attacks (deliberate/ intentional)
Physical Incidents
Cyber attacks (deliberate/intentional)
Cyber incidents
Outages
Natural hazards
- Sabotage
- Vandalism
- Theft (devices, storage media and documents):
Theft of documents
- Armed Assault
- Unarmed Assault
- Bombing / Explosion
- Hostage, barricade and kidnapping
- Hijacking
- CBRN attack
- Arson attack
- Vehicle ramming
- Derailment
- Collision
- Individual hit by a train
- Electrocution by rail line
- Structural Collapse
- Level-crossing accident
- Overspeeding
- Equipment defects
- Signaling error / failure
- Fire at station
- Fire in rolling stock
- Man in the middle / Session hijacking
- Identity theft (Identity Fraud / Account)
- Denial of service
- Malicious code/ software/ activity
- Social Engineering
- Manipulation of hardware and software
- Manipulation of information
- Unauthorized activities
- Unauthorized installation of software
- Compromising confidential information (data breaches)
- Remote activities (execution)
- Targeted attacks (APTs etc.)
- Brute force
- Ransomware
Human error
Failures/Malfunction
- Information leakage/sharing due to human error
- Erroneous use or administration of devices and systems
- Using information from an unreliable source
- Unintentional change of data in an information system
- Inadequate design and planning or improperly adaptation
- Damages resulting from penetration testing
- Loss of information in the cloud
- Loss of (integrity of) sensitive information
- Loss of devices, storage media and documents
- Destruction of records
- Failure of IT/OT devices or systems
- Failure or disruption of communication links (communication networks)
- Failure or disruption of main supply
- Failure or disruption of service providers (supply chain)
- Loss of resources
- Internet outage
- Network outage
- Earthquake
- Heavy snowfall / ice
- Heavy wind
- Landslide
- Flood
- Fire
- Thunder stroke

FIGURE 19: THE CATEGORISATION OF THREATS [57]

CAMS enable end-users such as light rail, metro, regional railways, and long distance trains to update existing budget plans and optimise investment policies and strategies for cyber-physical attacks (including other possible threats discussed in deliverable 7.3 and classified in deliverable 3.1, Figure 19) by categorising and storing asset data as referenced in ANNEX II & III (see Figure 20[3]).

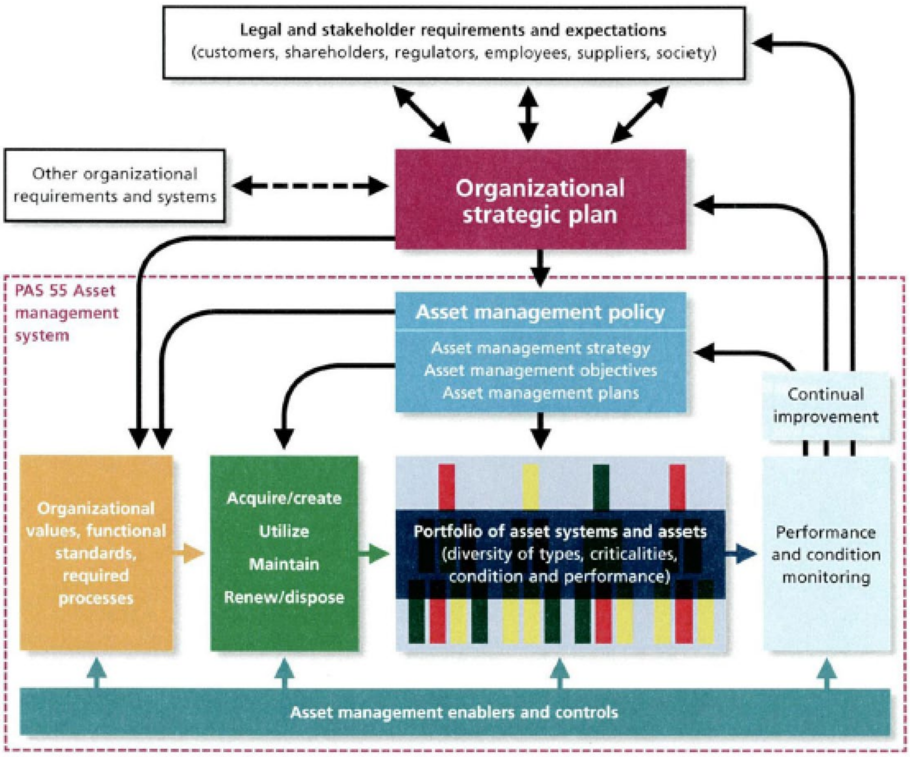
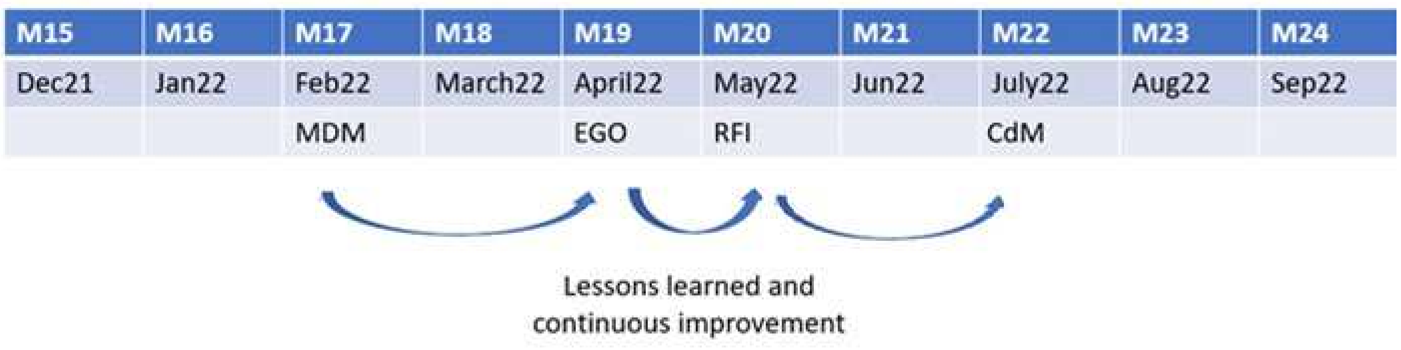

Legal and stakeholder requirements and expectations
(customers, shareholders, regulators, employees, suppliers, society)
Other organizational requirements and systems
Organizational strategic plan
PAS 55 Asset management system
Asset management policy
Asset management strategy
Asset management objectives
Asset management plans
Continual improvement
Organizational values, functional standards, required processes
Acquire/create
Utilize
Maintain
Renew/dispose
Portfolio of asset systems and assets (diversity of types, criticalities, condition and performance)
Performance and condition monitoring
Asset management enablers and controls

FIGURE 20: CENTRAL ASSET MANAGEMENT PROCESS RELATIONSHIP WITH BUDGET POLICY [3]

6. Case-studies addressed

The FIGURE 21 presents the timeline of the four Simulation Exercises, Metro de Madrid (MdM), Ankara Metro (EGO), Rete Ferroviaria Italiana (RFI) and Comune di Milano (CdM).



M15	M16	M17	M18	M19	M20	M21	M22	M23	M24
Dec21	Jan22	Feb22	March22	April22	May22	Jun22	July22	Aug22	Sep22
		MDM		EGO	RFI		CdM		

Lessons learned and
continuous improvement

FIGURE 21: TIMELINE FOR SIMULATION EXERCISES IS TAKEN FROM D8.3 [59]

6.1 Madrid SE

The Madrid Simulation exercise was held between 9th February and 10thFebruary 2022 at MdM. CAMS evaluated the optimal deployment of resources and control of financial losses during recovery based on the assets' final damage conditions and costs as described in the summarisation.

6.1.1 MdM Scenario for Madrid Simulation Exercise

According to the text provided to EU in an Annex to a deliverable with a confidential dissemination level, the section was removed to enable a public version. Please refer to deliverable D83 for more details.

6.1.2 Role of CAMS

In a simulation exercise involving the MdM personnel in the Asset Management Department, the following topics were discussed:

1) Optimal resource allocation based on information about the time and cost involved in responding to a crisis,

2) Use time, cost, and performance loss information to optimise resource deployment and financial loss control during recovery.

6.1.3 Objectives of CAMS tool

The main objectives of the simulation were to test user friendly user interfaces, complete information developed, and to introduce updated features (Prediction of normal deterioration due to aging and degradation of railway assets, Maintenance and repair budget calculation for railway components, Deterioration and budget calculation in the event of extreme events). Simulation Exercises gave MdM the chance to spot strong and weak points and to gather suggestions from the end-user perspective.

6.1.4 Actions made by CAMS

1. Starting with input parameters, RMIT explained the functionalities and how MDM should interact with the tool
2. Input parameters were reviewed and improved by MDM, and then input parameters were entered
3. MDM received information about an investment plan (costs of intervention and repair).
4. MDM reviewed CAMS's output
5. RMIT requested feedback for the purpose of improving functionality and user interface.

6.1.5 Data acquisition needs by CAMS

As shown in FIGURE 22, CMAS collects data from end-user organizations, their staff experiences, researchers and/or inspectors from historical incidents including but not limited to: Capital value of the elements; Cost of asset maintenance under normal degradation; time allocated for maintenance of the element; Cost of asset repair under normal degradation and hazard event. Time and cost spent in maintenance, repair or renewal, Cost and time of asset rehabilitation under normal degradation and/or hazard event.

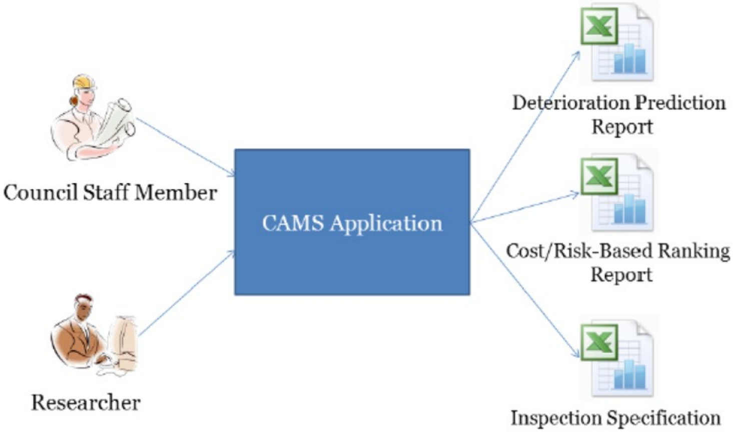


FIGURE 22: CAMS DATA INPUT DIAGRAM [3]

6.1.6 SE result from CAMS

The reports include the lifecycle costs before the incident and the cost variation due to the incident. The list of assets affected during the incident was provided with guidelines on what to replace and what to maintain. The recovery condition ratings were provided with the ability to adjust the outcome condition rating of the whole rail station, depending on the components that are selected to repair. As can be seen in the images below, lifecycle costs have increased significantly due to the incident occurring. The increased cost is highlighted in blue in FIGURE 24. As an impact of incident, the total cost of funding increased from half a million (The orange one before the incident in FIGURE 23) to 22 million (The blue one after the incident in FIGURE 24). This cost was generated by allocating the condition rating of assets from their pre incident condition rating to condition rating 5 (failed status) post incident. Further optimisation of these budgets will be reported in the deliverable D7.5.

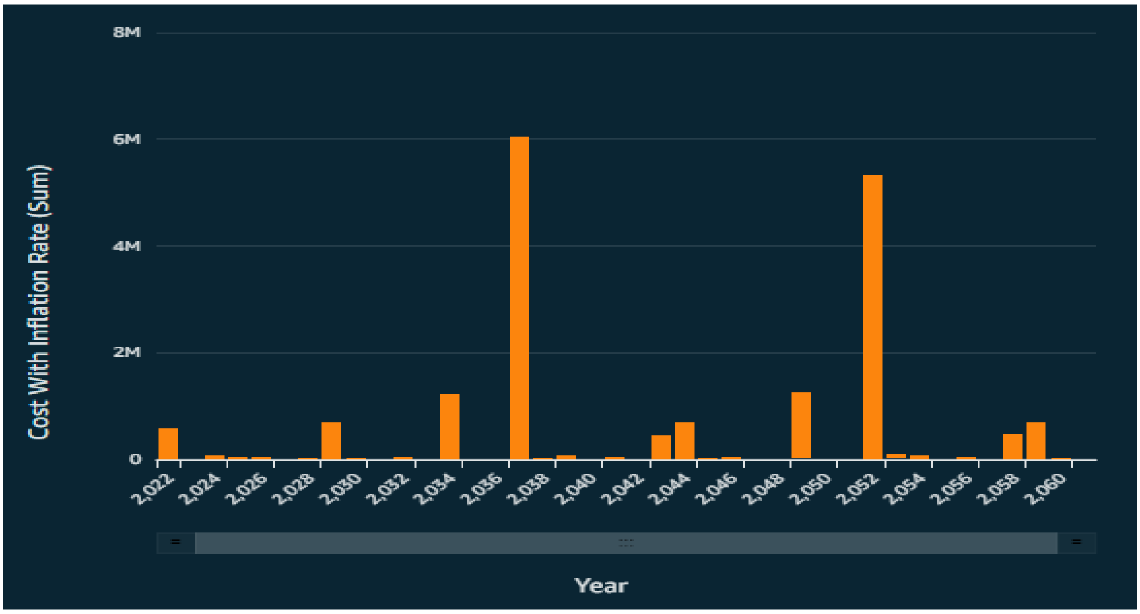


FIGURE 23: CAMS SUGGESTED FINANCIAL MODEL (BEFORE INCIDENT)

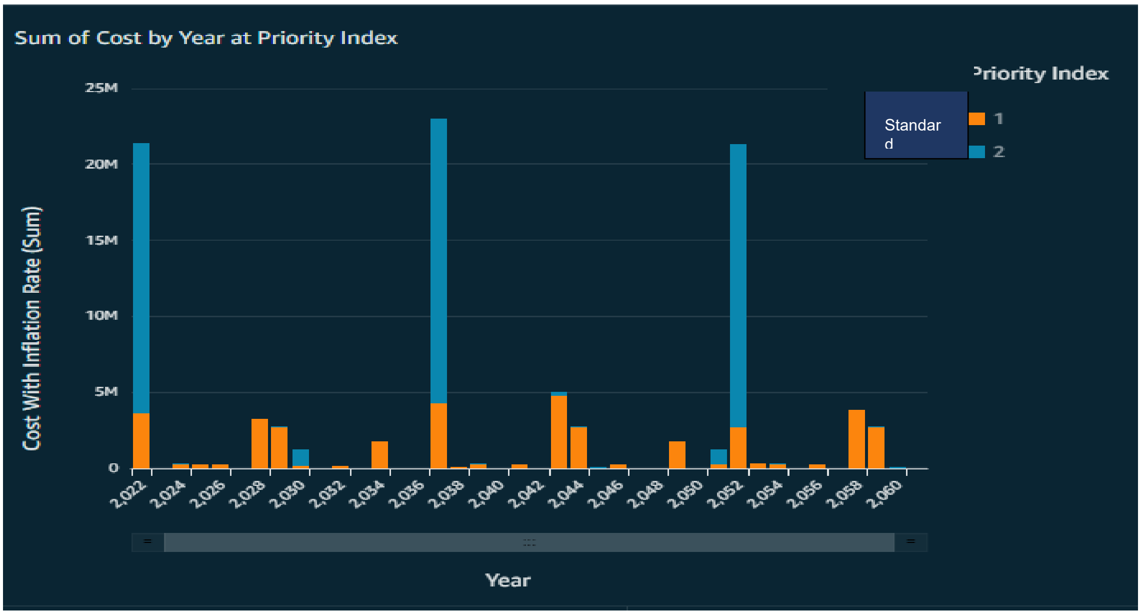


FIGURE 24: CAMS GENERATED FINANCIAL MODEL (AFTER INCIDENT)

6.2 Ankara SE

Ankara Simulation 2022 was held from 26 to 28 April 2022 around EGO & TCDD. CAMS evaluated the optimal deployment of resources and control of financial losses during recovery based on the asset final damage conditions and costs as described in the summary report.

6.2.1 EGO& TCDD Scenario for Ankara Simulation Exercise

According to the text provided to EU in an Annex to a deliverable with a confidential dissemination level, the section was removed to enable a public version. Please refer to deliverable D8.3 for more details.

6.2.2 Role of CAMS

CAMS aimed to calculate the variation of lifecycle cost of assets due to the incident and identify areas of vulnerability of the station using a resilience factor. The outcome included costs of repair and maintenance costs. The outcome provided the decision makers of the Ankara Railway station the ability to identify locations of high vulnerability during an attack with the resilience factor calculated for this specific scenario. An impact factor was used in the calculation to identify the assets that impacted the operation of the station or damaged.

6.2.3 Objectives of CAMS tool

Resilience index was calculated for each assetand rolled up to provide a resilience index for the whole infrastructure (i.e. station). This index is to help the project managers with the decision of improving different parts of the station which will in turn improve the overall resilience of the structure.A detailed evaluation of the technical functionality ahead of the use-case was carried out to compare the predictions of recovery budgets by CAMS with those based on real data, as well as a tabletop exercise aimed at evaluating the predictions of investment asset management by CAMS.

6.2.4 Actions made by CAMS

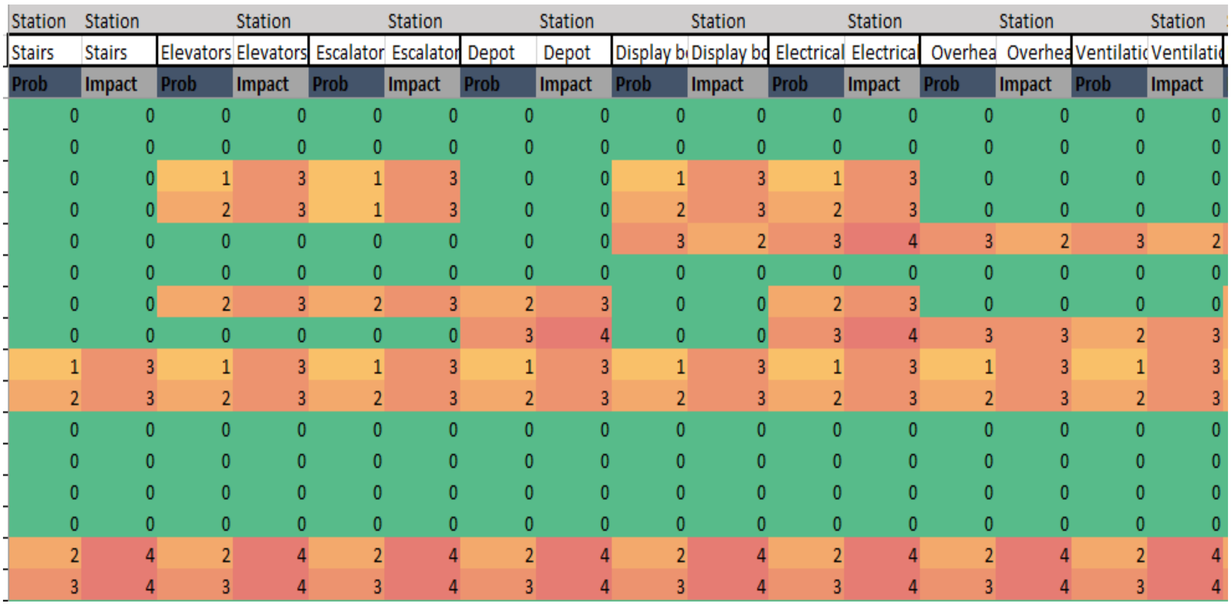
CAMS had the ability to collect data that is related to the incident including location, list of assets, condition of assets before and after incident, cost of replacement/recovery. The acquired condition is used by the system to calculate the resilience of the assets and in turn for the whole infrastructure.

1. Gathering of data to be uploaded to CAMS.
2. EGO evaluated the input from CAMS.
3. The CAMS team analysed the data and presented the findings to the EGO.
4. As a result of the CAMS evaluation, the results were assessed in terms of structural resilience, performance loss assessment, cost, and the recovery time for the service.
5. As part of the best resource deployment generated after a crisis, consideration has been given to degradation of critical assets under normal conditions and degradation of critical assets during a simulated crisis; maintenance, repair, and replacement costs associated with critical assets.
6. The CAMS team supported the analysis of the results and developed alternative budgetary strategies to address the crisis.

6.2.5 Data acquisition needs by CAMS

To calculate the resilience index, visual inspection data was acquired and used to access the current state of the station. Then the condition of these assets after the incident was estimated and uploaded to the software. CAMS software used these condition ratings to calculate the resilience index with inbuilt factors that were available for different components. The calculated resilience index is then used to calculate the index for the whole infrastructure level (whole station).

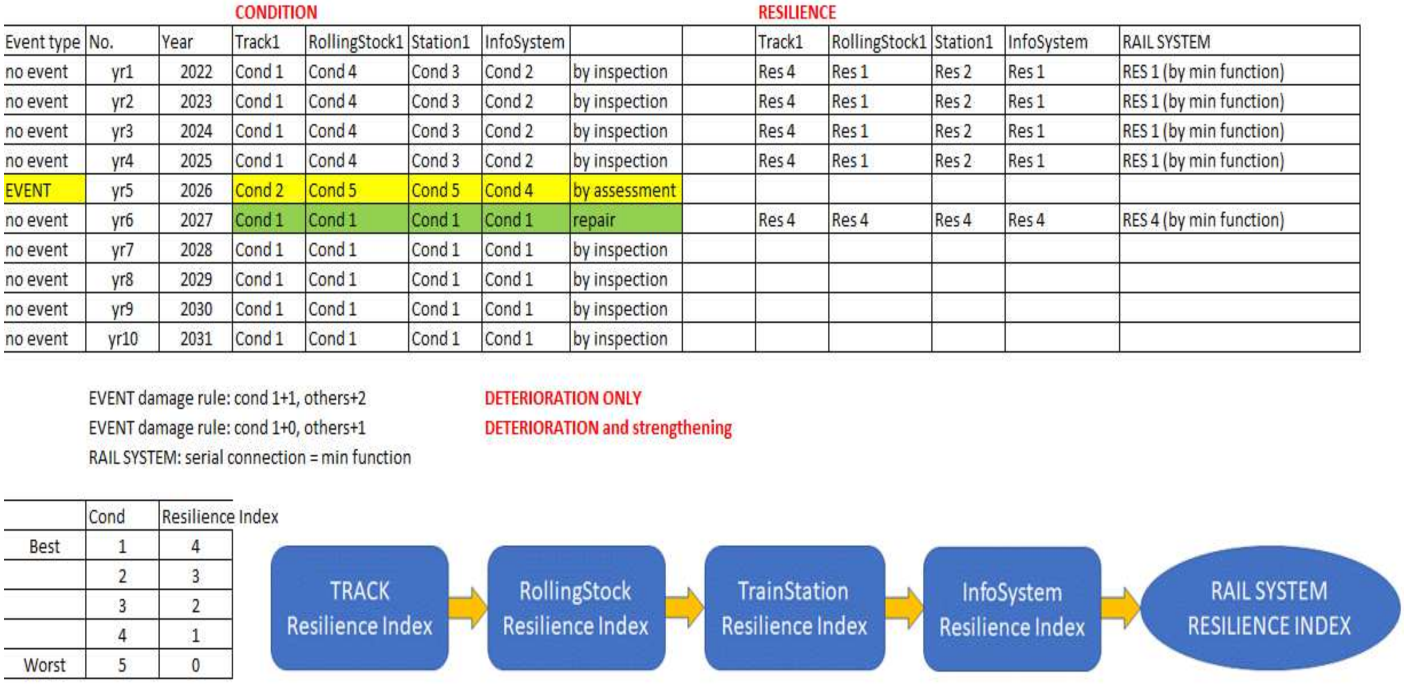
6.2.6 SE Result from CAMS



Station	Station		Station		Station		Station		Station		Station		Station		Station
Stairs	Stairs	Elevators	Elevators	Escalator	Escalator	Depot	Depot	Display b	Display bo	Electrical	Electrical	Overhea	Overhea	Ventilatic	Ventilatio
Prob	Impact	Prob	Impact	Prob	Impact	Prob	Impact	Prob	Impact	Prob	Impact	Prob	Impact	Prob	Impact
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	3	1	3	0	0	1	3	1	3	0	0	0	0
0	0	2	3	1	3	0	0	2	3	2	3	0	0	0	0
0	0	0	0	0	0	0	0	3	2	3	4	3	2	3	2
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	2	3	2	3	2	3	0	0	2	3	0	0	0	0
0	0	0	0	0	0	3	4	0	0	3	4	3	3	2	3
1	3	1	3	1	3	1	3	1	3	1	3	1	3	1	3
2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	4	2	4	2	4	2	4	2	4	2	4	2	4	2	4
3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4

FIGURE 25: ASSET IMPACT CALCULATION IS TAKEN FROM D7.3 [60]

The Figure 25 shows the calculated impact ratings. This 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. To ensure minimal damage is caused during incident, the resilience of rail assets should be improved before the occurrence of the extreme damage event. One way is to maintain or strengthen the structural condition of rail assets, which can enhance the resilience of the rail system. Figure 26 shows an example of condition-based resilience index calculation of rail assets change over time due to the change of asset condition. One can improve the resilience index of all rail assets with an unlimited budget. However, due to the limited budget the focus can be on critical assets that can contribute to the overall resilience of the rail system. Other factors contributing to the resilience index such as an emergency plans and reservation of resources should also be improved in parallel. (Since this report is "Public", we only displayed a part of non-sensitive results from Deliverable 7.3 in FIGURE 25, for the complete results, see D7.3).



			CONDITION						RESILIENCE				
Event type	No.	Year	Track1	RollingStock1	Station1	InfoSystem			Track1	RollingStock1	Station1	InfoSystem	RAIL SYSTEM
no event	yr1	2022	Cond 1	Cond 4	Cond 3	Cond 2	by inspection		Res 4	Res 1	Res 2	Res 1	RES 1 (by min function)
no event	yr2	2023	Cond 1	Cond 4	Cond 3	Cond 2	by inspection		Res 4	Res 1	Res 2	Res 1	RES 1 (by min function)
no event	yr3	2024	Cond 1	Cond 4	Cond 3	Cond 2	by inspection		Res 4	Res 1	Res 2	Res 1	RES 1 (by min function)
no event	yr4	2025	Cond 1	Cond 4	Cond 3	Cond 2	by inspection		Res 4	Res 1	Res 2	Res 1	RES 1 (by min function)
EVENT	yr5	2026	Cond 2	Cond 5	Cond 5	Cond 4	by assessment						
no event	yr6	2027	Cond 1	Cond 1	Cond 1	Cond 1	repair		Res 4	Res 4	Res 4	Res 4	RES 4 (by min function)
no event	yr7	2028	Cond 1	Cond 1	Cond 1	Cond 1	by inspection						
no event	yr8	2029	Cond 1	Cond 1	Cond 1	Cond 1	by inspection						
no event	yr9	2030	Cond 1	Cond 1	Cond 1	Cond 1	by inspection						
no event	yr10	2031	Cond 1	Cond 1	Cond 1	Cond 1	by inspection						

EVENT damage rule: cond 1+1, others+2 DETERIORATION ONLY

EVENT damage rule: cond 1+0, others+1 DETERIORATION and strengthening

RAIL SYSTEM: serial connection = min function

	Cond	Resilience Index
Best	1	4
	2	3
	3	2
	4	1
Worst	5	0

TRACK Resilience Index → RollingStock Resilience Index → TrainStation Resilience Index → InfoSystem Resilience Index → RAIL SYSTEM RESILIENCE INDEX

FIGURE 26: ASSET RESILIENCE INDEX CALCULATION

The steps used for this calculation is highlighted in the Figure 26. For more details, refer to deliverable D8.3[59] and CAMS presentation. With considerations given to the resilience factor and impact factors the cost model for the incident was completed. The FIGURE 27 shows the calculated cost of Ankara for the incident and its recovery. As seen in the previous simulation exercise, the spike in cost can be seen in 2022 due to the incident occurring.

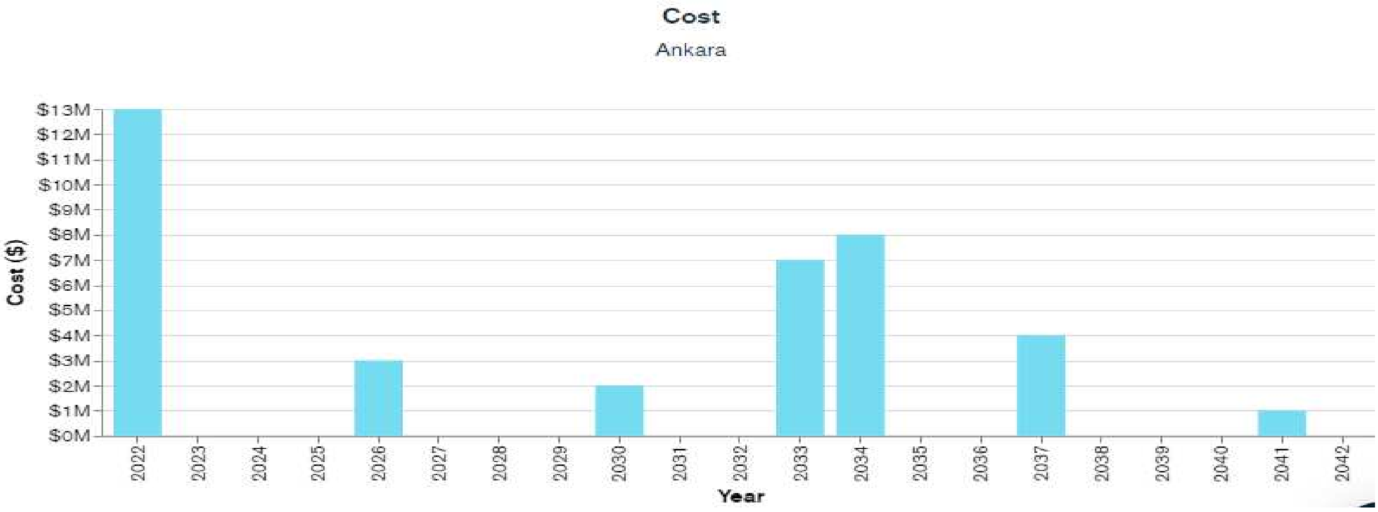


FIGURE 27: ASSET RESILIENCE INDEX CHART

6.3 Rome SE

The Rome Simulation exercise was held between 31 May and 1 June 2022 by the RFI. CAMS evaluated the optimal deployment of resources and control of financial losses during recovery based on the damage of the assets due to the incident.

6.3.1 RFI Scenario for Rome Simulation Exercise

According to the text provided to EU in an Annex to a deliverable with a confidential dissemination level, the section was removed to enable a public version. Please refer to deliverable D83 for more details.

6.3.2 Role of CAMS

As part of the Recovery phase, CAMS created a budget plan including recovery time tracking for the standard operation of the facility after events occurred in the scenario. It was a post-event evaluation to assist RFI experts in recovering infrastructure and ensuring business continuity. Therefore, the CAMS was responsible for providing accurate recovery costs for assets involved in the event through an assessment of the damaged assets. The final damage was assessed using both the initial condition of the assets before the incident and the impact that the incident has had on the assets, using an onsite inspection.

6.3.3 Objectives of CAMS tool

During RFI Simulation Exercise, the main objective was to test the capabilities of CAMS to provide an accurate recovery budget plan for assets involved in a sudden event through the assessment of the final damage to the involved components. The final damage to the asset was determined based on the initial condition of the asset (prior to the incident) and the impact measure of the specific incident on the asset. There was a budget that was provided to the end-user to restore the service as soon as possible.

6.3.4 Actions taken by CAMS

1. A brief explanation was provided by RMIT of the functionality of CAMS and how RFI should interact with the tool.
2. During the demonstration, RMIT updated the tool's parameters and demonstrated how the scenario would play out.
3. RFI received information regarding the final condition of the assets involved in the incident.
4. RFI received updated information about investment management and budget planning.
5. The RMIT team reviewed the output obtained and considered feedback for future improvements to the user interface and functionality.
6. RFI evaluated CAMS's output.

6.3.5 Data acquisition needs by CAMS

CAMS collected the necessary data, including the time and cost spent on maintenance, repair, and/or renewal. RMIT used this data (Table 11[5]) to generate information about all components of the system (station, rail geometry, platform, control room, wagon, and other structural elements) to provide an overall picture of asset management and budget planning. CAMS provided decision makers with the processed output based on the information that was collected.

[5] Potentially sensitive data, redacted in this Public report.

Asset Id	Asset name	Condition before incident	Condition after incident	Time required for replacement/repair (days)	Priority of recovery	Dependencies	Quantity of repair replacement	Unit of measure	Cost of repair	Cost of replacement per unit (€)
1	Stairs	1								
2	Elevators	1								
3	Escalator	1								
4	Depot	1								
5	Display board (timetable)	1								
6	Electrical and lighting system	1	5					meters		
7	Lights	1	5					lighting fixtures		
8	Overhead line	1								
9	Ventilation	1								
10	Drainage system	1								
11	Water system	1	5					meters		
12	Overpass/Underpass	1								
13	Overall roof	1	5					squared meters		
14	Turnstile/Toll gate	1								
15	Walls	1	5					squared meters		
16	Pavement	1	5					squared meters		
17	Polycarbonate Barrier	1	5					number of barriers		
18	CCTV system	1	5					Camera		
19	Ticketing System	1	5					ticketing systems		
20	Station Communication System	1	5					unit		
21	Signalling (information and commuciation system)	1	5					unit		
22	Rails geometry	1								
23	Eletrical System for traffic control system									
24	Switch system	1								
25	Ballast	1								
26	Overhead line	1								
27	Signalling system	1								
28	Singalling Communication system	1								
29	Ventilation	1								
32	Electrical and lighting system	1								
33	Fire protection	1								
34	Emergency escape system	1								
35	Fire hose connection	1	5					connection point		

TABLE 11: CAMS INPUT DATA FOR ROME SE

6.3.6 SE result from CAMS

As a sample of Rome SE results, CAMS generated a curve to show the normal deterioration prediction. The simulation included the demonstration of the deterioration curve that is used for the natural deterioration prediction. FIGURE 28 shows the blue curve which provides the probability of assets in condition 1 and red which is condition 5. As time increases, the probability of assets in condition one reduces and the probability of assets in condition 5 increases. This is the standard mechanism of deterioration of assets in CAMS. Further details on the theoretical aspects can be found in section 4.1.2.

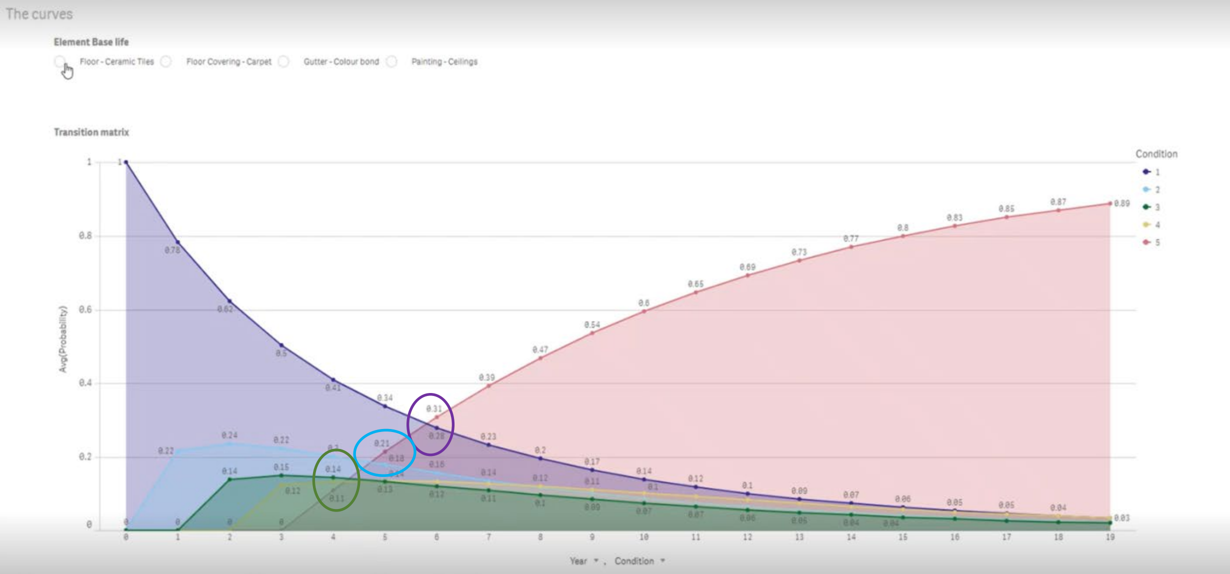


FIGURE 28: CAMS DETERIORATION CURVE

The FIGURE 29, shows the amended simplified curve due to the incident in Rome. The blue line represents the simplified average condition achieved using FIGURE 28. The average condition drops smoothly over time to reach condition 5 approximately in the year 2027. However, due to the incident in 2022, there is sharp drop in condition depicted by the orange line. This condition is then recovered immediately back to condition 1 and the curve continues ahead. The recovery requires the budget that is depicted in FIGURE 30. This budget is calculated with accumulated recovery costs from all the damaged components in the station.

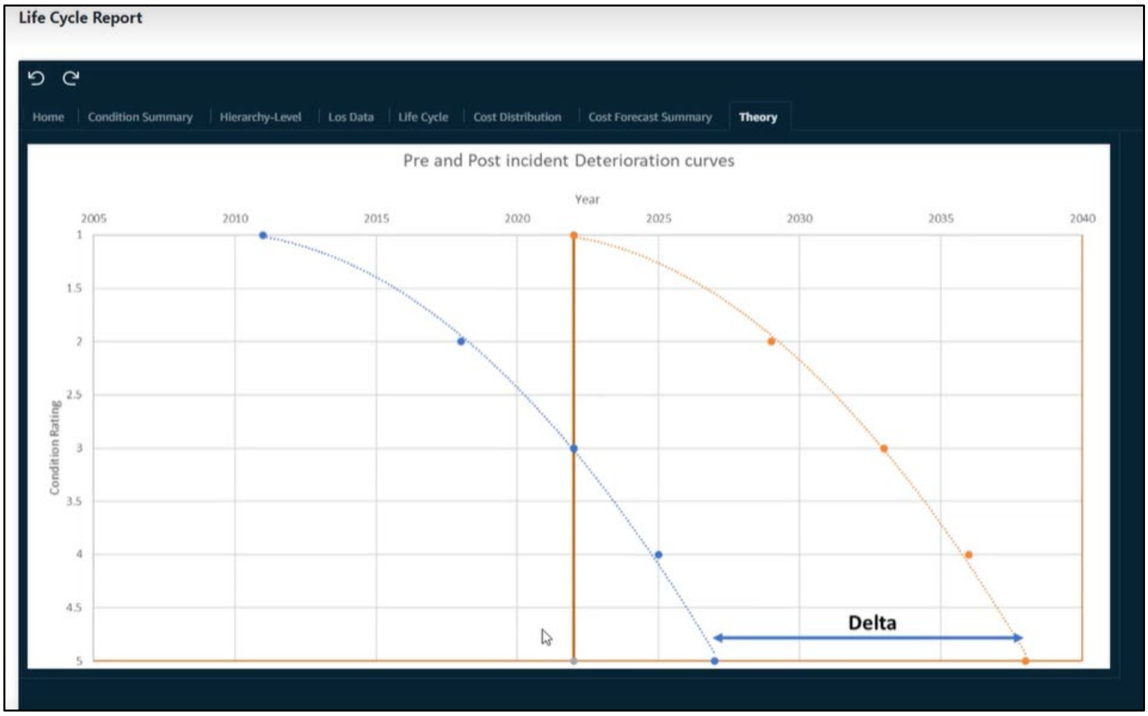


FIGURE 29: PRE AND POST INCIDENT DETERIORATION CURVE

The output life cycle model shows a large peak at the beginning of the incident FIGURE 30.

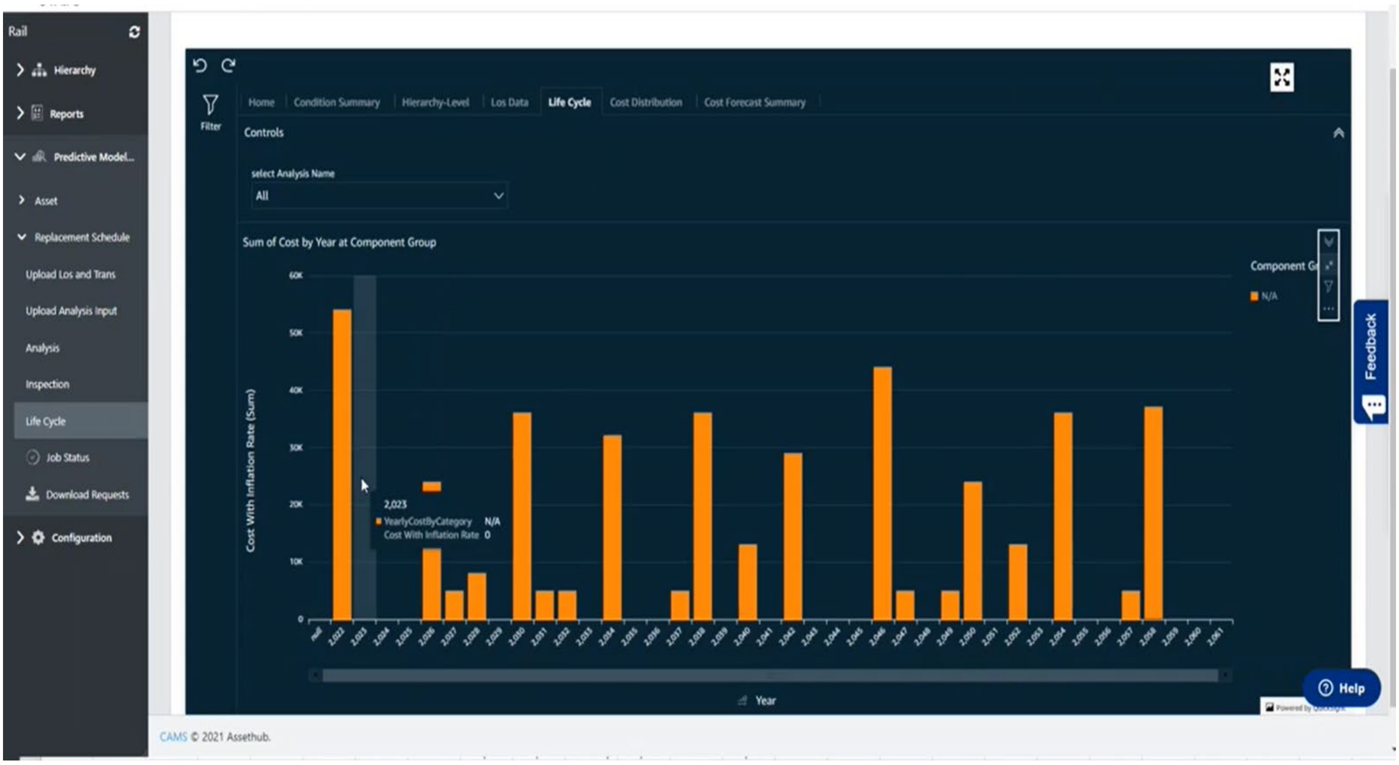


FIGURE 30: CAMS RESULT FOR ASSET REPLACEMENTS (LIFE CYCLE)

In general, the lifecycle costs (FIGURE 31) are generally spread over many years. For more details, refer to deliverable D8.3 and CAMS recorded presentation.

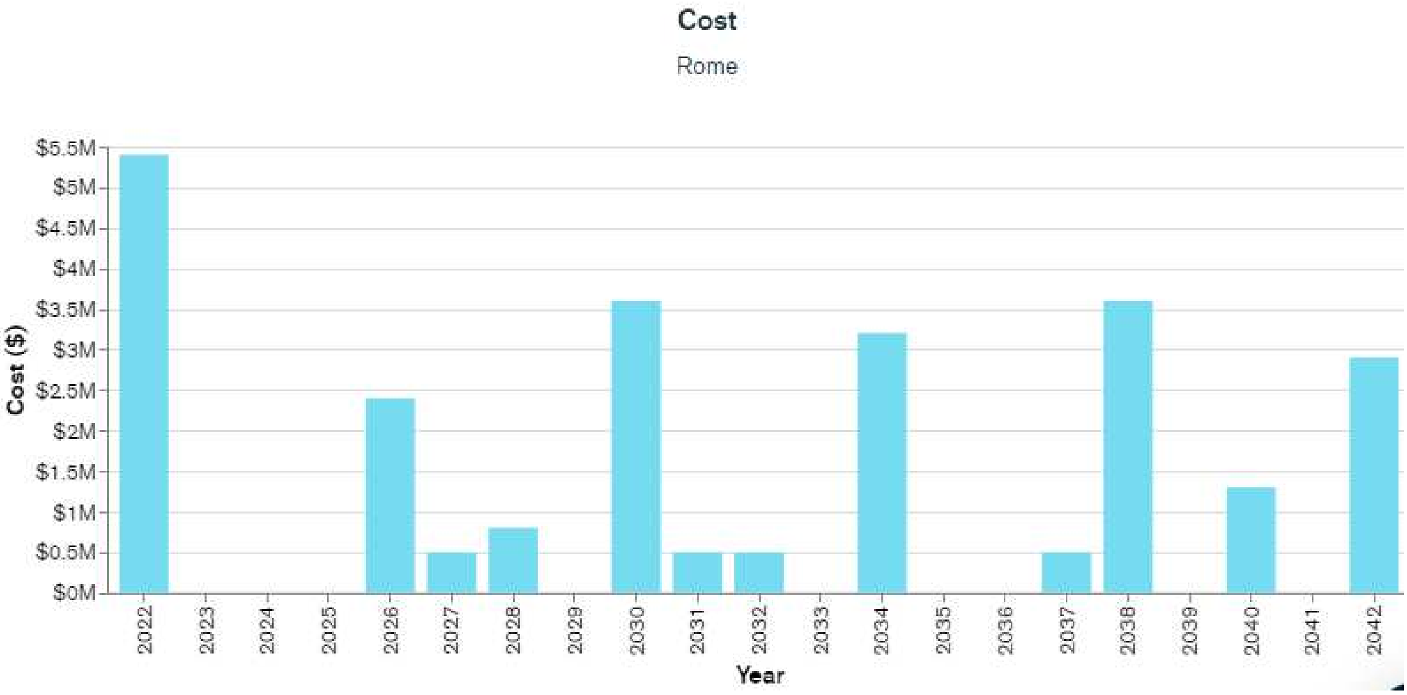


FIGURE 31: CAMS OUTPUT FOR ASSET REPLACEMENTS (LIFE CYCLE)

An additional parameter analysed in this simulation included recovery time, which is a major component of improving the resilience of a rail station. Information from Table 11 can be used to plot recovery timelines such as shown in the FIGURE 32 and FIGURE 33.

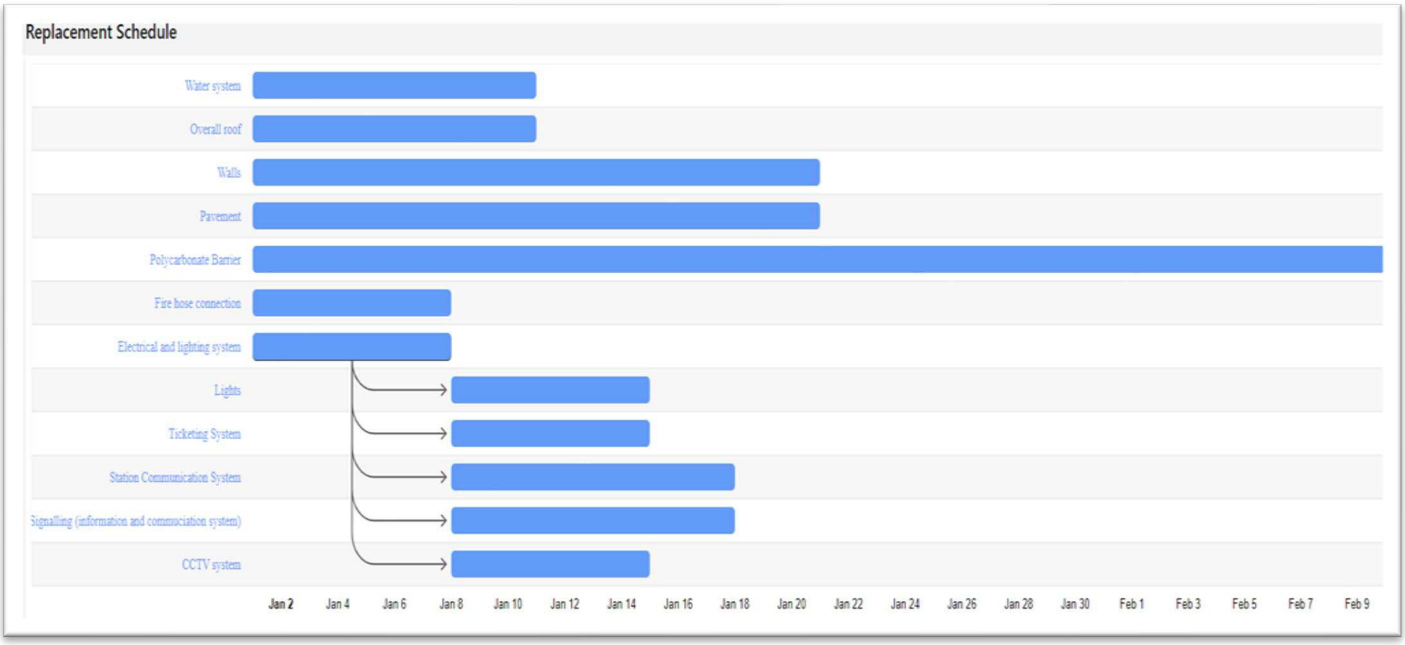


FIGURE 32: RECOVERY TIMELINE

Each task can have a start time and dependencies from which the total time of the project recovery can be calculated. In FIGURE 32 five of the tasks are dependent on completion of the Electrical and Lighting systems. However, the longest task – Polycarbonate barrier dictates the full time of recovery. Due to this reason, the five subtasks mentioned before do not interfere with recovery time. In FIGURE 33 an additional task –station communication system is dependent on CCTV system (example only). This change increases the total recovery time of the project as this is now the critical path of the timeline.

To create a timeline such as this, an expert needs to be consulted, information needs to be gathered and several site visits need to be done in a very risky environment during a disaster situation. The process could take up to 2 to 3 days, even weeks, which delays the recovery time of the station. Having this plan already completed and available within the system can assist the recovery program to initiate immediately cutting the cost of not having the station in an operational state by several days.

Following the critical timeline generated by CAMS, the budget of the recovery phase can be reduced by 15%-20% compared to starting the planning after an incident has already occurred.

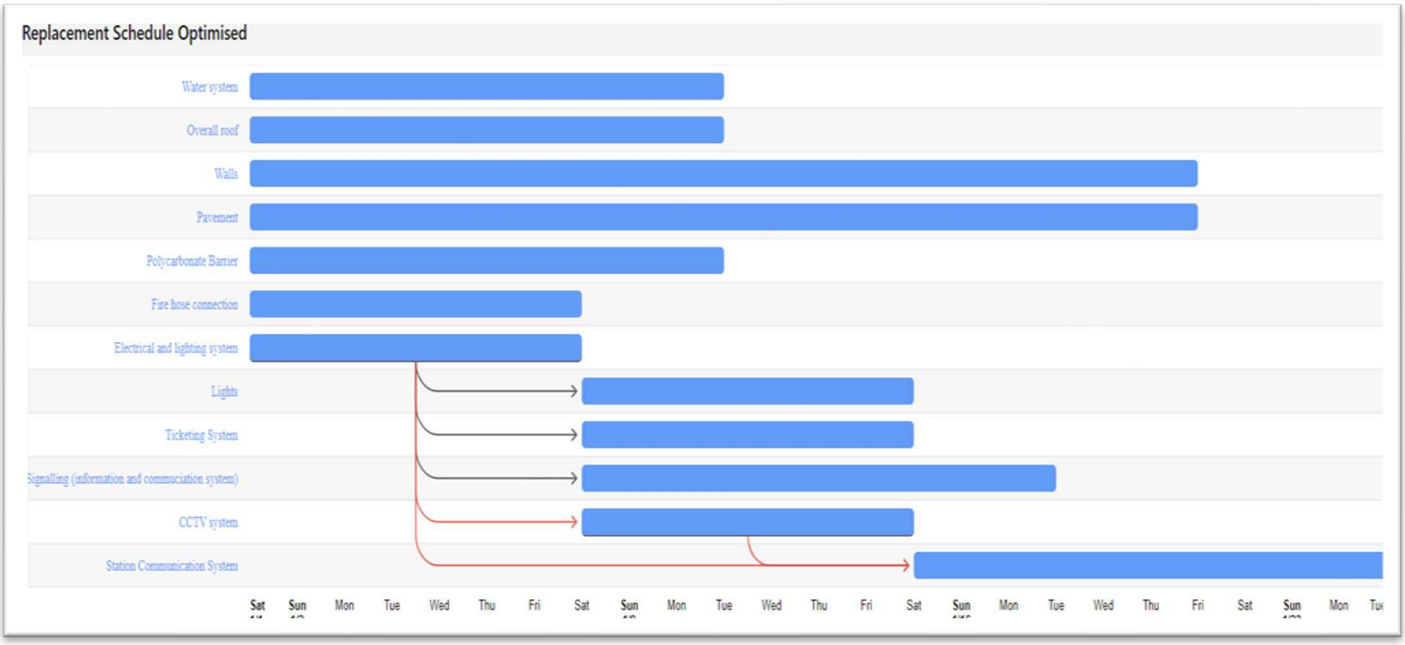


FIGURE 33: RECOVERY TIMELINE WITH CRITICAL PATH

In addition to the reduced cost due to having a plan in place to act on as soon as a disaster occurs, the continuous monitoring of assets as well as using the fragility index to ensure vulnerable areas of the station are maintained at optimal performance ensures damage caused by the incident will be reduced significantly as assets are in a better condition. It can be estimated that the improved resilience due to faster recovery time and lower damage can provide a cost benefit of at least 15% in terms of cost reduction. This topic is covered in detail in Deliverable 7.5.

6.4 Milan SE

6.4.1 CdM Scenario for Milan Simulation Exercise

In the CdM Simulation Exercise, the outcomes of the simulation were tested on the basis of flooding as a natural disaster (it was shown in the 3rd row in the left-hand side of FIGURE 19). For full details about scenario see deliverable D8.3.

6.4.2 Role of CAMS

As part of the Recovery phase, CAMS created a budget plan following end-user Investment Management to target recovery and restarting facilities after events occurred in the scenario. It was a post-event evaluation to assist CdM experts in recovering infrastructure and ensuring business continuity.

6.4.3 Objectives of CAMS tool

During CdM Simulation Exercise, the main objective was to test the capabilities of CAMS to provide an accurate recovery budget plan for assets involved in a sudden event through the assessment of the final damage to the involved components. The final damage to the asset was determined based on the initial condition of the asset (prior to the incident) and the impact measure of the specific incident on the asset. There was a budget that was provided by the end user in order to restore the service as soon as possible.

6.4.4 Actions taken by CAMS

1. A brief explanation was provided by RMIT on the functionality of CAMS and how CdM should interact with the tool.
2. During the demonstration, RMIT updated the tool's parameters and demonstrated how the scenario would play out.
3. CdM received information regarding the final condition of the assets involved in the incident.
4. CdM received updated information about investment management and budget planning.
5. The RMIT team reviewed the output obtained and considered feedback for future improvements to the user interface and functionality.
6. CdM evaluated CAMS's output.

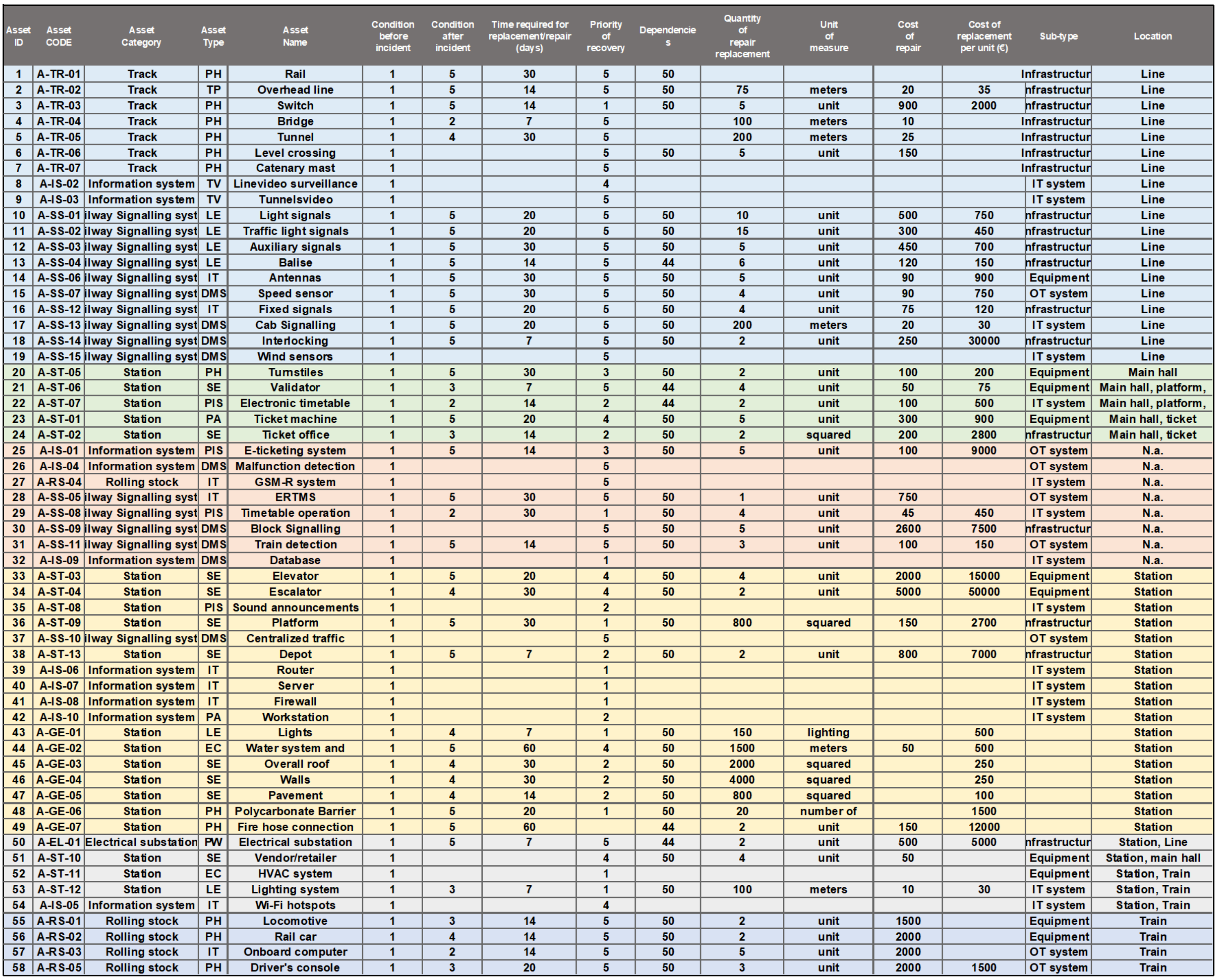
6.4.5 Data acquisition needs by CAMS

In the CdM Simulation Exercise, CAMS focused on evaluating selected aspects of physical recovery after a natural hazard as flooding. CAMS is designed to provide a preview of the Time and Cost concerns so that the end-users can be better prepared to serve their community effectively in unpredictable incidents in the future.

CAMS was focusing on two of the railway lines affected by this flood incident. CAMS has taken into account some historical information from similar incidents in metro stations, and this data was used to estimate the damage to the railway infrastructure caused by the natural hazards.

CAMS collected the historical data, including the time and cost spent on maintenance, repair, and/or renewal. RMIT used this data to generate information about all components of the system (station, rail geometry, platform, control room, wagon, and other structural elements) in order to provide an overall picture of asset management and budget planning.

CAMS provided decision makers with the processed output based on the information that was collected. In Table 12, CAMS data related to affected components under CdM incidents were summarised from Asset Lists in ANNEX II and ANNEX Condition in ANNEX III.



Asset ID	Asset CODE	Asset Category	Asset Type	Asset Name	Condition before incident	Condition after incident	Time required for replacement/repair (days)	Priority of recovery	Dependencies	Quantity of repair replacement	Unit of measure	Cost of repair	Cost of replacement per unit (€)	Sub-type	Location
1	A-TR-01	Track	PH	Rail	1	5	30	5	50					Infrastructur	Line
2	A-TR-02	Track	TP	Overhead line	1	5	14	5	50	75	meters	20	35	nfrastructur	Line
3	A-TR-03	Track	PH	Switch	1	5	14	1	50	5	unit	900	2000	nfrastructur	Line
4	A-TR-04	Track	PH	Bridge	1	2	7	5		100	meters	10		Infrastructur	Line
5	A-TR-05	Track	PH	Tunnel	1	4	30	5		200	meters	25		Infrastructur	Line
6	A-TR-06	Track	PH	Level crossing	1			5	50	5	unit	150		Infrastructur	Line
7	A-TR-07	Track	PH	Catenary mast	1			5						Infrastructur	Line
8	A-IS-02	Information system	TV	Linevideo surveillance	1			4						IT system	Line
9	A-IS-03	Information system	TV	Tunnelsvideo	1			5						IT system	Line
10	A-SS-01	ilway Signalling syst	LE	Light signals	1	5	20	5	50	10	unit	500	750	nfrastructur	Line
11	A-SS-02	ilway Signalling syst	LE	Traffic light signals	1	5	20	5	50	15	unit	300	450	nfrastructur	Line
12	A-SS-03	ilway Signalling syst	LE	Auxiliary signals	1	5	30	5	50	5	unit	450	700	nfrastructur	Line
13	A-SS-04	ilway Signalling syst	LE	Balise	1	5	14	5	44	6	unit	120	150	nfrastructur	Line
14	A-SS-06	ilway Signalling syst	IT	Antennas	1	5	30	5	50	5	unit	90	900	Equipment	Line
15	A-SS-07	ilway Signalling syst	DMS	Speed sensor	1	5	30	5	50	4	unit	90	750	OT system	Line
16	A-SS-12	ilway Signalling syst	IT	Fixed signals	1	5	20	5	50	4	unit	75	120	nfrastructur	Line
17	A-SS-13	ilway Signalling syst	DMS	Cab Signalling	1	5	20	5	50	200	meters	20	30	IT system	Line
18	A-SS-14	ilway Signalling syst	DMS	Interlocking	1	5	7	5	50	2	unit	250	30000	nfrastructur	Line
19	A-SS-15	ilway Signalling syst	DMS	Wind sensors	1			5						IT system	Line
20	A-ST-05	Station	PH	Turnstiles	1	5	30	3	50	2	unit	100	200	Equipment	Main hall
21	A-ST-06	Station	SE	Validator	1	3	7	5	44	4	unit	50	75	Equipment	Main hall, platform,
22	A-ST-07	Station	PIS	Electronic timetable	1	2	14	2	44	2	unit	100	500	IT system	Main hall, platform,
23	A-ST-01	Station	PA	Ticket machine	1	5	20	4	50	5	unit	300	900	Equipment	Main hall, ticket
24	A-ST-02	Station	SE	Ticket office	1	3	14	2	50	2	squared	200	2800	nfrastructur	Main hall, ticket
25	A-IS-01	Information system	PIS	E-ticketing system	1	5	14	3	50	5	unit	100	9000	OT system	N.a.
26	A-IS-04	Information system	DMS	Malfunction detection	1			5						OT system	N.a.
27	A-RS-04	Rolling stock	IT	GSM-R system	1			5						IT system	N.a.
28	A-SS-05	ilway Signalling syst	IT	ERTMS	1	5	30	5	50	1	unit	750		OT system	N.a.
29	A-SS-08	ilway Signalling syst	PIS	Timetable operation	1	2	30	1	50	4	unit	45	450	IT system	N.a.
30	A-SS-09	ilway Signalling syst	DMS	Block Signalling	1			5	50	5	unit	2600	7500	nfrastructur	N.a.
31	A-SS-11	ilway Signalling syst	DMS	Train detection	1	5	14	5	50	3	unit	100	150	OT system	N.a.
32	A-IS-09	Information system	DMS	Database	1			1						IT system	N.a.
33	A-ST-03	Station	SE	Elevator	1	5	20	4	50	4	unit	2000	15000	Equipment	Station
34	A-ST-04	Station	SE	Escalator	1	4	30	4	50	2	unit	5000	50000	Equipment	Station
35	A-ST-08	Station	PIS	Sound announcements	1			2						IT system	Station
36	A-ST-09	Station	SE	Platform	1	5	30	1	50	800	squared	150	2700	nfrastructur	Station
37	A-SS-10	ilway Signalling syst	DMS	Centralized traffic	1			5						OT system	Station
38	A-ST-13	Station	SE	Depot	1	5	7	2	50	2	unit	800	7000	nfrastructur	Station
39	A-IS-06	Information system	IT	Router	1			1						IT system	Station
40	A-IS-07	Information system	IT	Server	1			1						IT system	Station
41	A-IS-08	Information system	IT	Firewall	1			1						IT system	Station
42	A-IS-10	Information system	PA	Workstation	1			2						IT system	Station
43	A-GE-01	Station	LE	Lights	1	4	7	1	50	150	lighting		500		Station
44	A-GE-02	Station	EC	Water system and	1	5	60	4	50	1500	meters	50	500		Station
45	A-GE-03	Station	SE	Overall roof	1	4	30	2	50	2000	squared		250		Station
46	A-GE-04	Station	SE	Walls	1	4	30	2	50	4000	squared		250		Station
47	A-GE-05	Station	SE	Pavement	1	4	14	2	50	800	squared		100		Station
48	A-GE-06	Station	PH	Polycarbonate Barrier	1	5	20	1	50	20	number of		1500		Station
49	A-GE-07	Station	PH	Fire hose connection	1	5	60		44	2	unit	150	12000		Station
50	A-EL-01	Electrical substation	PW	Electrical substation	1	5	7	5	44	2	unit	500	5000	nfrastructur	Station, Line
51	A-ST-10	Station	SE	Vendor/retailer	1			4	50	4	unit	50		Equipment	Station, main hall
52	A-ST-11	Station	EC	HVAC system	1			1						Equipment	Station, Train
53	A-ST-12	Station	LE	Lighting system	1	3	7	1	50	100	meters	10	30	IT system	Station, Train
54	A-IS-05	Information system	IT	Wi-Fi hotspots	1			4						IT system	Station, Train
55	A-RS-01	Rolling stock	PH	Locomotive	1	3	14	5	50	2	unit	1500		Equipment	Train
56	A-RS-02	Rolling stock	PH	Rail car	1	4	14	5	50	2	unit	2000		Equipment	Train
57	A-RS-03	Rolling stock	IT	Onboard computer	1	2	14	5	50	5	unit	2000		OT system	Train
58	A-RS-05	Rolling stock	PH	Driver's console	1	3	20	5	50	3	unit	2000	1500	OT system	Train

TABLE 12: CAMS INPUT DATA FOR CDM SE

6.4.6 SE result from CAMS

In addition to calculating required cost, an additional field – available budget - was included in Milan simulation. Available budget refers to the existing budget that was planned before the disaster occurs. In FIGURE 34, the budget is shown in dark blue while the CAMS suggested cost is shown in light blue. As can be seen due to the disaster, the available budget is not sufficient to cover the cost if the incident. The red plot in FIGURE 35, shows cumulative lack of funding over the course of the years generated by the incident. If the cumulative budget is in the negative, some assets are not repaired and this can affect the performance of the station. To ensure smooth operation of the station, an additional factor of priority can be applied which can be used to select assets that need to be attended to immediately and assets that can be attended with additional budget next year. As can be seen the backlog curve recovers to positive values after 2036, which indicates a surplus of funding. This is not ideal but shows that the incident recovery can happen over time.

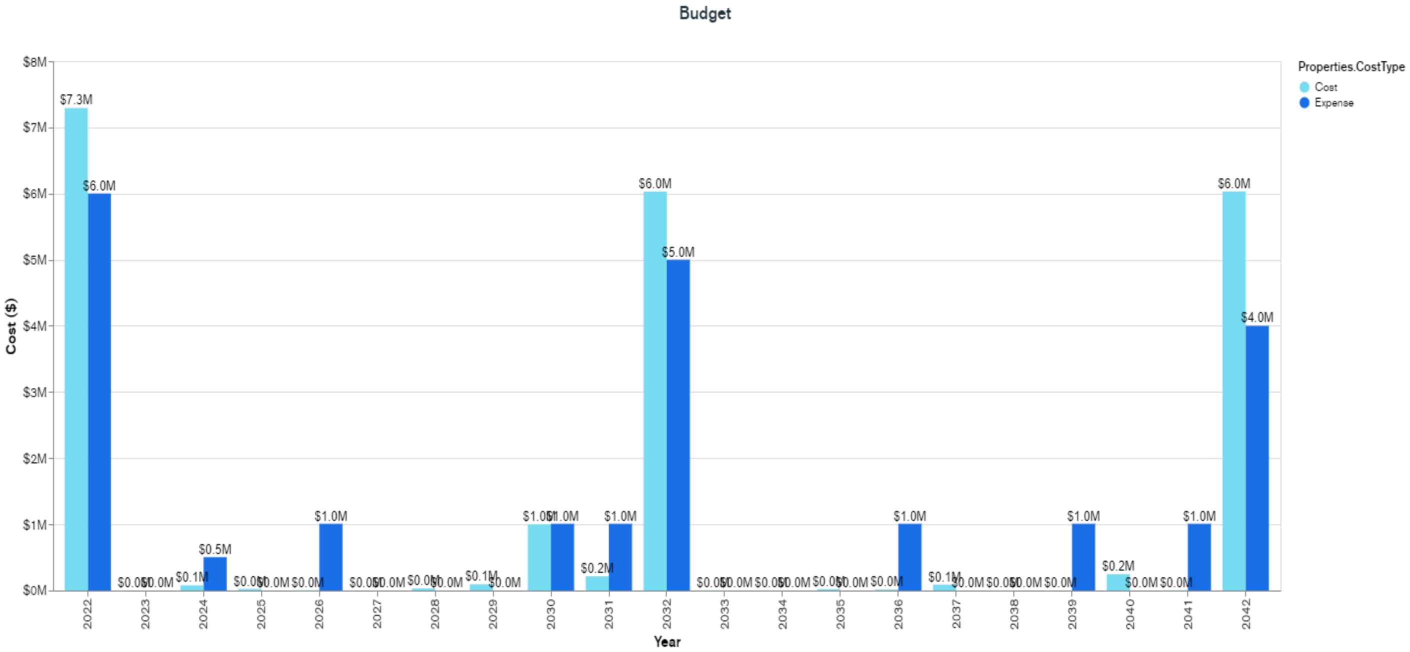


FIGURE 34: CAMS BUDGET RESULT IN CDM SIMULATION EXERCISE

To ensure that operation of the station does not get affected, optimisation of budget can be calculated using the resilience index discussed above. Further detail on budget optimisation is available on deliverable 7.5. For more details; refer to deliverable D8.3 and CAMS recorded presentation for CdM.

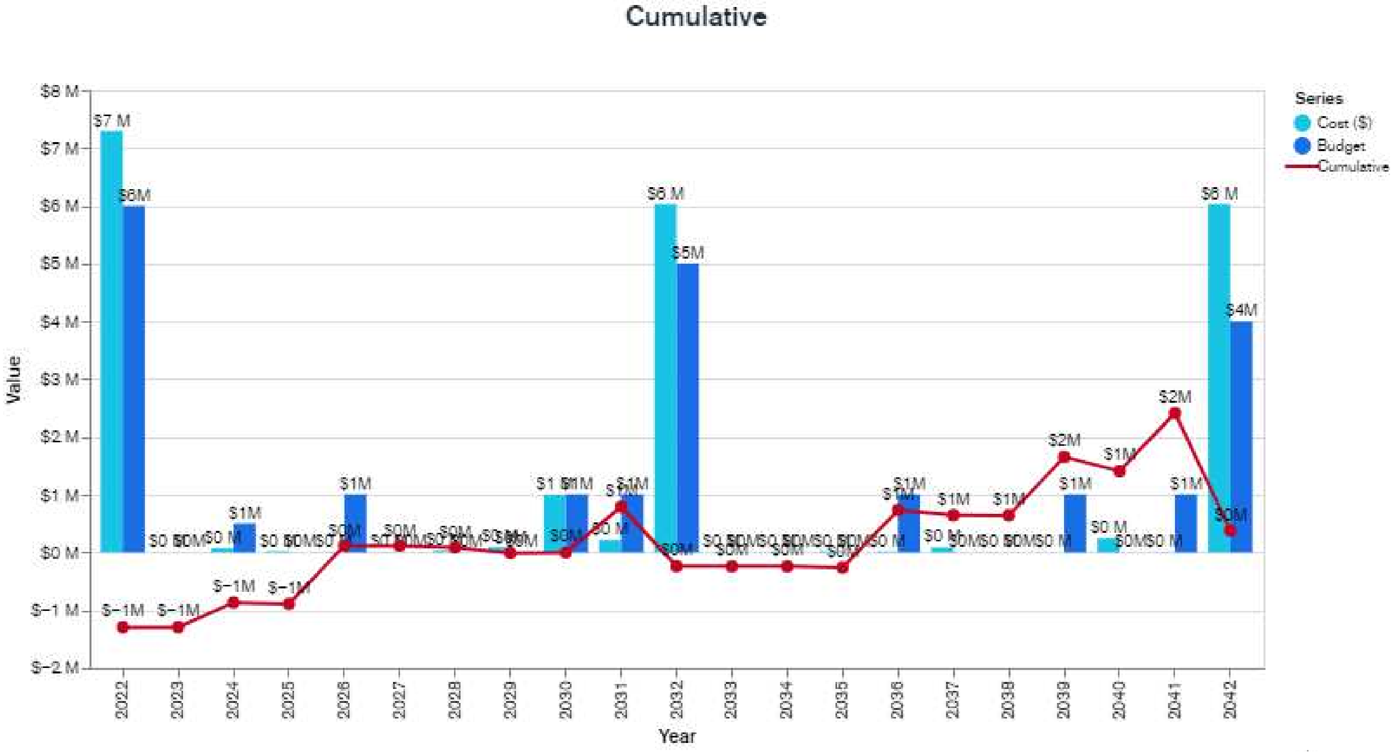


FIGURE 35: BUDGET CUMULATIVE DIFFERENCE

7. Future extensions (Dynamic Resilience Optimisation)

CAMS was the main software development in WP7. Many data exchanges could potentially be possible with other software artefacts, and some have been combined for further study, such as access and provision of asset management tool functionality to meet future end-user requirements. The effective budgeting for investments as targeted for resilience enhancement with respect to cyber-physical incidents is dependent on the categorisation and prototyping of the various incidents. Therefore, digitising cyber-physical events can generate additional vulnerabilities information for CAMS, which can make budget charts and predictive investment models more accurate. In this Chapter a novel framework is established to support iterative evolutionary Threats Severity Ranking and Combinatorial Countermeasures Prioritisation (TSR-CCP) to inform the maintenance of *agile resilience investments* by dynamic re-prioritisation of the most cost-effective set of safeguarding measures responsive to the evolution of the threat space -this requires iterative threats severity ranking to enable responsive countermeasures eco-system optimisation.

7.1 Threats Severity Ranking and Countermeasures (Re)-Prioritisation to support Dynamic Resilience Optimisation

In this section a novel framework is proposed to support iterative evolutionary Threats Severity Ranking and Combinatorial Countermeasures Prioritisation (TSR-CCP) to inform the maintenance of agile resilience investments by dynamic re-prioritisation of the most cost-effective set of safeguarding measures responsive to the evolution of the threat space -this requires iterative threats severity ranking to enable responsive countermeasures eco-system optimisation.

Within SAFET4RAILS, the work on the above framework (TSR-CCP) has been applied to the Cyber-Physical Privacy and Security threats as an example. However, the framework is underpinned by the generic UI-REF methodology for Use-Context-Aware Dynamic Requirements[11],[12]and as such can be applied to practically any threats, in any operational context, in any domain.

TSR-CCP was motivated by the shortcomings of the threat modelling state-of-the-art tools; in that these lack the following capabilities:

i) Transparent rating for likelihood of attack occurrence and attack impact rather than a black-box output as a generalised overall ranking
ii) Intuitively explainable threats severity ranking resolution
iii) Adequate coverage for the prioritisation of all the relevant attack vectors
iv) High resolution and dynamic use-context-specific threats prioritisation
v) Integrated heterogenous threats severity ranking
vi) Dynamic combinatorial re-prioritisation of countermeasures

The priority of a cyber-physical attack can vary depending on its potential context-specific impact. If a spoofing attack, for example, may result in the theft of sensitive (personal) data, this attack must be regarded as being of high severity as it can lead to large scale data breach and violation of legislation relating to data privacy protection; whereas, a spoofing attack on the audio broadcasting system is of a much lower severity, given that it is very unlikely to occur and that its impact would be comparatively limited and less critical. A threat modelling tool would treat all spoofing attacks to be of high priority -this is not cognisant of the context-specific variability of the impact of such an attack. This is primarily the reason why each attack vector output from a threat modeller would have to be subsequently re-examined and reprioritised using an operational context-aware severity ranking framework such as that which has resulted from this study.

Therefore, a novel framework has been established in order to address the above shortcomings and to support Agile Resilience Optimisation responsive to any threats in any domain.

The preparatory analysis for TSR-CCP and the full details of its development are documented in internal SAFETY4RAILS deliverables. Here we briefly outline the main phases of the development which started with a methodologically guided approach based on UI-REF and accordingly, in the first phase, an extensive Domain Knowledge Analysis of railway systems was conducted. This led to the second phase namely an ontology of railway systems which also delivered a mapping of the sub-ontology related to the threats of interest, namely, privacy-security threat types. Next, data flow models for the targeted operational contexts were derived based on this ontological mapping to support the semantic modelling of privacy-security threats. This enabled the framing of the assumptions arising from the railway systems architectural and operational use-context data flows, vulnerabilities and transaction types. Subsequently, threat modelling for both privacy and security threats was carried out using the threat modelling tools LINDDUN[6] and STRIDE[7] respectively.

Following this, the UI-REF Dynamic Requirements Prioritisation Methodology was applied to develop the Decision Framework based on severity ranking and responsive optimisation of the countermeasure sub-sets. In this phase the prioritised threats resulting from the privacy and security modelling tools were severity-ranked separately using a colour-coded tabularised schema to support the intuitive understanding of the proposed severity-ranking calculus and the TSR-CCP Decision Tables implementing it. Next the mapping from the highest-ranked threats to the corresponding vulnerabilities and their fixes enabled the associated countermeasures to be identified.

Finally, the two sets of all the highest-severity-ranked security and privacy threats were integrated together with their respective countermeasures and then the combinatorial countermeasures prioritisation rules were applied to eliminate redundancies in countermeasure sub-sets, resolve the priority subsets and arrive at the integrative countermeasure's prioritisation for both privacy and security threats.

In what follows, to keep the focus on the key stages of the TSR-CCP which are applicable to any threats in any domain, we start the analysis from the stage in the above pipeline after the semantic threat modelling for our exemplar threats (security and privacy) has been completed and has resulted in a set of threat-modeller-ranked security and privacy threat listings which are labelled and tabularised together with their respective countermeasures. This means that, for any other threats, all that need be done to be able to mirror the pipeline is to have identified the set of threats and their respective countermeasures for the application domain and then one is able to follow through with steps similar to what is described below as the generic rules and procedural stages of the TSR-CCP pipeline i.e. the TSR-CCP Decision Tables that implement the TSR-CCP rules. Here then we set out the principles (the rules) underpinning the TSR-CCP Decision Process. Thereafter we follow on the implementation steps of the framework in sifting through and ranking the privacy and security threats separately to conclude the severity ranking decisions for the single-threat-specific TSR tables and the prioritisation of their respective countermeasures.

Finally, we combine the tables of the highest-severity-ranked threats and their respective prioritised countermeasures and apply the TSR-CCP framework to this integrated prioritised list, iteratively, to arrive at the countermeasures prioritisation rules to be described later in this section.

7.2 (Meta) Rules and Procedures for Integrative Prioritisation of Threats and Responsive Countermeasures

The ultimate analysis goal is to proceed through all the aforementioned stages in order to finally arrive at a set of pruned and prioritised security and privacy threats and their respective prioritised countermeasures, effectively prioritised investments, to be actioned. Throughout this process, three fundamental sets of assumptions have had to be considered. The first set are assumptions regarding the security and privacy threat modelling stages. These particular assumptions relate to the use-contexts and the extent to which a threat is likely to occur in the specific operational context in which the usage scenarios are envisaged to run within the application domain.

The second set of assumptions relate to the level of risk that is assumed to be acceptable. It is a practical impossibility for absolutely every conceivable threat vector to be mitigated and to attempt to do so would run counter to the objective of optimal resilience. The ideal of 100% threat-proofing of a system, even if attainable, would require inordinately large scale of countermeasures and the interplay between various constraints would make the operational environment far too complicated; defeating both the goal of optimal operation and agile resilience assurance to evolve cost-effectively and efficiently[13]. Therefore, this analysis is based upon a realistic target of having between 80% to 90% of the *prioritised* threats being mitigated with

[6]https://www.linddun.org
[7]STRIDE-LM Threat Model - CSF Tools

their accompanying countermeasures. Thus, the mitigation strategies are designed to be deployed in order to mitigate the top 80-90% threats by prioritisation.

The third type of assumption is a countermeasure-pruning assumption that is applied in prioritisation of the threat and countermeasure sub-sets in order to arrive at a *minimum* set of countermeasures that are to be implemented and thus budgeted for as priority resilience investments. This process is required in order to optimise the managed mix of countermeasures as an evolving countermeasures echo system providing for maximum return (resilience) on investments.

In the case of the cyber-physical threats, this is to ensure that the finalised set of countermeasures are able to block and mitigate the privacy-security risks as much as possible, whilst also ensuring that there is minimum overlap in the countermeasures – i.e., that the orthogonality in the countermeasures pool is maximised as much as possible, whilst also ensuring that the required mutual complementarity of some countermeasures is maintained so that countermeasures can support one another in the case that a particular countermeasure does not function as intended.

This threat mitigation strategy is required in order to achieve the highest Return-on-Investment (RoI) for the implemented mitigation strategies in terms of protection against systemic and sub-systemic attacks that may impact different layers of the system in a vertical and/or horizontal manner and with variable severities of impact.

The necessary required first step in order to compile such a list of mitigation strategies is to establish the safeguarding priorities within the target domain. These particular priorities are dependent on the appropriate perception of risk and, here, on the most-valued privacy-security countermeasures as have been highlighted in the respective deployment contexts. These should, in turn, constitute a set of **A) Pragmatic** and **B) In-Principle** guidelines that would naturally point to the most optimal mix of countermeasures for the given domain context as per the rules set out in Table 13 below.

7.3 Establishing the Requisite Pragmatic and In-Principle Strategic Options for the selection of Countermeasures to mitigate Cyber-Physical Threats

Table 13, Pragmatic and In-Principle Strategic Options for the Selection of Countermeasures

In-Principle:

1. Protections against privacy threats must be prioritised against any security threats unless the security threat presents a risk to human life.

2. Moreover, threats, and thus their mitigating countermeasures, that act as a systemic threat must be prioritised over any threats that pose a risk at a sub-system level.

Pragmatically:

1) As the reduction of risks to zero is unattainable in any scenario, the selected countermeasures must mitigate the level of risk to an acceptable level: i.e., accepting the bottom 10-20% of threat vectors (lowest-severity-ranked), in each iteration as being possible risks that may or may not be mitigated by the selected, optimal mix of countermeasure strategies [13]. This is because the marginal mitigation utility of a specific countermeasure for each low-ranking threat, decreases significantly (diminishing return) and can even become negative in impose restrictions onto a system that result in greater in inconvenience than the potential impact the low-ranking threat might cause were it ever to materialise as an attack.

2) The framework must also ensure that the following criteria are fulfilled at all operational stages of the resilience optimisation:

- The formulation of 'work-around options' that are effectively non-digital countermeasures can act to eliminate or re-design operational steps that would otherwise naturally pre-dispose the system to a particular threat. This essentially removes or modifies the vulnerability sub-space thereby eliminating the threat and the need for its countermeasure(s).

- Specialised single-threat-blocking countermeasures should, when deemed necessary, be balanced by and work in conjunction with various multi-threat-blocking countermeasures in such a way as to formulate the most optimal mix of threat-specific and spectral countermeasures possible.

- The countermeasures, as aforementioned, should, overall, be in a position of optimal equilibrium re their relative mutual orthogonality/exclusivity/complementarity (e.g., minimising overlapping effect between countermeasures with some exceptions only when it can be seen that some complementarity could help prevent catastrophic failure i.e., whole system shut down an enable a self-limiting graceful degradation with essential safety (life and limb) protected.

- The lowest 10% of severity-ranked threats are not addressed, but the countermeasure(s) for any severity-ranked threats should be given higher priority if as a side-effect they can provide some protection against the lowest-severity threats.

TABLE 13: PRAGMATIC AND IN-PRINCIPLE STRATEGIC OPTIONS FOR THE SELECTION OF COUNTERMEASURES

7.3.1 Privacy-Security Threat Severity Ranking and Mitigation Procedure

To arrive at the optimum set of countermeasures the following privacy-security threat prioritisation and mitigation procedure is proposed.

1. Set out the selected threats to be mitigated as derived through vulnerabilities analysis and/or a threat modelling tool.
2. Establish the typology of the relevant attacks in terms of the various privacy threats, security threats (whether systemic or sub-systemic in nature) and the operational model of the threats themselves in terms of their pre-condition(s) and trigger(s) whether the execution of the attack requires synchronous triggers, and/or complex orchestration with other attack types, and other possible specific attributes of the attack(s).
3. Apply In-Principle and Pragmatic Assumptions for Threat Priority Resolution as set out in Table 13 above.

    - Determine the Impact Severity and Threats Likelihood related to the system architecture use-cases and operational deployment context.
    - Categoric Threat Sets Severity Ranking: Establish the scale of attack impacts in terms of the extent of (sub)systemic impacts of each attack type:
        - In the context of our example threat categories here, namely cyber-physical privacy-security threats, the privacy threats tend to materialise into attacks which involve systemic impacts (data breaches comprising mainly Personally Identifiable Information (PII)-relevant information[14].
        - Privacy-security impacts (partial or total leakages of PII data that arising from malicious actor(s) exploiting some systemic vulnerability), as well as very-high impact threats compromising the operational security of the whole system and possibly endangering the lives of train passengers.

4. Individual Threats Severity Ranking: resolve the severity ranking of remaining threats in accordance with the Severity Ranking Calculus as shown in Table 14,Table 15 and Table 16 below.

7.4 Combinatorial Countermeasures Prioritisation Procedure

This is to determine the responsive countermeasures for the severity-ranked threats and carry out a comparative and contrastive analysis of the relative merits of each respective countermeasure in order to establish an optimal set of countermeasures that mitigate the 80-90% of the highest-severity threats as follows:

I. Exploit the countermeasures topology: identify countermeasures sub-set using a relationships-based model of relevant countermeasures so as to integrate an optimal echo-system of countermeasures. Consider the relative effectiveness and efficiency of each countermeasure in terms of its relative strength relative to others and its overlap with other countermeasures; this constitutes a Criteria of Merit, including:

- Mitigation-value
- Implementation complexity
- Systemic or sub-systemic protection capability

- Single-attack-blocking, attacks cluster blocking, attack-type-agnostic-block (spectral mitigation)
- Upgrade-of Relationship - of already adopted categorically prioritised countermeasures
- Mutuality* (Mutual Orthogonality/Exclusivity/Complementarity/ of effects
- Self* properties (protective against attacks on self, self-aware, self-auding, self-diagnostic)
- Cross* properties: cross-asset type protective, cross-platform integrative, interoperable,

II. Optimise the prioritisation of countermeasures for best trade-off in respect of as many Criteria of Merit as possible e.g., particularly in terms compound criteria such as relative efficacy which is based on:

- Number of (sub)systemic threats mitigated relative to implementation complexity
- Number of sub-systems that would have to be re-adapted in order for the respective countermeasure to be integrated into the legacy system (system in its present current condition) - this can be represented as the 'number-of-interconnects' to be added/modified

Table 14below provides a characterisation of the countermeasures threat mitigation value within a particular calculus that is based upon the above formula in terms of efficacy versus resource investment needed (time, set-up and operational cost) and interconnect complexity of a countermeasure to be ranked into 1) Gold. (workaround), 2) Gold -Digital, 3) Silver, 4) Bronze.

Table 14, Countermeasure Prioritisation - Mitigation-Value-Efficacy-Complexity Model	
Countermeasures Ranking	Context-Aware Countermeasures Threat Mitigation- Value based upon Cost/Implementational-Complexity Assessment Criteria
GOLD (Non-Digital) Countermeasure: Operational Workaround)	**A Procedural Countermeasure** that is implemented through a re-design of the operational deployment modes and/or system interactions with the user and the environment. This is specifically designed to eliminate the pre-disposing factors that expose the system to a particular threat. Therefore, the threat is eradicated as the critical attack pre-condition(s) and/or trigger(s) are removed, preventing the threat from ever originating or materialising as an attack.
Gold-Digital Countermeasure	**A Spectral Countermeasure** that provides either local critical or systemic protection against one or more of the highest-ranking threats. It does so with high efficacy and relatively low complexity: in other words, the countermeasure is relatively easy to implement in terms of resources invested and implementation complexity, whilst still being very effective at mitigating the most dangerous threats and/or mitigating a large number of different threats, providing a very high amount of safeguarding coverage within the system.
Silver Countermeasure	**A Cluster Countermeasure** that blocks several local (i.e., sub-systemic) attack vectors with acceptable level of efficacy versus cost and complexity as can be computed by the following mathematical expression: Relative Efficacy or Mitigation Value of Countermeasure = <number_of_attack_triggers_mitigated_by_the_countermeasures> / <number_of_interconnects needed>* <investment resources required>
Bronze Countermeasure	**A Partial Countermeasure that** would block only a single attack trigger or acts as a mutually complementary countermeasure to a number of high efficacy countermeasures; however, it may not be capable of mitigating a threat by itself and would have relatively low mitigation value as assessed based on Relative Efficacy or Mitigation Value of Countermeasure = <number_of_attack_triggers_mitigated_by_the_countermeasures> / <number_of_interconnects_-needed>* <investment_resources _required>

TABLE 14: COUNTERMEASURE PRIORITISATION - THREAT MITIGATION-VALUE-EFFICACY-COMPLEXITY MODEL

7.5 Integrating the Threat Severity Ranking Calculus and Countermeasures Prioritisation

In order to arrive at a finalised set of countermeasures that are most optimal for the given use-case, one must prioritise the threats themselves at a resolution that is greater than that of typical threat modelling tools, such as the Microsoft STRIDE modeller [15][16].In order to do so, one must integrate the probabilistic assessment of two attributes of each threat being considered:

a) the likelihood of the threat resulting in an attack

b) the impact of the threat if it were to materialise as an attack.

The assessment of the values of the above two attributes of an attack, enables the overall severity ranking of the threat to be derived. Moreover, given to the duality of likelihood-impact ranking, one can exercise attack-teleology-informed context-aware rankings of threats which amount to pragmatically reasonable judgements re the overall severity with appropriate level of weighting accorded to the level of likelihood or impact depending on the operational context. For example, a threat with a high-impact-severity ranking may be deemed of still higher impact than another high-impact-severity threat if the former threat has a greater likelihood of occurrence.

This intuitive calculus facilitates practitioners' threat ranking and can be applied to severity-rank any threats or a combination of threats in any domain.

7.5.1 Ranking the Likelihood of Occurrence of Attacks

Initially we identify each specific threat to which the system may have some vulnerability as can be established by a threat modelling tool/process including through practitioners' security analysis. Each such identified threat is then given a ranking for the likelihood of it materialising as an attack. This likelihood of attack occurrence can take one of the following values: 'Very Low', 'Low', 'Medium', 'High', and 'Very High'. Such probabilistic determination is fundamentally at the discretion of the security and resilience planning staff and can be estimated, as is normally the case, on a data-driven and/or experiential knowledge basis of the practitioners. However, the colour-coded visualisation schema provides support for practitioners in intuitive reasoning through the threats severity ranking calculus and its explainability. Various factors relevant to the use-context, exposed attack surfaces and vectors would need to be considered in arriving at the determination of overall severity ranking in each case.

Firstly, one must assess the various pre-conditions/triggers that need to be fulfilled in order for the attack vector to be initiated. These triggers must be considered in terms of their synchronicity (orchestration, sequential, simultaneous), time-bound, channel-bound, and distance-bound conditions that may need to be fulfilled, as may be the case, for each respective threat to translate to an attack.

The more likely the pre-conditions that are expected to be fulfilled within the system, the higher the likelihood of the threat turning into an attack. Similarly, the smaller the number of pre-conditions that are required to be fulfilled for the attack to occur, the more likely that the attack will occur [17], and thus it should be allocated a greater severity ranking.

Threats that require no active triggers for them to turn into an attack, and that just require some pre-condition that may be a static feature of the system design, are more likely to give rise to an attack than a threat type that requires both a pre-condition and trigger for its execution. This may involve, for instance, user co-participation, synchronicity, or time/channel/distance conditions in order to be fulfilled. A man-in-the-middle attack, for instance, requires data to be transmitted between two entities, along some unauthorised/insecure route and with possibly some other timing/sequencing/co-location constraints also satisfied for the attack to be successfully executed[18].

In general, the fewer the conditions that have to be met for a threat to lead to an attack within a given system architecture and workflow design, the more likely the threat will turn into an attack. Potential cyber-attacks pre-conditions are set out in Table 15 below.

Table 15, Potential Preconditions for a Cyber-Physical Attack to Occur & Succeed	
1.	Critical dependency on a-priori knowledge (such as a user's password) as a pre-requisite

2.	Requiring a specific, complex sequence of steps that are pre-conditions/triggers to one another.
3.	Requiring steps that are synchronous with other events; for example, a particular user being online.
4.	Requiring time-bound and/or timing-critical steps.
5.	Requiring multi-actor-dependent steps.
6.	Requiring cyber-physically co-placed and/or co-located steps.
7.	Requiring single or multi-stage execution for the attack to successfully occur.
8.	Requiring steps that span across two or more platform/channels of authentication.
9.	Requiring wide-spread orchestration and/or swarm mobilisation.
10.	The existence of common countermeasures that are already assumed to be integrated within the system design and thus must be overcome before the attack can be initiated.
11.	The flexibility of sequence of steps that need to be executed; if this can be in any arbitrary order/timing/distance then this would reduce the threshold for an attack to be triggered and successfully executed.
12.	Requiring insider knowledge related to the actual context of the attack and credentials (e.g., specific employee interactions and/or physical entities within the target context that may alter how a cyber-attack can be carried out).

TABLE 15: POTENTIAL PRECONDITIONS FOR A CYBER-PHYSICAL ATTACK TO OCCUR-SUCCEED

7.5.2 Assessing the Likely Impact of a Threat were it to materialise as an Attack

The second phase of the severity ranking is to estimation of the likely scale of impact should a particular privacy or security attack occur. The *teleological signature* of an attack, i.e., *the theory of action and purpose* as determinants of ultimate objectives of an attack, in general, constitute the key pointers to the scale and nature of the impact of the attack. As such, the rules for the assessment of impact of privacy and security attacks are similar and are set out as follows:

7.5.2.1 Privacy Threats Impact Assessment

After having applied the initial assumptions so as to eliminate the inapplicable privacy threats and assessed the respective likelihood of the relevant privacy threats according to the aforementioned rules, one can proceed to assess their respective impacts in the order of severity as follows.

From a privacy impact analysis perspective, some personal data elements are categorised as being highly sensitive and confidential. These are data elements relating to properties/attributes such as health data, gender identity, financial data or any associated data element(s) that may enable a malicious actor to deduce elements of such sensitive data points Thus, any threats that could lead to unauthorised access to any confidential data, including such personal data, has to be classified as of high impact.

The more sensitive and confidential the (personal) data is, the greater the assumed impact of and data breach[19].The assessment of how high the impact would be dependent on the user-specified confidentiality level and respective privacy protection preferences in for a specific use-context and covering a range from the most sensitive personal data or most mission-criticality business confidential data to the data with relatively less sensitivity). Additionally, the higher the number of sensitive data items (PIIs) that could potentially be compromised, the greater the perceived impact of the threat should be and vice versa.

The ranking of the privacy impact of an attack type that has not directly targeted personal or other confidential data, should be based on the quantity/number of personal or other confidential data elements that are indirectly compromised and ultimately on the number of data elements that a malicious actor may be able to infer as a result of a particular attack.

7.5.2.2 Security Threats Impact Assessment

Subsequent to having applied the initial assumptions as to eliminate the redundant/inapplicable security threats and having assessed the likelihood of every relevant security threat, one can proceed to ranking the impact of the threat itself.

The criteria for ranking the impact assessment of security threats would be based on the scale of damage their attack may cause as follows:

1. Any attack that could potentially pose a danger to human life or cause injury.
2. Any attack vector that could potentially result in an existential risk to the system as a whole, or to a set of subsystems i.e., a systemic-scale attack to disrupt the normal order of operations drastically and/or cause a stoppage of operations in their entirety.
3. Any threat that could result in a malfunction in more than one subsystem, especially the respective subsystems that are required for mission critical areas of the enterprise operational frontline and in this example on the railway systems operational network.
4. For the attack types that can have a potentially negative impact on the same number of subsystems, the attack type that is able to target the most critical subsystem of the set should be ranked as being of the highest severity. In general, the higher the number of subsystems that are impacted, the higher the threat severity ranking should be. Moreover, as aforementioned, if the number of subsystems that are impacted are identical, the threat(s) should be prioritised in accordance with the critical importance of the impacted subsystem(s),

Potential cybersecurity attacks pre-conditions are set out in Table 16 below.

Table 16, Criteria for Ranking the Overall Severity of the Impact of a Cyber-Physical Threat Materialised as an Attack	
1)	Teleological Fingerprint-Footprints (The Trajectory of Action & Purpose), Ultimate Objective of the Attack
2)	The scale and nature of the resulting attack in terms of significance with respect to all (privacy and security) violations.
3)	The sensitivity of the data that is breached.
4)	The extent to which any Personally Identifiable Information (PII) is stolen e.g., the stolen data can be linked to a particular identity.
5)	The extent of stolen passwords, multi-factor authentication credentials, secret keys, biometrics among other confidential and security parameters / values.
6)	The extent to which the attack can enable the cloning and duplicate confidential security credentials for one-time or multiple usage.
7)	The IoT-enabled and Cyber-Physical nature of the attack - thus a hybrid attack
8)	The swarming type attack wave – e.g., a Distributed Denial of Service (DDoS) attack.
9)	The respective boundaries of the various data pipelines and/or system layers that could be compromised through the attack.
10)	The lack of any intermediary defence (firewall) between the entry point and the most critical sub- systems.
11)	The various (if any) cascading effects of the threat vector.
12)	The involvement of any other associated and orchestrated malicious attack vectors, such as a large-scale biometric spoofing attack designed to facilitate other attack vectors.
13)	The mission criticality of the attacked sub-systems and the resulting functionality degradation.
14)	The extent of the operational downtime resulting from the attack and the required time for recovery.
15)	The extent of the direct and/or indirect financial, reputational, and human losses caused by the attack.

TABLE 16: CRITERIA FOR RANKING THE OVERALL SEVERITY OF THE IMPACT OF A THREAT MATERIALISED AS AN ATTACK

The above rules are summarised in the colour-coded decision Table 17, below to support the TSR-CCP pipeline.

Table 17, Colour-Coded Severity Ranking Rules for Cyber-Physical Threats Likelihood of Occurrence and Impact			
Likelihood	Likelihoods Ranking – Indicative Determinants	Impacts	Impacts Ranking Indicative Determinants

Very Low	If the attack vector requires many different preconditions to occur and/or several countermeasures are already in place that would mitigate the attack vector.	Very Low	The Privacy-Security attack vector would only partially affect one sub-system and would not cause further damage within the system. In effect, the system would run practically normally; however, the attack vector would have caused some inconvenience.
Low	If the attack vector requires several preconditions to occur and/or countermeasures are already in place to safeguard against the potential attack.	Low	Data Privacy-Security Breach that would affect one data-subject /sub-system and would not extend beyond secondary elements of personal data or beyond a sub-system. Any damage inflicted onto the respective subsystem is minor and would thus not cause any downtime.
Medium	If the attack vector requires more than two preconditions to occur and/or no countermeasures are already in place to safeguard against the potential attack.	Medium	Data Privacy-Security Breach that would impact more than one data-subject/sub-system and/or extend beyond secondary elements of personal data. The attack as a whole would cause considerable functional degradation but limited downtime (i.e., the subsystem(s) would be able to recover quickly).
High	If the attack vector requires one or two preconditions to occur and no countermeasures are already in place to safeguard against the potential attack.	High	The attack vector would either affect many data-subjects and extend to various sensitive PIIs resulting in a systematic data breach / loss of consumer privacy. Moreover, if the attack vector is a security one, the attack would result in critical malfunctions and catastrophic and cascaded effects / downtime. The respective downtime may be temporary; however, there would be a period of time in which the system is out of service. In addition to this, there are also likely to be some irrecoverable costs, such as irreversible damage to reputation and some loss of market share.
Very High	If the attack vector requires no preconditions to occur and no countermeasures are in place to safeguard against the potential attack, and not even partial mitigation strategies are in place against the potential attack.	Very High	An attack vector with an impact rating of 'very high' would cause immense, potentially permanent, damage to the system in question. In terms of a privacy threat, the respective data breach would be so severe that the enterprise would face legal proceedings for substantial violations of the data protection regulations and would incur huge financial losses, considerable reputational damage and legal measures that may threaten the future operation of the system in question. Moreover, as a security attack this could also result in severe damage to operational assets and injury to human actors and/or loss of life.

TABLE 17: SEVERITY RANKING RULES FOR CYBER-PHYSICAL THREATS LIKELIHOOD OF OCCURRENCE AND IMPACT

Now that the framework of rules and procedures for cyber-physical Threat Severity Ranking and Combinatorial Countermeasures Prioritisation (TSR-CCP) have been elaborated and tabularised, we can proceed to implement the complete TSR-CCP Decision Framework by progressing from severity ranking of single and then multiple threats to the prioritisation of their individual countermeasures, and finally to prioritising the integrative security-privacy combinatorial countermeasures.

7.5.2.3 TSR-CCP Reference Schema for Colour-Coded Threats-Countermeasures Ranking Visualisation-Explanation

The following sections set out the deployment of the TSR-CCP Decision Framework which is described stage-by-stage and also illustrated using a colour-coded visually intuitive schema to support the ranking and prioritisation pipeline to reduce the cognitive load and enhance the expressivity of the TSR-CCP decision process[20].

Table 18 below presents the Reference Colour Coding Schema to be used in the TSR-CCP Ranking Decision Tables.

Table 18, TSR-CCP Decision Tables Colour Coding Schema Reference Table for Estimation of Likelihood of Attack Occurrence, Impact upon Occurrence and Efficacy of Countermeasure Sets	
Threat/Countermeasures Type / Integrative Countermeasures Prioritisation Resolution	Colour Coding
Privacy Threats	Light Green
Actionable Privacy Countermeasures	Warm Green

<table>
<tr><td colspan="3">Security Threats</td><td colspan="3">Light Purple</td></tr>
<tr><td colspan="3">Actionable Security Countermeasures</td><td colspan="3">Pink</td></tr>
<tr><td colspan="3">Gold Class Countermeasures</td><td colspan="3">Gold</td></tr>
<tr><td colspan="3">Silver Class Countermeasures</td><td colspan="3">Silver</td></tr>
<tr><td colspan="3">Bronze Class Countermeasures</td><td colspan="3">Bronze</td></tr>
<tr><td colspan="3">Threat / Countermeasure to be Omitted at Final Design Stage Due to the top 90% highest-severity attacks mitigation rule</td><td colspan="3">Sky Blue</td></tr>
<tr><td colspan="6"><b>Severity Ranking Colour Scheme & Legend</b></td></tr>
<tr><td><b>Severity Levels Assessment Legend:</b></td><td>▶▶ Very Low</td><td>▶ Low</td><td>▶ Medium</td><td>▶ High</td><td>▶▶ Very High</td></tr>
</table>

TABLE 18: TSR-CCP DECISION TABLES COLOUR CODING SCHEMA REFERENCE TABLE FOR ESTIMATION OF LIKELIHOOD OF ATTACK OCCURRENCE, IMPACT UPON OCCURRENCE AND EFFICACY OF COUNTERMEASURE SETS

7.6 Cyber-Physical Security Threat Modeller Output as Augmented by Expert Practitioners

Table 19, Table 20 and Table 21, below, list the security and privacy threats as generally prioritised by the threat modelling tools (respectively STRIDE and LINDDUN) plus the selected cyber-physical security-privacy threats to which, specifically, the IoT-enabled railway system are exposed considering their particular operational use-contexts.

Accordingly, for the railway systems domain, the security threat modelling tool generated a total of 315 cyber security threats. However, only 73 of these threats were deemed to be distinct threats of which some could be merged, and some others could be unified. The final list of threats as tabularised and indexed for processing in the following Table 19 and Table 20 amounted to 49 most relevant security threats selected from the threat modeller tool plus a further 35 specialised threats that are specific to the SAFETY4RAILS framework, resulting in a total of 84 security threats as indexed, labelled, analysed and severity-ranked within the respective TSR-CCP decision tables. The privacy modelling tool output resulted in 9 selected privacy threats as set out in Table 21.

After the conclusion of the TSR-CCP, 33% were ultimately ranked as high severity, a further 34% as medium severity and finally 26% were deemed low severity. Using TSR-CCP the countermeasures responsive to each set of severity-ranked security and privacy threats were identified and in turn these countermeasures were ranked using the Combinatorial Countermeasure Prioritisation rules to arrive at the 38 highest priority countermeasures prescribed for implementation planning to mitigate a total of 363 security and privacy threats as resulted from the initial threats modelling phase.

The list of indexed Cyber-Physical Security Attack Vectors particularised for IoT-enabled Railway Systems as input to the TSR-CCP Decision pipeline, is as follows in Table 19 below.

Table 19, Specialised Security Attack Vectors for IoT-enabled Railway Systems

Threat ID	Cyber-Physical Threat Type	Category	Priority	State	Justification
AA!	General Distributed Denial of Service Attack	Active Cyber-Attacks	High	Mitigated	High availability of services within the railway sector and the S4R framework.
AA2	Man-in-the-Middle (MitM) Attacks	Active Cyber-Attacks	High	Mitigated	High availability of services within the railway sector and the S4R framework.
AA3	Eavesdropping Attacks	Active Cyber-Attacks	Medium	Mitigated	High availability of services within the railway sector and the S4R framework.

Table 19, Specialised Security Attack Vectors for IoT-enabled Railway Systems

Threat ID	Cyber-Physical Threat Type	Category	Priority	State	Justification
AA4	Wardriving Attack	Active Cyber-Attacks	Medium	Mitigated	High availability of services within the railway sector and the S4R framework.
AA5	Theft of Private Data Stored in Customer SQL Database	Active Cyber-Theft	High	Mitigated	High availability of services within the railway sector and the S4R framework
AA6	Ransomware Attack	Active Cyber-Attacks	High	Mitigated	High availability of services within the railway sector and the S4R framework.
AA7	Manipulation of Public Information Display (PID) System	Active Cyber-Attacks	Low	Needs Investigation	Unique emerging threat. S4R will have innovative mitigation strategy.
AA8	Drive-by-Download Attack via Wireless AP	Active Cyber-Physical Attack	Medium	Mitigated	High availability of services within the railway sector and the S4R framework
AA9	Backdoors/Supply-Chain Attacks	Active Cyber-Attacks	Medium	Mitigated	High availability of services within the railway sector and the S4R framework.
AA10	Web Application Attacks	Active Cyber-Attacks	Low	Mitigated	High availability of services within the railway sector and the S4R framework.
AA11	Zero-Day Exploits/Vulnerabilities/Attacks	Active Cyber-Attacks	Medium	Mitigated	High availability of services within the railway sector and the S4R framework.
AA12	Insider Threat	Active Cyber-Physical Attack	High	Needs Investigation	Awareness Training Required. Will be part of S4R innovative framework.
UD1	Human Error	Unintentional Damage	High	Needs Investigation	Awareness Training Required. Will be part of S4R innovative framework.
UD2	Unencrypted Data Transmission	Unintentional Damage	Medium	Mitigated	High availability of services within the railway sector and the S4R framework.
UD3	Insecure Systems/Policies	Unintentional Organisational Error	High	Mitigated	Secure Organisational Policies and Training is part of the S4R Countermeasure Framework
UD4	Multi-layered Attacks that Exploit Cascading Effects	Active Cyber-Physical Attack	High	Mitigated	High availability of services within the railway sector and the S4R framework.
SF1	Spoofing	Active Cyber-Attacks	High	Mitigated	High availability of services within the railway sector and the S4R framework.
SF2	Social Engineering Attack	Active Cyber-Attacks	High	Needs Investigation	Awareness Training Required. Will be part of S4R innovative framework.
SF3	Personal Data Interception via Transmission over Wireless AP	Active Cyber-Attacks	High	Mitigated	High availability of services within the railway sector and the S4R framework.
SF4	Direct Data Theft from Ticketing System	Active Cyber-Attacks	High	Mitigated	High availability of services within the railway sector and the S4R framework.
FM1	Chain-Effect from Disruption to External Service Providers	Unintentional Organisational Error	Medium	Needs Investigation	S4R framework will include respective countermeasures to combat interconnected threats.
FM2	Failure of Devices/Systems	Unintentional Damage	Medium	Mitigated	High availability of services within the railway sector and the S4R framework.
FM3	Lack of Resources/Available Storage	Unintentional Damage	Low	Mitigated	High availability of services within the railway sector and the S4R framework.
L1	Regulation/Violation of Laws	Legal	Medium	Needs Investigation	Awareness Training and Regulation Framework provided by S4R framework.
CPT1	Sabotage of Wayside Devices	Active Cyber-Physical Attack	High	Mitigated	High availability of services within the railway sector and the S4R framework.
CPT2	Sabotage of HVAC System	Active Cyber-Physical Attack	Low	Mitigated	High availability of services within the railway sector and the S4R framework.

Table 19, Specialised Security Attack Vectors for IoT-enabled Railway Systems					
Threat ID	Cyber-Physical Threat Type	Category	Priority	State	Justification
CPT3	Sabotage of Carriage CCTV System	Active Cyber-Physical Attack	Medium	Mitigated	High availability of services within the railway sector and the S4R framework.
CPT4	Manipulation of Audio Broadcasting System	Active Cyber-Attacks	Low	Mitigated	High availability of services within the railway sector and the S4R framework.
CPT5	Direct Attack on Critical SCADA System	Active Cyber-Attacks	High	Mitigated	High availability of services within the railway sector and the S4R framework.
CPT6	Sabotage of GSM-R Radio used in Communication Flow	Active Cyber-Physical Attack	High	Mitigated	High availability of services within the railway sector and the S4R framework.
CPT7	Sabotage of LTE Tower used in Communication Flow	Active Cyber-Physical Attack	High	Mitigated	High availability of services within the railway sector and the S4R framework
CPT8	Specialised Infrared Attack	Active Cyber-Physical Attack	Medium	Needs Investigation	Highly specialised attack that will be mitigated by the S4R framework
CPT9	Specialised Radio Interference Attack	Active Cyber-Physical Attack	Medium	Needs Investigation	Highly specialised attack that will be mitigated by the S4R framework
CPT10	Specialised Electromagnetic Interference Attack	Active Cyber-Physical Attack	Medium	Needs Investigation	Highly specialised attack that will be mitigated by the S4R framework
CPT11	Sabotage of Train Vehicles through Direct Attack	Active Cyber-Physical Attack	High	Mitigated	High availability of services within the railway sector and the S4R framework.

TABLE 19: SPECIALISED SECURITY ATTACK VECTORS FOR IOT-ENABLED RAILWAY SYSTEMS

The Cyber-Physical Security Attack Vectors as generated by the Threat Modelling Tool are indexed and listed in Table 20 below.

Table 20, Generated Security Attack Vectors by Threat Modelling Software/Framework					
ThreatID	Cyber Security Threat Type	Category	Priority	State	Justification
ST1	Spoofing of Train Systems	Spoofing	Low	Mitigated	Strong authentication and authorisation within the S4R framework.
ST2	Spoofing of Train Cameras	Spoofing	Low	Mitigated	Strong authentication and authorisation within the S4R framework.
ST3	Spoofing of Ethernet Switch	Spoofing	Low	Mitigated	Strong authentication and authorisation within the S4R framework.
ST4	Denies Ethernet Switch Potentially Writing Data	Repudiation	Low	Mitigated	Best cyber security practices within the S4R framework.
ST5	Data Flow Train Bus Is Potentially Interrupted	Denial Of Service	Medium	Mitigated	Best cyber security practices within the S4R framework.
ST6	Data Store Inaccessible	Denial Of Service	Low	Mitigated	Best cyber security practices within the S4R framework.
ST7	External Entity Adversary Potentially Denies Receiving Data	Repudiation	Medium	Mitigated	Best cyber security practices within the S4R framework.
ST8	Weak Access Control for a Resource	Information Disclosure	Low	Mitigated	Strong authentication and authorisation within the S4R framework.
ST9	The Ethernet Switch Could Be Corrupted	Tampering	Medium	Mitigated	Best cyber security practices within the S4R framework
ST10	Spoofing of TCMS -	Spoofing	High	Mitigated	Strong authentication and authorisation within the S4R framework.
ST11	Spoofing of HMI	Spoofing	Medium	Mitigated	Strong authentication and authorisation within the S4R framework.
ST12	Spoofing of Train Router	Spoofing	Medium	Mitigated	Strong authentication and authorisation within the S4R framework.

Table 20, Generated Security Attack Vectors by Threat Modelling Software/Framework					
ThreatID	Cyber Security Threat Type	Category	Priority	State	Justification
ST13	Spoofing of GSM-R Radio	Spoofing	High	Mitigated	Strong authentication and authorisation within the S4R framework.
ST14	Spoofing of Destination LTE Tower	Spoofing	High	Mitigated	Strong authentication and authorisation within the S4R framework.
ST15	Adversary Denies LTE Tower Potentially Writing Data	Repudiation	High	Mitigated	Best practices of logging and digital signature within the S4R framework.
ST16	Data Flow GSM-R Flow Is Potentially Interrupted	Denial Of Service	High	Mitigated	Best cyber security practices within the S4R framework.
ST17	Adversary Denies GSM-R Radio Potentially Writing Data	Repudiation	High	Mitigated	Best practices of logging and digital signature within the S4R framework.
ST18	Spoofing of Operational Control Centre	Spoofing	High	Mitigated	Strong authentication and authorisation within the S4R framework.
ST19	Denies Firewall Potentially Writing Data	Repudiation	Low	Mitigated	Best cyber security practices within the S4R framework.
ST20	Data Flow LTE Flow Is Potentially Interrupted	Denial Of Service	High	Mitigated	Best cyber security practices within the S4R framework.
ST21	Adversary Denies Operational Control Centre Potentially Writing Data	Repudiation	Medium	Mitigated	Strong authentication and authorisation within the S4R framework.
ST22	Spoofing of Wayside Devices	Spoofing	Medium	Mitigated	Strong authentication and authorisation within the S4R framework.
ST23	Adversary Denies Wayside Devices Potentially Writing Data	Repudiation	High	Mitigated	Strong authentication and authorisation within the S4R framework.
ST24	Data Flow IP/MPLS Flow Is Potentially Interrupted	Denial Of Service	Medium	Mitigated	Best cyber security practices within the S4R framework.
ST25	Spoofing of Train Stations	Spoofing	Low	Mitigated	Strong authentication and authorisation within the S4R framework.
ST26	Spoofing of Other trains	Spoofing	Low	Mitigated	Strong authentication and authorisation within the S4R framework.
ST27	Adversary Denies Other Trains Potentially Writing Data	Repudiation	Medium	Mitigated	Strong authentication and authorisation within the S4R framework.
ST28	Spoofing of Ticketing System	Spoofing	Medium	Mitigated	Strong authentication and authorisation within the S4R framework.
ST29	The Operational Control Centre Could Be Corrupted	Tampering	High	Mitigated	Best cyber security practices within the S4R framework.
ST30	Data Flow Malicious IP/MPLS Flow Is Potentially Interrupted	Denial Of Service	Medium	Mitigated	Best cyber security practices within the S4R framework.
ST31	Spoofing of Public Information Display System	Spoofing	Medium	Mitigated	Strong authentication and authorisation within the S4R framework.
ST32	Spoofing of Customer Database	Spoofing	High	Mitigated	Strong authentication and authorisation within the S4R framework.
ST33	The Ticketing System Could Be Corrupted	Tampering	Medium	Mitigated	Best cyber security practices within the S4R framework.
ST34	Adversary Denies Ticketing System Potentially Writing Data	Repudiation	Medium	Mitigated	Strong authentication and authorisation within the S4R framework.
ST35	Data Flow Ticket Interaction Is Potentially Interrupted	Denial Of Service	Low	Mitigated	Best cyber security practices within the S4R framework.
ST36	Spoofing of Audio Broadcasting System	Spoofing	Low	Mitigated	Strong authentication and authorisation within the S4R framework
ST37	Spoofing of Station HVAC System	Spoofing	Low	Mitigated	Strong authentication and authorisation within the S4R framework.
ST38	Spoofing of Carriage HVAC System	Spoofing	Low	Mitigated	Strong authentication and authorisation within the

Table 20, Generated Security Attack Vectors by Threat Modelling Software/Framework

ThreatID	Cyber Security Threat Type	Category	Priority	State	Justification
					S4R framework.
ST39	The Station HVAC System Could Be Corrupted	Tampering	Low	Mitigated	Best cyber security practices within the S4R framework.
ST40	Adversary Denies Station HVAC System Potentially Writing Data	Repudiation	Low	Mitigated	Best cyber security practices within the S4R framework.
ST41	Spoofing of Train Station CCTV System	Spoofing	Medium	Mitigated	Strong authentication and authorisation within the S4R framework.
ST42	The GSM-R Radio Could Be Corrupted	Tampering	High	Mitigated	Best cyber security practices within the S4R framework.
ST43	Lower Trusted Subject Updates Logs	Repudiation	Medium	Mitigated	Best practices of logging and digital signature within the S4R framework.
ST44	Data Logs from an Unknown Source	Repudiation	Medium	Mitigated	Best practices of logging and digital signature within the S4R framework.
ST45	Adversary Denies Train Router Potentially Writing Data	Repudiation	Medium	Mitigated	Best cyber security practices within the S4R framework.
ST46	Spoofing of Passenger Wireless AP	Spoofing	High	Mitigated	Strong authentication and authorisation within the S4R framework.
ST47	Adversary Denies Passenger Wireless AP Potentially Writing Data	Repudiation	High	Mitigated	Best cyber security practices within the S4R framework.
ST48	The Passenger Wireless AP Could Be Corrupted	Tampering	Medium	Mitigated	Best cyber security practices within the S4R framework.
ST49	Authenticated Data Flow Compromised	Tampering	High	Mitigated	Strong authentication and authorisation within the S4R framework.

TABLE 20: GENERATED SECURITY ATTACK VECTORS BY THREAT MODELLING SOFTWARE/FRAMEWORK

7.7 Cyber-Physical Privacy Threat Modeller Output as Augmented by Expert Practitioners

Table 21, below, sets out the Privacy Threats identified as potentially likely in the operational context of the IoT-enabled Railway Systems.

Table 21, Privacy Threats in the Operational Context of the IoT-enabled Railway Systems

Privacy Threat ID	Privacy Threat Definition
PT1	**Data linkable to other data store** Data entries within the IoT railway system can be linked to the same individual.
PT2	**Linkability of Customer, Transaction, CCTV, and Travel Data** Data flows and entries within the smart IoT railway system can be traced back and linked to the same individual(s).
PT3	**Linkable login using untrusted and/or unencrypted communication** The login of the user, in any area of the S4R framework, can be linked to his/her identity.
PT4	**Data linkable to login data** The user's identity is revealed due to the malicious interception of data flow(s) that are transmitted within the IoT railway system and that contain respective privacy data.
PT5	**Non-anonymous Communication that is then traced to the entity itself** Given the non-anonymous nature of the communication flow, the user's / passenger's identity can be revealed if it is intercepted by a MisActor.

PT 6	**Based on Session ID** The user's identity is revealed using the session ID as a proxy.
PT7	**Policy and Consent Noncompliance** Third parties (Railway Operators) do not process user personal data in compliance with the user's consent and other EU regulatory policies.
PT8	**Consent Inaccuracy** The relevant employees failed to update the consent information of the respective users.
PT 9	**Non-Repudiation of an Update** The employee / system fails to update the customer's information whenever a transaction or change is made.

TABLE 21: PRIVACY THREATS IN THE OPERATIONAL CONTEXT OF THE IOT-ENABLED RAILWAY SYSTEMS

7.8 Strategies and Criteria for Prioritisation of Countermeasures

This section of the threat-driven analysis highlights the various countermeasures. The nature of the respective countermeasures varies drastically as is expected. Some countermeasures offer systemic protection against a range of attack types as may occur in a number of operational use-contexts e.g., 'Multi Factor Authentication' (MFA) [21], other countermeasures may offer a narrower, sub-systemic or single use-context protection. This section provides an analysis of the distinctions between various attack sources and respective countermeasures that inform the ranking of threats and countermeasures as implemented in the TSR-CCP decision pipeline.

7.8.1 The Castle Approach to Cyber-Security Mitigation Strategies

The Castle Approach, or otherwise referred to as Defence in Depth, is a very well-known information assurance concept within the field of cybersecurity [22]. The fundamental aim of such an approach is to combine multiple layers of different security defences around a given system. This is specifically done to ensure that, if one particular countermeasure fails, there are multiple other countermeasures that overlap and mitigate the cyber-attack vector [23][24][25]. This cyber-defence strategy is often divided into three areas: namely, administrative defence, technical defence, and physical defence.

Administrative Defence

Administrative defences refer to any policy, framework, and/or procedure that is specifically set out by the organisation in order to clarify access and data protection restrictions for their given infrastructure system. The key objective of these respective policies is to ensure that logic-based guidelines exist that employee can follow in effect, individuals are aware of an effective response procedure to the various security challenges and regulations, which exist within that particular organisation. These countermeasures may include, for instance, general security requirements, hiring practices, and data handling procedures among many others.

Physical Defence

This category of countermeasures is simply the set of all countermeasures that enforce a physical limit that the adversary in question must overcome in order to access the infrastructure system itself. Such defences are incredibly common and can include, for example, reinforced doors, guard dogs, cameras, and any other protective and/or surveillance equipment deemed necessary.

Technical Defence

Technical defence system countermeasures are very similar to the aforementioned physical defence countermeasures in their objective; however, they focus more on the software/hardware side of the system that needs protection. Examples of such countermeasures may include biometric-based systems, for instance, which contain fingerprint readers, iris scanners, and many other authentication services.

7.9 Prioritised Cyber-Security Countermeasures for IoT-enabled Railway Systems

IoT-enabled railway infrastructure systems are complex systems that rely on many different technologies throughout the entirety of their network-centric hardware/software stack including passenger-facing, operational frontline, back-office and management decision support systems. Such a system requires a multi-layered resilience engineering approach with specialised security countermeasures as use-context-specific and sub-systems-specific security-privacy attacks countermeasures as well as some of the more generalisable countermeasures (i.e., countermeasures that can be found in any/most infrastructure systems). For example, some countermeasures, such as the use of 'Multi Factor Authentication' [21]will naturally apply to a range of cyber-attacks. Such types of countermeasures are often not powerful enough to completely block a threat by themselves; however, they can offer complementary mitigation to some other related countermeasures against some threats. Other countermeasures are designed to mitigate only a few specific attacks as these particular threat vectors are highly specialised to the given domain such as IoT-enabled Railway Systems.

Following the TSR severity ranking of threats the corresponding commonly deployed countermeasures were tabularised and indexed so that they could be prioritised. The Countermeasures Prioritisation involved the consideration of the aforementioned CCP rules relating to the Countermeasure set relationship (mutual complementarity /exclusivity, the efficacy (mitigation-value), for given cost-complexity as well as common criteria based on established previous analysis regarding countermeasures mitigation strategies as follows:

Accordingly, following the aforementioned TSR-CCP rules 27 highest priority cyber security countermeasures for the IoT-Enabled Railway systems were concluded as defined below:

Physical Defences (SCM1)

Physical defences are simply countermeasures that are specifically designed to mitigate cyber-physical attacks. Such defences can include walls, doors, fences, secure door-locks, security guards, and any other surveillance equipment deemed necessary [25].

Honeypots (SCM2)

Honeypots are a type of computer security mechanism that is designed to detect and counteract attempts of adversaries to access data through an unauthorised manner. In this context, the aim of the honeypot is to redirect the adversaries to attack a "dummy" part of the system. In other words, the adversaries are redirected to attack a part of the system that seems legitimate by nature, but it is actually isolated and enables the monitoring of the adversary and their respective actions[26].

Monitoring (SCM3)

Monitoring refers to network monitoring that is very similar to an IDS. However, network monitoring aims to monitor network traffic that exists from within the network rather than outside. In addition to this, its objective is not to detect attacks but rather to detect the status of the servers themselves: to gather information about their availability, uptime, and response time. If the benchmark of a monitored host drops for any reason, an administrator will have automatic notification, so that they can investigate the issue further [27].

Encryption (SCM4)

Encryption is a mathematically based cryptographic process that is used to convert information into ciphertext using a secret key. Thus, only authorised individuals can decrypt and process the information again. Encryption should be in place for any sensitive data that is transferred or handled within the system[28]. Common examples of a hash-function encryption technique are that of SHA-256 and SHA-512.

Intrusion Prevention Systems (SCM5)

An Intrusion Prevention System (IPS) is a network security prevention technology that is designed to continuously monitor network traffic with the intent to detect and prevent security incidents by taking the necessary corresponding actions. These actions may include some or all of the following, to drop malicious packets, to notify the administrator, to block traffic from the source and to reset the malicious connection itself[29].

Role-based Access Control (SCM6)

Role-Based Access Control (RBAC) aims to restrict access to various network resources based on the role/privilege of a user. Thus, RBAC enforces the security measure that employees are only allowed to access the necessary information required in order to fulfil their work. Thus, users with low privileges (if configured correctly) should not be able to access sensitive information[30].

Strong Password Policies (SCM7)

Strong password policies fall into the exact same category as awareness training. This is due to the fact that employees tend to use easy-to-remember passwords, which tend to be very weak passwords by their very nature. Strong password policies should therefore be enforced and follow expert recommendations [31]. In addition to this, users should be required to regularly reset their passwords. Therefore, even if there is a password breach, any leaked passwords would be made redundant as they will be commonly reset and updated.

Awareness Training (SCM8)

This involves awareness training policies within IT cyber security in order to ensure that all employees possess the fundamentals of cyber security training. For example, all employees should be able to detect phishing and ransomware attacks and should make every decision/action within the domain in a manner that upholds all standard cybersecurity policies and measures[32].

Intrusion Detection Systems (SCM9)

An Intrusion Detection System (IDS) is a network security detection technology that is very similar to an IPS. Exactly like an IPS, an IDS is designed to also continuously monitors network traffic, but it only focuses on the detection of security incidents. Any intrusion detected is then reported to the respective administrator or to any other relevant member(s) of the management team [33].

Penetration Testing (SCM10)

Penetration testing is an authorised and simulated cyber-attack against an organisation's networks or systems. This test acts as an extremely realistic way to test implemented security measures, and to find any corresponding methods of improvement [34]. However, penetration test experts, in contrast to cyber criminals, are usually limited by their resources (e.g., time, money), so they cannot realistically cover the entire scope of possible attacks on the network. Moreover, penetration test experts may not even be as skilled as certain cyber criminals who tend to be extremely apt in hacking and computer technology in general.

Whitelisting vs Blacklisting (SCM11)

Blacklisting and whitelisting are both strategies that are designed to assist in ensuring that networks, applications, infrastructure systems are kept secure. A whitelisting policy aims to block every entity that is not on a specified pre-defined list. On the other hand, blacklisting accepts every entity except those that exist on a pre-defined list. Blacklisting is commonly used in a public network, where entities should be allowed to access the system, except those with malicious intent. Whitelisting is commonly used for private networks, where access should only be granted to a specific trusted group. Inevitably, there exists the possibility of incorporating a hybrid approach of whitelisting and blacklisting in a multi-layer network [35].

Firewalls (SCM12)

A firewall is a network security system that monitors incoming and outgoing network traffic in a computer network based on several, predetermined security rules. Firewalls are normally used to establish a barrier between a trusted internal system and a corresponding untrusted external system. It is important to note that the network filtering rules need to be updated regularly to adapt to changes in the systems - in other words, to mitigate the negative effects of 'concept drift'. The filtering can happen on several layers, such as the application layer, network layer or simply by filtering each network packet separately. Furthermore, firewalls can also be placed at network barriers or just directly on host computers that control all of the network traffic on each machine [36].

Air-Gapped Networks (SCM13)

An air gap is a rather extreme network security measure. In this scenario, a secure computer is physically isolated from any network that is considered insecure. Normally, this means that data can only be exchanged by using a removeable storage medium, such as external hard drives or flash drives – it is not connected to any network, especially not a network that is connected to the Internet in some fashion. Critical infrastructure systems usually have air-gapped systems for backup and critical systems. Air-gapped networks, however, still have their – albeit specialised – cyberattack vulnerabilities [37].

Multifactor Authentication (SCM14)

Multifactor authentication is a method which only grants the user access if the user can present at least two or more pieces of predetermined evidence to an authentication method. This 'evidence' can vary in nature and can be distance, channel, knowledge, medium or time bound. An example could be (1) knowledge – something that only the user knows, such as a password; (2) inherence – something that is unique to the user, such as a biometric fingerprint; (3) possession – something that only the user should possess, such as a hardware token [38].

Anomaly Detection (SCM15)

Anomaly detection is the process of automatically identifying unexpected events or items in a data set. In network monitoring, for example, an anomaly could be an unusual data stream that might occur during a cyber-attack. Anomaly detection systems are usually developed using state-of-the-art neural networks, such as Generative Adversarial Networks (GANs) [39].

Antivirus Software (SCM16)

Antivirus software (AV software) is a standard and common cyber-security approach for companies and private users [40]. AV solutions are used to detect, prevent, and remove malware. In addition to this, modern solutions also have in-built browser extensions that are able to detect malware when accessing malicious websites. These are especially useful for any sensitive work, such as online interactions with a railway system (e.g., when a consumer may be purchasing a ticket online).

Input Sanitisation and Output Encoding (SCM17)

Input sanitisation and output encoding are particularly good practices within software development. In such a technique, each input is cleared from any illegal characters and every piece of data presented is properly encoded. A faulty or missing implementation of this could lead to the unexpected behaviour of a system, which could then be exploited via common attacks, such as SQL injections and/or Cross Site Scripting (XSS)[41].

Password Hashing (SCM18)

Cryptographical hash functions are common one-way transformation of converting passwords into a hash. Such a process is irreversible and should therefore be used on any sensitive information before it is stored into a database [42]. However, it is vital to use state-of-the-art algorithms in order to be safe from hash-collisions and brute-force attacks.

Data-centric Security (SCM19)

Data-centric security focuses on the security of the data within a network, rather than the security of the networks, servers, or applications - the actual architecture of the network itself. Large institutions and infrastructures usually provide such data-centric security though in-house systems; however, they may also rely on infrastructure that is provided by large service providers, such as Amazon Web Services (AWS) or Microsoft Azure [43].

Logging and Auditing (SCM20)

Logging and auditing information is another important standard practice within IT security. In any form of logging, it is necessary to log any data that can be used to reconstruct and analyse any future incidents. However, it is very important that no sensitive data is logged (such as passwords) as this may just contribute to a database breach [44].

Virtual Private Networks (SCM21)

Virtual Private Networks (VPN) are used to extend a secure, private network across an insecure public network, such as the Internet. This enables users to access computers, send, and receive data and access applications that are running in the private network. This is also commonly used for remote work and allows for users securely connect to a network from practically anywhere in the world [45]. To ensure outmost security, the connection is often established by an encrypted layered tunnelling protocol. In an IoT railway system setting, a VPN can be used to connect critical components of the infrastructure with a centralised backend or to connect ticketing machines with the private network of the railway SCADA system.

Pro-active Update and Maintenance of Software alongside corresponding Penetration Testing to Ensure Patches/Updates are Effective (SCM22)

Many cyber-attacks are only launched due to old vulnerabilities that are found within various propriety software used by the infrastructure system itself. By constantly updating and maintaining software, network administrators are able to mitigate the number of attacks that rely on old (already 'patched') vulnerabilities within the software. Moreover, penetration testing should also be correspondingly used whenever a piece of software is updated, or a 'patch' is applied, in order to ensure that the update itself does not introduce any new vulnerabilities [46].

Design-embedded legislation and standardisation compliance (SCM23)

Newly built systems should always be compliant with the relevant standardisation and legislation in respect to the numerous governing legal bodies within the domain of railway systems and their respective cybersecurity measures, all the way from the design phase to the deployment of the system itself. This is especially important when handling sensitive data.

Sandboxing (SCM24)

Sandboxing is a security measure that is used to run software processes in containers that are separated from other software. The sandbox possesses its own memory space and storage and is further limited in accessing other resources, such as networking or reading data from / writing data to other devices. The overall aim of sandboxing is to prevent software vulnerabilities from spreading or to prevent one faulty process from negatively affecting other processes [47]. This means, for example, that a railway system app on a mobile phone cannot be affected by any other malicious application on the same mobile device, mitigating various mobile-based drive-by-download, wardriving, or phishing attacks.

Awareness Training and High-Quality Management for Security and Cyber-Intelligence Team (SCM25)

Close co-operation with and management of various cyber/counter-intelligence teams that will facilitate the necessary methods to mitigate against any potential cyber-physical attacks before they even occur [48]. For example, an intelligence team, working closely with the required authorities, could discover and prevent a terrorist attack plot before the attack is actually carried out. This is very common within critical national infrastructure systems, such as the railway system domain.

Biometrics (SCM26)

Various forms of biometrics, such as fingerprints and/or iris detection can be used as an authentication method [49]. Despite their seeming complexity, biometric scans are not fully secure and thus they are usually incorporated within several multi-factor authentication processes [50].

Emergency Protocol for Unexpected Disruptions to System (SCM27)

There is a possibility that, although the railway system/organisation itself may not have been directly attacked, it is negatively impacted due to an attack on a third-party organisation that the system relies on. Therefore, extensive emergency plans and protocols have to be put in place in preparedness for countering the cascaded effects of any such attacks occurring; so that should such a situation arise, the railway organisation will be able to quickly and effectively mitigate the negative impacts that could potentially follow from such "supply-side shocks" and ensure operationally continuity with albeit temporarily at sub-capacity. A potential solution may include, for instance, direct access to multiple third-party vendors; thus, if one vendor/supplier falls victim to a cyber-attack, the railway system can rely on the provision of goods and services from another third-party organisation. This same planned organisational policy of building in some reserve capacity, essentially contingently deployable spare resources fir selected critical and potentially vulnerable components, should also be applied to mitigate against any unexpected disruptions to the organisation itself: for example, through a sudden lack of storage and/or failure of critical devices.

7.10 Prioritised Privacy Threat Countermeasures for IoT-enabled Railway Systems

The following section sets out the prioritised privacy safeguarding measures, arrived at through the TSR-CCP pipeline after analysis of the various privacy threats to which the operational use-contexts of IoT-enabled Railway Systems could be exposed. Unlike security threats, threats that target the privacy side of a domain are far more generalisable between various infrastructure systems. Therefore, here we define a list of priority countermeasures that could mitigate any privacy threats within such a railway system network. Due to the complexity of this system, typically user data are processed on a large scale whether this be financial or geographical in nature, thus it is absolutely imperative that strong, rule-based access control is in place as well as countermeasures to ensure the integrity of such a system and to prevent and mitigate against the risks of any data breach and privacy threats specifically.

Legal guidance (PCM1)

Legal advice is to be sought to ensure that a system is compliant with local and international data protection directives as applicable to all systems and services involved in processing any data as well as any data transfer across jurisdictions.

Project/Programme Management (PCM2)

A project/programme management should be established that adopts an integrated security and privacy-by-design approach that is deliberatively risk-aversive and threat-driven. The system is also to be designed with safeguards in place to prevent, protect and mitigate as many threats as possible to ensure that the respective management programme is efficient by nature.

Security Assessment and Authorisation (PCM3)

It is absolutely imperative to ensure that security standards have been complied with, and the security assessment and authorisation process and privacy risks analysis are conducted to inform the deployment of safeguarding measures and in particular to be able to demonstrate and document that all necessary sensitive, shared data is stored and processed on secure and reliable systems.

Awareness and Training (PCM4)

A system of training end-users and/or staff has to be put in place to raise awareness about how to keep various data assets, particularly any personal data, secure and how an attacker may target such data. Selected policies for organisational level privacy risk aversive protocols can be formulated for staff to follow, as well as for any users that interact with the network [51] – e.g., through any financial interaction or sharing of data. An example use-case may be a security warning to a user, whenever they connect to a Wireless Passenger Access Point, which highlights the potential risks of joining a public network and processing any sensitive data on the respective network.

Incident Response (PCM5)

This involves a specific, versatile, and coherent plan to minimise the negative impacts of any privacy-security attack and to restore the system as fast as possible to its safe operational condition as is normally to be maintained.

Maintenance (PCM6)

To ensure that the system (software and hardware) is kept up-to-date; avoiding all known Common Vulnerabilities and Exposures (CVEs) [52], as these would facilitate/provide an attacker with direct access to a system or network and expose the system to the real risk of data breaches that may lead to personal data privacy being compromised on a large scale.

System and Information Integrity (PCM7)

This involves providing assurances that the system is performing its intended functions and its information is consistent and unchanged despite any attacks/changes/disruptions that may occur.

Access Control Mechanism (PCM8)

The system must establish and maintain compliance and audit the end-to-end security of the rule-based system that is to ensure role-based access policy control for specific parts in the network and system under the specific pre-determined conditions with execution to be regularly audited and reviewed at randomly selected points-of-inspection [30].

Securing Network Communication (PCM9*)*

This countermeasure acts to ensure that no network traffic can be intercepted. For example, this may involve tunnelling data transfers through a VPN and/or using a security protocol, such as HTTPS [53][45].

Trust Management (PCM10)

The implementation of an abstract trust-model-based system for the allocation of trust/access permissions to the various technical members of staff in accordance with their respective access rights.

Anonymisation (PCM11)

The act of removing or irreversibly altering personally identifiable information (PII) from data sets, such that the data subject being described is anonymous. The process could also involve the use of a secret key to ensure that the data can be reversed if necessary, such as for a legal investigation [54].

7.11 TSR-CCP Pipeline Decisions Implementation

7.11.1 Applying the TSR-CCP rules to the Security Threats Severity Ranking and Responsive Countermeasure Prioritisation

The security threats severity ranking pipeline starts from the weighted assessment of the chance of the risk occurring, its impact upon occurrence, the difficulty of executing the attack, and the number of preconditions and triggers that are required to be fulfilled if the attack is to be executed. The previously tabulated rules (Table 15,Table 16 and Table 17) were applied to the security and Privacy threats list in Table 19, Table 20 and Table 21, respectively, to arrive at the threats severity rankings for security and privacy threats as tabularised in the decision tables that follow, Table 22, and Table 23 respectively. The subsequent TSR-CCP decision tables set out the integrated security-privacy threats. Thereafter the corresponding countermeasures are prioritised by reference to the Combinatorial Countermeasures Prioritisation rules as set out in Table 14.

The tabularised colour-coded visualisation in the following TSR-CCP decision tables follows a consistent format throughout and is designed to avoid cognitive overload for any operator/manager/resilience planning staff by presenting the required information in a clear, coherent and explainable manner[20].

The first column (*Security Threat*) represents the index of the security threat which can be referenced with the attack vectors as previously labelled, tabularised and indexed.

The second column (*Likelihood of Attack Occurrence*) is to represent the probability that a security/privacy threat will occur within the system, as defined by the rules in Table 15.

The third column (*Impact upon Attack Occurrence*) represents the scale of the expected disruptions, harm and losses of resulting from the attack as estimated based on the TSR rules set out in Table 16.

The fourth column (*Overall Severity Ranking)* is the overall ranking of the threat as deduced by the aforementioned TSR rules.

The fifth column, *Ranked Threats (Highest to Lowest),* represents the respective ranking of all the security threats within the system from highest to lowest. Thus, the first attack vector in the table is deemed to be that of the highest-severity-ranking, and the last attack vector is that of the lowest severity.

The sixth and last column (Prioritised *Countermeasures)* provides the countermeasures for the adjacent attack vector found in the '*Ranked Threats (Highest to Lowest)*'.The Ranked Cyber Security Threats and their Countermeasures for the IoT-Enabled Railway Systems are presented in the Security Threats Severity Ranking Decision Table (Table 22) below. In this table, consistent with the Reference Colour Coding Table (Table 18), a 'light purple and pink' colour schema is used to represent the security threats; the lighter and darker shades highlighting representing, respectively, the threats to be ranked and already ranked as I the final column.

Table 22, TSR-CCP Security Threat Ranking Decision Table for the IoT-enabled Railway Systems

Rubric	🟦🟦 Very Low	🟦 Low	🟧 Medium	🟥 High	🟥🟥 Very High
Security Threat	Likelihood of occurrence	Impact upon occurrence	Overall Threat Severity Ranking		Safeguarding Measures
			Overall Severity Ranking of the Threat	Ranked Threats (Highest to Lowest)	Prioritised Countermeasures for Severity Ranked Security Threats
AA1	🟧	🟥	🟥	CPT11	SCM8, SCM1, SCM25
AA2	🟧	🟥	🟥	ST16	SCM14, SCM1, SCM15, SCM27
AA3	🟧	🟧	🟧	ST20	SCM14, SCM1, SCM15
AA4	🟦	🟥	🟧	CPT5	SCM25, SCM1, SCM8, SCM22
AA5	🟧	🟥	🟥	CPT1	SCM1, SCM5
AA6	🟧	🟥	🟥	CPT6	SCM1, SCM3, SCM11
AA7	🟦🟦	🟧	🟦	CPT7	SCM1, SCM3, SCM11
AA8	🟧	🟧	🟧	ST17	SCM14, SCM1, SCM26, SCM27
AA9	🟦	🟧	🟧	ST15	SCM14, SCM1, SCM26, SCM22
AA10	🟦	🟦	🟦	ST18	SCM5, SCM9, SCM2, SCM14
AA11	🟧	🟧	🟧	ST29	SCM1, SCM6, SCM4, SCM10, SCM14, SCM27, SCM20
AA12	🟧	🟥	🟥	ST42	SCM20, SCM24, SCM23, SCM22, SCM1
UD1	🟥	🟥	🟥	SF2	SCM8, SCM7, SCM14
UD2	🟧	🟧	🟧	UD1	SCM8, SCM7, SCM14

Table 22, TSR-CCP Security Threat Ranking Decision Table for the IoT-enabled Railway Systems

Rubric	🟦🟦 Very Low	🟦 Low	🟧 Medium	🟥 High	🟥🟥 Very High
Security Threat	Likelihood of occurrence	Impact upon occurrence	Overall Threat Severity Ranking		Safeguarding Measures
			Overall Severity Ranking of the Threat	Ranked Threats (Highest to Lowest)	Prioritised Countermeasures for Severity Ranked Security Threats
UD3	🟧	🟥	🟥	AA12	SCM8, SCM7, SCM14, SCM6
UD4	🟧	🟥	🟥	AA1	SCM15, SCM3, SCM21
SF1	🟧	🟥	🟥	AA2	SCM15, SCM10, SCM4, SCM9
SF2	🟥🟥	🟥	🟥	AA5	SCM4, SCM6, SCM7, SCM14
SF3	🟧	🟥	🟥	AA6	SCM8, SCM6, SCM10, SCM15, SCM16
SF4	🟧	🟥	🟥	UD4	SCM25, SCM22, SCM19, SCM10
FM1	🟦	🟥	🟧	SF1	SCM14, SCM15, SCM8
FM2	🟦	🟥	🟧	SF3	SCM4
FM3	🟦🟦	🟧	🟦	SF4	SCM4, SCM26, SCM6, SCM1
L1	🟦🟦	🟥	🟧	ST13	SCM5, SCM9, SCM2, SCM15
CPT1	🟦	🟥🟥	🟥🟥	ST14	SCM5, SCM9, SCM2, SCM15
CPT2	🟦🟦	🟧	🟦	ST32	SCM5, SCM9, SCM2, SCM14, SCM3, SCM4,
CPT3	🟦	🟧	🟧	ST23	SCM14, SCM1
CPT4	🟦🟦	🟧	🟦	UD3	SCM8, SCM19, SCM25
CPT5	🟦	🟥🟥	🟥🟥	ST49	SCM3, SCM13, SCM5, SCM6, SCM10
CPT6	🟦	🟥🟥	🟥🟥	ST47	SCM14, SCM1, SCM26
CPT7	🟦	🟥🟥	🟥🟥	ST46	SCM5, SCM9, SCM2, SCM14
CPT8	🟦🟦	🟥🟥	🟧	AA4	SCM15, SCM10, SCM4, SCM9
CPT9	🟦🟦	🟥🟥	🟧	FM1	SCM27, SCM8
CPT10	🟦🟦	🟥🟥	🟧	ST5	SCM14, SCM1, SCM15
CPT11	🟧	🟥🟥	🟥🟥	ST10	SCM5, SCM9, SCM2, SCM14
ST1	🟦🟦	🟥	🟦	ST11	SCM5, SCM9, SCM2, SCM14
ST2	🟦🟦	🟦	🟦🟦	ST22	SCM5, SCM9, SCM2, SCM14
ST3	🟦🟦	🟥	🟦	ST27	SCM14, SCM1, SCM26
ST4	🟦🟦	🟥	🟦	ST45	SCM14, SCM1, SCM26
ST5	🟦	🟥	🟧	ST9	SCM1, SCM3, SCM5
ST6	🟦🟦	🟦	🟦🟦	ST12	SCM5, SCM9, SCM2, SCM14
ST7	🟧	🟧	🟧	FM2	SCM27
ST8	🟦🟦	🟧	🟦	AA3	SCM15, SCM10, SCM4
ST9	🟦	🟥	🟧	AA11	SCM22, SCM12
ST10	🟦	🟥	🟧	AA8	SCM5, SCM9, SCM4

Table 22, TSR-CCP Security Threat Ranking Decision Table for the IoT-enabled Railway Systems					
Rubric	🟦🟦 Very Low	🟦 Low	🟧 Medium	🟥 High	🟥🟥 Very High
Security Threat	Likelihood of occurrence	Impact upon occurrence	Overall Threat Severity Ranking		Safeguarding Measures
			Overall Severity Ranking of the Threat	Ranked Threats (Highest to Lowest)	Prioritised Countermeasures for Severity Ranked Security Threats
ST11	🟦	🟥	🟧	UD2	SCM4
ST12	🟦	🟥	🟧	ST28	SCM5, SCM9, SCM14, SCM15
ST13	🟧	🟥	🟥	ST24	SCM14, SCM1, SCM15, SCM27
ST14	🟧	🟥	🟥	ST30	SCM14, SCM1, SCM15
ST15	🟦	🟥🟥	🟥🟥	ST33	SCM20, SCM24, SCM23, SCM22
ST16	🟧	🟥🟥	🟥🟥	ST31	SCM5, SCM9, SCM2, SCM14
ST17	🟦	🟥🟥	🟥🟥	ST34	SCM14, SCM1, SCM26
ST18	🟦	🟥🟥	🟥🟥	ST7	SCM19, SCM6, SCM1
ST19	🟦🟦	🟧	🟦	ST44	SCM19, SCM20, SCM18, SCM26, SCM14
ST20	🟧	🟥🟥	🟥🟥	ST43	SCM20, SCM18, SCM19, SCM14, SCM26
ST21	🟦🟦	🟥	🟧	ST48	SCM20, SCM24, SCM23, SCM22, SCM1
ST22	🟦	🟥	🟧	CPT8	SCM14, SCM15, SCM25, SCM27
ST23	🟧	🟥	🟥	CPT10	SCM14, SCM15, SCM25, SCM27
ST24	🟧	🟧	🟧	CPT9	SCM14, SCM15, SCM25, SCM27
ST25	🟦🟦	🟧	🟦	L1	SCM23
ST26	🟦🟦	🟧	🟦	ST21	SCM14, SCM1
ST27	🟦	🟥	🟧	CPT3	SCM1, SCM3, SCM11, SCM13
ST28	🟧	🟧	🟧	AA9	SCM19, SCM12
ST29	🟦	🟥🟥	🟥🟥	ST41	SCM5, SCM9, SCM2, SCM14
ST30	🟧	🟧	🟧	ST1	SCM5, SCM9, SCM2, SCM14
ST31	🟧	🟧	🟧	ST4	SCM14, SCM1
ST32	🟧	🟥	🟥	ST3	SCM5, SCM9, SCM2, SCM14
ST33	🟧	🟧	🟧	CPT2	SCM1, SCM5
ST34	🟧	🟧	🟧	AA7	SCM19, SCM9, SCM3
ST35	🟧	🟦	🟦	FM3	SCM27
ST36	🟦🟦	🟧	🟦	CPT4	SCM19, SCM9, SCM3
ST37	🟦🟦	🟧	🟦	ST8	SCM7, SCM14, SCM26
ST38	🟦🟦	🟦	🟦🟦	ST25	SCM5, SCM9, SCM2, SCM14
ST39	🟦	🟦	🟦	ST19	SCM14, SCM1
ST40	🟦	🟦	🟦	ST26	SCM5, SCM9, SCM2, SCM14
ST41	🟦	🟧	🟧	ST37	SCM5, SCM9, SCM2, SCM14

Table 22, TSR-CCP Security Threat Ranking Decision Table for the IoT-enabled Railway Systems					
Rubric	🟦🟦 Very Low	🟦 Low	🟧 Medium	🟥 High	🟥🟥 Very High
Security Threat	Likelihood of occurrence	Impact upon occurrence	Overall Threat Severity Ranking		Safeguarding Measures
			Overall Severity Ranking of the Threat	Ranked Threats (Highest to Lowest)	Prioritised Countermeasures for Severity Ranked Security Threats
ST42	🟦	🟥🟥	🟥🟥	ST36	SCM5, SCM9, SCM2, SCM14
ST43	🟧	🟧	🟧	ST35	SCM14, SCM1, SCM15
ST44	🟧	🟧	🟧	ST39	SCM20, SCM24, SCM23, SCM22, SCM1
ST45	🟦	🟥	🟧	AA10	SCM17, SCM18, SCM4
ST46	🟥	🟧	🟥	ST40	SCM14, SCM1, SCM26
ST47	🟥	🟧	🟥	ST2	SCM5, SCM9, SCM2, SCM14
ST48	🟧	🟧	🟧	ST38	SCM5, SCM9, SCM2, SCM14
ST49	🟧	🟥	🟥	ST6	SCM19, SCM15

TABLE 22: TSR-CCP SECURITY THREAT RANKING DECISION TABLE FOR THE IOT-ENABLED RAILWAY SYSTEMS

7.11.2 Applying TSR-CCP to the Privacy Threats Severity Ranking and Responsive Countermeasure Prioritisation

Table 23 below shows The Ranked Privacy Threats and Countermeasures for the IoT-Enabled Railway Systems.

Table 23, TSR-CCP Privacy Threat Ranking Decision Table for the IoT-enabled Railway Systems					
Rubric	🟦🟦 Very Low	🟦 Low	🟧 Medium	🟥 High	🟥🟥 Very High
Privacy Threat ID	Likelihood of occurrence	Impact upon occurrence	Overall Threat Severity Ranking	Safeguarding Measures	
			Overall Severity Ranking of the Threat	Ranked Threats (Highest to Lowest)	Prioritised Countermeasures for Severity Ranked Privacy Threats
PT1	🟦	🟥	🟧	PT2	PCM9 PCM10 PCM11
PT2	🟧	🟥🟥	🟥🟥	PT7	PCM3 PCM1
PT3	🟦	🟥	🟧	PT8	PCM2 PCM6 PCM7
PT4	🟦	🟥	🟧	PT9	PCM2 PCM5 PCM6 PCM7
PT5	🟦	🟥	🟧	PT3	PCM4 PCM9
PT6	🟦	🟧	🟧	PT4	PCM4 PCM8 PCM9
PT7	🟧	🟥	🟥	PT5	PCM4 PCM9
PT8	🟧	🟥	🟥	PT1	PCM4 PCM8
PT9	🟧	🟥	🟥	PT6	PCM4 PCM9

TABLE 23: TSR-CCP PRIVACY THREAT RANKING DECISION TABLE FOR THE IOT-ENABLED RAILWAY SYSTEMS

The above TSR-CCP decision table sets out the severity-ranked privacy threats using the same colour-coded decision method as described for the above security severity ranking threats in Table 22 above. The only difference is that consistent with the colour coding schema as set out in the TSR Decision Tables Colour Coding Schema Reference Table 18, a ‘light and dark green’ colour schema is used to represent the privacy threats; the lighter and darker shades highlighting representing, respectively, the threats to-be-ranked and already-ranked as in the final column.

In the following after the TSR decision tables for privacy severity ranking have been presented we proceed to the next stage in the TSR-CCP pipeline which is to integrate the severity-ranked security and privacy threats together with their respective prioritised countermeasures so as to conclude the process with the prioritised combinatorial countermeasures as the highest priority safeguarding measures prescribed by TSR-CCP for resilience investment planning.

7.11.3 Applying TSR-CCP to the Integrated Security-Privacy Threats Severity Ranking and Responsive Combinatorial Countermeasures Prioritisation

In accordance with the aforementioned TSR rules for integrative severity ranking of privacy and security threats, privacy threats are assumed to be ranked as more severe than security threats, by default, unless the respective security threat(s) can cause physical harm and/or loss of life to humans. It is noted that a ‘medium’ ranked privacy threat, for example, is therefore deemed to be of higher priority than a ‘high’ ranked security threat but not a security threat that is assessed as being of ‘very high’ severity ranking. Table 24 presents the categoric priority classification of countermeasures for the IoT enabled Railway systems domain based on the Combinatorial Countermeasures Prioritisation rules as defined and colour-coded in Table 14, as follows.

Table 24, Prioritisation Ranking Categories of Responsive Security & Privacy Countermeasures	
Countermeasures Mitigation Value Ranking	Countermeasure(s) Index
GOLD (Non-Digital) Countermeasure (Operation Workaround)	Not applicable to the particular semantic model and corresponding threat-model data-flow diagram (DFD) of the Railway system
Gold-Digital Countermeasure	SCM1, SCM4, SCM5, SCM9, SCM14, SCM8, SCM15, SCM19, SCM27 PCM1, PCM2, PCM4, PCM9, PCM11
Silver Countermeasure	SCM3, SCM6, SCM7, SCM10, SCM13, SCM22, SCM23, SCM26, SCM11, SCM25, SCM2 PCM3, PCM5, PCM6, PCM7, PCM8, PMC10
Bronze Countermeasure	SCM12, SCM16, SCM17, SCM18, SCM21, SCM20, SCM24

TABLE 24: PRIORITISATION RANKING CATEGORIES OF RESPONSIVE SECURITY & PRIVACY COUNTERMEASURES

The results of categoric prioritisation of countermeasures as concluded in Table 24 above are then set out in final TSR Decision Table 25 which implements the integrated privacy and security severity ranking and combinatorial countermeasures prioritisation

This final stage of the TSR-CCP Decision Pipeline, as set out in Table 25 below, implements the conclusive prioritisation of threats and countermeasures as follows:

Column-1 of the table lists the ‘Severity *Ranked Privacy Threats’,* which is to the ordered rank, in severity, of the privacy threats from highest to lowest.

Column-2 sets out the ‘*Countermeasures for Severity Ranked Privacy Threats*’.

Column-3 and 4 set out the respective prioritisations similarly to Column 1 & 2 for the Severity Ranked Security Threats and their Countermeasures.

Column 5, titled ‘*Integrated Privacy-Security Threat Severity Ranking*’ derives the final integrated severity ranking of privacy and security threats

Column 6 – *Countermeasures for Privacy-Security Severity Ranked Threats*’ present the countermeasures associated with the respective severity-ranked security and privacy threats: this effectively integrates the countermeasure sets from columns 2 and 4.

Finally, Column-7, '*Prioritised Countermeasures'* determines the combinatorial prioritisation of the countermeasures. The colour coding, consistent with the CCP Table 14, signifies the final ranking assigned to each countermeasure.

Consistent with the TSR Decision Tables Colour Coding Schema Reference for Threats Table 18, and the table for Countermeasures Colour-Coded Ranking (Table 14), any threats and/or countermeasures that are highlighted in 'Sky Blue', as can be found within the final TSR Decision table, Table 25 below, can be excluded from the final list of the prescribed prioritised countermeasures. This is due to the aforementioned 80%-90% rule (Point of Diminishing Return on Resilience Investment). These lowest ranked 10% of the threats and their respective attack vectors and/or countermeasures are deemed to be of too low a severity/priority ranking to be considered in the recommendation list of highest priority countermeasures to be included in the implementation plan for the normally targeted level of resilience maintenance but should their priorities change dynamically, these may become sufficiently highly ranked to be included whilst other currently more highly ranked threats and thus their respective countermeasures may recede in severity or just vanish and thus excluded or demoted.

Table 25 is the final TSR-CCP Decision table presenting the Integrated Privacy-Security Ranking and Combinatorial Countermeasures Prioritisation for the IoT enabled Railway systems as a demonstrator. This table compiles the results of the separate security and privacy threat decision tables (Table 23, Table 24) and conforms to the Reference TSR-CCP Decision Tables Colour Coding Schema for Threats Severity Ranking (Table 18) and for Countermeasures Prioritisation (Table 14).

Table 25: Integrated Privacy-Security Ranking and Combinatorial Countermeasures Prioritisation (TSR-CCP) Cumulative Decision Table for the IoT-enabled Railway Systems

Privacy Threats-ID (Severity-Ranked Highest to Lowest)	Prioritised Countermeasures Responsive to the PrivacyThreats	Security Threats ID (Severity-Ranked Highest toLowest)	Prioritised Countermeasures Responsiveto theSecurity Threats	Integrated Privacy-Security Ranking (Highest to Lowest)	Combinatorial CountermeasuresResponsive to Integrated Severity-RankedPrivacy &Security Threats	Prioritised Countermeasures Best to Worst [Gold, Silver, Bronze]
PT2	PCM9 PCM10 PCM11	CPT11	SCM8, SCM1, SCM25	CPT11	SCM8, SCM1, SCM25	SCM8
PT7	PCM3 PCM1	ST16	SCM14, SCM1, SCM15, SCM27	ST16	SCM14, SCM1, SCM15, SCM27	PCM4
PT8	PCM2 PCM6 PCM7	ST20	SCM14, SCM1, SCM15	ST20	SCM14, SCM1, SCM15	PCM2
PT9	PCM2 PCM5 PCM6 PCM7	CPT5	SCM25, SCM1, SCM8, SCM22	CPT5	SCM25, SCM1, SCM8, SCM22	SCM4
PT3	PCM4 PCM9	CPT1	SCM1, SCM5	CPT1	SCM1, SCM5	SCM27
PT4	PCM4 PCM8 PCM9	CPT6	SCM1, SCM3, SCM11	CPT6	SCM1, SCM3, SCM11	SCM5
PT5	PCM4 PCM9	CPT7	SCM1, SCM3, SCM11	CPT7	SCM1, SCM3, SCM11	PCM11
PT1	PCM4 PCM8	ST17	SCM14, SCM1, SCM26, SCM27	ST17	SCM14, SCM1, SCM26, SCM27	PCM9
PT6	PCM4 PCM9	ST15	SCM14, SCM1, SCM26, SCM22	ST15	SCM14, SCM1, SCM26, SCM22	SCM1
		ST18	SCM5, SCM9, SCM2, SCM14	ST18	SCM5, SCM9, SCM2, SCM14	SCM15
		ST29	SCM1, SCM6, SCM4, SCM10, SCM14, SCM27, SCM20	ST29	SCM1, SCM6, SCM4, SCM10, SCM14, SCM27, SCM20	SCM9
		ST42	SCM20, SCM24, SCM23, SCM22, SCM1	ST42	SCM20, SCM24, SCM23, SCM22, SCM1	SCM14
		SF2	SCM8, SCM7, SCM14	PT2	PCM9 PCM10 PCM11	PCM1
		UD1	SCM8, SCM7, SCM14	PT7	PCM3 PCM1	SCM19
		AA12	SCM8, SCM7, SCM14, SCM6	PT8	PCM2 PCM6 PCM7	SCM6
		AA1	SCM15, SCM3, SCM21	PT9	PCM2 PCM5 PCM6 PCM7	PCM8
		AA2	SCM15, SCM10, SCM4, SCM9	PT3	PCM4 PCM9	PCM3

Table 25: Integrated Privacy-Security Ranking and Combinatorial Countermeasures Prioritisation (TSR-CCP) Cumulative Decision Table for the IoT-enabled Railway Systems

Privacy Threats-ID (Severity-Ranked Highest to Lowest)	Prioritised Countermeasures Responsive to the PrivacyThreats	Security Threats ID (Severity-Ranked Highest toLowest)	Prioritised Countermeasures Responsiveto theSecurity Threats	Integrated Privacy-Security Ranking (Highest to Lowest)	Combinatorial CountermeasuresResponsive to Integrated Severity-RankedPrivacy &Security Threats	Prioritised Countermeasures Best to Worst [Gold, Silver, Bronze]
		AA5	SCM4, SCM6, SCM7, SCM14	PT4	PCM4 PCM8 PCM9	PCM7
		AA6	SCM8, SCM6, SCM10, SCM15, SCM16	PT5	PCM4 PCM9	SCM7
		UD4	SCM25, SCM22, SCM19, SCM10	PT1	PCM4 PCM8	PCM5
		SF1	SCM14, SCM15, SCM8	PT6	PCM4 PCM9	PCM6
		SF3	SCM4	SF2	SCM8, SCM7, SCM14	SCM25
		SF4	SCM4, SCM26, SCM6, SCM1	UD1	SCM8, SCM7, SCM14	SCM3
		ST13	SCM5, SCM9, SCM2, SCM15	AA12	SCM8, SCM7, SCM14, SCM6	PCM10
		ST14	SCM5, SCM9, SCM2, SCM15	AA1	SCM15, SCM3, SCM21	SCM10
		ST32	SCM5, SCM9, SCM2, SCM14, SCM3, SCM4,	AA2	SCM15, SCM10, SCM4, SCM9	SCM11
		ST23	SCM14, SCM1	AA5	SCM4, SCM6, SCM7, SCM14	SCM20
		UD3	SCM8, SCM19, SCM25	AA6	SCM8, SCM6, SCM10, SCM15, SCM16	SCM13
		ST49	SCM3, SCM13, SCM5, SCM6, SCM10	UD4	SCM25, SCM22, SCM19, SCM10	SCM12
		ST47	SCM14, SCM1, SCM26	SF1	SCM14, SCM15, SCM8	SCM18
		ST46	SCM5, SCM9, SCM2, SCM14	SF3	SCM4	SCM16
		AA4	SCM15, SCM10, SCM4, SCM9	SF4	SCM4, SCM26, SCM6, SCM1	SCM17
		FM1	SCM27, SCM8	ST13	SCM5, SCM9, SCM2, SCM15	SCM21
		ST5	SCM14, SCM1, SCM15	ST14	SCM5, SCM9, SCM2, SCM15	SCM2
		ST10	SCM5, SCM9, SCM2, SCM14	ST32	SCM5, SCM9, SCM2, SCM14, SCM3, SCM4,	SCM24
		ST11	SCM5, SCM9, SCM2, SCM14	ST23	SCM14, SCM1	
		ST22	SCM5, SCM9, SCM2, SCM14	UD3	SCM8, SCM19, SCM25	
		ST27	SCM14, SCM1, SCM26	ST49	SCM3, SCM13, SCM5, SCM6, SCM10	
		ST45	SCM14, SCM1, SCM26	ST47	SCM14, SCM1, SCM26	
		ST9	SCM1, SCM3, SCM5	ST46	SCM5, SCM9, SCM2, SCM14	
		ST12	SCM5, SCM9, SCM2, SCM14	AA4	SCM15, SCM10, SCM4, SCM9	
		FM2	SCM27	FM1	SCM27, SCM8	
		AA3	SCM15, SCM10, SCM4	ST5	SCM14, SCM1, SCM15	
		AA11	SCM22, SCM12	ST10	SCM5, SCM9, SCM2, SCM14	
		AA8	SCM5, SCM9, SCM4	ST11	SCM5, SCM9, SCM2, SCM14	
		UD2	SCM4	ST22	SCM5, SCM9, SCM2, SCM14	
		ST28	SCM5, SCM9, SCM14, SCM15	ST27	SCM14, SCM1, SCM26	
		ST24	SCM14, SCM1, SCM15, SCM27	ST45	SCM14, SCM1, SCM26	

Table 25: Integrated Privacy-Security Ranking and Combinatorial Countermeasures Prioritisation (TSR-CCP) Cumulative Decision Table for the IoT-enabled Railway Systems

Privacy Threats-ID (Severity-Ranked Highest to Lowest)	Prioritised Countermeasures Responsive to the PrivacyThreats	Security Threats ID (Severity-Ranked Highest toLowest)	Prioritised Countermeasures Responsiveto theSecurity Threats	Integrated Privacy-Security Ranking (Highest to Lowest)	Combinatorial Counter-measuresResponsive to Integrated Severity-RankedPrivacy &Security Threats	Prioritised Countermeasures Best to Worst [Gold, Silver, Bronze]
		ST30	SCM14, SCM1, SCM15	ST9	SCM1, SCM3, SCM5	
		ST33	SCM20, SCM24, SCM23, SCM22	ST12	SCM5, SCM9, SCM2, SCM14	
		ST31	SCM5, SCM9, SCM2, SCM14	FM2	SCM27	
		ST34	SCM14, SCM1, SCM26	AA3	SCM15, SCM10, SCM4	
		ST7	SCM19, SCM6, SCM1	AA11	SCM22, SCM12	
		ST44	SCM19, SCM20, SCM18, SCM26, SCM14	AA8	SCM5, SCM9, SCM4	
		ST43	SCM20, SCM18, SCM19, SCM14, SCM26	UD2	SCM4	
		ST48	SCM20, SCM24, SCM23, SCM22, SCM1	ST28	SCM5, SCM9, SCM14, SCM15	
		CPT8	SCM14, SCM15, SCM25, SCM27	ST24	SCM14, SCM1, SCM15, SCM27	
		CPT10	SCM14, SCM15, SCM25, SCM27	ST30	SCM14, SCM1, SCM15	
		CPT9	SCM14, SCM15, SCM25, SCM27	ST33	SCM20, SCM24, SCM23, SCM22	
		L1	SCM23	ST31	SCM5, SCM9, SCM2, SCM14	
		ST21	SCM14, SCM1	ST34	SCM14, SCM1, SCM26	
		CPT3	SCM1, SCM3, SCM11, SCM13	ST7	SCM19, SCM6, SCM1	
		AA9	SCM19, SCM12	ST44	SCM19, SCM20, SCM18, SCM26, SCM14	
		ST41	SCM5, SCM9, SCM2, SCM14	ST43	SCM20, SCM18, SCM19, SCM14, SCM26	
		ST1	SCM5, SCM9, SCM2, SCM14	ST48	SCM20, SCM24, SCM23, SCM22, SCM1	
		ST4	SCM14, SCM1	CPT8	SCM14, SCM15, SCM25, SCM27	
		ST3	SCM5, SCM9, SCM2, SCM14	CPT10	SCM14, SCM15, SCM25, SCM27	
		CPT2	SCM1, SCM5	CPT9	SCM14, SCM15, SCM25, SCM27	
		AA7	SCM19, SCM9, SCM3	L1	SCM23	
		FM3	SCM27	ST21	SCM14, SCM1	
		CPT4	SCM19, SCM9, SCM3	CPT3	SCM1, SCM3, SCM11, SCM13	
		ST8	SCM7, SCM14, SCM26	AA9	SCM19, SCM12	
		ST25	SCM5, SCM9, SCM2, SCM14	ST41	SCM5, SCM9, SCM2, SCM14	
		ST19	SCM14, SCM1	ST1	SCM5, SCM9, SCM2, SCM14	
		ST26	SCM5, SCM9, SCM2, SCM14	ST4	SCM14, SCM1	
		ST37	SCM5, SCM9, SCM2, SCM14	ST3	SCM5, SCM9, SCM2, SCM14	
		ST36	SCM5, SCM9, SCM2, SCM14	CPT2	SCM1, SCM5	
		ST35	SCM14, SCM1, SCM15	AA7	SCM19, SCM9, SCM3	
		ST39	SCM20, SCM24, SCM23, SCM22, SCM1	FM3	SCM27	

Table 25: Integrated Privacy-Security Ranking and Combinatorial Countermeasures Prioritisation (TSR-CCP) Cumulative Decision Table for the IoT-enabled Railway Systems

Privacy Threats-ID (Severity-Ranked Highest to Lowest)	Prioritised Countermeasures Responsive to the PrivacyThreats	Security Threats ID (Severity-Ranked Highest toLowest)	Prioritised Countermeasures Responsiveto theSecurity Threats	Integrated Privacy-Security Ranking (Highest to Lowest)	Combinatorial Counter-measuresResponsive to Integrated Severity-RankedPrivacy &Security Threats	Prioritised Countermeasures Best to Worst [Gold, Silver, Bronze]
		AA10	SCM17, SCM18, SCM4	CPT4	SCM19, SCM9, SCM3	
		ST40	SCM14, SCM1, SCM26	ST26	SCM5, SCM9, SCM2, SCM14	
		ST2	SCM5, SCM9, SCM2, SCM14	ST25	SCM5, SCM9, SCM2, SCM14	
		ST38	SCM5, SCM9, SCM2, SCM14	ST2	SCM5, SCM9, SCM2, SCM14	
		ST6	SCM19, SCM15	ST8	SCM7, SCM14, SCM26	
				ST36	SCM5, SCM9, SCM2, SCM14	
				ST37	SCM5, SCM9, SCM2, SCM14	
				ST35	SCM14, SCM1, SCM15	
				ST39	SCM20, SCM24, SCM23, SCM22, SCM1	
				AA10	SCM17, SCM18, SCM4	
				ST40	SCM14, SCM1, SCM26	
				ST19	SCM14, SCM1	
				ST38	SCM5, SCM9, SCM2, SCM14	
				ST6	SCM19, SCM15	

TABLE 25: INTEGRATED PRIVACY-SECURITY RANKING AND COMBINATORIAL COUNTERMEASURES PRIORITISATION (TSR-CCP) CUMULATIVE DECISION TABLE FOR THE IOT-ENABLED RAILWAY SYSTEMS

As the above final TSR-CCP Decision Table shows, for safeguarding against the 84 cyber-security and 9 privacy attack types, a total of38 combinatorial security-privacy countermeasures were prescribed by the TSR-CCP framework as the highest priority optimised countermeasures for maintaining the resilience of the IoT-enabled Railway Systems as supported by SAFETY4RAILS.

8. Summary and Conclusion

8.1 Prediction of Normal Deterioration due to Ageing and Degradation of Assets

CAMS forecasts the condition of assets due to the normal ageing process. CAMS can provide the end-users with data on the level of deterioration process of each asset. This information is crucial for developing a comprehensive maintenance plan and budget forecast. CAMS outputs are curves representing the variation of conditions overtime which are generated using transition matrices that are trained based on inspection data collected over time. A database of approximately 720 curves is available within the software. The end-user is capable of choosing appropriate curves for their components. Alternatively, the user can upload user-defined curves. The user-defined matrix can be imported from an excel file or CSV format or it can be configured in GUI.

Data from at least two consecutive inspections are required to train the data-based model. Further, repair records of the inspected assets are supplied to calibrate standard curves. Data can be provided in CSV format or other database formats.

Based on the current condition of a given asset, the CAMS model can predict the condition of the asset components in the future. It is based on a Markov chain model which is a probabilistic model for describing stochastic processes. The outcome of the model is a transition matrix that gives the probability of an asset being in a certain condition after one defined interval of time.

8.2 Contributing to Response and Recovery Phases

Through the CAMS state-dependent fragility analysis, it is possible to determine the impact of a disruptive event on an asset based on its condition before the incident. Users can evaluate various scenarios of attacks and calculate the damage to their assets. By considering the condition before the event, CAMS will generate realistic predictions for the damage after the event. This step is crucial for computing the resilience when using CAMS. This process results in a family of curves for each intensity of a disruption event and the initial condition of the damage. These curves will determine the extent of the final damage condition after the disruption event.

Deterioration depends on the intensity of disruption events. CAMS inputs for this module are the initial damage condition and the intensity of the event. Inputs include intensity measures for each type of incident. Damage limit states must also be determined for each asset by CAMS.

The final damage condition is determined by this module after a disruptive event has occurred. Fragility functions are used to describe the probability of reaching or exceeding a level of damage at a given intensity measure of the disruptive event. The ability of an asset to respond to a certain event is also dependent on its current infrastructure. This means that the fragility analysis is also dependent on the deterioration module.

First, defining the extreme event is necessary to perform this analysis. The event can be defined using an intensity measure related to the likelihood of the event occurring. It also includes the definition of thresholds including limiting damage states for each asset. As a final step, it is necessary to define whether the asset has or has not reached the limit state for each limit state as set for the different intensities of the event.

8.3 Resilience Module

End-users are equipped to find the resilience parameter (integral of performance over time) by using the given functions. To evaluate different response strategies, it is necessary to calculate this parameter. Resource-time curves are used to define response strategies, which are either uploaded into an excel file or in the GUI by the user.

By using the GUI, the user can also set the relationship between damage and performance indicators at the asset level. Moreover, the user gives each of the assets its contribution to the performance of the higher level in the hierarchy. As a result, the performance of the complete system is derived by aggregating lower-level performances.

According to the intensity measure, the assets that are affected, and the time when the event occurred, a threat scenario is defined by the user. Initially, the damage state of the system is determined. Next, the impact on assets is calculated using the fragility module, and then the loss of performance on the complete CAMS is calculated using the hierarchy. Both normal and sudden responses are evaluated. The full performance-time curve is generated by CAMS, and the resilience can thus be assessed.

The degradation and fragility analysis module are directly related to this module. To calculate the recovery time, it would also be necessary to know the response plan. A clear definition of the performance variable and its relationship to damage states is also required.

The resilience factors are calculated using cumulative performance (or depending on the convention, performance loss) over time. The first step is to clearly define the relationship that exists between the damage condition or variable and the performance variable.

The workflow for responding to given event occurring in a given time would be as follows:

1. Estimation of the initial condition before the event using the deterioration module/site audit.
2. Calculation of the damage after the event using the fragility module.
3. Transforming the damage variable to performance.
4. Determination of the recovery time (based on assumptions or historical data), depending on the response plan.

5. Calculation the cumulative function (integral).

Budgeting policies will also impact resilience: different recovery plans, meaning different budget allocations, will produce different recovery times, resulting in different resilience factors.

8.4 Backlog Estimation

End-users can obtain realistic estimates of maintenance and repair backlogs. CAMS calculates the deterioration based on the first result as described above. CAMS calculates the budget allocations as the second result based on the above statement. End-users need to specify the available budget for each year in order to estimate the backlog. Moreover, different scenarios can also be analysed. These can be done via the GUI by entering the relevant data. A simple subtraction of the available budget from the required budget yields the backlog. This is based on the deterioration module, the maintenance and budget calculations depending on the deterioration levels. It also requires the results of the risk cost evaluation. A budget is also needed in order to address the necessary maintenance to maintain a certain level of service.

When future maintenance expenditure is calculated using the damage forecasts, the difference between the available budget and the required resources is used to identify backlogs. Based on the expected budget, different scenarios can be considered. Inflation can also be factored in based on the inflation rate. Backlog estimation based on the forecasting of damage and maintenance costs provides valuable information for the asset manager during the resilience investment decision-making process

8.5 Optimisation of Budget

By using CAMS, end-users can optimise their maintenance, repair, and response strategies on a budget while meeting resilience requirements. In order to maximise the impact of such investments, the asset manager will receive information on when and where to make the investments.

An optimisation tool with multiple variables and constraints is available. More information about this tool can be found in deliverable 7.5, the optimisation algorithm will work as a black box with the rest of the modules, taking inputs (initial budget, investment policies, threat scenarios, response strategies, etc) and generating resilience parameters. Moreover, the required level of resilience, the initial budget to be optimised, and the event intensity are required.

The optimal budgeting strategy means making a minimum level of resilience investment on assets to mitigate an event of a given disruption level. This informs the asset manager of the best financial strategy to enhance resilience against various threats, given the trade-offs with respect to other actions within asset management such as maintenance, repair, and rehabilitation.

8.6 Extension of the Framework to IT Assets

IT assets are also included in CAMS, just like physical asset; by using the transition matrices. For the most common assets, transition matrices are developed offline, and user-defined matrices can be uploaded via Excel files or by direct input in the GUI.

End-users are able to manage both physical and IT assets in one place. CAMS enables users to define IT asset management practices. This requires establishing a condition rating scale similar to that used for physical assets and obtaining data on maintenance of IT assets, such as the costs of maintenance, rehabilitation, and replacement.

The features of the model that were previously developed for physical assets have been applied to digital assets as well. This resulted in a centralised asset management system for both physical and digital assets. By including IT assets, the impact of cyber and combined attacks is also examined.

Digital assets are introduced similarly to physical assets. It is possible to predict the future conditions of the digital assets based on the deterioration module framework. The digital assets functionalities and vulnerabilities can be predicted. For instance, the damage conditions can refer to the updated status of each asset.

The state-dependent fragility analyses determine the impact that a cyber-attack may have on an IT asset based on its previous vulnerability level. Data losses are greater if, for instance, a database is out-of-date during an attack. The budgetary tools as described earlier are also used for IT assets. By integrating physical and digital elements, budgetary and financial strategies become more effective.

8.7 Analysis of Compromises between Maintenance, Repair, Rehabilitation and Resilience Enhancement Efforts

When a disruptive event occurs, an asset performance and resilience are not only impacted by the event itself, but also by its prior condition. Resilience is also determined by the measures taken in response to the event. From a resilience perspective, this leads to the problem of allocating resources in the most efficient way. Alternative budgetary scenarios can be analysed using the tool based on a variety of strategies for maintenance, repair, rehabilitation, and enhancement. CAMS optimises resilience enhancement strategies within the framework of normal asset management using the optimisation and budgeting modules.

When a disruptive event occurs, an asset performance and resilience are not only impacted by the event itself, but also by its prior condition. Resilience is also determined by the measures taken in response to the event. From a resilience perspective, this leads to the problem of allocating resources in the most efficient way. Alternative budgetary scenarios can be analysed using the tool based on a variety of strategies for maintenance, repair, rehabilitation, and enhancement. CAMS optimises resilience enhancement strategies within the framework of normal asset management using the optimisation and budgeting modules.

8.8 Assessment of Recovery

Budgetary and time considerations can be considered when analysing different recovery strategies. The asset manager can analyse multiple scenarios and forecast the budget required to meet the resilience goal. The CAMS result can be applied to different recovery strategies. Each strategy is defined by how much time and resources it will take. The result will be the resilience for each scenario. The recovery strategies are input using excel files or manually. Each response strategy requires an overall recovery plan. This requires information from both the fragility analysis and the budget module.

A key component of post-event recovery is the mobilisation of resources, whether they are monetary, human, or technological. The rate of recovery of the infrastructure to its original performance depends on the availability of resources. Thus, the investment models enable the end-user to find the relationship between time and resources and their implications for resilience. This enables the asset manager to compare different recovery strategies from a financial/budgetary point of view. The definition of normal and crash times and cost is essential as this enables the evaluation of all possible strategies. Normal time corresponds to the lowest possible financial resources for normal operation to resume. In summary, crash time refers to the minimum time it takes to re-establish performance with a large number of resources after a crash.

The ability to pre-shape a recovery plan and timelines enables the work to be initiated as soon as the incident happens. This ensures there is the least amount of delay for the asset being in operation and can have significant savings. The monitoring of condition and strengthening of weak areas can ensure that the damage caused by an incident is minimal. A cost-benefit digit (which is started from 1 to 5 in different divided limits up to <5%, <10%, <15% and <20%), for achieving the Recovery Reduced Cost can estimated in comparison to the existing budget plan of end-user (by less than 5% and no more than 20%). Therefore, in deliverable 7.5, the cost-benefit limit percentage is derived quantitatively based on accurate and reliable items below;

Cost of assets maintenance; cost of assets repair[8]; cost of assets renewal; cost of assets replacement[9]; as well as time of assets maintenance; time of assets repair[10]; time of assets renewal; time of assets

[8] Column 11th of Table 12: CAMS Input Data For CDM SE.

[9] Column 14th of Table 12: CAMS Input Data For CDM SE.

[10] Column 8th of Table 12: CAMS Input Data For CDM SE.

replacement and components dependency[11]; components priority[12] (in recovery phase after an incident) and Risk Determination[13] under the CMAS basic reference as "*Deterioration prediction of community buildings in Australia, HESSAM MOHSENI, 2012*"*[3]*. The range of cost-benefit percentage is achievable when the above-requested data exist, valid, accurate, reliable and accessible under end-user regulations and data protection protocol. In Deliverable 7.5, as the final report of work package 7, we discussed quantitatively how we meet the above limitation (range of cost-benefit percentage) through an optimization of the budget for a given level of resilience under the specific risk determination.

8.9 Dynamically Responsive Resilience Optimisation

Over time, both condition degradation, and cumulative lack of upgraded status, as well as new threats emerging and responsive innovation of new countermeasures mean there is a compelling need for iterative assessment of the latest vulnerabilities to check for new conditions of assets, their new vulnerabilities and any exacerbation of the earlier vulnerabilities that may have become severe enough to have to be given a higher priority for safeguarding steps being implemented to mitigate them. All these dynamic factors call for a continuous review of the evolving vulnerabilities due to the emerging threats landscape and responsive prioritisation of fixes to counter them so as to maintain the target resilience envelop.

Accordingly, the novel TSR-CCP framework as developed in this deliverable, supports the deployment of CAMS for enhanced dynamic prioritisation of safeguards to enable an agile resilience investments optimisation framework.

In this deliverable, cyber-physical threats have been considered, as an example, to show the deployment of TSR-CCP for the IoT-enabled railway systems. Accordingly, this work has established a comprehensive analysis base which enables resilience engineering to remain responsive to the operational use-context-aware, threat-driven and risk-based vulnerabilities in the face of the combinatorial attacks as they evolve.

The analysis base for TSR-CCP is underpinned by the UI-REF methodology [11],[12] for context-aware dynamic requirements prioritisation as applied to threats severity ranking and countermeasures prioritisation resolution. An ontologically committed and methodologically guided analysis has led to the development of this novel framework to arrive at an optimal managed mix of countermeasure sets to support cost-effective and efficient resilience assurance against *combinatorial threats* (with cyber-physical security and privacy threats as an exemplar). This has prescribed 38 highest priority countermeasures for safeguarding IoT-enabled railway systems to counter a total of 363 probable privacy and security threats as resulted from the initial threats modelling phase.

Thus, TSR-CCP supports the operational capability for dynamic vulnerabilities assessment as a pre-requisite for maintaining resilience with responsive safeguards (preventative) and mitigation (remedial) measures to be actioned. This enables the latest state of the most critical vulnerabilities and severest threats, resilience index and resilience engineering strategy and thus the planned resilience investment to be dynamically revised and adapted responsive to emerging threats.

Accordingly, this framework supports Agile Resilience Assurance by Design to protect and mitigate against any risks in any domain provided one could estimate the likelihood of the risks leading to threats and materialising as attacks/incidents and the scale of their impacts.

****

[11] Column 10th of Table 12: CAMS Input Data For CDM SE.

[12] Column 9th of Table 12: CAMS Input Data For CDM SE.

[13] Page 160, Deterioration prediction of community buildings in Australia, HESSAM MOHSENI, 2012.

Bibliography

1. SAFETY4RAILS *(H2020 GA no. 883532).*
2. SAFETY4RAILS, *Deliverable D2.1 Grid analysis of end-user needs and workshops minutes*, May 2021, *{32}*.
3. *Hessam Mohseni*, *Deterioration prediction of community buildings in Australia*, 2012.
4. *Lu, X. Yu, M. Jia, G. Wang, Simplified fragility analysis methods for minimum life-cycle cost seismic design of generic structures (2010).*
5. *Capacci, F. Biondini, Probabilistic life-cycle seismic resilience assessment of aging bridge networks considering infrastructure upgrading, Structure and Infrastructure Engineering 16 (2020) 659{675.*
6. *Mohseni, S. Setunge, G. Zhang, R. Wakefield, Markov process for deterioration modelling and asset management of community buildings, Journal of Construction Engineering and Management 143 (2017) 04017003.*
7. *M. Qeshta, M. J. Hashemi, R. Gravina, S. Setunge, Review of resilience assessment of coastal bridges to extreme wave-induced loads, Engineering Structures 185 (2019) 332 {352}.*
8. *Tran, H. D. 2007. Investigation of Deterioration Models for Stormwater Pipe Systems. PhD Thesis, Victoria University.*
9. *Micevski, T., Kuczera, G. & Coombes, P. 2002. Markov Model for Storm Water Pipe Deterioration. Journal of Infrastructure Systems, 8, 49-56.*
10. *Ross, S. M. 2000. Introduction to probability models, San Diego, Calif.; Academic*
11. *A. Badii, “User-intimate requirements hierarchy resolution framework (UI-REF),” AmI-08: Second European Conference on Ambient Intelligence, 2008.*
12. *A. Badii, D. Fuschi, A. Khan and A. Adetoye, “Accessibility-by-Design: A Framework for Delivery-Context-Aware Personalised Media Content Re-purposing,” HCI and Usability for e-Inclusion, 2009.*
13. *Fisher. E, 2016. Cybersecurity Issues and Challenges: In Brief. [online] Available at: <https://a51.nl/sites/default/files/pdf/R43831.pdf> [Accessed 13 June 2021].*
14. *Poyraz, O., Canan, M., Mc Shane, M., Pinto, C. and Cotter, T., 2020. Cyber assets at risk: monetary impact of U.S. personally identifiable information mega data breaches. The Geneva Papers on Risk and Insurance - Issues and Practice, 45(4), pp.616-638. [Accessed: 24 June 2021].*
15. *Kavallieratos, G., Katsikas, S. and Gkioulos, V., 2019. Cyber-Attacks Against the Autonomous Ship. Computer Security, pp.20-36.*
16. *Microsoft.com. Microsoft Threat Modeling Tool 2016 from Official Microsoft Download Center. [online] Available at: <https://www.microsoft.com/en-us/download/details.aspx?id=49168> [Accessed 14 June 2021].*
17. *Almulhem, A., 2011. Threat Modeling for Electronic Health Record Systems. Journal of Medical Systems, 36(5), pp.2921-2926.*
18. *Nath Nayak, G. and Ghosh Samaddar, S., 2010. Different flavours of Man-In-The-Middle attack, consequences and feasible solutions. 2010 3rd International Conference on Computer Science and Information Technology. [Accessed: 21 June 2021].*
19. *Abouelmehdi, K., Beni-Hessane, A. and Khaloufi, H., 2018. Big healthcare data: preserving security and privacy. Journal of Big Data, 5(1).*
20. *Xie, H., Wang, F., Hao, Y., Chen, J., An, J., Wang, Y. and Liu, H., 2017. The more total cognitive load is reduced by cues, the better retention and transfer of multimedia learning: A meta-analysis and two meta-regression analyses. PLOS ONE, 12(8), p.e0183884. [Accessed: 15 June 2021].*
21. *Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. and Koucheryavy, Y., 2018. Multi-Factor Authentication: A Survey. Cryptography, 2(1), p.1. [Accessed: 13 June 2021].*
22. *Coole, M., Corkill, J. and Woodward, A., 2012. Defence in Depth, Protection in Depth and Security in Depth: A Comparative Analysis Towards a Common Usage Language. [online] Available at: <https://ro.ecu.edu.au/asi/24/> [Accessed 6 July 2021].*
23. *Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments., 2010. https://citadel-information.com/wp-content/uploads/2010/12/nsa-defense-in-depth.pdf*
24. *Defence in Depth Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-DepthStrategies,2016.https://www.cisa.gov/uscert/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_Defense_in_Depth_Strategies_S508C.pdf*
25. *S. Woodside, Defence in Depth: The medieval castle approach to internet security, 2016.*

26. R. Sarma and F. Barbhuiya, "Internet of Things: Attacks and Defences", 2019 7th International Conference on Smart Computing & Communications (ICSCC), 2019.
27. L. Spitzner, "Honeypots: catching the insider threat", 19th Annual Computer Security Applications Conference, 2003. Proceedings.
28. I.Ghafir, V. Prenosil, J. Svoboda and M. Hammoudeh, "A Survey on Network Security Monitoring Systems", 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), 2016.
29. B. Kaliski, "A survey of encryption standards", IEEE Micro, vol. 13, no. 6, pp. 74-81, 1993.
30. X. Zhang, C. Li and W. Zheng, "Intrusion prevention system design", The Fourth International Conference onComputer and Information Technology, 2004. CIT '04., 2004.
31. R. Sandhu, "Role-based Access Control", Advances in Computers, pp. 237-286, 1998.
32. P. Inglesant and M. Sasse, "The true cost of unusable password policies", Proceedings of the 28th international conference on Human factors in computing systems - CHI '10, 2010. [Accessed: 24 June 2021].
33. R. Sabillon, J. Serra-Ruiz, V. Cavaller and Jeimy J. Cano M., "An Effective Cybersecurity Training Model to Support an Organisational Awareness Program", Research Anthology on Artificial Intelligence Applications in Security, pp. 174-188, 2021.
34. A. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection", IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153-1176, 2016.
35. P. Shinde and S. Ardhapurkar, "Cyber security analysis using vulnerability assessment and penetration testing", 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), 2016. [Accessed: 25 June 2021].
36. L. Li, E. Berki, M. Helenius and S. Ovaska, "Towards a contingency approach with whitelist- and blacklist-based anti-phishing applications: what do usability tests indicate?", Behaviour & Information Technology, vol. 33, no. 11, pp. 1136-1147, 2014. [Accessed: 23 June 2021].
37. S. Kim, S. Yoon, J. Narantuya and H. Lim, "Secure Collecting, Optimizing, and Deploying of Firewall Rules in Software-Defined Networks", IEEE Access, vol. 8, pp. 15166-15177, 2020. [Accessed: 15 June 2021].
38. M. Guri, B. Zadov and Y. Elovici, "ODINI: Escaping Sensitive Data from Faraday-Caged, Air-Gapped Computers via Magnetic Fields", IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1190-1203, 2020. [Accessed: 12 June 2021].
39. S. Ibrokhimov, K. Hui, A. Abdulhakim Al-Absi, h. lee and M. Sain, "Multi-Factor Authentication in Cyber Physical System: A State of Art Survey", 2019 21st International Conference on Advanced Communication Technology (ICACT), 2019.
40. D. Kwon, H. Kim, J. Kim, S. Suh, I. Kim and K. Kim, "A survey of deep learning-based network anomaly detection", Cluster Computing, vol. 22, no. 1, pp. 949-961, 2017. [Accessed: 17 June 2021].
41. G. Post and A. Kagan, "The use and effectiveness of anti-virus software", Computers & Security, vol. 17, no. 7, pp. 589-599, 1998.
42. R. Grabowski, M. Hofmann and K. Li, "Type-Based Enforcement of Secure Programming Guidelines — Code Injection Prevention at SAP", Lecture Notes in Computer Science, pp. 182-197, 2012. [Accessed: 28 June 2021].
43. G. Hatzivasilis, "Password-Hashing Status", Cryptography, vol. 1, no. 2, p. 10, 2017. [Accessed: 16 June 2021].
44. C. Kotas, T. Naughton and N. Imam, "A comparison of Amazon Web Services and Microsoft Azure cloud platforms for high performance computing", 2018 IEEE International Conference on Consumer Electronics (ICCE), 2018.
45. B. Putz, F. Menges and G. Pernul, "A secure and auditable logging infrastructure based on a permissioned blockchain", Computers & Security, vol. 87, p. 101602, 2019.
46. M. Wright, "Virtual Private Network Security", Network Security, vol. 2000, no. 7, pp. 11-14, 2000.
47. K. Vaniea and Y. Rashidi, "Tales of Software Updates", Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, 2016. [Accessed: 25 June 2021].
48. M. Vasilescu, L. Gheorghe and N. Tapus, "Practical malware analysis based on sandboxing", 2014 RoEduNet Conference 13th Edition: Networking in Education and Research Joint Event RENAM 8th Conference, 2014. [Accessed: 17 June 2021].
49. J. Tioh, M. Mina and D. Jacobson, "Cyber security training a survey of serious games in cyber security", 2017 IEEE Frontiers in Education Conference (FIE), 2017.
50. S. Dutta, A. Kar, N. Mahanti and B. Chatterji, "Network Security Using Biometric and Cryptography", Advanced Concepts for Intelligent Vision Systems, pp. 38-44, 2008.

51. *S. Boukhonine, V. Krotov and B. Rupert, "Future Security Approaches and Biometrics", Communications of the Association for Information Systems, vol. 16, 2005. [Accessed: 14 June 2021].*

52. *C. Addis and M. Kutar, "The General Data Protection Regulation (GDPR), emerging technologies and UK organisations: awareness, implementation and readiness", in the 23rd UK Academy for Information Systems (UKAIS) International Conference, 2018 [Online]. Available: http://usir.salford.ac.uk/id/eprint/60051/. [Accessed: 16 June 2021].*

53. *V. Pham and T. Dang, "CVExplorer: Multidimensional Visualization for Common Vulnerabilities and Exposures", 2018 IEEE International Conference on Big Data (Big Data), 2018. [Accessed: 12 June 2021].*

54. *Durumeric, Z., Kasten, J., Bailey, M. and Halderman, J., 2013. Analysis of the HTTPS certificate ecosystem. Proceedings of the 2013 conference on Internet measurement conference.*

55. *P. Gouvas, A. Zafeiropoulos, K. Perakis and T. Bouras, "An Innovative Approach for the Protection of Healthcare Information Through the End-to-End Pseudo-Anonymization of end-users", Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 210-216, 2015.*

56. RMIT university – (CAMS Platform) https://test.camsassethub.com.au/products/#cam.

57. SAFETY4RAILS, *Deliverable D3.1 Identification and characterization of cyber(-physical) systems and threats in railway environment*, February 2022. *{25, 28}.*

58. Nader Naderpajouh, RMIT university - SAFETY4RAILS, 15th November 2020, 5. *[Online]. Available: https://dms-prext.fraunhofer.de/livelink/livelink.exe?func=ll&objaction=overview&objid=24100464. [Accessed: 11 June 2020].*

59. SAFETY4RAILS, *Deliverable D8.3 Final version of development of a blueprint exercise handbook*, June 2022. *{28}.*

60. SAFETY4RAILS, *Deliverable D7.3 Budget simulation module of S4RIS*, July 2022. *{13}*

61. SAFETY4RAILS, *Deliverable D2.5 Specific requirements for multimodal transport systems*, June 2021. *{67}*

ANNEXES

ANNEX I. Glossary And Acronyms

TABLE 26: GLOSSARY AND ACRONYMS

Term	Definition/description
ATP	Automatic Train Protection
ATC	Activity Train control
CdM	Comune di Milano (City of Milan)
CO	Confidential
D	Deliverable
DMS	Document Management System
DoA	Description of Action
GUI	Graphical user interface
IoT	Internet of things
EGO	Ankara Metro
ERTMS	European Railway Traffic Management System
ETCS	European Train Control (and Management) System
ETML	European Traffic Management Layer
EVC	European Vital Computer
GSM-R	Global System for Mobiles – Railway
IDS	Intrusion Detection System
IoC	Indicator of Compromise
IT	Information Technology
KMC	Key Management Centre
MA	Movement Authority
MdM	Metro de Madrid
OSINT	Open-Source Intelligence
OT	Operational Technology
RFI	Rete Ferroviaria Italiana
S4RIS	SAFETY4RAILS Information System

SCADA	Supervisory Control and Data Acquisition
SOC	Security Operations Centre
TCC	Traffic Control System
TL	Task leader
ToC	Table of Contents
TRL	Technology Readiness Level
WG	Working Group
WP	Work package
WS	Work Workshop

ANNEX II. Assets List

Sample of railway asset lists, which were categorized and prioritized for CAMS based on D3.1's asset classification guidelines[57] (Such an example used in Table 11: CAMS Input Data For Rome SE and Table 12: CAMS Input Data For CDM SE).

ANNEX II. ASSETS ID	Asset category	Asset name	Type	Sub-type	Location	Description	Functionality
A-TR-01	Track	Rail	Tangible, fixed	Infrastructure	Line	Rails enable trains to move by providing a dependable surface for their wheels to roll up upon.	It allows proper rail traffic.
A-TR-02	Track	Overhead line	Tangible, fixed	Infrastructure	Line	An overhead line is an electrical cable that is used to transmit electrical energy to electric locomotives.	It allows proper rail traffic.
A-TR-03	Track	Switch	Tangible, fixed	Infrastructure	Line	A switch is a mechanical installation enabling railway trains to be guided from one track to another.	It allows proper rail traffic.
A-TR-04	Track	Bridge	Tangible, fixed	Infrastructure	Line	A bridge is a structure to span a physical obstacle without blocking the way underneath.	It allows proper rail traffic.
A-TR-05	Track	Tunnel	Tangible, fixed	Infrastructure	Line	A tunnel is an underground passageway, dug through the surrounding soil/earth/rock and enclosed except for entrance and exit, commonly at each end.	It allows proper rail traffic.
A-TR-06	Track	Level crossing	Tangible, fixed	Infrastructure	Line	A level crossing is an intersection where a railway line crosses a road or path.	It allows proper rail traffic.
A-TR-07	Track	Catenary mast	Tangible, fixed	Infrastructure	Line	Catenary masts are used to support the overhead lines of trains.	It allows proper rail traffic.
A-ST-01	Station	Ticket machine	Tangible, mobile	Equipment	Main hall, ticket office	A ticket machine is a vending machine that produces paper or electronic tickets.	It provides the main source of revenue for the railway company.
A-ST-02	Station	Ticket office	Tangible, fixed	Infrastructure	Main hall, ticket office	An office where passengers can buy Train tickets.	It provides the main source of revenue for the railway company.
A-ST-03	Station	Elevator	Tangible, fixed	Equipment	Station	An elevator s a type of cable-assisted, hydraulic cylinder-assisted, or roller-track assisted machine that vertically transports people or freight between floors of a building.	It provides services for the well-being of the users.
A-ST-04	Station	Escalator	Tangible, fixed	Equipment	Station	An escalator is a moving staircase which carries people between floors of a building or structure.	It provides services for the well-being of the users.
A-ST-05	Station	Turnstiles	Tangible, fixed	Equipment	Main hall	A turnstile is a form of gate which allows one person to pass at a time.	It provides services for the well-being of the users.
A-ST-06	Station	Validator	Tangible, mobile	Equipment	Main hall, platform, corridors	It is a system that validates the tickets.	It provides the main source of revenue for the railway company.
A-ST-07	Station	Electronic timetable	Tangible, fixed	IT system	Main hall, platform, corridors	An electronic timetable is an electronic time-management tool which consists of a list of times at which possible tasks, events, or actions are intended to take place.	It provides services for the well-being of the users.
A-ST-08	Station	Sound announcements system	Tangible, fixed	IT system	Station	A sound announcement system is s an electronic system comprising microphones, amplifiers, loudspeakers, and related equipment.	It contributes to a sufficient level of safety.
A-ST-09	Station	Platform	Tangible, fixed	Infrastructure	Station	A platform is an area alongside a railway track providing convenient access to trains.	It contributes to a sufficient level of safety.
A-ST-10	Station	Vendor/retailer	Tangible, fixed	Equipment	Station, main hall	A vendor/retailer is an enterprise that contributes goods or services.	It provides additional services to the user.
A-ST-11	Station	HVAC system	Tangible, fixed	Equipment	Station, Train	HVAC system is the technology of indoor and vehicular environmental comfort. Its goal is to provide thermal comfort and acceptable indoor air quality.	It provides services for the well-being of the users.
A-ST-12	Station	Lighting system	Tangible, fixed	IT system	Station, Train	A lighting system deliberately uses light to achieve practical or aesthetic effects.	It provides services for the well-being of the users.
A-IS-01	Information system	E-ticketing system	Intangible, fixed	OT system	N.a.	E-ticketing system is a method of ticket entry, processing, and marketing for companies in the railways industry.	It provides the main source of revenue for the railway company.
A-IS-02	Information system	Linevideo surveillance	Tangible, fixed	IT system	Line	The video surveillance of strategic sections of line consist in the use of video cameras to transmit a signal regarding specific section of the railway system to a control room.	It contributes to a sufficient level of safety.

ANNEX II. ASSETS ID	Asset category	Asset name	Type	Sub-type	Location	Description	Functionality
A-IS-03	Information system	Tunnelsvideo surveillance	Tangible, fixed	IT system	Line	The video surveillance of tunnels consist in the transmission of signals generated by video cameras, located in tunnels, to a control room.	It contributes to a sufficient level of safety.
A-IS-04	Information system	Malfunction detection systems	Intangible, mobile	OT system	N.a.	Malfunction detection systems monitor a system, identify when a fault has occurred, and pinpoint the type of fault and its location.	It contributes to a sufficient level of safety.
A-IS-05	Information system	Wi-Fi hotspots	Tangible, mobile	IT system	Station, Train	A Wi-Fi hotspot is a physical location where people may obtain Internet access via a wireless local-area network (WLAN) using a router connected to an Internet Service Provider (ISP).	It provides additional services to the user.
A-EL-01	Electrical substation	Electrical substation	Tangible, fixed	Infrastructure	Station, Line	An electrical substationconverts electric power from the form provided by the electrical power industry for public utility service to an appropriate voltage, current type and frequency to supply railways with traction current.	It allows proper rail traffic.
A-RS-01	Rolling stock	Locomotive	Tangible, mobile	Equipment	Train	A locomotive is a rail transport vehicle that provides the motive power for a train.	It allows proper rail traffic.
A-RS-02	Rolling stock	Rail car	Tangible, mobile	Equipment	Train	A rail car is a self-propelled railway vehicle designed to transport passengers.	It allows proper rail traffic.
A-RS-03	Rolling stock	Onboard computer	Tangible, fixed	OT system	Train	On board computer guides the train driver with performance enhancing procedures to optimise transit time and fuel consumption, according to safety requirements.	It contributes to a sufficient level of safety.
A-RS-04	Rolling stock	GSM-R system	Intangible, mobile	IT system	N.a.	GSM-Railway system uses the international wireless communications standard for railway communication and applications. It is used for communication between train and railway regulation control centres.	It contributes to a sufficient level of safety.
A-RS-05	Rolling stock	Driver's console	Tangible, fixed	OT system	Train	Ensemble of all the instrumentation required to drive a train.	It contributes to a sufficient level of safety.
A-SS-01	Railway Signalling system	Light signals	Tangible, fixed	Infrastructure	Line	A railway signal is a visual display device that conveys instructions or provides advance warning of instructions regarding the driver’s authority to proceed.	It contributes to a sufficient level of safety.
A-SS-02	Railway Signalling system	Traffic light signals	Tangible, fixed	Infrastructure	Line	Traffic lights are Signalling devices positioned at intersections, crossings, and other locations to control flows of traffic.	It contributes to a sufficient level of safety.
A-SS-03	Railway Signalling system	Auxiliary signals	Tangible, fixed	Infrastructure	Line	They are used in railway practice to regulate train movement and provide an indication to the driver of conditions ahead, a range of auxiliary signals soon developed. They included whistles and bell rings, as well as numerous lineside boards, subsidiary lights on signal masts, and more.	It contributes to a sufficient level of safety.
A-SS-04	Railway Signalling system	Balise	Tangible, fixed	Infrastructure	Line	A balise is an electronic beacon or transponder placed between the rails of a railway as part of an automatic train protection (ATP) system.	It contributes to a sufficient level of safety.
A-SS-05	Railway Signalling system	ERTMS	Intangible, fixed	OT system	N.a.	ERTMS is the system of standards for management and interoperation of Signalling for railways by the European Union.	It contributes to a sufficient level of safety.
A-SS-06	Railway Signalling system	Antennas	Tangible, fixed	Equipment	Line	An antenna is the interface between radio waves propagating through space and electric currents moving in metal conductors, used with a transmitter or receiver.	It contributes to a sufficient level of safety.
A-SS-07	Railway Signalling system	Speed sensor	Tangible, fixed	OT system	Line	The vehicle speed sensor (VSS) measures transmission/transaxle output or wheel speed.	It contributes to a sufficient level of safety.
A-SS-08	Railway Signalling system	Timetable operation	Intangible, fixed	IT system	N.a.	A timetable is a time-management tool which consists of a list of activities at which possible tasks, events, or actions are intended to take place.	It allows proper rail traffic.
A-SS-09	Railway Signalling system	Block Signalling	Intangible, fixed	Infrastructure	N.a.	Signalling block systems enable the safe and efficient operation of railways by preventing collisions between trains. The basic principle is that a route is broken up into a series of sections or "blocks". Only one train may occupy a block at a time, and the blocks are sized to allow a train to stop within them. That ensures that a train always has time to stop before getting dangerously close to another train on the same line.	It contributes to a sufficient level of safety.
A-SS-10	Railway Signalling system	Centralised traffic control	Tangible, fixed	OT system	Station	Centralised traffic control is a system used to consolidate train routing decisions.	It contributes to a sufficient level of safety.
A-SS-11	Railway Signalling system	Train detection	Intangible, mobile	OT system	N.a.	Train detection is a system us to detect the presence of a train on a specific section of the railway.	It contributes to a sufficient level of safety.
A-SS-12	Railway Signalling system	Fixed signals	Tangible, fixed	Infrastructure	Line	Any type of signal which is along the sections or inside the stations and which is not removable	It contributes to a sufficient level of safety.
A-SS-13	Railway Signalling system	Cab Signalling	Tangible, fixed	IT system	Line	Cab Signalling is a railway safety system that communicates track status and condition information to the cab, crew compartment or driver's compartment of a locomotive, railcar or multiple units.	It contributes to a sufficient level of safety.

ANNEX II. ASSETS ID	Asset category	Asset name	Type	Sub-type	Location	Description	Functionality
A-SS-14	Railway Signalling system	Interlocking	Tangible, fixed	Infrastructure	Line	An interlocking is an arrangement of signal apparatus that prevents conflicting movements through an arrangement of tracks such as junctions or crossings.	It contributes to a sufficient level of safety.
A-SS-15	Railway Signalling system	Wind sensors	Tangible, fixed	IT system	Line	The wind sensors are located along the line and they measure the speed and direction of the wind continuously. The data is sent to the Operating Center (OC) and the Centralised Traffic Control Centre (CTC) in real time for adapting the speed of the train.	It contributes to a sufficient level of safety.
A-ST-13	Station	Depot	Tangible, fixed	Infrastructure	Station	The railway depot is the place where locomotives are usually housed, repaired and maintained when not being used.	It allows proper rail traffic.
A-IS-06	Information system	Router	Tangible, mobile	IT system	Station	A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet.	It is a fundament element of the IT infrastructure.
A-IS-07	Information system	Server	Tangible, mobile	IT system	Station	A server is a piece of computer hardware or software that provides functionality for other programs or devices, called "clients". Servers can provide various functionalities, often called "services", such as sharing data or resources among multiple clients, or performing computation for a client.	It is a fundament element of the IT infrastructure.
A-IS-08	Information system	Firewall	Tangible, mobile	IT system	Station	A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.	It is a fundament element of the IT infrastructure.
A-IS-09	Information system	Database	Intangible, mobile	IT system	N.a.	A database is an organised collection of data stored and accessed electronically from a computer system.	It is a fundament element of the IT infrastructure.
A-IS-10	Information system	Workstation	Tangible, mobile	IT system	Station	A workstation is a special computer designed for technical or scientific applications.	It is a fundament element of the IT infrastructure.

ANNEX III. Assets Condition

Sample of railway asset conditions, which were categorised and prioritised for CAMS input according to D3.1's asset classification guidelines [57].

ID	ANNEX III: Assets Involvement in Railway Operations					Purchase Cost	Operation Cost	Maintenance Cost	Renewal Cost	Disposal Cost	Connection to External networks	UIC RIS 30100 Classification
	Ticketing	Railway Freight Traffic	Railway Passenger Traffic	Train boarding alighting	Station operations							
A-TR-01	Negligible	Essential	Essential	Essential	Negligible	High	Low	Medium	High	High	no	Physical Object
A-TR-02	Negligible	Essential	Essential	Negligible	Negligible	Medium	Low	Medium	Medium	Medium	EN	Topology
A-TR-03	Negligible	Essential	Essential	Negligible	Negligible	High	Medium	High	Medium	High	EN	Physical Object
A-TR-04	Negligible	Essential	Essential	Negligible	Negligible	Very High	Low	Medium	Very High	Very High	no	Physical Object
A-TR-05	Negligible	Essential	Essential	Negligible	Negligible	Very High	Low	Medium	Very High	Medium	no	Physical Object
A-TR-06	Negligible	Essential	Essential	Negligible	Negligible	High	Low	Medium	Medium	High	EN, TN	Physical Object
A-TR-07	Negligible	Essential	Essential	Negligible	Negligible	Medium	Very Low	Very Low	Medium	Medium	no	Physical Object
A-ST-01	Essential	Negligible	Accessory	Negligible	Accessory	Low	Low	Low	Low	Medium	EN, IC	Physical Object
A-ST-02	Essential	Negligible	Accessory	Negligible	Accessory	Medium	Medium	Low	Medium	Medium	EN, IC	Physical Object
A-ST-03	Negligible	Negligible	Negligible	Negligible	Essential	Medium	Low	Low	Medium	Medium	EN	Physical Object
A-ST-04	Negligible	Negligible	Negligible	Negligible	Essential	Medium	Low	Low	Medium	Medium	EN	Physical Object
A-ST-05	Negligible	Negligible	Accessory	Accessory	Essential	Low	Low	Low	Low	Low	EN, TN	Physical Object
A-ST-06	Essential	Negligible	Accessory	Negligible	Accessory	Low	Low	Low	Low	Low	EN, TN	Physical Objects
A-ST-07	Negligible	Negligible	Accessory	Negligible	Essential	Medium	Low	Low	Medium	Low	EN, TN	Immaterial Object
A-ST-08	Negligible	Negligible	Negligible	Accessory	Essential	Medium	Low	Medium	Medium	Medium	EN, TN	Immaterial Object
A-ST-09	Negligible	Negligible	Accessory	Essential	Essential	High	Very Low	Low	High	High	no	Physical Objects
A-ST-10	Negligible	Negligible	Negligible	Negligible	Accessory	High	Very Low	Very Low	Very Low	High	EN, TN, IC	Physical Objects
A-ST-11	Negligible	Negligible	Negligible	Negligible	Essential	Medium	Medium	Medium	Low	High	EN	Immaterial Object
A-ST-12	Negligible	Negligible	Negligible	Negligible	Essential	Medium	Low	Low	Medium	Low	EN	Immaterial Object
A-IS-01	Essential	Negligible	Accessory	Negligible	Accessory	High	Low	Low	Medium	Low	EN, IC	Immaterial Object
A-IS-02	Negligible	Accessory	Accessory	Accessory	Accessory	High	Low	Medium	High	Low	EN, TN	Immaterial Object
A-IS-03	Negligible	Accessory	Accessory	Accessory	Negligible	High	Low	Medium	High	Low	EN, TN	Immaterial Object
A-IS-04	Negligible	Accessory	Accessory	Negligible	Negligible	High	Low	Low	Medium	Low	EN, TN	Logical Object
A-IS-05	Negligible	Negligible	Negligible	Negligible	Accessory	Low	Medium	Very Low	Low	Low	EN	Physical Object
A-EL-01	Negligible	Essential	Essential	Negligible	Negligible	HIgh	Low	Low	High	High	EN	Physical Object
A-RS-01	Negligible	Essential	Essential	Negligible	Negligible	High	Low	Low	High	High	EN	Physical Object
A-RS-02	Negligible	Essential	Essential	Negligible	Negligible	High	Low	Low	High	High	EN	Physical Object
A-RS-03	Negligible	Essential	Essential	Negligible	Negligible	Medium	Low	Low	Medium	Low	EN, TN, IC	Physical Object
A-RS-04	Negligible	Essential	Essential	Negligible	Negligible	Medium	Low	Low	Medium	Low	EN, TN	Immaterial Object
A-RS-05	Negligible	Essential	Essential	Negligible	Negligible	Medium	Low	Low	Medium	Low	EN	Physical Object
A-SS-01	Negligible	Essential	Essential	Negligible	Negligible	Low	Low	Low	Low	Low	EN	Physical Object
A-SS-02	Negligible	Essential	Essential	Negligible	Negligible	Low	Low	Low	Low	Low	EN, TN	Physical Object
A-SS-03	Negligible	Essential	Essential	Negligible	Negligible	Low	Low	Low	Low	Low	no	Physical Object
A-SS-04	Negligible	Essential	Essential	Negligible	Negligible	Low	Low	Low	Low	Low	EN, TN	Physical Object
A-SS-05	Negligible	Essential	Essential	Negligible	Negligible	High	Medium	Low	Medium	Low	EN, TN	Immaterial Object

ID	ANNEX III: Assets Involvement in Railway Operations					Purchase Cost	Operation Cost	Maintenance Cost	Renewal Cost	Disposal Cost	Connection to External networks	UIC RIS 30100 Classification
A-SS-06	Negligible	Essential	Essential	Negligible	Negligible	Low	Low	Low	Low	Low	EN, TN	Physical Object
A-SS-07	Negligible	Essential	Essential	Negligible	Negligible	Very Low	Very Low	Very Low	Very Low	Low	no	Logical Object
A-SS-08	Negligible	Essential	Essential	Essential	Essential	Very Low	Very Low	Very Low	Very Low	Very Low	EN, TN	Immaterial Object
A-SS-09	Negligible	Essential	Essential	Negligible	Negligible	High	Medium	Medium	Medium	Medium	EN, TN	Logical Object
A-SS-10	Negligible	Essential	Essential	Negligible	Negligible	Very High	Medium	Medium	High	Medium	EN, TN, IC	Logical Object
A-SS-11	Negligible	Essential	Essential	Negligible	Negligible	Medium	Low	Low	Medium	Low	EN	Logical Object
A-SS-12	Negligible	Essential	Essential	Negligible	Negligible	Low	Low	Low	Low	Low	no	Physical Object
A-SS-13	Negligible	Essential	Essential	Negligible	Negligible	Medium	Low	Low	Medium	Medium	EN, TN	Logical Object
A-SS-14	Negligible	Essential	Essential	Negligible	Negligible	High	Low	Medium	High	HIgh	EN, TN	Logical Object
A-SS-15	Negligible	Essential	Essential	Negligible	Negligible	Low	Very Low	Very Low	Very Low	Low	EN, TN	Logical Object
A-ST-13	Negligible	Accessory	Accessory	Negligible	Accessory	High	Medium	Medium	High	High	EN	Physical Object
A-IS-06	Accessory	Negligible	Negligible	Negligible	Accessory	Low	Very Low	Very Low	Low	Very Low	EN, IC	Physical Object
A-IS-07	Accessory	Negligible	Negligible	Negligible	Accessory	Low	Very Low	Very Low	Low	Very Low	EN, IC	Physical Object
A-IS-08	Accessory	Negligible	Negligible	Negligible	Accessory	Low	Very Low	Very Low	Low	Very Low	EN, IC	Physical Object
A-IS-09	Accessory	Negligible	Negligible	Negligible	Accessory	Low	Very Low	Very Low	Low	Very Low	EN, IC	Immaterial Object

SAFETY4RAILS

Partners:

Fraunhofer EMI

uic

Metro
Metro de Madrid

EGO
EGO Genel Müdürlüğü

RFI
RETE FERROVIARIA ITALIANA
GRUPPO FERROVIE DELLO STATO ITALIANE

LEONARDO

ceis
avisa partners

STAM
MASTERING EXCELLENCE

TCDD

RMIT UNIVERSITY

University of Reading

etra I+D

ΔΗΜΟΚΡΙΤΟΣ
DEMOKRITOS
NATIONAL CENTRE FOR SCIENTIFIC RESEARCH

IC information company

RINA

WINGS
ICT SOLUTIONS

Newcastle University

EOS
EUROPEAN ORGANISATION FOR SECURITY

CyberServices
MADE IN EUROPE

Innova Integra

LAUREA
AMMATTIKORKEAKOULU
University of Applied Sciences

FGC
Ferrocarrils
de la Generalitat
de Catalunya

erarGE

MTRS

INTRACOM
TELECOM

MH
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.