SAFETY4RAILS

Report on past failure analysis and lessons learnt

Deliverable 2.2

Lead Author: CS

Contributors: CEIS, FHG, UIC, LDO, RMIT, NCSRD, ERARGE, MTRS, IC

Dissemination level: PU - Public

Security Assessment Control: passed

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

D2.2 REPORT ON PAST FAILURE ANALYSIS AND LESSONS LEARNT			
Deliverable number:	2.2		
Version:	1.5		
Delivery date:	16/02/2022		
Deliverable due date:	31/12/2020		
Dissemination level:	PU - Public		
Nature:	Report		
Main author(s)	Róbert Szabó Fleur de Belloy	CS CEIS	
Contributor(s) to main deliverable production	Florence Ferrando Lemonia Argyriou Stelios C.A Thomopoulos Sujeeva Setunge Nader Naderpajouh Paul Abbott Yupak Satsrisakul Marie-Hélène Bonneau Ahmet Abdulkerim Claudio Porretti Ferenc Frész Anett Mádi-Nátor Katalin Béres Zsuzsanna Kéri Eros Cazzato	CEIS NCSRD NCSRD RMIT RMIT MTRS FHG UIC ERARGE LDO CS CS CS CS IC	*Support to main author*
Internal reviewer(s)	Atta Badii Andreas Georgakopoulos Antonio De Santiago Laporte Stephen Crabbe	UREAD WINGS MDM Fraunhofer	*Ethics Board* *Quality Manager* *Security Advisory Board* *Project Coordinator*
External reviewer(s)	Per-Erik Johansson	The European CBRNE Center	

Document control			
Version	**Date**	**Author(s)**	**Change(s)**
0.1	12/11/2020	CEIS	Initial version
0.2	17/12/2020	CEIS	Version 2
0.3	18/12/2020	CS	Version 3
0.4	23/12/2020	CS	Version 4
1.0	12/01/2021	UREAD/CEIS	Version 1.0 created from V0.4
1.1	15/01/2021	CEIS	Update to reflect PC reviewl
1.2	15/01/2021	CEIS	Format updates
1.3	15/01/2021	Fraunhofer/ CEIS	Update of document details, format updates, reference and source updates.
1.4	28/01/2022	CEIS	Integration of EC midterm evaluation's comments
1.5	15/02/2022	CEIS	Iteration with FHG & UIC reviews on version 1.4. - Page 13: Two sentences added in section 2.1.1 (Step 2, last paragraph) - Pages 13 to 14: Footnotes n°13, n°14 and n°16 reviewed - Page 14: One sentence added in Section 2.1.1 (Step 4) - Page 14: One sentence added in Section 2.2 paragraph 1. - Page 19: One sentence added in Section 3.1.2 paragraphs 3, 4 and 5. - Page 19: Addition in Section 3.1.2 of 3 paragraphs (6, 7 and 8)

		- Page 26: Addition of an introductive paragraph to Section 3.2.1 - Page 28: One sentence added in paragraph 1 of the page within Section 3.2.1 - Page 34: One sentence added in paragraph 4 within Section 3.3.1. - Page 34: New paragraph (7) in Section 3.3.1. - Page 40: Footnote n°37 added in paragraph 1. - Update of shading in Annex 2.

DISCLAIMER AND COPYRIGHT

ABOUT SAFETY4RAILS

SAFETY4RAILS is the acronym for the innovation project: Data-based analysis for SAFETY and security protection FOR detection, prevention, mitigation and response in trans-modal metro and RAILway networkS. Railways and Metros are safe, efficient, reliable and environmentally friendly mass carriers, and they are becoming an 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 2014) and combined cyber-physical attacks, which are important emerging scenarios given increasing IoT infrastructure integration.

SAFETY4RAILS concentrates on rush hour rail transport scenarios where many passengers are using metros and railways to commute to work or attend mass events (e.g. large multi-venue sporting events such as the Olympics). When an incident occurs during heavy usage, metro and railway operators have to consider many aspects to ensure passenger safety and security, e.g. carry out a threat analysis, maintain situation awareness, establish crisis communication and response, and they have to ensure that mitigation steps are taken and communicated to travellers and other users. **SAFETY4RAILS will improve the handling of such events through a holistic approach.** It will analyse the cyber-physical resilience of metro and railway systems and deliver mitigation strategies for an efficient response, and, in order to remain secure given everchanging novel emerging risks, it will facilitate continuous adaptation of the SAFETY4RAILS solution; this is validated by two rail transport operators and the results supporting the re-design of the final prototype.

TABLE OF CONTENTS

List of tables

List of figures

Executive summary

This document is the deliverable D2.2 – Report on past failure analysis and lessons learnt of SAFETY4RAILS, aiming to present an inventory of past accidents or attacks with a comprehensive analysis of how the project could help to prevent or mitigate vulnerabilities and the requirements needed to do it. The report presents the results of one main task, T2.2 which addresses both the identification of operational requirements derived from the analysis, lessons learnt from past failures, and the technical requirements for defining the architecture of a tool that would automate the collection, the analysis and proper usability of this data. The overall added value of understanding the past events is to support end-users to prevent similar incidents from happening and enable the end-users to be better prepared. To achieve this ambitious goal, past incidents have been analysed and attack scenarios derived and formalised in such a manner that automated prevention tools can be subsequently developed and prevention procedures deployed automatically where operationally and ethically suitable.

The report also considers how automated data analysis methods could be integrated into the SAFETY4RAILS Information System (S4RIS). The related chapter introduces the concept, its relevance for the SAFETY4RAILS project and examines the applicability of the different methods, in addition to providing examples of potential use-cases.

Preliminary outputs of these activities helped the preparation of the first End-User Workshop, which was held in December 2020 (14th and 15th), and this deliverable will feed into the further tasks in WP2 and the deliverables D1.4, D2.1, D2.3, D2.4 and D2.5. These tasks and deliverables focus on other user requirement aspects and the overall S4RIS system architecture and specifications.

The document is structured as follows:

- Introduction
- Building the past failure inventory
- Comprehensive analysis of past failures and trends in threats
- Definition of an automated data analysis method
- Derived preliminary operational requirements for S4RIS
- Conclusions
- Bibliography
- Annexes
  - Inventory – Raw data of past failures analysed
  - List of Abbreviations

1. Introduction

1.1 Initial definitions

As a starting point to build-up a structured analysis of past failure, covering incidents due to both physical, cyber and combined threats, a need arose to establish clear and simple definitions of frequently used words or phrases, in order to align their understanding within the consortium.

- **Asset** is understood as « a major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems. »[1]
- **Attack** is understood as « An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity. »[1]
- **Accident** is understood as " an unwanted or unintended sudden event or a specific chain of such events which have harmful consequences; accidents are divided into the following categories: collisions, derailments, level-crossing accidents, accidents to persons caused by rolling stock in motion, fires and others"[2]
- **Failure** is understood as « a state of inability to perform a normal function. »[3] In this document, the term is used synonymously with “event”, which includes accidents and incidents.
- **Incident** is understood as « any occurrence, other than accident or serious accident, associated with the operation of trains and affecting the safety of operation"[4]
- **Risk** is understood as « combination of the likelihood of a threat of exploiting an existing vulnerability, and the resulting impact of that unwanted situation. »[1]
- **Threat** is understood as « any circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image or reputation), organisational assets, IACS (Industrial Automation and Control System), or individuals who, contrary to security policy, intentionally or unintentionally prevent access to data or cause the destruction, disclosure, or modification of data. »[1]
- **Vulnerability** is understood as « weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. »[1]
- **False positive** is understood as « An instance in which an intrusion detection and prevention technology incorrectly identifies benign activity as being malicious. »[1]

In addition, to the above definitions which were defined from the railway and metro stakeholders’ perspectives, notably regarding the unwanted perspective of damage generated by the threat, three notions required more research: what can be understood as a physical, a cyber and a combined cyber-physical threat:

- **Threats with physical effect(s)** is understood as « an event or an action that is likely to cause unwanted physical damage ».
- **Threats with cyber effect(s)** is defined as « an event or action that is likely to cause unwanted damage in Information and Communication Technology (ICT) ».

Furthermore, it is noted that affects can be viewed from the perspective of their *likelihood*, *modality* and *severity* (e.g., scale and scope). In this respect, one can also recognise combined effects that many or may not arise from *hybrid attacks* translating into cyber-physical threats with cascaded effects, as defined within the User-Intimate Requirements Hierarchy Resolution Framework (UI-REF) Resolutions Requirements and Evaluation Methodology[5]:

Effects → Side-Effects → Cross-Effects → Affects

---

[1] CYRail Recommendations on cybersecurity of rail signaling and communication systems, September 2018
[2] European Railway Agency, Guidance on the decision to investigate accidents and incidents, Articles 3(l), 19 and 21(6), March 2011.
[3] Failure, Merrian-Webster, https://www.merriam-webster.com/dictionary/failure
[4] European Railway Agency, Guidance on the decision to investigate accidents and incidents, Articles 3(l), 19 and 21(6), March 2011.
[5] UI-REF Integrative Requirements and Evaluation Methodology, Badii Atta, 2009.

When it comes to defining combined threats, further research was requested in order to provide a common understanding on the combined aspect e.g., when and how and which aspect of the threat may lead to qualifying it as a combined physical-cyber threat. Research and analysis activities performed did not result in the selection of a commonly agreed definition for combined threats to railways and metro.

A description of cyber physical systems (CPS) was used as a starting point, defined and explained as follow: "Cyber Physical Systems (CPS) are networked systems of cyber (computation and communication) and physical (sensors and actuators) components to interact in a feedback loop with the possible help of human intervention, interaction and utilisation. »[6] (Human in the loop, HITL). Within this framework, any physical attempt designed to achieve unauthorised access to sensors and actuators could be considered as a cyber-physical attack. Yet, this definition is built solely on how the attack is conducted and tends to presume that combined cyber-physical attacks usually start from hardware whereas the attacks may apply either physical or cyber, digital ways to violate a system. As an illustration, a perpetuator physically damages the network cables and deploys a tempering or low-level attack to access the system.

The above approach to combined physical-cyber was considered reduced, since the purpose of this preliminary definition work is to focus on threats and not only on how an attack can be performed through first physical mean(s) and then cyber one(s). For this reason, SAFETY4RAILS partners decided to also consider combined effects, as well as threats from a combined origin, leading to considering a wider range of possibilities of what should be included in this category, as described below with illustrative examples.

Option 1: Event or action in the cyber space that is likely to cause unwanted damage to the physical environment. This definition includes cyber threat events (source) causing physical damage (consequences).

Example: A malware causing a malfunctioning of signals and a train or metro collision.

Option 2: Event or action in the physical space causing damage to the cyber environment. This definition includes physical threat events (source) causing damage to ICT, networks and nodes assets (consequences).

Example: An arson fire of ICT control panels.

Option 3: Event or action in the cyber space using a physical vector to cause damage to the physical or cyber environment. This definition includes cyber threat events (source) facilitated by a physical vector, causing damage to cyber and/or physical assets (consequences).

Example: High-jacking of connected devices.

Option 4: Simultaneous event or action in both the cyber and physical space to cause damage to the physical and cyber environment. This definition includes simultaneous cyber and physical threat events (source) causing damages to cyber and/or physical assets (consequences).

Example: Malware attack during a terrorist physical attack to prevent any reaction (such as use of communication and information systems used during the management of the physical attack).

1.2 Overview

The SAFETY4RAILS project aims to deliver methods and systems to increase resilience against physical, cyber and combined cyber-physical threats (including natural hazards) targeting or impacting track-based intercity railway and intra-city metro transportation.

As a preliminary step, one of the first activities conducted by the consortium within Work Package 2, which is on-going presently, is to identify the needs, requirements, specifications and concept architecture of the SAFETY4RAILS framework, through the strong involvement of end-users with expertise in railway security

[6] Ashibani, Yosef, and Qusay H. Mahmoud. "Cyber physical systems security: Analysis, challenges and solutions." Computers & Security 68 (2017): 81-97.

issues and by analysing past failures and experiences, current and future physical, cyber and combined threats based on OSINT. Analysing past incidents and attacks enables the collection of best practice and lessons learnt on the threats and methods to detect threats.

To this end, two main activities were conducted which are reported in this deliverable, namely the identification of operational requirements and the definition of an automated data analysis method.

The combination of literature review, analysis of data in open-source (more than 100 sources exploited) and consultations with experts and end-users enabled to elaborate:

- A dynamic inventory of past incidents and failures to produce statistics and derive key findings on trends and commonalities among threats.
- The principles for creating a data analytics model for the SAFETY4RAILS Information System (S4RIS).
- Some preliminary conclusions as to the way forward.

1.3 Structure of the deliverable

This document includes the following sections:

- Section 1 is the current chapter.
- Section 2 contains the description of the methodology and process used to build the inventory, followed by an analysis of the data sample – main figures and representativity.
- Section 3 encompasses the core analysis of the past failures, starting from the classification of incidents to achieve a common understanding of the various threats included in the scope of the project, followed by both quantitative and qualitative analysis, as well as a related news analysis to derive key findings on trends and commonalities.
- Section 4 focuses on the definition of the S4RIS data analysis method and possible use-cases.
- Section 5 presents preliminary operational requirements derived from the analysis which could support the developments of the S4RIS.
- Section 6 presents the conclusions.
- Section 7 contains the bibliography.
- Annexes include the complete presentation of the full inventory and the list of abbreviations used in the report.

2. Building the inventory of past failures

In 2019, rail freight transport in the EU was estimated at almost 400 billion tonne-kilometres7 and 8 billion passengers travelled on national railway networks in the EU in 20188, making railways a key asset and a critical infrastructure in the European Union and vulnerable to numerous threats.

Digital transformation is impacting all sectors of society and has resulted in an increased demand for smart and user-friendly solutions, particularly in the transport domain. This trend impacts all modes of transport with a significant technological shift and with the proliferation of intelligent transportation solutions.

Until recently, railways tended to be generally considered as a safe area with regard to cybersecurity, with security and crisis management staff focusing mainly on physical threats. This is due to the fact that they relied mainly on proprietary, segregated networks with specific protocols for management, communication and signalling. In other words, such systems were unlikely to be compromised due to the fail-safe design.

However, the changing landscape of ICT solutions, the digitalisation of several components of railway networks, the deployment of connected devices combined with increasing customer demands are leading railways to upgrade their existing legacy systems with more modern and standard-based infrastructures such as IP communication networks, in order to improve reliability, efficiency, capacity and customer experience. As a consequence, railway environment and systems are now vulnerable to both physical, cyber, and combined cyber-physical attacks.

The consequences are dire and as Emma Megan, from Global Rail Review, stated: "Since most railway operations focus more on core functionality and affordability, the entire industry side-lined cyber-security until certain breaches went public"[9] which can also apply for combined cyber-physical attacks.

Even though extensive literature has already been produced on the analysis of various physical and cyber threats targeting railways and metro, the SAFETY4RAILS project empirical research approach aimed at conducting a literature review of past failure events to get a better understanding of these two types of threats and of emerging combined cyber-physical threats to identify operators' challenges, associated needs and derive operational requirements to be addressed by SAFETY4RAILS solutions.

The outcome of this activity is a dynamic past failure inventory structured according to several key criterion to facilitate the analysis and get a common understanding of all the different types of threats to be addressed within the project.

2.1 Overview of the methodology to build the inventory

The methodology to identify, collect and analyse data on past incidents and attacks, typical threats and vulnerabilities impacting both railways and metro infrastructure, as well as their infrastructures is illustrated in Figure 1 below. The series of steps of the methodology is presented in this chapter.

[7] Eurostat Statistics Explained, *Railway freight transport statistics.*
[8] Eurostat Statistics Explained, *Passenger transport statistics.*
[9] Emma Megan, Why is cyber-security so important for the rail industry?, Global Railway Review, 31 January 2019.

FIGURE 1: OVERVIEW OF THE METHODOLOGY

2.1.1 A six-step approach

Step 1 – Initial definition of the research focus for the data collection process

The research focus of the inventory was defined in collaboration with different partners in line with the SAFETY4RAILS overall objective, namely collecting information on recurrent, on-going and emerging threats targeting railways and metros to support the development of solutions to enable operators to enhance their resilience capabilities.

Bearing in mind that it would not be feasible to produce a comprehensive inventory of all physical, cyber, and combined incidents which happened in Europe and beyond within the time allocated for this activity, a consensus took place to focus the scope of research on the following types of events and incidents:

- **Thematic criterion:** Events to be investigated should take place in urban areas and preferably multimodal configurations.
- **Geographical criterion:** Events to be investigated should take place in Europe or in a restricted list of third countries (namely the United-States (US), the United Kingdom (UK), Turkey, India, Israel, Russia, China, Switzerland).
- **Time criterion:** Events to be investigated should have taken place in the past 15 years or provide useful lessons learnt for current threats faced by railways and metro stakeholders.
- **Impact criterion:** Events to be investigated should be large scale incidents or incidents with cascading effects.
- **Data availability criterion:** Events should be investigated as long as there is sufficient information available in open sources to extract valuable outputs.
- **Redundancy criterion:** Events should be investigated as long as there is not already one or several similar incidents already included in the inventory.

The outcome of this definition of the scope enabled research to be focused on the most interesting past failure incidents to derive relevant operational requirements to feed the different work packages of the project and development of the S4RIS tool.

Step 2 – Desk research on railways and metro past incidents

This second step consisted in developing a data collection template to collect information on past incidents in a structured manner. To that purpose an analysis grid setting criteria and theme was created to classify the information collected on the past failure events.

The following preliminary list of criteria where validated by members of the Consortium:

- **Date** of the incident.
- **Country and city** where the incident happened.

- **Transport type** impacted: railways, metro, multimodal.[10].
- **Failure Type**: Cyber, Physical, Combined.
- **Main causes of the incident**: Man-Made, Natural Hazard, Technical Failure.[11]
- **Sub-causes of the incident**: flooding, landslide, fire, terrorist attack, cyber-attack, etc.[12]
- Component impacted or targeted.
- Casualties & other consequences.
- Short description of the event.
- Mitigation & corrective measures during crisis.
- **Lessons learnt**: revision of security or safety measures, update and corrective actions implemented after the event.
- Key points regarding technical requirements.
- Sources.

Once the template was validated, the work consisted in conducting a literature review and open-source research in order to collect data on the pre-defined scope. A collaborative desk research mobilised several members of consortium knowledge of open-source information, such as general medias or specialised on railways domain to collect raw data on past failures. All sources of information identified provide partial or complete data are sorted by accident in Annex 1[13].

Step 3 – Collation of Raw Data

During a preliminary data collection phase, a first team of analysts gathered the relevant data in the data collection grid. A second team of analysts validated and further enriched the preliminary data. The full inventory is presented in Annex 1[14]. Once the collation of incidents reached a satisfactory level, partners involved initiated an analysis of the different incidents by exploring various parameters which included:

- The origin, nature and type of threats.
- The stakeholders involved.
- The segments and assets targeted or impacted.
- The unfolding of the events.
- The mitigation and corrective measures implemented during the crisis.
- The recovery and patching measures deployed after the crisis and/or update of crisis management / security procedures.

Step 4 – Consultation with railways and metro end-users

The data collection team performed a first analysis of the raw data which led to the review of the incident inventory template and to the development of a draft set of key findings and lessons learnt. This was then shared with other partners and end-users belonging to the consortium to collect their inputs, comments and feedbacks.

In parallel, preliminary results were presented to both internal and external railways and metro end-users and to the SAFETY4RAILS Advisory Board during the SAFETY4RAILS first End-User Workshop which took place on December 14th and 15th, 2020.

---

[10] In the scope of the SAFETY4RAILS Project, multi-modal environment can be defined as an environment which combined several transport mode (train and metro, or with other transport mode).
[11] This classification was restructured at the analysis phase.
[12] Ibid.
[13] Annex 1 data is based on open-source information, yet it could be a useful collation of tactics providing information for would be attackers. On this basis, the Annex 1 was declared confidential.
[14] Ibid.

This enabled end-users to provide their input anonymously considering also confidential experiences, including without reference to specific details, for example by commenting on the open-source information.

Step 5 – Analysis of the consolidated raw data

After the virtual workshop and once all final comments were received, a second analysis was conducted to refine the research outputs. The methodology used in this step was a qualitative use of the Delphi Method[15]. This method ensures that the data collection team and the data analysis team benefit from and build on each other's expertise, and that the final analysis addresses all aspects of the request presented in a concise, coherent and comprehensive way.

Step 6 – Reporting

This final step consisted in further developing findings and in drafting the present report in collaboration with different partners to present the inventory and analysis.

Close interactions and exchanges with end-users ensured that the final recommendations were in line with the end-users' needs and expectations.

2.2 Representativity of the inventory

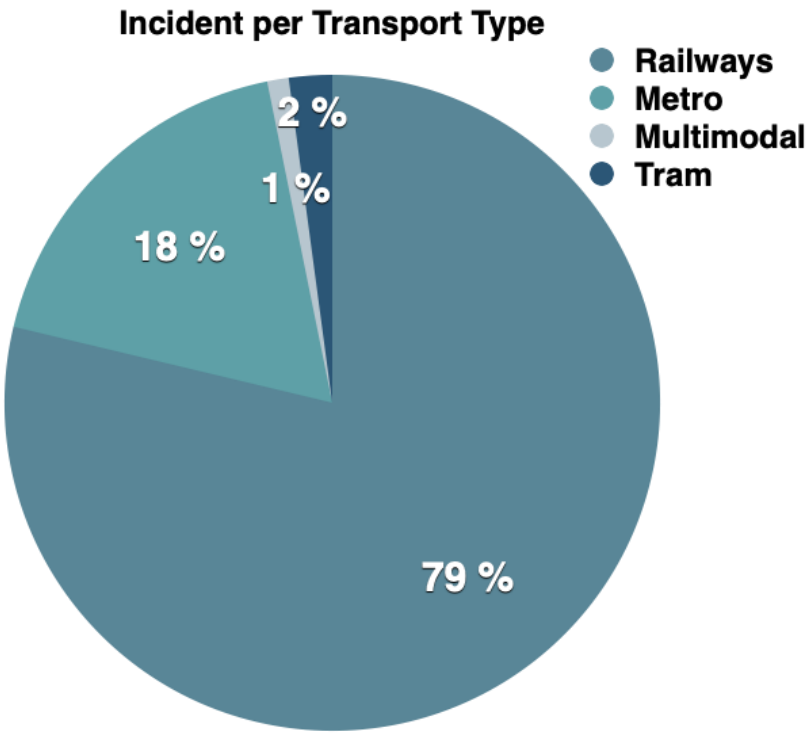
The identification of reliable and qualitative data was crucial throughout the research. During the open-source desk research phase, information on **95 past failures and incidents** was collected. Composed of mainly articles available online, several sources were cross analysed to extract and complete partial information in order to cover the most added-value information. All these open-sources references are sourced in Annex 1, for each identified past failures[16].

Figure 2 shows a presentation of the data sample representativity according to three main criteria: incident per transport type, incident per failure type and per country.

[15] For an explanation of the Delphi Method please see: Delphi Method | University of Phoenix Research Hub

[16] Annex 1 data is based on open-source information, yet it could be a useful collation of tactics providing information for would be attackers. On this basis, the Annex 1 was declared confidential.

FIGURE 2 REPRESENTATIVITY OF THE INCIDENT TYPE INVENTORY PER TRANSPORT AND FAILURE TYPE



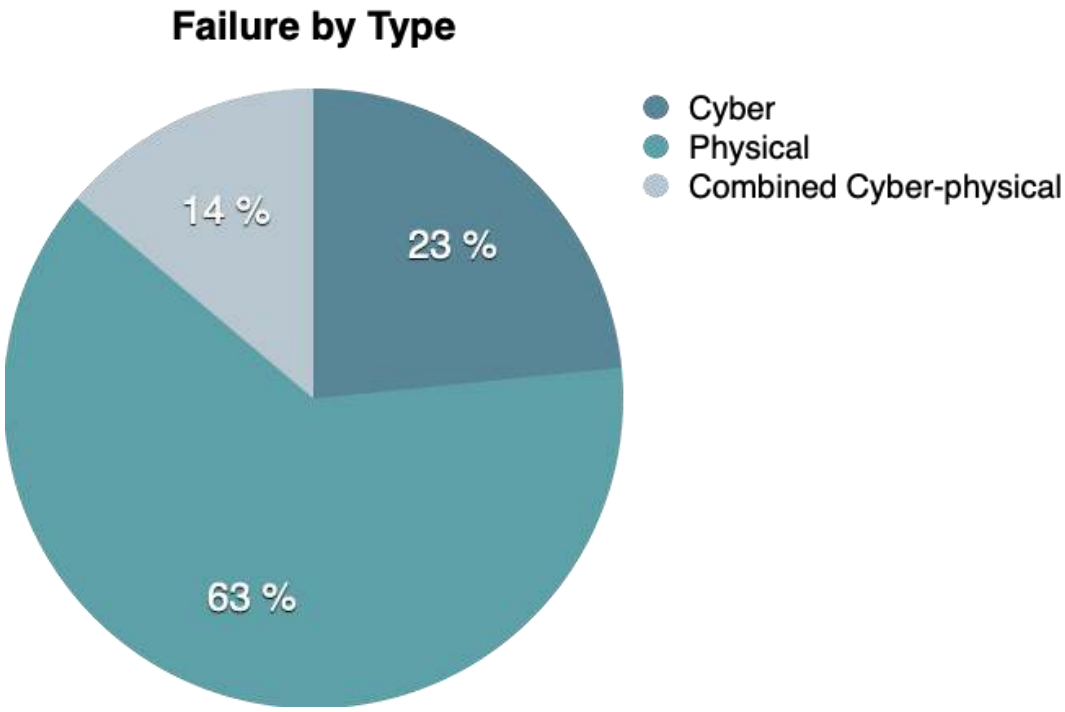
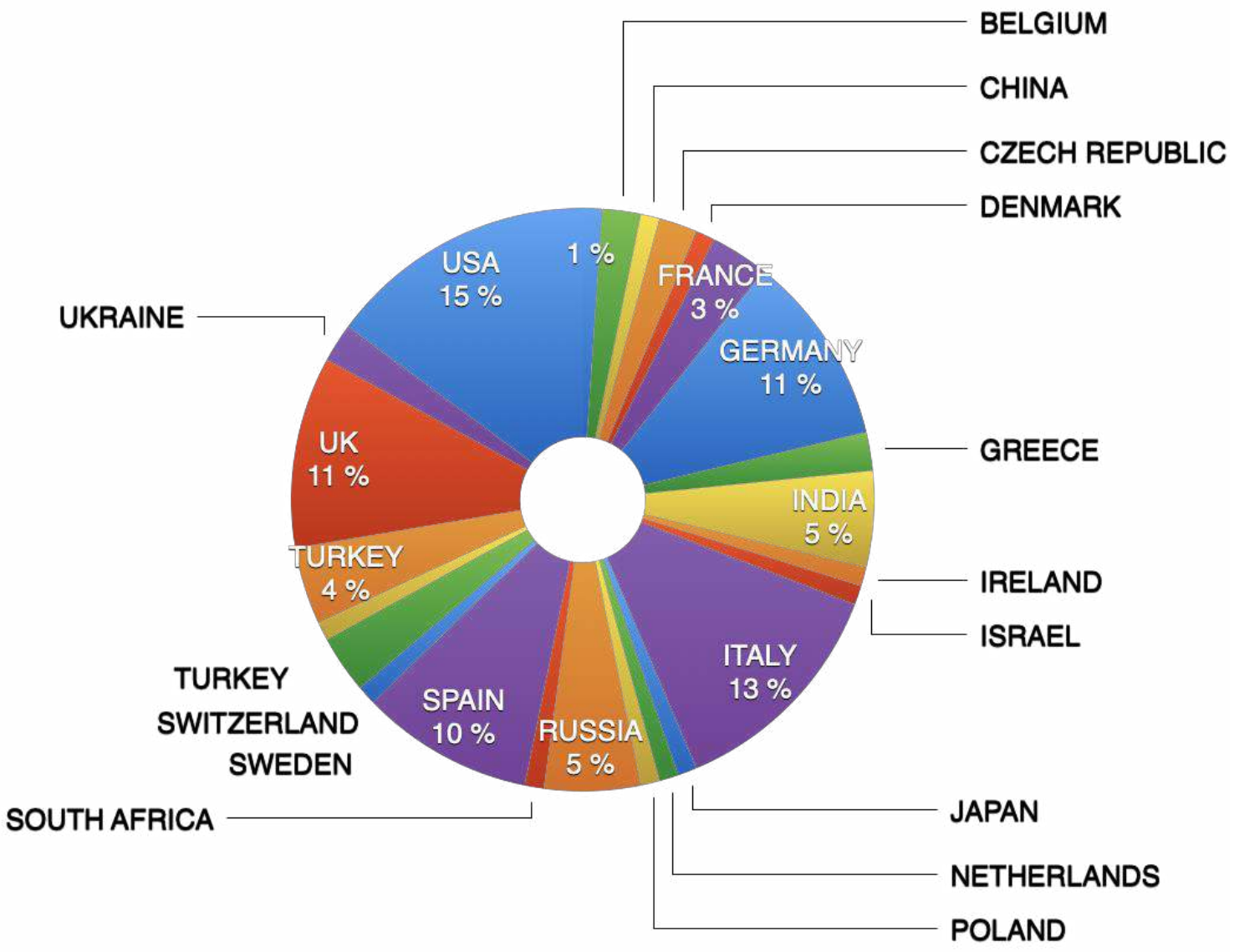


FIGURE 3: REPRESENTATIVITY OF THE INCIDENT INVENTORY PER TRANSPORT PER COUNTRIES



3. Comprehensive analysis of past failures

According to a preliminary study carried out by Steer Davies Gleave/DG MOVE in 2016[17], there were four main challenges impacting the assessment of threats targeting the railway sector, which actually also applies to the metro sector. These challenges are presented below:

- An insufficient understanding of the security threat, partly a result of the infrequency of severe security incidents but also due to a lack of reporting and sharing of data.
- An inadequate response to the threat to the European rail network as a whole, reflecting a focus on specific risks arising at the national level and weak incentives to address unspecified and poorly understood threats.
- Different approaches to the mitigation of security risks among rail industry decision-makers across the EU, e.g. driven by cultural differences and by the application of inconsistent methodologies for risk assessments; and
- Fragmentation of and gaps in security arrangements and responsibilities at both the national and EU level, a result of failures to coordinate security measures on international services accentuated by the growth of the cross-border rail network.

To partially address these challenges, the present analysis of past failures intends to provide a common understanding of what constitutes security and safety threats, propose a comprehensive classification and typology of both physical, cyber, and combined threats that will be used within the SAFETY4RAILS project to derive some first lessons learnt on mitigation actions and corrective measures which could be applied.

3.1 Typology of incidents and past failures

3.1.1 The need for a common typology of incidents and threats covering both threats with physical, cyber, and combined effects within S4R

Metro and railways ecosystems are continuously exposed to endless cases of failures and incidents from very different origins. Within the European Union (EU), Member States (MS) are required to establish independent National Investigation Bodies (NIBs)[18] to investigate serious accidents and sometimes incidents to collect lessons learnt to improve security and safety performance. However, each Member State tends to rely on its own standards and classification and there is currently no common pan-European definition of what constitutes a threat or standard classification used by all. Despite the fact that extensive literature has been produced on risks, threats and vulnerabilities in the railway and metro sectors, each organisation or researcher tends to rely on a different classification or typology of incidents and threats.

Existing threat classification methods can be based on several parameters:

- Threat source
- Attack techniques
- Threat impacts
- Threat agent
- Threat motivation
- etc.

Furthermore, there is no existence of a threat typology or classification covering cyber, physical, and combined threats applying to both metro and railways environments as shown in the examples below:

[17] Report on options for the security of European high-speed and international rail services, Final Report, December 2016.
[18] European Union Agency for Railways, *Rail Accident Investigation.*

TABLE 1 ILLUSTRATIONS OF THREAT CLASSIFICATION

	Physical	Cyber	Combined
ISO standard (ISO 7498-2)		X (not dedicated to rail or metro)	
ISO standard (ISO 27005)		X (not dedicated to rail or metro)	
Microsoft STRIDE Model		X (not dedicated to rail or metro)	
RAND corporation Threat tactic classification	X (railways)		
Cyber-Physical Security Risk classification (Rerik, Gransart & Berbineau)	X (railways)	X (railways)	
ENISA cybersecurity Threat model (2015)		X (all transport)	

Consequently, partners decided to build a hybrid incident classification to facilitate this analysis and derive lessons-learnt for the development of the S4R information system.

3.1.2 A structured typology of threats

As the end-goal of the SAFETY4RAILS is to support the prevention and mitigation of threats, it was crucial to start by defining a certain number of notions and sort the incidents and failures according to different parameters:

- The incident origin; Was the incident intentional or unintentional?
- The threat origin: Was the incident source from a natural or human origin?
- The threat actor's motive: Was the incident caused by a threat actor with unknown, criminal or terrorist motives?
- The type of event or threat techniques: what kind of event occurred or how did the event/attack occur?

Each parameter is presented below, within a step-by-step approach that was designed to ensure that the entire spectrum of cyber, physical, and combined risk and threats currently faced by railways and metro environments are considered in the scope of the project. This classification has been presented to end-users and SAFETY4RAILS Advisory Board members to collect their insights and refine the table.

Held in December 2020, this workshop gathered in two different interactive online sessions two different audiences, first the « internal end-users » (e.g. end-users who are partners in SAEFTY4RAILS) and members of

the SAFETY4RAILS External Advisory Board. The second audience enables feedback from a more diverse audience that include relevant stakeholders with railways and metro operators.

First Segmentation layer - Based on the intention

At the root of the concept of an incident is the intent, the clear intention to inflict harm or cause damage or the incident from a natural origin which was not intended.

Therefore, the primary segmentation of the incidents reviewed was made as follows:

Incident origins	
Unintentional	Incident that has not been planned or intended
Intentional	Incident that is planned or intended

This distinction is crucial for safety and security management when it comes to the preventive actions which could be implemented. Moreover, this distinction between unintentional and intentional origin of accident can represent a helpful basis to distinguish safety and security concepts based on the origin of incidents and accidents.

In the case of natural incidents, nothing can be done to prevent the incident from happening, stakeholders can only try to forecast it or focus on response, mitigation and recovery - which belong to safety domain. Safety is protection against accidental events, but these can come from internal causes (faults, errors, omissions…) and external causes (for example third parties at level crossings or natural disasters and climate events).

In the case of intentional incidents, actions could be taken to prevent it - which fall under the security domain. Security is protection against intentional damage (delinquency, terrorism, cyber-attacks ….)

On the one hand, safety policy is managed internally by a rail company in a precise framework involving human factors, technical failures, probabilisation of safety events and reflection on the ratio cost/benefit. On the other hand, security policy is structured around partnerships with national authorities. Railways focus on their vulnerabilities and level of threat is defined by the authorities. The threats, especially regarding cybersecurity, are constantly evolving, consequently a probability-based analysis and a cost-benefice approach are less relevant than they are for safety.

Safety and security requirements are originally different but need to be coherent since both safety risk and security threats can lead to exploitation or accidents, causing serious damages and many casualties.

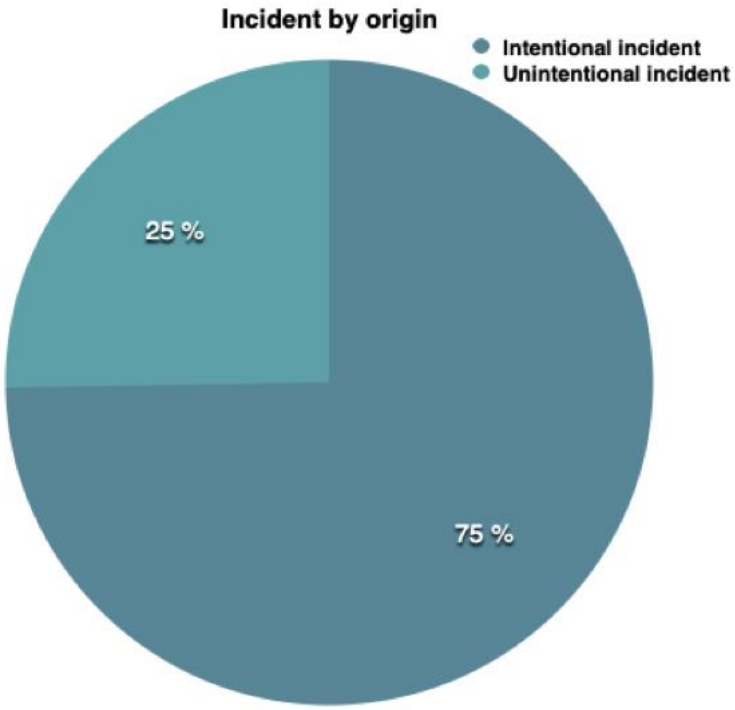
In a nutshell, if the failure is due to unintentional cause (such as a natural disaster, a human error resulting in so-called "accident") safety measures can be developed and implemented to ensure efficient response to its consequences. On the other hand, in cases of accident/incident of intentional origin, security mechanisms aimed at protection are applied.

The notion of safety and/or security hazards can add an additional layer of analysis to capture the range of threats and risk possibilities, since safety and security hazard are considered as an action or environment conditions that could lead potentially, but not for sure, to an incident or accident.

Within our past failure literature inventory, the distribution of incidents using the first segmentation showed that a majority of incidents were intentional, **since 75% of the data sample were planned or intended[19].**

[19] Bearing in mind that redundant incidents have been excluded from the data sample.

FIGURE 3: DISTRIBUTION OF INCIDENTS BY ORIGIN



Second Segmentation layer - Based on the origin of the threat

A second parameter which is often considered in threat classification is the origin of the threat. Is the threat origin natural or man-made? By definition, all intentional threats are man-made, but a certain number of unintentional events can have a human origin. For example, a flooding event of a train or station originated from a broken dyke which have been misconceived or mal maintained or a dysfunction at an organisational level can result in an incident.

Therefore, the secondary segmentation of the incidents reviewed was made as follows:

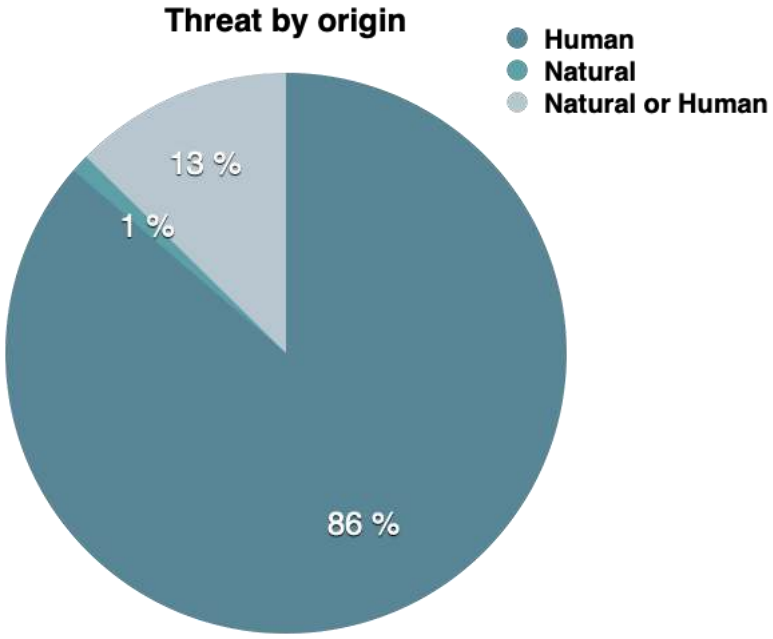
Incident origins	Threats origins	Description
Unintentional	Natural	Elements of the physical environment, harmful to man and caused by forces extraneous to human activities
	Human	Harmful events generated by a human action or resulting from a dysfunctioning at organisational level, whose consequences were not intended or expected
Intentional	Human	Actions generated by a human, who intended or expected these consequences

The distinction based on the threat origin is crucial within the S4R project as all incidents with a natural origin are treated as safety threats, therefore managed by the safety department whereas incidents with a human origin are treated as security incidents, therefore managed by the security department.

Within our past incident literature inventory, the distribution of incidents using the second segmentation showed that a majority of threats were caused by humans, since **86% of the data sample were from human origin**.

Within our sample, 13% of the incidents were classified as “Natural or Human” as there was not enough information on the incident to be certain if the incidents were due to a dysfunction at an organisational level/generated by a Human action or purely caused by elements of the physical environment.

FIGURE 4: DISTRIBUTION OF INCIDENTS BY ORIGIN



Third Segmentation layer - Based on the motives behind the threat (when applicable)

The third segmentation integrates the motives behind the threat, which of course do not apply to unintentional incidents. This third segmentation layer can be divided between unknown motives, criminal motives or terrorist motives. Therefore, the third segmentation of the multiple incidents reviewed was made as follows:

Incident origins	Threats origins	Threats motives	Definition
Unintentional	Natural	***Not applicable***	*Not applicable*
	Human	***Not applicable***	*Not applicable*
Intentional	Human	**Unknown**	Action perpetuated without any political or financial motives clearly identified or claimed
		Criminal*	Action perpetuated for financial gain or other malicious motives
		Terrorist*	Action perpetuated with a political, ideological and/or advocacy motive

** Insider threat would be integrated within those two motives if the threat agent is internal to the railway or metro organisation*

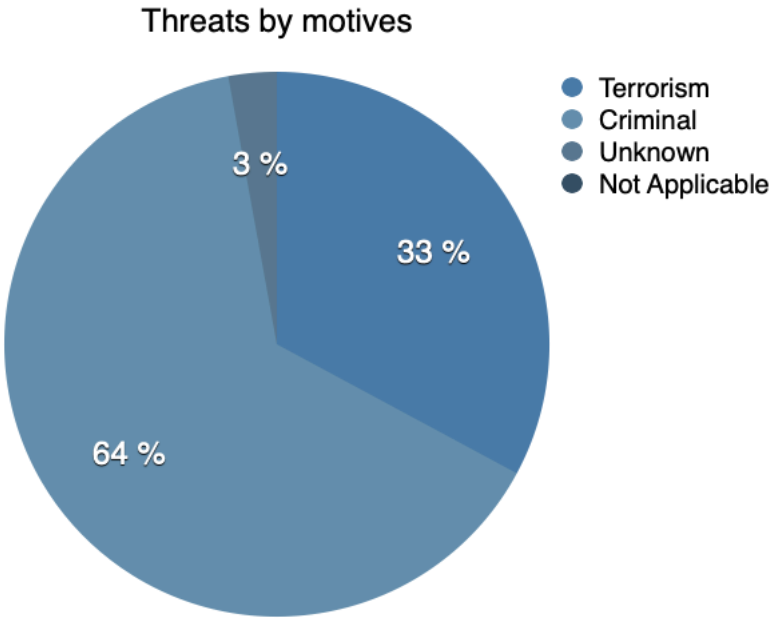
Within this segmentation, a transversal component should be considered: the insider threat. Insiders are often considered as a distinct category of threat as it requires specific prevention, detection, response and recovery actions from the stakeholders. Within the S4R project, insiders are a transversal notion which is included in both criminal and terrorist motives as an insider can decide to cause an incident for one or the other motive.

When it comes to terrorist motives, as the core definition can change significantly, from one country or organisation to another, it was decided to use a hybrid definition encompassing several elements provided by an end-user, the core one being having an ideological motive.

This segmentation is essential as the first responders and authorities involved to respond to the incident will differ according to the motives. A terrorist attack, being considered a national security threat, the threat management will be dealt in a different manner than for a criminal attack (involvement of national authorities, intelligence services, special forces, etc.).

Within our past incident literature inventory, the distribution of incidents using the third segmentation showed that a majority of motives were criminal, since 64% of the data sample threats were conducted for criminal motives.

FIGURE 5: DISTRIBUTION OF INCIDENTS BY MOTIVE



Fourth Segmentation layer - Based on the event itself

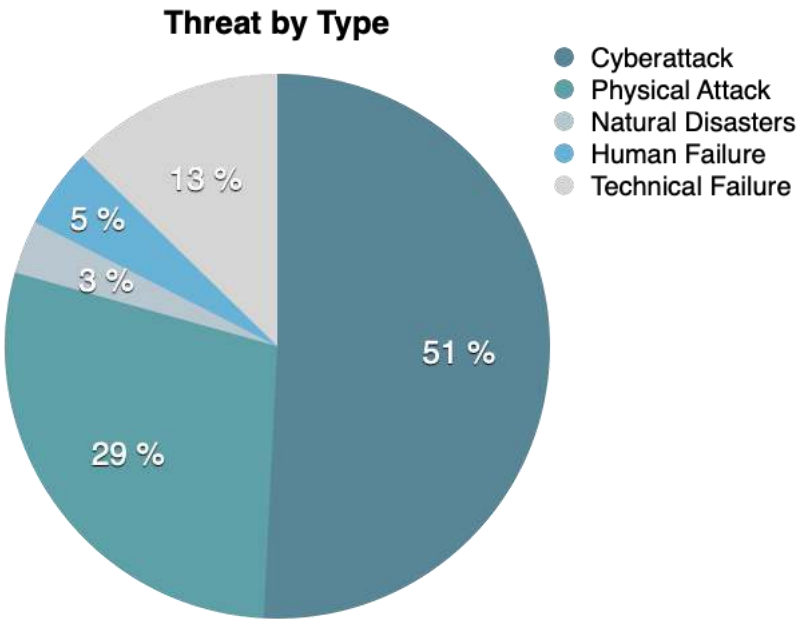
Finally, the fourth segmentation integrates the nature of the event itself (natural disasters, technical failure or environmental disasters) or, for intentional incident, the attack technique which can be physical, cyber or combined. Therefore, the fourth segmentation of the multiple threats reviewed was made as follows:

Incident origins	Threats origins	Threats motives	Threats events
Unintentional	Natural	*Not applicable*	Natural disasters
	Human	*Not applicable*	Human factor
			Technical failure
			Environmental disasters
Intentional	Human	Unknown	Physical attack
			Cyberattack
			Combined
		Criminal	Physical attack
			Cyberattack
			Combined
		Terrorist	Physical attack on infrastructure
			Physical attack on persons
			Cyberattack
			Combined

This segmentation is important within the project to adapt safety and security procedures and tools according to the threat techniques or events.

Within our past incident literature inventory, the distribution of threats using the fourth segmentation showed that a majority of threat events or actions were cyber-attacks **since 51% of the data sample were cyber-attacks**.

FIGURE 6: DISTRIBUTION OF THREAT BY TYPE


Threat by Type
Cyberattack
Physical Attack
Natural Disasters
Human Failure
Technical Failure
51 %
29 %
3 %
5 %
13 %

3.1.3 SAFETY4RAILS proposed typology of threats

Once reviewed by end-users and other members of the consortium, the final typology of threats which will be used within the project is as follows:

Incident origins	Threats origins	Threats motives	Threats events	Actions or events (non-exhaustive list)
Unintentional	Natural	*Not applicable*	Natural disasters	Floods, wind storms, snow, blizzard, earthquake, tsunami, landslide, avalanche
	Human	*Not applicable*	Human failure	Trouble of attention, fatigue, lack of training and/or awareness, disfunctionning at organisational level (lack of/poor safety culture, management)
			Technical failure	Infrastructure, vector, systems or signals failure, energy power, ICT failure due to lack of maintenance or misfunction/malfunction
			Environmental disaters	Floods, fires, rock or object fall, landslide due to infrastructure/equipment misconceived or poorly-maintained
Intentional	Human	Unknown	Physical attack	Vandalism, fire
			Cyberattack	Hacking, intrusion
			Combined attack	Combination of actions from the above two categories
		Criminal	Physical attack	Theft, agression of person
			Cyberattack	Theft, espionnage, leackage, manipulation, compromise, abuse
			Combined attack	Combination of actions from the two above categories
		Terrorist	Physical attack on infrastructure	Explosive device, CBRN threats, destruction of infrastructure and goods
			Physical attack on persons	Explosive device, CBRN threats, shooting, stabbing, highjacking, kidnapping, hostage crisis
			Cyberattack	Theft, espionnage, leackage, manipulation, compromise, abuse
			Combined attack	Combination of actions from the above two categories

This typology includes a non-exhaustive list of examples which were encountered during the literature review for each category of threat event. This list is not comprehensive but rather illustrates the important diversity of threats which could be tackled within the project.

3.2 Findings from the past failure analysis

In the past twenty years, both railways and metro stakeholders have experienced a wide variety of incidents and threats which are constantly evolving as the environment, ecosystem and technologies are also changing.

Though many incidents are very singular, three important trends are emerging from the review of past failures: the constant threat posed by terrorist actors impacting both infrastructures and passengers, an explosion of the number of criminal cyber-attacks and the regular catastrophic natural disasters impacting urban areas.

It is worth mentioning that these trends are based on the sample of past failures analysed which is not meant to be comprehensive of all the incidents faced by railways and metro stakeholders. The inventory, as any other sample, is biased at least at two levels:

- Partners might have preferences to research the areas/domains they are familiar with – possibly resulting in research gaps.
- Media are more likely to cover malicious, intentional incidents rather than unintentional ones with a similar severity of the outcome – possibly skewed towards intentional incidents.

However, these trends have been supported by the review of additional threat landscape reports which confirm the following findings.

3.2.1 Key findings from past failures

Despite interesting following findings derived from past failures, it is to be noted that these summarised conclusions relying on historical data and should be completed with prospective research on emerging and future threats to ensure the preparedness of railways stakeholders to threats evolutions, especially related to cyber and combined cyber-physical aspects. This observation emphases the need to consult railways experts and operators to integrate prospective approach on threats on railways safety and security[20].

Continuous terrorist threats in Europe Targeting passengers and crowded areas

As highlighted by the European Commission (DG MOVE), transport infrastructure in general, railways and metros in particular, are particularly targeted by terrorist attacks:

"Terrorist attacks in the European Union have over recent years shown a greater focus on attacking public areas, where crowds of people with little or no protection can be killed or injured. Rail transport is one of these targets due to the large numbers of people travelling and the relatively open nature of rail transport compared with air transport."[21]

From the Madrid 2004, London 2005 or Brussels 2016 Bombing attacks, railways and metro stakeholders are continuously under the threat of terrorist groups. Unpredictable, often dramatically deadly and provoking important damages, those physical attacks also have major psychological impact on European citizens, contributing to maintain a climate of fear in numerous countries.

According to our research the main techniques of terrorist attacks are:

- Explosives devices which represent 78% of terrorist attacks in the analysed sample.
- Fire.
- Hostage crisis.

[20] Activity conducted within the Task 2.1 with workshops and meetings to present and improve results of Task 1.1 activities.
[21] European Commission – DG MOVE, *Improving passenger railway security.*

The main characteristic of these attacks is that they are targeting passengers in crowed areas (rolling stock or metro, crowded stations, etc.) to inflict the highest number of casualties. These attacks tend to have major impact on infrastructure such as property damage in the case of explosives, or unavailability of ICT systems in the case of cyber-attacks.

In terms of consequences, the terrorist attacks are causing important transport disruptions, including long interruption of services and often cascading effects, in particular for explosives devices blast which usually has a negative impact on power generation in the area.

As the social/crowd panic following such type of events is often important, first responders' activities on site are always made more complex. Coordination and communication are jeopardized by the high numbers of stakeholders involved as illustrated by the London 2005 Bombing Attack for which several false elements were reported or alleged such as the origin of the blast (initially mistaken with a power surge), the exact number of bombs, or the death toll.

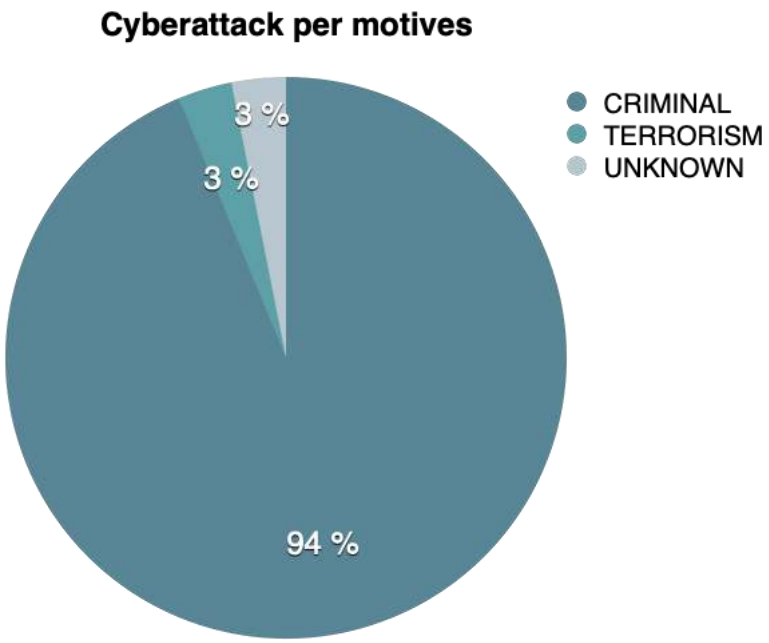
A dramatic increase of criminal cyber-attacks with a large panel of threat vectors which can impact both cyber and physical assets

The increasing digitalisation of railway and metro sectors, the growing deployment of connected devices while indisputably contributing to enhance passengers' experience, at the same time also exposed those sector ecosystems to new threats. The review of past failures highlights the fact that in the last decade, both railways and metros have been experiencing an explosion in the number of cyber-attacks, using different attack vectors and targeting different assets.

A minor number of cyber-attacks analysed are characterised as unknown, which can be referred to as acts which cannot be affiliated to criminal or terrorist motives, such as persons conducting cyber-attacks as personal challenges, just to see if they are actually able to hack into a system (the term 'hobby hackers' or 'script kiddies' is usually applied).

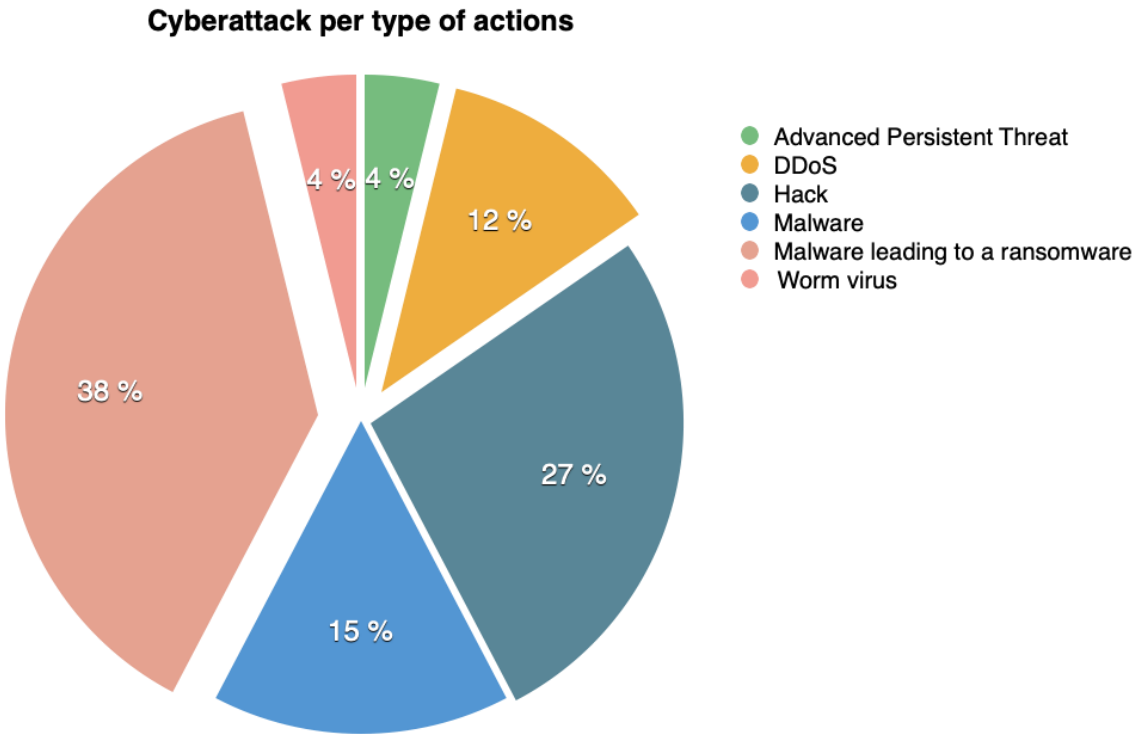
With a second exception made for a few terrorist motivated cyber-attacks, the grand majority of cyber-attacks are criminals, motivated by financial gains as illustrated in the graph below. Within our data sample, **94% of cyber-attacks are conducted for criminal motives.**

FIGURE 7: DISTRIBUTION OF CYBER-ATTACKS PER MOTIVE



Cyberattacks targeting railways and metros can take very different shape but according to our data sample, the three most recurrent cyber-attacks used tools such as malware, with a large majority leading to a ransomware, hack and Distributed Denial-of-Service (DDoS).

FIGURE 8: DISTRIBUTION OF CYBER-ATTACKS PER TYPE OF ACTIONS



These cyber-attacks are leveraging different vulnerabilities from organisation servers and computers, to ATM and vending machines in the stations and even if they rarely tend to provoke human casualties, the most important consequences are financial losses and damage organisational reputation. Here the need to implement cybersecurity policies and use technologies to protect railways ICT systems - and consequently their physical assets - from vulnerabilities exploitation appears essential to ensure the overall security of railways systems and infrastructures.

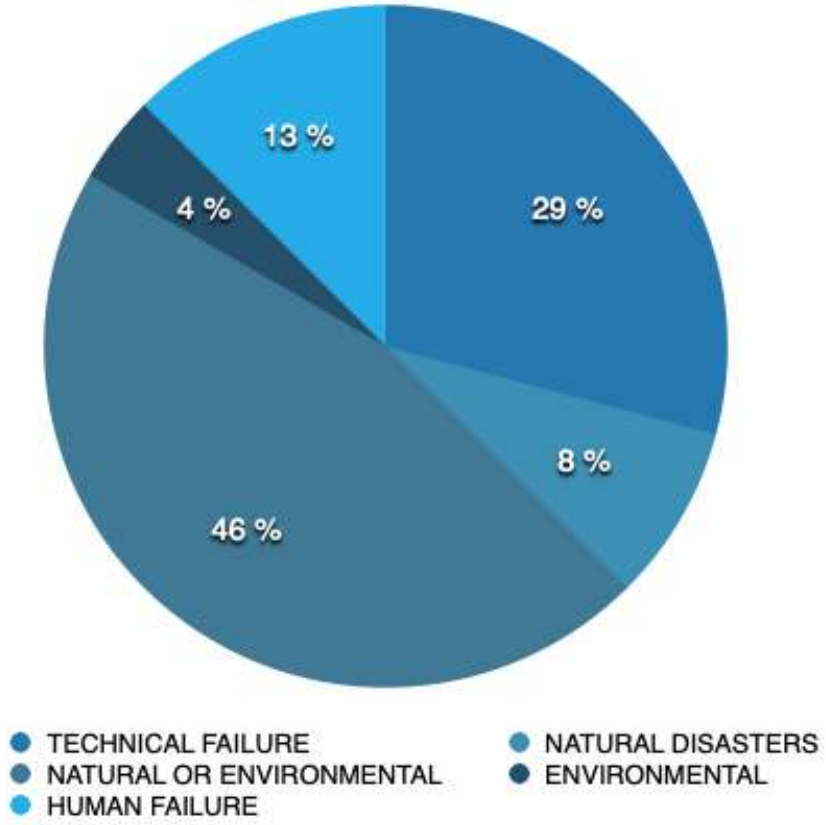
Frequent natural disasters impacting metropolitan and urban areas

As climate change has become a major concern within the European Union, the mitigation of natural disaster impacts remains a crucial goal at both EU and National level.

As illustrated in our past incident review, numerous metropolitan and urban areas are particularly vulnerable to natural disasters and regularly experience these catastrophic events. The regular flooding phenomenon and earthquakes in Italy, periodic flooding in Ankara (Turkey) or annual forest fires in southern Europe (France, Spain, Portugal) can have major impacts on railways and metro environment causing both important damages on infrastructure and long business interruptions.

The visual representation below highlights that regarding unintentional incidents, the **combination of the natural and/or environmental disasters represents 58% of past failures analysis**, among them 33% related to floods. The second position in terms of number of incidents after this first large category of unintentional incidents is related to technical failure, when human failure represents 13% of the data sample.

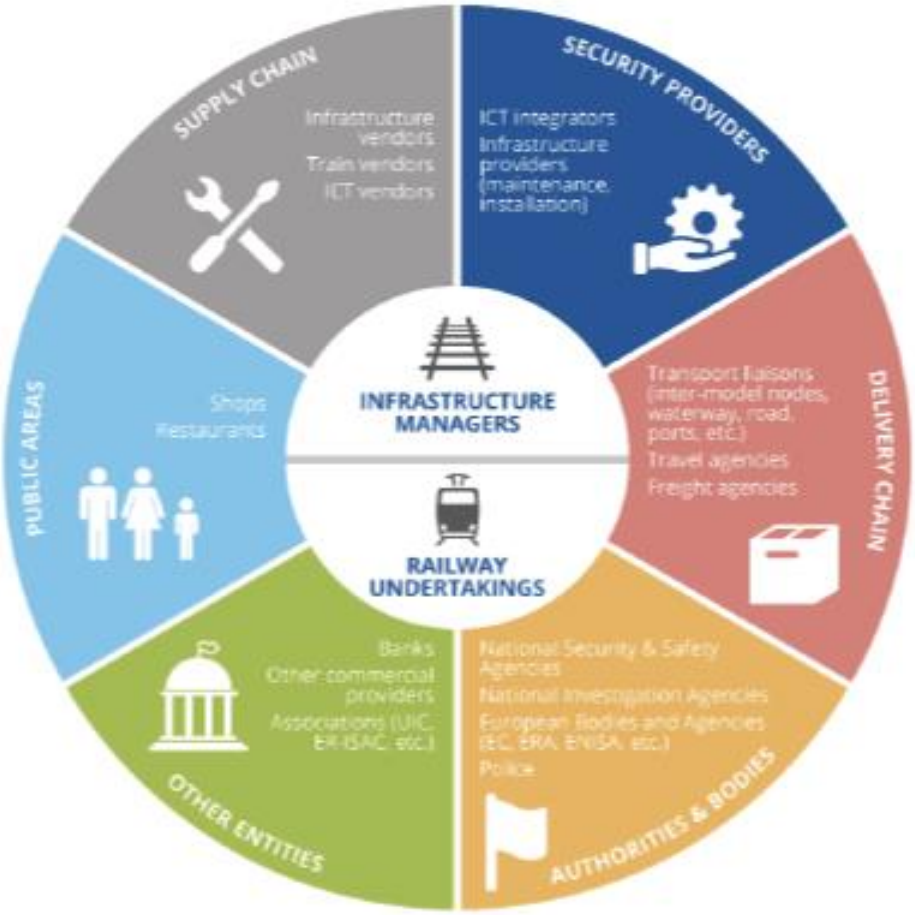
FIGURE 9: DISTRIBUTION OF UNINTENTIONAL INCIDENTS BY EVENT TYPE



3.2.2 Key findings regarding stakeholders

Starting from ENISA mapping of railways stakeholders (see below), and the different parties encountered in the past failures analysed during the review, a typology of the stakeholders which could be involved and/or impacted during an incident targeting both railways and metros, was built.

FIGURE 10: RAILWAY STAKEHOLDER MAP (SOURCE: ENISA)



This typology was used to analyse the different threats but will also be useful further along in the project to identify which stakeholders can benefit from each individual tool and solutions developed in the SAFETY4RAILs project.

Stakeholders types concerned	Description
Infrastructure Manager (IM)	Public or private person or entity owner or responsible for establishing, managing and maintaining infrastructure (traffic management, control & command, signalling) including security department and crisis management personnel
Railway undertaking (RU)	Public or private undertaking which provides services for the transport of goods and/or passengers by rail (railway & metro)
Supply chain stakeholders	Stakeholders providing rail and IT/OT assets to RUs and IMs: vendors of trains, metros, IT systems, etc.
Service providers (third parties)	Third party contracted by RU or IM to perform all or part of a security, business, IT/OT services: advisors, works contractor, consultants, systems providers, integrators, etc.
Delivery chain	Stakeholders involved in delivering the transport service to customers, for freight or passengers
Authorities and bodies	Stakeholders in charge of defining, and applying policies and regulations in the railway sector (security & safety agencies, metropolitean authorities, police, civil protection, first responders, intelligence services)
Public areas	All third parties who use premises to deliver goods and services (on board and in station)
Passengers	Passengers, customers, crowd in and around the stations

The key lessons learnt derived from the past failure analysis regarding stakeholders involved in incident and attacks targeting railways and metros are the challenges posed by:

- The large number of stakeholders to be considered, acknowledging that the majority of them are external to the operator's organisation such as supply chain stakeholders, services providers, passengers, customers and crowd in an around railways and metros ecosystems.

As SAFETY4RAILS has a particular interest in railways and metros environment in multimodal configuration, past failures analysis also highlighted the interdependencies and interconnectivity with other infrastructures (critical or not) such as energy distribution networks, or other transport mode (if the railway or metro station is located at a transport node).

The different roles and attributions of the stakeholders to be considered. The typology of stakeholders encompassed actors which can be either:

- Targets or used as entry point to reach railways and metro assets.
- Direct or indirect victims (collateral damages) of the incident or attacks.
- Key actors or partners to respond, mitigate, or recover from an incident or an attack.

These challenges have to be considered for the S4RIS development and testing.

3.2.3 Key findings regarding assets targeted or impacted

The review of past incidents also allowed for reflection on the assets targeted or impacted during incidents or attacks. This reflection is crucial to be able to identify existing vulnerabilities and derive the related measures which could be implemented to mitigate these vulnerabilities.

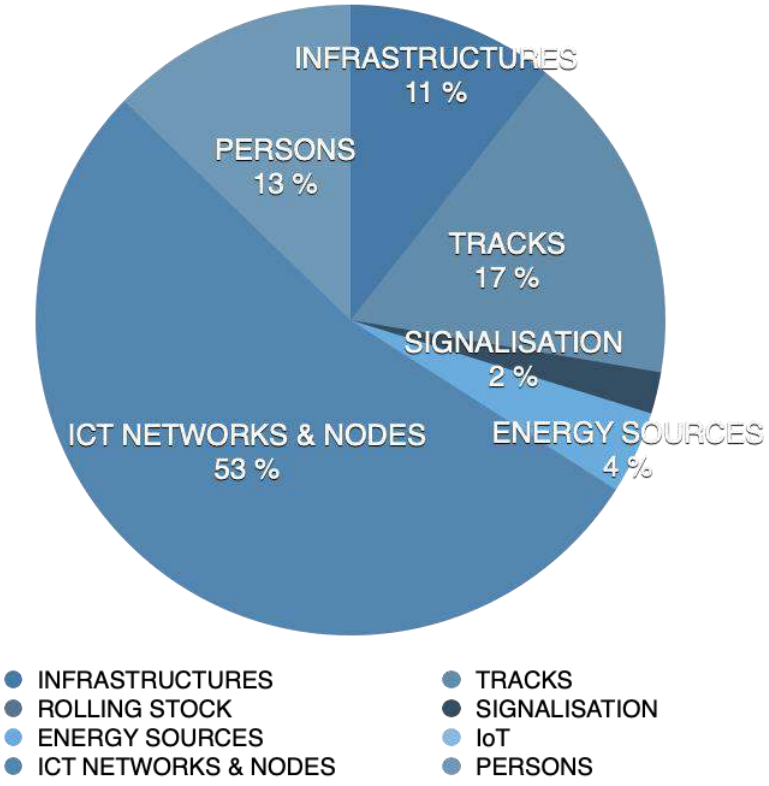
As for the classification of threats and stakeholders, since the scope of the project encompasses both metro and railways environment and large variety of threats, it was decided to build a hybrid classification of assets which was further enriched by end-users during the first End-User Workshop.

Segment impacted or targeted		Description
Railways & Metro	Infrastructures	All the fixed structures, buildings, land, and equipment to support operations and commercial services
	Tracks	Tracks and overhead
	Rolling stock	Vehicles, including both powered and unpowered vehicles
	Signalisation	All signalling systems used to control traffic
	Energy sources	Power stations, transmitters
	IoT	All connected equipments and systems
	ICT networks & nodes	Industry Control Systems, Control & Command systems, support systems, security systems, communication systems, commercial systems
	Persons	Management, security & operational staff, passengers, customers, general public

The analysis of past failures allowed to derive the following lessons learnt:

- **Attacks conducted for criminal motives tends to target ICT networks and infrastructure** rather than persons. This was illustrated in our past incident inventory by the following distribution:

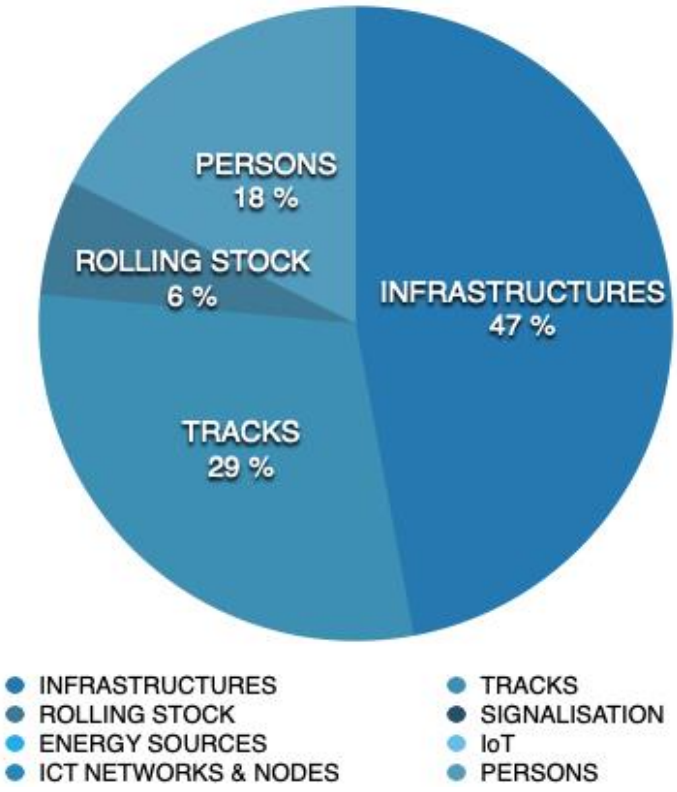
FIGURE 11: SEGMENTS TARGETED BY CRIMINAL THREATS



For assessment of the scale of impact of attacks on citizens, a qualitative analysis of the data sample highlights that since the majority of the criminal attacks targeting persons were cyber-attacks, it follows that personal data breach was involved in the majority of attacks that targeted citizens.

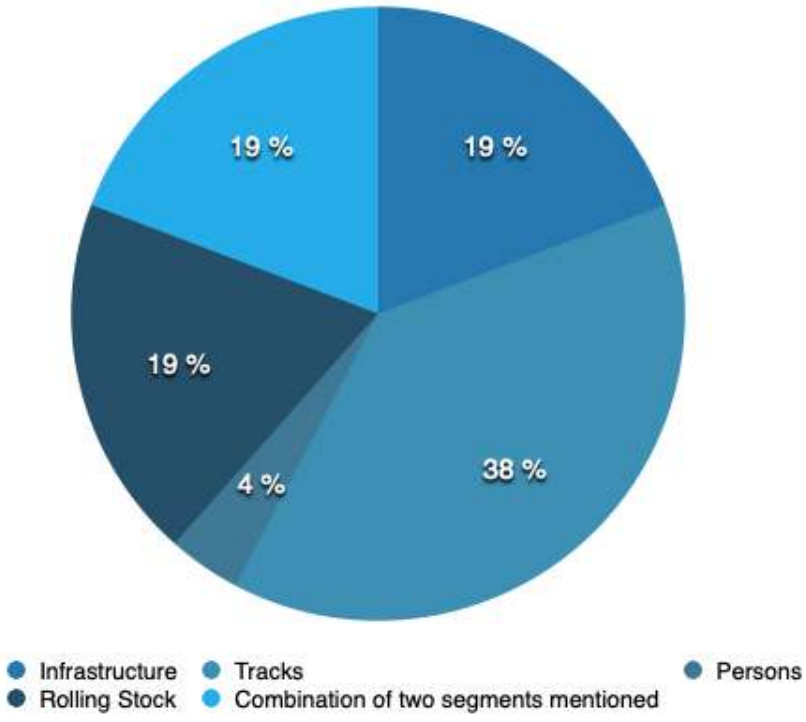
- **Attacks conducted for terrorist motives tend to target infrastructure and persons** rather than ICT, networks and nodes. This was illustrated within our past incident inventory by the following distribution:

FIGURE 12: SEGMENTS TARGETED BY TERRORIST THREATS



- Unintentional incidents (natural and environment disasters) logically mostly impact primary infrastructure. This was illustrated within our past incident inventory by the following distribution:

FIGURE 13: SEGMENTS IMPACTED BY UNINTENTIONAL INCIDENTS



3.3 Key insights from the analysis

3.3.1 Convergence between logical and physical security

Technologies for implementing security services in the physical and in the electronic domain are both stable and mature, but they have been developed independently of each other.

Security Operations Centre (SOC) technology has improved significantly, but SOC solutions have typically been developed using vertical approaches, i.e. based on custom specific needs.

Other key security technologies (such as: Video Surveillance, Forensic support and Building Automation) have also made dramatic improvements, but there is still a limited capability of performing complex correlation on security relevant data. The fragmentation of security approaches is perceived by citizens with confusion, disorientation, and fear. This discomfort is also amplified by the still too high rate of false alarms.

Convergence of security technologies are therefore needed in order to increase control and monitoring functions in infrastructures such as railways and metro stations, where attackers could manipulate either the ICT applications or physical system. In many other environments, convergence of security technologies could be useful for incrementing and/or increasing the infrastructure security and the awareness of security by users. It has been notably observed in literature highlighting those benefits can cover "*reliability, maintainability, operational efficiency, capacity and passenger experience, capacity and passenger experience, as the use of Internet-connected sensors and devices can provide timely and accurate information about the physical world.*"[22].

Security Systems designed to protect Critical Infrastructures have to consider the convergence of physical and logical security, meaning effective cooperation (i.e. a coordinated and results-oriented effort to work together) among previously disjointed functions, which ultimately will result in the achievement of two goals of paramount importance and precisely:

- Guaranteeing the protection of citizens and assets.
- Reducing the perception of fragmentation of security approaches, thus improving citizen's perception of security.

In order for remediation to be effective, the right actions must be taken at the right time meaning Security & Dependability monitoring facilities must be implemented as dependable (i.e. accurate, timely, and trustworthy) functions:

- The availability of Fault and Intrusion Detection and Diagnosis facilities is the precondition for performing appropriate remediation actions.
- Enhanced situation awareness is needed to allow dependable detection and diagnosis of faults and attacks.

Such approach could be summarised in the adoption of an efficient cybersecurity approach including technological solutions designed to ensure safety of both digital and physical elements composing the rail infrastructure. Considering that information and operational digitalised systems rely on physical assets, their protection requires to be developed on both safety risks and security threats assessment.

3.3.2 Interdependencies and cascading effects

One of the main challenges when dealing with threats, whether they are physical, cyber or combined, is to mitigate cascading effects. “A cascading failure occurs when a disruption in one infrastructure causes the failure of a component in a second infrastructure, which subsequently causes a disruption in the second infrastructure.” (Rinaldi, 2001).[23] Railways and metros systems and sub-systems have numerous dependencies with

[22] Ravdeep Kour, Adithya Thaduri and Ramin Karim, Railways Kill Chain to Predict and Detect Cyber-Attacks, 2019.
[23] FP7 PREDICT project, Cascading Effect Joint Final conference, Public report, 2017.

power networks, water distribution, transport or supply chain systems[24] which must be considered in security and safety plans.

Cascading effects represent a domino characteristic of chained events of failure. The size of effects depends on the complexity and the interdependencies of a given system, modelling software that can help analyse the multi-physics behaviour of the complex system. [25] The modelling tool simulates the interdependent infrastructures as a grid network in a form of graphical visualization. The network connections refer to identified (sub)system dependencies (power network, communications, supply chains, etc.), or connections within the same system (i.e. component dependencies).

When failure occurs in one (sub)system or within the same system, its impacts can propagate to another or more (sub)system or components according to its intricate connection. This phenomenon characterises cascading effects. The modelling hence explains to the observer the failure propagation on this multi-domain grid, which can be derived by mathematical methodology based on the probability of individual events.

With a software-based approach, the tool applied[26] numerical and analytical codes to design and optimise the event propagation on the critical infrastructures so that it can investigate the possible consequences after a local disruption and its undesirable behaviour under critical loads. In this method, the software tool supports risk assessment and resilience of the target critical infrastructure. SAFETY4RAILS introduces the software tool 'CaESAR' developed by Fraunhofer for the analysis of the cascading effects. Its methodology and further details will be set out in WP5.

3.3.3 Human factor as the weakest link

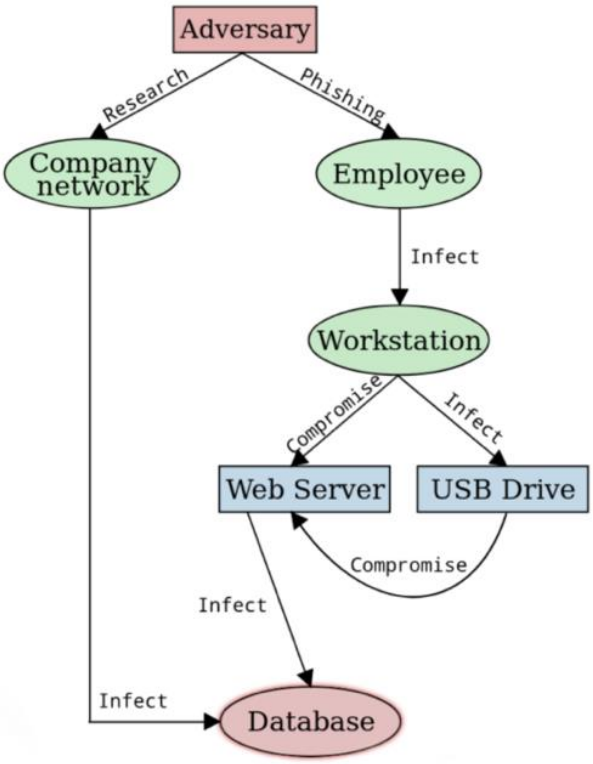
For both physical, cyber, and combined threats, the human factor is often the weakest link in the chain. This is particularly relevant for cyber and combined threats. As highlighted in the analysis of the stakeholders involved or concerned by threats in both railway and metro environments, humans can be intentionally or unintentionally threat agents. The analysis of past cyber incidents has shown that human factor (both railways personnel and passengers) are often unintentionally facilitators of cyber-attacks.[27]

For cyber threats in particular, ENISA publishes on an annual basis a threat landscape which highlights a rise in phishing attacks, enabling criminals to collect the necessary information to hack into staff workstations and from there access to operators' web servers. Access being the key element, making access control security the main challenge to safeguard system safety[28].

« Previous work has considered human error as an intersecting concept between cyber security and safety. Humans may cause harm by making mistakes (active failures) or by inducing errors within systems (latent failures), with human intent as a differentiating factor. If humans are benevolent (unintentional), they may alert the safety engineers by causing hazards and accidents; if malevolent (intentional), they may carry out threats and exploit vulnerabilities that compromise system security, thereby leading to a risk instigating a safety hazard. »[29]

[24] Samane Faramehr, Investigating dependencies between railway systems and other infrastructure systems: using a scenario-based case study approach, 2020.
[25] Hiermaier, S., Hasenstein, S., & Faist, K. (2017). RESILIENCE ENGINEERING-HOW TO HANDLE THE UNEXPECTED.
[26] Ibid.
[27] Amanda Widdowson, Human Factors in Rail Cyber Security, 2019.
[28] Adithya Thaduri, Mustafa Aljumaili, Ravdeep Kour and Ramin Karim; Cybersecurity for EMaintenance in railway infrastructures: risks and consequences, International Journal of System Assurance Engineering and Management, March 2019.
[29] Amna Altaf, Shamal Faily, Huseyin Dogan, Alexios Mylonas: Identifying Safety and Human Factors Issues in Rail Using IRIS and CAIRIS.

FIGURE 14: A POTENTIAL ATTACK GRAPH ILLUSTRATING THE IMPACT OF HUMAN ERROR IN CYBER-ATTACKS (SOURCE: I. BRATOVIĆ, 2019)



If human error and mistakes can lead to unintentional incidents due to a lack of cybersecurity awareness, ENISA research shows that in addition there is also a lack of advanced cybersecurity expertise to deploy protective and defensive security measures, in particular to protect personal data within the railway ecosystem. The fast pace of technology evolution on one side and the constant changes and upgrades in criminals' modus operandi make it very difficult for security operators to implement the adequate protection and defensive security measures at operational level.

ENISA conducted a survey among railways stakeholders within the EU which confirm a limited implementation of both protection and defensive security measures.

FIGURE 15: IMPLEMENTATION LEVEL OF "PROTECTION" SECURITY MEASURES (SOURCE: ENISA)

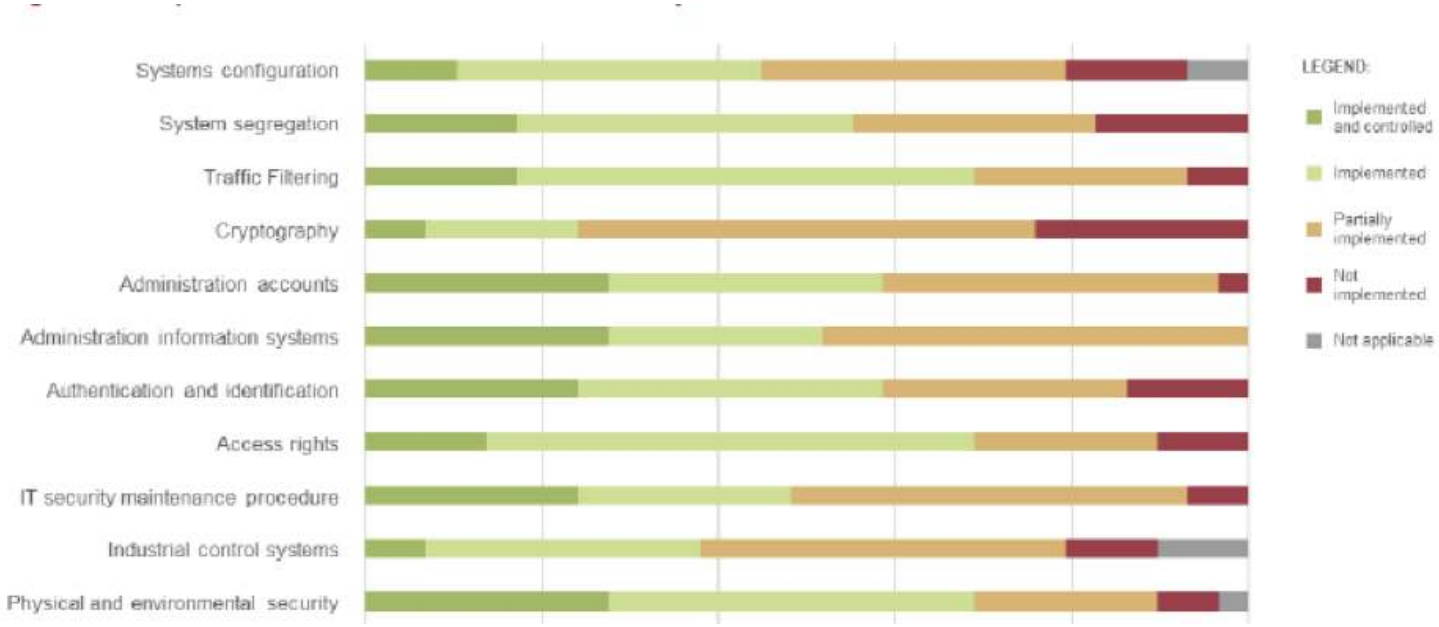
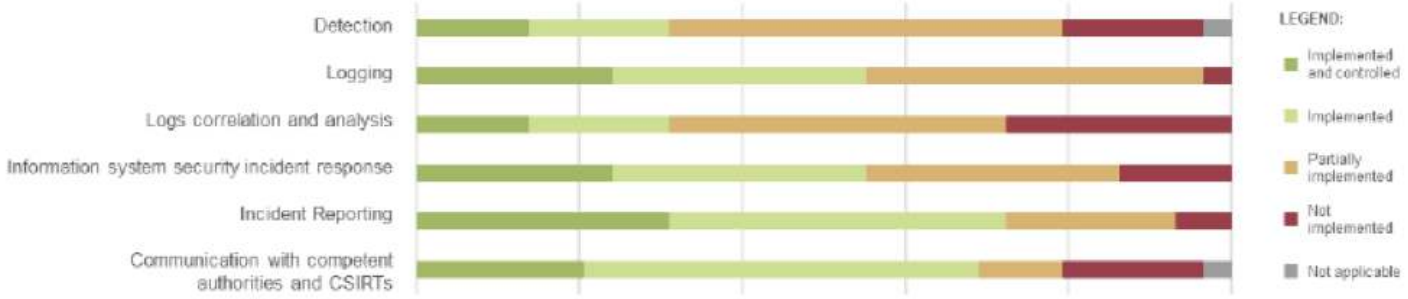


FIGURE 16: IMPLEMENTATION LEVEL OF "DEFENSE" SECURITY MEASURES (SOURCE: ENISA)



3.4 Trend analysis based on news and media

Beyond the above analysis of collected past failures, certain important conclusions can also be drawn from a broader news analysis on the topic of railway infrastructure safety and security. As cyber and cyber-physical threats are an important part of the scope the SAFETY4RAILS project, it should also be mentioned that for cyber-related threats, an in-depth Cyber Threat Intelligence review usually reveals additional insights, beyond the results of a more traditional literature review.

The main results of the trend analysis carried out for the purposes of this document are as follows:

Railway infrastructure is still an attractive target for deliberate attacks. Public transportation in general plays a central role in major cities and intra-city transport, is easily accessible, thus disruptions, even inflicted by only a few individuals, have the possibility of affecting a large number of people and attracting public attention. There are numerous examples of attacks with political and ideological motivation from the past,

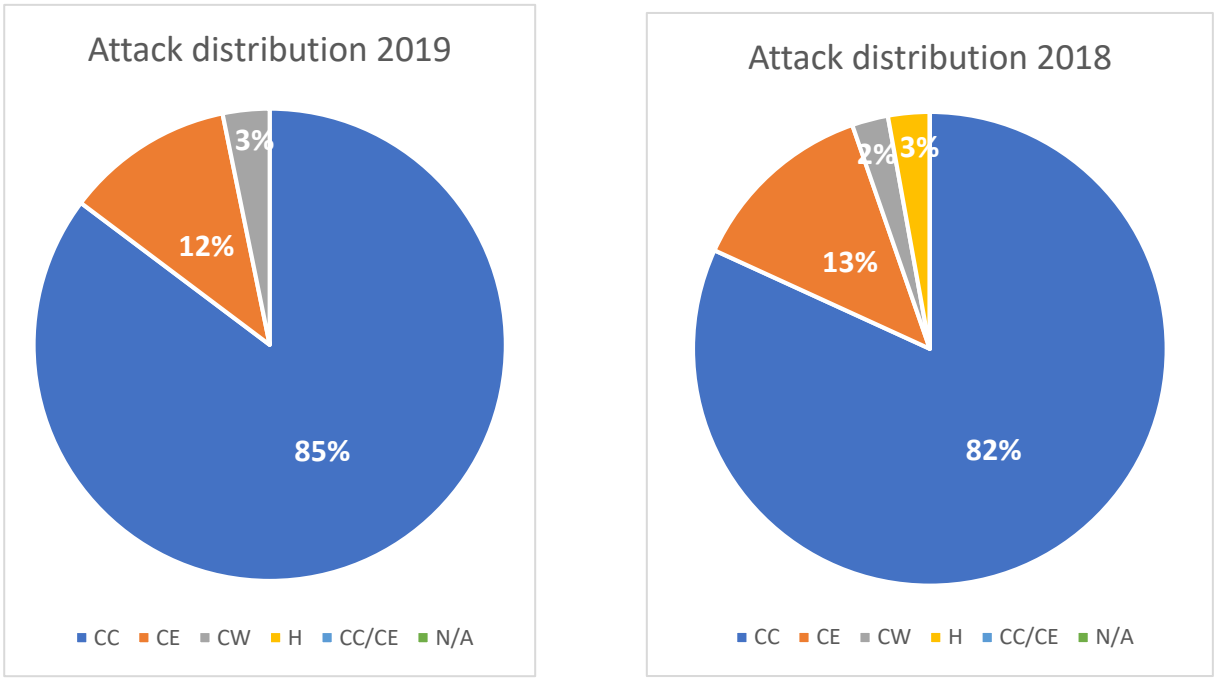
terrorism being a constant threat, as also highlighted by the European Commission (DG MOVE)[30]. However, it is important to note that there is shift in terrorism (especially in Western Europe) from threats based on professional cadres to grassroots operatives. This shift combined with the security enhancements applied following earlier attacks result in slight mitigation of the potential impacts of terrorist related attacks.

Another notable trend connected to the attractiveness of railway transport as a target is the impacts of mass protest activities. The autumn of 2019 saw attacks by demonstrators in 3 major cities worldwide, Hong Kong, Barcelona (Spain) and Santiago (Chile). Since the COVID-pandemic and related societal and economic issues (among other factors) have been causing a rise in the number of representations of social unrest, similar events affecting end-users can also be expected, at least in the following years. An important addition to this threat vector is the fact that hacktivist and state-sponsored groups have been observed coordinating cyber-attacks with physical protests [31].

Similar to other industries, the transport and railway sector has been undergoing rapid digitalisation in the past decades. The increase in the number of IT systems and components used in back-offices, operations and by passengers also brings with it an increase in the cyber-attack surface. Consequently, general trends in cybersecurity will also affect SAFETY4RAILS end-users.

The present trend analysis shows an increase in all types of cyber-attacks, by almost 35% from 2018 to 2019. If we examine the numbers distributed according to attack types, targeted attacks, malware and account hijacking rank highly, both in general and in the transport industry or other critical infrastructure. The distribution according to intentions behind the attacks is shown in the below figures[32].

FIGURE 17: DISTRIBUTION OF CYBERATTACKS ACCORDING TO INTENTIONS, BASED ON NEWS ANALYSIS



As in the case of most critical infrastructure, railway has also seen an **increasing integration of IT and OT systems**. Unfortunately, this results in a higher cybersecurity risk, due to the connectedness of legacy systems

[30] European Commission – DG MOVE, *Improving passenger railway security.*
[31] Ben West, Public transportation threat matrix evolves with geo-political climate, Security Info Watch, 13th December 2019.
[32] Labels used in the figure: CC – Cyber Crime, CE – Cyber Espionage, CW – Cyber warfare, H – Hacktivism.

(which are in many cases highly vulnerable) and the usage of IP-based applications for monitoring and controlling railway systems[33].

According to François Hausman, cyber security WP leader of the Shift2Rail project, cyber-attacks on industrial control systems increased by more than 600% between 2012 and 2014, bringing with them severe financial and safety concerns. Railway specifics, such as electronic components scattered along tracks or trains, a very long life-cycle (in excess of 25 years), diversity both of supply chain and technology and other characteristics make this a complex domain.[34]

In connection with cybersecurity concerns, a final general trend to be highlighted is **the importance of data management and data protection**. While cybercrime is increasingly targeting PII (personally identifiable information) and other sensitive datasets, regulators, especially in the European Union, have created strict requirements for digital data management. This, in turn, means for end-users that a data breach or data theft can be expected to lead to serious legal and economic consequences for the organisation. The most recent and probably largest such case so far has been the ransomware attack against Stadler in May 2020. The full extent of its repercussions is yet to be revealed, but analysis of the already published parts of the stolen data shows sensitive personal, financial and technical information. Beyond the short-term effects (i.e. disruption of operations) of the attack, on the longer run both the acquired user account information and the technical details of products can be used for preparing new cyber-attacks, also against the vendor and customer base of Stadler.[35]

In an article published in 2019, Global Security Analyst Ben West offered a summary of the key takeaways that public transport operators (and, in the case of the SAFETY4RAILS project, railway and metro operators) should draw from the above trends. In his words:

“First, they must understand the political leverage attackers of any motivation can gain by compromising public transportation infrastructure: its openness and criticality make it a soft yet highly impactful target for anybody seeking political or financial concessions. Second, physical security and cooperation with national and international law enforcement and intelligence communities are crucial to preventing transnational or domestic terrorist groups from coordinating another massive attack against public buses, subways, and trains. Third, public transport authorities must have plans in place for how to respond to protest movements that target their infrastructure - even when the underlying grievances have nothing to do with transportation infrastructure. Fourth, and finally, network security and employee digital hygiene is just as important to public transportation as it is to governments and international financial institutions. The fate of millions of commuters can literally hang in the balance of one negligent click on a link.”[36]

[33] White Paper Cyber security for railways, Nokia.
[34] Morand Fachot, Protection railways networks from cyber threats, e-Tech, 15 March 2018.
[35] Rail and Ransomware, Railway News, 3rd November 2020.
[36] Ben West, Public transportation threat matrix evolves with geo-political climate, Security Info Watch, 13th December 2019.

4. Definition of an automated data analysis

Building on the past failure data collected and analysed in this report, as well as the end-user requirements identified within the first phase of the project[37], the S4RIS system will include automated data analysis functions to process real-time data from existing systems and apply AI-based prediction methods for simulation and prevention of severe impacts from potential incidents. A detailed specification of a data analysis method for this purpose requires technical information about the systems, sensors providing input to S4RIS, and also a detailed documentation of the future S4RIS components, containing the acceptable data formats and their processing capabilities.

While such necessary inputs are being collected, this chapter aims to provide an introduction into the process of setting up a defensive AI-based automated data analysis method and optimising a model for railway infrastructure. Based on the information set collected from public sources and analysed in previous chapters of this document, a use-case will also be applied to illustrate the practical application of the proposed method. The actual details of the data analysis method that is to be applied in the S4RIS will be developed in collaboration with other tasks of the project, focusing on the individual components of the system.

4.1 Introduction to AI-based data analytics from a cybersecurity aspect

A system with large amounts of available collectible data, such as in the case of the railway operators, requires a Big Data Cybersecurity Analytic System. This section will introduce the main processes of such a system and the related considerations which are important during the system development. The key processes are:

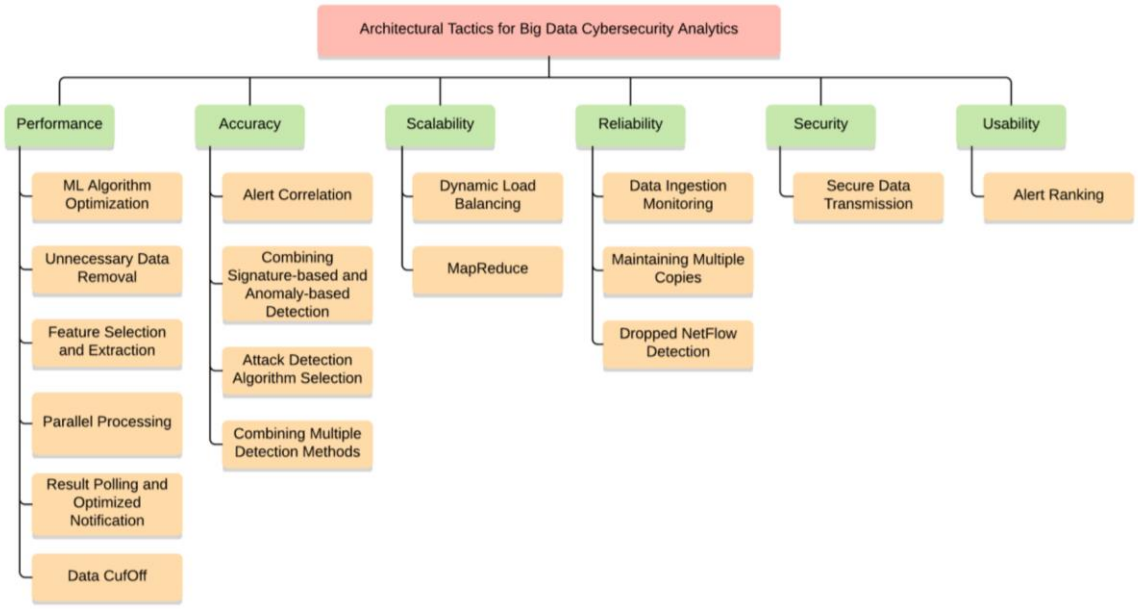
- Data pre-processing
- Classification
- Labelling

A summary of important considerations for designing such systems is provided in Figure 18. The typical way to interpret the method in the figure in the case of SAFETY4RAILS is to imagine that the OT and sensor systems are already connected to the IT infrastructure and the data collection is already set up.

FIGURE 18: ARCHITECTURAL TACTICS FOR BIG DATA CYBERSECURITY ANALYSIS[38]

[37] The combination of these two sources of inputs (e.g., findings from past failures and end-user requirements) allow to balance findings derived from historical data (data collected regarding past failures) and those derived from end-users' perception of current and future threats to infrastructure and passengers safety and security, based on their feedback on initial findings on threats built-on open-sources research on previous railways failures.

[38] The source of figures 19-23 in Chapter 4 is: Faheem Ullaha, Muhammad Ali Babara, Architectural Tactics for Big Data Cybersecurity Analytic Systems: A Review, 2018.

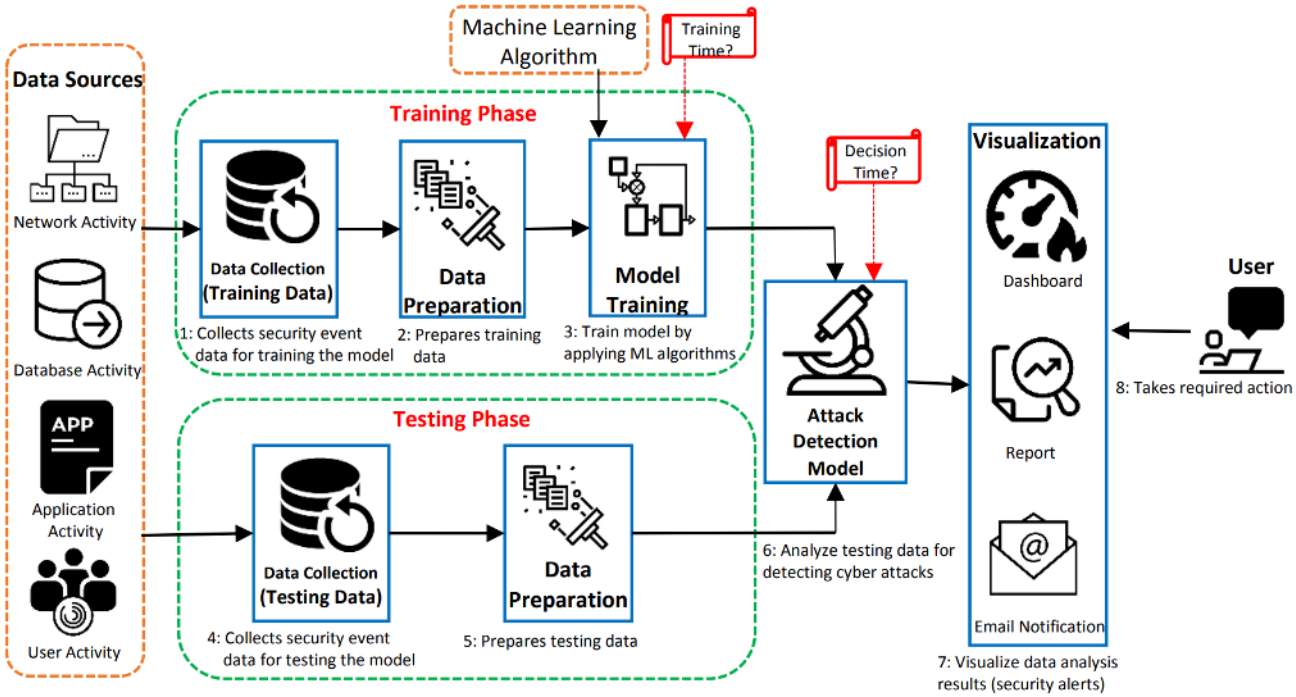


The key factors to be considered from this figure are Performance and Accuracy. The collectible data in the project is expected to come from several different source types and source channels. To generate reliable and usable information for decision makers, the data processing and later data analysis models should be well specified and maintained.

The next important aspect to be considered is the classification method and its flexibility. When examining end-user systems from multiple angles, it should be considered that the combination of smaller events might indicate a larger incident, when examined together (in context) even if individually none of them are considered significant. Therefore, the application of a classification algorithm is recommended (The decision maker can also be another AI system). In this case, accuracy will be ensured by proper classification and the weighing of the different threats to the systems.

Figure 19 below explains an algorithm optimisation strategy of a Security Big Data System.

FIGURE 19: ALGORITHM OPTIMIZATION IN A SECURITY BIG DATA SYSTEM

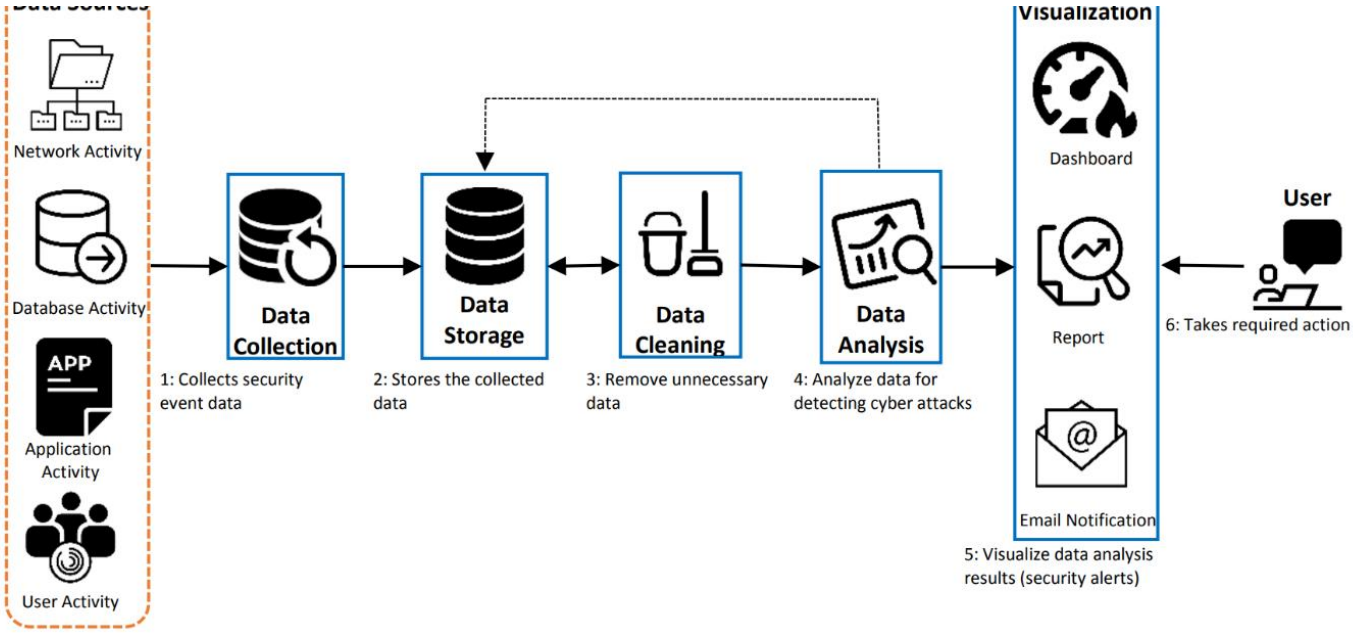


The method presented above illustrates an example of multiple systems analysed in parallel and real-time, where the highest efficiency can be achieved by the best selection of data. The example is similar in complexity to the future S4RIS system but is not an accurate representation of it.

Unwanted data removal and its method can be a key factor in detection and prevention of attacks and incidents since the size of the analysed data affects the processing time and thus also the incident response time.

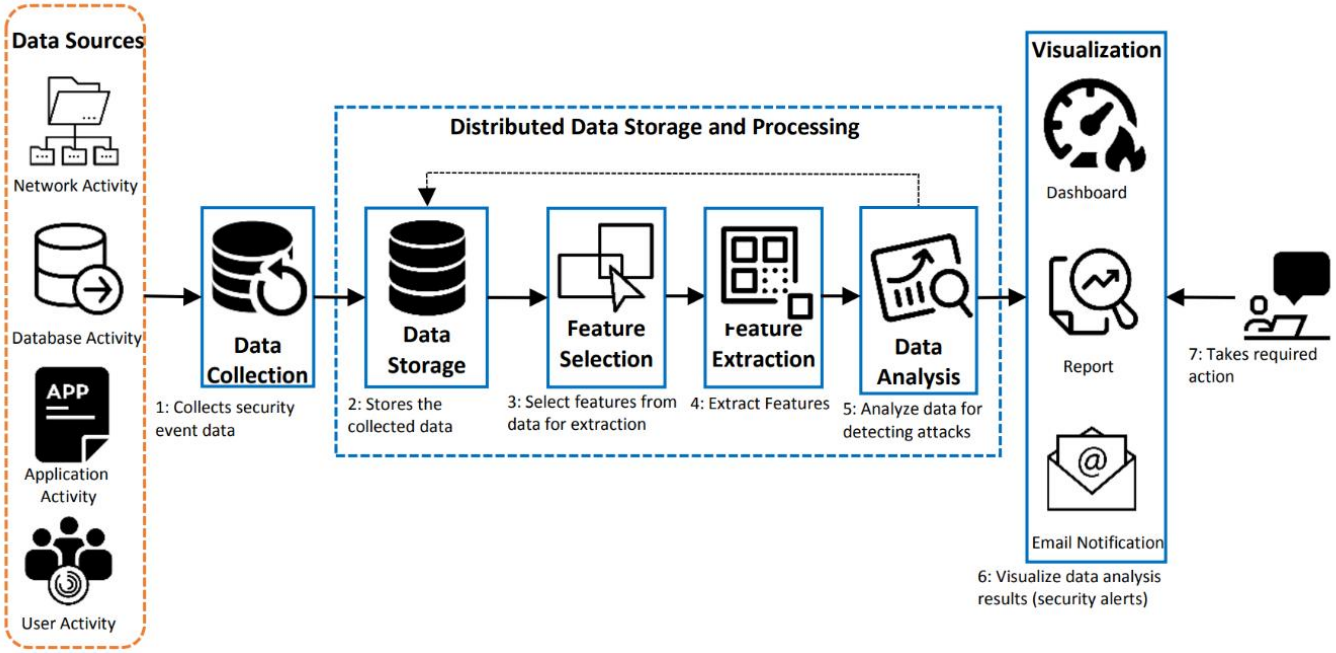
Figure 20 below shows the process of cleaning the data before processing (a phase of data preparation).

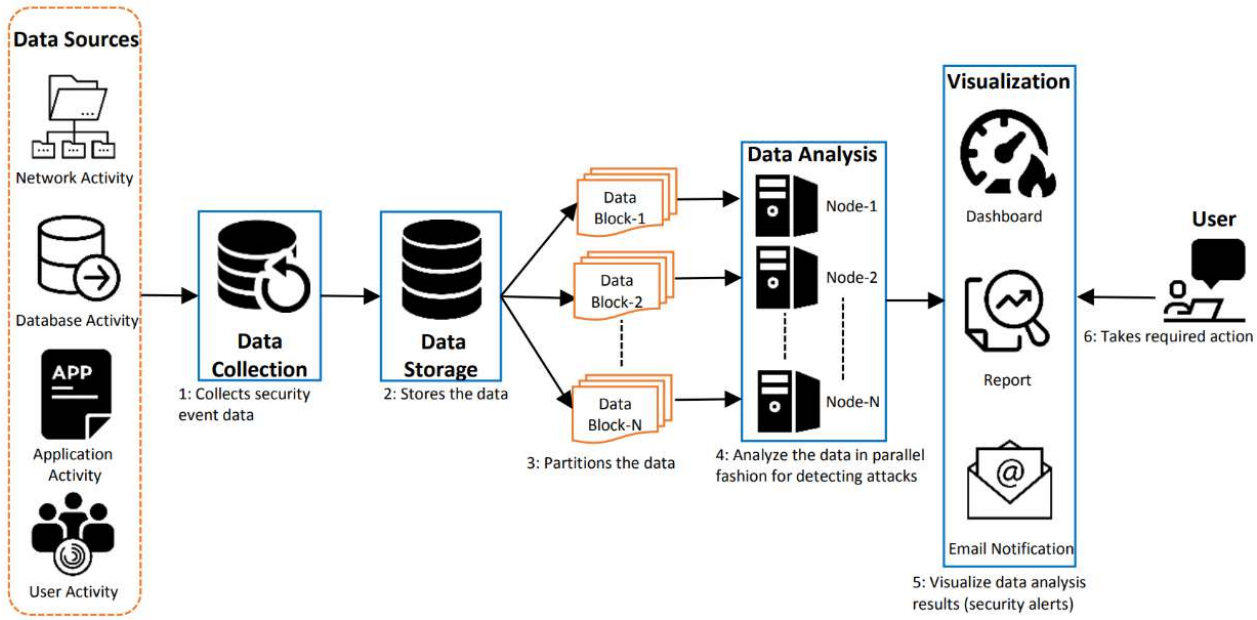
FIGURE 20: DATA CLEANING PROCESS



Based on the resulting classifications, different threats can be monitored from separate systems and the results can be combined later. Therefore, the data distribution method can also affect the efficiency and the processing speed of the system. In Figure 21 below the distribution and extraction model of the collected data is sorted by its features. (In this case these are going to be the labels.)

FIGURE 21: DATA DISTRIBUTION AND EXTRACTION MODEL



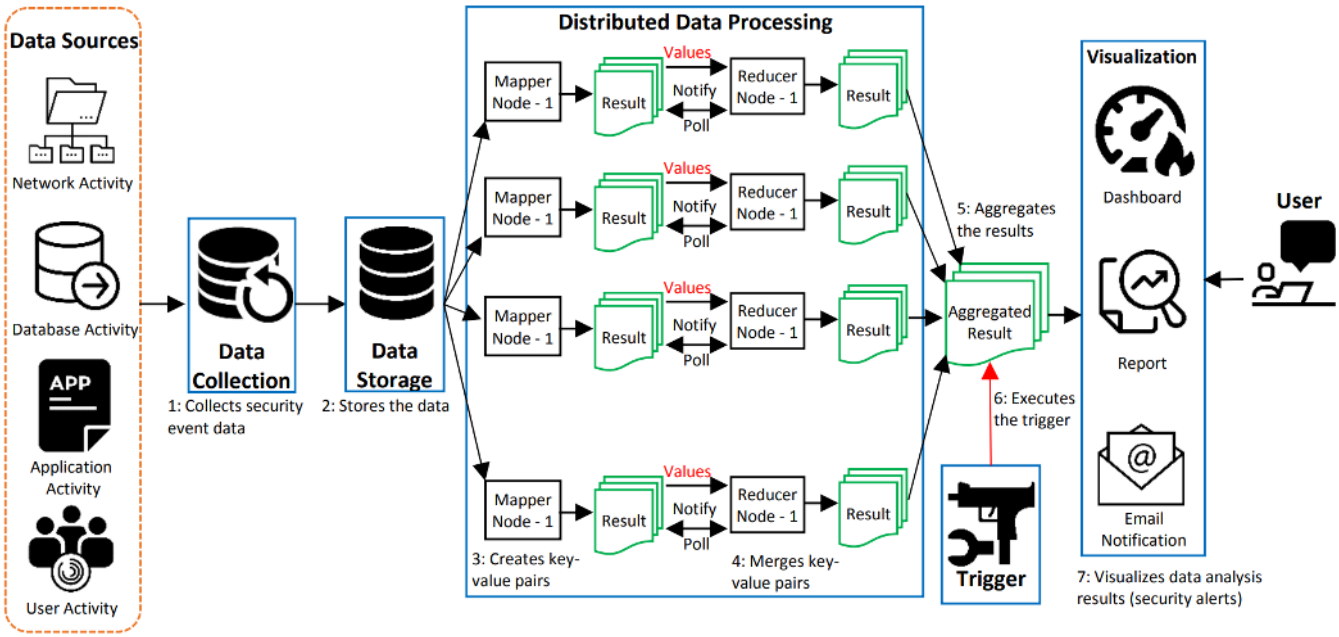


The proper architectural design of the analytics is just as important as the model itself. In Figure 22 below, the parallel process method explains how to accelerate the system and achieve results faster.

FIGURE 22: PARALLEL PROCESS METHOD

Figure 23 explains the Distributed Data Processing of a security big data analytics system. As a next step, from the cleaned and structured data formats, the S4RIS system should be able to generate a model that operates similar to this model, with the difference that the data source is not only network activity.

FIGURE 23: DISTRIBUTED DATA PROCESSING



By following the above steps, the data collected by the SAFETY4RAILS system components can be converted into a data structure that could be processed by a Big Data Cybersecurity Analytic System. This analytic system and its basic functionality should be kept flexible and scalable in terms of size and capacity.

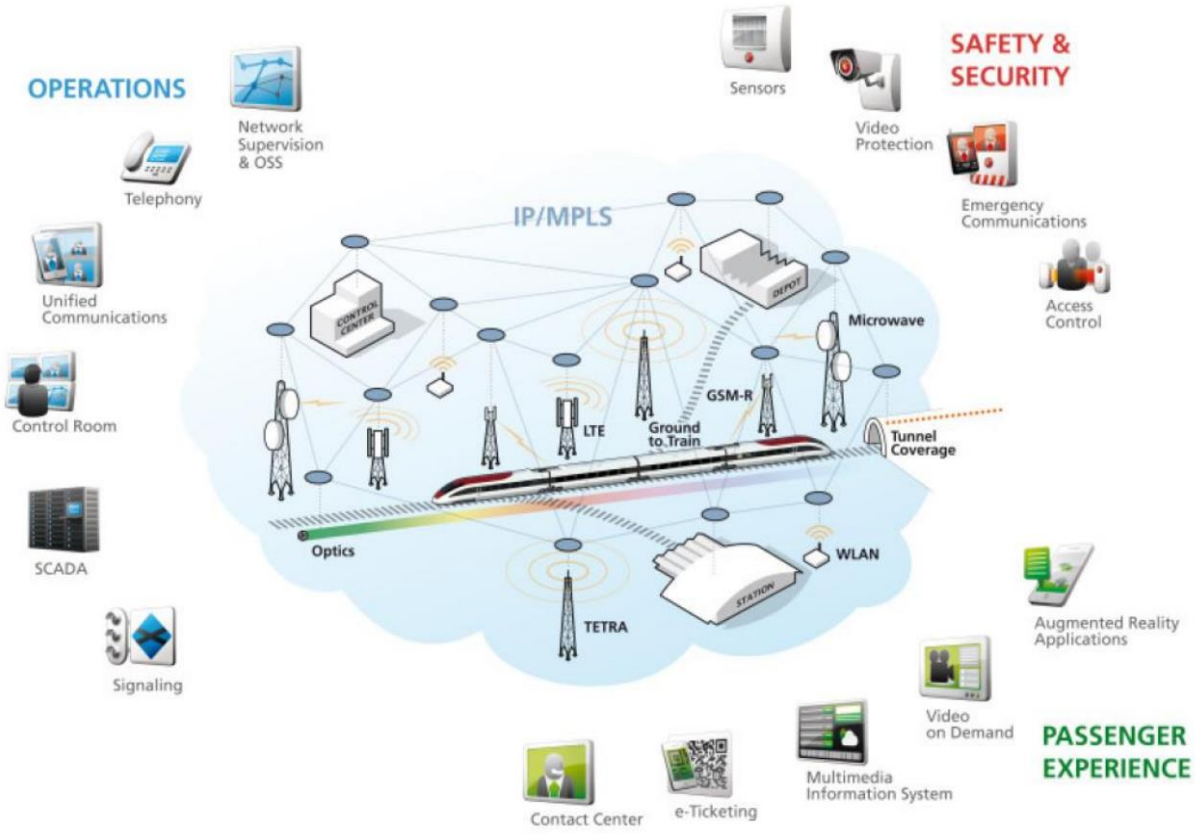
4.2 Modelling

A proper data analysis model for the S4RIS will be built on two key inputs: the data sets and the data classifications. They generate the data labelling and their analysis will result in decision and action. The weighing and scaling of the different data classes and their labels could generate an initial input for a machine learning algorithm to start processing the sample data sets.

Because of the high variety of data types, labelling based on data features might not be enough in the case of the S4RIS tool. The suggested method for the classification -- to support a holistic approach in cybersecurity -- is to accept, in principle, the assumption that all possible incidents that could happen in the analysed system can and most probably will have at least some detectible signs of an incident. Based on machine learning in monitoring systems, certain incidents could even become predictable in the future.

Figure 24 below shows the current infrastructure base of a railway system. As the figure illustrates, there are many data sources to select from and the highest achievable objective should be that the SAFETY4RAILS project analysis model is capable of using all of them.

FIGURE 24: RAILWAY SYSTEM INFRASTRUCTURE



In order to identify the data that can be potentially used, and its sources, it is crucial to categorise and weigh the importance/reliability of the data source and the collected data itself.

4.3 Data type classification example

This section aims to provide a concrete example of data classification based on the review of past failures in the current document. Therefore, the values shown below are hypothetical and are merely used to illustrate the classification process in an environment similar to S4RIS. Once the actual datasets from existing and planned data sources/systems become available, the classification process can be refined and integrated into the final system.

The following table shows the identified data types and the potential source categories used for the purposes of the example. The source categories and data types indicated in the table can be defined as follows:

- Crawled data can be any data from the open internet.
- Measured data is usually the sensor data but in this case, there can be different statistical data as well.
- Calculated data is data input which is generated by the system process with the combination of measured and crawled data, for example weather information from the internet and through the weather and environmental sensors.
- Predicted data can be the source of maintenance information to prevent accidents or any incidents causing business interruption. Predicted data can appear as input and output data as well, therefore it is useful to identify it separately when creating new analysis models.

TABLE 2 : IDENTIFIED DATA TYPES

	Crawled data	Measured data	Calculated data	Predicted data
SOCMINT	1	0	0	0
HUMINT	1	0	0	0
IT System	0	1	1	1
Sensor	1	1	1	0
Equip-ment	0	1	1	0
OT Sys-tem	0	1	1	0
3rd party	1	1	1	1
Internal	0	1	1	1
Serviced	0	1	1	1

Based on the table the weighing of the data sources can be defined. If a social media-based intelligence (SOCMINT) data input is compared with sensor data input, it is clear that these data types originate from very different sources and will have different weights assigned to them in relation to different types of events. For example, sensor data is considered more effective and useful in the case of a gas leak and social media intelligence can be used to monitor and prevent potential terrorist or criminal activities.

A data source can also belong to two or more categories at the same time, as in the case of sensor or equipment data, which can be related to an OT system or an IT system or potentially both.

As a second example for classification, the following table shows the classification for network loss impact.[39] The same kind of classifications should be prepared by the S4RIS system operators to generate further labels. With more potential data connection points (i.e. labels to the same data), the system capability to provide more efficient analysis and output could be increased significantly.

This means that each connected system in the S4RIS tool should have its own data classification which delivers data input to S4RIS. These classifications need to be merged and combined to detect most of the possible incidents. The data should be gathered, selected and cleaned, then it should be converted into a form that can be analysed by the SS4RIS tool (pre-processing). The pre-processed data should then be analysed according to the classifications of each system within S4RIS, both separately and combined.

[39] CYRail project, Recommendations on cybersecurity of rail signalling and communication systems, September 2018.

TABLE 3: CLASSIFICATION FOR NETWORK LOSS IMPACT

Network	Description	Impact loss in human context	Impact loss in financial context	Impacto loss in operational context
Field I/O equipment	To interconnect field elements between them and with the interlocking	High	Medium/High	Medium/High
Interlocking	To interconnect interlockings and RBC between them	Medium/High	High	High
Control center	To connect the interlockings to control centers and control center between them	Low	High	High
Passenger services	Information to passenger services (timetables displays, automated public adress)	Low	Medium	Medium
Freight services	Freight tracking for clients, international handover of freights, ...	Low	Medium/High	Low
Ticketing services	Connecting with travel agencies with reservation systems, connection with accounting, etc	Low	Medium/High	Low
Infra manger intranet	Internal services for infraestructure manager	Low	Medium/Low	Low

4.4 Labelling method example

Following the example of classification, the next step of the analysis process, data labelling, is also illustrated through a similar sample in this section.

The example below shows a potential labelling method with some ideal classes of identifiable scenarios that could be detectable and/or predictable. The columns of the table (1-5) indicate the severity of the incident in the column heading, and the numbers associated with each row indicate whether a weight needs to be associated to the incident with that severity level. It is important to maintain and validate the labelling system and adjust it according to end-user needs. (The threat types and severity values listed in the table are merely used as an example. In a real-life application of labelling, these values need to be defined by relevant experts, in a process that is pre-defined and enables the establishment of objective and repeatable results).

TABLE 4 : POTENTIAL LABELLING METHOD

Threats	Severity scale between 1 and 5
Physical attack (deliberate/ intentional)	different in each scenario
Fraud	5
Sabotage	5
Vandalism	5
Theft (devices, storage media and documents)	5
Information leakage/sharing	5
Unauthorised physical access / Unauthorised entry to premises	5
Coercion, extortion or corruption	5
Damage from the warfare	5
Terrorists attack	5
Unintentional damage / loss of information or IT assets	
Information leakage/sharing due to human error	5

Threats	Severity scale between 1 and 5
Erroneous use or administration of devices and systems	5
Using information from an unreliable source	5
Unintentional change of data in an information system	5
Inadequate design and planning or improperly adaptation	5
Damage caused by a third party	5
Damage resulting from penetration testing	5
Loss of information in the cloud	5
Loss of (integrity of) sensitive information	5
Loss of devices, storage media and documents	5
Destruction of records	5
Disaster (natural, environmental)	
Disaster (natural earthquakes, floods, landslides, tsunamis, heavy rains, heavy snowfalls, heavy winds)	5
Fire	5
Pollution, dust, corrosion	5
Thunder stroke	5
Water	5
Explosion	5
Dangerous radiation leak	5
Unfavourable climatic conditions	5
Major events in the environment	5
Threats from space / Electromagnetic storm	5
Wildlife	5
Failures/ Malfunction	
Failure of devices or systems	5
Failure or disruption of communication links (communication net-works)	5
Failure or disruption of main supply	5
Failure or disruption of service providers (supply chain)	5

Threats	Severity scale between 1 and 5
Malfunction of equipment (devices or systems)	5
Outages	
Loss of resources	5
Absence of personnel	5
Strike	5
Loss of support services	5
Internet outage	5
Network outage	5
Eavesdropping/ Interception/ Hijacking	
War driving	5
Intercepting compromising emissions	5
Interception of information	5
Interfering radiation	5
Replay of messages	5
Network Reconnaissance, Network traffic manipulation and Information gathering	5
Man in the middle/ Session hijacking	5
Nefarious Activity/ Abuse	
Identity theft (Identity Fraud/ Account)	5
Receive of unsolicited E-mail	5
Denial of service	5
Malicious code/ software/ activity	5
Social Engineering	5
Abuse of Information Leakage	5
Generation and use of rogue certificates	5
Manipulation of hardware and software	5
Manipulation of information	5
Misuse of audit tools	5

Threats	Severity scale between 1 and 5
Misuse of information/ information systems (including mobile apps)	5
Unauthorized activities	5
Unauthorized installation of software	5
Compromising confidential information (data breaches)	5
Hoax	5
Remote activity (execution)	5
Targeted attacks (APTs etc.)	5
Failed of business process	5
Brute force	5
Abuse of authorisations	5
Legal	
Violation of laws or regulations / Breach of legislation	5
Failure to meet contractual requirements	5
Unauthorized use of IPR protected resources	5
Abuse of personal data	5
Judiciary decisions/court orders	5

The table above is of course not complete and should be reviewed after the end-user requirements and needs have been collected, to be adjusted to their policies and internal communications.

4.5 Use case example

To show the process of labelling through a real-life use-case, the above sample classification and labelling methods are applied to analyse a news article in this section.

The table below includes the article as an example based on the information found on a news website and it is related to a railway service provider. From the related key words and information, the labelling and the analysis of the severity of the issue results in an output that could support quick decision-making and could trigger an executable mitigation tactic to handle the potential incident.

Article text: The article text itself could be used as an input data. In our example case we will use the case itself.

Article link: [Hackers are holding San Francisco's light-rail system for ransom - The Verge]

'You Hacked, ALL Data Encrypted' By Andrew Liptak@AndrewLiptak Nov 27, 2016, 4:16pm EST

Source San Francisco Examiner

"San Francisco Municipal Railway riders got an unexpected surprise this weekend after the system's computer systems were apparently hacked. According to the San Francisco Examiner, the MUNI system had been attacked on Friday afternoon.

MUNI riders were greeted with printed "Out of Service" and "Metro Free" signs on ticket machines on late on Friday and Saturday. MUNI first became aware of the intrusion on Friday, according to the *Examiner*.

Computer screens at MUNI stations displayed a message: "You Hacked, ALL Data Encrypted. Contact for Key(cryptom27@yandex.com)ID:681 ,Enter." MUNI Spokesman Paul Rose spoke to the Examiner and noted that his agency was "working to resolve the situation," but refused to provide additional details.

Reached by email, the hacker confirmed he was seeking a deal with MUNI to undo the damage:

"we don't attention to interview and propagate news ! our software working completely automatically and we don't have targeted attack to anywhere ! SFMTA network was Very Open and 2000 Server/PC infected by software ! so we are waiting for contact any responsible person in SFMTA but i think they don't want deal ! so we close this email tomorrow!"

In September, Morphus Labs linked a hacker by the same name to a ransomware strain called Mamba, which employs tactics similar to those demonstrated against MUNI."

In the below table the data gathered from the article is labelled according to its informational content.

TABLE 5 : EXAMPLE OF LABELLING METHOD

Threats	Severity scale between 1 and 5
Physical attack (deliberate/ intentional)	different in each scenario
Fraud	5
Sabotage	5
Information leakage/sharing	5
Unintentional damage / loss of information or IT assets	
Disaster (natural, environmental)	
Failures/ Malfunction	

Threats	Severity scale between 1 and 5
Failure of devices or systems	5
Failure or disruption of communication links (communication networks)	5
Failure or disruption of service providers (supply chain)	5
Malfunction of equipment (devices or systems)	5
Outages	
Eavesdropping/ Interception/ Hijacking	
Replay of messages	5
Network Reconnaissance, Network traffic manipulation and Information gathering	5
Man in the middle/ Session hijacking	5
Nefarious Activity/ Abuse	
Receive of unsolicited E-mail	5
Denial of service	5
Malicious code/ software/ activity	5
Social Engineering	5
Abuse of Information Leakage	5
Manipulation of hardware and software	5
Manipulation of information	5
Unauthorised activities	5
Unauthorised installation of software	5
Compromising confidential information (data breaches)	5
Remote activity (execution)	5
Targeted attacks (APTs etc.)	5
Failed of business process	5
Abuse of authorisations	5
Legal	
Violation of laws or regulations / Breach of legislation	5
Abuse of personal data	5

In the case of an automated analysis system, the application of this labelling method would produce at least the following results in our systems' output data (Dashboard):

1) There is an incident going on in connection with the physical infrastructure → Alert message
2) There are multiple failures in the IT and OT infrastructures which caused total halt of the transport operations. → Alert message
3) The failure originated from a cyber-attack which is a ransomware, therefore it is considered as cybercrime. → Alert message
4) Additional information based on facts from the failure detection methods of the OT infrastructure. → This can generate a possible mitigation tactic scenario to be followed by the operational staff.

The information above could be assembled from the labels and weights in the table.

There is a further potential output of the labelling process: In case of personnel or an AI-based text processing robot application processes the selected labels, a fully comprehensible report about the incident in their system can be generated. The labels could also be matched with the mitigation action policies used by the operator and could be used as triggering mechanism or as its supportive element.

The following is an example of a generated report text:

There is a:

Nefarious Activity/ Abuse occurring that includes a part what could be considered as Physical attack (deliberate/ intentional). The potentially used threats that allowed the incident to happen was Eavesdropping/ Interception/ Hijacking. The used threats and their effects are considered as a crime; therefore it has Legal consequences.

A potential action scenario output can also be outlined based on the results:

1) Involve related operation's staff leaders to handle the incident internally.
2) Use cyber incident protocol.
3) Inform police/law enforcement.
4) etc.

The outputs described above are used as examples. The correct output requirements should be generated by the operator (end-user) groups and their policies in combination with legislative requirements according to the legislation of the country where the railway service provider operates.

The importance of these outputs might also be scaled to support the best incident handling method. For example, involving the public relations department might not be relevant if the attacker would not cause any damage that could be easily detected by any user. In the San Francisco case the attacker was obviously looking for public attention. (These types of incidents should be further investigated before PR is getting involved.)

If we use this case as a scenario to explain the modelling of how SAFETY4RAILS should detect this incident, the related systems and potential data sources need to be identified first. Based on this, the system could provide prediction and prevention capabilities for the end-user. For example, in the article other sources may be found related to similar kinds of attacks from the near past. In the case that a Social Media Intelligence module is used, it can search for information on similar past attacks and report findings from Internet sources, then send warning or alert messages to the end-user's IT department.

4.6 Defining the best data analysis method and potential applications

Considering all of the points detailed in this chapter, the potential data analytics model of the SAFETY4RAILS system can be outlined as follows: an AI-based IT network Intrusion Detection / Prevention System (IDS/IPS) is used as a starting point and multiplied as many times as many systems are interconnected, using network-

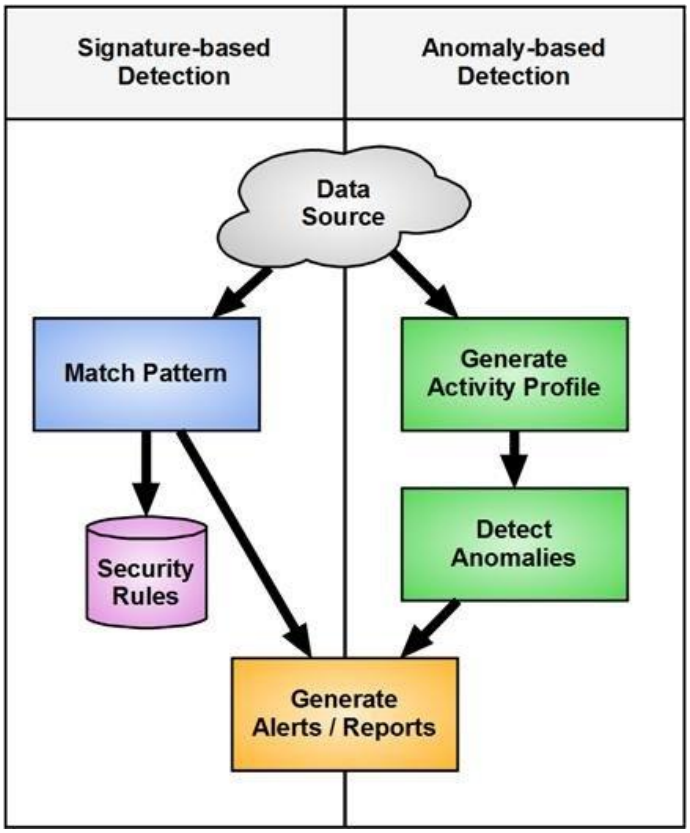
based communication protocols. The input data arriving from each of the source systems is analysed separately and then forwarded to a central data analytics system. This system will provide usable and processable output in correlation with the part of the railway infrastructure operations which was requesting it.

The result of the data analysis should generate a flexible monitoring system which can have multiple output / dashboard forms. This means that the different operational groups can have their own user interfaces where they receive the filtered event messaging results (e.g. a maintenance department is shown different, relevant information than the IT department).

Both signature-based and anomaly detection-based models should be implemented.

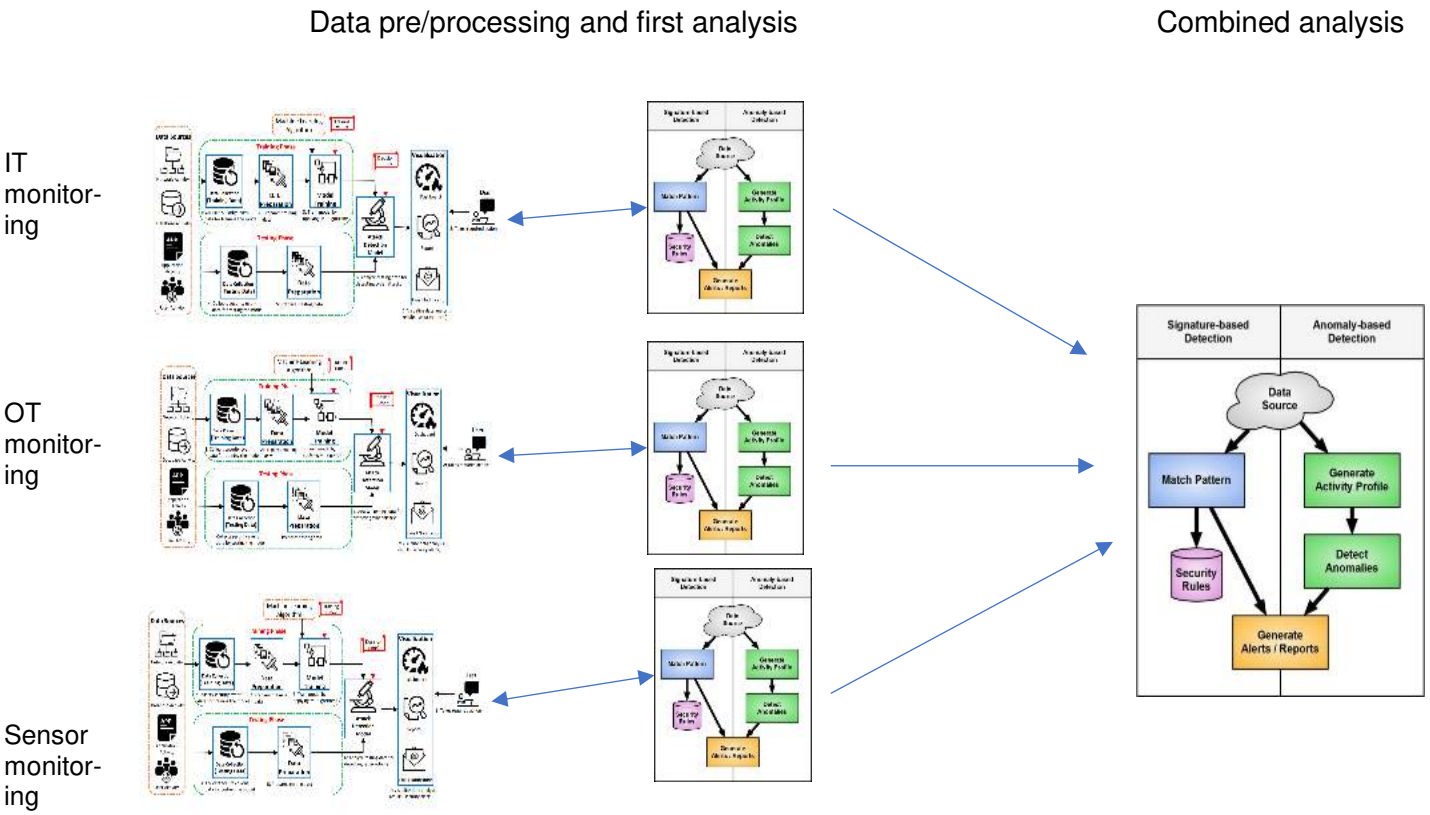
Figure 25 below shows the typical mechanism of the alert report generation in a combined IDS/IPS system. Usually, measured and monitored data sources can provide a higher efficiency for OT and its supportive IT systems, with the signature-based model. Meanwhile, internet-based and end-user related service analysis works better with the anomaly detection model.

FIGURE 25: ALERT REPORT GENERATION IN IDPS



The structure illustrated in the figure is capable of providing a sentiment analysis method within different plotted outputs. This could be applied in the SAFETY4RAILS infrastructure, e.g. for the prediction of a potential vandalism incident, which can come from targeted social media analysis.

FIGURE 26: SIMPLIFIED ARCHITECTURE



The figure above explains the simplified architecture of how the data analysis should operate and feed the decision support system or strategic alert messaging infrastructure. Different systems require different classifications and algorithms to operate properly, therefore each system involved and possibly monitored should be indicated in the figure and should operate with its own properties. The results from each system should be channelled into a more robust AI architecture for further analysis. Of course, each individual monitoring system can and should have a separate output to their own operational staff.

Conclusively, analysing and investigating a sophisticated, combined infrastructure, such as an automated railway security system from the safety and security perspective requires a holistic approach which can expand the potential threat landscape. AI-based analytics can provide the necessary solution and a high value tool to the end-users.

From the Cyber, Physical and Cyber-Physical perspective the following services could be achieved through AI-based data analysis:

4.6.1 Condition monitoring:

Any machine, whether it is a rotating machine (pump, compressor, gas or steam turbine, etc.) or a non-rotating machine (heat exchanger, distillation column, valve, etc.) will eventually reach a point of poor health. That point might not be that of an actual failure or shutdown, but one at which the equipment is no longer acting in its optimal state. This signals that there might be need of some maintenance activity to restore the full operating potential. In simple terms, identifying the “health state” of the equipment is the domain of condition monitoring.

A combination of Principal Component Analysis involving the calculation of Mahalanobis distance to find the datapoints could result into a forecasting model to predict the time of the potential failure caused by a combination of different equipment used in the system.

This kind of prediction model requires sensor data and a data set of the normal condition to train the machine learning algorithm.

4.6.2 Real-time threat detection:

The variety of log files in an infrastructure such as a railway service provider company is very high. The combination and the analysis of different selected log data together could indicate future threats by providing valid data about the potential vulnerabilities, weaknesses of the used systems from both a cyber and physical perspective. Several different AI based anomaly detection models are available in IDS and IDPS systems. The combination of physical sensor systems log data with the IT and other log data from operations could generate a real-time threat/incident detection system. Using an Artificial Neural Network model could also provide prediction in the case that the log data is combined with open source or serviced Cyber Threat Intelligence data.

Another potential application of the log analysis could be the evaluation of discovering shadow IT in the systems in use. Shadow IT is one of the highest potential threats since it generally does not require significant financing and the knowledge base to build shadow IT devices is openly available on the Internet. Some of the systems are not hidden from civilians and some could also interact with the end-users. All systems that are physically accessible to customers, partners, suppliers etc. are potential attack points for shadow IT elements, should it be a USB, Ethernet or any other communication ports or even wireless communication platforms.

4.6.3 Sentiment Analysis:

The importance of sentiment analysis in supporting the safety and security of railway infrastructure and railway operations should not be underestimated. It is an effective tool for predicting potential threats and incidents if the right data input source is selected. These could include open-source platforms such as websites of law enforcement services and social media networks. Adding more location based social media and internet content to a text mining application and analysing them together with the openly available CTI data could give indicative results. Their main use could be in indicating the potential risk of terror or criminal activities especially vandalism and physical crime related threats.

Communication is paramount to handling incidents, especially those with cascading effects, which have a dedicated focus within the SAFETY4RAILS project. A sentiment analysis tool could also help the communication of the end-user towards the customers / passengers and could prevent (some of) the cascading effects.

4.6.4 Image analysis:

CCTV / IP based camera systems and AI-based detection models are widely used together globally, for example in traffic signs detection, speed measurement, size measurement, face recognition, symbols detection, language detection, device detection, behaviour and body language detection, thermal image analysis to provide environmental measurements. Image analysis can provide many potential ways to be used for threat detection. The combination of the processed images with the other safety and operations related data could provide better safety and security. The example below explains one scenario for preventing crime and accidents. In the example the focus is on how to use a camera system to detect and validate the internal workflow of the daily maintenance staff.

In a platform maintenance scenario, each metro station is cleaned twice a day. The cleaning personnel uses a company-issued uniform with a QR code printed on the back and front, including the key to their personal info in the company HR database. The HR database contains the information of the schedule of the personnel. While a person is working on the platform, the camera system can match the QR code and face of the personnel with the one stored in the database. This method could be extended with recognition of the tools used, for example signs to be used to prevent accidents, such as the wet floor sign. At the same time, it can be used to prevent criminal activity – ensuring that only the individuals according the schedule are present for the cleaning activity and are not bringing suspicious objects to the platforms. Of course, the (ethical) implications of using AI-based methods for potential face recognition would need to be thoroughly examined.

4.7 Conclusions

The already vast amount of available data related to railway infrastructure and operations is expected to constantly increase in the future. Operators should therefore consider data as an important resource and identify the best methods to utilise it for keeping railways safe and secure from future and yet unknown threats. Most of the existing AI and Machine Learning models could be applied for this purpose but choosing the proper ones is highly dependent on knowing the existing systems and their capabilities. In addition to this, sourcing the

required data processing while constantly adding more data and more models connected to each other is a difficult and currently quite resource-intensive task. These aspects should be specifically considered for the S4RIS system and support the implementation of the right data analysis methods. For the best achievable efficiency, the operators should apply strict policies with reliable asset management.

The basics of future safety and security should be driven by humans but providing more and better processed information to the decision-makers is already possible based on big data analysis. It is also true that to make the data easily and quickly understandable, the analytic systems should be adjusted and visualised according to the operators' needs and industrial requirements. Adopting the upcoming technologies and open-source information will also be crucial for the data models to be applied.

5. Preliminary operational requirements for S4RIS

5.1 Case Studies

As part of the research process to derive operational requirements for S4RIS, three use-cases where selected encompassing several parameters of real past failures.

5.1.1 Method to select use-cases

- Use-case 1: a use-case covering an incident or attack that end-users are very likely to encounter and which can have major effects on services and business activities
- Use-case 2: a use-case covering an incident or attack that is rarer but results in severe casualties and has an important impact on public opinion
- **Use-case 3:** a use-case covering an incident that **may happen in the future** (prospective) **more often** and could have **major impacts**

FIGURE 27: USE-CASES

5.1.2 Case 1: Cyberattack – Ransomware

As ransomware is the one of the most recurrent cyber-attack used by criminals lately (high likelihood), and that the past incident review provided many illustrations on these attacks targeting railways and metros stakeholders, it was seen as an interesting case study to identify end-users specific needs to deal with this category of threat and derive the operational requirements.

In addition to the likelihood aspect, this particular threat often targets a very sensitive asset, namely passengers and customers personnel data, and can have an important impact on companies' reputations. It was seen as a representative use-case for cyber threat.

5.1.3 Case 2: Physical attack – Terrorist (explosive device and shooting with cascading effects)

Though less likely to be encountered, the past incident analysis showed that the prevention and response to physical terrorist attacks remains a major concern for all critical infrastructure and for railways and metros operators in particular, as serious attacks took place in these environments in the past 15 years.

The critical impact of these type of threat, both in terms of casualties and damages to infrastructure, combined with the effect on public opinion, make a physical terrorist attack a representative use-case, especially if cascading effects are included.

5.1.4 Case 3: Combined cyber – physical attack – Data Breach

As better prevention and response to combined cyber-physical attacks is one of the key objectives of the SAFETY4RAILS project, the third use-case focuses on a threat scenario that is likely to happen more often in the future, as technology evolves. For this specific use-case, it was interesting not only to have a threat scenario with combined effects (impact on both physical and digital assets) but also for which the threat agent or vector is dual, namely, a physical access to an asset to launch a cyber-attack.

These three use-cases have been presented to end-users and to members of the Advisory Board to collect their needs based on the current procedures, processes and tools in place in their organisation.

The results of this activity will be presented during the next end-user workshop and associated deliverable.

Bearing in mind that S4RIS aims at providing a combination of tools and systems to support the risk and threat management cycles within railways and metros stakeholder's organisations, the past incident review enabled the derivation of some preliminary operation requirements to be considered in the design and testing of the information system.

5.2 SAFETY4RAILS Risk and Threat Management cycle

Derivation of operational requirements from past failures enabled the compilation of a common typology of the different actions implemented by security and safety railways and metro stakeholders to face threats.

As each entity relies on its own risk and threat management cycle, it was decided to use the following cycle of actions within the SAFETY4RAILS project which is applicable to both railways and metros. This cycle was used as a baseline to research information on the different measures.

Risk & Threats management cycle		
	Domains of actions	**Definition**
Risk Management cycle	**Forecast**	Estimate what events are likely top happen in the future
	Prevent	Stop the happening of a event or the actions of people
	Detect	Detect earlier, or at the right time, abnormal behaviors or events
Threat (or crisis) Management cycle	**Respond & Mitigate**	To reduce the impact, severity of the crisis
	Recover	Restore the right functioning
	RETEX Return of Experience	Establish best practices, learn from previous experiences & update methodolgies, approaches or process

As the review focused on past incidents, the core research focused on security measures implemented for three specific phases of the cycle: the detection phase, the mitigation phase and the recovery phase.

The draft version presented during the end-user first workshop included only the « Domains of actions » column. In order to provide an improved and more detailed understanding, end-users suggested the addition of the first level of entry by listing which domains of actions are related to risk management cycle and which are related to threat or crisis management cycle. This comment was considered as valuable to the SAFETY4RAILS framework, which looks at both cycles.

5.3 Preliminary operational needs expressed by end-users

Railway and Metro companies have well established accident response arrangements to deal with the immediate need to ensure safety then mitigation, recovery, post incident review and identify corrective actions. This is generally applied at Strategic (offsite), Tactical (on site) and Operational (on and off site) and normally managed as far as rail is concerned by the Innovation Manager (IM) who coordinates other rail responders such as train operators.

Strategic decision-makers, as the name implies, decide the strategic priorities and liaise with external responders at strategic level to seek a coordinated strategic approach. They will also consider the media relations and business continuity issues involved.

Tactical responder on site (IM Lead) coordinates the rail responders on site to achieve the strategic aims also liaises with the other organisations responding e.g. police, health & safety and rail accident investigators who will have their own legal responsibilities and priorities. Good site liaison is essential with regular liaison meetings on site.

Operational responder, both on and off site, supports the Tactical response needs with the necessary personnel, equipment etc.

Debriefs are held during or after recovery in which facts and necessary follow-up actions are determined.

Clearly this approach has to be flexible to meet the type and degree of the scenario faced. If the situation involves a terrorist attack the police lead may well dictate what/when the IM does in terms of any physical recovery. With a cyber issue there may or may not be an 'accident' to deal with and the circumstances may be dealt with at a strategic level only.

Bearing in mind that with some potential terrorist actions e.g. where there is an increased background threat level then counter measures may be decided and instituted before an incident occurs. Where a real-time threat warning is received this will be dealt with by the police and the IM/train operators on the basis of a documented system requiring rapid response.

Acknowledging the specificities of these response arrangements to support End-Users, the objective of the SAFETY4RAILS is to identify within the Risk and Threat management cycles specific needs that they may have for enhancing each domain of actions.

To achieve this a preliminary exchange was conducted with end-users internal to the consortium to gather their preliminary and most pressing needs which can be summarised as follows:

	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 such effects
	Detect	**Improve the detection of weak signals** for early alerting of 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 responses accordingly
	Recover	**Methodologies for managing cyber-physical events** and foster the recovery
	RETEX	**Lessons learnt from cyber-physical events** to update procedures, approaches and tools

5.4 Requirements - key findings by type of threats

Starting from the common understanding of the threats faced by railways and metros stakeholders (section 3), an analysis of the risk and threat management cycles, the collection of end-users' needs (above sub-sections), preliminary requirements were derived from past failures and organised around the risk and threat management cycle, according to the type of threat encountered, namely physical, cyber or combined.

For each threat, the key lessons learnt from past incidents were displayed and related operational requirements indicated. The list of requirements was not meant to be exhaustive but rather to highlight the main ones to initiate a discussion with end-users during the first End-User Workshop and collect more operational inputs.

The result of this activity is presented below.

- **Initial key findings derived from past failures analysis**

Effects	Lessons learnt	Main Operational Requirements
Physical Effects	**Interdependencies of systems** lead to cascading effects on external environnement components	• Conduct **mapping of systems** interdependencies • Develop **simulation to identify vulnerabilities** and implement corrective measures • **Adapt facilities and fitting designs** to mitigate cascading effects • Develop **collaboration procedures** with external parties linked to systems
	Physical threats targeting tracks or external systems and infrastructures (tunnel, etc.) are **very challenging** (distance and difficulty to access)	• Deploy **real-time monitoring systems** and **remote track monitoring systems** • Use of « **sweeper trains/metros** » prior to the start of a service day • Put in place **sub-service communications equipment** capable of allowing rescue teams to maintain contact with victims
	Complex identification of high risk profiles and suspect goods and/or luggages in multimodal environments	• Design or **modernise railway and metro environment** to reduce hiding places for both human and goods • Deploy **threat intelligence tools, smart sensors**, but also **security or law enforcement staff**
	Very complex early detection of insider threat (important number of stakeholders involved)	• Conduct both initial **vetting (pre-employment screening) and ongoing care and review processes** on the various staff and stakeholders involved (including suppliers)

- **Initial key findings derived from past failures analysis**

Effects	Essential Services impacted	Lessons learnt	Operational requirements
Cyber Effects	Railway/Metro infrastructure management	**Low cybersecurity awareness** and cultural differences	• Conduct **continuous training & awareness raising**, in particular on phishing and authentification process
		Cyberattacks are mostly **targeting operators servers and work stations**	• Use **encryption and secure authentification processes** as much as possible and deploy firewall
		IoT technologies expand the **surface of exposure**	• Implement **cybersecurity standards for IoT** before deployment
		Lifecycle of physical infrastructure, OT and IT are not aligned, making update and maintenance difficult	• Implement automated **IT & OT monitoring, supervision and administration systems.** • Safety and cybersecurity requirements by design for OT systems
	Railway/Metro services	Operators **website**, ticket **vending machines** and **ATM** are effective **entry points** for cyberattackers	• Deploy **automated response solutions** that can respond to threats before they become breaches
			• Install **automatic software updates** when possible
		Passengers personnel data are the most interesting asset to target for criminals	• Use **encryption and secure authentification processes** as much as possible

- **Initial key findings derived from past failures analysis**

Effects	Lessons learnt	Operational requirements
Cyber-Physical Combined Effects	**Physical access to ICT systems** represents the biggest backdoor for attackers	• **Ensure limited access** to areas containing sensitive information or equipment • **Establish well-communicated procedures** for the physical protection of assets • Implement **multi-factor authentication processes**
	Human is generally the weakest link in the kill chain (lack of awareness, risky behavior)	• Conduct **continuous training & awareness raising activities**
	Lifecycle of physical infrastructure, OT and IT are not aligned, making update and maintenance difficult	• Implement automated **IT & OT monitoring, supervision and administration systems** • **Safety and cybersecurity requirements** by design for OT systems
	Lack of **adapted security procedures & processes for combined threats**	• Develop **flexible operational security & safety guidelines** to fit the specificities of railway and metro environments

These preliminary requirements have been evaluated as relevant by end-users during the first end-user workshops, who made some fruitful remarks to refine these requirements.

- The deployment of IoT, smart sensors and surveillance technologies is often to ensure the security of physical access to sensitive assets. Though reducing the surface of exposure to physical threats, at the same time can induce an increase of the surface of exposure to cyber threats. Thus, there is a need, should an organisation decide to deploy such technologies, to ensure that those solutions are as secured as possible by design, and that associated cyber vulnerabilities are considered by security operators.
- The implementation of automated IT and OT monitoring, supervision and maintenance systems, though particularly relevant, can be very difficult to enforce at operational level because of the interdependencies between systems.

These preliminary requirements will be further refined to be fed into the development of the S4RIS within the other activities of WP2.

6. Conclusion

The analysis of past failures is an important first step towards defining the requirements of the future S4RIS system. The analysis will help to avoid the reproduction of known events, already experienced by railways and metro sectors, by being better prepared to face them.

The past failure analysis allowed to build a series of key elements:

- A typology covering incidents targeting or impacting both railways and metro that would be considered in the scope of the S4RIS system.
- A typology of stakeholders involved or concerned by incidents targeting or impacting both railways and metro.
- A classification of the segments and assets targeted or impacted during both railways and metro incidents.

Each element will be used to build a final grid analysis or threats and risks that will be validated during the 2nd End-users' workshop. This grid analysis will ensure the added-value & interoperability of the S4R Information System for end-users by addressing their needs and requirements.

Furthermore, the classification grid of incidents allowed to derive, and extract lessons learnt from the commonalities and discrepancies between the past incidents. The key trends and insights drawn from the reviewed cases are:

- A rise in the proportion of cyber-attacks amongst the incidents, especially those with criminal motivation.
- The railway and metro sector experience the same increasing convergence between logical and physical security, that is observed in other OT-related environments.
- The nature of the systems applied in the sector and the typical incidents will require a special attention towards interdependencies and cascading effects.
- From a security aspect, the human factor, due to a lack of awareness, is the weakest link and related requirements need to be defined within the project.

Based on the analysis of past failures and current and future railway infrastructure components, automated data analysis methods need to be incorporated into the S4RIS development. For the application of AI-based and Machine Learning algorithms to process the vast amount of data arriving from different sources, the existing systems and their capabilities need to be identified and thoroughly analysed. The currently available technologies in data analysis offer a wide range of application options within the rail and metro sector, but their costs/resource requirements should also be considered.

Finally, the report identified a first set of operational requirements for the S4RIS. Initially these were defined based on the results of the analysis, but consultations with end-users and experts helped refine the list. These initial operational requirements will support the definition of more detailed requirements and connected specifications, which are amongst the next expected outcomes of the SAFETY4RAILS project.

7. Bibliography

Main sources consulted

Adithya Thaduri, Mustafa Aljumaili, Ravdeep Kour and Ramin Karim; *Cybersecurity for Maintenance in railway infrastructures: risks and consequences*, International Journal of System Assurance Engineering and Management, March 2019.

Amanda Widdowson, Human Factors in Rail Cyber Security, 2019.

Amna Altaf, Shamal Faily, Huseyin Dogan, Alexios Mylonas: *Identifying Safety and Human Factors Issues in Rail Using IRIS and CAIRIS*, February 2020.

Badii A, Fuschi D, Khan A, Adetoye A. *Accessibility-by-Design: A framework for delivery-context-aware personalised media content re-purposing*, Proceedings of the Symposium of the Austrian HCI and Usability Engineering Group, 2009.

Ben West, *Public transportation threat matrix evolves with geo-political climate*, securityinfowatch.com 2019 - Public transportation threat matrix evolves with geo-political climate | Security Info Watch, last accessed on 18.12.2020.

Bratović I, Simulation of red teaming in cybersecurity (English title), University of Zagreb.

CYRail project, Recommendations on cybersecurity of rail signalling and communication systems, September 2018 CYRail Recommendations on cybersecurity of rail signalling and communication systems, September 2018, last accessed on 18.12.2020.

European Cyber Security Organisation (ECS), Transportation Sector Report - Cyber security for road, rail, air, and sea, WG3 I Sectoral Demand, March 2020.

Emma Megan, Why is cyber-security so important for the rail industry?, Global Railway Review, 31 January 2019.

ENISA, ENISA Threat landscape 2015, January 2016.

ENISA, Railway cybersecurity: Security measures in the Railway Transport Sector, November 2020.

European Commission, *SAFETY4RAILS Grant Agreement*, version 1.0, dated 21 April 2020.

European Commission – DG MOVE, *Improving passenger railway security*, last consultation December 2020 https://ec.europa.eu/transport/modes/rail/consultations/improving-passenger-railway-security_sk?2nd-language=ro

European Railway Agency, Guidance on the decision to investigate accidents and incidents, Articles 3(l), 19 and 21(6), March 2011.

European Union Agency for Railways, *Rail Accident Investigation*, consulted in December 2020 https://www.era.europa.eu/activities/rail-accident-investigation_en

Eurostat Statistics Explained, *Passenger transport statistics,* consulted in December 2020 - https://ec.europa.eu/eurostat/statistics-explained/index.php/Passenger_transport_statistics#Rail_passengers

Eurostat Statistics Explained, *Railway freight transport statistics,* consulted in December 2020 https://ec.europa.eu/eurostat/statistics-explained/index.php/Railway_freight_transport_statistics

Faheem Ullaha, Muhammad Ali Babara, Architectural Tactics for Big Data Cybersecurity Analytic Systems: A Review, 2018.

FP7 PREDICT project, Cascading Effect Joint Final conference, Public report, 2017.

Hiermaier, S., Hasenstein, S., & Faist, K., Resilience Engineering-How To Handle The Unexpected, 2017.

ISO 7498-2:1989(fr), Systèmes de traitement de l'information — Interconnexion de systèmes ouverts — Modèle de référence de base — Partie 2: Architecture de sécurité.

ISO/IEC 27005:2018, Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information.

Mouna Rekik, Christophe Gransart, Marion Berbineau. Cyber-physical Threats and Vulnerabilities Analysis for Train Control and Monitoring Systems. IEEE ISNCC 2018, International Symposium on Networks, Computers and Communications, Jun 2018, Rome, Italy. 6p. hal-01852042.

Morand Fachot, *Protecting railway networks from cyber threats*, etech.iec.ch 2018 – https://etech.iec.ch/issue/2018-02/protecting-railway-networks-from-cyber-threats, last accessed on 18.12.202.0

NOKIA White paper, Cyber security for railways, 2017.

Railway-News, Why I Think Ransomware Is a Major Danger to the Rail Industry, 3 November 2020.

Ravdeep Kour Adithya Thaduri and Ramin Karim, Railways Kill Chain to Predict and Detect Cyber-Attacks, 2019.

Samane Faramehr, Investigating dependencies between railway systems and other infrastructure systems: using a scenario-based case study approach, 2020 https://discovery.ucl.ac.uk/id/eprint/10098193/1/Samane-FaramehrThesis.pdf

Steer Davies Gleave /DG MOVE, Report on options for the security of European high-speed and international rail services, Final Report, December 2016.

Vegard Flovik, *How to use machine learning for anomaly detection and condition monitoring*, towardsdatascience.com, 2018 – https://towardsdatascience.com/how-to-use-machine-learning-for-anomaly-detection-and-condition-monitoring-6742f82900d7, last accessed on 18.12.2020

Wikipedia, STRIDE (security model), last consultation December 2020.

ANNEXES

7.1 ANNEX I. INVENTORY - RAW DATA ANALYSED

Annex 1 data is based on open-source information, yet would be a useful collation of tactics with indication of potential impact for would be attackers. On this basis, the Annex 1 was declared confidential.

7.2 ANNEX II. LIST OF ABBREVIATIONS

TABLE 6 : LIST OF ABBREVIATIONS

Term	Definition/description
AL	Activity leader
AB	Advisory Board
AP	Action point
AI	Artificial Intelligence
CO	Confidential
D	Deliverable
DC	Data controller
DDoS	Distributed Denial-of-Service
DM	Dissemination manager
DMS	Document Management System
DoA	Description of the Action (Annex 1 to the Grant Agreement)
EB	Ethical Board
EC	European Commission
EM	Ethics manager
ENISA	European Union Agency for Cybersecurity
EUB	End-user Board
EUC	End-users coordinator
EXM	Exploitation manager
HUMINT	Human intelligence (intelligence gathering)
IDS/IPS	Intrusion Detection / Prevention System
IM	Innovation manager
IPR	Intellectual Property Rights
OSINT	Open-Source Intelligence
ML	Machine Learning
MIN	Minutes

Term	Definition/description
PC	Project coordinator
PGA	Project General Assembly
PMT	Project Management Team
PR	Partner representatives
QM	Quality manager
SAB	Security Advisory Board
SM	Standardisation manager
SOCMINT	Social media intelligence
SR	Semestral report
S4RIS	SAFETY4RAILS Information System
TL	Task leader
TM	Technical manager
ToC	Table of Contents
TRL	Technology Readiness Level
WP	Work package
WPL	Work package leader

SAFETY4RAILS

Partners:

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

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