- FORESEE -

Future proofing strategies FOr RESilient transport networks against Extreme Events

– Deliverable 6.6 –

SP Case Study #5 Madrid Calle30 Ring Road

Project reference no.	769373
Deliverable no:	6.6
Work Package no:	6
Status	Final Version
Version:	12
Author:	FERR (David Fernández Haro)
Date:	22/03/2022
Nature:	Demonstrator
Dissemination level:	Public

	Participant Legal Name	Country
1	FUNDACION TECNALIA RESEARCH & INNOVATION (TEC)	Spain
2	RINA CONSULTING SPA (RINA-C)	Italy
3	FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V. (FRAUNHOFER)	Germany
4	UNIVERSIDAD DE CANTABRIA (UC)	Spain
5	FUTURE ANALYTICS CONSULTING LIMITED (FAC)	Ireland
6	FERROVIAL AGROMAN SA (FERR)	Spain
7	UNIVERSITY OF BATH (BATH)	United Kingdom
8	CENTRO DE ESTUDIOS DE MATERIALES Y CONTROL DE OBRA SA (CEMOSA)	Spain
9	LOUIS BERGER SPAIN SA (LB)	Spain
10	INGENIERÍA Y CONSERVACIÓN CONTRAINCENDIOS, S.L. (ICC)	Spain
11	INFRAESTRUTURAS DE PORTUGAL SA (IP)	Portugal
12	AISCAT SERVIZI SRL (AIS)	Italy
13	Autostrade per l'Italia S.p.A. (ASPI)	Italy
14	EUROPEAN UNION ROAD FEDERATION (ERF)	Belgium
15	EIDGENOESSISCHE TECHNISCHE HOCHSCHULE ZUERICH (ETH Zürich)	Switzerland
16	TELESPAZIO VEGA UK LIMITED (TVUK)	United Kingdom
17	THE UNIVERSITY OF EDINBURGH (UEDIN)	United Kingdom
18	Ingenieurgesellschaft für Verkehrs- und Eisenbahnwesen mbH (IVE)	Germany

Authors list		
Reviewer: Name, surname	Organisation	email
David Fernández Haro,	Ferrovial **FERR**	d.fernandezharo@ferrovial.com
Jaime Martín Alfageme	Ferrovial **FERR**	jmalfageme@ferrovial.com
Pablo Sánchez Gómez	Ferrovial **FERR**	p.sanchezgomez@ferrovial.com
Manuel del Jesus Peñil	Universidad de Cantabria **UC**	manuel.deljesus@unican.es
Salvador Navas Fernández	Universidad de Cantabria **UC**	salvador.navas@unican.es
David Zamora Martínez	Tecasem	dzamora@tecasem.com
Juan Zamorano Martín	Tecasem	juanzamoranomartin@gmail.com

Reviewers list		
Reviewer: Name, surname	Organisation	email
David Fernández	FERROVIAL **FERR**	d.fernandezharo@ferrovial.com
Iñaki Beltran Hernando	TECNALIA **TEC**	inaki.beltran@tecnalia.com

Document History			
Version	**Date**	**Comments**	**Author**
01	25/09/2021	Draft 1	David Fernández Haro
02	30/09/2021	Draft 2	David Fernández Haro
03	06/10/2021	Draft 3	David Fernández Haro
04	07/10/2021	Draft 4	David Fernández Haro
05	25/10/2021	Draft 5	David Fernández Haro
06	27/10/2021	Draft 6	David Fernández Haro
07	03/11/2021	Draft 7	David Fernández Haro
08	22/11/2021	Draft 8	David Fernández Haro
09	24/11/2021	Draft 9	David Fernández Haro
10	30/11/2021	Draft 10	David Fernández Haro
11	15/12/2021	Draft 10	David Fernández Haro
12	20/02/2022	Draft 11	Tobias Hanel
13	15/03/2022	Final version	Tobias Hanel

TABLE OF CONTENTS

TABLE OF TABLES

TABLE OF FIGURES

1 INTRODUCTION

This deliverable will consist in the test and validation (in the Madrid Calle30 Ring Road, Spain) of the FORESEE project outcomes in order to select and design the best technical solutions for preventive maintenance to plan future maintenance, continency and emergency interventions and to set up of procedures for events management (Task 6.2)[1].

2 CASE STUDY #5 DESCRIPTION

2.1. DESCRIPTION OF THE INFRASTRUCTURE

Madrid Calle 30 Ring Road is the most important and the busiest road infrastructure in Spain. 1.5 million vehicles per day use (part of) the Calle 30, of which 200,000 vehicles per day make a "full" journey that covers the use of all tunnels (48 km in total).

Tunnel sections mostly have two or more lanes. Heavy vehicles are not allowed, with the exception of buses, and, likewise, dangerous goods traffic is prohibited. During peak hours, the traffic load can exceed 200,000 vehicles per day.

There is a main Control Centre, as well as the possibility of managing the infrastructure from a secondary Traffic Control Centre, in case of emergency. This secondary centre does not have the operational management capacity of the main Control Centre, among other reasons because it has only one permanent operator, until the Emergency Plan is activated.

There is also a First Intervention Team, with similar equipment as the public fire brigade, that is mobilised in the first part of the event. The team will control the event until the arrival of the external public emergency response services, to whom they will report and continue their intervention as auxiliaries, since the responsibility for emergency management falls on the Fire Services of the Madrid City Council. The First Intervention Team received dedicated education and training, adapted to their tasks.

The Main Control Centre is managed by a team, consisting of at least three operators, one supervisor, and one operation manager.

The rest of the organisation is related to the Maintenance and Conservation services, which are under the responsibility of an Operation Manager, who reports to the Authorities, in this case the Madrid City Council.

The availability for traffic of Calle 30 is critical, since closure of the road would have a major impact. Not only on Madrid, the capital of Spain, but also on a national level. Such a closure could paralyze and at least collapse road communications "transports of people and goods", and could generate great economic and social damage. So it is adequate to qualify the road as strategic and of vital importance.

The applied tunnel regulations are related to the European regulations for tunnel safety, and included in the Spanish Standard R.D. 635/2006. Although not all requirements are mandatory,

[1] GRANT AGREEMENT NUMBER — 769373 — FORESEE

there is a commitment to fully comply with this standard, since it represents the highest safety level.

Another standard that is applied, R.D. 393/2007, aims to assure Civil Protection, and includes requirements for self-protection measures, provisions in relation to critical infrastructures, as well as regulations applicable to Traffic and Road Safety.

2.2. DESCRIPTION OF THE HAZARD AND MAIN CONCLUSION OBTAINED IN PREVIOUS DOCUMENTS

2.2.1. MAN-MADE EVENT: CYBERATTACK

The "hacking hazard" or cyberattack is a relatively new anthropogenic hazard to be considered in transport infrastructure. The term describes a wide range of security hazards that are generated by humans and can directly or indirectly affect the infrastructure's operational, economic and safety parameters. Whether they attack the transport modes, the transport network, the traffic flow control, revenue, management or communications systems, they can directly affect public safety and critical operations, as well as the infrastructure operation and organization.

Hacking events are very different and broad in nature. They use a wide variety of tools and methods to gain control or have an impact on the normal functionality of their electronically controlled targets. The tools range from deceiving applications, logic bombs, botnets, trojan apps, viruses, worms, keyloggers and specialized toolkits, while the methods vary from brute force, DOS (Denegation of Service), to social engineering such as phishing, crypto-ransomware, CEO fraud or more recently by tricking machine-learning systems into misinterpreting traffic signals on autonomous vehicles. These methods and tools are challenged by the Intelligent Transport System (ITS) defense mechanisms, the security culture and the network control procedures that are in place. Best management practices against cyberattack incidents involve an organized Security Operations Center as well as their technological infrastructure and tools to defend and protect the infrastructure (firewalls, white/blacklists, antivirus, Honeypots, intrusion detection and prevention systems, etc.).

Regardless of the objective of the attacks (ransom, sabotage, theft), when these overcome the security measures that are in place, the potential consequences range from a purposed malfunction of specific systems, to disruption of the network control center, resulting in loss of partial or complete control and visibility of operating systems, rendering the operation unsafe, and - in the worst case - causing direct or indirect fatalities. Hacking hazards against transport infrastructures are not common. However, the higher complexity of the transportation systems, the higher degree of digitization and the elevated level of interconnectivity lead in a correspondingly higher fragility and vulnerability of the transport system against cyberattack.

It is important to know that Madrid Calle 30 Ring Road has not only tunnels, also has connection galleries with the exterior, connections with other infrastructures and emergency galleries. Having one Main Control Centre, means that happening a serious damage at one point of Madrid Calle 30 Ring Road will affect in one way or another on the rest of the connected parts.

Important to note that there has not been any cyberattack event on the M-30 during the whole life of the infrastructure management. However, this kind of events are getting more popular, and we consider of a vital importance to take them into account. This infrastructure is one of the most

important ones in Spain, thus having this new anthropogenic hazard into consideration is one of the main outputs coming from the present study.

The following list describes the scenarios that we consider possible to happen. First scenarios on the list have more serious consequences:

- Is it proven that the emergency is caused by a cyber-attack?

- Does the Control Centre maintain full or partial management capacity?

- Is the cyber-attack only limited to the Control Centre's ability to operate?

- Does the cyber-attack allow the intruder to maliciously operate the management systems?

The scenario that we consider most serious in terms of its negative effects is the one in which the intruder manages to maliciously operate the management systems.

The purpose is to describe the scope of a cyber-attack on Madrid Calle 30's control equipment, its effects on traffic management and security, including the possible effects on the infrastructure, listing and describing those elements that are considered critical, defining the meaning of critical, and the capacity to maintain or not the service in the circumstance of the degraded system or systems.

The tunnel safety control system shall monitor a series of installations, equipment and elements, without the proper level of monitoring it will be impossible to guarantee the minimum level of safety required to maintain operation. These are the critical elements or systems.

The systems which we consider to be critical are listed below in order of importance:

- Tunnel closing system
- External and internal power supply.
- Ventilation System.
- Equipment for fire control.
- Lighting system.
- Signalling system.
- Video Automatic Incident Detection (VAID)
- SOS system.
- Systems for analysis and control of environmental factors.
- Evacuation management systems.
- Communications equipment.

Each of the invalidated or maliciously managed systems will require a response from the Control Centre, and the degraded service situation generated by the simultaneous failure must trigger systematic response and decision making for security.

In order to focus on the outcome of a cyber-attack and its consequences, we have defined two categories that can summarise its classification:

a) Routine: They get access, without the ability to operate on the Control Centre.

b) Extreme: They get access and operate on the system.

According to the recommendations provided in the Foresee Project, which is specified the resilience of Calle 30 in a cyber-attack event, the study parameters have been defined and the procedures for a systematic response and implementation of measures to minimise the consequences of an attack on Calle 30's installations and management equipment, following the methodology whose final result coincides with the objectives listed below:

- Preventive measures against a cyber-attack event.

- Analysis of the resilience capacity of the installations and equipment managed by the Calle 30 Control Centre.

- Description of possible scenarios.

- Definition of applicable systems to mitigate the effects of a cyber-attack.

- Approval and inclusion of the system in accordance with current regulations.

- Implementation of the approved measures.

- The procedure for the quantification of values and measures will be that defined in the Foresee Project.

- The data used come from the official reports of Calle 30, collected in its Operation Report, Audits and Quality System.

All of the above has shaped the work carried out and reflected in the documentation contained in this report.

2.2.2. FLOODING

Floods are a global problem and are considered the most frequent natural disaster worldwide. They may result into serious socio-economic impacts, causing loss of lives, population displacement, business bankruptcy. As part of the future proofing strategies For RESilient transport networks against Extreme Events (FORESEE) program, the Environmental and Hydraulics Institute "IH Cantabria" come up with a novel methodology for improving the estimation of return periods of flooding events. This innovative procedure aims to provide a better understanding of the true magnitude of disruptive flood events.

With the aid of Calle 30 and Ferrovial Construction, the methodology has been applied to the M-30 motorway in Madrid (Spain) to check its response against low frequency events at two specific locations along the Manzanares River - i. Upstream of "Puente de Toledo" and ii. Upstream of Dam Nº9.

All the work developed has been included in a following chapter in the present report.

2.2.3. FIRE

Another hazard that has been analyzed and studied for the M-30 Ring Road case scenario is the fire. Some fire dynamic simulations that are explained in the deliverable D7.4 have been performed in this pilot.

Characteristics of design fires

Input parameters and fire development phases
The basis of the design fire scenarios are the design fires, which are described by certain variables that are used for a quantitative analysis of the scenario. These variables include the rate of heat release or the rate of toxic gas generation as a function of time.

Input features
Each fire scenario represents a particular situation of specific physical events combined with a particular set of active and passive protective measures. As a consequence, a fire scenario is representing a unique combination of factors such as:

- type, size and location of ignition source,
- distribution and type of fuel
- fuel load density
- type of fire
- fire growth rate
- fire's peak heat release rate g) tunnel ventilation system
- external environment conditions
- fire suppression
- human intervention(s)

A full specification of a design fire scenario may include the following phases:

- incipient phase – characterised by a variety of fire sources, such as smouldering or flaming fire

- growth phase – covering time of fire propagation up to flashover or full fuel involvement
- fully developed phase – characterised by a substantially steady burning rate as may occur in ventilation or fuel controlled fire
- decay phase – covering the period of declining fire severity
- extinction – when there is no more energy being produced.

All the work developed for this particular hazard will be explained later in this report as part of the summary of the updates from the contingency plans included in the deliverable D7.4.

3 SCENARIO CARD & VALIDATION CONDITIONS

3.1 Scenario card for CASE STUDY#5 MADRID CALLE 30 RING ROAD

As the M30 ring road is an existing route, corresponding to the life cycle (LC) of the operating and maintenance phase - in relation of the management and contingency plans, is considered in the following.

Three different scenarios for three different hazards have been studied specifically in the section of the tunnels that are located in the southwest part of the M30 ring road.

Criticalities:

1. Man-made events including cyberattack (to the ITS, particularly in the tunnel section), intentional or not intentional - like accidents (average number of 14 interventions/day due to accidents) or fire after accidents.

2. Flooding and other extreme events derived from raining in the valley (in several sections of the open air section of the ring road) and the proximity of the river (tunnels in the west side) interaction with other infrastructures and buildings, and the influence of the water level in the tunnels located at the west side.

3. Fire inside the tunnels, taking into consideration a dynamic approach for the contingency and emergency plans.

The disruptions in the M-30 cause delays, traffic jams and have very relevant social-economic impact that will be studied in this case study, as it affects the daily commuting of an important percentage of the city.

Some of the data gathered includes traffic and speed of vehicles, weather data and intelligent transport systems out of service.

The outcomes of the project will implement the advantages of real and accurate predictive maintenance strategies.

Scenario:

1. Cyber attack on ITS: develop an effective emergency management plan/contingency plan in the event of disruptive cyberattack on the Security Operational Center (Control centre in which all infrastructure security devices are managed). This cyberattack scenario involves a total lost of control of the Control Centre, and therefore ITS cannot be managed remotely from this Control Centre [Specific Scenario: Losing total control of the Control Center, how can we decide what M30 can do and select the actions].
2. Flood in open air and tunnel sections: Using historical data to implement a predictive warning system to evaluate a more effective/responsive approach (to evaluate an update on design and operational maintenance plans)

3. Fire: Specific Scenario: ICC is performing fire analysis in Calle 30 to update the contingency and communication plans. The current plans are static, but the new plans will consider a dynamic approach, considering the evolution of the fire in the time, and the reaction of the people (according to their age, sex, nationality, etc) during the evacuation.

Table 1. CS#5 SCENARIO.

CS #5	Scenario
LC Phase	Operation and Mainenance, **M**
Risk	Cyber-atttack, **C** Flooding, **Fl** Fire, **F**
Transport	Road, **R**
	Tunnel, **T**
Scale	National, **N**
Location	Spain, **S**
	*risk **(C, Fl, F)**, transport (**R**), scale (**N**), location (**S**)*

3.2 Validation methodology and procedure

In the following chapter, the input variables from the existing models and comparative data mentioned above will be comparatively validated with the output from the newly developed FORESEE tools in order to improve the resilience of the railway infrastructure in the event of hazards.

For this purpose, the Key Resilience Indicator (KRI) and Key Resilience Targets (KRT) are defined in the first step (see section 3.3) and used for the selection of the FORESEE tools for this CS#5 (see section 3.3) as well as an evaluation benchmark in the further procedure.

The following tool validation is adapted to the normative of tunnels:

- RD 653/2006 on safety requirements in tunnels.
- RD 393/2007 on self-protection.
- General traffic and road regulations.

According to the document D6.1 a V-model procedure has been followed. The linear approach in the V-Model is basically divided into the phases of requirements analysis, implementation and validation. The selected FORESEE tools are additionally subdivided according to the time phase in which they are used (before, during or after an event) (see section 4).

The information regarding the requirements, modelling and output will be theoretically validated mainly on the basis of the deliveries of the individual FORESEE tools in the first step (see section 5). In the second step, the subsequent validation of the implementation of the requirements will also include comparisons with the current situation (see section 9).

In the final evaluation, possible suggestions for improvements for a real use and commercialization of the FORESEE tools are pointed out (see section 10) and the results of the validation of CS#4 are summarised once again as a conclusion (see section 11).

3.3 Resilience current indexes and resilience targets

Madrid Calle 30 Ring Road is the most important and the busiest road infrastructure in Spain. 1.5 million vehicles per day use (part of) the Calle 30, of which 200,000 vehicles per day make a "full" journey that covers the use of all tunnels (48 km in total).

The infrastructure is managed and operated by Calle 30, which is responsible for the operation and maintenance of this infrastructure only. This company is part of the Madrid City Council it is a public-private mixed economy company that is fully dependent on the City Council. The private part is a consortium of O&M service providers including Ferrovial Servicios SA.

Man-made events include cyber-attacks (due to the importance of Intelligent Transport Systems, particularly in the tunnel section) and unintentional events such as accidents (average number of 14 interventions/day due to accidents) or fires (generally caused by accidents).

Interruptions on the M-30 cause delays, traffic jams and have a very relevant socio-economic impact as they affect the daily transportation of people and goods of a significant percentage of the city. The socio-economic analysis carried out for the Calle 30 scenario can be consulted in Annex 3 of this report.

In the different data tables contained in deliverable D1.1, the characteristics of the infrastructure have been detailed, which are considered necessary input data for estimating the service and resilience of this ring road of the city of Madrid. They can be consulted as part of Annexes 2 and 3 included in this report.

Event-independent input data have been introduced to measure the service, such as the annual maintenance cost, number of people travelling per day, goods travelled per day, leisure and socio-economic cost per person, and others. On the other hand, data that depend on the outcome of the event have been included, such as the cost of intervention after the event, days to recover normal service, and the outcome on people and property.

HOW TO MEASURE THE SERVICE:

This transport infrastructure is considered to be managed along its life cycle, to provide service, in the best safety conditions, service that allows:

- a vehicle to travel along the ring road known as Calle 30 in a specific period of time (travel time),
- In conditions that guarantee its safety (safety),
- In conditions that guarantee its maintenance and response to events (interventions),
- the inhabitants of the Metropolitan Area of Madrid to benefit from a good road connection (socio-economic activities).

In order to measure these characteristics of the service, we have therefore established and assessed journey times, safety, the cost of interventions, and the impact on socio-economic activities.

In the tables contained in deliverable D1.1 (Annex 1), we have defined the measure of the expected loss in the level of service after an event, in this case a cyber-attack event.

For this purpose, we have used 28 indicators, selected to measure resilience to man-made events. It is included an explanation of each indicator, and the reasons why it has been chosen. They have been grouped into different levels, and respond to the following groups:

- Operation: Those aspects related fundamentally to the infrastructure and its condition.
- Protective measures: Those aspects related to the safety of the operation.
- Preventive measures: All those related to the legal requirements applied to the maintenance and management of the infrastructure.

We have considered and pointed out that it would be convenient to relate these factors to the existence of a quality plan that helps in the permanent monitoring of the established indicators.

Of particular relevance is the analysis of indicators related to the organisation of operation management, with indicators defined prior to the event, highlighting the strategy and existence of a maintenance plan, as well as others related to the activities to be carried out in the presence of the event and afterwards, indicating the existence and practices of the emergency plan, as well as the forecasts for the timely restoration of normality in the service.

The assignment of the values of the resilience indicators takes into account the state of the infrastructure in the phases before, during and after the event, the protection measures, which include alternative routes, the existence of a warning system and evacuation measures.

Finally, the indicators relating to the environment and the value of the effect on different past events are assessed, and related to the indicators described above.
The assessment of these indicators, and of what is presented as a procedure, can be carried out using equal weights, considering the method that consists of assessing the impact that the indicators have on the expected service under optimal conditions to be the most objective.

LEGAL REQUIREMENTS FOR THE PROVISION OF THE SERVICE:

It was mentioned earlier that the requirements for the provision of the service are conditioned on the one hand by legal regulations:

- RD 635/2006 on safety requirements in tunnels.
- RD 393/2007 on self-protection.
- General traffic and road regulations.

On the other hand, and in the specific case of Calle 30, those derived from the requirements contained in the Concession and Operation Contract for the road, which, where appropriate, are specified in indicators that are reviewed during audits and constantly monitored in the Quality Plan. By way of summary, the indicators chosen for this chapter are detailed below, referring to the occurrence of the event:

- Interventions for restoration.
- Impact on travel times.
- Impact on safety.
- Impact on socio-economic activities.

The reference values and the objectives to be achieved in the face of man-made events have been set.

The case study application shows how the service and resilience objectives can be set for the M-30 ring road in Madrid. This is done both directly and for resilience indicators, with and without cost-benefit analysis, based on the road resilience measure estimated in Appendix 1 of deliverable D1.1 (Annex 1).

- **When serviceability and resilience targets are set without a cost-benefit analysis,** experts and stakeholders consider it acceptable that the costs of the restoration intervention are less than 70% of the estimated maximum after a man-made event. The acceptable reduction with reference to service travel time is set at 80% of the maximum for the hazard, while for the three specific Tier 2 service safety impacts (i.e. property damage, injuries and fatalities), the acceptability is set at 40%. 50% y 60%. The acceptable reduction with reference to the socio-economic activities service is set at 70% of the maximum. These values are an expression of stakeholder opinion and the requirements set out in tasks 1.1 and 1.2.
- **Where resilience indicator targets are set without a cost-benefit analysis**, experts and stakeholders have set the level of acceptability, in terms of a minimum value to be guaranteed for each selected indicator. Indicators for which no targets have been set are indicators that have been considered outside the control of the infrastructure manager (e.g. hazard zone). These values are an expression of stakeholder opinion and the requirements set out in tasks 1.1 and 1.2.
- **When setting service and resilience targets with cost-benefit analysis**, the target set TS_M1 (no change in service) has proven to be the best solution with reference to man-made events. This implies that when infrastructure managers agree on the input used, this set of targets provides the highest net benefit.
- **When resilience indicator targets are set with cost-benefit analysis**, the target value for each indicator has been estimated directly from the cost-benefit analysis. This implies that when infrastructure managers agree on the input used, the targets set for each indicator provide the greatest net benefit.

In summary, the case study application shows how service and resilience can be estimated for the M-30 in such a way that:

- The service measure allows the impact of any loss of service to stakeholders to be quantified; and
- The resilience measure allows quantifying the impact of human interventions with system intrusions, cyber-attack, on the service.
- Indicators that reflect the expected service values have been chosen.

The transport system resilience measure should be read differently depending on which of the three ways the measure is used:

- When equal or differentiated weights are used, resilience is expressed in terms of service loss, i.e. the higher the service loss (quantified in monetary values), the lower the resilience of the system;
- Whereas when no weights are used, resilience is expressed in terms of percentage of target achievement, i.e. the extent to which actual conditions match the condition that is considered optimal for each indicator.

Furthermore, it is possible to note that the three proposed ways of doing the measurement (i.e. without weights, with equal weights and with differentiated weights) imply different levels of complexity to be realised, but also provide different degrees of refinement in the measures.

It is also to be noted that the results of the analysis can be broken down to narrow a particular subsection of any level of the indicators structure. This implies that, other than considering the overall measure of resilience of the infrastructure, it is also possible for Calle 30 to investigate in detail the measure of resiliency specifically due to the organization, rather than due to the infrastructure in itself, or the environment. Or, even in more detail, the measure of resiliency due only to the condition state of the infrastructure. This is seen as a useful tool to realize both:

(a) What is the overall resilience of the infrastructure; and
(b) How to intervene to improve it, where possible.

Taking into consideration the outputs coming from the previous study, we can obtain the following key resilience indexes, whose values are under the maximum possible level. In result, these are the indicators we could improve using the tools developed as part of the Foresee project.

Definition and Calculation of level of service and index resilience targets
- M1.1.2 Age of replacement of safe shutdown system
- M1.1.3 Condition state of infrastructure
- M1.1.4 Condition state of protective structure and systems
- M2.1.6 Traffic

Other resilience Index
- M1.1.1 Age of replacement of the warning systems (uneconomical)
- M2.1.3 Hazard zone (difficult to change it)
- M2.1.4 Duration of past down time due to hazard (already with max resilience level)
- M3.1.2 The presence of a maintenance plan (already with max resilience index)
- M3.2.1 The presence of an emergency plan (already with max resilience index)
- M3.2.2 Practice of the emergency plan (already with max resilience index)
- M3.2.3 Review/update of the emergency plan (already with max resilience index)

3.4 Selected FORESEE Tools

The FORESEE tools selected to improve the resilience of this infrastructure are:

Table 2. CS#5, Foresee Tools

Result ID	*Name*	*Description*	*Developer*	*KPI-KRI connection*	*Case Study 5* SCENARIO	
					Design & Construction, **D**	Operation & Maintenance, **M**
D 1.1	**Resilience Guidelines to measure Level of Service & Resilience**		**ETHZ**		√	√
D 1.2	**Set Targets**		**ETHZ**		√	√
T 1.3	**Governance Module**		**UC**			
T 2.2	**Risk Mapping**		**UC**			
T 2.4	**Virtual modelling Platform**		**UEDIN**			
T 2.5	**Alerting SAS platform**		**TVUK**			
T 3.4.1	**Traffic Module**		**WSP**			
T 3.4.2	**Fragility and Vulnerability Analysis & Decision Support Module**		**RINA-C**			
T 4.1	**Flooding Methodology**		**IH**		√	√
T 4.4	**Hybrid Data Fusion Framework**		**ETH**			√
T 5.5	**Command and Control Center**		**FRA**		√	√
T 7.1	**Definition of framework: use cases, risk scenarios and analysis of impact**		**CEM**		√	√
T 7.2	**Design, construction and remediation plans**		**CEM**		√	
T 7.3	**Operational and maintenance plans**		**TEC**			√
T 7.4	**Management and contingency plans**		**ICC**			√
		Solutions catalogue				
T 4.2	Earthquake Platform		CEM			
T 3.3	Sustainable Drainage System		CEM		√	√
T 4.3	Development of algorithms for the selection and definition of efficient and optimal actions		ETH/CEM			
D 3.5	New Family of PA-pavements		UC		√	√
D 3.6	Smart & Integral slope stabilization system		UC			
D 4.4	SHM Algorithms		TEC			

Ferrovial has worked hand by hand with some of the tool developers giving them all the relevant information needed so they can develop their tools. This information is mainly focused on the characteristics of the infrastructure (number of lanes, type of lane, total length…), the characteristic

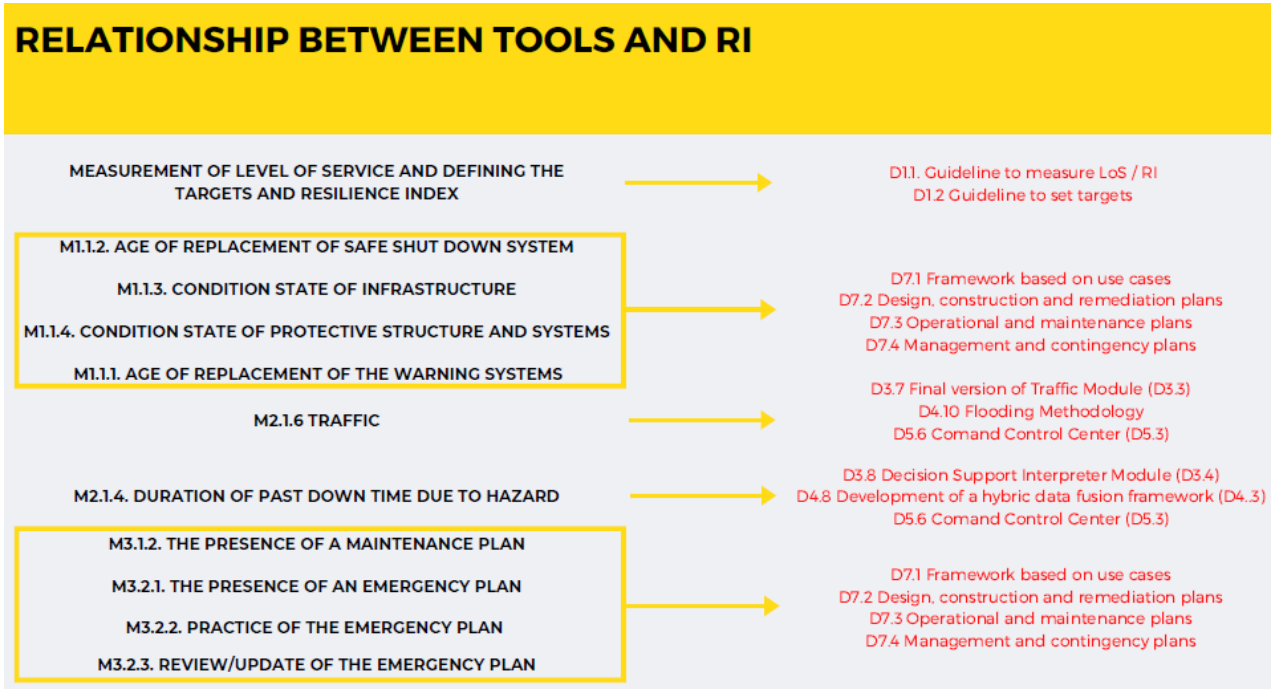
of the users (number of people travelling, number of goods, cost of travel, etc…) and the raw traffic data for simulations.

This information has mostly been used on the validation of the "Hybrid Data Fusion Framework" and the "Traffic Module" tools working together with ETH and WSP.

On the other hand, our hydraulic technical department has also been worked among the Flooding Methodology developer, which is the University of Cantabria. Information about HEC RAS and HEC HSM models and simulations have also been shared.

And finally, we have also worked with ICC in the fire tests they have been performed to update the emergency and contingency plans. Information about the HVAC systems and the fire extinguisher plans have been part of the input data.

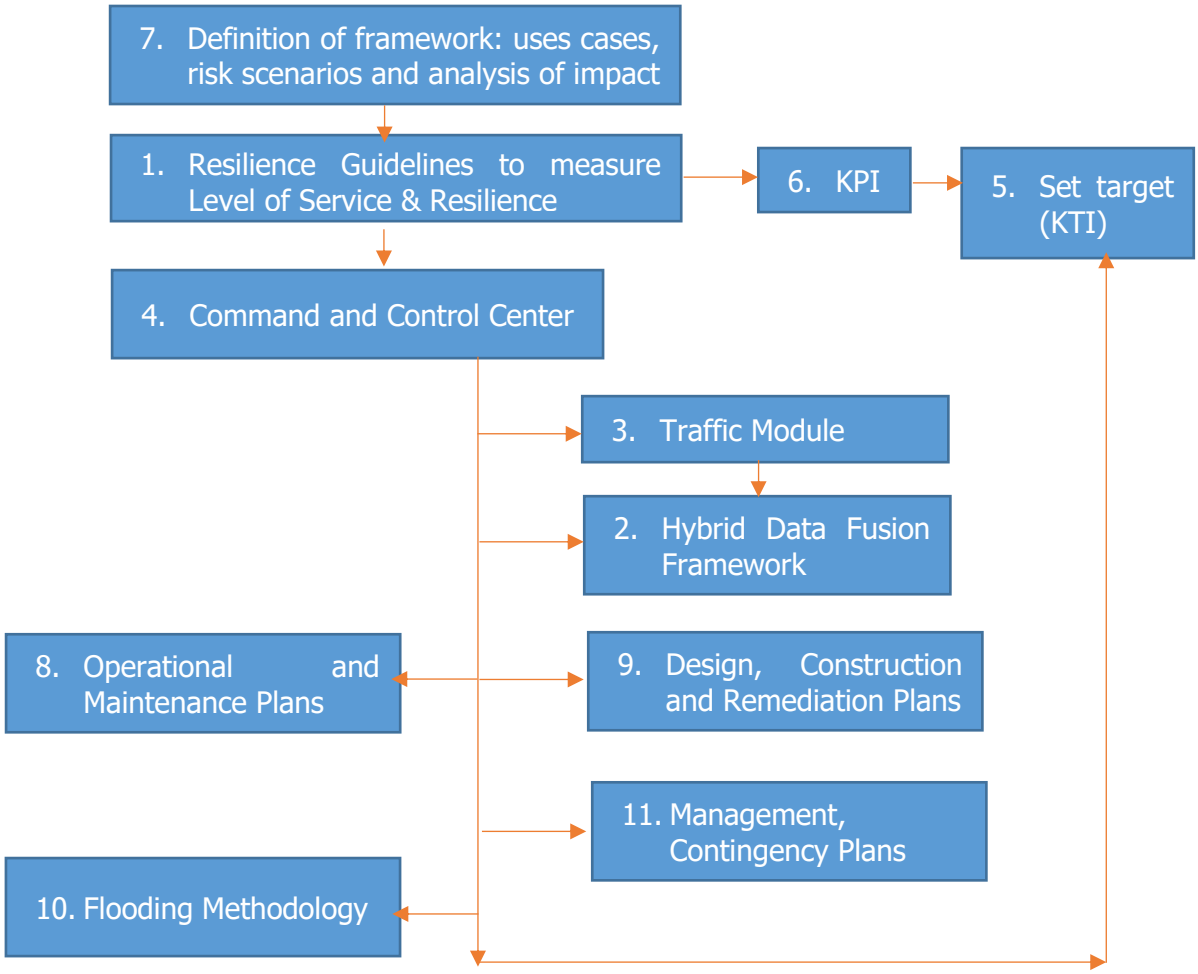
One of the key aspects of the present working package is to be able to make a cross reference or to link the previously identified key resilience indexes with the Foresee developed tools. With that purpose, on the chart below, this connection can be checked.



4 SYSTEM VALIDATION IN CASE STUDY #5 BY CASE STUDY LEADER

The approach to validate the tools have been the following:

- In order to better understand each tool without reading their specific deliverable, a summarize of the tool has been provided
- Definition of the main KPIs that each tool uses as an input and gives as an output
- Relation between the previously mentioned selected KPIs wit the ones obtained from the tools (point 2)
- Analysis of the KPIs that will improve the resilience of the infrastructure by using each tool
- Executive analysis and conclusions of each tool developed by the infrastructure manager



1. The Tool Definition of framework: use cases, risk scenarios and analysis of impact, defines the potentials risks.
2. The infrastructure is digitized through Indicators, KPI and thresholds KRT – Deliverables D1.1 and 1.2
3. The Tool Command and Control Center represents graphically the indicators and the thresholds.
4. The Flooding methodology define graphically the flood zone, for different Return Periods.
5. The Traffic Module is an stochastic algorithm that predict the most probable input data before using it in a traffic simulation software
6. The Hybrid Data Fusion Framework predict the k-ahead traffic volume

Figure 1. FORESEE TOOL Flow. Operation & Maintenance, M

5 OUTPUTS COMING FROM THE VALIDATION PHASE

In the present report we are going to summarize the main results of the application of the FORESEE Tools to the CS#5 Madrid Calle30 Ring Road. There are a total of 5 tools that have had the Madrid Calle 30 as a case scenario:

- Hybrid Data Fusion Framework
- Traffic Module
- Flooding Methodology
- Command and Control Centre
- Fire dynamic simulations

The main conclusions are going to be analyzed, and we will pay attention to the main indicators and their possible connection with the previously mentioned KRIs.

5.1. TRAFFIC MODULE (T4.4 – D3.3)

5.1.1. SUMMARIZE OF THE TOOL

The Traffic Module includes a multiscenario software script that makes use of existing traffic simulations, through traditional traffic analysis tools, in order to estimate the potential loss of service associated with multiple values of resilience indicators from them using stochastic algorithms.

The purpose of the Traffic Module is to enable resilience measurements with traffic simulations even when some uncertain input parameters are present.

The traffic forecasting capability -assuming some underlying future parameter changes- is what makes traffic simulations interesting. For example, assuming there is the possibility that a disruptive event might cause a change in the future capacity or speed, the traffic simulations can forecast the expected traffic flow changes over the network.

However, as with any forecast model, "accuracy" will depend on the robustness of the assumptions and their relationships. Therefore, when the input parameters are questionable some amount of sensitivity tests must be carried out on the areas of uncertainty. To avoid over or understatement of the range of potential deviations on this type of analysis, it is good practice to use probabilistic algorithms such as Monte Carlo simulations. Unfortunately, most common traffic simulation tools do not have this capacity.

This module demonstrate how Monte Carlo simulations can be used together with a well-known traffic simulation tool to narrow down the outcome uncertainty of the resilience assessments by using traffic simulations.

Measuring resilience for a transport system should be a combination of measuring the services without a hazard and measuring the loss of service when withstanding difficulties and while intervening to recover quickly afterwards (as explained in D1.1 and D1.2).
There are many different ways to evaluating the "resiliency" of transport systems, taking into account the varying scope of factors, and the different disruptive events and their effects on the service they provide. From the methodologies and definitions described in WP1 we can characterize the methods as a combination of "qualitative vs quantitative", with the "based on indicators vs the based on simulations". Following this characterization the traffic module aim is to help assess the resiliency on wide scope transport network scenarios using quantitative methods able to **measure volume, speed and trip duration, based on traffic simulations.**

The LOS for traffic purposes can be measured by estimating the time required to transport good and persons for a specific volume demand.

CASE STUDY 5 Calle30 Madrid (ES)

- MODEL: The Use Case does Not have a Transport demand model available to FORESEE. However the Domiciliary Mobility Survey (EDM) from 2018 is made available.

- TRAFFIC DATA: 2020-04-14: The Use Case provided 15min raw traffic data of 4276 different traffic counting points in the city from 2014-01-01 till 2020-03-31. The granularity of the traffic data makes the case interesting if we can match past disruptive events with the effects on traffic.

- SCENARIO/PROBABILISTIC DATA: 2020-06-02: The Case Study provides maps and event examples to match disruptive events with dates+time and data.

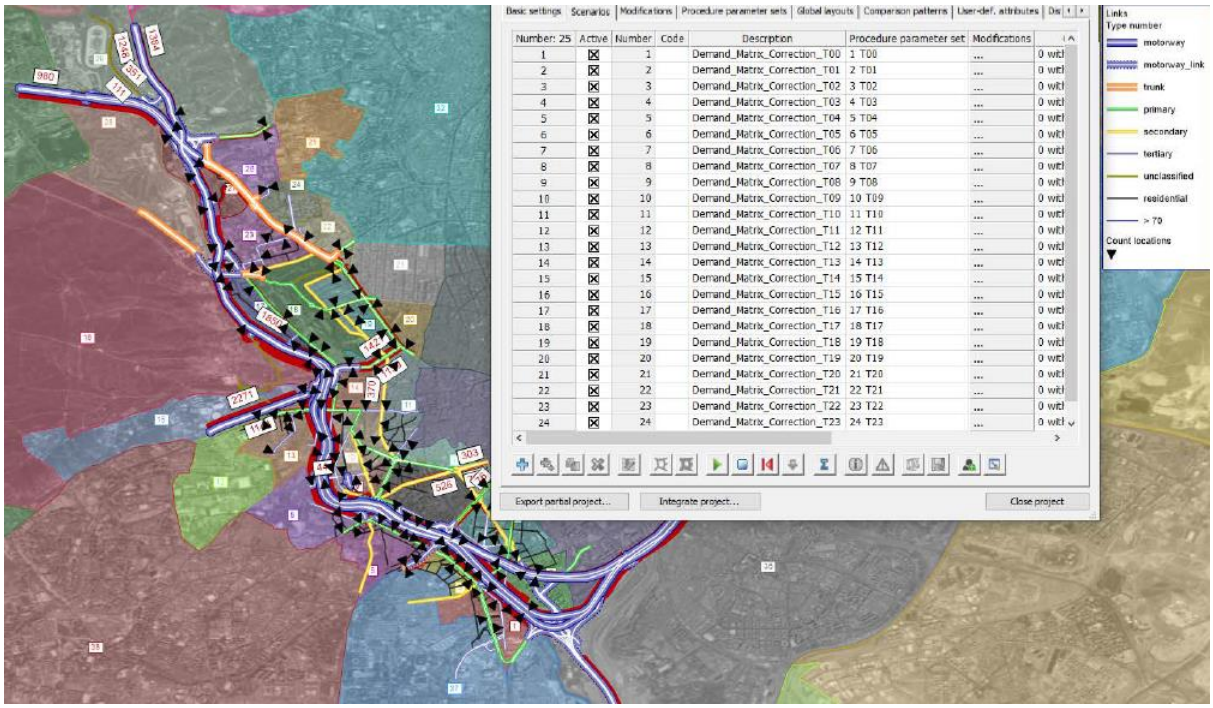


Figure 2. PTV VISUM Network codification for Case Study #5 Calle 30 - Madrid

In short, the Traffic Module describes a **conceptual framework and methodology designed for the development of the FORESEE Traffic Module**. It includes a stochastic multiscenario Python script algorithm called Monte Carlo, that makes use of existing traffic simulations, through a traditional traffic analysis tool called PTV VISUM. The purpose of the traffic module is **to enable the resilience assessment over transport demand models when probabilities or uncertain input parameters are present**.

5.1.2. TRAFFIC MODULE RESULTS

As previously mentioned, the traffic module is a Python script that creates a multi-scenario set of inputs to be used in existing traffic analysis tools. It allows to predict the future traffic volume considering the available set of traffic data and different scenarios, such as the closure of some lanes during some specific time.

The outputs from this module have been used in the Hybrid Data Fusion Framework package.

The resulting traffic model covers the South-West area of the M30, which features the tunnels under the river Manzanares, as well as the main nearby alternatives to the corridor.

The modifications thar are required to be implemented on the traffic model for the current hybrid exercise are outlined as follows:

- Ferrovial has suggested to use a representative day of the week, namely a Monday from June 2019. The 10th of June 2019 was thus selected, with corresponding datasets downloaded.

- Then a scenario management procedure was set up, executing simulations over hourly periods (from 00:00+1h to 23:00+1h) and producing the resulting .CSV (and OMX) files per hour. The resulting traffic levels and indicators that are measured are: **Speed and Traffic Volume per hour, road section and direction, as well as the hourly Travel Time** OD Matrix calculated from the mean over the path volume from the route assignment.

The implemented *worst-case scenario* is summarized as follows:

External circumstances:

- Affected sections: between "Vicente Calderón" and "San Pol de Mar".
- Day of the week: Monday.
- Month June.
- Time: 07:20 h. (Morning Peak Time)
- Traffic intensity per hour: 4'570 vh / h. Vicente Calderón direction and 5'780 in the opposite direction.
- Traffic status: heavy traffic due to rush hour.
- Other circumstances: none of note, clear day outside.

Expected Protocol Response actions:

- Prevent access to the affected section.
- Evacuation of vehicles that are inside.
- Divert traffic to alternative routes.

Times (indicative) for response and execution of measures:

- Access cut-off: It must be in person of the equipment as it does not have control of the signalling (could require ca. 40 minutes).
- Alternative diversions. They can only be done by face-to-face teams. Estimated 90 minutes.
- Evacuation of vehicles from the interior. Estimated 30 minutes.
- 90 minutes to be able to start a service recovery in degraded conditions, with the possibility of carrying out a direct control, which would require, for example, and among other measures, restricting a maximum capacity of 1'000 vehicles / hour per direction.

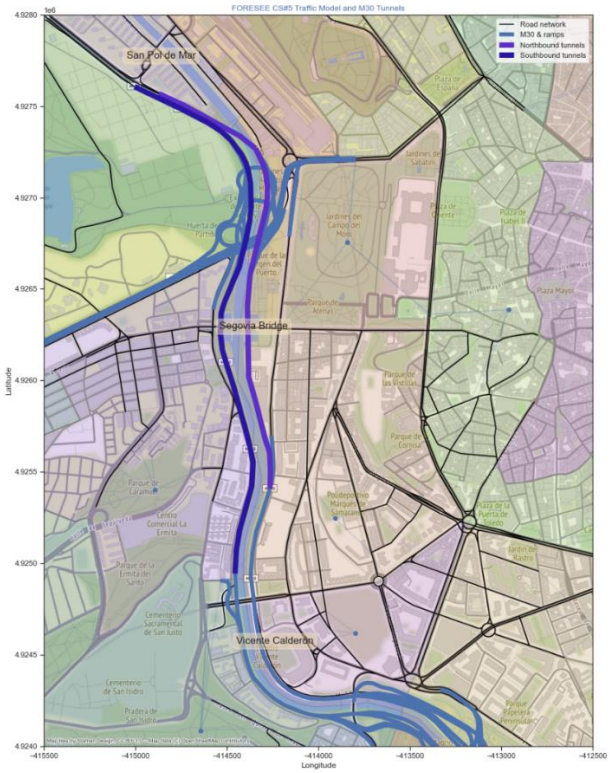


Figure 3. CS#5 Traffic model extract between San Pol de Mar and Vicente Calderon

Feature Modifications

The implementation of such a scenario in the PTV VISUM software, requires use of a so-called *modification file*, which enforces the closure and partial re-opening conditions in the affected network sections. Below is an example of such a modification to be imposed under occurrence of a cyber-attack shortly before 8:00am.

- Modification 1: at 8:00 a.m. close all access ramps in the affected section
- Modification 2: at 8:00 a.m. close the trunk in both directions in the affected section
- Modification 3: at 11:00 reopening of the trunk with capacity limitation to 1 lane less and speed reduction to 50Km/h
- Modification 4: full capacity re-opening at 12:00

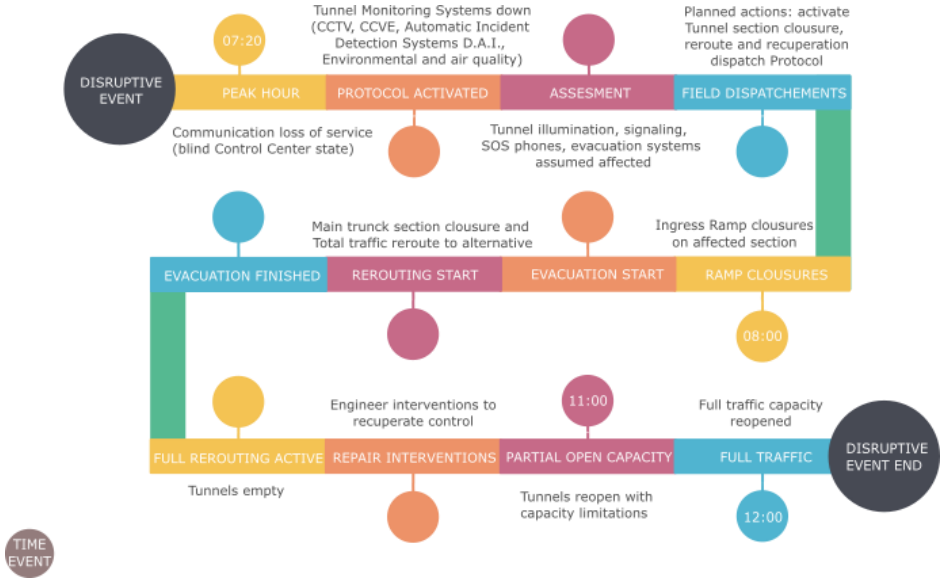


Figure 4. Example of total closure scenario

In the simulations produced for the RF we experimented with different parameters for such possible scenarios (or modifications). These parameters are:

- **Closure time (CT)**, which was assumed to vary from 12:00am to 12:00pm at 3 hour intervals, i.e., is linked to different discrete possible times of the day [0, 3, 6, 9, 12h], when a cyber-attack may occur.
- **The Partial opening time (POT),** which is defined by the duration of closure (DC). Due to limitations on the number of simulations which could be generated by WSP (as the procedure is not fully automated), we kept the DC parameter fixed to exactly 1 hour.
- **The Opening time (OT)**, which is defined by the partial closure (DPC) duration. During re-opening all links return to normal definitions, and the PO modifications ceases to apply. Due to the afore-mentioned limitations on the number of simulations which could be generated, we kept the DPC parameter fixed to exactly 1 hour.
- During PO, the following parameters are further varied for the affected links of the network (denoted in **¡Error! No se encuentra el origen de la referencia.**):
    - **NL: The number of lanes that are retained closed** with respect to regular operation. In our simulated scenarios, we use this as a dummy variable, which in fact does not affect the PT Visum output (as the choice of capacity reduction bypasses this option). This variable is thus used merely to check the capacity of the algorithm to reject non-sensitive parameters. NL can correspond to 1 or 2 lanes that are shut.
    - **CaP: The capacity modification** with respect to a baseline reduction. We enforce three scenarios of such a capacity modification: i) following the original FERROVIAL specification, ii) allowing 500 more vehicles/hour, and iii) allowing 500 less vehicles/hour
    - **V: velocity modification**. This implies that the speed limit is set equal to the reduced values of 30,50,70 km/hr for the affected links of the network.

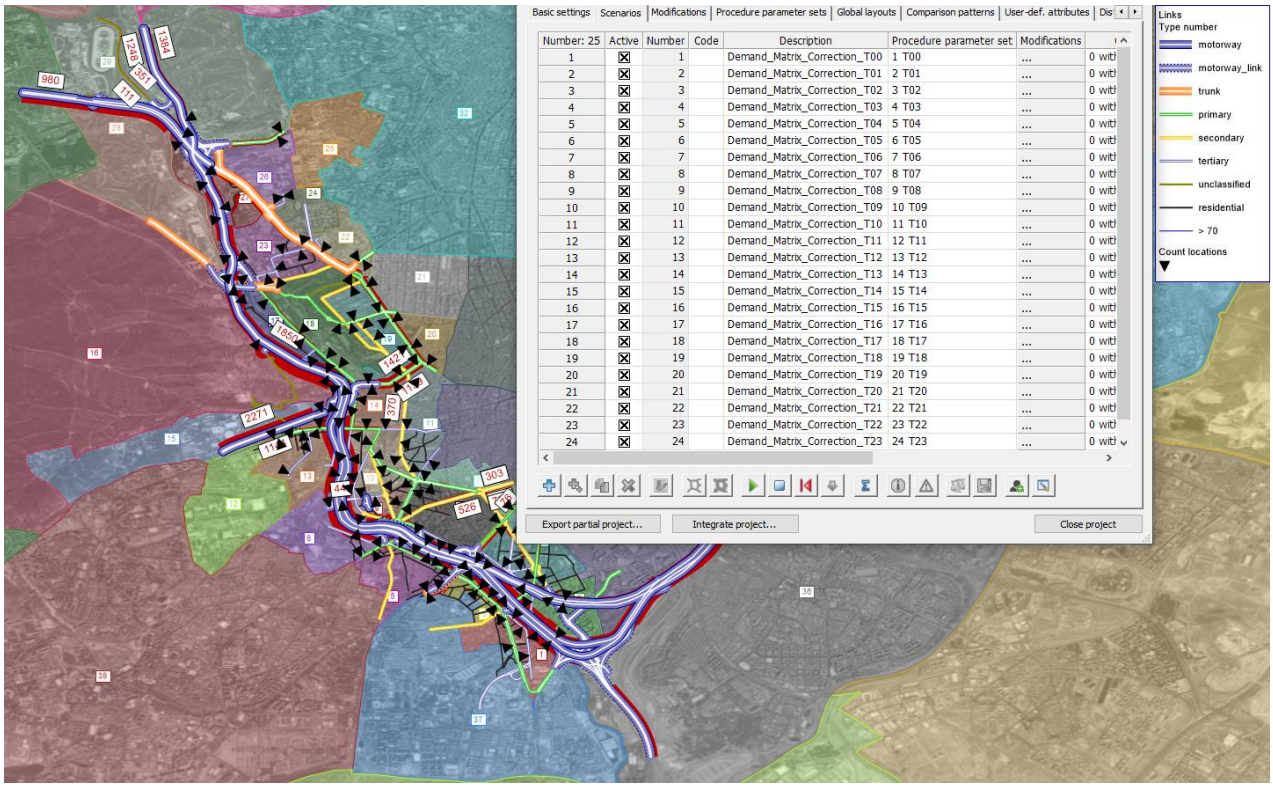


Figure 5. PTV VISUM Network codification for CS #5 Calle 30 - Madrid

The objective of the traffic model for this exercise is to produce different simulation scenarios for the desired hazard, **in order to deliver simulated data of the network performance (flows, travel times)** and assess the consequences of such hazards over regular traffic. These results yield important information regarding the evolution of traffic parameters with and without the cyber-attack hazard occurrence, or between different hour simulations. **These differences in travel time and traffic volume provide the keystone indicators for the indirect costs the hazards and their resilient strategies might have to society.**

The results are the k-hour ahead traffic on the infrastructure section studied as it can be seen below:

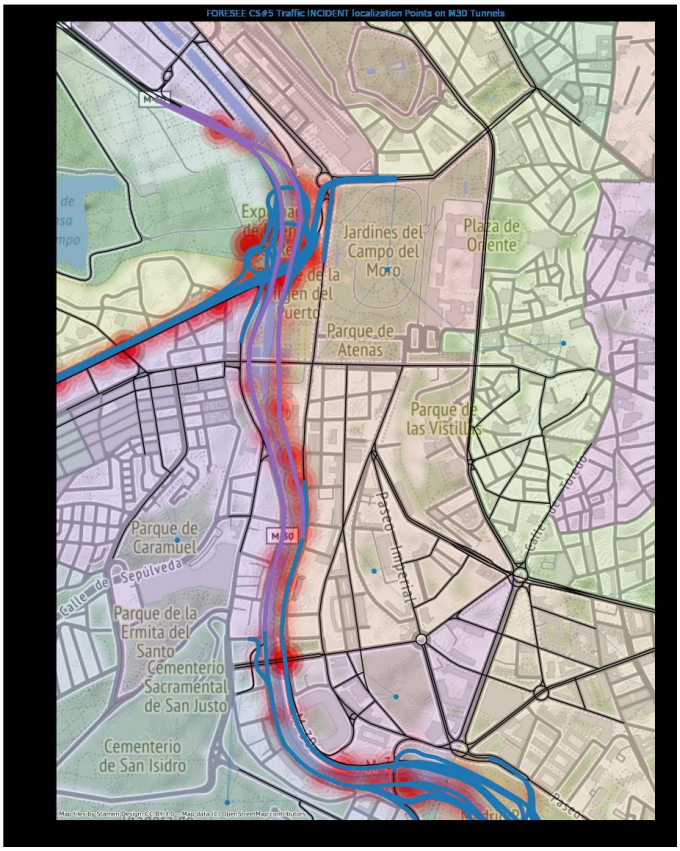


Figure 6 CS#5 Results

5.1.3. SUMMARIZE AND RELATED KEY RESILIENCE INDEXES

The main input data is the following:

- Closure time (CT),
- The Partial opening time (POT),
- The Opening time (OT),
- NL: The number of lanes that are retained closed.
- CaP: The capacity modification
- V: velocity modification.

The output data are the following:

- Travel time,
- Traffic volume at a future time (k-hours ahead),

Let us remember all the Key Resilience Indexes that were previously selected:

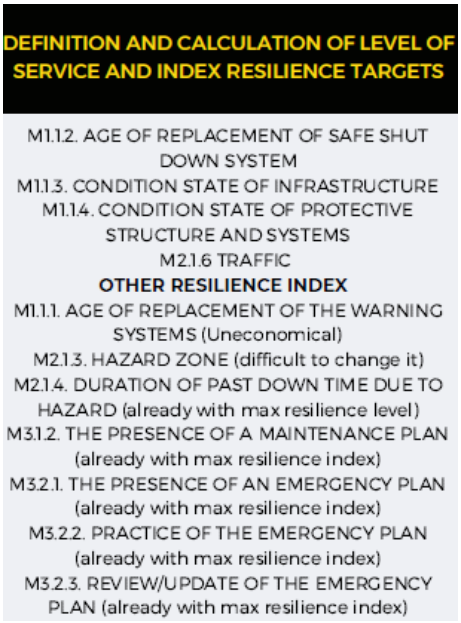


Figure 7. Key Resilience Indexes previously selected

Therefore, we can now see that there is a direct link between this tool and the next previously mentioned KRIs:

- M.2.1.6. Traffic
- M.2.1.4. Duration of the past down time due to hazard event

In conclusion, this tool will give the infrastructure manager a very important information to be able to predict the traffic volume and the duration of the closure time after the cyberattack event.

5.1.4. EXECUTIVE ANALYSIS FROM INFRASTRUCTURE MANAGER

"This report describes a conceptual framework and methodology for the development of the FORESEE Traffic Module. The Traffic Module includes a multi-scenario software script that makes use of existing traffic simulations, through traditional traffic analysis tools, to estimate the potential loss of service associated with multiple resilience indicator values from them using stochastic algorithms. The purpose of the traffic module is to enable resilience measurements with traffic simulations even when there are some uncertain input parameters".

"To measure resilience, we not only need to take into account the probability and possible consequences of disruptive events, but also the different ways in which service is restored, either temporarily through alternative routes or with restrictions during interventions. Traffic simulations are very powerful tools to measure and compare the service provided with and without events and interventions. The use of traffic simulations is required to obtain good estimates of service delivery and resilience of transport systems as explained in D1.1 and D1.2 (Annexes 1 and 2)".

The space between "inverted commas" belongs to the Executive Summary of the deliverable, and we have applied it directly to define that the objective of this module/tool is to provide

infrastructure managers with a system to help them make decisions in the case of extreme events, and to study and train Control Centre Operators, through the possibility of using simulations under normal operating conditions.

All of this contributes to improve the resilience of the infrastructure and ensure that the expected level of service is maintained, even in the face of the disruption caused by extreme events, by adapting operating procedures.

It includes a description of the scope, variables and data management requirements needed to assess resilience in transport models when some input variables are questionable.

It explains the methodology used, and the practical description of the traffic simulation tool in which the FORESEE traffic module will be implemented, which allows the explicit quantitative connection between the service provided by transport infrastructure systems and their resilience.

Service indicators for traffic purposes can be measured by estimating the time needed to transport goods and people for a specific volume demand.

To measure resilience, we need to compare a base case reference with conditions during and after the disruptive event, using simulations.

The objective of the traffic module is to simulate traffic scenarios considering variables with uncertainty. It intends to make use of existing traffic simulations and demonstrate that it is possible to generate statistical results related to uncertainty input parameters by applying stochastic methods.

APPLICATION TO THE CASE OF MADRID CALLE 30 RING ROAD

The "hacking hazard" or cyber-attack is a relatively new anthropogenic hazard to be considered in transport infrastructure.

In different sections of our collaboration with the Foresee Project, we have described the effects that a cyber-attack can have on the Madrid Calle 30 infrastructure, devoting space to how to prevent them, and to the possible impact that this type of event can have on critical management systems.

An important section is dedicated to incident management in the event of an event, using the methodology described in the Foresee Project and the existing regulations in the case of Spain.

In the case of Calle 30, which is an urban motorway that includes 48 km of tunnels, the traffic module takes on special relevance, since, through simulations, it must become the support tool for making decisions that avoid or improve the capacity to maintain the expected service, and avoid collapse or congestion inside the tunnels, which could generate situations of special gravity with risk for people.

COMPARISON BETWEEN CURRENT SITUATION AND THE POSSIBLE APPLICATION OF THE TOOL

Was this type of analysis made before FORESEE? How it was made?	This tool give us the possibility to improve the input data given to a traffic simulation model by using stochastic algorithms of Montecarlo. This kind of analysis has not been done before in Calle 30

How does FORESEE improve the results/analysis previously made?	It improves the input data for all traffic simulations, and therefore, the quality of the output data coming from that models. It also allows the simulation of the event, and its consequences on the concrete infrastructure and the incidence in the corridor.
How does this FORESEE result improve your infrastructure's management	We will have previous studies and training of the operators, for the application of measures during the event.
If it was not made, How does this FORESEE result improve your infrastructure's management?	It provides objectivity to decisions, which supports the results for third parties, especially for administrations. From a technical point of view, it allows you to combine variables and obtain results directly.
What cost/resource efficiencies you expect these tools/results to have on your day-to-day business? (e.g. 10%-20% decrease in working hours over the first year; reduction of maintenance costs (20%-25%), Return on Investment (ROI) – 10-15%, increase in productivity 25-30%)	It is difficult to assess the individual contribution of each tool, in this case the "Traffic Module", but it will probably significantly reduce the costs associated with a traffic cut in the event of an event, reducing cut-off time and travel times on alternative routes. Given the high average daily intensity (ADI) of this infrastructure, only by obtaining a 5% reduction in time and its associated cost, we would be facing a substantial advance.

CONCLUSIONS

We consider that this tool - Traffic Module - responds to the requirements that the infrastructure manager can expect in the event of an extreme event, in terms of traffic management, through the experience acquired in simulations prior to the event, and using indicators as input variables related to traffic, such as hourly intensity, travel times, speed, and others.

We consider that it would be an advantage to have simulation modules in the Control Centres to study the results of the application of different management strategies based on different scenarios.

The availability of a tool in which the Manager can immediately introduce different variables to solve the questions indicated below, and which the methodology explained in the Traffic Module of the Foresee Project allows, will be decisive for its application:

- Effects on traffic, congestion, in the face of the adoption of different alternatives, whether partial total cut-off or reduction of capacity.
- Decision on the maximum speed required.
- Incremental journey times.
- Possible impact on alternative routes in the event of diversion.

The responses, so decisive for the result of the assessment of infrastructure resilience indicators, which were defined in the different phases of the study provided during the course of the Project, represent the assistance expected by the Manager in the operation under extreme negative events.

5.2. FINAL VERSION OF THE HYBRID DATA ASSESSMENT PACKAGE (T4.4 – D4.8)

5.2.1. SUMMARIZE OF THE TOOL

This deliverable presents the final version of the hybrid data assessment package developed as part of Task 4.4 on "Development of a Hybrid Data Fusion Framework". This report contains just a summarize of the information given by the tool developer as part of the deliverable D4.8.

Two classes of tools were presented and further described in Deliverable 4.6, namely Bayesian Networks and Random Forests, which reflect a learning framework trained on heterogeneous (hybrid) data. Such data can be obtained either via monitoring information and telemetry, or from simulations exploiting appropriate models.

Bayesian Networks (BNs) have, within the Tasks 4.4. and Task 5.2.1 FORESEE context, primarily been developed as tools for classification for the purpose of diagnosing faults, or occurrence of events under extremes. BNs come with a probabilistic description, which ideally situates them as aids for decision support.

On the other hand, the Random Forest (RF) framework, is within the FORESEE toolkit primarily set up as a tool for regression, i.e., prediction of the value of a continuous Quantity of Interest (QoI), which is though critical for driving decisions under occurrence of an extreme event. This is the case in prediction of the evolution of traffic flow and distribution within a network, particularly in the face of extreme events (e.g. flood or cyber-attack). This tool, which comprises a further graph-based machine learning approach, has been demonstrated on an illustrative example that draws from Case Study 5 – The Madrid Ring Road. This simulation, which was delivered as part of Deliverable 4.6, involved an artificial highway network, serving as imitating case study, allowing for conceptualization and demonstration of the predictive algorithm. Telemetry information from the nodes (links) of this network is assumed available, with the RF used to **predict the k-hour-ahead traffic intensity level** on a given node, given context information, such as **weather** (precipitation) **or events** (e.g., sporting events, or cyber-attacks).
The outcome of the predictions of the tool aim to support decisions on road closure, based on the predictions of the trained Random Forest algorithm regarding the expected loading (traffic flow & speeds) of the network.

Here we present a summarize of the main work and conclusion of this specific tool. The developed algorithmic toolkit on data has been checked on the CS5 – the Madrid ring road. We specifically explore the scenario of a cyber-attack, which occurs on a characteristic summer day, thus imposing a need for closure of affected tunnel sections and surrounding pathways, together with a selection of restrictions to impose during , a second, partial re-opening phase of these links. The case study offers an illustration of the function of the two tools that have been setup; the Random Forest tool, employed for regression-based predictive tasks and the Bayesian Network tool, employed for classification tasks. Both are demonstrated for use with this anthropogenic hazard scenario (cyber/attach/Tunnel hacking hazard) on CS5.

The "Case Study#5 M30 Madrid" describes an urban highway that includes several tunnels under the river Manzanares. The case is quite unique in several aspects. On one hand, it offers a large stream of heterogeneous data that are suitable for testing the developed hybrid data fusion schemes. On the other hand, it is the only FORESEE case study that analyses a direct anthropogenic hazard example, the "hacking tunnel systems hazard" for which historical examples are scarce – if

at all available. Thus, we here exercise the idea of hybrid fusion, where the input/output training dataset is extracted from models, namely traffic simulations.

5.2.2. TRAFFIC SIMULATIONS

The resulting traffic model covers the South-West area of the M30, which features the tunnels under the river Manzanares, as well as the main nearby alternatives to the corridor.

These traffic simulations are part of the input data that this methology needs. Please, read the previous chapter to better understand the results coming from the traffic module.

5.2.3. RANDOM FOREST AND BAYESAN NETWORKS RESULTS

Modelling

Given the closure time and the known state of traffic, an agent would present the model with control actions in terms of the number of lanes to close, the capacity and maximum speed to allow, for the time of occurrence of the attack.

Then, the model predicts the traffic volume at a future time (k-hours ahead) defined by the agent, for specific links (road segments) of interest that are also selected by the agent. We use a Random Forest Regressor to solve this problem.

The use of a Random Forest regression model further allows for extraction of metrics that are reveal the significance of input features, or in other words, elucidate the input features that are most important in determining the prediction.

In our example the top ranked features are **traffic volume, closure time (hour), flow speed at closure, location, and the nominal speed permitted** at the link.

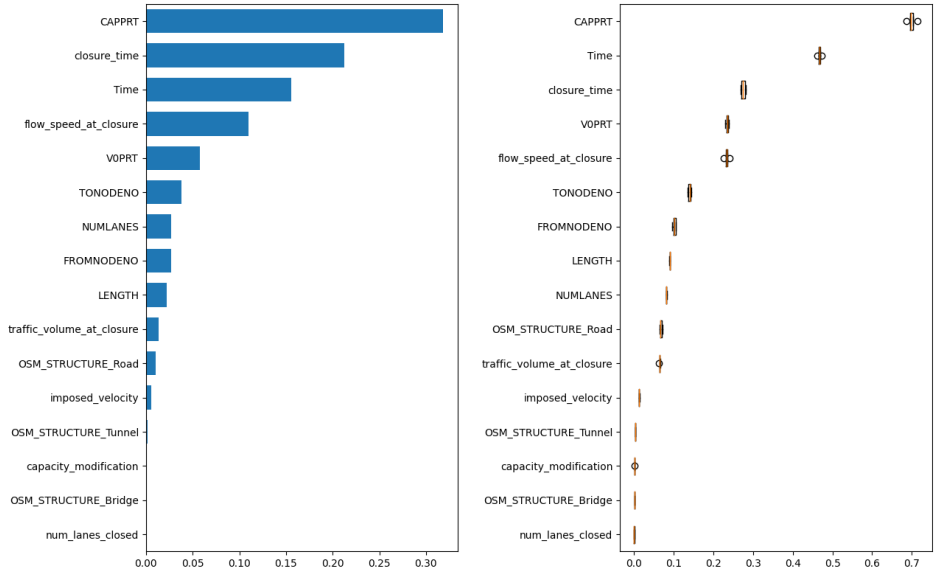


Figure 8. Impurity-based feature importance of Random Forest (left) versus the permutation importance on the test data

Once the model is trained on information derived from data, it can be used to predict the state of the system and for visualizing the expected congestion under selection of a specified scenario of imposed flow restrictions (modifications).

Here we present the main simulations performed by ETH:

The figures below demonstrate such a recovery for different sets of actions. In this illustrative case, we have simulated 9 possible actions given the scenarios we assume that allow for three possibilities **for capacity restrictions** during partial reopening (light, moderate, heavy) and three possibilities of **speed at partial re-opening** (30, 50, 70 Km/hr).

describes the action set and their numbering from 1 to 9.

Table 3 Action scenarios for this illustrative case study. In an actual setting, these possible scenarios are to be configured form the designer/operatory. It is reminded that the choice of number of lanes is here included

#	capacity restriction	velocity
1	heavy	70.0
2	light	70.0
3	moderate	70.0
4	heavy	50.0
5	light	50.0
6	moderate	50.0
7	heavy	30.0
8	light	30.0
9	moderate	30.0

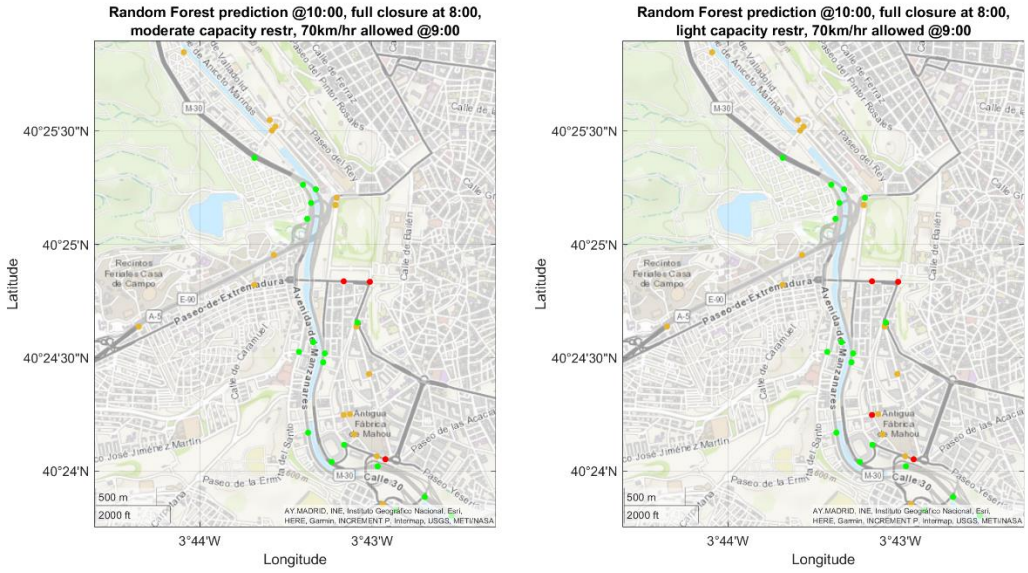


Figure 9. RAG time annotation of traffic flow in terms of the index rrec, which quantifies the recovery of flow as compared against the traffic flow at closure time. In this plot we illustrate the effect of two separate actions scenarios, namely action set 3 versus action set 2, which relate to a change in the allowed capacity at partial re-opening. These maps are offered for a closure scenario due to a cyber-attack occurring at 8:00, with partial reopening at 9:00 and prediction of traffic flow at the time of full reopening at 10:00

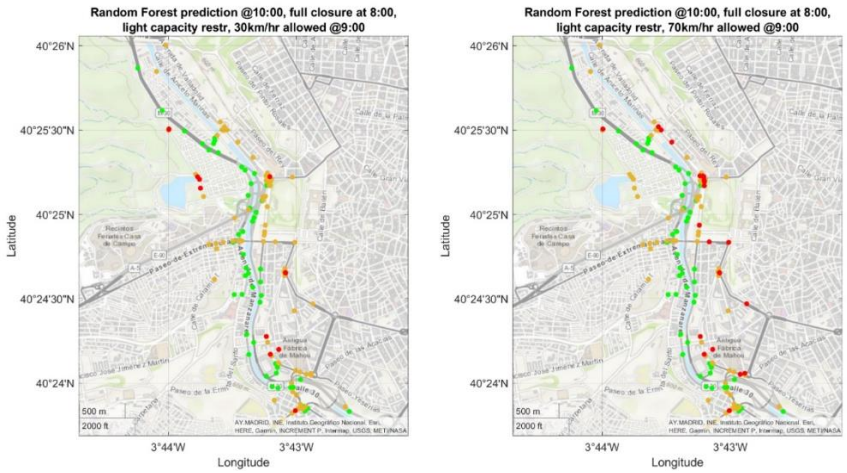


Figure 10. RAG time annotation of traffic flow in terms of the index rrec, which quantifies the recovery of flow as compared against the traffic flow at closure time. In this plot we illustrate the effect of two separate actions scenarios, namely action

As observed in Figure 7 and Figure 8, which illustrate the predicted versus the actual (simulated) flow for a closure scenario at 8:00, the RAG time annotation converts the predicted data into information that can be readily exploited for decision support for a given action scenario. For example, we note that the choice of a moderate versus light capacity restriction (Figure 7) does not lead to a highly differentiated outcome. Thus, a heavier restriction also seems tolerable and thus perhaps desired for investigation works during the suspected cyber-attack period. On the other hand, increased velocities (Figure 8) would lead to different subclusters (regions in the map) of red alerts (reduced recovery)

Cost of Travel Time (CTT)

The service provided by the route is estimated as a measure of travel time in economic terms (CTT). This is computed as the number of minutes a vehicle spends on average on a specific route.

We will thus use the Bayesian Network, in order to understand if, given a set of actions (complete closure, restrictions in velocity/capacity during partial re-opening), context (speed/traffic volume at closure) and some nominal information (capacity, velocity) on the network, it can predict the CTT indicator at a given time of the day.

The results of the study indicate an adequately trained BN model, which can be the used for prediction of the CTT, given notification on the occurrence of a cyber-attack at a given hour of the day, and for a specific-hour ahead prediction.

The estimates of the CTT describe probabilistic quantities, as is the nature of outcome of the BNs. The plot reflects the allocation of such a probability by means of a colormap, which assumes darker colors when the probability of an outcome approaches 1. **We see for example that the lowest cost in this case would be achieved by a moderate capacity modification and imposition of a permissible speed limit of 50km/hr in the affected links**, since this is the combination offering the most probably outcome for a relatively lower regularized travel time cost (CTT = 43).

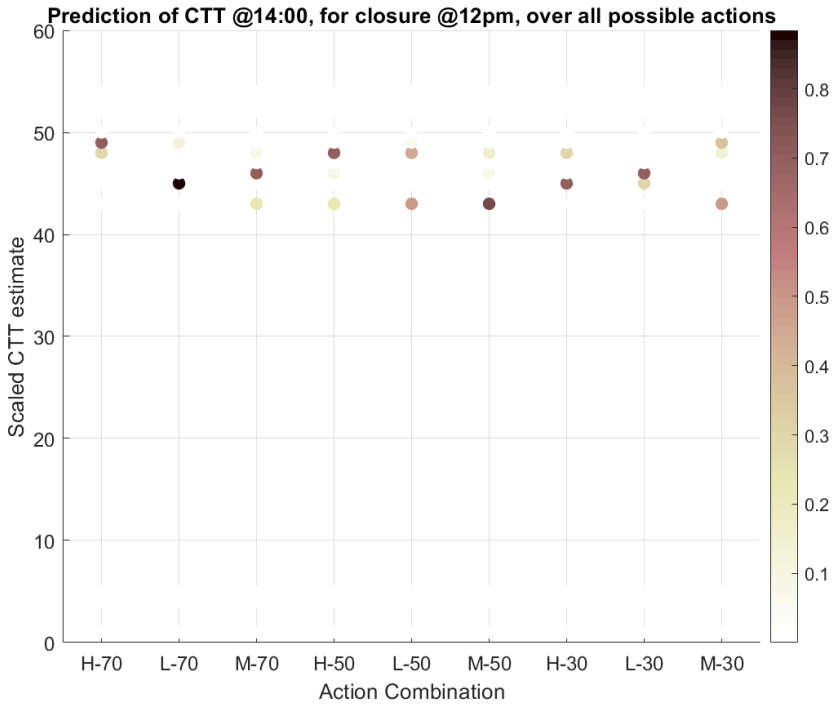


Figure 11. Prediction of CTT at 14:00 for closure at 12 pm, over all possible actions

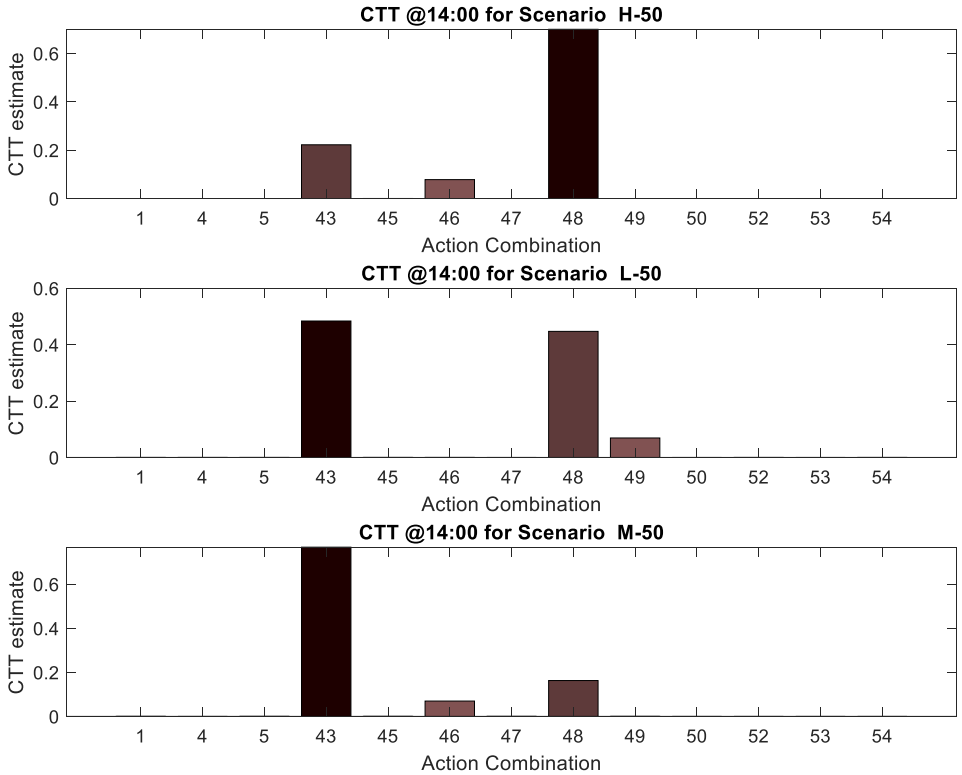


Figure 12. CTT Estimations

5.2.4. SUMMARIZE AND RELATED KEY RESILIENCE INDEXES

As previously said, this tool consists on two different algorithms: the Bayesian Networks and the Random Forest, which relies on the output data extracted from traffic simulations coming from the Traffic Module.

The main input data is the following:

- Closure time (CT),
- The Partial opening time (POT),
- The Opening time (OT),
- NL: The number of lanes that are retained closed.
- CaP: The capacity modification
- V: velocity modification.

The output data is the following:

- Travel time,
- Traffic volume at a future time (k-hours ahead),
- Cost of travel time.

Let us remember all the Key Resilience Indexes that were previously selected:

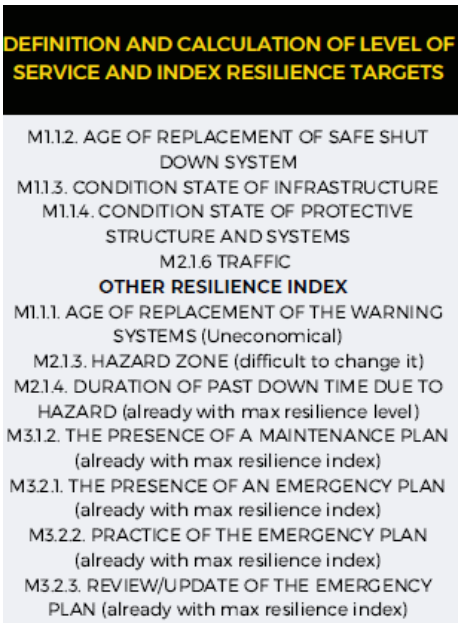


Figure 13. Key Resilience Indexes previously selected.

Therefore, we can now see that there is a direct link between this tool and the next previously mentioned KRIs:

- M.2.1.6. Traffic
- M.2.1.4. Duration of the past down time due to hazard event

In conclusion, this tool will give the infrastructure manager a very important information to be able to predict the traffic volume and the duration of the closure time after the cyberattack event to be able to perform the best actions in order to reduce the cost of travel time to the minimum.

5.2.5. EXECUTIVE ANALYSIS FROM INFRASTRUCTURE MANAGER

Transport infrastructures are exposed to a variety of anthropogenic threats, both accidental (such as an unintentional explosion) and intentional, man-made (such as terrorist attacks). These trends, together with growing transport demand and increasing traffic loads, will put further pressure on European infrastructure.

It is therefore clear that action must be taken to make infrastructure more resilient, minimising disruptions, as well as damage and costs, in short, maintaining the best possible level of service.

This is the purpose of the Foresee Project, and as part of the overall study involving the analysis of the infrastructure in its different phases, a series of tools such as the one in this deliverable have been set up.

The input data for the study of resilience and its assessment, as well as the study of the different scenarios that may occur in the event of an extreme event, involve inputs from different sources which, on their own or in combination with others, may determine a result in accordance with the expected level of service, or the opposite, and all of this immersed in time space, and a constant variation.

The development of a hybrid data fusion tool, as part of the FORESEE toolkit, is driven by advances in terms of application of diversified monitoring schemes in infrastructure systems, offering the ability to monitor the condition and performance of infrastructure assets (roads, bridges, tunnels) and use this information to support decision making.

The predictive output of the tool aims to support decisions on road closures, based on the predictions of the trained Random Forest algorithm with respect to the expected load (traffic flow and speeds) of the network.

We call this module "hybrid" to denote its ability to merge heterogeneous data, coming from both simulations, as well as monitoring data at different levels/components.

Thus, heterogeneous information is currently collected that may be available on different components of the infrastructure network (roads, bridges, tunnels), but cannot be immediately exploited for decision support when it remains in its original form. The decision support task requires the intermediate step of translating the collected data/measurements into meaningful system performance information.

The tools developed as part of Task 4.4 employ a graph-based approach, which ensures interpretability.

There is a need to facilitate the use of this tool by practitioners and managers, which is currently under construction.

Traffic simulations are traffic forecasts resulting from complex transport demand models, and represent within the FORESEE project, the possibility for infrastructure managers to have elements to support decision making in the face of events.

DIRECT ANTHROPOGENIC HAZARD

The "hacking hazard" or cyber-attack is a relatively new anthropogenic hazard to be considered in transport infrastructure. The term describes a wide range of security hazards that are human-generated and can directly or indirectly affect the operational, economic and security parameters of the infrastructure. Whether they attack transport modes, the transport network, traffic flow control, revenue, management or communications systems, they can directly affect public safety and critical operations, as well as the operation and organisation of the infrastructure.

THE CASE OF CALLE 30 RING ROAD

Describes an urban road that includes several tunnels under the Manzanares River. The case is quite unique in several respects. On the one hand, it offers a large amount of heterogeneous data that are suitable for testing the developed hybrid data fusion schemes. On the other hand, it is the only FORESEE case study that analyses an example of a direct anthropogenic hazard, the "piracy tunnel system hazard" for which historical examples are scarce, if available at all.

Therefore, here we exercise the idea of hybrid merging, where the input/output simulation dataset is extracted from models, i.e. traffic simulations.

Among the transport infrastructure components, tunnels represent perhaps the most intensive active systems, requiring traffic control mechanisms, electromechanical systems, lighting, ventilation and many other associated security systems to ensure their safe functionality, critical elements mentioned in our report on the effects of a cyber-attack. All these systems are interconnected and managed from a network control centre.

Control centres are responsible for managing operations through the use of intelligent transport systems (ITS), or other management systems. They receive the information, and after evaluation, respond with previously established procedures.

In our example, the characteristics on which the work has been set are the traffic volume, the closure time (hour), the flow speed at closure, the location and the nominal speed allowed on the link, as well as the number of lanes closed.

Once the model is trained with data-derived information (e.g. SHM/traffic telemetry and more) and possibly with complementary data from available traffic simulations, it can be used to predict the state of the system and to visualise the expected congestion under selection of a specific scenario of imposed flow restrictions (modifications).

COMPARISON BETWEEN CURRENT SITUATION AND THE POSSIBLE APPLICATION OF THE TOOL

Was this type of analysis made before FORESEE? How it was made?	This is a module that predicts the k-ahead traffic by using two types of algorithms and relying on heterogeneous data. They are able to learn from traffic simulations and to give future predictions based on this previous learning. Traffic simulations are done by using commercial software; however, this kind of analysis have never been done before.
How does FORESEE improve the results/analysis previously made?	This kind of study was never applied before. It allows the simulation of the event, introducing the variables of all the critical elements of tunnel management.
How does this FORESEE result improve your infrastructure's management	It gives you additional information to value the impact of partially or totally closing some lines or the whole section of the tunnels. We will have previous studies and training of the operators, for the application of measures during the event.
If it was not made, How does this FORESEE result improve your infrastructure's management?	It allows you to predict how the traffic will be after a hazard and depending on how you manage it. It provides objectivity to decisions, which supports the result for third parties, especially for administrations. From a technical point of view it allows you to combine variables and obtain results directly.
What cost/resource efficiencies you expect these tools/results to have on your day-to-day business? (e.g. 10%-20% decrease in working hours over the first year; reduction of maintenance costs (20%-25%), Return on Investment (ROI) – 10-15%, increase in productivity 25-30%)	The application of this tool can reduce the time of travel time, the traffic volume at a future time and the cost of travel time after a hazard event. It is complicated to quantify the impact in terms of cost or ROI, but it will surely have an important impact.

CONCLUSIONS

We consider that the tool described under section 4.8, responds to the requirement that the infrastructure manager can expect in the face of an extreme event, as it answers questions as decisive for decision making as the following:

- Effects on traffic, congestion, in the face of the adoption of different alternatives, whether partial total cut-off or reduction in capacity.
- Decision on the maximum required speed.
- Incremental travel times.
- Possible impact on alternative routes in the event of diversion.

The responses, so decisive for the result of the assessment of infrastructure resilience indicators, which were defined in the different phases of the study provided during the course of the Project, represent the assistance expected by the Manager in the operation under extreme negative events.

5.3. COMMAND AND CONTROL CENTRE

5.3.1. SUMMARIZE OF THE TOOL

The Command Control Centre serves for training purposes to increase situation awareness of the users in the FORESEE toolkit.

It provides interactive real time visualization and natural human computer interaction by using big data analytics and machine learning.

It uses neural networks to achieve efficient anomaly detection by learning the normal behaviour of the infrastructure. This allows the neural networks to detect when new data points lay outside of this normal behaviour and issue meaningful alerts.

It uses a supervised machine learning approach, using historical data randomly split into trainset and testset (80% - 20%). While the model is trained and built on trainset of historical data, the model ix fixed, tested and validated on the testset of historical data.

Once the model is trained and tested, whenever it is fed with new data (live data or near real time data), it can give prediction for anomalies such as flooding events.

For the particular scenario of the Madrid Calle 30 Ring Road, the following tasks have been developed:

- Traffic data pre-processing
- Neural networks trained
- Built REST API with endpoints
- Deployment as Docker Container on FRA server
- Hazards: heavy rains and flooding

5.3.2. SUMMARIZE AND RELATED KEY RESILIENCE INDEXES

There is not a direct relationship between the previously selected resilience indicators and the output coming from this tool.

The only output that this tool gives us is an anomaly score based on the comparison of the real traffic with the historical data. If this score surpasses a threshold, and anomaly or hazard event is detected, and thus an alarm is deployed. However, if this threshold is not surpassed, the algorithm considers that there is not an specific event.

Therefore, as said before there is not a direct link with the KRI.

5.3.3. EXECUTIVE ANALYSIS FROM INFRASTRUCTURE MANAGER

One of the most interesting aspects of this tool is that it gives us an anomaly score based on the current traffic and it compares it with the historical data. If the traffic surpasses a level, it gives us an alarm. In this particular case, the scenario of heavy rains and flooding was considered, therefore if this alarm is triggered, it means that a possible flooding event is about to happen.

In the Calle 30 ring road, there are a lot of cameras and sensors located not only on the tunnels, but also on the surface. This infrastructure relies on a very efficient Control Centre that is always monitoring the global performance of the system. For that reason, Calle 30 has more than enough ways to know if a flooding event is happening, and that is why we do not see a direct application of this tool in this infrastructure.

However, we consider that this tool will be very useful in any kind of infrastructure without cameras or any other type of monitoring sensors, such us remote highways or roads, bridges, etc.

5.4. FRAMEWORK FOR THE APPLICATION OF FORESEE RESILIENCE PLANS (D7.1)

5.4.1. SUMMARIZE OF THE TOOL

Here we present the main conclusions extracted from deliverable D7.1:

In this case, it has been considered for analysis the route of a highway with tunnels that suffers a cyber-attack on the infrastructure (and not on the vehicles using it).

- **What can happen?**

Similarly, each of the components that assemble the highway and the tunnels were analyzed to identify which are the major risks. In this case, regarding the road the main two direct components that were considered susceptible to this type of threat were: the communication system and signaling; while regarding the tunnel three components were identified: the fire protection system, the ventilation and drainage systems. Table 4 shows the results obtained: the first column indicates the component considered and, on the right, the major risks that they could suffer.

Table 4. CS#03: Risks on components

ROADWAYS - GENERAL		CYBER-ATTACK
ROAD COMPONENT	RISK ID	MAJOR RISKS
Communication systems	CM.02	Communication failures &/ impersonation
Signalling	SI.01	Equipment failures &/ control loss
	SI.02	Damage or control loss of signs, variable message signs (VMS), lighting, street lights, control access, toll booths and supports
	SI.03	Collapse of the above
TUNNEL COMPONENT		
Fire protection system	FP.01	Failure &/ control loss
Ventilation system	VE.01	Equipment failures &/ control loss
Drainage system	DR.05	Pump failures &/ control loss

- **If it does happen, what are the consequences?**

Next, the theoretical impacts following a cyber-attack are analyzed. Table 5 shows the results obtained for the analysis: the first column indicates the type of impact identified (operational, safety, etc.) and, on the right-hand side, the theoretical impacts.

Table 5. CS#03: Theoretical impacts

ROADWAYS		CYBER-ATTACK
TYPE OF IMPACT	IMPACT ID	IMPACT DESCRIPTION
Operational	OP.01	Reduced traffic capacity
	OP.02	Temporary closure
	OP.03	Collapse / long-time closure
	OP.04	Traffic restrictions
	OP.05	Travel delays
Safety	SF.01	Accidents (vehicles)
	SF.05	Passage obstruction
	SF.07	Vehicle immobilization
Social - safety	SS.01	Direct loss of lives

ROADWAYS		CYBER-ATTACK
TYPE OF IMPACT	IMPACT ID	IMPACT DESCRIPTION
	SS.03	Difficulty for response operations
Social	SO.01	Quality of transport service
	SO.02	Loss of reputation
Economic	EC.01	Maintenance costs
Socio - economic	SE.03	Disruption of economic activity

A cyberattack is any type of offensive manoeuvre that targets computer information systems, electronically controlled infrastructures, computer networks, or personal computer devices. The "hacking hazard" or cyberattack is a relatively new anthropogenic hazard to be considered in transport infrastructure. The term describes a wide range of security hazards created by humans that can affect directly or indirectly to the infrastructure's operational, economic and safety parameters. Whether they attack the transport modes, the transport network, the traffic flow control, revenue, management or communications systems, they can directly affect public safety and critical operations, as well as the infrastructure operation and organization.

Hacking events are very different and broad in nature, they use a wide variety of tools and methods to gain control or have an impact on the normal functionality of their electronically controlled targets. The tools range from deceiving applications, logic bombs, botnets, trojan apps, viruses, worms, keyloggers and specialized toolkits, while the methods vary from brute force, DOS (Denegation of Service), to social engineering such as phishing, crypto-ransomware, CEO fraud or more recently by tricking machine-learning systems into misinterpreting traffic signals on autonomous vehicles. These methods and tools are challenged by the ITS defences, security culture and network control procedures. The best management practices against cyberattack incidents involve an organized Security Operations Centres as well as their technological infrastructure and tools to defend and protect the infrastructure (firewalls, white/blacklists, Antivirus, Honeypots, intrusion detection and prevention systems, etc.).

- **Types – What kinds of cyber-attack hazards can occur?**

Cyber-attack hazards can take place mainly according to one or more of the following processes:

Internet connected vehicles attack. (Future autonomous vehicles): As with any other device that connects to the internet, there is a potential risk to automotive security from cyber criminals. Security breaches can result in leaked personal data, threats to a vehicle's essential security and safety mechanisms and, in extreme cases, full remote control of the car.

Infrastructure active system attacks: ventilation, lighting, control access/barriers, toll booths, bascule bridges or other movable/actionable structures.

Traffic Control System / Centre Attack: Traffic control systems, including signal controllers, sensors, and centralized coordination software all have the capacity to be vulnerable to malicious attacks.

Regardless of the objective of the attacks (ransom, sabotage, theft, destruction) when the attacks overcome the defences, the potential consequences range from the purposely malfunction of specific systems, to provoking the network Control Centre to lose some or all control and visibility of the systems, rendering the operation unsafe and creating a disruption. In the worst case causing direct or indirect fatalities.

- **Main causes - What can a cyber-attack be due to?**

A cyber-attack can be caused mainly by one of the following aspects or by a combination of several of them:

Human crime: for a wide variety of reasons, such as political, financial, criminal reasons and wide variety of actors such as terrorists, hacktivists, nation states, criminals, thieves, disgruntled employees, amateurs, unintentional.

Insecure IT infrastructures and networks.

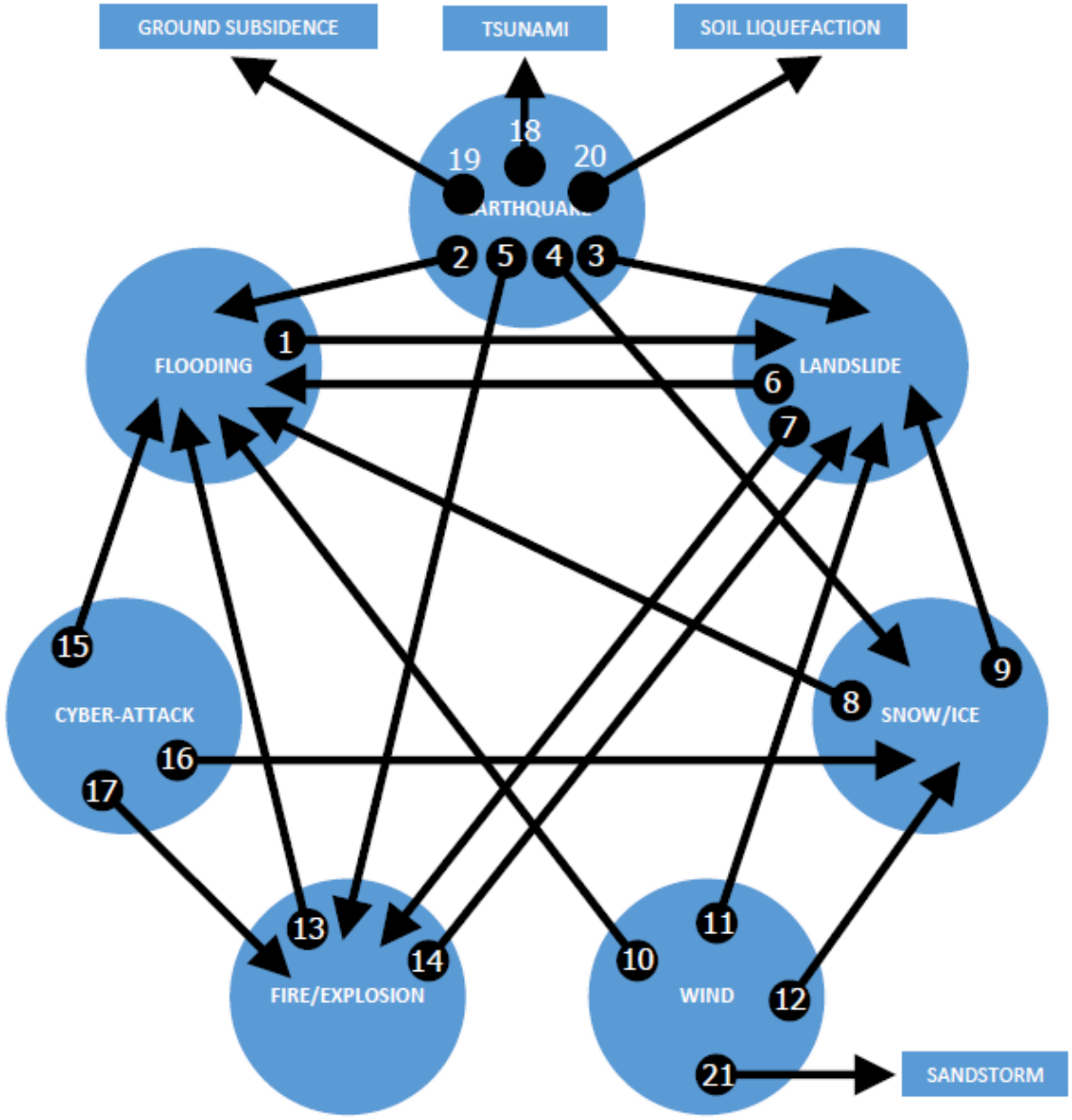


Figure 14. Hazard cause-effect relationships diagram

5.4.2. EXECUTIVE ANALYSIS FROM INFRASTRUCTURE MANAGER

In addition to extreme weather events, transport infrastructure is exposed to a variety of anthropogenic threats, both accidental (such as an unintentional explosion) and intentional, man-made (such as terrorist attacks). These trends, together with growing transport demand and increasing traffic loads, will put further pressure on European infrastructure. It is therefore clear that actions must be taken to make infrastructure more resilient, minimising disruptions, as well as damage and costs, in short, maintaining the best possible level of service.

Task 7.1, aims to implement the framework for the application of the FORESEE Resilience Plans.

This document has been divided into eleven sections. Section 1 includes this introduction and some definitions of key terms used throughout the document. It also presents the most relevant results of other WPs in the FORESEE project, through their linked deliverables, as they are related to the development of the framework and related plans. Then, Section 2 presents the concept of resilience, its fundamental principles, its relation to time and how it can be measured. This section also presents the scope of the FORESEE Resilience Plans.

Section 3 presents the framework that drives the steps to assess the resilience of a system and guides the implementation of the Resilience Plans; Sections 4, 5, 6 and 7 present the different stages of the framework respectively: system definition, hazard definition, resilience assessment and implementation of the Resilience Plans. Section 8 defines a set of use cases covering a wide range of transport infrastructure and risk scenarios. This ensures a holistic analysis as both the framework presented in this report and the Resilience plans in the following WP7 tasks are designed to meet the needs of the wide variety of use cases presented here.

To enrich this report, section 9 provides useful qualitative information on the different hazards considered in FORESEE.

THE CASE OF CALLE 30 RING ROAD

As with all other transport infrastructures, we need to answer the following questions:

- What can we do to better anticipate the impact of an extreme event?
- What can we do to minimise the vulnerability of our infrastructure to extreme events?
- What can we do to restore service quickly?

By answering these questions, and introducing the definition of resilience, we will be addressing the fundamental objective of the Foresee Project, which is to assess the resilient nature of an infrastructure and, as mentioned above, to implement the methodology to ensure the availability of the service at all times during the different phases of the project, construction and operation.

MEASURING RESILIENCE

Resilience can be measured by the level of services provided by an infrastructure system after a hazard event and by the time it takes to return to the pre-event level of service, all referring to the conditions of a base case (in the absence of a hazard event).

There are many different ways to measure the resilience of a transport system; two different procedures have been developed within the FORESEE project:

- Based on traffic simulations.
- Indicator-based.

We consider these two measurement methods as the most applicable to an infrastructure in service, as is the case here.

The first stage of the framework includes identifying which assets, locations and operations should be considered within the resilience assessment, which has already been done by defining the 28 indicators on which we have conducted the study in Calle 30.

Deciding who will participate in the study has a major impact on how the study is conducted and the final results. Interdisciplinary teams are often needed to effectively address the range of issues included in the assessment. Stakeholder participation is also of utmost importance, as they are needed to ensure that the results of the study are used in future decision-making processes.

In our case we have used all the information provided by Madrid Calle 30, the experience of participation in the exploitation phase of the signatory team, and the knowledge acquired throughout the development of the Foresee Project.

The Foresee Project has been applied to the assumption of a cyber-attack, and we consider that it could be applied to all the activities of the operation, taking into account that it is an infrastructure in service.

It is worth recalling how the Foresee Project defines this attack.

"A cyber-attack is any kind of offensive manoeuvre targeting computer information systems, electronically controlled infrastructures, computer networks or personal computing devices. The "hacking hazard" or cyber-attack is a relatively new anthropogenic hazard to be considered in transport infrastructure. The term describes a wide range of human-created security hazards that can directly or indirectly affect the operational, economic and security parameters of the infrastructure. Whether they attack transport modes, the transport network, traffic flow control, revenue, management or communications systems, they can directly affect public safety and critical operations, as well as the operation and organisation of the infrastructure".

In this case, the analysis considered the route of a road with tunnels that suffers a cyber-attack on the infrastructure (and not on the vehicles that use it).

In addition, each of the components that make up the road and the tunnels were analysed to identify the greatest risks. In this case, with regard to the road, the two main direct components considered to be susceptible to this type of threat were: the communication and signalling system; while in the tunnel, three components were identified: the fire protection system, the ventilation and drainage systems.

In our work, we have considered the types of cyber-attacks that can occur, their causes and how to prevent them, as well as their possible effects.

COMPARISON BETWEEN CURRENT SITUATION AND THE POSSIBLE APPLICATION OF THE TOOL

Was this type of analysis made before FORESEE? How it was made?	This analysis has not been performed

How does FORESEE improve the results/analysis previously made?	It introduces the concept of resilience and the calculation procedures for its evaluation
How does this FORESEE result improve your infrastructure's management	This tool will determine the resilience of the infrastructure, and the capacity to respond to extreme incidents.
If it was not made, How does this FORESEE result improve your infrastructure's management ?	It provides objectivity to response capacity, which supports the results for third parties, especially for administrations. From a technical point of view, we will be able to obtain a resilience value for each of the critical elements, and as a whole
What cost/resource efficiencies you expect these tools/results to have on your day-to-day business? (e.g. 10%-20% decrease in working hours over the first year; reduction of maintenance costs (20%-25%), Return on Investment (ROI) – 10-15%, increase in productivity 25-30%)	It is difficult to assess the individual contribution of each tool, in this case the "Plans Based on use cases, risk scenarios and 7.1 impact analysis", but it will undoubtedly reduce infrastructure management costs, increasing its capacity. response to extreme events. Only by obtaining a 5% reduction in costs, we would be facing a substantial advance.

CONCLUSIONS

D7.1 includes the framework that will serve, on the one hand, as a tool to drive the steps to assess the resilience of a transport system to an extreme event and, on the other hand, to guide the implementation of the FORESEE Resilience Plans according to the results of the resilience assessment, which basically coincide with the criteria that we have applied in the drafting of our reports throughout the successive stages, and which we specify in the following documents:

- Description of the scenario caused by a cyber-attack on Madrid Calle 30 control systems and associated response (see Annex 4).
- Socio-economic analysis, impact on traffic and alternative routes following the interruption of service due to a cyber-attack on Madrid Calle 30 (see Annex 3).
- Recommendation of measures to be adopted, evaluation and implementation of these measures for the risk of cyber-attack on the control centres of the Calle 30 infrastructure (see Annex 5).
- Description of scenario and impact on Traffic: Practical Case.

We believe that the following phases, which include the participation of those responsible for the infrastructure, can enrich everything that has been developed so far in the Foresee Project.

5.5. DESIGN, CONSTRUCTION AND REMEDIATION PLANS (D7.2)

5.5.1. SUMMARIZE OF THE TOOL

In Deliverable D7.1, resilience was characterized using the following four principles, which are: **robustness** (i.e.: the ability to absorb shocks and keep operating), **resourcefulness** (i.e.: the ability to manage a disruption as if unfolds), **rapid recovery** (i.e.: the ability to get back to normal as quickly as possible) and **adaptability** (i.e.: the ability to absorb new lessons that can be drawn from past events).

The objective of this deliverable is to present a design resilient aware approach based on **performance criteria**, which will allow evaluating the functionality of a transport infrastructure under different **risk scenarios**, in order to set different performance objectives during and after an extreme event, according to the needs of the community and stakeholders.

In order to be able to analyse the variation in performance during an extreme event, performance measures are needed. Since resilience is a combination of service quality and recovery time during and after a hazard event, the following performance metrics have been defined:

> **Performance Levels:** this parameter encompasses both the level of damage observed in the infrastructure after a hazard event and the level of service that the system is able to provide (e.g.: fully operational, partially closed, etc.).
>
> **Recovery time:** this parameter represents the period of time needed to restore the service to a desired level. It can typically range from hours to months.

The proposed performance-based design approach consists of setting objectives for these two measures (performance level and recovery time). Nevertheless, setting performance objectives is only meaningful if the level of hazard against which they are being set is also specified. For this reason, **three hazard levels** have been defined: **routine, design and extreme** and performance objectives will be established for those hazard levels.

In this document, a methodology has been developed to objectively assess the criticality of a route. The methodology consists of a separate assessment of the following four criteria (which encompass the above-mentioned factors in section 5.2).

- **Criterion 1: Operational and economic relevance.**
- **Criterion 2: Access to critical infrastructure.**
- **Criterion 3: Access to essential services.**
- **Criterion 4: Presence and suitability of alternative routes.**

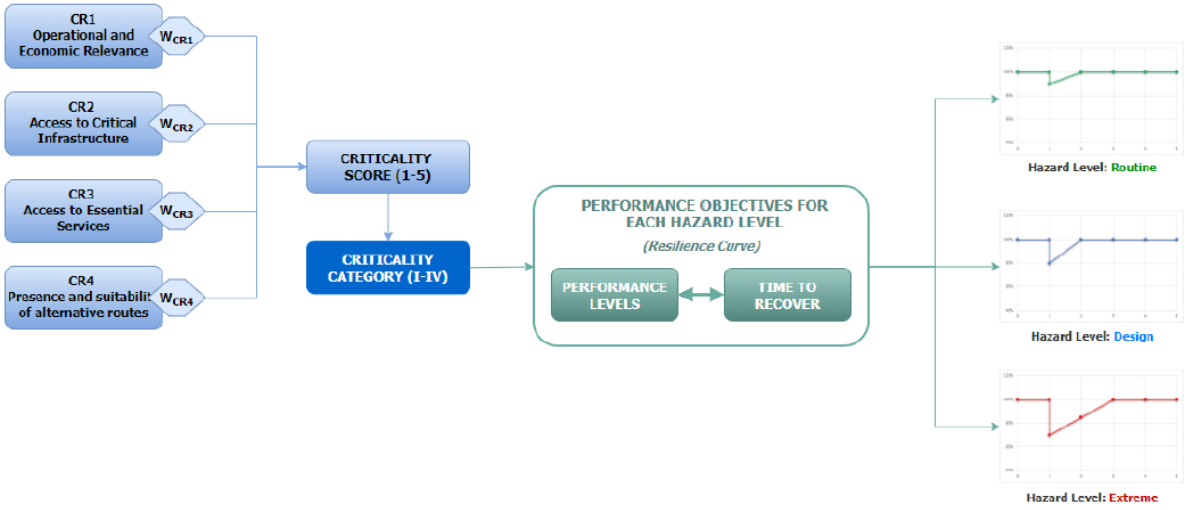


Figure 15. Assess Methodology Developed

EVALUATION OF CRITERION CR1 (OPERATIONAL AND ECONOMIC RELEVANCE)

a) Traffic volume and composition

Complete the following information to obtain a score for factor (a):

Traffic composition:		
Number of vehicles travelling per day	625.000,00	veh/day
% vehicles travelling per work	90,00	%
% vehicles travelling per leisure	10,00	%
Number of vehicles travelling per work per day	562.500,00	veh/day
Number of vehicles travelling per work per day	62.500,00	veh/day
Amount of goods travelling per day	6.250,00	veh/day
Characteristics of the route		
Length	6,00	km
Average speed	65,00	km/h
Costs associated:		
Cost of work time	0,33	€/veh/min
Cost of leisure time	0,20	€/veh/min
Cost for goods	2,00	€/min/truck
Total costs associated	429.576,92	10^3€

The total costs obtained is then compared to the following ranges shown in the table below. Category A is equivalent to a motorway-type road category, while Category D is equivalent to a minor accesss. The reference values of these ranges are obtained based on the number of vehicles usually defined for this hierarchy multiplied by the different costs defined by the users in the previous step.

Category	A	B	C	D	E
Range cost (€)	(> 22102,15384615 38)	(22102,15384 61538 - 12398,769230	(12398,7692 307692 - 4380)	(4380 - 1718,307692307 69)	(< 1718,30769 230769)
Score	5	4	3	2	1

Suggested Score for Factor (a)	5
Adopted Score for Factor (a)	5

EVALUATION OF CRITERION CR1

b) Additional transport modes

Select one of the following answers to obtain a score for factor (b):

Does the route provide additional transport modes? (Select only **one** option)

No.	☑
Yes, pedestrians and/or cyclists.	☐
Yes, pedestrians and/or cyclists, and rail/road.	☐

Suggested Score for Factor (b)	1
Adopted Score for Factor (b)	1

c) Population of linked places

This factor is scored according to the following population reference ranges:

Population (10^3 hab)	> 100	100 - 40	40 - 10	10 - 1	< 1
Score	5	4	3	2	1

Population of linked places	3.500.000,00	hab

Suggested Score for Factor (c)	5
Adopted Score for Factor (c)	5

CR1 - Results

Factors	*Score*	*Weight*
(a) Traffic volume and composition	5	0,66
(b) Additional transport modes	1	0,15
(c) Population of linked places	5	0,19

Suggested Score CR1	4,4
Adopted Score CR1	**4,4**

EVALUATION OF CRITERION CR2

Complete the following inventory of critical infrastructures, indicating whether they are nationally / regionally / locally relevant

Critical Infrastructures inventory	Relevance	Quantity
Water and waste water utilities		
There is no critical infraestructures along the M30.		
	National	0
	Regional	0
	Local	0
Energy		
There is no critical infraestructures along the M30.		
	National	0
	Regional	0
	Local	0
Transport		
Madrid Airport		
	National	
	Regional	3
	Local	3
Telecommunications services		
There is no critical infraestructures along the M30.		
	National	
	Regional	
	Local	

Is it an evacuation route? Yes

CR2 - Results

Suggested Score CR2	5
Adopted Score CR2	5

EVALUATION OF CRITERION CR3

Please, indicate whether the route provides access to any of the following services:

Hospital	☐	Retail stores	☐
Shelters	☐	Hardware stores	☐
Large age-care facilities	☐	Construction resources	☐
Ambulance operations	☑	Supermarkets	☐
Fire Station	☑	Schools	☐
Police Station	☑	Post office	☐
Route for emergency Operations	☐	Major industry	☐
Utility control centres	☐	Power plants	☐
Telecom centres	☐		

CR3 - Results

Suggested Score CR3	4
Adopted Score CR3	**4**

EVALUATION OF CRITERION CR4

Please, indicate whether the route provides access to any of the following services:

a) Presence of an alternative route	Yes
b) Likelihood of the alternative route being affected by the same hazard	Low
c) Capacity of the route to absorb additional traffic volumes	Low
d) Detour Length	High

CR4 - Results

Suggested Score CR4	3
Adopted Score CR4	**3**

CRITICALITY EVALUATION

Finally, the criticality of the route is assessed based on the score obtained for each criteria:

Criteria	Score	Weight
CR1. Operational and economic relevance	4,4	0,25
CR2. Access to Critical Infrastructures	5	0,25
CR3. Access to essential services	4	0,25
CR4. Alternative routes	3	0,25
CRITICALITY SCORE	4,10	

HAZARD LEVELS

In this page, user can select a hazard and define the return period of the event to be in each of the hazard levels: routine, design and extreme.

HAZARD 1

CYBER-ATTACK	Routine	Design	Extreme
Return Period of the event (years)	50	300	2500
Probability of being exceeded in 50 years (%)	63,58	15,38	1,98

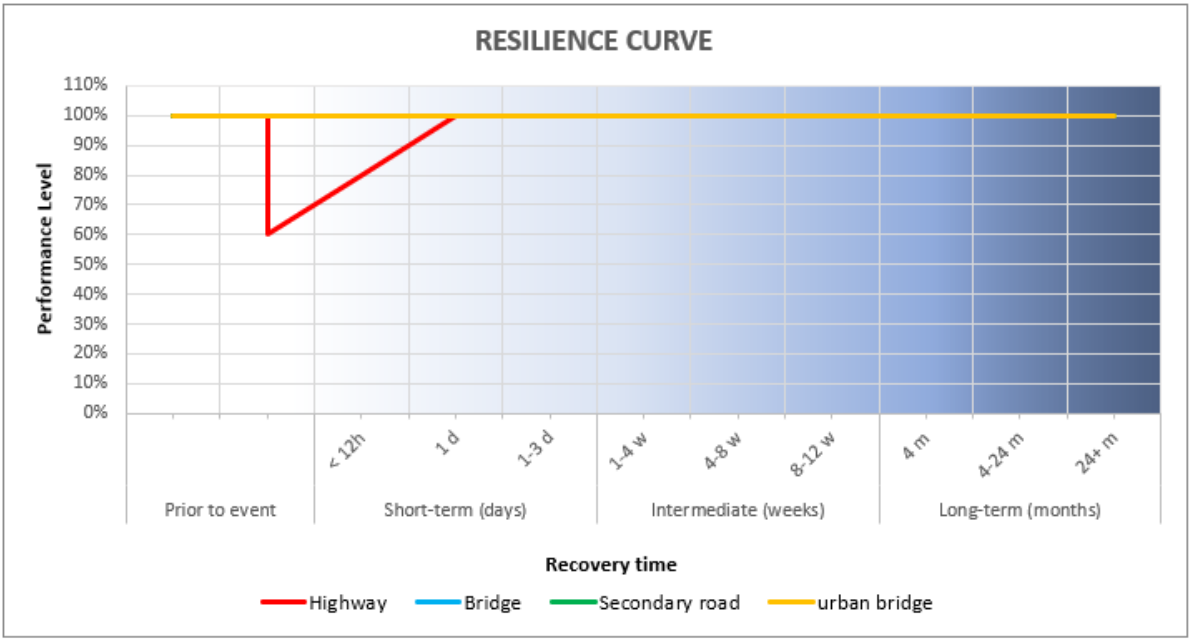
PERFORMANCE-BASED DESIGN - RESILIENCE CURVE

HAZARD

Hazard Type	**CYBER-ATTACK**
Hazard Level	**Extreme**
Return Period of the event (years)	2500
Probabiilty of being exceeded in 50 years (%)	1,98

PERFORMANCE OBJECTIVES

	TRANSPORT INFRASTRUCTURE		DESIRED PERFORMANCE LEVELS								
			Short-term			Intermediate			Long-term		
			Days			Weeks			Months		
	Description	Category	0-12h	1 d	1-3 d	1-4	4-8	8-12	4	4-24	24+
1	Highway	IV	60%	80%	100%						
2	Bridge	I									
3	Secondary road	II									
4	Urban bridge	IV									
5											
6											
7											
8											
9											



5.5.2. SUMMARIZE AND RELATED KEY RESILIENCE INDEXES

The main input data is the following:

- Traffic composition (number and type of vehicles)
- Characteristic of the route (length and average speed)
- Cost of travel time
- Additional transport modes
- Population
- Presence of critical infrastructure (energy, water, transportation hubs…)
- Presence of critical services (hospitals, fire station, police stations…)
- Return period of the event and probability of exceedance

The output data are the following:

- Performance level
- Recovery time

Let us remember all the Key Resilience Indexes that were previously selected:

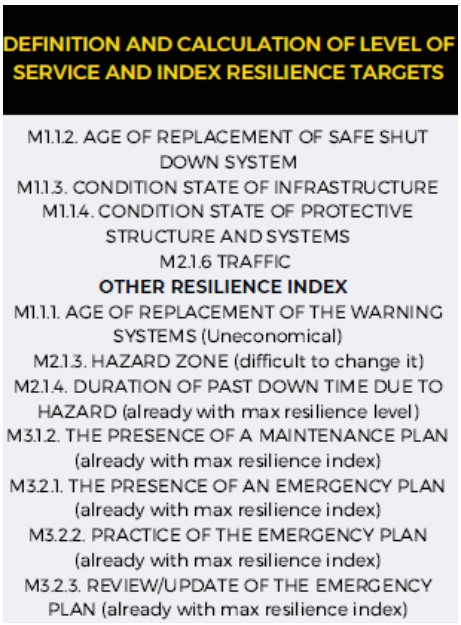


Figure 16. Key Resilience Indexes previously selected

Therefore, we can now see that there is a direct link between this tool and the next previously mentioned KRIs:

- M.2.1.4. Duration of the past down time due to hazard event
- M.3.2.1. The presence of an emergency plan

In conclusion, this tool will give the infrastructure manager a very important information to be able to predict the duration of the closure time after the cyberattack event, and also very useful information to update the emergency and the contingency plans.

5.5.3. EXECUTIVE ANALYSIS FROM INFRASTRUCTURE MANAGER

This work seeks to identify tools to ensure the resilience of infrastructure in its different phases, from the design to the in-service phase.

From the design stage, the infrastructure must be defined in such a way that it meets the expectations of the service for which it is built, and with an optimum resilience capacity in adverse circumstances, whether due to events occurring without the voluntary and criminal intervention of man, or in the case of an affirmative event.

An Excel tool has been defined and developed to assess the criticality of the infrastructure.

This chapter reviews the different stages of the life cycle of an infrastructure, particularly the stages related to the planning and design process, as they are the initial scope of application of the Design, Construction and Recovery Plans to be developed in the current task 7.2 of the FORESEE project.

Madrid Calle 30, which is the case in point, has gone through all the steps foreseen in the existing road regulations in Spain, which are listed in this tool, and which are specified as follows:

Stage 1: Identification of a demand/problem/opportunity.
Stage 2: Planning.
Stage 3: Project design.
Stage 4: Tendering / competition.
Stage 5: Construction.
Stage 6: Operation and maintenance phase.

The Foresee project provides that, from the analysis of the preliminary planning and design and the successive steps, it can be extracted that it is at this stage that the general characteristics of the new infrastructure are defined, such as location, alignment or grade level, which can have a great influence on the final design of the infrastructure components, as well as on the resilience of the infrastructure.

Although in the deliverables carried out so far, the work for Calle 30 has focused more directly on the analysis and assessment of indicators related to the operation phase, other indicators have been included that refer to other processes related to the aforementioned stages, for example when dealing with the age of the infrastructure or the replacement values of the damage suffered in the event of a cyber-attack, the replacement time and others, all of them determining factors for the assessment of the resilience capacity of the infrastructure.

We have considered as decisive those indicators that allow monitoring of compliance with the provisions of current regulations, especially the specifications of RD. 635/2006 on tunnel safety, and 393/2007 on self-protection plans, and Maintenance Contract, indicators subject to constant monitoring through the Quality Plan and both internal and external audits.

Resilience is more than simply preventing a disaster from occurring; resilience involves how a system plans and prepares to withstand and absorb, recover and adapt to disruptions and hazards (Linkov, Trump and Hynes 2019).

This is what our current regulations contemplate, and that in our work on successive deliverables we have put in value, when we have taken into account indicators related to the state of the infrastructure, to the forms of operation, to the existence of contingency plans, and above all to the recommendations to avoid as far as possible the existence of cyber-attack, and, if it is the case, for the restitution of the service in the shortest possible time.

COMPARISON BETWEEN CURRENT SITUATION AND THE POSSIBLE APPLICATION OF THE TOOL

Was this type of analysis made before FORESEE? How it was made?	This analysis has not been performed
How does FORESEE improve the results/analysis previously made?	This tool tries to determine procedures that make possible to guarantee the resilience of the infrastructure in its different phases, from the project to the in-service phase.
How does this FORESEE result improve your infrastructure's management	Detailed analysis of the different processes up to the commissioning of the infrastructure.
If it was not made, How does this FORESEE result improve your infrastructure's management ?	It helps with the audit in the different phases in order to achieve adequate resilience of the infrastructure, with a process that guarantees the achievement of the planned service objectives.
What cost/resource efficiencies you expect these tools/results to have on your day-to-day business? (e.g. 10%-20% decrease in working hours over the first year; reduction of maintenance costs (20%-25%), Return on Investment (ROI) – 10-15%, increase in productivity 25-30%)	As part of the tools that make up the Foresee Project, in this case it is about guaranteeing the service objective, and as has been said repeatedly, achieving a cost reduction of 5% would mean a notable improvement in general results.

CONCLUSIONS

Deliverable 7.2 contains an analysis of the entire procedure proposed in the Foresee Project for the different phases of the infrastructure, relating the decisions and solutions adopted with the expected resilience, expressed in quantitative terms.

In the opinion of those responsible for this report, it is worth considering the importance that resilience has on the reputational character of the infrastructure as such, as it could, after an event, fail to meet the expectations of the expected service, and consequently lose an important part of its usefulness.

5.6. OPERATIONAL AND MAINTENANCE PLANS (D7.3)

5.6.1. EXECUTIVE ANALYSIS FROM INFRASTRUCTURE MANAGER

This deliverable (D7.3) corresponds to the third WP7 report. The objective of this interim report is to provide a suitable framework to increase the safety, efficiency and productivity factors of transport infrastructures (among others) with respect to the occurrence of extreme events (as explained in D7.1) during the lifecycle of the operational phase, by introducing guidelines and a tool form to be developed in the coming months in this task, in order to provide assistance to transport infrastructure stakeholders on how to implement resilience schemes in the Operational and Maintenance plans.

This task will give infrastructure managers and other stakeholders guidelines on how to implement these new or traditional operation and maintenance actions in order to optimise and improve the level of resilience of the infrastructure.
To this end, the General Standards and asset management framework are established in which the relationship between the study of risks, their management and the relationship with the resilience of the infrastructure is defined.
The structure for effective, transparent, systematic and credible risk management consists of three main elements:

- Risk management principles.
- Risk management framework.
- Risk management process.

THE CASE OF CALLE 30 RING ROAD
At different times in the work contributed by our group to the Foresee project, we have indicated that the regulatory axes that define Calle 30's ad-hoc compliance, and in general terms are:

- Royal Decree 635/2006 on safety in tunnels.
- R.D. 393/2007 on self-protection plans.
- Infrastructure Maintenance Contract.

Continuing with the relationship established between these regulations and the Foresee Plan, always with the aim of assessing the resilience of the infrastructure, we can make a parallelism between the Foresee project and which we summarise below, and which have been included in the successive deliverables made by the team.

OPERATING MANUAL (R.D.635/2006)
The basic principle for guaranteeing the safety of a tunnel is an integral approach describing a model by means of which, on the basis of the life cycle, the expected level of safety for its operation is established and maintained.

However, in this integral vision, it is necessary to introduce the interaction of aspects such as the infrastructure itself, the equipment, the behaviour of the tunnel users, the suitability of the operating formula, and the emergency response procedures and capacity.

A proper analysis of tunnel-specific hazards which may affect the health and safety of tunnel users, their property, the tunnel infrastructure or its surroundings is required.

This analysis requires the implementation of efficient safety measures which can be defined by regulatory requirements and/or adapted to the specific conditions of a particular tunnel, in our case Calle 30.
With the establishment and development of standards, international regulations, recommendations and directives, a framework is needed in which all aspects of safety in tunnel operation are taken into account, and in which the following sections can be highlighted:

- Regulations
- Infrastructure and operational measures
- Safety assessment (risk analysis and evaluation)
- Operating conditions
- life cycle of the tunnel (planning, design, construction, commissioning, operation, renewal, upgrading)
- Operating experience
- System conditions
- Emergency procedures (self-protection plan).

It is considered a step forward to include among these sections the preparation and implementation of a Quality Plan, which sets out indicators to check compliance with the objectives set at all times.

CONTENTS OF THE OPERATING MANUAL

This is the specific document for each tunnel, which must be drafted, approved and applied during its operation. Based on its specific characteristics and the assigned safety level, it defines the operating rules, both for operation and maintenance, and the actions to be carried out both in normal operating conditions and in the event of degraded or emergency service.

This is a requirement derived from the application of R.D. 635/2006 on tunnel safety, and its development, as in the Foresee Project, includes all the stages of the infrastructure's life.

The Operating Manual, approved and under permanent revision in Calle 30, requires, as detailed in previous reports, a Maintenance Plan, which includes the sections contemplated in the Foresee Project, although in the latter case with the main objective of knowing the resilience of Calle 30.

Resilience can be measured by the level of service) provided by an infrastructure system after a hazard event and by the time it takes to return to the pre-event level of service, all of them referring to the conditions of a base case (in the absence of a hazard event).

SELF-PROTECTION PLAN (R.D. 393/2007)

The Basic Self-Protection Standard will be applicable to all those activities, centres, establishments, spaces, facilities and premises that may be affected by emergency situations, in this case Calle 30.

The essential requirements set out in the Basic Self-Protection Regulations must be complied with, in accordance with the provisions of Royal Decree 393/2007, for activities, centres, establishments, spaces, facilities or premises that are obliged to have a Self-Protection Plan, Royal Decree 393/2007 of 23 March, which approves the Basic Self-Protection Regulations.

CONCEPT AND PURPOSE

The Self-Protection Plan is the document that establishes the organic and functional framework, with the aim of preventing and controlling risks to people and property and providing an adequate response to possible emergency situations in the area under the responsibility of the owner of the activity, guaranteeing the integration of these actions with the public civil protection system.

The Self-Protection Plan deals with the identification and evaluation of risks, the actions and measures necessary for the prevention and control of risks, as well as the protective measures and other actions to be taken in the event of an emergency.

As we can see, this document, which exists as a legal imperative in Calle 30, follows the steps described in 7.3 of the Foresee Project.

MAINTENANCE CONTRACT

This is the specific document that specifies the Indicators that the Maintenance Services must comply with, as an essential part of the contract with the Administration, in the case of Calle 30 the Madrid City Council.

It determines the procedures to be followed in the predictive, preventive and corrective maintenance plans, setting, among other indicators that have been applied in our study, the replacement time, the response time to events, the costs of the services, and the minimum level of service, an essential element to consider that the objective set for the infrastructure has been met.

QUALITY PLAN

We have mentioned this in our reports, and we consider it an essential element for monitoring the provision of the service in optimal conditions, by verifying compliance with the 28 indicators that we set in our initial deliverables, and which is recorded in the periodic or extraordinary inspections, whether internal or external, and carried out by independent services.

COMPARISON BETWEEN CURRENT SITUATION AND THE POSSIBLE APPLICATION OF THE TOOL

Was this type of analysis made before FORESEE? How it was made?	Only partially, through compliance with current regulations, RD635 / 2006, 393/2007, Quality Plan and Maintenance Contract.
How does FORESEE improve the results/analysis previously made?	In D7.3, the general and specific strategies are designed, in detail, to guarantee the resilience of the infrastructure
How does this FORESEE result improve your infrastructure's management	It facilitates the description of scenarios, the study of the socio-economic impact, and the measures to be adopted before and after the event.
If it was not made, How does this FORESEE result improve your infrastructure's management ?	From the Technical point of view, it offers a complete guide that supposes the exhaustive monitoring of the critical elements to be managed.
What cost/resource efficiencies you expect these tools/results to have on your day-to-day business? (e.g. 10%-20% decrease in working hours over the first year; reduction of maintenance costs (20%-25%), Return on Investment (ROI) – 10-15%, increase in productivity 25-30%)	Due to its overall vision, it will have a positive effect that, as a cautious assessment, we can estimate 5% of each of the aspects mentioned in the question.

CONCLUSIONS

In D7.3, the general and specific strategies are designed, in detail, to guarantee the resilience of the infrastructure, and which basically coincide with the criteria that we have applied in the drafting of our reports throughout the successive stages, and which we can mention in a non-exhaustive manner:

- Description of the scenario caused by a cyber-attack on Madrid Calle 30 control systems and associated response.
- Socio-economic analysis, impact on traffic and alternative routes following the interruption of service due to a cyber-attack on Madrid Calle 30.
- Recommendation of measures to be adopted, evaluation and implementation of these measures for the risk of cyber-attack on the control centres of the Calle 30 infrastructure.
- Description of the scenario and impact on traffic: Practical Case.

5.7. CONTINGENCY PLANS (D7.4)

5.7.1. SUMMARIZE OF THE TOOL

In general, a contingency plan is a set of **alternative procedures and instructions to the normal operating conditions** in the development of the infrastructure's own activity (at a strategic, organizational, operational and personnel level), **so that the operation of this, despite the fact that some of its activities stop doing so due to external conditions**.

In general, a Contingency Plan is a set of **alternative procedures and instructions to the normal operating conditions** in the development of the infrastructure activity itself (at the strategic, organizational, operational and personnel level**), in a way that allows the operation of this, despite the fact that some of its activities stop due to an internal or external accident**.

The main function of a Contingency Plan is the continuity of infrastructure operations. In general terms, any contingency plan includes four stages:

1. Evaluation
2. Planning
3. Testing
4. Execution

Specific action procedures

This point will be of great importance in the Contingency Plan since it is where all the response procedures to any emergency are collected. All the actions to be developed and the team in charge of carrying out those actions will be defined to give a quick and effective response to emergencies.

These procedures will have a general basis with similar characteristics based on the following points:

I. Emergency Detection and Alert.
II. Alarm Mechanisms.
III. Emergency response mechanisms.
IV. Evacuation and / or Confinement.
V. Provision of First Aid.
VI. Ways of receiving external aid.

As part of D7.4, there has been developed a study to check the performance of each kind of infrastructure user when they have to evacuate it.

Objective
The purpose of this study is to be able to determine the impact of these factors on human behavior in order to obtain an adequate interpretation of the evacuation phenomenon and to be able to improve communication systems based on the reaction time of users.

During the execution of the project, the impact of the following factors will be analysed:

- Disruption in evacuation routes by blocking certain exits, to modify user routes.
- Movement of the occupants right after the alarm is activated and until they decide to look for an exit.
- Process for choosing evacuation routes known, unknown and indicated.
- Characteristics of the occupants, emphasizing multiculturalism.

The evacuation process is developed in four phases, each with an execution time, which can vary depending on a multitude of conditions. The sum of these partial times will determine the total evacuation time:

1. Detection time: time it takes to discover and confirm an emergency (**tD**).
2. Alarm: The time of emission of the corresponding messages by the means of public address, lights or sounds encoded (**tA**).
3. Reaction: Time elapsed since the evacuation decision is communicated until the first person begins to leave (**tR**).
4. Evacuation time: The proper evacuation time begins when the first person begins to use the evacuation routes to move to a safer place until the last arrives to this place(**tE**).

The present study aims to **analyze the factors of the communication strategies that directly affect the alarm time (tA) and consequently the reaction time (tR), in order to arrive at a more effective communication plan in the process evacuation**.

Scenario 1

The development of the first scenario is intended to represent the fire caused by a dangerous goods lorry burning with a maximum power of 100MW on the study section. For this first scenario it is considered that the planned ventilation pattern works correctly and both the extraction station upstream (17NC20) and downstream (17NC50) of the fire zone operate in extraction mode at full capacity. As explained in previous sections, each extraction station is able to move a flow rate of 450m3/s through the simultaneous use of three fans of 150m3/s each.
In a fire calculation, the light extinction coefficient, , is the key parameter used to calculate both

Scenario 2

The development of the second scenario is intended to represent the fire caused by a dangerous goods lorry burning with a maximum power of 100MW on the study section. For this second scenario it is considered that the planned ventilation pattern does not work correctly and the extraction station downstream (17NC50) has one of the fans damaged so the station is not able to extract at full capacity.

Scenario 3

The development of the second scenario is intended to represent the fire caused by a dangerous goods lorry burning with a maximum power of 100MW on the study section. For this third scenario

it is considered that the planned ventilation pattern does not work correctly and the extraction station downstream (17NC50) has two of the fans damaged so the station is not able to extract at full capacity. In this case the upstream station extracts with a Q=450m3/s and the downstream station extracts with a Q provided by two of the three fans =**150m3/s.**

Scenario 4

The development of the second scenario is intended to represent the fire caused by a dangerous goods lorry burning with a maximum power of 100MW on the study section. For this fourth scenario it is considered that the planned ventilation pattern does not work correctly and there is a total failure in all the ventilation system of the tunnel, there is no extraction and the smoke is able to propagate freely through the tunnel.

The analysis of these four scenarios has been repeated for the case of a fire power corresponding to a LIGHT GOODS VEHICLE.

FIRE SIMULATION:

The purpose of this section is the definition of dynamic contingency plan concept that is capable of optimally integrating the capabilities provided by advanced fluid dynamic fire simulation models and evacuation simulations in order to optimize the response and efficiency of the agents involved in resolving the emergency.

Threats and critical scenarios in road tunnels
Currently the main inputs required by a fire safety engineering approach to fire safety for new tunnel fires and to develop an assessment of existing protection measures in existing tunnels are design fire and fire scenario analyses.

- Design fire scenario for ventilation design and assessment
- Design fire scenario for evacuation analysis
- Design fire scenario for thermal action on structures
- Design fire scenario for the safety of tunnel fire equipment
- Design fire for work on tunnel construction, refurbishment and maintenance

Scenario 1

The development of the first scenario is intended to represent the fire caused by a dangerous goods lorry burning with a maximum power of 100MW on the study section. For this first scenario it is considered that the planned ventilation pattern works correctly and both the extraction station upstream (17NC20) and downstream (17NC50) of the fire zone operate in extraction mode at full capacity. As explained in previous sections, each extraction station is able to move a flow rate of 450m3/s through the simultaneous use of three fans of 150m3/s each.
In a fire calculation, the light extinction coefficient, , is the key parameter used to calculate both visibility and light obscuration. The fundamental value to be reflected by the unidemensional model will correspond to the evolution of the air opacity, as a function of the extinction coefficient (k), along the tunnel and as a function of time. **It is considered that k = 0.4 m-1 is a critical value of extinction coefficient for smoke in a road tunnel.**

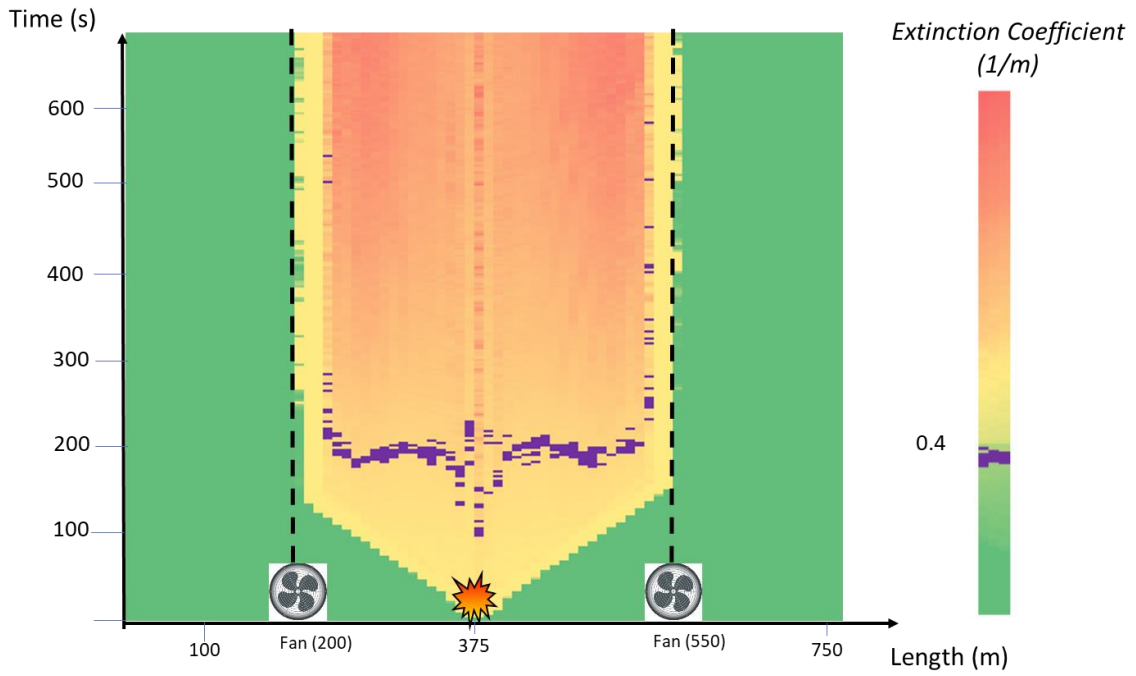


Figure 17. Fire Simulation - Scenario 1

In the previous graph it can be seen there is no propagation of the smoke to other sectors of the tunnel, the extraction capacity of both stations are enough to guarantee the isolation of the sectors, the values of the extinction coefficient remain under 0,4 until **210 seconds** in the section of the tunnel simulated.

The one-dimensional models for temperature, CO and CO2 concentration were also analyzed.

Scenario 2

The development of the second scenario is intended to represent the fire caused by a dangerous goods lorry burning with a maximum power of 100MW on the study section. For this second scenario it is considered that the planned ventilation pattern does not work correctly and the extraction station downstream (17NC50) has one of the fans damaged so the station is not able to extract at full capacity. In this case the upstream station extracts with a Q=450m3/s and the downstream station extracts with a Q provided by two of the three fans =**300m3/s.**

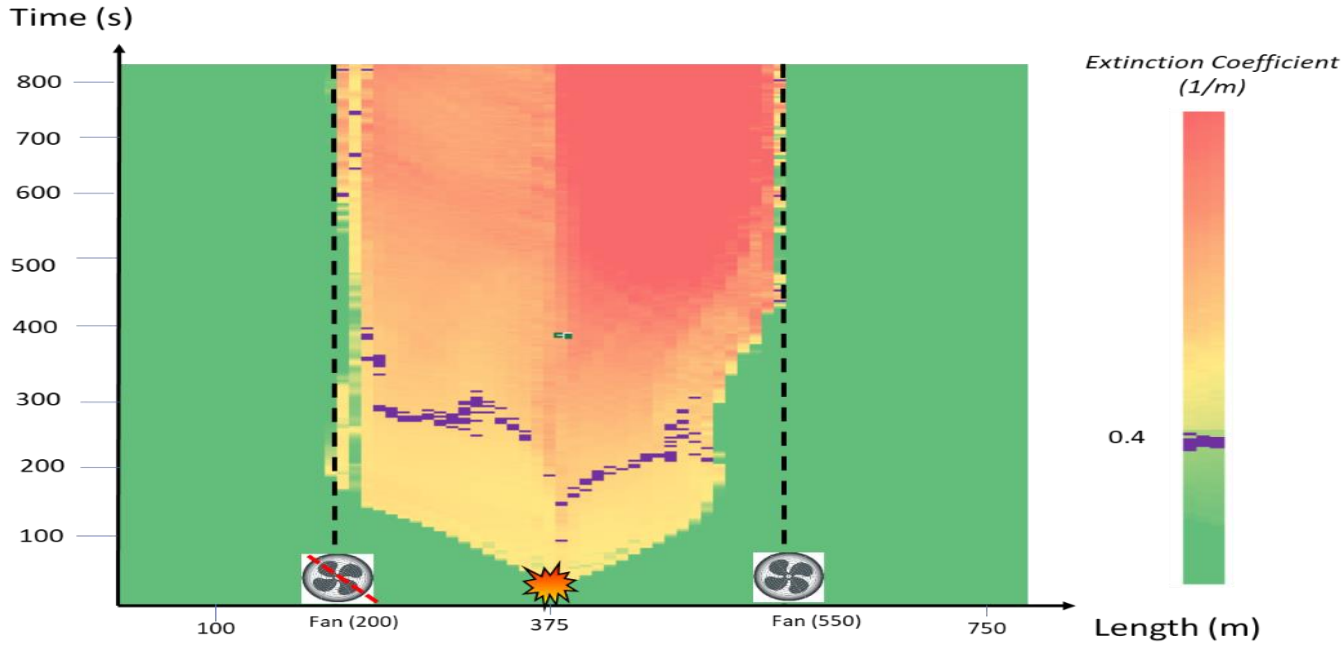


Figure 18. Fire Simulation - Scenario 2

In the previous graph it can be seen there is no propagation of the smoke to other sectors of the tunnel, the extraction capacity of both stations are enough to guarantee the isolation of the sectors, downstream the fire the values of the extinction coefficient remain under 0,4 until **190 seconds**, and upstream the fire, the extinction coefficient values start to overcome 0,4 at 200 seconds in the section of the tunnel simulated. As expected, the smoke tends to accumulate upstream the fire because the extraction station has more power than the downstream one because of the fan failure in this scenario.

The one-dimensional models for temperature, CO and CO2 concentration were also analyzed.

Scenario 3

The development of the second scenario is intended to represent the fire caused by a dangerous goods lorry burning with a maximum power of 100MW on the study section. For this third scenario it is considered that the planned ventilation pattern does not work correctly and the extraction station downstream (17NC50) has two of the fans damaged so the station is not able to extract at full capacity. In this case the upstream station extracts with a Q=450m3/s and the downstream station extracts with a Q provided by two of the three fans =**150m3/s.**

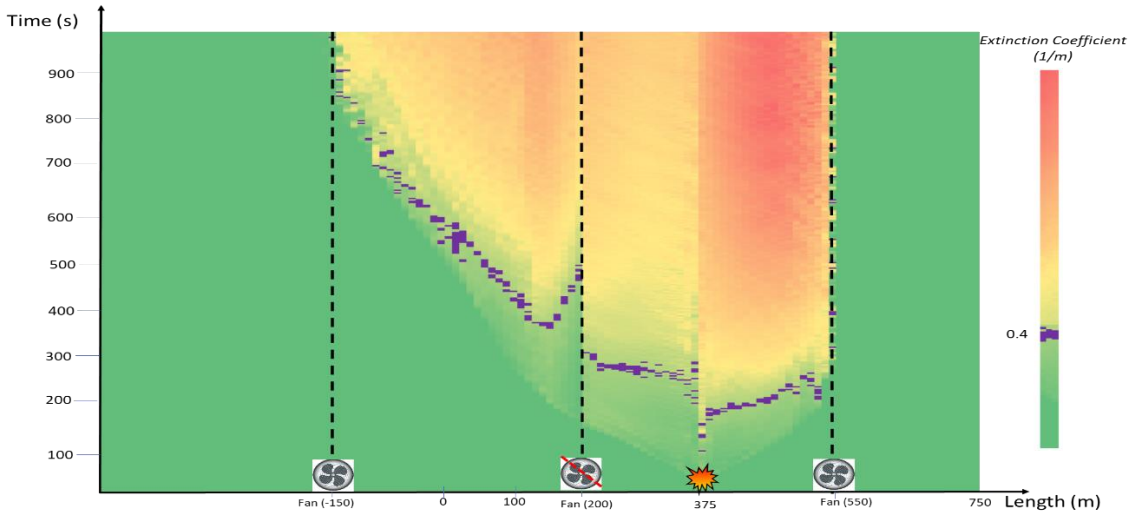


Figure 19. Fire Simulation - Scenario 3

In the previous graph it can be seen there is propagation of the smoke to other sectors of the tunnel, the extraction capacity of both stations are not enough to guarantee the isolation of the sector downstream, downstream the fire the values of the extinction coefficient remain under 0,4 until 300 seconds, and upstream the fire, the extinction coefficient values start to overcome 0,4 at **180 seconds** in the section of the tunnel simulated. As expected, the smoke tends to accumulate upstream the fire because the extraction station has more power than the downstream one because of the fan failure in this scenario.

Smoke propagation to the sector downstream of the analysed sector starts to exceed the permissible visibility values (0.4) after 400 seconds.

The one-dimensional models for temperature, CO and CO2 concentration were also analyzed.

Scenario 4

The development of the second scenario is intended to represent the fire caused by a dangerous goods lorry burning with a maximum power of 100MW on the study section. For this fourth scenario it is considered that the planned ventilation pattern does not work correctly and there is a total failure in all the ventilation system of the tunnel, there is no extraction and the smoke is able to propagate freely through the tunnel.

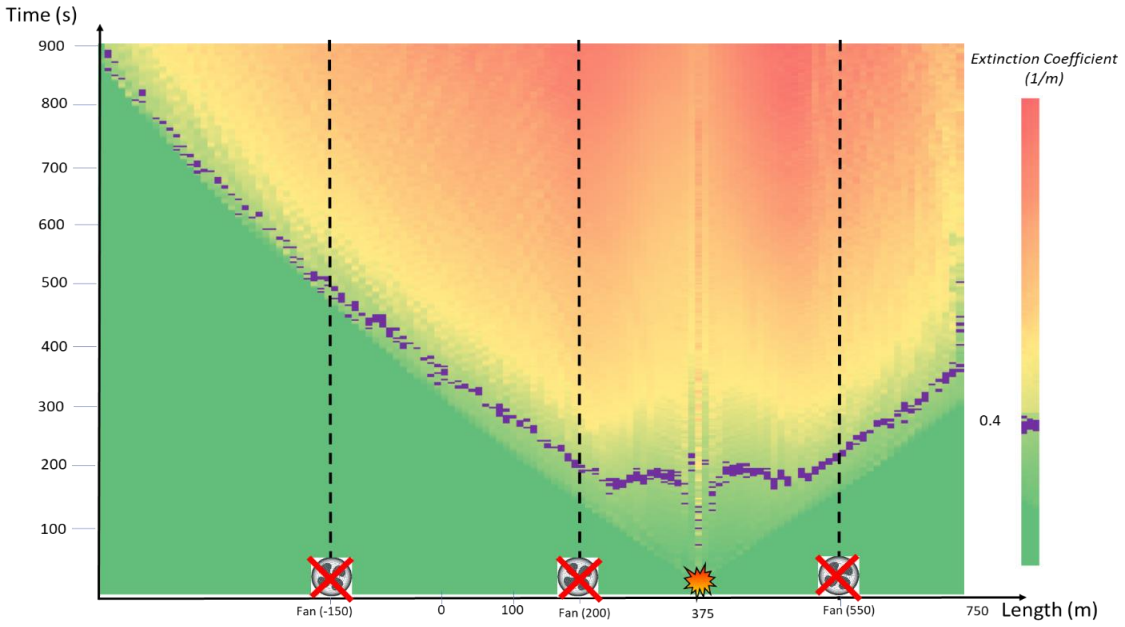


Figure 20. Fire Simulation - Scenario 4

The total failure of the tunnel ventilation causes the free propagation of smoke along all tunnel sectors, the extinction coefficient remains under 0,4 until **160 seconds** in the analyzed sector. Smoke propagation to the sector downstream of the analyzed sector starts to exceed the permissible visibility values (0.4) after 200 seconds.

The one-dimensional models for temperature, CO and CO2 concentration were also analyzed.

The analysis of these four scenarios has been repeated for the case of a fire power corresponding to a LIGHT GOODS VEHICLE.

STUDY FOR MADRID CALLE 30 RING ROAD – EVACUATION AND DYNAMIC THREAD SIMULATION

Scenarios

For the development of the threat scenarios, an analysis has been carried out of the type of vehicles that are most abundant in the surroundings of the Madrid tunnels. This is why it has been decided to carry out three fire scenarios that are detailed below:

- Scenario 1: Car

  The first fire scenario considers a car burning inside the tunnel, for this case a maximum peak of 5-6 MW will be considered.

- Scenario 2: Light goods vehicle (LGV)

The second fire scenario considers an LGV burning inside the tunnel, for this case a maximum peak of 30 MW will be considered.

- Scenario 3: Dangerous goods vehicle

  The third fire scenario considers an LGV burning inside the tunnel, for this case a maximum peak of 100 MW will be considered.

In order to make the self-protection plans more dynamic, the main factors that characterise the fire and make evacuation difficult in the infrastructures described are analysed in detail by means of specific graphs such as the one shown below: D7.4 Management and contingency plans.

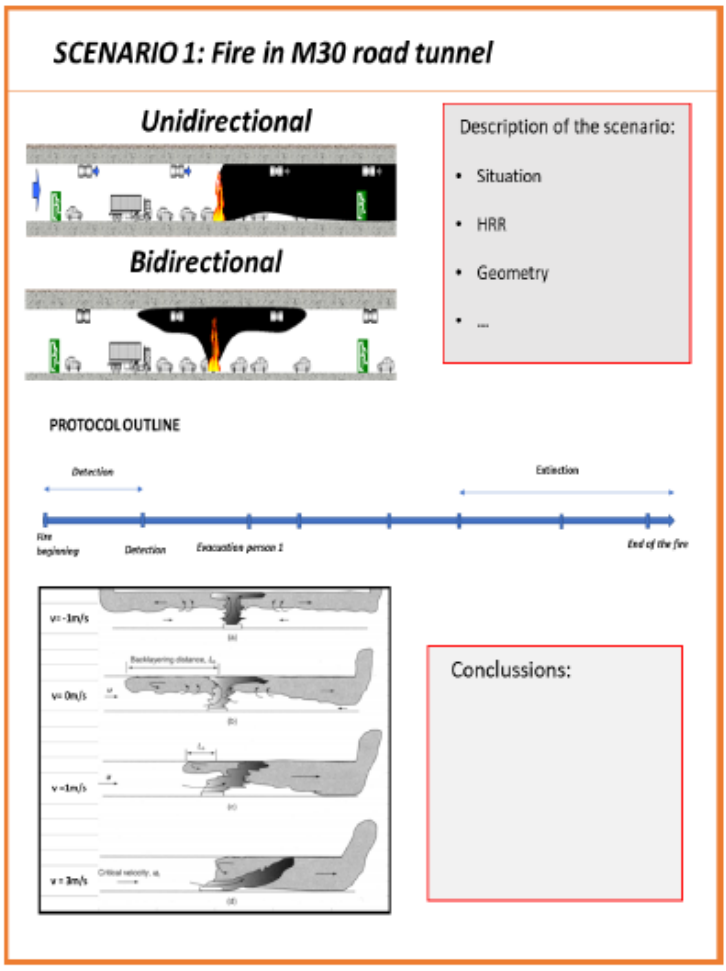


Figure 21. Main factors characteristics analysis

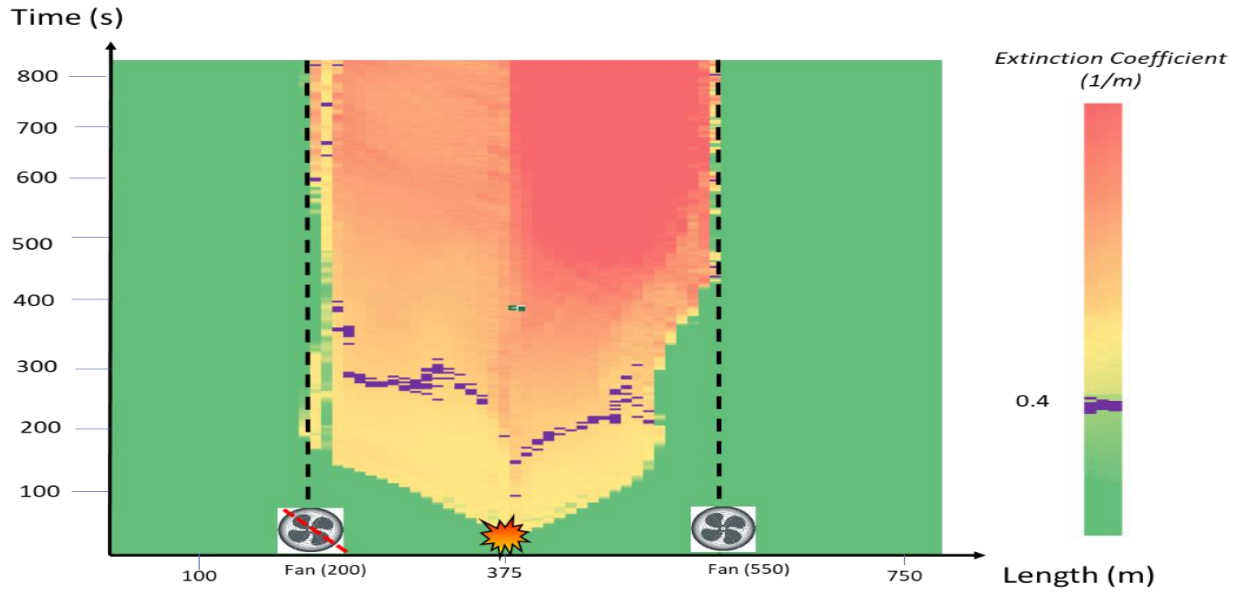


Figure 22. Fire Scenario

On the x-axis is the kilometer of the tunnel where the fire begins, and on the y-axis the time in seconds. With this graphic the people involved in the emergency can see the behavior of the key fire aspects at any time at any point of the tunnel. In addition, you can introduce the main milestones of the emergency protocol such as detection, turning on the fans, start of evacuation...

By overlapping the previous graph with the graphs that define the evolution of the evacuation over time, we will have detailed and precise information about the physical phenomenon of the fire and its evolution over time, as well as its interaction with the evacuation process of the people in the infrastructure at any time and at any point of the infrastructure.

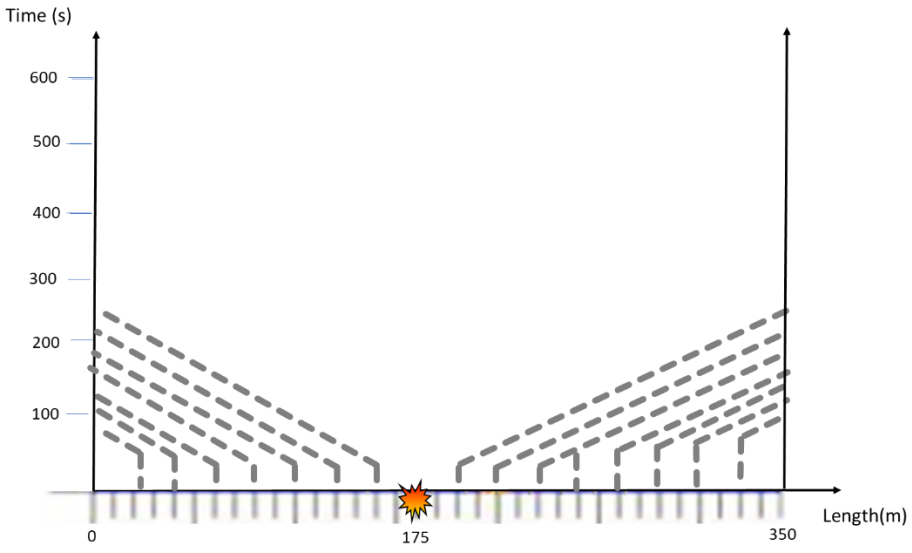


Figure 23. Physical phenomenon of fire. Evolution over time.

In accordance with the conclusions obtained in the fire analysis section, it is considered that the evacuation graphs will be integrated with the one-dimensional model obtained from the extinction coefficient for each scenario, as this is the most restrictive variable in terms of time of all those analyzed. For the development of the combined one-dimensional models that integrate both the fluid dynamic results with the results of the evacuation process, the length of the section has been limited to the analyzed sector located between two extraction wells.

HGV

SCENARIO1

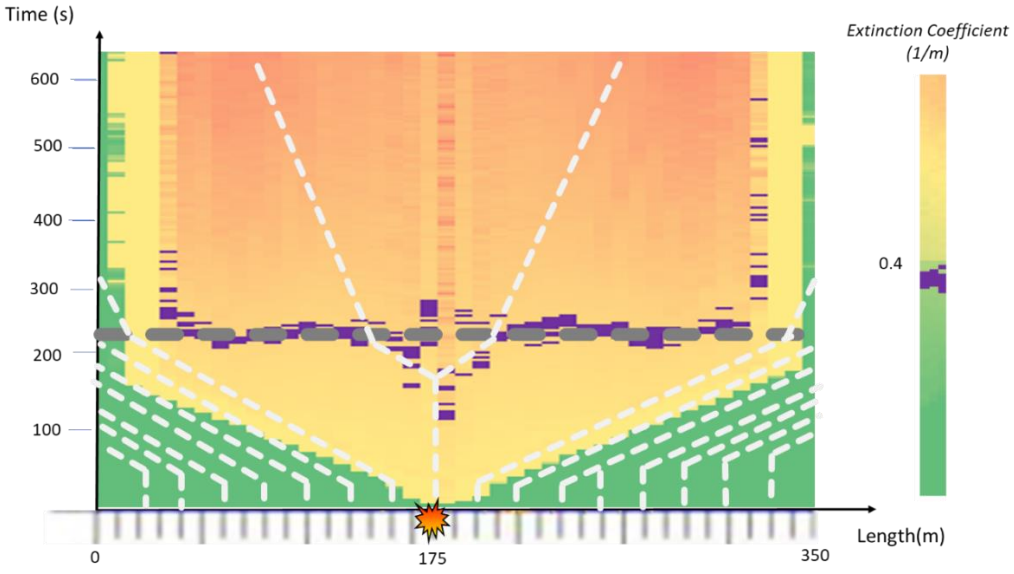


Figure 24. HGV - Scenario 1

SCENARIO2

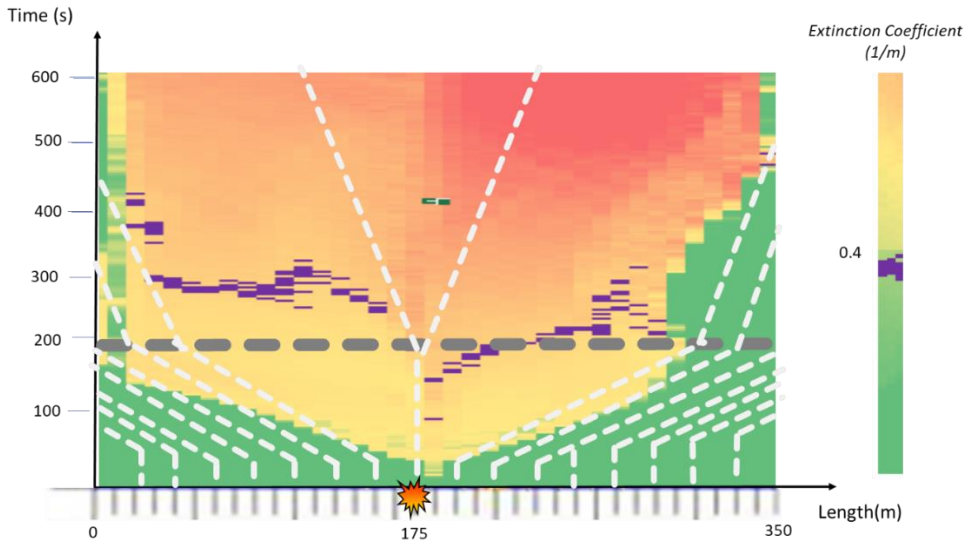


Figure 25. HGV - Scenario 2

SCENARIO 3

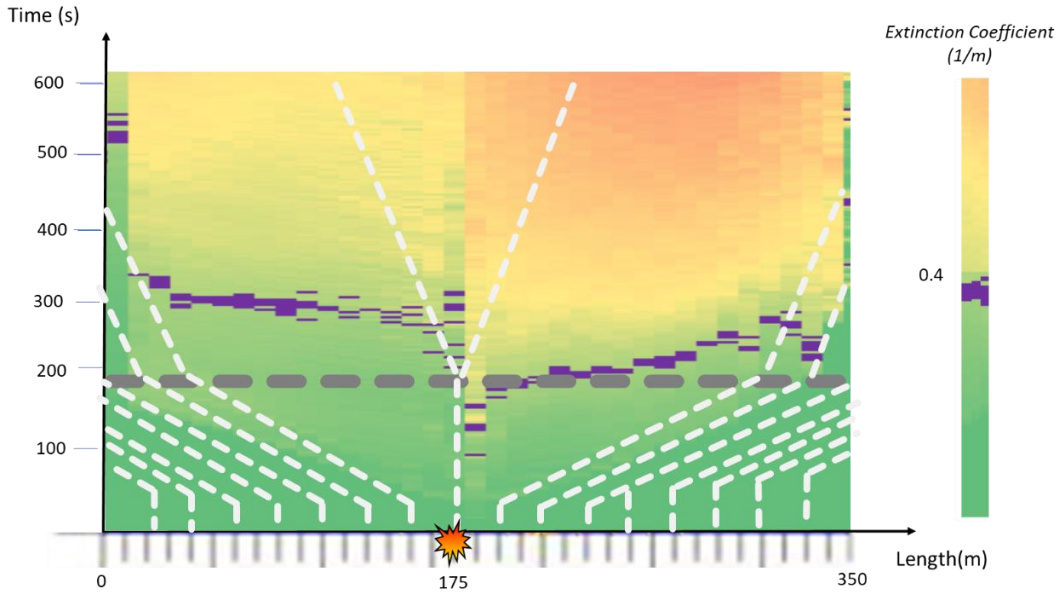


Figure 26. HGV - Scenario 3

SCENARIO 4

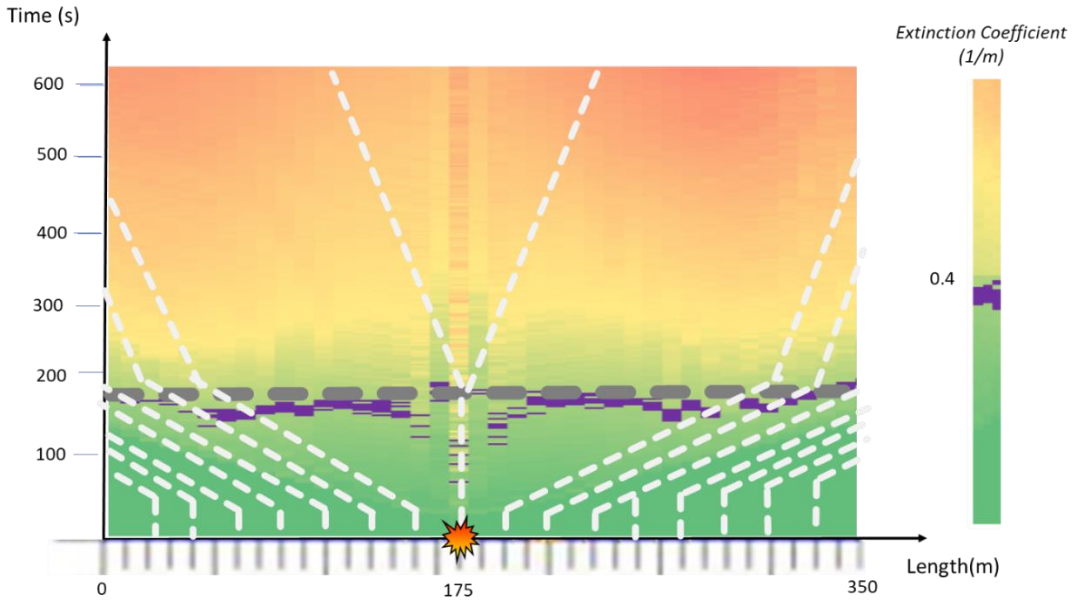


Figure 27. HGV - Scenario 4

LGV

SCENARIO 1

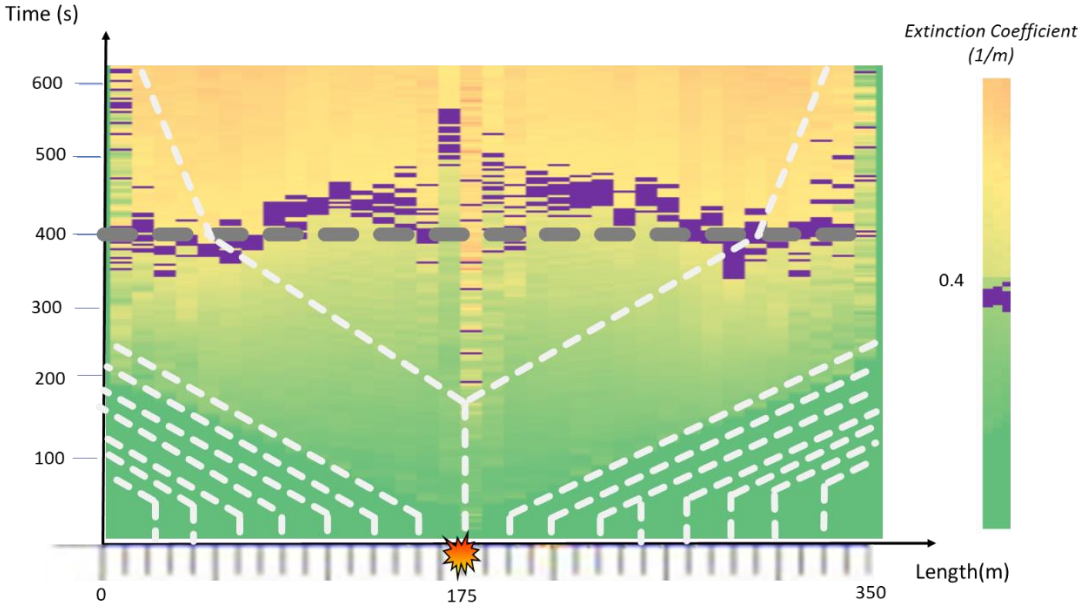


Figure 28. LGV - Scenario 1

SCENARIO 2

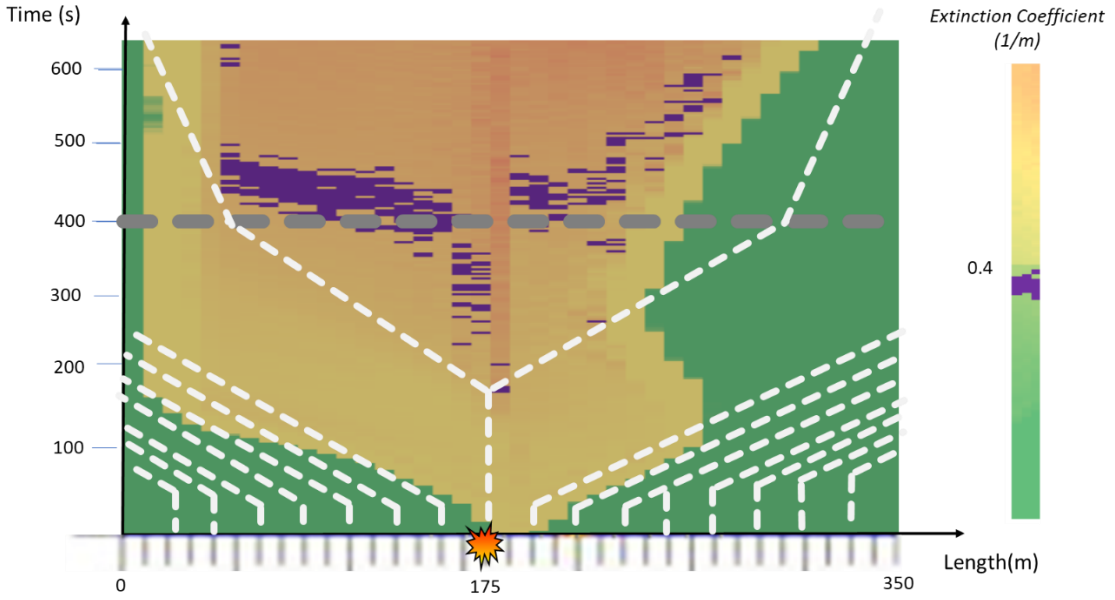


Figure 29. LGV - Scenario 2

SCENARIO 3

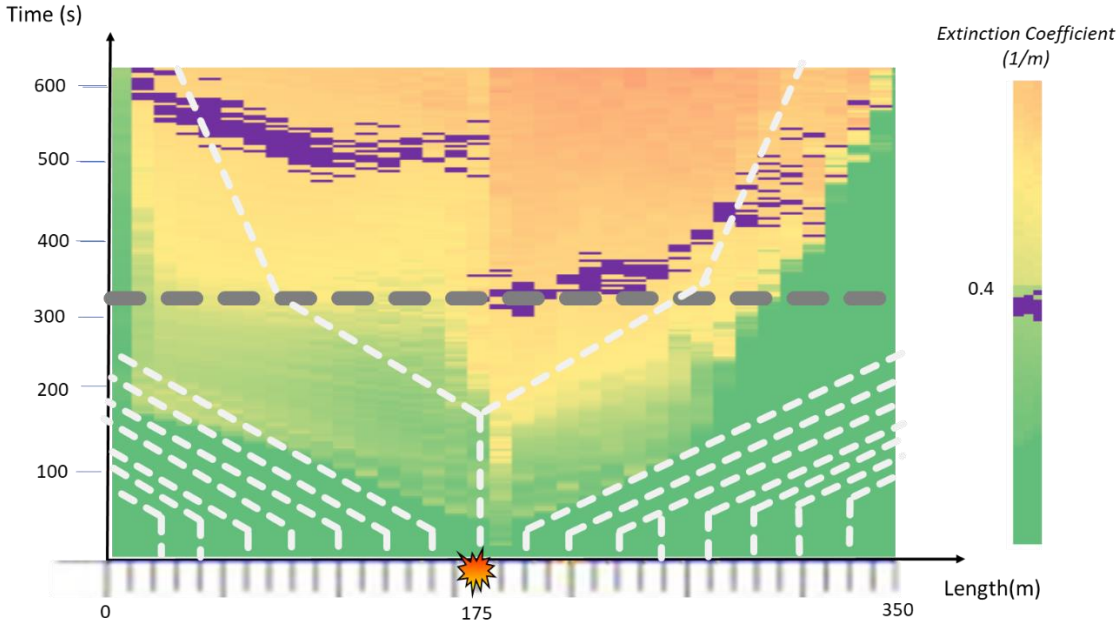


Figure 30. LGV - Scenario 3

SCENARIO 4

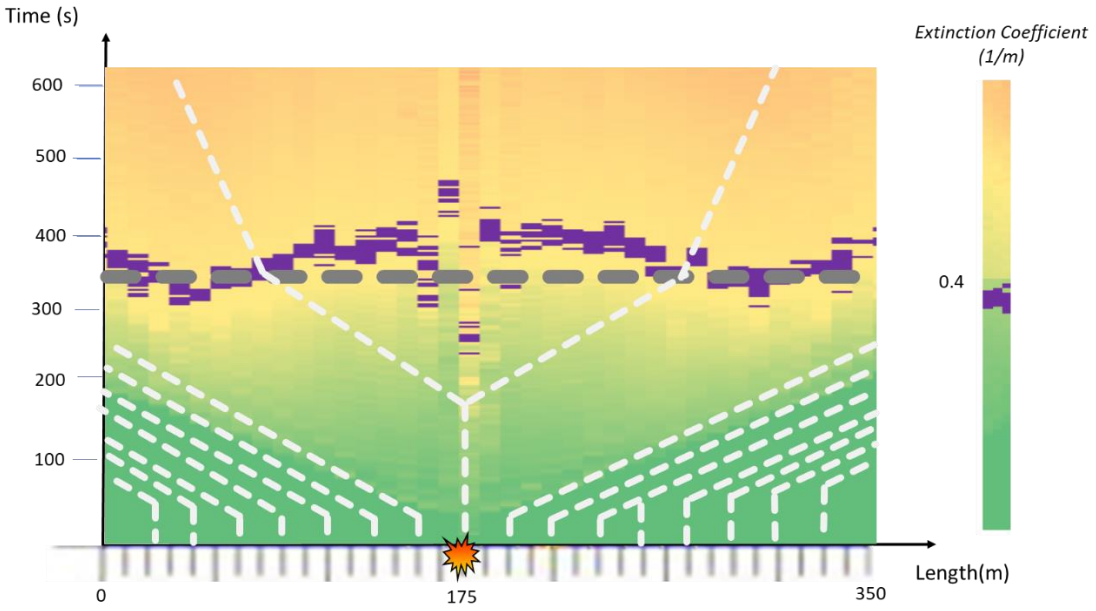


Figure 31. LGV - Scenario 4

5.7.2. CONCLUSIONS AND EXECUTIVE ANALYSIS FROM INFRASTRUCTURE MANAGER

ANALYSIS OF TOOLS

According to different studies, most of the accidents in infrastructures are due to collapses and catastrophes originated in the operation and maintenance phase, so it makes sense to work and delve into these last phases of the life cycle of the structure in order to reduce the economic, social and environmental impact.

It is in this phase that deliverable 7.4 focuses on, and specifically to define the Management and Contingency Plans, from the point of view of the resilience of the infrastructure.

FORESEE aims to transform real static emergency and contingency plans into dynamic plans adapted to more variables. It seeks to incorporate the benefits of moving to "dynamic" approaches that consider the timing of the threat, people and the evolution of alerts, in order to optimise emergency protocols and communication strategies.

It defines the Contingency Plan as a set of procedures and instructions at the strategic, organisational, operational and personnel levels that arise in the face of an extraordinary situation that puts the continuity of the infrastructure at risk.

This is how the Foresee Project defines and understands the Contingency Plan, which to a large extent coincides with what is defined in RD 393/2007 as the Self-Protection Plan.

THE CASE OF CALLE 30 RING ROAD

At different times in the work contributed by our group to the Foresee project, we have indicated that the regulatory axes that define the ad-hoc compliance of Calle 30, and in general terms are:

- Royal Decree 635/2006 on safety in tunnels.
- R.D. 393/2007 on self-protection plans.
- Infrastructure Maintenance Contract.
- Quality Plan.

In the development of these regulatory axes, and generally in parallel with the knowledge provided by this deliverable 7.4, abundant documentation has been provided in order to establish the procedures and instructions which, based on its organisational structure, define the operations established as a response when an extraordinary event, whatever its origin, may put the continuity of the infrastructure at risk.

For this purpose, a large part of the structured knowledge mentioned in deliverable 7.4 has been used, which undoubtedly represents an important compendium of all the knowledge that exists to date on the subject of emergency forecasting and action in the event of emergencies.

The drafters of this report have actively participated in such decisive aspects for the success of the Contingency Plan, such as the review of the existing one in Calle 30, the training of the Operational Staff, and the execution of the drills that make up the ideal scenario for analysing the validity of the operational measures established in the Self-Protection Plan.

In our opinion, the Foresee vision contained in the sociological study, section 3, where aspects to be taken into account for the management of emergency situations in transport infrastructures are developed, is a contribution that distinguishes it from the plans and tools used so far.

In the following chapters, in summary, in addition to developing different approaches for resolving emergency situations, in our opinion, it concludes with a proposal for lines of research for future studies, always with the objective of improving the integrity of the Contingency Plan, permanently maintaining integral safety, and maintaining the infrastructure in service in the best possible conditions.

Special mention should be made of the chapter dedicated to communication, an aspect in which much remains to be done, and the detailed studies and experiences on evacuation, which, in both cases, have inspired the Calle 30 Contingency Plan, which is the Self-Protection Plan required by current regulations.

COMPARISON BETWEEN CURRENT SITUATION AND THE POSSIBLE APPLICATION OF THE TOOL

Was this type of analysis made before FORESEE? How it was made?	Partially, with the preparation of the Self-Protection Plan, required by RD393 / 2007
How does FORESEE improve the results/analysis previously made?	It aims to transform real static emergency and contingency plans into dynamic plans adapted to more variables. It is about incorporating the benefits of moving to "dynamic" approaches
How does this FORESEE result improve your infrastructure's management	With a set of procedures and instructions at a strategic, organizational, operational and personnel level that arise in an extraordinary situation that puts the continuity of the infrastructure at risk
If it was not made, How does this FORESEE result improve your infrastructure's management ?	The nine sections that make up D7.4, represent an exhaustive compendium of the applicable regulations, the knowledge and the experience acquired in the matter, which together with the rest of the tools, guarantees the management of extreme events.
What cost/resource efficiencies you expect these tools/results to have on your day-to-day business? (decrease in working hours over the first year; reduction of maintenance costs, Return on Investment (ROI), increase in productivity)	We consider that the timely management of extreme events can improve, as a whole, by 20%, based on saving resolution time and reducing associated costs.

CONCLUSIONS

In D7.4, the general and specific strategies are designed, in detail, to guarantee the resilience of the infrastructure, from the point of view of the provision of Management and Contingency Plans, which basically coincide with the criteria we have applied in the drafting of our reports throughout the successive stages, and which we specify in the following documents:

- Description of the scenario caused by a cyber-attack on Madrid Calle 30 control systems and associated response.
- Socio-economic analysis, impact on traffic and alternative routes following the interruption of service due to a cyber-attack on Madrid Calle 30.

- Recommendation of measures to be adopted, evaluation and implementation of these measures for the risk of cyber-attack on the control centres of the Calle 30 infrastructure.
- Description of the scenario and impact on traffic: Practical Case.

A new "dynamic contingency plan" concept has been defined, that is capable of optimally integrating the capabilities provided by advanced fluid dynamic fire simulation models and evacuation simulations in order to optimize the response and efficiency of the agents involved in resolving the emergency.

Specifically, this dynamic contingency plan aims to improve the traditional approach by enhancing the following aspects:

- Respond more quickly and efficiently to any contingency and emergency caused by fire that involves risk to human life, health, the environment and the project, handling the emergency with responsibility, speed and effectiveness.
- Use the capabilities of advanced fluid dynamic modeling to establish in an improved way the immediate measures and/or actions to follow in case of disasters and/or disasters caused by fire, minimizing the risks to workers, third parties, facilities and infrastructure associated with the Project.
- Generate adequate channels to transfer the necessary information to ensure timely internal communication between the personnel who detected the emergency, the personnel in charge of controlling it and the personnel responsible for the project; as well as timely external communication for the necessary coordination with support institutions.
- Through the integration of advanced simulation models that allow to realistically visualize the consequences of a fire, the aim is to minimize potential risks and/or avoid damages caused by fires and disasters, optimizing technical procedures and safety controls that protect those involved and the active contingency and emergency response brigades.
- Develop fire simulation tools in realistic scenarios that allow for improved control actions before, during and after the occurrence of disasters.
- Continuously training of personnel through lectures, courses, and drills.

5.8. FLOODING METHODOLOGY: D4.10 APPLICATION OF A NEW METHODOLOGY FOR IMPROVING THE ESTIMATION OF FLOODING FRECUENCIES IN CALLE30

5.8.1. INTRODUCTION

Floods are a global problem and are considered the most frequent natural disaster worldwide. They may result into serious socio-economic impacts, causing loss of lives, population displacement, business bankruptcy. As part of the future proofing strategies For RESilient transport networks against Extreme Events (FORESEE) program, the Environmental and Hydraulics Institute "IH Cantabria" come up with a novel methodology for improving the estimation of return periods of flooding events. This innovative procedure aims to provide a better understanding of the true magnitude of disruptive flood events.

With the aid of Calle 30 and Ferrovial Construction, the methodology has been applied to the M-30 motorway in Madrid (Spain) to check its response against low frequency events at two specific locations along the Manzanares River - i. Upstream of "Puente de Toledo" and ii. Upstream of Dam Nº9 where the original design already encountered flooding problems

5.8.2. CASE STUDY – CALLE 30

The proposed methodology has been applied in a study of the Manzanares River in Madrid (Spain). More precisely, this study focusses on the stretch of the river that runs parallel to the M-30 motorway and is affected by the undergrounding works conducted in 2007. Figure 32. Calle 30. Study Location Map, shows the stretch of the Manzanares River under study, starting at "Puente del Rey" and finishing 700 m downstream of "Puente de La Princesa". The picture below also shows the two specific locations where the methodology has been checked.

When looking at the tunnel configuration, one can imagine that any major flooding event might pose major threats to the motorway. A complicated system of pumps, cut walls, storm water detention facilities and flood defenses keep M30 safe and dry for the commonly used 500-yr storm event. However, is that design event truly a 500-yr event?

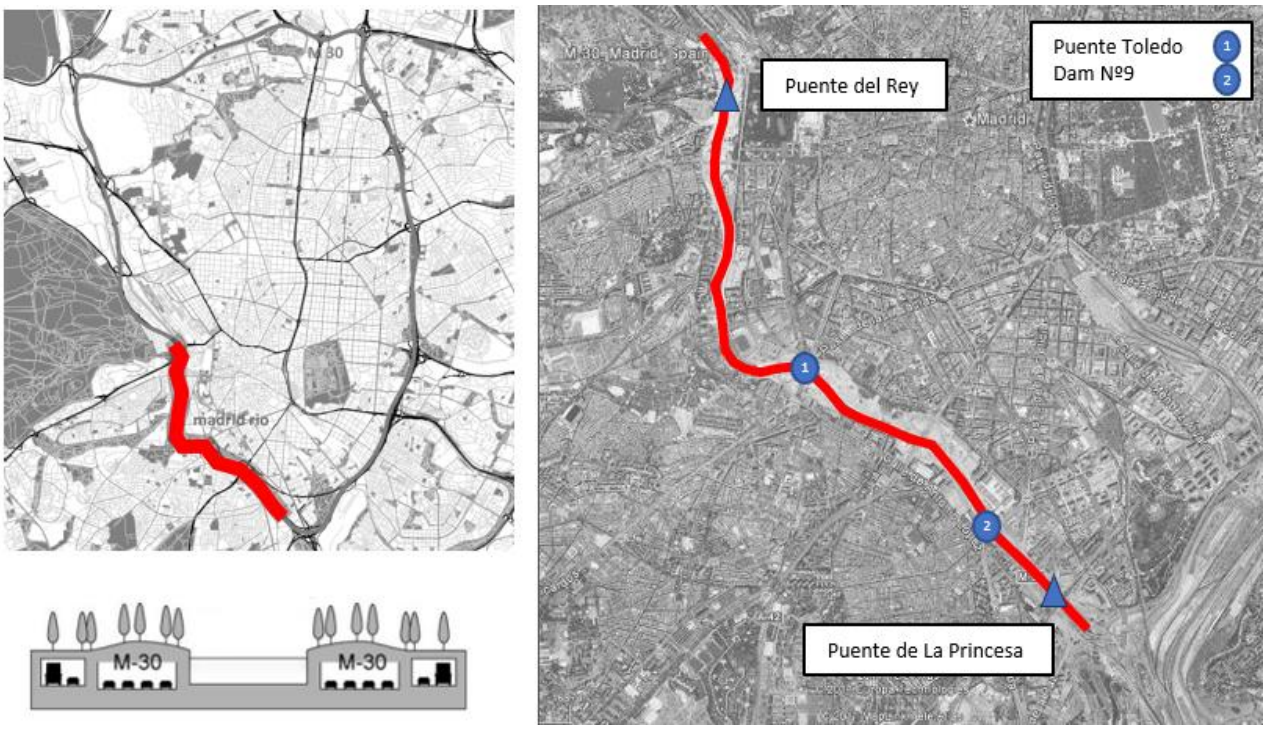


Figure 32. Calle 30. Study Location Map

5.8.2.1. Hydrology Studies

The Manzanares River is a tributary of the Jarama River on its right bank. It runs in a north-south direction, with a total route of about 80 km. The first third of the basin is located in the foothills of the "Sierra de Guadarrama", with a granite substrate covered by coniferous forest masses. The central third sits on tertiary materials, covered by grassland and scrubland, except in Monte de El Pardo, where trees predominate. The lower third is occupied by the urban agglomeration of Madrid and its area of influence, which is partly based on the alluvial river. Most of the land is urbanized, leaving only some green areas covered by vegetation.

The Manzanares contributions are regulated by the Santillana-El Pardo reservoir system with drainage basins of 246.80 km2 and 529.29 km2 respectively. For the purpose of this study, the hydrologic models from the original M30 project were used. Following the original approach, it was assumed that the water surface elevations for both dams were at the spillway elevation when the storm comes. That is, the dams do not help storage any of the extreme events leading to a conservative design of the M30 project.

The figure below represents a sketch of the HEC-HMS model used.

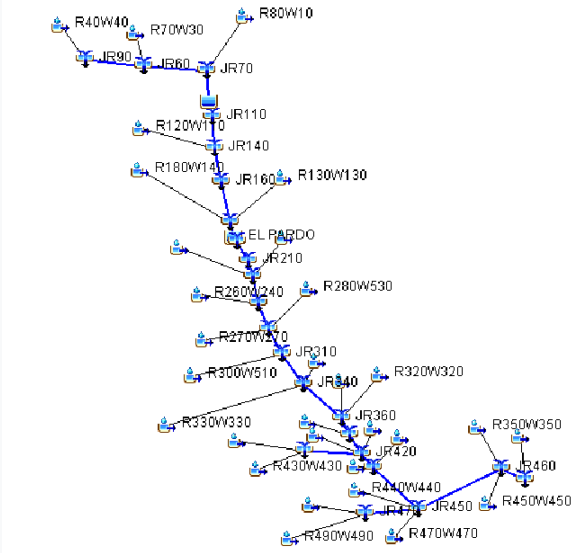


Figure 33. HEC-HMS model of the original M30 project

5.8.2.2. Hydraulic Studies

In most of the section under study, the Manzanares River is channeled by means of a rectangular section 40 m wide formed by masonry walls with a 10: 1 slope and a substantially horizontal bottom. At the end of the water downstream of the section under study, at the height of dam No. 9, the channel section becomes trapezoidal, over a length of 500 m, with 3: 4 slopes. Upstream of the section under study, the channeling also has a trapezoidal section, up to the "Puente de los Franceses".

The channelization works of the Manzanares River were conducted based on the results of the 500-yr event resulting from a HEC-RAS model of the stream. The original M30 project considered the excavation of the riverbed as well as several flood defenses at both margins of the river. Two locations in particular, required extra works: i. Upstream of "Puente de Toledo" and ii. Upstream of Dam Nº9.

The latest available hydraulic model was taken for this study.

5.8.2. PROPOSED METHODOLOGY

The main methodology is based on the methodology proposed in (IH Cantabria, 2020) where the main source of the work is the flow series. In this case, we start from a situation in which we have hourly information on precipitation at the basin's stations. With hourly information at the stations in the basin it is possible to characterize in detail the hyetograph corresponding to the storm events at each station.

Furthermore, by having simultaneous information at all stations, it is possible to simultaneously characterize the correlations between stations. With this information, the stochastic generator can be calibrated to perform the flood analysis.

The stochastic generator is calibrated to reproduce the most important precipitation statistics at each station (mean rainfall, maximum rainfall, event duration, etc.). The generator automatically

reproduces the observed correlations and therefore serves to produce realistic rainfall events at all stations simultaneously.

The generator would be used to produce multiple events (equivalent to several decades or centuries of observations). From this database of events, the most representative events would be selected for dynamic simulation, i.e., for transformation into flood elevation through the hydrological and hydraulic model. Once this dynamic transformation has been carried out, machine learning methods (statistical) are used to calculate the flood level and flow of the remaining cases.

Finally, an extremes analysis is carried out on the flood elevation time series.

The figure below shows an outline of the methodology developed in this study. The following sections will show the analysis carried out in each of the steps defined in the methodological scheme.

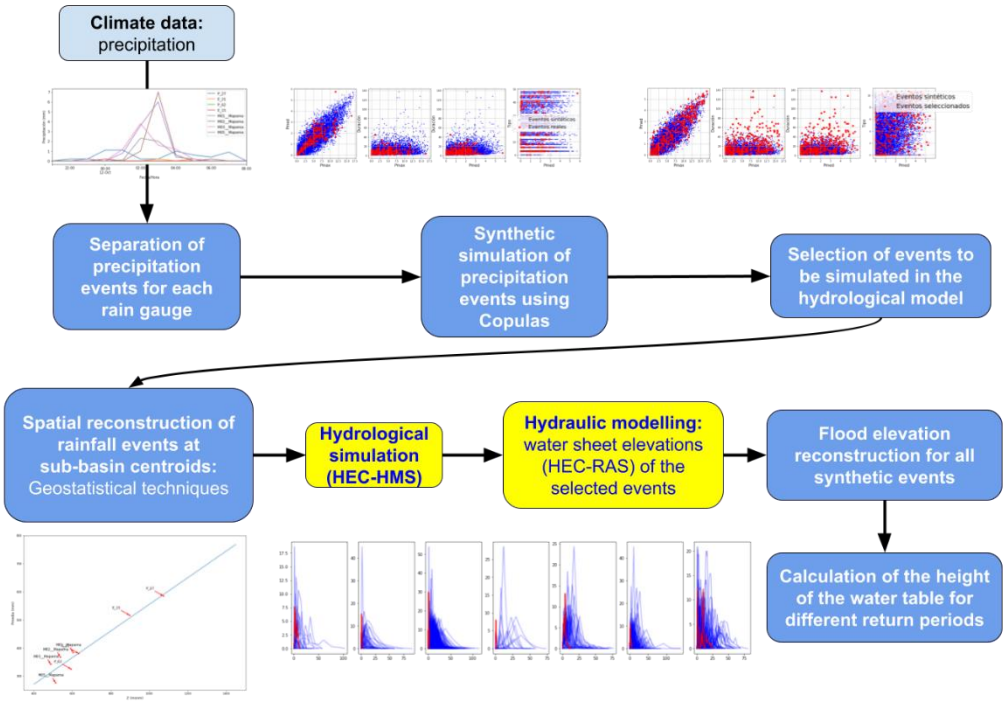


Figure 34. Methodological outline

5.8.3. PRECIPITATION ANALYSIS

In this study, the main analysis is carried out on rainfall, as it is the meteorological variable that has the greatest influence on flooding episodes.

The rainfall data have been provided by the Confederación Hidrográfica del Tajo (CHT) and the Ministerio de Agricultura, Pesca y Alimentación (MAPAMA). CHT data are every fifteen minutes while the MAPAMA data are hourly data. With this temporal resolution it is possible to apply a methodology such as the one proposed in this study, as it allows the detailed identification of rainfall events over time.

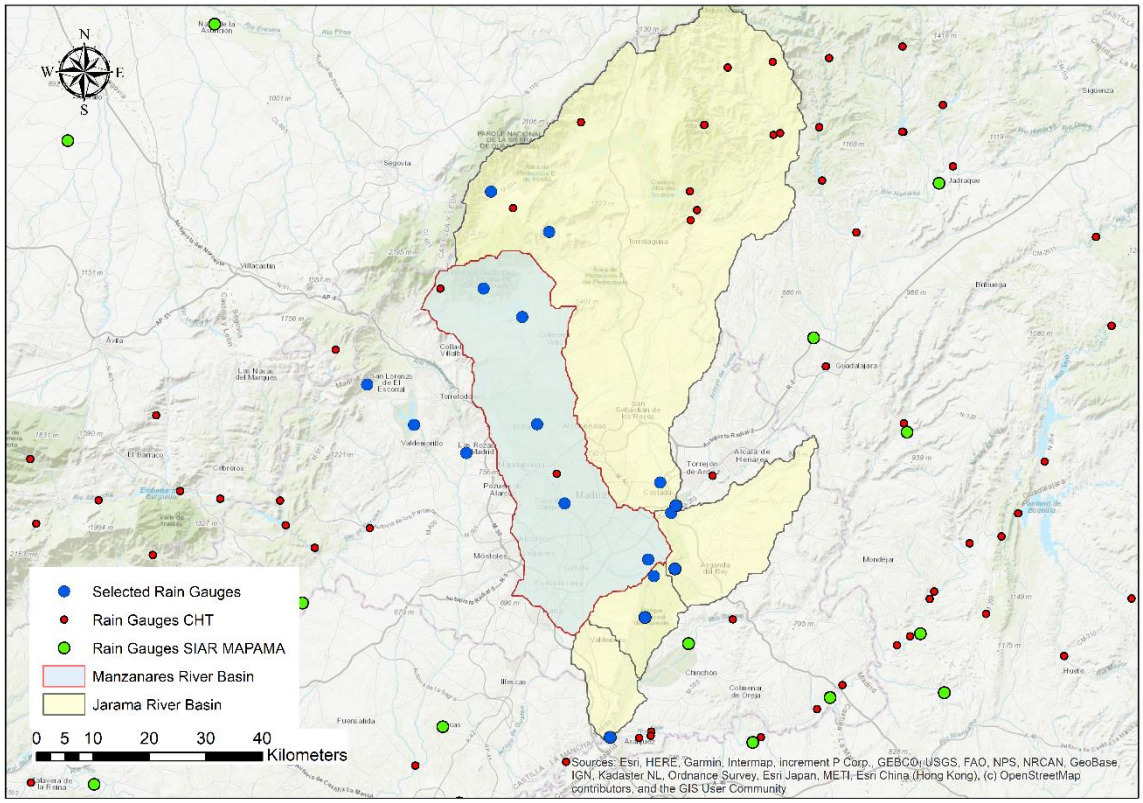


Figure 35. Existing rain gauges

For the analysis of precipitation, data from 17 meteorological stations have been used. The selection criterion is that they are located close to the study basin, have a low percentage of gaps, and have a temporal length of more than 15 years.

Figure 35. Existing rain gaugesshows the geographical location of these stations. The figure also shows the boundary of the study basin. In addition, Table 6. Characteristics of rain gaugesshows the characteristics of the selected stations.

Table 6. Characteristics of rain gauges

	Nº full years	Percentage of gaps (%)	Nº years with data	Nº full months	Nº FULL DAYS	Starting year	Year end
P_27	0	0.24	20	0	6813	2002	2021
E_21	0	0.15	20	0	6874	2002	2021
P_62	4	0.22	20	0	6914	2002	2021
E_15	0	0.20	20	0	6834	2002	2021
AR17	0	0.11	20	0	6898	2002	2021
AR18	0	0.10	20	0	6910	2002	2021
AR19	0	0.16	20	0	6866	2002	2021
E_16	0	0.14	20	0	6873	2002	2021
E_22	0	0.12	20	0	6895	2002	2021
MC02	1	0.10	20	0	6905	2002	2021
P_26	1	0.29	20	0	6778	2002	2021
P_31	0	0.17	20	0	6866	2002	2021
PN23	1	0.26	20	0	6802	2002	2021
M01__Mapama	0	5.86	18	0	6167	2003	2020
M02__Mapama	0	6.41	18	0	6132	2003	2020
M03__Mapama	0	6.45	18	0	6116	2003	2020
M05__Mapama	0	4.42	16	0	5499	2005	2020

Before any use is made of the precipitation data, a quality control and homogenization of the input data has been carried out.

The aim of this process is to ensure that the time series from the different stations represent signals associated with the climate system in the area concerned, and not with other factors (e.g., sensor error, human error, station displacement, change in the environment surrounding the station, etc.).

The process is as follows:

1. Elimination of outliers: outliers are observations that deviate greatly from other records, which arouse suspicions of constituting errors in data collection. To define these outliers, we have taken as a criterion those outliers that exceed 5 times the sample variance.

$$Si\ X_i > 5\,\sigma_n^2\ \ es\ un\ outlier$$

Where $\sigma_n^2 = \frac{1}{n}\sum_{i=1}^{n}\left(X_i - \bar{X}\right)^2$, X_i each of the data, n the number of data and y $\bar{X}$ the mean of the data.

2. Elimination of repeated consecutive data: this control attempts to detect sequences of repeated values over several consecutive days. Persistence of the same value may suggest transcription errors or problems in the case of instruments with electronic data logging, e.g. automatic weather stations. (Estévez et al., 2011).

In the methodology developed in this work it is necessary to spatially reconstruct the precipitation events in points where no data is available. For this reason, the relationship between the altitude at which the meteorological stations are located and the mean annual precipitation is evaluated to determine whether it is possible to use geostatistical interpolation techniques, in which a covariate such as altitude can add information on how precipitation is distributed spatially.
Figure 4 shows that in this area there is a significant relationship between precipitation and altitude, so it can be observed that the precipitation is significantly higher than the altitude.

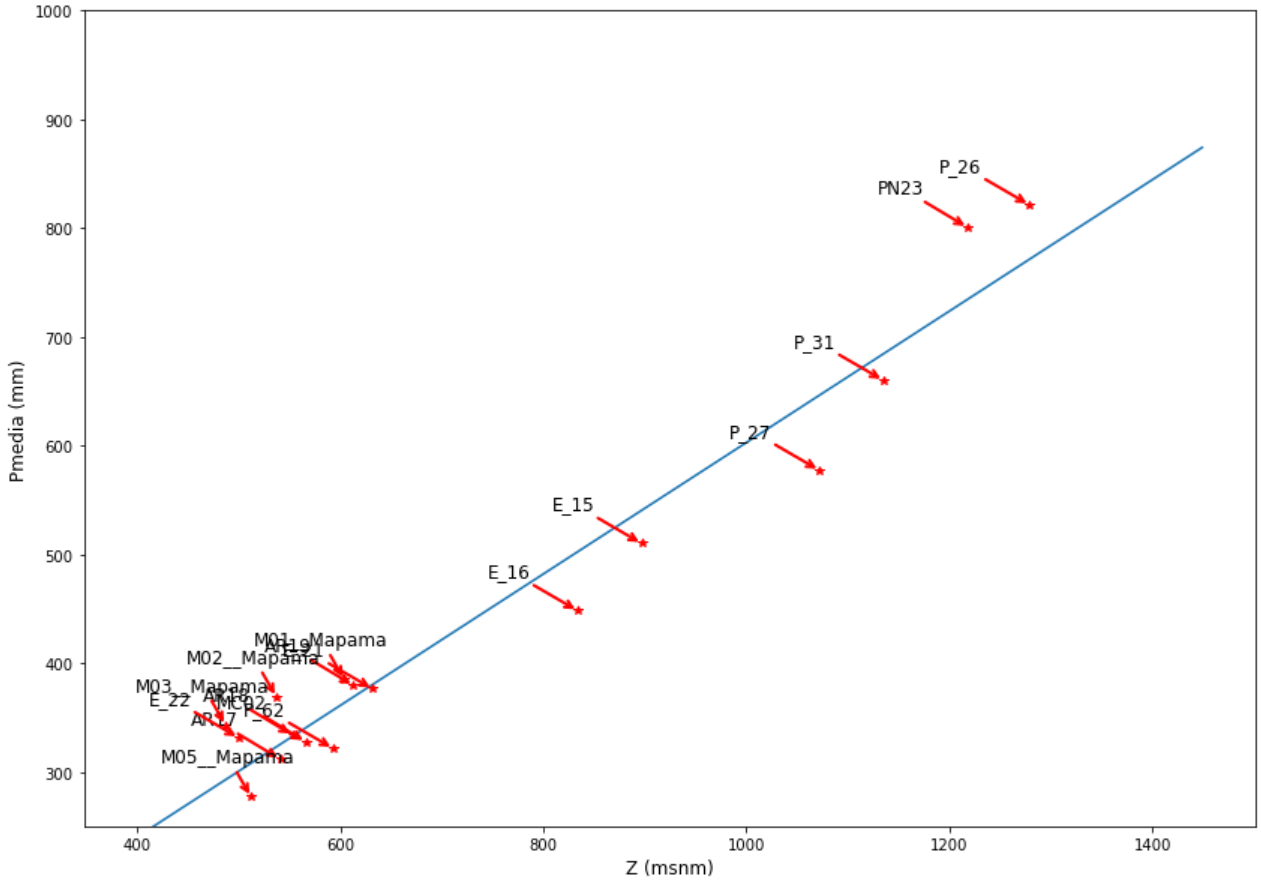


Figure 36. Relationship of precipitation to altitude.

5.8.4. SEPARATION OF PRECIPITATION EVENTS

After having carried out the quality analysis of the selected rainfall stations, we proceed to separate the series into precipitation events. To do this, it is necessary to define a threshold above which a precipitation event is a precipitation event; in this study, 5 mm of maximum precipitation has been considered as the threshold. Once the threshold has been established, it is necessary to resort to simple mathematical operations and programming language techniques based on conditional loops. In this calculation process, the initial and final instants of each of the events that meet the maximum precipitation above the established threshold are obtained. Because precipitation behaves spatially unevenly, once the event is identified in a rain gauge, it is necessary to extract what happens in the other stations in that period. As the precipitation peak does not occur simultaneously at all stations, it is necessary to identify the beginning and end of the storm's passage through all of them. In total 1761 events are obtained.

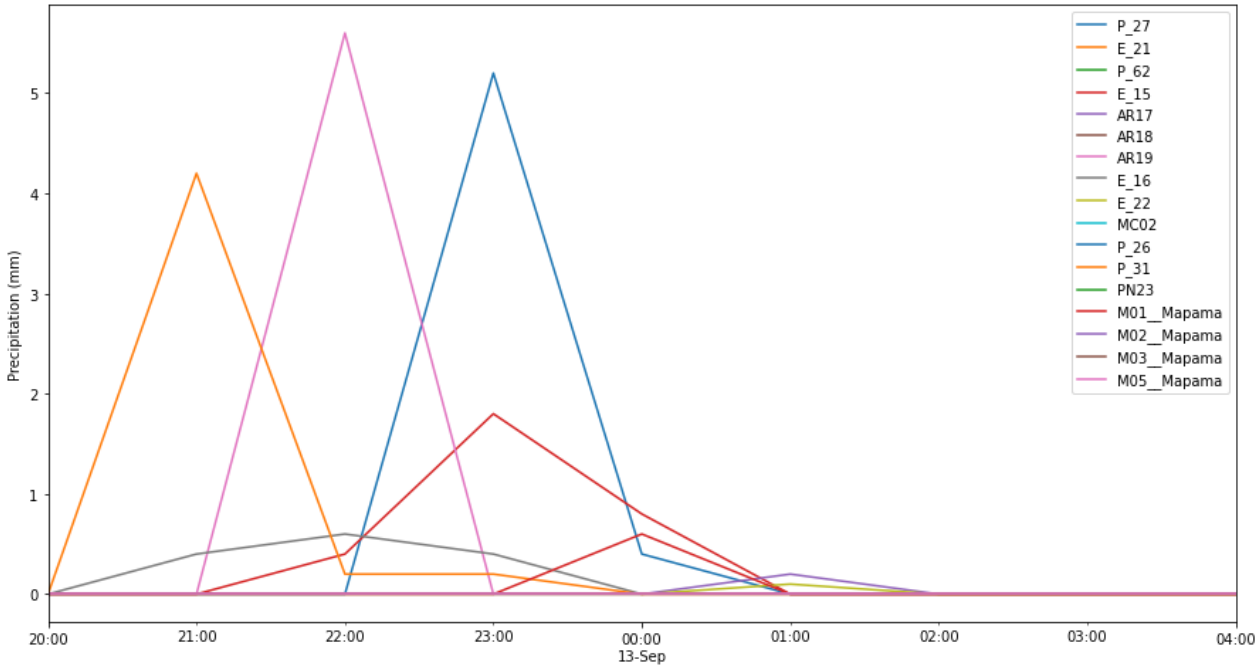


Figure 37. Separation of precipitation events.

To generate synthetic events from real data, it is necessary to classify real events into groups according to several descriptive parameters such as:

- Maximum Precipitation (Pmax).
- Average precipitation (Pmed).
- Time (T).
- Type or shape of the hyetograph (Type).

To identify which, type of hydrograph it is necessary to perform an initial classification by hydrograph types according to their shape. Each of the hydrographs defining the events obtained from the separation are discretized into 100 parts and the following algorithms are applied:

- Principal Component Analysis (PCA): reduces the number of dimensions of the matrix by capturing the initial variance of the data series. (Smith, 2002).
- K-Means algorithm: classifies events into a certain number of groups considered representative, in this case 25 (Camus et al., 2011).

The classification process is as follows: once the dimensionalization has been performed by the PCA method, the *K - Means* algorithm implemented in the *Sklearn Python* package is executed to obtain the classification by types of hyetographs. Figure 38. Classification by types of hyetographs. shows the classification performed.

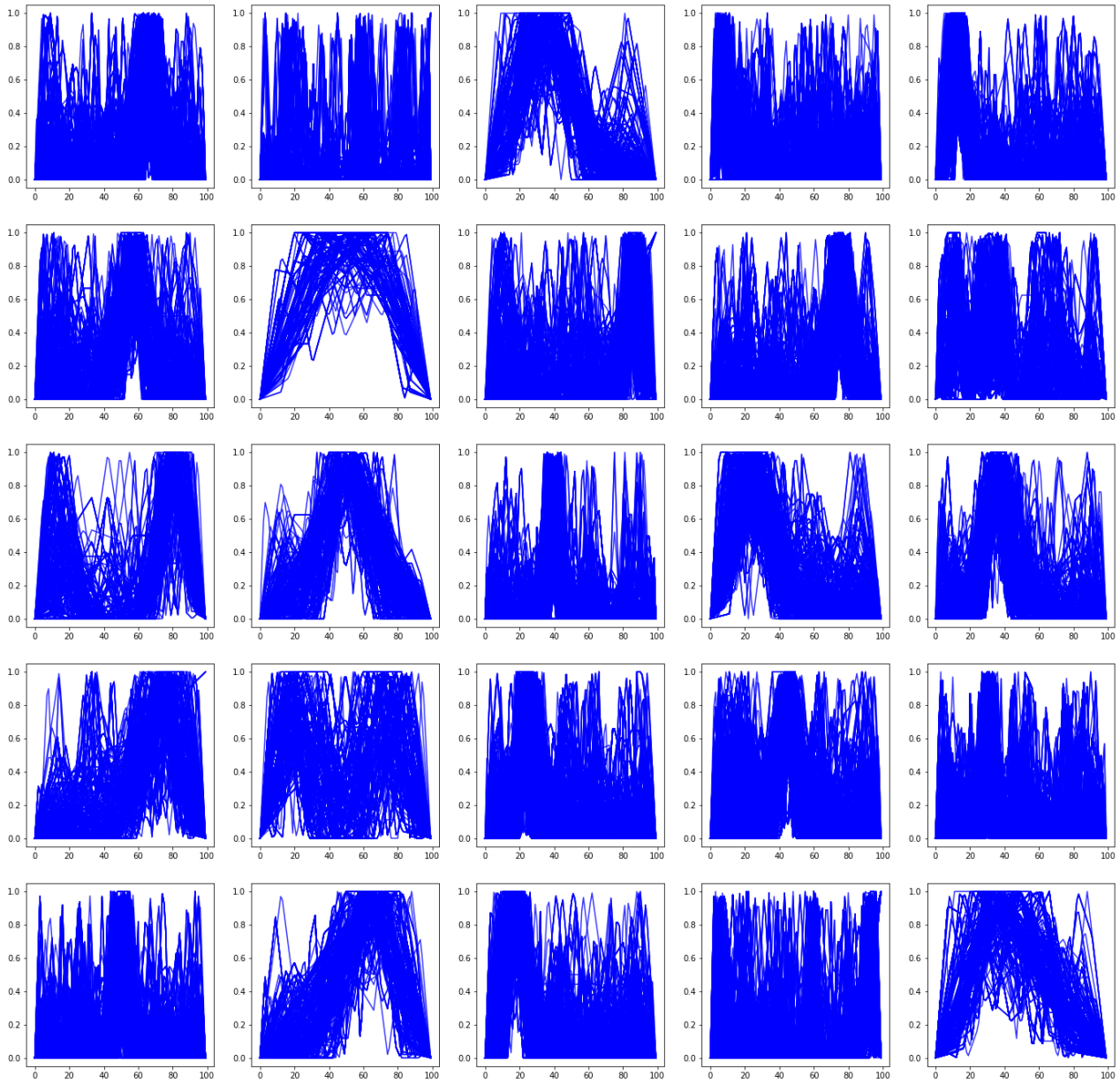


Figure 38. Classification by types of hyetographs.

It should be noted that each of the events is composed of the 4 parameters of each of the rain gauges, i.e., the matrix constructed would have a dimension of 1761x68. This matrix will be the one used in the following process of the methodology.

5.8.5. SYNTHETIC SIMULATION OF PRECIPITATION EVENTS

Once the events of the precipitation series have been separated and classified according to their shape, it is necessary to generate synthetic events. This will make it possible to obtain a whole series of probable simultaneous events in the 17 rain gauges characterized by the 4 parameters defined above.

The generation of synthetic events is performed through the probabilistic regression method using Gaussian copulas[1].

Marginal distribution functions are used as inputs to the copula, and these can be any set of disparate distributions. In this work we have analyzed which distribution function best defines each of the variables. Figure 39. Example distribution function settings. shows an example of the fit made for the maximum precipitation at rain gauge P27.

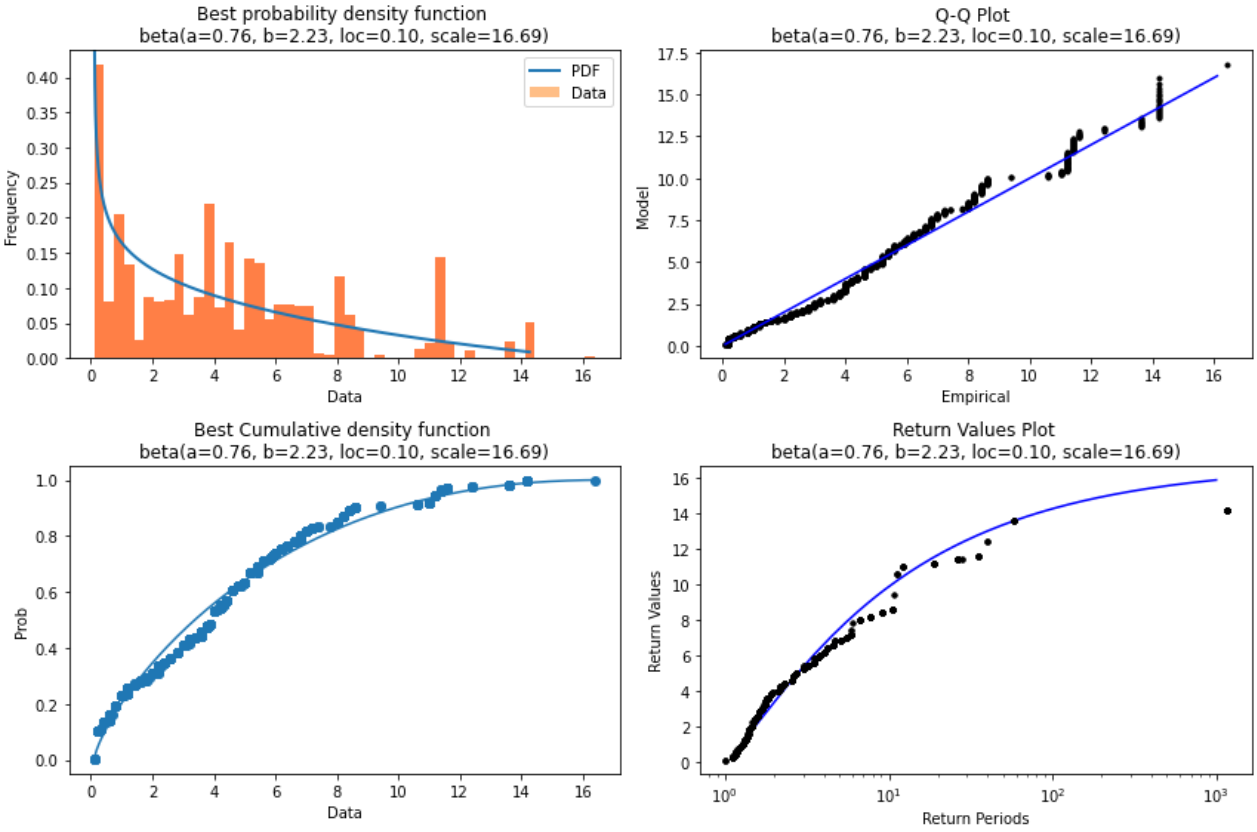


Figure 39. Example distribution function settings.

Once the different probabilities obtained from the distribution function have been entered into the copula, it is necessary to establish the number of synthetic events to be generated. In this study, 1 million events are simulated to have a good representation of the distribution of events for the 17 rain gauges. Figure 40. Synthetically generated events. shows an example of the events generated by copulas.

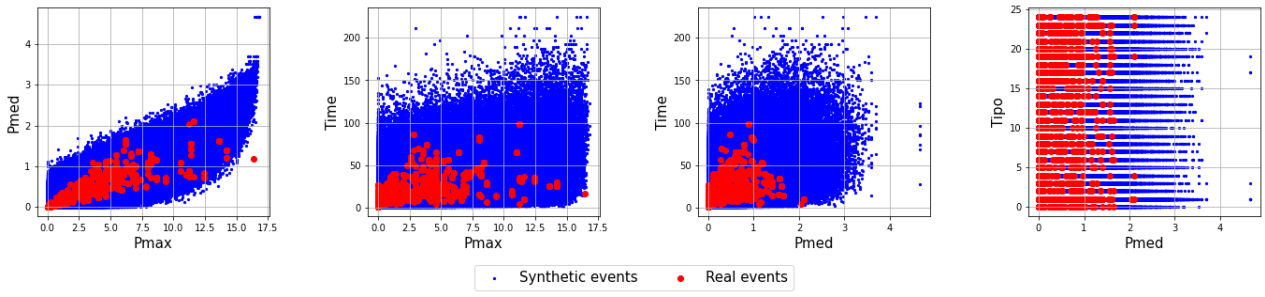


Figure 40. Synthetically generated events.

Since the number of synthetic events generated is large and not every single event can be simulated by hydrologic and hydraulic modeling, it is necessary to select a smaller number by ensuring that the set of selected synthetic events collects a representative sample of the likely data

set. This selection is carried out using the MaxDiss method (Camus et al., 2011)[2]. In total, 625 synthetic events are selected to perform the hydrological and hydraulic simulations. Figure 41. Selected synthetic events. shows an example of the selected events in rain gauge P27.

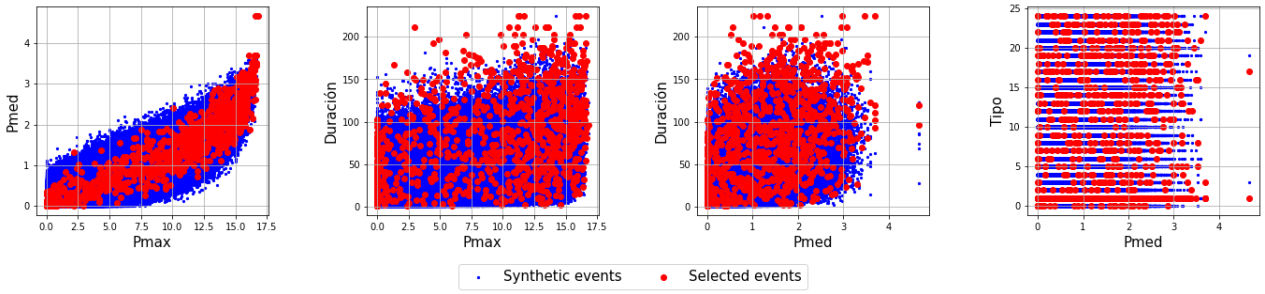


Figure 41. Selected synthetic events.

5.8.6. SPATIO-TEMPORAL RECONSTRUCTION OF SELECTED SYNTHETIC EVENTS.

Once the synthetic events have been selected, it is necessary to reconstruct the hydrographs according to the four parameters that define them (Pmax, Pmed, T and Type hydrograph). The first objective is to give the shape of the type of hydrograph to the synthetic event. To reconstruct the hydrographs of each event according to its shape and to ensure that the parameters Pmed, Pmax and T continue to characterize each of them, adjustment techniques using polynomials of degree 2 are used.

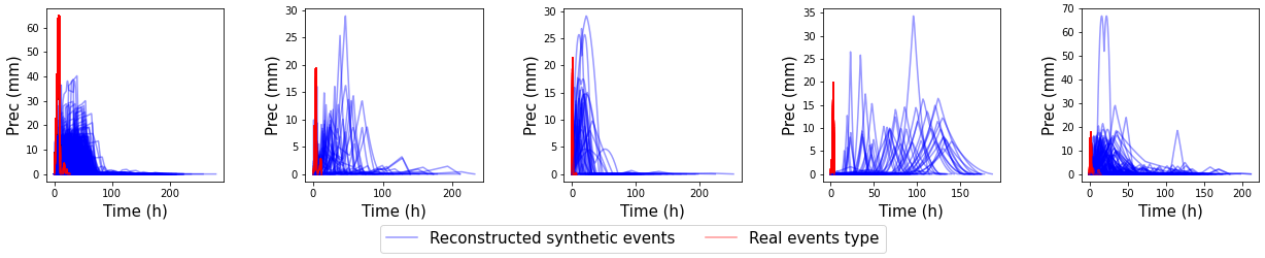


Figure 42. Example distribution function settings.

5.8.7. SIMULATION OF SELECTED EVENTS.

After selecting the most dissimilar synthetic events and reconstructing the associated hyetograph, the hydrological simulation is carried out using the model defined in section 5.8.2.1 . After simulating all the events, the hydraulic simulation is carried out using the hydraulic model defined in section 5.8.2.2.

5.8.8. RECONSTRUCTION OF DEPTHS.

The rest of the synthetic events generated are reconstructed from the hydraulic model. For the reconstruction of the draughts, it is necessary to resort to interpolation techniques and statistical techniques. The process followed is as follows:

- Inverse distance interpolation of the k nearest neighbors (Larose, 2005). In this case, the inverse distance of the k nearest simulated events to the synthetic event generated by copulas is calculated.

- Statistics of extremes in each section using the empirical distribution function to obtain the draft and flow associated with a return period.

5.8.9. RESULTS AND DISCUSSIONS

Once the methodology has been applied, the results are obtained for all the sections of the model defined in section 5.8.2.2. However, due to the problems existing in the two zones described above, the analysis is focused on the sections that make up these two zones of the river flow. The results presented below are divided into four parts:

- Analysis of the flows corresponding to each return period obtained with the defined methodology.
- Analysis of the corresponding flows for each return period using the methodology defined in this work.
- Comparison of the draft with the design flow of the canalization.
- Analysis of the probability of overtopping using the methodology defined in this work.

ANALYSIS OF FLOWS CORRESPONDING TO EACH RETURN PERIOD.

The most important variable for determining the design draughts is the flow rate, which is why in this section we analyze the flow rates for the different return periods obtained with the methodology defined in this work. Once all the synthetic events have been simulated, the flow values are extracted from the hydrological model at the point where the boundary conditions of the subsequent hydraulic modeling are located and then the flow value for each of the return periods is evaluated through the empirical probability. Table 7. Flows for each return period shows the results obtained.

Table 7. Flows for each return period

	T2	T5	T10	T20	T50	T100	T500
Flow (m3/s)	75.39	142.19	214.47	293.11	400.17	491.42	739.05

ANALYSIS OF THE WATER LEVEL CORRESPONDING TO EACH RETURN PERIOD

Once the water levels in the channel have been reconstructed for all the synthetic events obtained during the development of the methodology, the return periods in each section are obtained for the return periods analyzed. As mentioned above, the final analysis focused on the sections of the two conflicting points along the channel. Table 8. Results of bridge sections. and Table 9. Results dam sections. below show the results obtained through the methodology defined in the sections of the two conflict zones that have been identified. In these two tables, the drafts associated with each return period in the sections that make up the two areas of interest, the bridge, and the dam, are shown.

Table 8. Results of bridge sections.

HEC RAS XS	WS Elev (m) T_2	WS Elev (m) T_5	WS Elev (m) T_10	WS Elev (m) T_20	WS Elev (m) T_50	WS Elev (m) T_100	WS Elev (m) T_500
6262	3.44	4.05	4.59	5.22	6.16	7.09	9.12
6282	3.40	4.01	4.56	5.18	6.12	7.04	9.08
6332	3.31	3.92	4.47	5.09	6.03	6.95	8.98

6382	3.22	3.84	4.38	5.00	5.95	6.85	8.88
6402	3.19	3.80	4.35	4.97	5.91	6.81	8.83
6432	3.14	3.75	4.29	4.92	5.86	6.75	8.76
6482	3.05	3.66	4.20	4.83	5.77	6.65	8.62
6502	3.01	3.62	4.17	4.80	5.74	6.62	8.56
6512	3.06	3.68	4.24	4.89	5.91	6.94	8.56
6532	3.03	3.65	4.21	4.86	5.87	6.90	8.53
6582	2.93	3.55	4.11	4.76	5.78	6.80	8.42
6632	2.85	3.47	4.03	4.67	5.69	6.71	8.30
6682	2.76	3.38	3.94	4.59	5.61	6.62	8.21
6732	2.68	3.30	3.86	4.50	5.52	6.53	8.11
6772	2.62	3.23	3.79	4.43	5.45	6.46	8.04
6782	2.60	3.22	3.77	4.42	5.43	6.45	8.02
6832	2.53	3.14	3.69	4.34	5.35	6.37	7.94
6882	2.46	3.07	3.62	4.26	5.28	6.29	7.86

Table 9. Results dam sections.

HEC RAS XS	WS Elev (m) T_2	WS Elev (m) T_5	WS Elev (m) T_10	WS Elev (m) T_20	WS Elev (m) T_50	WS Elev (m) T_100	WS Elev (m) T_500
4112	3.09	3.73	4.32	5.12	5.98	6.79	8.91
4132	3.06	3.70	4.30	5.10	5.96	6.76	8.87
4182	2.98	3.62	4.22	5.02	5.89	6.68	8.78
4232	2.90	3.53	4.13	4.93	5.80	6.59	8.73
4282	2.81	3.45	4.05	4.84	5.71	6.51	8.64
4332	2.73	3.37	3.96	4.76	5.63	6.53	8.71
4362	2.69	3.32	3.91	4.70	5.58	6.43	8.55
4382	2.65	3.28	3.88	4.67	5.55	6.37	8.46
4432	2.58	3.21	3.80	4.59	5.47	6.29	8.37

COMPARISON OF DRAFT WITH THE DESIGN FLOW RATE OF THE CHANNEL.

During the development of the infrastructure under study, an action was carried out in the river to evacuate the flow corresponding to the 500-year return period flood in the channelization, which was set from the hydrological study at **550 m3/s**.

This section analyzes the differences between the results of the design flow with which the construction of the channelization was projected and those obtained through the methodology developed in this project. Table 10. Comparison of results in the bridge sections and Table 11. Comparison of results in the dam sectionsshow the discharges obtained for a return period of 500 years using the design flow of **550 m3/s** and with the methodology proposed in this work. In addition, the differences in draft between the two results are analyzed.

Table 10. Comparison of results in the bridge sections

	WS Elev (m)

HEC RAS XS	T_500 Design	T_500 Methodology	Difference
6262	6.58	9.12	2.54
6282	6.54	9.08	2.54
6332	6.45	8.98	2.53
6382	6.37	8.88	2.51
6402	6.33	8.83	2.50
6432	6.28	8.76	2.48
6482	6.19	8.62	2.43
6502	6.16	8.56	2.40
6512	6.43	8.56	2.13
6532	6.39	8.53	2.14
6582	6.30	8.42	2.12
6632	6.21	8.3	2.09
6682	6.12	8.21	2.09
6732	6.04	8.11	2.07
6772	5.97	8.04	2.07
6782	5.95	8.02	2.07
6832	5.87	7.94	2.07
6882	5.79	7.86	2.07

Table 11. Comparison of results in the dam sections

	WS Elev (m)		
HEC RAS XS	**T_500 Design**	**T_500 Methodology**	**Difference**
4112	6.24	8.91	2.67
4132	6.23	8.87	2.64
4182	6.16	8.78	2.62
4232	6.07	8.73	2.66
4282	5.99	8.64	2.65
4332	5.91	8.71	2.80
4362	5.86	8.55	2.69
4382	5.82	8.46	2.64
4432	5.74	8.37	2.63

As it can be observed in Table 10. Comparison of results in the bridge sections and Table 11. Comparison of results in the dam sections, there are differences between the draft with which the infrastructure was sized, and the drafts obtained through the methodology of this work. Therefore, it is necessary to identify the probability of overtopping or the return period for which the infrastructure was finally built.

ANALYSIS OF THE PROBABILITY OF OVERRUN BASED ON THE METHODOLOGY DEFINED IN THIS WORK

As mentioned above, there is an important difference between the obtained draughts. For this reason, we will now analyze the elevation at which the channel sections are sized according to the methodology used in this work.

First, it is necessary to identify the cumulative distribution function (CDF) (Figure 43) of the flood elevations obtained in each synthetic event and section of the two problem areas.

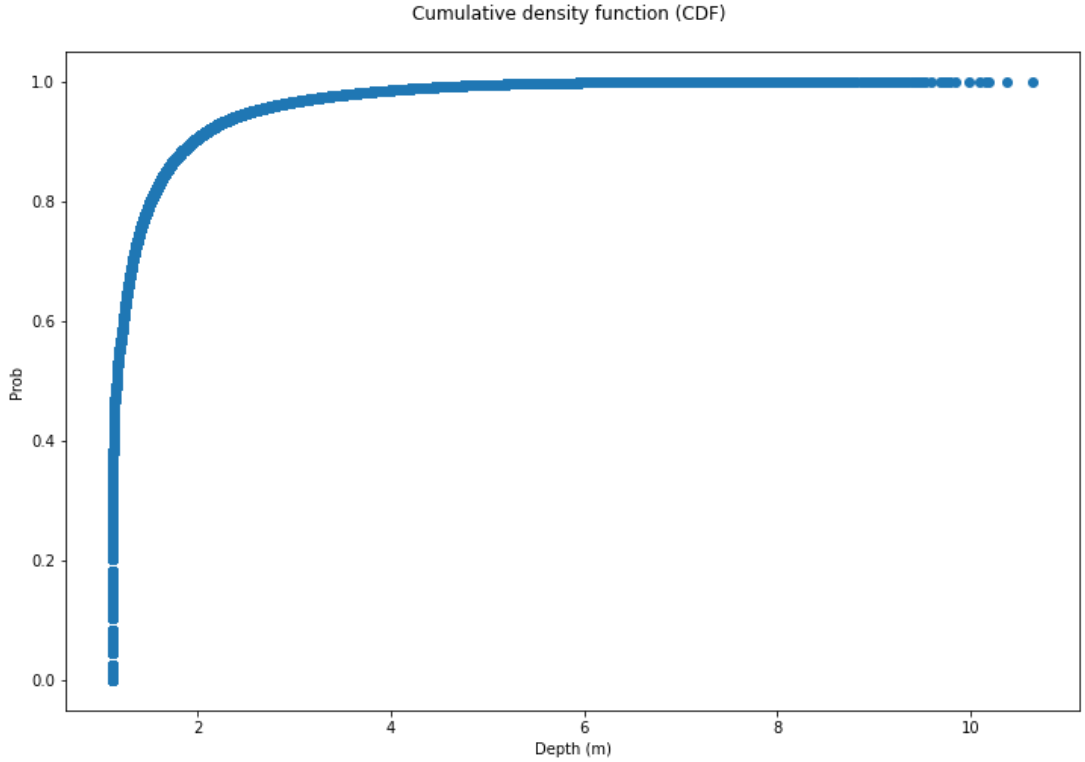


Figure 43. Example cumulative density function in section 6262.

Once the CDFs are obtained, the maximum elevations of the channel pockets on both banks are extracted and the minimum elevation is identified.

From the minimum elevations, the CDF and the following expression, the minimum elevation of the section in the pockets is obtained for the return period, where λ is the number of events per year that occur, which in this study area is equal to 5.17 events/year.

$$t_r = \frac{1}{\lambda - \lambda * cdf(Minimum\ profile\ height)}$$

Table 12. Return periods for channel banks heights. Bridge sections and Table 13. Return periods for channel banks heights. Dam sections show the elevations of the sections on both banks of the channel, the minimum elevation of both banks and each section, and the return period associated with this minimum elevation.

Table 12. Return periods for channel banks heights. Bridge sections

HEC RAS XS	Left bank	Right bank	Min Height	Return Period
6262	575.41	575.39	575.39	168
6282	575.47	575.46	575.46	179
6332	575.57	575.53	575.53	189
6382	575.65	575.64	575.64	209
6402	575.68	575.7	575.68	216
6432	575.77	575.78	575.77	239
6482	575.92	575.89	575.89	271
6502	575.98	575.96	575.96	289
6512	575.98	575.96	575.96	251
6532	576.01	575.98	575.98	254
6582	576.1	576.06	576.06	272
6632	576.18	576.16	576.16	301
6682	576.27	576.29	576.27	331
6732	576.33	576.39	576.33	345
6772	576.43	576.41	576.41	372
6782	576.46	576.42	576.42	373
6832	576.53	576.61	576.53	419
6882	576.64	576.68	576.64	463

Table 13. Return periods for channel banks heights. Dam sections

HEC RAS XS	Left bank	Right bank	Min Height	Return Period
4112	570.74	571	570.74	170
4132	570.91	571.07	570.91	202
4182	571.23	571.19	571.19	259
4232	571.43	571.3	571.3	283
4282	571.44	571.4	571.4	312
4332	571.49	571.55	571.49	305
4362	571.61	571.64	571.61	352
4382	571.69	571.65	571.65	372
4432	571.83	571.74	571.74	403

Despite having used a lower flow rate in the sizing, after the modification of the channel section in these problem areas, the height of the channel banks are built for return periods greater than the 100-year return period as shown in Table 12. Return periods for channel banks heights. Bridge sections and Table 13. Return periods for channel banks heights. Dam sections, therefore the probability of overtopping has low return periods.

5.8.10. CONCLUSIONS

To adequately characterize the climate of an area, it is necessary to have long series of climatic data and a certain density of meteorological stations distributed throughout the territory. Short series and a small number of stations prevent accurate studies. Despite the reconstruction of climatic series at points where there is no data, there is still some uncertainty that will influence the hydrological modeling.
Furthermore, even if more complex models are used, this does not mean that the prediction at points without data will be more accurate, but depends on the length and number of series, the higher the quality of the data, the better the fit. Studies in the United States have shown that a high spatial resolution of precipitation data is essential for simulating flood peaks. Short and sparse precipitation series can underestimate the value of flood peaks by 50% - 60% (Michaud & Sorooshian, 1994).

For this reason, it is essential to generate synthetic events to cover the range of precipitation events that produce flooding to avoid underestimation of flooding. When climatic variables are related to physical parameters such as altitude, slope orientation..., the prediction can be much more accurate despite having little starting data.

The methodology presented in this paper requires more computer resources and computational time than methodologies based on the design storm, however, an accurate and detailed flood study, and a sizing with adequate flow rates can avoid serious effects on the population during flooding episodes, provided that.

The use of a small number of precipitation series can lead to an underestimation of the maximum flows that cause flooding and, in turn, to inadequate sizing; however, the generation of synthetic events by means of copulas makes it possible to cover the range of possible flows that cause flooding. These flows are higher than those obtained by means of the usual methodologies, therefore, the obtained draughts would allow sizing on the safety side.

It also happens that due to the great uncertainty of the usual methodologies, infrastructures are sized with low return periods. This means that in increasingly frequent and more intense episodes caused by climate change, infrastructures may overflow, giving rise to situations of collective risk.

COMPARISON BETWEEN CURRENT SITUATION AND THE POSSIBLE APPLICATION OF THE TOOL

Was this type of analysis made before FORESEE? How it was made?	Yes, but with a different approach
How does FORESEE improve the results/analysis previously made?	It allows to create a better design for the infrastructure considering a new methodology that is more accurate
How does this result increase the resilience of your infrastructure?	It allows to create a better design for the infrastructure considering a new methodology that is more accurate
How does this FORESEE result improve your infrastructure's management	This tool is useful during the design and construction phase. For management purposes, it can give you decision support if some reconstruction or elevation of the water defences is needed.
What cost/resource efficiencies you expect these tools/results to have on your day-to-day business? (e.g. decrease in working hours over the first year; reduction of maintenance costs, Return on Investment (ROI), increase in productivity.	It will highly reduce the maintenance cost if a flooding event bigger than the calculated during the design phase is triggered

5.9. SUISTENABLE DRAINAGE SYSTEMS

CONSIDERATIONS

In the study carried out in the Foresee Project in the Sustainable Drainage section, considerations are made applicable to the systems used in the open air, which are applicable in the areas of the M-30 managed by Madrid Calle 30 in the outer zone, and partly in the section most studied by this team, with regard to the 48 kilometres of tunnels.

In these kilometres of tunnels, the pumping equipment that controls and drains the seepage from the ground itself and the water that flows through the internal drains from the outside is of particular importance.

It should be considered that there are specific regulations for these drainage systems, taking into account the added risk in tunnels (R.D.635/2066), due to the spillage of dangerous goods, and the possibility of the spread of fires and gases through these evacuation systems.

CONCLUSIONS

With regard to the effects of a possible cyber-attack on drainage systems, it is necessary to consider the possible effects on pumping systems.

In this sense, the Self-Protection Plan, contemplated in R.D.393/2007, sets out the measures to be adopted in the event of flooding, measures that could be improved by adopting the resilience criteria provided by the Foresee Project.

5.10. NEW POROUS ASPHALT PAVEMENT

INTRODUCTION

The Foresee Project carries out an exhaustive study on the different types of pavement, concluding on the basis of the resilience analysis, in advising the new mixes, as opposed to the more traditional ones, based on the duration time, and their capacity to drain water, fundamentally.

THE CASE OF MADRID CALLE 30 RING ROAD

It should be pointed out that we are referring in particular to the 48 kilometres of tunnels, as they have a singular problem, since there is a specific regulation in the Spanish ad-hoc regulations.
After the experience of the years that have elapsed since it was put into operation, backed up by the studies carried out for this purpose, Calle 30 has opted to use discontinuous bituminous mixes type BBTM 11 A and BBTM 11B, justifying the influence of the asphalt mix on the safety of the tunnels by considering the following aspects:

- Fire resistance.
- Rolling noise: Decrease with this type of porous pavement.
- Improved skid resistance.
- Greater comfort and capacity in longitudinal and transversal regularity is obtained.

- It should be taken into account that, in tunnels, among other circumstances, the absence of rain that would naturally contribute to the cleaning of the porous voids, requires a certain type of bituminous mix.

CONCLUSIONS

We consider that, by different routes, a treatment similar to that provided by the Foresee Project has been reached.

5.11. SUMMARIZE OF THE INPUTS AND OUTPUTS

Table 14. Outputs by Phase Foresee Tool cs#5

Case Study#5	*INPUTS*	*OUTPUTS*	*PHASE*
TRAFFIC MODULE	• Closure time (CT), • The Partial opening time (POT), • The Opening time (OT), • NL: The number of lanes that are retained closed. • CaP: The capacity modification • V: velocity modification.	• Travel time, • Traffic volume at a future time (k-hours ahead),	Design & Construction, D Maintenance and Operation, M & O
HYBRID DATA FUSSION FRAMEWORK	• Closure time (CT), • The Partial opening time (POT), • The Opening time (OT), • NL: The number of lanes that are retained closed. • CaP: The capacity modification • V: velocity modification.	• Travel time, • Traffic volume at a future time (k-hours ahead), • Cost of travel time	Design & Construction, D Maintenance and Operation, M & O
COMMAND AND CONTROL CENTER	• Historical Traffic Data	• Anomaly Score	Maintenance & Operation, M & O
FLOODING METHODOLOGY	• Hourly information on precipitation at the basin's stations	• Heigh of the water table for different return periods	Design & Construction, D
D7.1	• None	• Type of hazard • Road and tunnel component • Mayor risk • Type of impact • Impact Description	Design & Construction, D
D7.2	• Traffic composition (number and type of vehicles) • Characteristic of the route (length and average speed) • Cost of travel time • Additional transport modes • Population • Presence of critical infrastructure (energy, water, transportation hubs…) • Presence of critical services (hospitals, fire station, police stations…)	• Performance level • Recovery time	Design & Construction, D

	• Return period of the event and probability of exceedance		
D7.3	• None	• Regulations and normatives • Infrastructure and operational measures • Safety assessment (risk analysis and evaluation) • Operating conditions • life cycle of the tunnel (planning, design, construction, commissioning, operation, renewal, upgrading) • Operating experience • System conditions • Emergency procedures (self-protection plan).	Maintenance & Operation, M & O
D7.4	• Type of users • Multicultural and characteristic of users • Fire simulations and scenarios • Type of cars	• Emergency Detection and Alert. • Alarm Mechanisms. • Emergency response mechanisms. • Evacuation and / or Confinement. • Provision of First Aid. • Ways of receiving external aid. • Detection, alarm, reaction and evacuation times	Maintenance & Operation, M & O

6. SOCIO ECONOMICAL STUDY CONSIDERING A CYBERATTACK AFFECTING THE M-30 RING ROAD. IMPACT ON TRAFFIC AND ALTERNATIVE ROUTES

6.1. OBJETIVE

To describe the impact on traffic and alternative routes to the Madrid Calle 30 tunnel system, analysing the socio-economic impact, based on the data available and already provided in the previous deliverables of the Foresee report.

6.2. GENERAL CONSIDERATIONS

As a preliminary starting point, it should be pointed out that any intrusion by means of a cyber-attack on the management systems of the Calle 30 Control Centre, provided that one of the systems or subsystems considered critical has been affected, should mean that access to and evacuation of the tunnel system should be cut off, until the possible scope of the attack is known.

It should be pointed out that Calle 30 is made up of a system of tunnels, connection galleries with the exterior, connections with other infrastructures and emergency galleries, interrelated with each other, and with a single Main Control Centre, which means that if one section is affected, the safety of the rest will be compromised.

This work will focus on the foreseeable negative socio-economic effects.

6.3. SOCIO ECONOMIC ANALYSIS

We start from the scenario we consider most likely, in which initially, and for a period of time already justified in previous works of 180 minutes, access is totally prohibited.

It should be noted that, in the operational response system, the actions to be taken immediately by the Calle 30 Control Centre have been detailed to guarantee the safety of users and operators, even in these circumstances.

Although we consider that the social and economic effects will be related, in order to be able to analyse both aspects in greater depth, we have made an initial assessment separately.

6.3.1. SOCIAL IMPACT

In this section we include the effects on the following matters:

- Environmental aspects:
  - Derived from the environmental pollution that will be produced due to the circulation of all the vehicles on the surface, without the corrective factor of the elimination of harmful gases through the filtering elements in the circulation tubes, in the ventilation systems, which means that the air released to the outside is free of polluting elements.
  - Effects derived from the generation of an increase in noise, due to the surface traffic of all the circulation.

- Social aspects:
  - Decrease in average speed on equivalent journeys, due to congestion on surface roads, due to the increase in traffic.
  - Increased travel times on equivalent journeys, due to lower average speed.
  - Increased accident risks as a result of the increase in traffic intensity, possible adverse weather phenomena, and the composition of traffic, in which heavy traffic is present, and even the possibility of the circulation of dangerous goods.
  - Increased access times for emergency vehicles due to traffic congestion and complexity.

6.3.2. ECONOMIC IMPACT

While it is true that direct and in some cases indirect costs are derived from all the social and environmental impacts, there are others that are inferred directly from the cyber-attack event itself.

- Damage caused to the management system itself, and the costs of restitution.
- Possible damage caused to the infrastructure, caused directly or indirectly, among which we highlight:
  - Possible flooding as a consequence of the stoppage of the leakage control pumps.
  - Damage to pipes as a result of uncontrolled start-up of water mist systems.
  - Damage due to uncontrolled operation of ventilation systems.
  - Damage to evacuation systems and subsystems (external ramps, pressurisation systems and others).
- Increase in the economic cost of travel times, for which the tables in the previous deliverables will be used.
- Possible claims from users of the infrastructure, due to loss of capacity and collateral damage.

6.4. CONCLUSIONS

As described above, there are different socio-economic impacts, which will be all the more serious the longer the duration of the incident caused by the cyber-attack, the quantification of which can be calculated in the initial interval of 180 minutes, using the data contained in the tables of deliverables 1.1 and 1.2, with the exception of those other costs of damage that may occur in the infrastructure and facilities in the initial phase of the cyber-attack.

It should be mentioned that there will be a very significant cost to the image of the company and its management capacity, which, although difficult to assess in economic terms, is easily extensible to the rest of the management, and even in future business commitments.

7. SCENARIO CAUSED BY A CIBERATTACK. DESCRIPTION OF THE SCENARIO CAUSED BY A CYBER ATTACK ON THE M-30 RING ROAD (MADRID) CONTROL SYSTEMS AND ASSOCIATED RESPONSE

7.1. OBJECTIVE

The present work aims to describe the scope of a cyber attack on the M-30 Ring Road control equipment, its effects on traffic management and safety, including the possible impact on the infrastructure, listing and describing those elements that are considered critical, defining the quality of critical, and the ability to maintain or not the service in the circumstance of degraded system or systems.

7.2. DEFINITION OF ELEMENTS / CRITICAL SYSTEM

The safety control system of a tunnel, fixes the monitoring of several systems, equipment and elements, without whose disposition, the minimum level of safety cannot be guaranteed to keep on service the infrastructure. These are the critical elements or systems.

7.3. GENERAL CONSIDERATIONS

It should be noted that M-30 Ring Road is made up of a system of tunnels, connecting galleries with the exterior, connections with other infrastructures and emergency galleries, interrelated with each other, and with a single Main Control Centre, so one event in certain point of the M-30 Ring Road could have affections on the rest.

It is logical to think that if the cyberattack is executed by experts in this type of actions, it will be carried out in such a way that it will be difficult to attribute initially the loss of control to an attack of this type, then the time of incidence will be longer.

For this reason, we consider that the first thing should be to generate tools that allow to rule out other circumstances or failures as quickly as possible, in order to be able to quickly take the actions to neutralize and reduce the damage caused.

Therefore, we proceed to describe the scenarios that we consider possible, detailing the severity of the consequences from least to greatest:

- Is a cyberattack the control system failure reason?
- Does the Control Centre maintain total or partial management capacity?
- Is the cyberattack only limiting the Control Centre's ability to operate?
- Does the cyberattack allow the intruder to maliciously operate management systems?
- Once the questions have been answered, we proceed to describe the possible affected systems.

7.4. AFFECTED SYSTEMS

Next, and starting from the scenario that we consider most serious due to its negative effects, which is the one in which the intruder manages to operate the management systems in a malicious way.

It should be noted that in the operational response protocol, the actions to be taken immediately by the M-30 Ring Road Control Centre will be detailed to guarantee the safety of users and operators, even in these circumstances.

But in the scenario that occupies us, we must pay our attention to the services, systems, and critical facilities affected.

For this reason, and in order of severity, we list those facilities that we consider critical, even if they only manage to simulate the failure in the system, a series of actions or decisions can be triggered that would generate dangerous situations.

Let's take an example:

The affected system is the firefighting control system and equipment, and it has been simulated that there is a fire with serious characteristics, and that manages to activate the "water mist" system, with vehicles circulating, which may cause a loss of visibility to drivers and the consequent risk of collision.

Well, following this scenario, we go on to detail in order the systems that we consider critical:

- Tunnel closure system.
- External and internal power supply.
- Ventilation system.
- Firefighting control system and equipment. Water mist system.
- Lighting system.
- Variable Signalling system.
- Video surveillance system. DAI
- SOS Calling points / PA/VA Systems.
- Analysis and control systems for environmental factors.
- Evacuation management systems.
- Communications equipment.

Each of the invalidated or maliciously managed systems will require a response from the Control Centre, and the degraded service situation that generates the simultaneous failure should trigger the systematic response and decision-making in favour of safety.

7.5. MANAGEMENT AND CONTROL SYSTEMS

According to the legal regulations, the permanent control of the tunnel equipment and facilities, traffic management, maintenance supervision, and emergency management, is managed by the Control Centre (CC).

For this, this CC., Receives permanent information from the ITS elements that manage and control equipment and facilities.

It is not the objective of this document to analyse how to prevent an attack on these ITS elements, but it is to establish the response to the emergency.

All critical elements are shown in the control and management systems, with alarms, programmed with the admissible values established by the standard as correct service, and which enable the objective response of the CC operator.

The CC., therefore, is the point where all the information converges, and from where the immediate response is coordinated.

This response is established, approved and standardized in the basic documents mentioned in the regulations, and already mentioned repeatedly, such as the Operation Manual and the Self-Protection Plan. Moreover, generally and to avoid errors, the answer is integrated into the SCADA management system itself. Both documents are CONFIDENCIAL, and accessible exclusively to intervention services, so we will only mention with the indication of the use sheet in the event of an attack.

In these documents, together with the Degraded Service Manual, which are not a legal required document, if the answers are provided, will appear as annexes to this document.

7.6. PERFORMANCE INDICATORS

Each of the control systems and subsystems has a supervision equipment associated with it, and an indicator that assesses the operation, its contribution to the overall safety, and the acceptable level of operation in the event of degraded service.

The level of service is generally standardized, either by the applicable tunnel regulations itself, or by the operation's own quality system, generally referred to in the service contract.

For all of the above, once the questions posed in the paragraph entitled "general considerations" have been answered, a response table such as the one detailed below should be completed:

Table 15. General considerations

AFFECTED EQUIPMENT	DETECTION SOURCE	IT'S A CIBER-ATTACK	BEATS STANDARDIZED INDEX	SELF-PROTECTION PLAN/ DEGRADED SERVICE FILE	CLOSED ACCESS
CLOSURE SYSTEM TUNNEL / BARRIERS					
POWER SUPPLY					
VENTILATION SYSTEM					
FIREFIGHTING CONTROL SYSTEM AND EQUIPMENT					
ILLUMINATION SYSTEM					
SIGNALING SYSTEM					
VIDEOSURVEILLANCE SYSTEM / DAI					
SOS / PA/VA SYSTEMS					
ANALYSIS AND CONTROL SYSTEM OF ENVIRONMENTAL FACTORS					
EVACUATION MANAGEMENT					
INTERNAL / EXTERNAL COMMUNICATIONS EQUIP.					

7.7. STANDARDIZED RESPONSE, INCLUDED IN THE SELF-PROTECTION PLAN

Each of the invalidated or maliciously managed systems will require a response from the Control Centre, and the degraded service situation that generates the simultaneous failure should trigger the systematic response and decision-making in favour of safety, in which, and in a coordinated manner, the priority actions are:

- Prevent access to the affected area and progressively to the entire tunnel length.
- Evacuation of vehicles that are inside.
- Verification of the origin of the loss of Control.
- Divert traffic to alternative routes.

We consider as indicative times, with the premise of loss of communications, so the instructions and monitoring of the First Intervention teams, Local Police, Firefighters and Health Services can only be carried out by telephone, with the consequent risk of collapse of the communications, we can estimate:

- Access cut-off: It must be in person of the staff as it does not have control of the signalling, for which we estimate 40 minutes.
- Alternative detours. They can only be done by site present teams. Estimated 90 minutes.
- Evacuation of vehicles from the interior. Estimated 30 minutes.

From these 90 minutes, we would enter the service recovery scenario, which with the location of the attack, and possible alternative solutions, to be able to start a recovery of the service in

degraded conditions, with the possibility of carrying out a direct control, counting so that once the first actions have been taken to preserve safety, it is the Administrative Authority that has the responsibility to restart the service, under the conditions established in the Degraded System Manual.

7.8. CONCLUSIONS

The Scenario that creates a cyberattack on the safety of Madrid M-30 Ring Road, has common elements that we must highlight:

- Detection and identification time.
- Difficulty in the real assessment of the scope.
- Criterion elements to determine the service restitution time.
- Difficulty isolating the scope of a cyberattack in sections.

It is true that the necessary systems are in place for the rapid detection of malfunctioning systems and equipment, as well as the inventory of elements available for a safe response, however, it would be desirable to create tools that allow rapid discrimination of the existence of a cyberattack.

Therefore, what is recommended is the adoption of a common systematic initial response, which preserves the safety of users, operators and the infrastructure itself.

This document does not reflect the content of the provisions in the Operation Manual, Self-Protection Plan, and Degraded Service Manual (Non-mandatory document written and approved by Madrid M-30 Ring Road), as they all have the quality of CONFIDENTIAL DOCUMENTS. We consider that, with the authorization of the related authorities, these documents could appear as annexes.

8. RECOMMENDATIONS OF ACTIONS TO BE ADOPTED

8.1. INTRODUCTION

This document contains a proposal of actions to be adopted to improve the resilience level of the transport system in case study 5: The M-30 Ring Road (Madrid), in case of a cyber-attack event.

8.2. METHODOLOGY

This document covers the following tasks, which will be analyzed individually, to reach conclusions and proposals:

- ACTIONS TO BE ADOPTED WITH A GENERIC CHARACTER.
- ANALYSIS OF THE INFRASTRUCTURE CONTROL SYSTEMS, AND THEIR VULNERABILITY IN CASE OF A CYBER ATTACK EVENT.
- SYSTEMATIC RESPONSE TO A CYBER ATTACK EVENT.
- SPECIFIC RECOMMENDATIONS FOR M-30 RING ROAD.

Due to the characteristics of this type of threat, its diverse etiology, and the constant evolution of the technical systems and equipment dedicated to its neutralization, we consider that this chapter should be the purpose of a separate study.

8.3. GENERIC ACTIONS TO BE ADOPTED

The generic actions to be adopted in this type of facility susceptible to a cyberattack are listed below, generally accepted and recognized by the experts and entities that deal with the matter:

- Safety culture, which implies information and permanent training of the organization's participants
- Inventory of existing computer security risks, specifically in those systems related to the control and management of security elements.
- Inventory of protected devices.
- Passwords. Each Operator may only enter the system with their personal password.
- Security protocols, which includes all operations, whether preventive or corrective maintenance of the systems.
- Do not download programs that have not been previously authorized by the security officer, in a reliable way.
- Control of removable devices, of which there will be an inventory and protocol for use.
- Personal data will never be used or provided, and the accreditations approved and provided by the Organization will be used instead.
- Any message that is not credited by the person responsible for the system will not be accepted or executed.
- Any suspicion of cyberattack, and prior study by the person in charge of the system, will be reported, and where appropriate reported, to the authorities.
- Web filtering.

8.4. ANALYSIS OF THE INFRASTRUCTURE CONTROL SYSTEMS, AND THEIR VULNERABILITY IN CASE OF A CYBERATTACK

In this section we will go through the specific aspects of the systems considered as critical that are managed from the M-30 Ring Road. The critical systems are listed below:

- External and internal power supply system.
- Ventilation and air pollution control system
- Fire fighting system.
- Lighting system.
- Emergency signage system.
- CCTV system.
- SOS posts.
- Evacuation management systems.
- Automatic incident detection (AID)
- Signalling using lights and traffic signals
- Communications network

Each of these systems and equipment manage services considered critical, and which require an individual study, which includes the possibility of maintaining the service even in degraded system conditions.

In this case, there is an approved by M-30 Ring Road protocol, which provides for alternative and palliative actions to be adopted in the event of degraded service, integrated into its Self-Protection Plan, and which are part, by regulation, of the Operation Manual.

The peculiarity of the M-30 Ring Road Control Centre system, integrated into one of its redundant positions in the Traffic Control and Management Centre of the Madrid City Council, requires a specific study section to be dedicated to preventive defense actions against a cyber-attack, of this Centre.

Alternative management positions will be analysed, planned for their commissioning in the event of a failure of the Main Control Centre.

8.5. SYSTEMATIC RESPONSE TO A CYBERATTACK EVENT

This section will try to answer some questions related to different alternatives for crisis management in the total failure of the Main Control Centre like:

- Is a cyber-attack the proven reason of the total failure of the Main Control Centre?
- Does the Control Centre maintain total or partial management capacity?
- Is the cyber attack only limited to nullifying the Control Centre's ability to operate?
- Does the cyberattack allow the intruder to operate the management systems maliciously?

The result of the answers and the systematic that it entails must be part of the document called the Self-Protection Plan, which is integrated into the Operation Manual, and which must go through the approval procedure established by current regulations.

8.6. SPECIFIC RECOMMENDATIONS FOR M-30 RING ROAD

The regulation that applies to the M-30 Ring Road operations, which is essentially governed by safety aspects, by the provisions of RD 635/2006 on Safety in Tunnels, and RD 393/2007 on Self-Protection Measures, as well as various provisions in relation to critical infrastructures, or those derived from Traffic Management, they themselves frame the measures of forecasting and

response to a situation that, as in the case of a cyberattack, disables the use of the systems and equipment managed from the Main Control Centre.

Specifically, and extracted from the regulation mentioned, in the Operation Manual, a key document for infrastructure management, and in the Self-Protection Plan that will collect the inventory of resources for a systematized response to an emergency, the recommendations and specific measures to be adopted in M-30 Ring Road will be collected.

We consider that the dedicated chapter to the service maintenance and affected equipment, degraded conditions, should be extended.

Consequently, and for its approval and consolidation in the regulatory framework, the suitability of the proposal must be proven, through the execution and assessment of the contribution, with the execution of a DRILL, in which the scenario is approximated to the real situation generated by a cyberattack, the results are analysed, opportunities for improvement are provided, and finally the described actions are implemented, without forgetting the need for training and information to the operators of all its content.

8.7. SUMMARY AND CONCLUSIONS

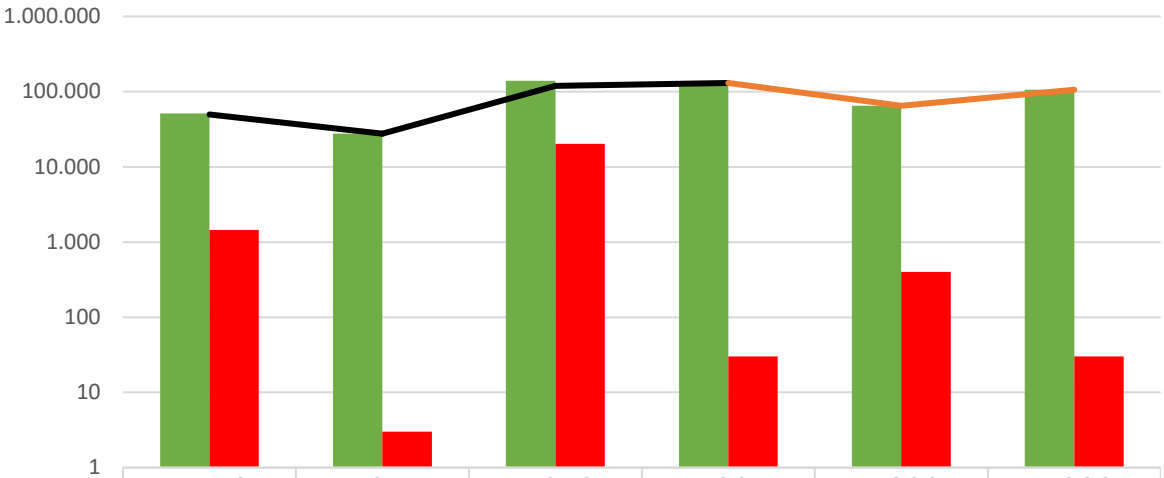
Through the systematic study provided in the Foresee Project, which is specified in the resilience of M-30 Ring Road 30 in the event of a cyber-attack, information that will be specified the quantification of the study parameters, and in the proposal for a systematic response and implementation of actions that minimize the consequences of an event and attack on M-30 Ring Road facilities and management teams, the methodology proposed in this document will be followed, the final result must coincide with objectives listed below:

- Preventive measures aimed at preventing a cyber-attack.
- Analysis of the resilience capacity of the facilities and equipment managed by the Main Control Centre.
- Description of possible scenarios.
- Definition of applicable systematics to lessen the effects of a cyber-attack.
- Approval and inclusion of the system in accordance with current regulations.
- Implementation of the approved measures.
- The procedure for quantifying the values and measurements will be defined in the Foresee Project.
- The data will come from the official reports of M-30 Ring Road, collected in its Operation Report, Audits, and Quality System.

All of the above will be part of the work to be carried out, and the first general framework report and first measures to be adopted.

9. ASSESMENT OF THE RESILIENCE LEVEL OF THE INFRASTRUCTURE AND IMPROVEMENT AFTER THE USE OF THE FORESEE RESULTS.

9.1. NET BENEFIT ANALYSIS CS#5



	M.1.1.2	M.2.1.4	M.3.1.2	M.3.2.1	M.3.2.2	M.3.2.3
Total benefit	51.124	27.607	139.569	130.366	65.183	105.827
Total costs	1.448	3	20.296	30	400	30
Net Benefit	49.676	27.604	119.273	130.336	64.783	105.797

Figure 44. CBA final graph obtained

The NBA obtained to applicate the FORESEE Tool (Selection of the adequate Design to resilient the specifics hazards), and posteriorly applicate the Operation & Maintenance Plan[1], to CS#5 is very beneficious to the leader of infrastructure, as demonstrate in the Figure 10.

The results have been obtained in function of indicators more representatives of specifics hazards, traffic, the presence of a safe shutdown system and hazards good traffic (see Annex 2).

10. FORESEE IMPACT IN CASE STUDY#5. COMPARISON WITH CURRENT SITUATION REGARDING ASSET MANAGEMENT PLANS

There is a very extensive available information about the comparison between the existing management plans of Madrid Calle 30 and the updated ones developed as part of the Foresee Project.

This information has been extensively analyzed as part of the chapter 5) of the present report, as well as in the chapters 6), 7) and 8) also included in this report.

Based on the previous requirements analysis and the additional indications, the validation of the selected FORESEE tools for the improvement of the defined KRI and KRT in CS#5 can be evaluated in the following.

As explained in the previous section, for most tools only descriptions of incoming requirements and outgoing outputs are available from the deliverables at the current time. As the newly developed tools can currently only be applied theoretically instead of practically, the validation is only qualitative by comparison with the current situation in the form of a tendential rating of the improvement.

The structural approach is similar to the previous requirements analysis. First of all, additional indications are pointed out regarding the improvements through the use of the selected FORESEE tools. The comparison of the identified improvements with the current situation and the tools used is summarised in Table 16. Comparison with current situation regarding Asset Management Plan CS#5 which follows.

Furthermore, the validation will be critically assessed by checking the RAMSSHEEP and Resilience Principles in the Table 17. CS#5, RAMSHEEP & Resilience Principles and by performing a net benefit analysis in section and presenting the resilience factors after using the selected FORESEE tools.

Table 16. Comparison with current situation regarding Asset Management Plan CS#5

CS#5	***Comparison***		
	ACTUALY / CURRENT TOOLS	**FORESEE TOOL**	
Traffic Simulation	- Traffic simulations with in-house software adapted to Calle30 needs - Variable input data - Cameras - Sensors – induction loop traffic sensors	**Traffic module**	- Accurate input data as stochastic Montecarlo algorithms are performed
Rating	→ *"Improvement"*		
Traffic Prediction	*No comparable tool(s) available!*	**Hybrid Data Fusion Framework**	- Predictions using Bayesian Networks and Random Forest Algorithms - Heterogeneous data - Travel time, - Traffic volume at a future time (k-hours ahead), - Cost of travel time
Rating	→ *"Innovative & Improvement"*		
Hazard Management Design	- Hourly information on precipitation at the basin's stations - Flooding simulations using HEC RAS and HEC HSM models - Old methodology to calculate the return periods	**Flooding Methodology**	- Synthetic simulation of precipitation events using Copulas - Selection of events to be simulated in the hydrogeological model - Spatial reconstruction of rainfall events at sub basin centroids - Flood elevation reconstruction for all synthetic events - Calculation of the heigh of the water table for different return periods – new and more demanding methodology
Rating	→ *"Improvement"*		
Hazard Management	- Cameras - Flooding and water sensors located on the dewatering pumps - Fire detectors - Control Center - Automatic detection of incidents that is already implemented on the cameras	**C+C Center**	- Automatized alerts considering the existing traffic - Predictive risk prevention - AI-Based hazards analysis
Rating	= *"No improvement."*		
Hazard Planning	- *Subjective, based on Expert knowledge*	**T.7.2 T.7.3 T.7.4 Plan Review**	✓ Objective, science-based
	- *Static, based on Eu-wide and national regulations*		✓ Dynamic, adapted to more variables and simulations
	- *Incomparable and fixed, no reference or benchmark for possible optimisation available*		✓ Comparable and scalable, monetize resilience / LoS to identify optimal investment decisions
Rating	→ *"Improvement!*		

10.1. RAMSSHEEP AND RESILIENCE PRINCIPLES FOR CS#5

The implementation of the selected FORESEE tools should make the infrastructure (more) resilient. In addition to the improvement rating described in the previous sections, the terms of RAMSSHEEP[2] and resilience principles[3] are introduced to validate resilience in an also qualitative but structured method.

Within the FORESEE project, resilience has been defined as the ability to continue to provide service if a hazard event occurs (compare D.1.1).

The well-known RAMS analysis (compare also DIN EN 50126**iError! Marcador no definido.**) can b e seen as a risk concept that describes the primary performance and resilience of all the functions of a system. In comparison to a basic RAMS analysis, the new extended RAMSSHEEP analysis also takes more social, ecology and economy aspects into account. In this project resilience consists of four outcome-focused abilities which are described as resilience principles in the following. Since infrastructure resilience relies on these four concepts, improving any of them improves the overall resilience of the infrastructure (compare D.7.1).

In the following, it is qualitatively validated whether the FORESEE tools selected in CS#5 affect the RAMSSHEEP and resilience principles.

Table 17. CS#5, RAMSHEEP & Resilience Principles

CS#5 *TOOL*	*OUTPUT*												
	RAMSHEEP									RESILIENCE PRINCIPLES			
	R	A	M	S	S	H	E	E	P	*Robust-nes*	*Resources-fulness*	*Rapid-Recovery*	*Adaptability*
Traffic Module			√			√		√	√	√	√	√	√
Hybrid Data			√	√	√	√	√	√	√		√	√	√
C+C Center			√	√	√	√		√	√		√	√	√
Flooding Meth	√	√		√	√	√		√	√	√			√
T.7.2 **T.7.3** **T.7.4** Plan Review	√	√	√	√	√	√	√	√	√	√	√	√	√

For a better understanding, the terms and components of the RAMSHEEP and resilience principles are described again afterwards.

The acronym of **RAMSSHEEP** stands for [extracted from [2]]:

- **Reliability:**
  The probability that a system/structure will fulfil its function under certain circumstances and during a specific time interval.
- **Availability:**
  The probability that a system/structure can fulfil its function at any random moment under certain circumstances.
- **Maintainability:**
  The probability that a system/structure fulfils its function under certain circumstances during maintenance within the established time frame.
- **Safety:**
  The absence of unacceptable risks in the system/structure in terms of human injuries.
- **Security:**
  The guarantee of a safe system/structure with respect to vandalism, terrorism and human errors (including all kinds of sabotage of the system).
- **Health:**
  The feeling of good health with respect to the physical, mental and societal views. This does not implement if an individual is feeling well or not (subjective argument).
- **Environment:**
  To meet certain requirements which have been secured in Environmental Acts one suffices the rules of a good and clean environment. The environment can be seen as a physical environment wherein human life is even possible.
- **Economics:**
  The Cost-Benefit will form a central position in the aspect of Economy. The increase the performance of the RAMS aspects will lead also to an increase of the direct costs. A serious reflection in terms of a Cost-Benefit Analysis must be made to provide more insight for an economical choice.
- **Politics:**
  A rational decision has to be made based on the aspects above, including also some political aspects.

The **Resilience Principles** stand for [extracted from D.7.1]:

- Robustness:
  This concept refers to the ability for transport infrastructure to overcome and absorb disruptive event shocks and continue operating. This concept is mainly oriented toward the physical parts of the infrastructure. At first sight, robustness could be misunderstood if it is assimilated simply as "resistance" and only translated into designing structures that are strong enough to resist a shock. Nevertheless, this concept goes beyond being able to stand the hazard's punch; robustness could also be translated to redundant systems, so if something important stops working there is a substitute or an alternative path that would allow to keep operating. Robustness also relates to reliability: the capability to operate under a range of conditions. Finally, robustness also entails investing and maintaining elements of critical infrastructures.

- Resourcefulness:
  This concept refers to the ability to skilfully manage a disruption as it unfolds. Resourcefulness might depend on the resources available to overcome difficulties, but it is primarily people oriented as it is related for example to prioritizing what should be done, how to communicate an emergency message, how to manage people to evacuate the network, etc. This includes financial, social, physical, technological, information and environmental resources. This ability relies more on people, rather than on the infrastructure itself.

- Rapid recovery:
  This concept refers to the ability to get "back to normal" as quickly as possible after a disruption. It is oriented towards people as well as towards the infrastructure. With regards to people, this concept entails to carefully develop contingency plans, emergency plans, and counting with the right people and resources at the right place. With regards to the infrastructure orientation, it entails designs and constructions that provide the ability to recover from disruptions (e.g.: modular infrastructures that enables single components to be easily replaced, minimising the disruption or the loss of service, or flexible designs, such as bidirectional roads, that enable operators to temporarily adapt better to the required recuperation restrictions).

- Adaptability:
  More than the quality of being able to adjust to new conditions, which is already included in the rapid recovery ability, this concept refers to the ability to absorb new lessons that can be drawn from past events to improve resilience. Engineers, emergency planners, transport operators, owners, etc. are able to learn from experience and past failures. This concept is oriented towards people as it involves revising plans, procedures, and introducing new tools and technologies to improve the other three resilience concepts (robustness, resourcefulness, and rapid recovery). Learning from the past will allow to be better prepared for the next crisis.

11. POTENTIAL IMPROVEMENTS OF THE TOOLKIT FOR REAL COMMERCIALISATION

The Foresee Project recommendations for transportation infrastructures management have been used for Calle 30 case. Not only thinking on cyberattack hazard also for normal operation situations, taking especial consideration to resilience improvement. The conclusions of this study are shown in the following paragraphs.

- **Does FORESEE's results improve the quality of your analysis and infrastructure's management?**

  After the study it is clear the vital importance of the Calle 30 infrastructure.
  This case is already in service, by using the Foresee recommendations it is possible to improve the quality management. This is result of Analysing 28 indicators we can measure the level of resilience.

- **What could be improved for the final release of the components/Tool?**

  The document that develops the Foresee Project explains the procedures followed to develop the tools that will be used to assess resilience.
  In our opinion, and on the basis that only a part of these tools has been studied, we consider it particularly important to generate a tool for dialogue between the tools themselves and the user, so just introducing the data agreed for the operation of the system, it will be possible to obtain rapid and direct answers that will support the decisions to be taken, especially in the face of extreme events.

- **Would you pay for this kind of tool/service?**

  Decisions in the case of an extreme event, based on objective data and experienced with previous simulations, are a definitive support in the infrastructure management.
  As we have indicated in the reports, the tools provided by the Foresee Project give answers to decisive questions depending the situation. These are examples:

  - Effects on traffic, congestion. It helps to adopt properly decision of different alternatives, whether partial or total close or capacity reduction of the infrastructure load.
  - Decision on the maximum required speed.
  - Increase of travel time.
  - Possible impact on alternative routes.

  I would pay for this tool/service.

- **Was this type of analysis made before FORESEE? How it was made? How does FORESEE improve the results/analysis previously made? How does this FORESEE result improve your infrastructure's management**

  Spanish regulations for tunnels require an Operating Manual and a Self-Protection Plan, which cover most of the points covered by the Foresee Project.
  The difference is that it is not applied from the point of view of resilience as understood by Foresee.
  Sometimes there is an operating contract, which enhances the regulatory requirements, demanding service indicators such as response time, and time to return to normality.

The Foresee Project involves all phases from the initial study to the commissioning of the infrastructure as a whole, and always with the objective of improving resilience.
Furthermore, it allows measuring this resilience and scenarios simulation to train management options in order to improve the results of management in different events, especially those considered extreme.
All of the above improves and ensures management quality.

- **Does this tool/result facilitate your work? How? Can it be measured in working hours or €? What cost/resource efficiencies you expect these tools/results to have on your day-to-day business? (e.g. 10%-20% decrease in working hours over the first year; reduction of maintenance costs (20%-25%), Return on Investment (ROI) – 10-15%, increase in productivity 25-30% (check D8.6)**

  From the preliminary study to their management in the service phase, the Foresee tool/service is a genera compendium of regulations with a compilation of good practices that are applied to infrastructures. Consequently, it has an immediate effective application, and together with the definition of different indicators included in the Quality Plans, it allows a permanent monitoring of the management, also the requirements needed to keep the ideal level of resilience.

  Initially, it is difficult to quantify what the application of the Foresee tool represents in terms of working hours, maintenance costs, return of investment and increased productivity, but it is clear that, applying it we would be looking at a very positive scenario.

ANNEX 1. D1.1 – CASE STUDY 5: M-30 RING ROAD

1.1 INTRODUCTION

This appendix contains a proposal of how to measure service and resilience of the transport system in case study 5: The M-30 Ring Road (Madrid).

1.2 DEFINE TRANSPORT SYSTEM

1.2.1 Infrastructure

The M-30 ring-road is the most important and the busiest road infrastructure in Spain, with over than 1,5 million journeys per day, running through a complex urban environment, and includes circa 48 km of tunnels and a total of 118 lane km.

In terms of characteristics definition of the infrastructure, in Tables 1 and 2, a set of input data are reported that are necessary to estimate the service and the resiliency of the ring road. Given the illustrative purpose of this appendix, most of input data are received from the operators of the infrastructure and rest are assumptions, i.e. fictive, and should only be considered as such.

Madrid Calle 30 is a mixed economy company, that belongs to the Environment and Mobility Area of Madrid City Council.

Initially set up to carry out the M-30 ring road transformation project, with the aim of improving Madrid's competitiveness as a centre for economic, cultural, educational and leisure activities, between 2004 and 2007 the company carried out the reform of the M-30, with the renovation of seven junctions and the construction of more than fifty kilometres of tunnel, a work without parallel in the history of Madrid.

The company currently manages the operation, conservation and maintenance of the Calle 30 ring road and the surrounding infrastructure and spaces, such as junctions, bridges, green zones and open areas included in the ring road through its private partner and contractor of the public service management contract through a mixed economy company, the Empresa de Mantenimiento y Explotación de la M30, S.A. (M30 Maintenance and Operation Company).

This private partner, for the management of the conservation and maintenance of the infrastructure, has an operating staff made up of 280 qualified and experienced professionals, whose ultimate goal is to carry out the work quickly and with the quality demanded by the citizens of Madrid in the 21st century.

It also has a fleet of 80 vehicles of various types, depending on the function they are used for, including trucks for dealing with incidents, vans for signalling lane closures and self-propelled sweepers for cleaning.

Table 18. Event-independent inputs to measure the service.

Inputs	Symbol	Value
Annual cost of regular maintenance [€/m] *	Cm	172,0
Length of the infrastructure [m] *	Li	118000,0

Average length per person [m]*	L*	6000,0
N. of people traveling per day *	P	625000,0
N. of people traveling per work in a day *	Pw	562500,0
N. of people traveling per leisure in a day *	Pl	62500,0
Goods travelling per day [vehicles] *	G	6250,0
Cost of work time [€/min] Considering average 20€/hour.	Cwt	0,3
Cost of leisure time [€/min]*	Clt	0,2
Socio economic costs per person [€/p.p.]	SECp	0,1
Socio economic costs for goods [€/vehicles]	SECg	0,0
Impact of injuries per person [10^3€/p.p.]	Ip	10,0
Impact of death per person [10^3€/p.p.]	Dp	5000,0
Speed (average) [km/h] *	Sl	65,0
Delay per unit (person or vehicles) per day with no hazard event [min/p.u.]*	Dpud_0	5,2
Property damage probability with no hazard event [%] *	Ppd_0	4,4
Injury probability with no hazard event [%] *	Pi_0	0,0
Death probability with no hazard event [%] *	Pd_0	0,0
Property damage per person in case of accident [103€/p.p.]	PDp_0	2,0

Inputs with this asterisk are received from tunnel operator and rest are assumptions.

Table 19. Event-dependent inputs to measure the service

Inputs	**Symbol**	**Cyber-attack [_ca]**
Cost of intervention after the event [€/m]*	Ci	21,28
Delay per unit (person or vehicle) per day after an event [min/p.u.] *	Dpud	16
Days to recover in case of accident *	D	1
Property damage probability per event [%]	Ppd	4
Injury probability per event [%]	Pi	4
Death probability per event [%] *	Pd	0
Property damage per person in case of accident [10^3€/p.p.]	PDp	2

Inputs with this asterisk are received from tunnel operator and rest are assumptions.

1.2.2 Environment

This infrastructure is exposed to man-made events including cyberattack (due to the importance of Intelligent Transport Systems, particularly in the tunnel section) and not intentional like accidents (average number of 14 interventions/day due to accidents) or fire (generally caused by accidents).

The disruptions in the M-30 cause delays, traffic jams and have very relevant social-economic impact as it affects the daily commuting of an important percentage of the city.

1.2.3 Organization

The infrastructure is to be managed and operated by Calle 30, which is responsible for the operation and maintenance of this infrastructure only. This company is part of Madrid City Council and has a main peculiarity: it is a mixed public-private economy company that fully depends on the City Council. The private part is a consortium of O&M services suppliers that includes Ferrovial Servicios S.A.

Operation subcontractor company of the infrastructure is called Emesa and it is the M-30 Maintenance and Operation Company awarded the contract for the management and maintenance of the main ring road in Madrid.

1.3 MEASURE SERVICE

1.3.1 Define service to be considered

It is considered that this transport infrastructure is **managed throughout its life-cycle**, to provide service, i.e., to provide the ability,

- to a vehicle to travel around Madrid within a specific amount of time (travel time),
- to a vehicle to transport his/her property around Madrid without having his/her property damaged or being hurt or losing his/her life (safety),
- to a road manager to be able properly maintain the infrastructure without excessive spending (interventions),
- to the inhabitants of the Madrid Metropolitan Area to be able benefit of a good road connection (socio-economic activities).

The measure of all the services are defined in the following section along with the way these are computed.

1.3.2 Define the measure of service

A real measure of the 4 types of service introduced in the previous section is shown in Table 20. Annual estimated measure of service, along with the way it is computed in terms of annual estimate, along with the way it is computed. The measure is using the data given in Table 18. Event-independent inputs to measure the service. and Table 19. Event-dependent inputs to measure the service.

Table 20. Annual estimated measure of service, along with the way it is computed

Type of service	Measure	Annual estimate [10^3€]	Estimated as
Travel time	the travel time for all the people travelling between two points to be defined	*408.519,23 €*	*((Li/1'000)/Sl)*60* ((Pw*Cwt)+(Pl*Clt))*365*
Safety	the cost of repairing damaged property, the number of injuries and deaths due to people travelling from A to B as defined above	*20.257.500,00 €*	*(((Ppd_0/100)*P* PDp_0) + ((IPi_0/100)*P* Ip) + ((Pd_0/100)*P* Dp)))*365*
Interventions	The cost of keeping the infrastructure in, or restoring it to, an acceptable state	*20.296,00 €*	(Cm*Li)
Socio economic activities	This service is measured as the costs for the society due to the additional travel time for all the people travelling from A to B after a hazard. It is estimated the same way that the travel time is, except that here the socio-economic costs of delays	*118.625,00 €*	*((P*Dup_0*SECp)+ (G*Dup_0*SECg))*365*

	are considered, instead of the costs for travel time.		

1.3.3 Measure of the expected loss in level of service following a hazard event

In this section an example of how to quantify the expected loss of service of the infrastructure a cyber-attack event. The example is done using the data given in Table 18. Event-independent inputs to measure the service. and Table 19. Event-dependent inputs to measure the service.

Table 21 should be read as follows: the impact in terms of working travel time in case of cyber-attack event (€3.000.000) is estimated multiplying the number of workers traveling per day (562.500), for the average delay per person per day (16 minutes), for the cost of working time (0.3 €/min) for the average days in which the traffic is delayed due to interventions following the event (1). The formula used to compute each estimated loss in LOS, using the data Table 18. Event-independent inputs to measure the service. and Table 19. Event-dependent inputs to measure the service is given next to each impact.

Table 21. Example of the measure of the service on the M-30 following a cyber-attack event

Impact level 1	**Symbol**	**Description**	**Impact level 2**	**Symbol**	**Costs [10^3€]**		
					Estimate	**Computation**	**Estimate**
Interventions	Ii_m	The impact of executing interventions			2511	(Ci_m*Li)	2511
Travel time	Itt_m	The impact of travel condition in terms of time lost the impact of travel condition on the vehicle cost	Work	Itt.w_m	3000	(Pw*Dppd_m*Cwt*D_m)	3233
			Leisure	Itt.l_m	233	(Pw*Dppd_m*Clt*D_m)	
Safety	Is_m	The impact on the users and affected public due to the user being involved in an accident	Property damage	Is.pd_m	50000	((Ppd_m/100)*PDp_m*P)	300000
			Injury	Is.i_m	250000	((Ppd_m/100)*Ip_m*P)	
			Death	Is.d_m	0	((Ppd_m/100)*Dpp_m*P)	
Socio-economic activities	Ise_m	The contribution of the operation to socio-economic development, i.e. the socio and economical costs of people and goods not being able to travel	Persons	Ise.p_m	1000	(P*Dppd_m*D_m*SECp)	1000
			Goods	Ise.g_m	0	(P*Dppd_m*D_m*SECg)	
Total					306744	(Ii_m+Itt_m+Is_m+Ise_m)	306744

1.4 MEASURE RESILIENCE

1.4.1 Identify resilience indicators

In this section, 28 indicators are listed (Table 22, Table 23 and Table 24) that have been selected to measure the resilience to cyber-attack events. The indicators have been selected with the case study partners based on the list given in chapter 8 of this deliverable and a discussion on the need to also consider further ones. Each indicator is named with an ID that consists of a letter that stands for the hazard (i.e. "M" for cyber-attack events) and a progressive number that tracks the category the indicator belongs to (e.g. the indicator "Age / Age of replacement of the warning system" is identified among the resilience indicators for cyber-attack events, with the code M.1.1.1, as part of the category "Condition state of the infrastructure", identified with the ID M.1.1). This ID system helps to facilitate the logical traceability of each indicator to the categories it belongs to at the various levels.
An explanation is also reported for each indicator on the motivation for which it was chosen, i.e. the reason why it was considered relevant in the case study.

Table 22. Indicators of resilience to cyber-attack events (1/3): M.1. Infrastructure

ID	Level 1	ID	Indicator	Motivation (i.e. the indicator is selected for the case study because…)
M.1.1	CS of the infrastructure	M.1.1.1	Age / Age of replacement of the warning system	The older the warning systems, the more obsolete their performances and therefore the higher it is the probability of accidents due to a lack of signalling the danger in case of a cyber-attack event.
		M.1.1.2	Age / Age of replacement of safe shut down system	The older the safe shut down system, the more obsolete their performances and therefore the higher is the probability of accidents due to a lack of stopping the traffic in case of a cyber-attack event.
		M.1.1.3	Condition state of infrastructure	The better the condition state of the infrastructure, the lower is the probability of the infrastructure to be damaged following up with a cyber-attack event and the lower the consequences are in case it occurs.
		M.1.1.4	Condition state of protective structures/systems	The more deteriorated the protection systems, the lower is the probability that it can provide the LOS for which it was designed, and the higher the expected consequences are in case of a cyber-attack event.
		M.1.1.5	After-event condition state of infrastructure	The expected condition of the infrastructure after an event, is an indication of its ability to withstand it and, therefore, of higher resiliency.
		M.1.1.6	After-event condition state of protective structures/systems	The expected condition of the protective structures/systems after an event, is an indication of its ability to withstand the cyber-attack event and, therefore, of higher resiliency.
M.1.2	Protection measures	M.1.2.1	The possibility of using another means to satisfy transport demand	The possibility of re-routing people using temporary means reduces the consequences of an infrastructure being out of service.
		M.1.2.2	The presence of a safe shutdown system	The presence of a safe shut down system reduces the consequence of a cyber-attack event.
		M.1.2.3	The presence of a warning system	The presence of a warning system to prevent users to enter the stations in case of danger, reduces the consequence of a cyber-attack event.
		M.1.2.4	The presence of emergency / evacuation paths	The presence of an emergency path to allow users to escape in case of danger, reduces the consequence of a cyber-attack event.

		M.1.2.5	The presence of special measures to help evacuate persons	The possibility of using extraordinary measures to allow users to escape in case of danger, reduces the consequence of a cyber-attack event.
M.1.3	Preventive measures	M.1.3.1	Compliance with the current emergency design code	The more recent the level of compliance to the emergency design, the lower the impact of a cyber-attack event on the infrastructure.
		M.1.3.2	Strength of construction material used	The stronger the construction material of an infrastructure, the higher is the ability to withstand the effect of a cyber-attack event.

Table 23. Indicators of resilience to cyber-attack events (2/3): M.2. Environment

ID	Level 1	ID	Indicator	Motivation (i.e. the indicator is selected for the case study because…)
M.2.1	Context	M.2.1.1	Accessibility	The more the road is accessible, the less expensive it is to conduct the intervention on it.
		M.2.1.2	Extent of past damages due to hazards	The higher the past damages connected to a cyber-attack event, the higher is its probability of suffering strong events also in the future.
		M.2.1.3	Hazard zone	The more the road is in a zone exposed to cyber-attack events, the higher is its probability of being hit.
		M.2.1.4	Duration of past down time due to hazards	The highest the number of days per year that cyber-attack events have interrupted the service, the higher is its probability of suffering interruptions also in future.
		M.2.1.5	Budget availability	The higher the budget availability is, the higher is the probability and effectiveness of the executing the interventions to recover the disruption of a cyber-attack event.
		M.2.1.6	Traffic	The more traffic is on a road the higher is the exposition to consequences in case a cyber-attack event. occurs.

Table 24. Indicators of resilience to cyber-attack events (3/3): M.3. Organization

ID	Level 1	ID	Indicator	Motivation (i.e. the indicator is selected for the case study because…)
M.3.1	Pre-event activities	M.3.1.1	The presence of a monitoring strategy	The presence of a monitoring plan raises the awareness of the IM on the state of the road and his preparedness to react when necessary. A prepared IM is trusted to be more reactive and reduces the consequences of a cyber-attack event on traffic.
		M.3.1.2	The presence of a maintenance strategy	The presence of an intervention strategy lowers the probability that an infrastructure ends up in a deteriorated state.
		M.3.1.3	The extent of interventions executed prior to the event	The more it is spent on regular maintenance before the event, the lower is the probability that the infrastructure will suffer a drop in LOS following up with a cyber-attack event.
M.3.2	Post event activities	M.3.2.1	The presence of an emergency plan	The presence of an emergency plan reduces the time between the occurrence of a cyber-attack event and the moment an IM reacts.
		M.3.2.2	Practice of the emergency plan	The regular exercise of the emergency plan raises the ability of the IM to apply it when needed, reducing the time for execution and the risk of failure.
		M.3.2.3	Review/update of the emergency plan	The longer the time since the last review/update of the emergency plan the less the plan is trusted to be effective.
		M.3.2.4	Expected time for tendering	The longer the time for the for public tender the longer the infrastructure stays out of service.
		M.3.2.5	Expected time for demolition	The longer the time for demolition the longer the infrastructure stays out of service.
		M.3.2.6	Expected time for construction	The longer the time for construction the longer the infrastructure stays out of service.

1.4.2 Determine how resilience is to be measured

In this section the possible values of each resilience indicator are defined based on discussion and suggestions from the case study partners. The ranges of values are set so that the higher they are the more resilient the transport system. The ranges of values for cyber-attack events are given in tables (Table 25 -Table 29)

The indicators, or the entire tables of indicators, marked with an asterisk (*), e.g. "M.1.1.3 - condition state of the infrastructure", refers to multiple objects and can be measured in the following 5 ways:

(a) for each single object separately, i.e. for each tunnel, so that the condition state of each object is an indicator;
(b) as the average of all objects of one category, i.e. the average of the condition state of all the tunnels, so that the condition state of each category of objects is an indicator;
(c) as the worst of all objects of one category, i.e. the worst condition state of all the tunnels, so that the condition state of each category of objects is an indicator;
(d) as the average of all objects, i.e. the average of the condition state of all tunnels, so that the condition state the infrastructure is one indicator;
(e) as the worst of all objects, i.e. the worst condition state of all tunnels, so that the condition state the infrastructure is one indicator.

In this application we have assumed to consider the average (even though fictive) value of all objects. This was done because for illustrative purpose it brings no additional benefit to explode the number of indicators.

1.4.2.1. Possible values of resilience indicators for cyber-attack events

Table 25. Possible values of resilience indicators for cyber-attack events (1/5): M.1.1 - Condition state of the infrastructure*

ID	Indicator	Number of possible values	Number of possible values and meaning	
			N.	Meaning
M.1.1.1	"Age / Age of replacement of the warning system	3	0/3	> 80% of the expected life time achieved**
			1/3	> 50%, < 80% of expected life time achieved**
			2/3	> 20%, < 50% of expected life time achieved**
			3/3	< 20% of expected life time achieved**
M.1.1.2	Age / Age of replacement of the safe shut down system	3	0/3	> 80% of the expected life time achieved**
			1/3	> 50%, < 80% of expected life time achieved**
			2/3	> 20%, < 50% of expected life time achieved**
			3/3	< 20% of expected life time achieved**
M.1.1.3	Condition state of infrastructure	5	0/5	Condition State 5: A condition in which it is highly likely that the infrastructure would collapse under normal traffic loads over the next 20 years
			1/5	Not known. No information is available on the condition state of the infrastructure.
			2/5	Condition State 4: Bad (A condition in which it is moderately likely that infrastructure would collapse under normal traffic loads over the next 20 years)

			3/5	Condition State 3: Good (A condition in which it is unlikely that the infrastructure would collapse under normal traffic loads over the next 20 years)
			4/5	Condition State 2: Very good (A condition in which it is very unlikely that the infrastructure would collapse under normal traffic loads over the next 20 years)
			5/5	Condition State 1: Excellent A condition in which it is extremely unlikely that the infrastructure would collapse under normal traffic loads over the next 20 years
M.1.1.4	Condition state of protective structures/systems	5	0/5	Condition State 5: A condition in which it is highly likely that the infrastructure would collapse under normal traffic loads over the next 20 years
			1/5	Not known. No information is available on the condition state of the infrastructure.
			2/5	Condition State 4: Bad (A condition in which it is moderately likely that infrastructure would collapse under normal traffic loads over the next 20 years)
			3/5	Condition State 3: Good (A condition in which it is unlikely that the infrastructure would collapse under normal traffic loads over the next 20 years)
			4/5	Condition State 2: Very good (A condition in which it is very unlikely that the infrastructure would collapse under normal traffic loads over the next 20 years)
			5/5	Condition State 1: Excellent A condition in which it is extremely unlikely that the infrastructure would collapse under normal traffic loads over the next 20 years
M.1.1.5	After-event condition state of infrastructure	3	0/3	Collapsed, requires rebuilding
			1/3	Out of service, requires repair/rebuilding
			2/3	In service but repairs are necessary
			3/3	In service and no repairs necessary
M.1.1.6	After-event condition state of protective structures/systems	3	0/3	Collapsed, requires rebuilding
			1/3	Out of service, requires repair/rebuilding
			2/3	In service but repairs are necessary
			3/3	In service and no repairs necessary

** the percentage of expected life time achieved correspond to the amount of the expected total life of the object already passed, i.e. for an object that is expected to be functioning for 20 years and it is 10 years old at the moment of the evaluation, the percentage of life time achieved is 50%.

Table 26. Scale and measures of resilience indicators for cyber-attack events (2/5): M.1.2 - Protection measures

ID	Indicator	Number of possible values	Number of possible values and meaning	
			N.	Meaning
M.1.2.1	The possibility of using another means to satisfy transport demand	2	0/2	No alternative means
			1/2	Single alternative mean
			2/2	Multiple alternative means
M.1.2.2	The presence of a safe shutdown system	1	0/1	No safe shut down
			1/1	Safe shut down
M.1.2.3	The presence of a warning system	1	0/1	No warning system
			1/1	Warning system
M.1.2.4	The presence of emergency / evacuation paths	1	0/1	No emergency / evacuation paths
			1/1	Emergency / evacuation paths
M.1.2.5	The presence of special measures to help evacuate persons	1	0/1	No special measures
			1/1	Special measures

Table 27. Scale and measures of resilience indicators for cyber-attack events (3/5) M.1.3 - Preventive measures*

ID	Indicator	Number of possible values	Number of possible values and meaning	
			N.	Meaning
M.1.3.1	Compliance with the current emergency design code	2	0/2	Below current regulation
			1/2	According to current regulation
			2/2	Above current regulation
M.1.3.2	Strength of construction material used	3	0/3	Resistance D
			1/3	Resistance C
			2/3	Resistance B
			3/3	Resistance A

Table 28. Scale and measures of resilience indicators for cyber-attack events (4/5): M2 – Environment

ID	Indicator	Number of possible values	Number of possible values and meaning	
			N.	Meaning
M.2.1.1	Accessibility*	3	0/3	Accessible with specialised tunnelling equipment
			1/3	Accessible with normal tunnelling equipment
			2/3	Accessible with steps
			3/3	Accessible without equipment
M.2.1.2	Extent of past damages due to hazards*	3	0/3	Infrastructure collapse
			1/3	Serious damage
			2/3	Minor damage
			3/3	Aesthetic or no damages
M.2.1.3	Hazard zone*	3	0/3	High
			1/3	Medium
			2/3	Low
			3/3	None
M.2.1.4	Duration of past down time due to hazards*	2	0/2	2 weeks
			1/2	1-2 weeks
			2/2	1 day to 1 week
M.2.1.5	Budget availability	2	0/2	Enough for <50% of the intervention
			1/2	Enough for >50%, <100% of the intervention
			2/2	Enough for >100% of the intervention
M.2.1.6	Traffic*	3	0/3	<20% of capacity
			1/3	>20%, <50% of capacity
			2/3	>50%, <80% of capacity
			3/3	>80% of capacity

Table 29. Scale and measures of resilience indicators for cyber-attack events (5/5): M.3 – Organization*

ID	Indicator	Number of possible values	Number of possible values and meaning	
			N.	Meaning
M.3.1.1	The presence of a monitoring strategy	2	0/2	No condition state monitoring
			1/2	Periodic monitoring of the condition state
			2/2	Constant (i.e. automated) monitoring of the condition state
M.3.1.2	The presence of a maintenance strategy	2	0/2	No intervention strategy
			1/2	Only responsive interventions conducted
			2/2	Preventive interventions strategies are conducted
M.3.1.3	The extent of interventions executed prior to the event	2	0/2	<50% of the benchmark budget
			1/2	>50%, <80% of the benchmark budget
			2/2	> 80% of the benchmark budget
M.3.2.1	The presence of an emergency plan	2	0/2	No plan
			1/2	Generic plan
			2/2	Operative plan (with tasks, resources, ...)
M.3.2.2	Practice of the emergency plan	4	0/4	No exercise
			1/4	1 exercise every > than 2 years
			2/4	1 exercise every 2 years
			3/4	1 exercise every year
			4/4	1 exercise every 6 months
M.3.2.3	Review/update of the emergency plan	2	0/2	>5 years ago
			1/2	<5 years ago
			2/2	<2 years ago
M.3.2.4	Expected time for tendering	3	0/3	> 1 year
			1/3	> 8 months and < 1 year
			2/3	> 4 months and < 8 months
			3/3	< 4 months
M.3.2.5	Expected time for demolition	3	0/3	> 1 year
			1/3	> 8 months and < 1 year
			2/3	> 4 months and < 8 months
			3/3	< 4 months
M.3.2.6	Expected time for construction	3	0/3	> 1.5 year
			1/3	> 1 year and < 1.5 year
			2/3	> 6months and < 1 year
			3/3	< 6 months

1.4.3 Measure resilience using indicators

According to the explanation of the measure of resilience using indicators given in the chapter 1.4.2 of this deliverable, an example is reported in this section of resilience measure using: (i) differentiated weights, (ii) equal weights, and (iii) no weights (i.e. percentage of fulfilment).

1.5 MEASURE OF RESILIENCE USING DIFFERENTIATED WEIGHTS

A sample of the measure of resilience using differentiated weights is reported in this section for the three levels: the aggregated categories of indicator at level 0 and level 1, and the singular indicators. In particular, in Figure 45. Cyber-attack events. Measure of resilience using differentiated weights. Level 0 the measure of resilience for the level 0 is shown for cyber-attack events. In Figure 46. Cyber-attack events. Measure of resilience using differentiated weights. Level 1 for the category M.1 (Infrastructure) the measure of resilience for the level 1 categories belonging to the level 0 category M.1 (Infrastructure) is displayed, whereas in Figure 47. Cyber-attack events. Measure of resilience using differentiated weights. Single indicators part of the category M.2.1 (Environment – Context), the measure of resilience for the single indicators belonging to the level 1 category M.2 (Environment – Context) is displayed.

Each figure is built reporting at the top the resilience of each indicator, or category of indicators, with respect to all services, while on the other graphs this is reported for one service at a time (i.e., intervention, travel time, accident, and socio-economic). The figures in this section should be read as in the following examples.

When considering the 3 level 0 aggregated categories or resilience indicators to cyber-attack events (**¡Error! No se encuentra el origen de la referencia.**), i.e. Infrastructure (M.1), organization (M.2) and Environment (M.3), M.3 is the one with the lowest resiliency, with M.1 being the second and M.2 the first.

When looking specifically into the level 0 category M.1 (Figure 46. Cyber-attack events. Measure of resilience using differentiated weights. Level 1 for the category M.1 (Infrastructure)) it can be noticed that this is due to the percentage of fulfilment of 3 level 1 categories, i.e. condition state of the infrastructure (M.1.1), protection measures (M.1.2) and preventive measures (M.1.3), where M1.2 and M.1.3 are the categories have zero impact on the service and M1.1 is the responsible for the highest potential loss of service in general.

Finally, when investigating more in depth the reasons of the resiliency of the level 1 category M.2.1 for example (Figure 47. Cyber-attack events. Measure of resilience using differentiated weights. Single indicators part of the category M.2.1 (Environment – Context)), it can be seen that this is due to the percentage of fulfilment of 2 indicators (M.2.1.3, and M.2.1.6), in which M.2.1.3 (Hazard zone) is the one that contribute the most in increasing the resiliency related costs of the level 1 category M.2.1.

The measure of resilience for each indicator using differentiated weights is estimated as the sum of the measure of resilience for each service, which is obtained multiplying the remaining of the measure of the resilience without weight for the impact on the specific service (only for the services that are affected by the indicator). With differentiated weights the impact of each single indicator on the various services is computed as a percentage of the maximum impact on each indicator.

The (fictive) differentiated resilience weights of indicators on service used for are reported in Table 30. Differentiated resilience weights of indicators on service for cyber-attack events.

As an example, the measure of resilience on travel time for the indicator M.3.2.2 is 85% (i.e. 100%-15%) times €3.233 (the impact in terms of travel time in case of cyber-attack events, as given in **¡Error! No se encuentra el origen de la referencia.**). To aggregate the measures of single i ndicators for categories of indicators, e.g. the measure of resilience on the travel time service of the category "M.1.3. Preventive measures", the percentage of not fulfilment of M.1.3 (i.e. 50%) is multiplied for the average of the total impact on service of indicators M.1.3.1 to M.1.3.2.

The same logic holds true for the hazard of cyber-attack events.

Table 30. Differentiated resilience weights of indicators on service for cyber-attack events

ID	[%]	[€ x 10^3]				Total [€]
		Intervention	Travel time	Accident	Socio-econ.	
M.1.1.1	50%	1.256	1.617	150.000	500	153.372
M.1.1.2	50%	1.256	1.617	150.000	500	153.372
M.1.1.3	50%	1.256	1.617	150.000	500	153.372
M.1.1.4	50%	1.256	1.617	150.000	500	153.372
M.1.1.5	30%	753	970	90.000	300	92.023
M.1.1.6	30%	753	970	90.000	300	92.023
M.1.2.1	80%	2.009	2.587	240.000	800	245.395
M.1.2.2	80%	2.009	2.587	240.000	800	245.395
M.1.2.3	80%	2.009	2.587	240.000	800	245.395
M.1.2.4	80%	2.009	2.587	240.000	800	245.395
M.1.2.5	80%	2.009	2.587	240.000	800	245.395
M.1.3.1	80%	2.009	2.587	240.000	800	245.395
M.1.3.2	80%	2.009	2.587	240.000	800	245.395
M.2.1.1	80%	2.009	2.587	240.000	800	245.395
M.2.1.2	16%	402	517	48.000	160	49.079
M.2.1.3	65%	1.632	2.102	195.000	650	199.384
M.2.1.4	18%	452	582	54.000	180	55.214
M.2.1.5	70%	1.758	2.263	210.000	700	214.721
M.2.1.6	65%	1.632	2.102	195.000	650	199.384
M.3.1.1	79%	1.984	2.554	237.000	790	242.328
M.3.1.2	91%	2.285	2.942	273.000	910	279.137
M.3.1.3	91%	2.285	2.942	273.000	910	279.137
M.3.2.1	85%	2.134	2.748	255.000	850	260.733
M.3.2.2	85%	2.134	2.748	255.000	850	260.733
M.3.2.3	69%	1.733	2.231	207.000	690	211.654
M.3.2.4	12%	301	388	36.000	120	36.809
M.3.2.5	12%	301	388	36.000	120	36.809
M.3.2.6	12%	301	388	36.000	120	36.809

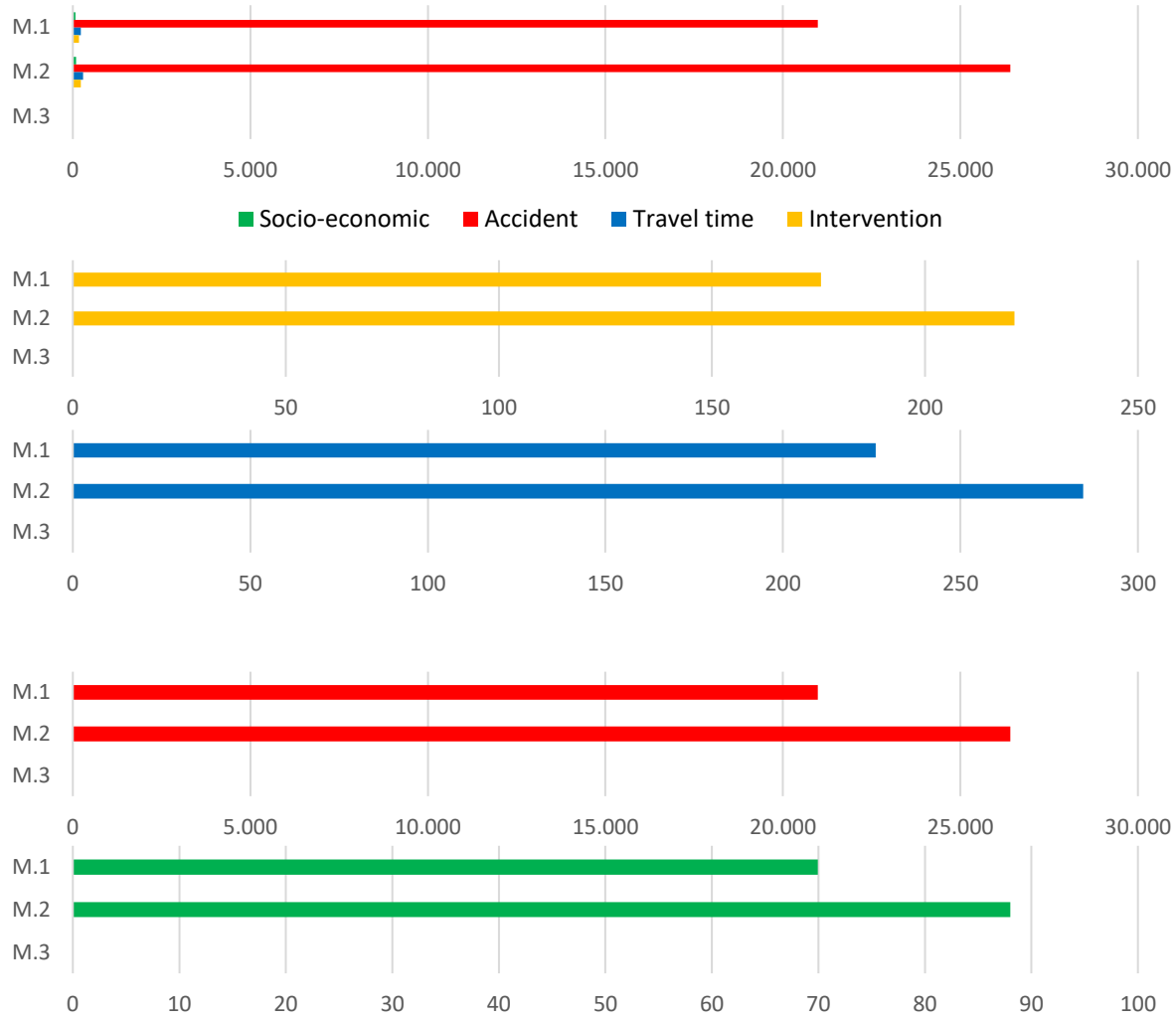
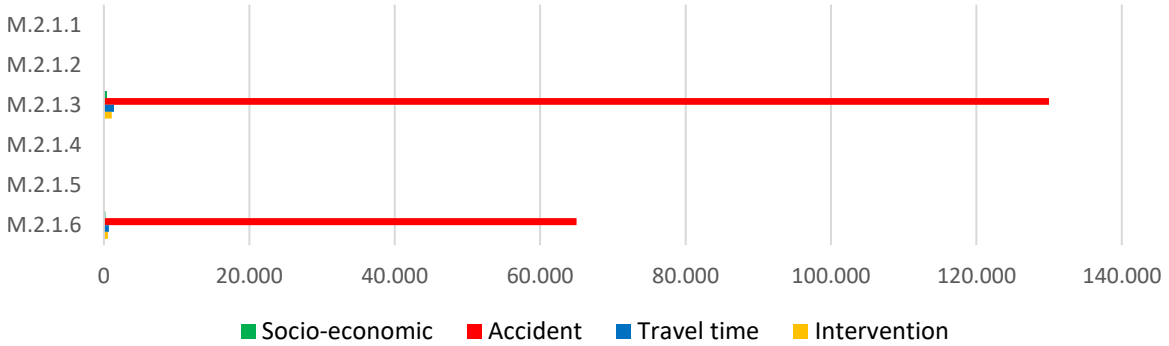


Figure 45. Cyber-attack events. Measure of resilience using differentiated weights. Level 0

Figure 46. Cyber-attack events. Measure of resilience using differentiated weights. Level 1 for the category M.1 (Infrastructure)



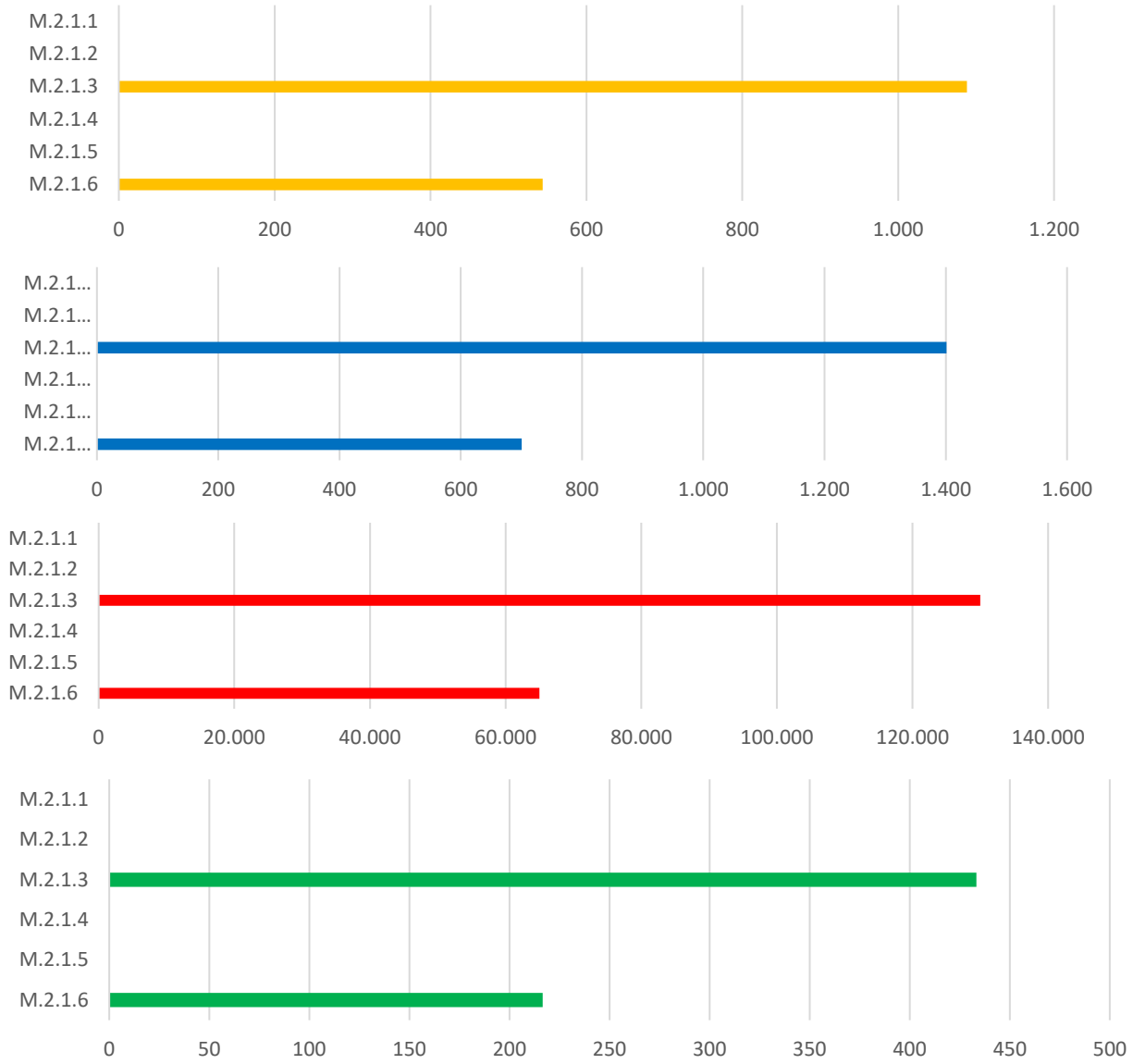


Figure 47. Cyber-attack events. Measure of resilience using differentiated weights. Single indicators part of the category M.2.1 (Environment – Context)

1.6 MEASURE OF RESILIENCE USING EQUAL WEIGHTS

When for the measure of resilience, the differentiated weights cannot (or do not want to) be used, a simplified possibility is to neglect the fact that different indicators impact the service differently and to make the simplified assumption that they have all equal weights.

A sample of the measure of resilience using equal weights is reported in this section for the three levels: the aggregated categories of indicator at level 0 and level 1, and the singular indicators.

Each figure is built and has to be read with the same logic used in the previous section for the measure of service using the equal weights.

With reference to the computation though, the measure of resilience for each indicator using equal weights is estimated as the sum of the measure of resilience for each service, which is obtained multiplying the remaining of the measure of the resilience without weight for the impact on the specific service (only for the services that are affected by the indicator). As an example, the measure of resilience on travel time for the indicator M.2.1.2is 16% (i.e. 100%-84%) times €3.233 (Impact in terms of travel time in case of cyber-attack event).

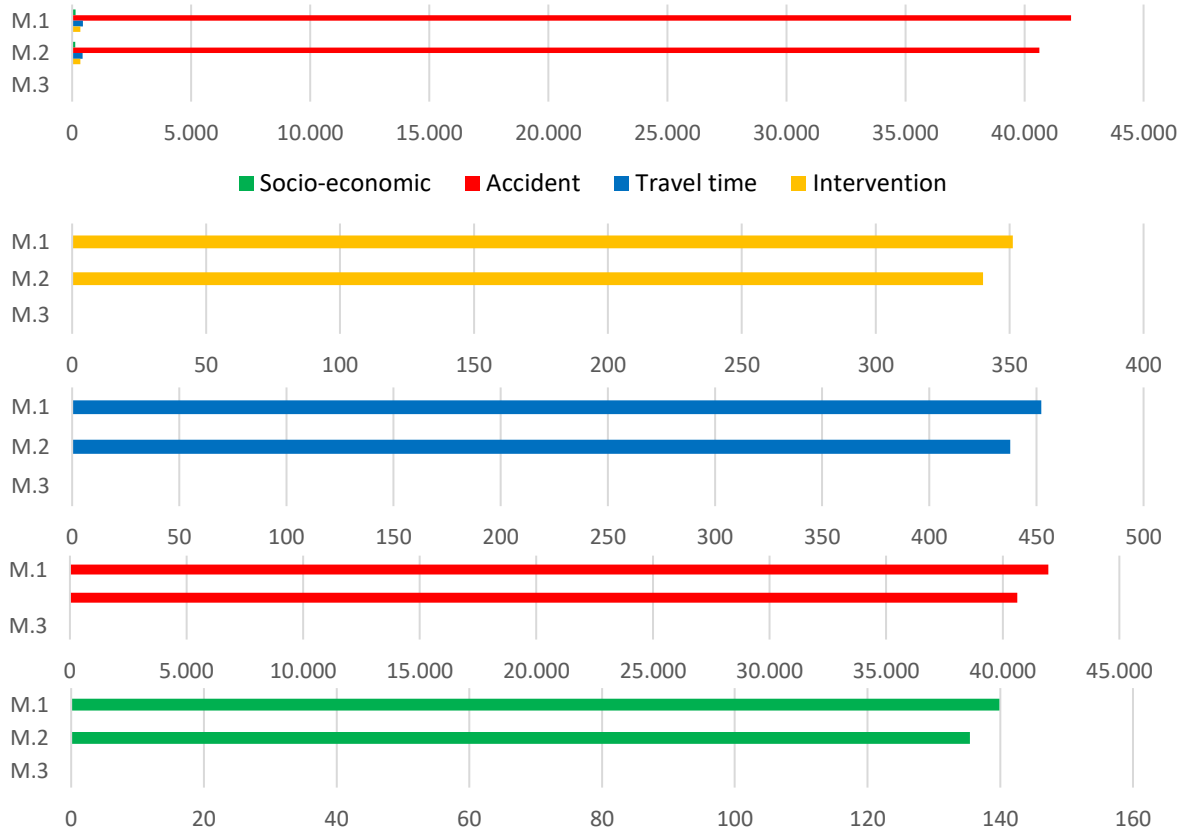


Figure 48. Cyber-attack events. Measure of resilience using equal weights. Level 0

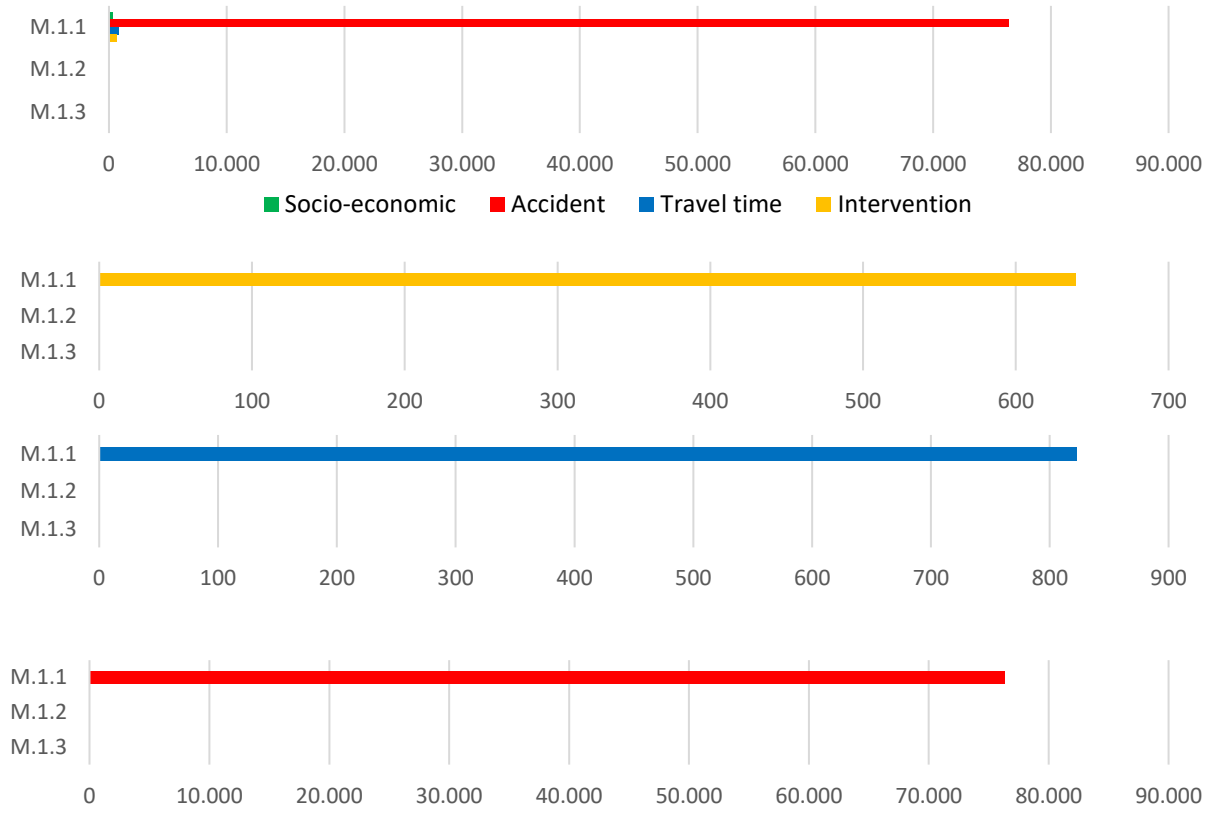
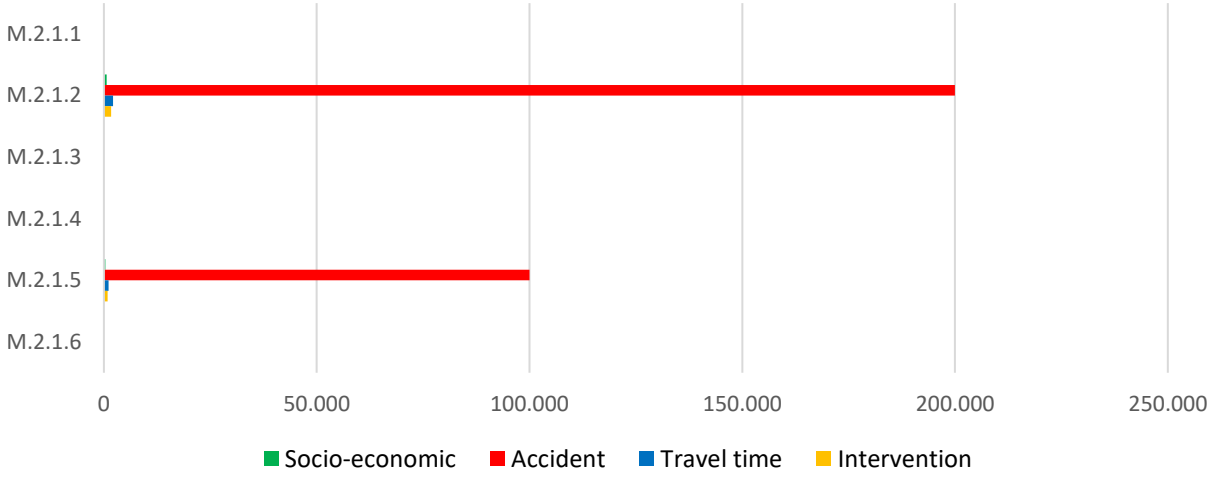


Figure 49. Cyber-attack events. Measure of resilience using equal weights. Level 1 for the category M.1 (Infrastructure)



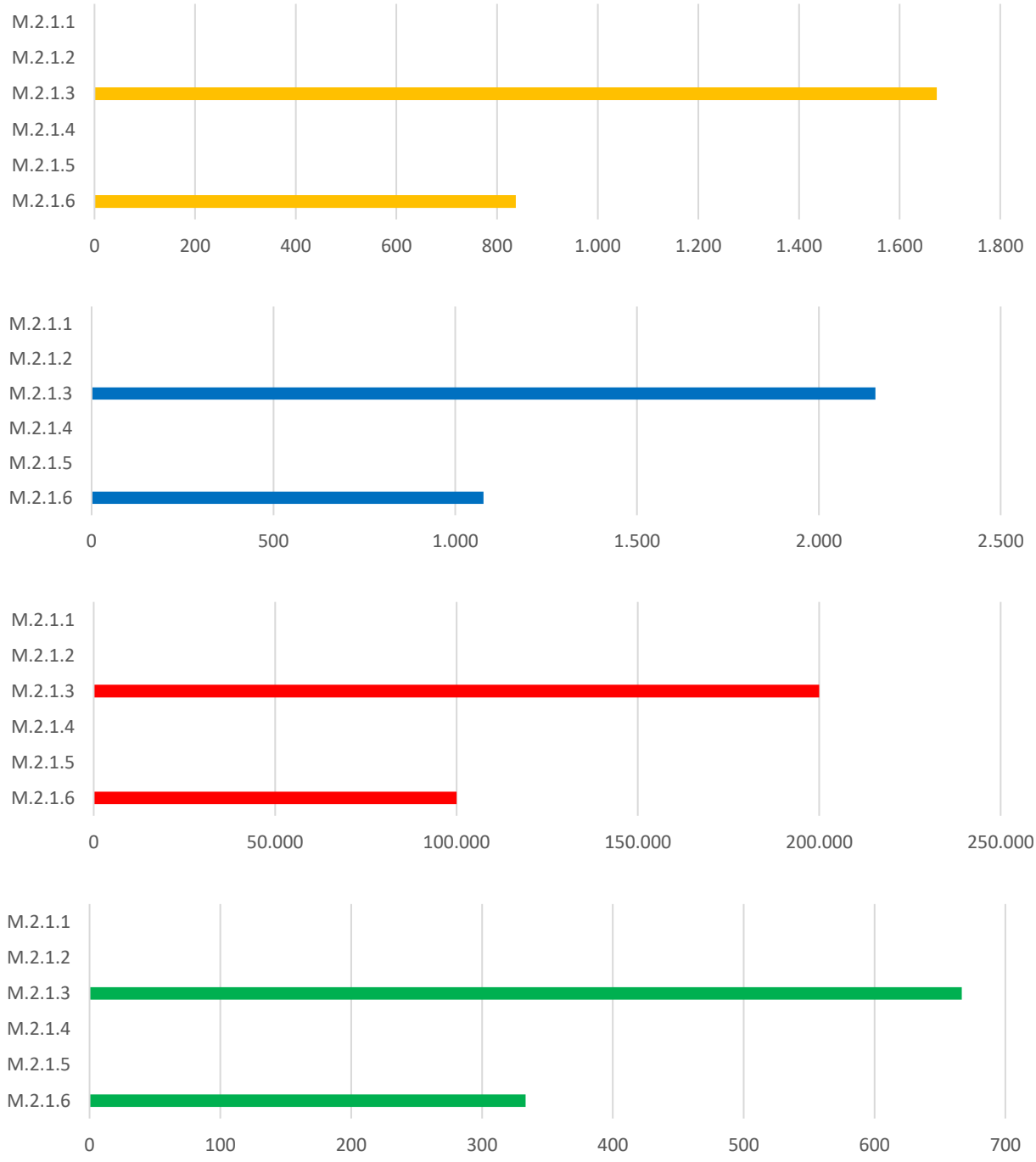


Figure 50. Cyber-attack events. Measure of resilience using equal weights. Single indicators part of the category M.2.1 (Environment – Context)

1.7 MEASURE OF RESILIENCE WITH NO WEIGHTS (USING PERCENTAGE OF FULFILLMENT)

When for the measure of resilience neither the differentiated, nor the equal weights should be used, a simplified possibility is to neglect the impact that indicators have on the service and only

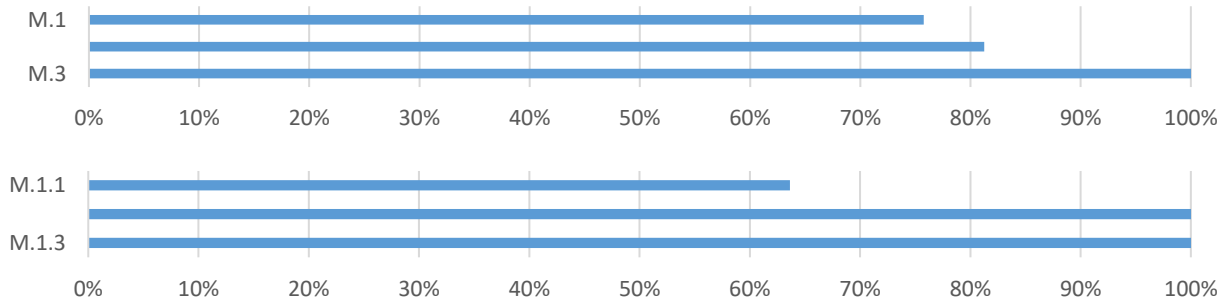
focus on their percentage of target fulfilment, i.e. the extent to which the actual conditions match the condition that are considered optimal for each indicator.

A sample of the measure of resilience using no weights is reported in this section for cyber-attack hazard and for the three levels: the aggregated categories of indicator at level 0 and level 1, and the singular

Figure 51. Cyber-attack events. Measure of resilience using no weights for the levels: 0, at the top; 1 for the category M.1 (Infrastructure), in the middle; and single indicators part of the category M.2.1 (Environment – Context), at the bottom. can be read as it follows: when considering the 3 level 0 aggregated categories or resilience indicators to cyber-attack (Figure 51. Cyber-attack events. Measure of resilience using no weights for the levels: 0, at the top; 1 for the category M.1 (Infrastructure), in the middle; and single indicators part of the category M.2.1 (Environment – Context), at the bottom., top), i.e. Infrastructure (M.1), organization (M.2) and Environment (M.3), M.1 is the one with the biggest gap between the maximum resiliency potential and the actual resiliency of the case, i.e. the biggest margin of improvement. When looking specifically into the level 0 category M.1 (Figure 51. Cyber-attack events. Measure of resilience using no weights for the levels: 0, at the top; 1 for the category M.1 (Infrastructure), in the middle; and single indicators part of the category M.2.1 (Environment – Context), at the bottom., middle) it can be noticed that this is due to the percentage of fulfilment of 3 level 1 categories, i.e. condition state of the infrastructure (M.1.1), protection measures (M.1.2) and preventive measures (M.1.3). Finally, when investigating more in depth the reasons of the resiliency of for example the level 1 category M.2.1 (Figure 51. Cyber-attack events. Measure of resilience using no weights for the levels: 0, at the top; 1 for the category M.1 (Infrastructure), in the middle; and single indicators part of the category M.2.1 (Environment – Context), at the bottom. bottom), it can be seen that this is due to the percentage of fulfilment of 2 indicators (M.2.1.3, and M.2.1.6), among which M.2.1.6 is the one with the lowest percentage of target fulfilment.

The measures of resilience for single indicators using no weights is obtained as the ratio between the value measured for the specific indicator and the maximum value of the scale, e.g. for the indicator M.3.2.2 (Practice of the emergency plan) the maximum scale is 4, while the measure achieved is 4, so the measure of resilience is 100% (4/4). These measures have then been aggregated for categories of indicators, dividing the sum of the measures of indicators by the sum of the scales.

The same logic applies to the hazard of cyber-attack events.



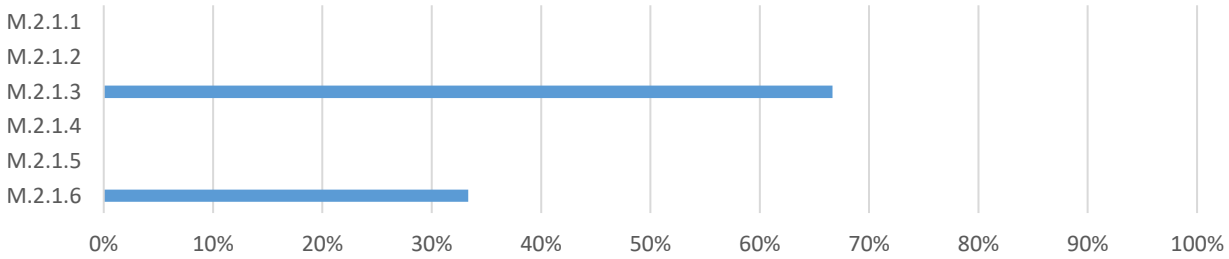


Figure 51. Cyber-attack events. Measure of resilience using no weights for the levels: 0, at the top; 1 for the category M.1 (Infrastructure), in the middle; and single indicators part of the category M.2.1 (Environment – Context), at the bottom.

1.8 DISCUSSION AND CONCLUSION

In the case study application, it is shown how the service and the resiliency can be estimated for the M-30, in such a way that:

- The measure of the service allows to quantify the impact of any loss of service for the interested stakeholders, and
- The measure of resilience allows to quantify the impact of cyber-attack event on the service

The measure of resilience of the transportation system is to be read differently depending on which of the three ways is used to do the measure:

- When equal or differentiated weights are used the resiliency is expressed in terms of loss of service, i.e. the higher the loss in service (quantified in monetary values) the lower the resiliency of the system;
- While when no weights are used the resiliency is expressed in terms of percentage of fulfilment of the target, i.e. the extent to which the actual conditions match the condition that are considered optimal for each indicator.

Moreover, it is possible to observe that the three ways proposed to do the measurement (i.e. with no weights, with equal weights and with differentiated weights) involve different levels of complexity in order to be performed, but also provide different degrees of refinements in the measures. In particular, for example:

- The measure with no weights only allows to identify indicators with the lowest percentage of target fulfilment. This is relatively easy to do but does not allow to consider if an indicator has an impact on many services (e.g. M.3.2.4) or only on few (e.g. M.1.2.3).
- The measure with equal weights allows to appreciate not only the target fulfilment but also the number of service it impacts, i.e. indicator M.2.1.3 register a relatively high value, while M.2.1.6 a lower one because the first impact on all services, while the second only on two. This though still doesn't allow to see how much each service is impacted.
- The measure with differentiated weights allows to appreciate also the difference how much each service is impacted by the target fulfilment of all indicators, and this impact the measure.

It is also to be noted that the results of the analysis can be broken down to narrow a particular subsection of any level of the indicators structure. This implies that, other than considering the overall measure of resilience of the infrastructure, it is also possible for Calle 30 to investigate in detail the measure of resiliency specifically due to the organization, rather than due to the infrastructure in itself, or the environment. Or, even in more detail, the measure of resiliency due only to the condition state of the infrastructure. This is seen as a useful tool to realize both:

(a) What is the overall resilience of the infrastructure, and
(b) How to intervene to improve it, when possible.

ANNEX 2. D1.2 – CASE STUDY 5: M-30 RING ROAD

1.1 INTRODUCTION

This appendix contains a proposal of how set target levels of service and resilience for infrastructures of the transport system in case study case study 5: The M-30 Ring road (Madrid).

To facilitate reading, chapter 1 presents again the case study description as from the appendix 1 of the deliverable D1.1, which includes a description of: the infrastructure, the environment, the organization and the inputs from the measure of service and resilience.

With this information, in the following chapters the four steps of the process to set service and resilience targets are applied, as presented in the deliverable D1.2:
1) gather all relevant stakeholders,
2) determine legal requirements,
3) determine stakeholder requirements, and
4) set targets.

The data and calculation process is a mere exercise, and it doesn't reflect the current and real numbers used by the Case Study, and the results cannot be in any way connected to the real situation.

1.1.1 Infrastructure

The M-30 ring-road is the most important and the busiest road infrastructure in Spain, with over than 1,5 million journeys per day, running through a complex urban environment, and includes circa 48 km of tunnels and a total of 118 lane km.

In terms of characteristics definition of the infrastructure, in Table 31. Event-independent inputs to measure the service. and Table 32 a set of input data are reported that are necessary to estimate the service and the resiliency of the ring road. Given the illustrative purpose of this appendix, most of input data received from the operators of the infrastructure and rest are assumptions, i.e. fictive, and should only be considered as such.

Operation subcontractor company of the infrastructure is called Emesa and it is the M-30 Maintenance and Operation Company awarded the contract for the management and maintenance of the main ring road in Madrid.

Table 31. Event-independent inputs to measure the service.

Inputs	Symbol	Value
Annual cost of regular maintenance [€/m] *	Cm	172,0
Length of the infrastructure [m] *	Li	118000,0
Average length per person [m]*	L*	6000,0
N. of people traveling per day *	P	625000,0
N. of people traveling per work in a day *	Pw	562500,0
N. of people traveling per leisure in a day *	Pl	62500,0
Goods travelling per day [vehicles] *	G	6250,0
Cost of work time [€/min] Considering average 20€/hour.	Cwt	0,3
Cost of leisure time [€/min]*	Clt	0,2
Socio economic costs per person [€/p.p.]	SECp	0,1
Socio economic costs for goods [€/vehicles]	SECg	0,0
Impact of injuries per person [10^3€/p.p.]	Ip	10,0
Impact of death per person [10^3€/p.p.]	Dp	5000,0
Speed (average) [km/h] *	Sl	65,0
Delay per unit (person or vehicles) per day with no hazard event [min/p.u.]*	Dpud_0	5,2
Property damage probability with no hazard event [%] *	Ppd_0	4,4
Injury probability with no hazard event [%] *	Pi_0	4,0
Death probability with no hazard event [%] *	Pd_0	0,0
Property damage per person in case of accident [103€/p.p.]	PDp_0	2,0

Inputs with this asterisk are received from tunnel operator and rest are assumptions.

Table 32. Event-dependent inputs to measure the service.

Inputs	Symbol	Cyber-attack [_ca]
Cost of intervention after the event [€/m]	Ci	21,28
Delay per unit (person or vehicle) per day after an event [min/p.u.] *	Dpud	16
Days to recover in case of accident *	D	1
Property damage probability per event [%] *	Ppd	4
Injury probability per event [%] *	Pi	4
Death probability per event [%] *	Pd	0
Property damage per person in case of accident [10^3€/p.p.] *	PDp	2

Inputs with this asterisk are received from tunnel operator and rest are assumptions.

1.1.2 Environment

This infrastructure is exposed to cyberattack events including cyberattack (due to the importance of Intelligent Transport Systems, particularly in the tunnel section) and not intentional like accidents (average number of 14 interventions/day due to accidents) or fire (generally caused by accidents).

The disruptions in the M-30 cause delays, traffic jams and have very relevant social-economic impact as it affects the daily commuting of an important percentage of the city.

1.1.3 Organization

The infrastructure is to be managed and operated by Calle 30, which is responsible for the operation and maintenance of this infrastructure only. This company is part of Madrid City Council and has a main peculiarity: it is a mixed public-private economy company that fully depends on the City Council. The private part is a consortium of O&M services suppliers that includes Ferrovial Servicios S.A.

Operation subcontractor company of the infrastructure is called Emesa and it is the M-30 Maintenance and Operation Company awarded the contract for the management and maintenance of the main ring road in Madrid.

1.1.4 Inputs from the measure of service and resilience

In order to set the target levels of service and resilience for infrastructures of the transport system in case study 5: The M-30 ring-road, some input information is required, namely:

- the expected reduction in the level of service following cyberattack event,
- the resilience indicators following cyberattack event, and
- the maximum expected reduction in the level of service for specific indicators, estimated considering both equal and differentiated weights.

For the scope of this work, this information is assumed as given in the appendix 1 of the deliverable D1.1.

1.2 TASK 1: GATHER ALL RELEVANT STAKEHOLDERS

In this task, all relevant stakeholders are gathered, whose opinion on setting the service and resilience targets, or the resilience indicator targets, should be considered. This includes Calle 30 as operator, employee's representatives, customer representatives, and government regulators.

In order to comply with this point, various meetings were held with the people responsible for the company EMESA.

1.3 TASK 2: DETERMINE LEGAL REQUIREMENTS

In this task, all relevant legal requirements are determined, by specially tasked legal experts from both the operator and the regulator side. For the illustrative purpose of this document, examples of legal requirements are shown both for the service (section 3.1) and for the indicators (section 3.2).

Legal requirements are set by the R.D.635/2006 related to the minimum requirements related to safety in road tunnels in Spain and R.D. 393/2007 related to the Basic Self-Protection Standard for places that are dedicated to activities that may give rise to emergency situations.

1.3.1 Determine legal requirements on the service

In this section an example of legal requirements on the service are reported with reference to both the occurrence of a cyberattack event (section 3.1.1).

1.3.2 Legal requirements on the service after a cyberattack event

With reference to the service following a cyberattack event, a legal requirement has been identified only for the service of "safety". Table 33 has to be read as follows: it is unacceptable by law that a total impact on the safety of users exceeds a value of € 145'000'000. This means that, considering the input value on the costs of property damages, injuries, and fatalities (as from **¡Error! No se encuentra el origen de la referencia.¡Error! No se encuentra el origen de la referencia.**), 25 fatalities and 2000 injuries following a cyberattack event would not be a tolerable value for the cyberattack event (i.e. it would be € 125'000'000 + € 25'000'000 = € 145'000'000).

Table 33. Legal requirements on the service after a cyberattack event

Impact level 1	Symbol	Legal requirement [10^3€]	Impact level 2	Symbol	Legal requirement [10^3€]
Restoration interventions	Ii_m	1.758			1.758
Travel time	Itt_m	2.587	Work	Itt.w_m	-
			Leisure	Itt.l_m	-
Safety	Is_m	145.000	Property damage	Is.pd_m	20.000
			Injury	Is.i_m	125.000
			Death	Is.d_m	0
Socio-economic activities	Ise_m	700	Persons	Ise.p_m	-
			Goods	Ise.g_m	-

1.3.3 Determine legal requirements on the indicators

In this section an example is reported on how legal requirements can be set also on indicators for a cyberattack event (section 3.2.1).

1.3.4 Legal requirements on the indicators of resilience to cyberattack event

A legal requirement has been hypothesized for 5 indicators of resilience to cyberattack in this document. With reference to these, Table 34 has to be read as follows: it is unacceptable by law that the indicator M.1.1.3 (Condition state of infrastructure), that has a maximum possible value of 5 (i.e. excellent condition state) and a minimum value of 0 (i.e. unable to provide protection) is set to a lower level than value 5.

Table 34. Legal requirements on the indicators of resilience to cyberattack

ID	Indicator	N possible values	Legal requirement
M.1.1.2	Age / Age of replacement of safe shut down system	3	-
M.1.1.3	Condition state of infrastructure	5	5
M.1.2.3	The presence of a warning system	1	1
M.1.3.1	The presence of emergency / evacuation paths	2	1
M.3.2.1	The presence of an emergency plan	2	2

1.4 TASK 3: DETERMINE STAKEHOLDER REQUIREMENTS

In this task, the requirements of the stakeholders, in addition to legal requirements, are determined. For the scope of this work it has been hypothesized that no additional requirements were set on the service. There are no additional requirement from the stakeholders.

1.5 TASK 4: SET TARGETS

In this task, the targets are set. The next 4 subsections show the application of the different methods, depending on whether service and resilience is measured directly or with indicators, and whether or not cost-benefit analysis should be used.

1.5.1 Service and resilience targets without cost-benefit analysis

In this section, the service and resilience targets are set taking into consideration the requirements defined in the previous two tasks, and by using direct measures of service and resilience without cost-benefit analysis. Table 35 has to be read as follows: the stakeholders have set the target for the service of restoration intervention costs at € 1.758.000, which is 70% of the maximum reduction in service estimated in the appendix 1 of the deliverable D1.1. The maximum reduction in service for restoration intervention (€ 2.511.000) was estimated multiplying an average cost of restoration intervention of 21.28 €/m for the whole 118.000m of the ring road. In setting this target the stakeholders have considered acceptable that following a cyberattack event, restoration interventions need to be run on 70% of the whole length of the ring road line, i.e. having at least half of the lanes restored fully, plus the most important turnoffs and exits. For the service of safety, targets have been sets for each of the specific impacts of level 2, i.e. property damage, injuries and fatalities. These were all set with a similar logic than the one used in the for the restoration intervention

Table 35. Service and resilience targets without cost-benefit analysis following cyberattack event

Impact level 1	Symbol	Description	Targets [10^3€]	Impact level 2	Symbol	Targets [10^3€]
Restoration interventions	Ii_e	The impact of executing interventions after the event	1.758			1.758
Travel time	Itt_e	The impact of the additional travel time on passengers	2.587	Work	Itt.w_f	-
				Leisure	Itt.l_f	-
Safety	Is_e	The impact on the users and affected public due to the user being involved in an accident	145.000	Property damage	Is.pd_f	20.000
				Injury	Is.i_f	125.000
				Death	Is.d_f	0
Socio-economic activities	Ise_e	The contribution of the road operation to socio-economic development, i.e. the socio and economical costs of people and goods not being able to travel	700	Persons	Ise.p_f	-
				Goods	Ise.g_f	-

1.5.2 Resilience indicator targets without cost-benefit analysis

In this section, the resilience indicator targets are set taking into consideration the requirements defined in the previous two tasks and by using resilience indicators without cost-benefit analysis. Table 36 has to be read as follows: for the indicator M.1.1.2 "Age / Age of replacement of safe shut down system", which can take a maximum value of 3 (i.e. < 20% of the service life achieved), and a minimum value of 0 (i.e. > 80% of the service life achieved), the target set, i.e. the level of acceptability to be guaranteed is 0.

Table 36. Resilience indicator targets for cyberattack event without cost-benefit analysis

ID	Indicator	N possible values	Targets
M.1.1.1	Age / Age of replacement of the warning system	3	0
M.1.1.2	Age / Age of replacement of safe shut down system	3	0

M.1.1.3	Condition state of infrastructure	5	5
M.1.1.4	Condition state of protective structures/systems	5	5
M.1.1.5	After-event condition state of infrastructure	3	3
M.1.1.6	After-event condition state of protective structures/systems	3	3
M.1.2.1	The possibility of using another means to satisfy transport demand	2	2
M.1.2.2	The presence of a safe shutdown system	1	1
M.1.2.3	The presence of a warning system	1	1
M.1.2.4	The presence of emergency / evacuation paths	1	1
M.1.2.5	The presence of special measures to help evacuate persons	1	1
M.1.3.1	Compliance with the current emergency design code	2	1
M.1.3.2	Strength of construction material used	3	3
M.2.1.1	Accessibility	3	3
M.2.1.2	Extent of past damages due to hazards	3	3
M.2.1.3	Hazard zone	3	3
M.2.1.4	Duration of past down time due to hazards	2	3
M.2.1.5	Budget availability	2	2
M.2.1.6	Traffic	3	2
M.3.1.1	The presence of a monitoring strategy	2	2
M.3.1.2	The presence of a maintenance strategy	2	2
M.3.1.3	The extent of interventions executed prior to the event	2	2
M.3.2.1	The presence of an emergency plan	2	2
M.3.2.2	Practice of the emergency plan	4	3
M.3.2.3	Review/update of the emergency plan	2	2
M.3.2.4	Expected time for tendering	3	3
M.3.2.5	Expected time for demolition	3	3
M.3.2.6	Expected time for construction	3	3

1.5.3 Service and resilience targets with cost-benefit analysis

In this section, the service and resilience targets are set taking into consideration the requirements defined in the previous two tasks, and the benefits and costs of achieving the targets. Table 37 has to be read as follows: three possible target sets have been defined, out of the many possible, namely:

- TS_M1: with which no change in any service is acceptable
- TS_M2: with which only the legal minimum has to be provided, and
- TS_M3: with which a desired maximum restoration budget after a cyberattack event has to be kept.

The three targets sets come at different costs, i.e. the costs of achieving the targets, and provide different benefits in terms of expected savings in the reduction of service (for each service). All costs and benefits are computed in terms of lower, medium and highest value expected to account for the uncertainty on the implementation of the target sets in practice. Consequentially, also the net benefit is estimated for three scenarios, as:

- low (low benefits-high costs),
- medium (medium benefits-medium costs) and
- high (high benefits-low costs)

Out of all three scenarios the TS_M3 is the one that provides the highest net benefit and is therefore selected as target set.

Table 37. Service and resilience targets with cost-benefit analysis following cyberattack

Impact level 1	**Estimate**	**Costs and benefits of the target sets [10^3€]**		
		Target set TS_M1	**Target set TS_M2**	**Target set TS_M3**

		"No changes in service"	"Legal minimum"	"Restoration budget"
Costs of achievement of target set	Low	286.682	0	720
	Medium	318.536	0	800
	High	350.390	0	880
Benefit in terms of reduction in restoration intervention costs	Low	2.385	0	716
	Medium	2.511	0	753
	High	2.637	0	791
Benefit in terms of reduction in travel time	Low	2.748	0	550
	Medium	3.233	0	647
	High	3.718	0	744
Benefit in terms of reduction in safety	Low	240.000	0	124.000
	Medium	300.000	0	155.000
	High	360.000	0	186.000
Benefit in terms of reduction in socio-economic activities	Low	900	0	270
	Medium	1.000	0	300
	High	1.100	0	330
Total benefit	Low	246.034	0	125.535
	Medium	306.744	0	156.700
	High	367.455	0	187.865
Net benefit	**Low**	-104.356	0	124.655
	Medium	-11.792	0	155.900
	High	80.772	0	187.145

1.5.4 Resilience indicator targets with cost-benefit analysis

In this section, the resilience indicator targets are set, taking into consideration the requirements defined in the previous two tasks, and based on the assumption that the net-benefit, i.e. the benefits – the costs should be maximised.

1.5.5 Resilience indicator targets with cost-benefit analysis for cyberattack event

Resilience indicator targets for cyberattack event are set with cost benefit analysis based on an incremental benefit/cost ratio calculation, i.e. investigating the benefit/cost ratio of increasing the indicator target by one level. According to the guideline given in the deliverable D1.2, Table 38-Table 40 are to be read as follows: the indicator M.1.1.1 "Age / Age of replacement of the warning system", for example, that has an impact on all four services, can correspond to 4 possible values. When this indicator is on the worst possible value (i.e. 0) the impact on all services is displayed in the line named "max" (e.g. for Safety € 150.000.000). These values correspond to the maximum loss in service per indicator, that can be estimated both with equal or differentiated weights, as from the deliverable D1.1. The cost for moving this indicator from value 0 to 1 is estimated being € 50.000.000, while the total benefit is estimated being € 51.124.000. The benefit/ cost (B/C) ratio of moving that value from 0 to 1 is then 0.49. Being the B/C ration higher than 1, value 1 is considered to be more beneficial than 0. This process is repeated for the following values as long as the B/C ratio is higher than 1, i.e. until the net benefit keeps increasing. Since the B/C ratio of moving the indicator value from 0 to 1 is 0.49, i.e. the cost are higher than the benefits, and there are no requirements related to this indicator, the target value is automatically set to 0.

Table 38. Resilience indicator targets for cyberattack event with cost-benefit analysis (1/3)

ID	Possible values	Costs [103]	Target	Max/ actual	Int.	Travel time	Safety	Socio-econ.	Total	B/C	Net benefit
M.1.1.1			0	Max	1.256	1.617	150.000	500	153.372		
	0	0		0			0	0	0	0,00	-
	1	105118		1	419	539	50.000	167	51.124	0,49	- 53.994

	2	210235		2	419	539	50.000	167	51.124	0,24	-213.105
	3	318536,375		3	419	539	50.000	167	51.124	0,16	-480.517
M.1.1.2			0	Max	1.256	1.617	150.000	500	153.372		
	0	0		0	0	0	0	0	0	0,00	-
	1	478		1	419	539	50.000	167	51.124	106,95	50.646
	2	956		2	419	539	50.000	167	51.124	53,48	100.814
	3	1447,648		3	419	539	50.000	167	51.124	35,32	150.491
M.1.1.3			5	Max	1.256	1.617	150.000	500	153.372		
	0	0		0	0	0	0	0	0	0,00	-
	1	0		1	251	323	30.000	100	30.674	Not Applicable	30.674
	2	0		2	251	323	30.000	100	30.674	Not Applicable	61.349
	3	0		3	251	323	30.000	100	30.674	Not Applicable	92.023
	4	0		4	251	323	30.000	100	30.674	Not Applicable	122.698
	5	1		5	251	323	30.000	100	30.674	30674,44	153.371
M.1.1.4			5	Max	1.256	1.617	150.000	500	153.372		
	0	0		0	0	0	0	0	0	0,00	-
	1	0		1	251	323	30.000	100	30.674	Not Applicable	30.674
	2	0		2	251	323	30.000	100	30.674	Not Applicable	61.349
	3	0		3	251	323	30.000	100	30.674	Not Applicable	92.023
	4	0		4	251	323	30.000	100	30.674	Not Applicable	122.698
	5	1		5	251	323	30.000	100	30.674	30674,44	153.371
M.1.1.5			3	Max	753	970	90.000	300	92.023		
	0	0		0	0	0	0	0	0	0,00	-
	1	83,16		1	251	323	30.000	100	30.674	368,86	30.591
	2	166,32		2	251	323	30.000	100	30.674	184,43	61.099
	3	252		3	251	323	30.000	100	30.674	121,72	91.522
M.1.1.6			3	Max	753	970	90.000	300	92.023		
	0	0		0	0	0	0	0	0	0,00	-
	1	19		1	251	323	30.000	100	30.674	1614,44	30.655
	2	37,125		2	251	323	30.000	100	30.674	826,25	61.293
	3	56,25		3	251	323	30.000	100	30.674	545,32	91.911

Table 39. Resilience indicator targets for cyberattack event with cost-benefit analysis (2/3)

ID	Possible values	Costs x 10e3	Target	Max/ actual	Int.	Travel time	Safety	Socio-econ.	Total	B/C	Net benefit
M.1.2.1			2	Max	2.009	2.587	240.000	800	245.395		

	0	0		0		0		0	0	0,00	-
	1	3		1	1.004	1.293	120.000	400	122.698	40899,25	122.695
	2	6		2	1.004	1.293	120.000	400	122.698	20449,62	245.386
M.1.2.2			1	Max	2.009	2.587	240.000	800	245.395		
	0	0		0		0		0	0	0,00	-
	1	1447,648		1	2.009	2.587	240.000	800	245.395	169,51	243.948
M.1.2.3			1	Max	2.009		240.000	800	242.809		
	0	0		0		0		0	0	0,00	-
	1	800		1	2.009		240.000	800	242.809	303,51	242.009
M.1.2.4			1	Max	2.009	2.587	240.000	800	245.395		
	0	0		0		0		0	0	0,00	974.161
	1	300		1	2.009	2.587	240.000	800	245.395	817,98	1.219.257
M.1.2.5			1	Max	2.009	2.587	240.000	800	245.395		
	0	0		0		0		0	0	0,00	977.895
	1	1		1	2.009		240.000	800	242.809	242808,83	1.220.703
M.1.3.1			1	Max	2.009	2.587	240.000	800	245.395		
	0	0		0	0	0	0	0	0	0,00	-
	1	15		1	2.009	2.587	240.000	800	245.395	16359,70	245.380
M.1.3.2			3	Max	2.009	2.587	240.000	800	245.395		
	0	0		0	0	0	0	0	0	0,00	-
	1	90		1	2.009	2.587	240.000	800	245.395	2726,62	245.305
M.2.1.1			3	Max	2.009	2	0		2.011		
	0	0		0	0				0	0,00	-
	1	2		1	670	1	0		670	335,14	668
	2	2,2		2	670	1	0		670	304,67	1.336
	3	8		3	670	1	0		670	83,78	1.999
M.2.1.2			3	Max	402	517	48.000	160	49.079		
	0	0		0	0				0	0,00	-
	1	0,99		1	134	172	16.000	53	16.360	16524,95	16.359
	2	1,98		2	134	172	16.000	53	16.360	8262,47	32.716
	3	3		3	134	172	16.000	53	16.360	5453,23	49.073
M.2.1.3			3	Max	1.632	2.102	195.000	650	199.384		
	0	0		0	0	0	0	0	0	0,00	-
	1	19		1	544	701	65.000	217	66.461	3497,96	66.442
	2	37,125		2	544	701	65.000	217	66.461	1790,20	132.866

	3	56,25		3	544	701	65.000	217	66.461	1181,53	199.271
M.2.1.4			3	Max	452	582	54.000	180	55.214		
	0	0		0	0				0	0,00	-
	1	0,99		1	151	194	18.000	60	18.405	18590,57	18.404
	2	1,98		2	151				151	76,09	18.552
	3	3		3	151	194	18.000	60	18.405	6134,89	36.954
M.2.1.5			2	Max	1.758	2.263	210.000	700	214.721		
	0	0		0	0	0	0	0	0	0,00	-
	1	400		1	879	1.132	105.000	350	107.361	268,40	106.961
	2	800		2	879	1.132	105.000	350	107.361	134,20	213.521
M.2.1.6			2	Max	1.632	2.102	195.000	650	199.384		
	0	0		0	0	0	0	0	0	0,00	-
	1	133		1	816	1.051	97.500	325	99.692	749,56	99.559
	2	140		2	816	1.051	97.500	325	99.692	712,09	199.111
M.3.1.1			2	Max	1.984	2.554	237.000	790	242.328		
	0	0		0	0	0	0	0	0	0,00	-
	1	1700		1	992	1.277	118.500	395	121.164	71,27	119.464
	2	3400		2	992	1.277	118.500	395	121.164	35,64	237.228
M.3.1.2			2	Max	2.285	2.942	273.000	910	279.137		
	0	0		0	0	0	0	0	0	0,00	-
	1	10148		1	1.143	1.471	136.500	455	139.569	13,75	129.421
	2	20296		2	1.143	1.471	136.500	455	139.569	6,88	248.693
M.3.1.3			2	Max	2.285	2.942	273.000	910	279.137		
	0	0		0	0	0	0	0	0	0,00	-
	1	126		1	1.143	1.471	136.500	455	139.569	1107,69	139.443
	2	252		2	1.143	1.471	136.500	455	139.569	553,84	278.759
M.3.2.1			2	Max	2.134	2.748	255.000	850	260.733		
	0	0		0		0		0	0	0,00	-
	1	15		1	1.067	1.374	127.500	425	130.366	8691,09	130.351
	2	30		2	1.067	1.374	127.500	425	130.366	4345,55	260.688
M.3.2.2			3	Max	2.134	2.748	255.000	850	260.733		
	0	0		0		0		0	0	0,00	-
	1	100		1	534	687	63.750	213	65.183	651,83	65.083
	2	200		2	534	687	63.750	213	65.183	325,92	130.066
	3	300		3	534	687	63.750	213	65.183	217,28	194.950

	4	400		4	534	687	63.750	213	65.183	162,96	259.733

Table 40. Resilience indicator targets for cyberattack event with cost-benefit analysis (3/3)

ID	Possible values	Costs	Target	Max/ actual	Int.	Travel time	Safety	Socio-econ.	Total	B/C	Net benefit
M.3.2.3			2	Max	1.733	2.231	207.000	690	211.654		
	0	0		0		0	0	0	0	0,00	-
	1	15		1	866	1.116	103.500	345	105.827	7055	105812
	2	30		2	866	1.116	103.500	345	105.827	3527	211609
M.3.2.4			3	Max	301	388		120	809		
	0	0		0	0	0		0	0	0,00	-
	1	0		1	100	129		40	270	Not Applicable	270
	2	0		2	100	129		40	270	Not Applicable	540
	3	1		3	100	129		40	270	269,77	808
M.3.2.5			2	Max	301	388		120	809		
	0	0		0	0	0		0	0	0,00	-
	1	0		1	100	129		40	270	Not Applicable	270
	2	0		2	100	129		40	270	Not Applicable	540
	3	1		3	100	129		40	270	269,77	808
M.3.2.6			1	Max	301	388		120	809		
	0	0		0	0	0		0	0	0,00	-
	1	0		1	100	129		40	270	Not Applicable	270
	2	0		2	100	129		40	270	Not Applicable	540
	3	1		3	100	129		40	270	269,77	808

1.6 DISCUSSION AND CONCLUSION

In the case study application, it is shown how the targets on service and resilience can be set for the M-30 ring road in Madrid. This is done both directly and for the resilience indicators, and both with and without cost benefit analysis, on the basis of the measure of resilience for the road estimated in the appendix 1 of the deliverable D1.1.

The targets obtained for the transportation system are influenced by the requirements (legal and stakeholders requirements) set in task 2 and 3, and are to be read differently depending how are set:

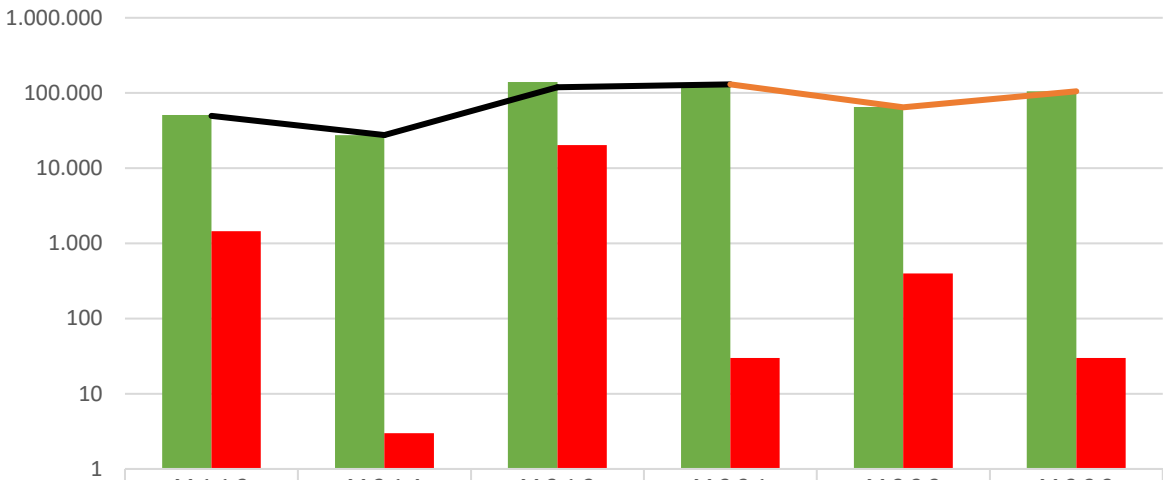
- **When service and resilience targets are set without cost benefit analysis**, experts and stakeholders consider that it is acceptable that the restoration intervention costs are lower than 70% of maximum estimated following a cyberattack event. The acceptable reduction with reference to travel time service is set to 80% of the maximum for the hazard, while for the three specific level 2 impacts of the service safety (i.e. property damage, injuries and fatalities) the acceptability is set on 40%, 50% and 60%. The acceptable reduction with reference to

socio economical activities service is set to 70% of the maximum. These values are an expression of the stakeholders' opinion and of the requirements set in task 2 and 3.

- **When resilience indicators targets are set without cost benefit analysis**, experts and stakeholders have fixed the level of acceptability, in terms of minimum value to be guaranteed for each selected indicator. The indicators for which targets have not been set are indicators that have been considered out of the control of the infrastructure manager (e.g. hazard zone). These values are an expression of the stakeholders' opinion and of the requirements set in task 2 and 3.
- **When service and resilience targets are set with cost benefit analysis**, the target set TS_E1 (no change in service) has resulted being the best solution with reference to cyberattack event. This implies that when the infrastructure managers agree on the input used, this target set provides the highest net benefit.
- **When resilience indicators targets are set with cost benefit analysis**, the target value for each indicator has been estimated directly from the cost benefit analysis. This implies that when the infrastructure managers agree on the input used, the targets set for each indicator provide the highest net benefit.

Table 41. Net benefit of the Indicators

ID	Indicator	Total costs	Total benefit	Net benefit
M.1.1.2	Age / Age of replacement of safe shut down system	1.448	51.124	49.676
M.2.1.4	Duration of past down time due to hazards	3	27.607	27.604
M.3.1.2	The presence of a maintenance strategy	20.296	139.569	119.273
M.3.2.1	The presence of an emergency plan	30	130.366	130.336
M.3.2.2	Practice of the emergency plan	400	65.183	64.783
M.3.2.3	Review/update of the emergency plan	30	105.827	105.797



	M.1.1.2	M.2.1.4	M.3.1.2	M.3.2.1	M.3.2.2	M.3.2.3
Total benefit	51.124	27.607	139.569	130.366	65.183	105.827
Total costs	1.448	3	20.296	30	400	30
Net Benefit	49.676	27.604	119.273	130.336	64.783	105.797

Figure 52. Net benefits of the Indicators

[1] Along to definition of Operation & Maintenance Plan D7.2
[2] RAMSSHEEP analysis: "A tool for risk-driven maintenance. Applied for primary flood defence systems in the Netherlands"
[3] Berkeley, Alfred R., and Mike Wallace. "A framework for Establishing Critical Infrastructure Resilience Goals.", 2010.