SARIL

Sustainability And Resilience for Infrastructure and Logistics networks

D2.1 Survey of methodologies for resilience management

Deliverable Number	D 2.1
Author(s)	Maria Pina Limongelli, Georgios Karagiannakis, Pablo Jose Vallhonrat Blanco, Raquel Ortega Hita, Gonzalo Durán Piñeiro, Jakub Kempski, Marta Waldmann
Due/delivered Date	30-10-24
Reviewed by	Lillian Hansen, Dang Ndoc Son, Ana Maia, Benjamin Lickert
Dissemination Level	PUB
Version of template	1.1

Start Date Project: 2023-06-01 Duration: 36months Project ID: 101103978

This project has received funding from the Horizon Europe program of the European Union under grant agreement ID 101103978.

Document contributors

NO.	Name	Organisation	Role (content contributor, reviewer, other)
1	Georgios Karagiannakis	Polimi	Content contributor
2	Maria Pina Limongelli	Polimi	Content contributor
3	Pablo Jose Vallhonrat Blanco	CEMOSA	Content contributor
4	Raquel Ortega Hita	CEMOSA	Content contributor
5	Gonzalo Durán Piñeiro	UVigo	Content contributor
6	Jakub Kempski	L-PIT	Content contributor
7	Marta Waldmann	L-PIT	Content contributor
8	Lillian Hansen	SIN	Reviewer
9	Dang Ndoc Son	UMinho	Reviewer
10	Ana Maia	Rangel	Security officer
11	Benjamin Lickert	Fraunhofer	Quality officer

Document revisions

Revision	Date	Comment	Author
01	20/07/2024	Draft version 1	Georgios Karagiannakis, Maria Pina Limongelli, Palbo Pablo Jose Vallhonrat Blanco, Raquel Ortega Hita, Gonzalo Durán Piñeiro, Jakub Kempski, Marta Waldmann
02	09/09/2024	Draft version 2	Georgios Karagiannakis, Maria Pina Limongelli, Palbo Pablo Jose Vallhonrat Blanco, Raquel Ortega Hita, Gonzalo Durán Piñeiro, Jakub Kempski, Marta Waldmann
03	27/09/2024	Draft version 3	Georgios Karagiannakis, Maria Pina Limongelli, Palbo Pablo Jose Vallhonrat Blanco, Raquel Ortega Hita, Gonzalo Durán Piñeiro, Jakub Kempski, Marta Waldmann
04	11/10/2024	Draft for internal revision	Lillian Hansen, Dang Ngoc Son
05	23/10/2024	Security control	Ana Maia
06	30/10/2024	Quality control	Benjamin Lickert

Executive summary

This Deliverable (D2.1) of the SARIL project provides a comprehensive review of resilience models, and of resilience management strategies for transport and logistics networks. It focuses on three key stakeholder groups: (R1-A) public authorities and operators who are responsible for the construction and maintenance of transport infrastructure; (R1-B) Entities responsible for the management of traffic; (R2) logistics companies who configure at long term the transport and logistic network using the infrastructure provided by R1; and (R3) stakeholders managing and executing short term logistic operations, using the network established by role R2.

In particular, current resilience management strategies implemented by end-users to deal with disruptions and the challenges they face are reviewed based on the interviews and surveys carried out in WP1 and presented in Deliverables D1.2 and D1.3 considering the scenario definitions documented in D1.1. A poll is carried out in this deliverable, which builds upon the previous surveys for identifying gaps or strategies not currently addressed by the tools of the end-users of SARIL project. Commercial tools are also proposed to fill these gaps. The poll of the current strategies highlighted several gaps consisting mainly of the planning and execution of pre-emptive actions to increase preparedness, the use of information as decision support tools, the consideration of an all-inclusive global resilience indicator, as well as the integration of green aspects in resilience management. To tackle these gaps and have a clear picture of the research efforts on resilience management, a literature review was carried out on system resilience modelling and management.

The outcomes of the literature review are presented in terms of the resilience components defined in D1.2: preparedness, robustness, recovery capacity, and adaptive capacity of the system. Herein, the systems are those managed by Roles 1 to 3. The objective is to facilitate the identification of common key performance indicators for different domains (infrastructure and logistics) that can be used as a base for the development of a resilience assessment framework consistent across different domains and scales. Consistently with the findings of the poll, a global resilience indicator is missing from the literature, especially to account for the components of preparedness and adaptive capacity. The same applies to indicators that assess the impact of information on system management.

The performance of any system, such as a transport infrastructure or a logistic network, is affected by uncertainty. The availability of information—such as that provided by monitoring systems for a physical infrastructure, or by traffic information for a logistic network—can mitigate this uncertainty, enhancing resilience management of the transportation or the logistic network, through a better knowledge of the system state. However, an effective use of information as decision support tools calls for the resilience of the information system prone to disruptions due, for example, to cyber-attacks. A further topic addressed in the deliverable is that the resilience of the information system supports decisions of the three Roles.

D2.1 is associated with WP 1 and linked to Task 2.1. It serves as a foundation for the development of an integrated green resilience assessment framework, which will be detailed in future SARIL project deliverables of WP2 and 3, and it supports the workshops of Task 1.4.

List of Contents

List of Figures

List of Tables

List of Acronyms

Acronym	Definition
ALE	Annual Loss Expectancy
ARO	Annual Rate of Occurrence
BCR	Benefit Cost Ratio
CER	Critical Entities Resilience
EFFIS	European Forest Fire Information System
FC	Fragility Curve
KPI	Key Performance Indicator
MITRE ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
NPV	Net Present Value
RF	Resilience Factor
ROSI	Return on Security Investment
SHM	Structural Health Monitoring
SIEM	Security Information and Event Management
SIRP	Security Incident Response Platform
SOAR	Security Orchestration, Automation, and Response

Glossary

Term	Definition
Adaptation	A strategy undertaken to adjust a system to a changing ecosystem (e.g., due to climate change) in view of reducing the consequences of disruptions.
Adaptive capacity	The ability of a system or operation to learn from previous disruptions. A system with adaptive capacity experiences fewer losses when a disruption with the same characteristics occurs.
Disruptive event	An incident, whether natural (e.g., floods or windstorms) or human-made (e.g., cyberattacks), that disrupts normal operations of a system or network.
Handling strategy	An action, measure or protocol taken to enhance specific resilience components (e.g., *Preparedness*, *Robustness*, *Recovery capacity*, and *Adaptive capacity*) of a system or network. A handling strategy can be either mitigation or adaptation
Important strategy	An approach or measure identified by stakeholders as critical for maintaining or enhancing system resilience. These strategies typically focus on operational priorities such as resource optimisation, rapid response during disruptions, and maintaining service levels.
Mitigation	A strategy taken to reduce the causes or minimise the impacts of an event.
Recovery capacity	The ability of a system or operations to regain their performance after disruptions. This ability is commonly measured with the recovery time.
Resilience component	A feature that contributes to the resilience of a system. These comprise *Preparedness*, *Robustness*, *Recovery capacity*, and *Adaptive capacity*.
Resilience factor or attribute	A factor defined in D1.2 (such as redundancy, visibility, or flexibility) that enhances a system's resilience against disruptive events.
Resilience index	A quantitative metric that accounts for all the components of resilience and is estimated based on the area below or above the resilience curve
Resilience phase	A phase in the process of resilience to disruptions. These comprise *Before*, *During*, *After* and *Beyond*.
Roles or end-users	Entities, companies or authorities responsible for: the development and maintenance of transport infrastructure (Role 1-A); the management of traffic (Role 1-B); configuration of transport and logistics networks (Role 2); management of logistics operations
Scenario	This refers to a specific geographical scale scenario within the SARIL project (e.g., *Regional*, *National*, or *European*) and its hazards (e.g., flood, cyber, wildfire, and global disruptions such as war/pandemics).
Sustainability factor	An attribute of sustainability (e.g., green practices, lean management) that describes the capability of a system to maintain its operations and services over time without depleting resources, harming ecosystems, or compromising the ability of future generations to meet their needs.

1. Introduction

The construction and maintenance of transport infrastructure, as well as the configuration and management of logistic networks and operations, are essential for ensuring the transportation of goods and services while contributing to the safety and socio-economic growth of communities. However, the resilience of these networks is threatened by natural (e.g., floods, windstorms, and wildfires) and human-induced hazards (e.g. war, accidents, and pandemics), such as the Covid-19 pandemic (Guan et al., 2020; Singh et al., 2021), the 2021 blockage of the Suez Canal (Topham, 2021), the catastrophic 2023 floods in Thessaly, Greece (Garini & Gazetas, 2023), the 2024 collapse of a bridge in Baltimore (BBC, 2024), and the ongoing war in Ukraine (Ben Hassen & El Bilali, 2022). The 2019 report of DHL ranked material shortages, which can be associated with pandemic or war, and climate change in the top four supply chain risks to watch. These threats have caused unprecedented long-term disruptions to international supply chains and have resulted in physical damage to critical transport infrastructure, leading to billions of euros for repairs and liability.

Regarding natural hazards, the sixth report of the *Intergovernmental Panel on Climate Change* (IPCC) expects an increase in the intensity and frequency of climate extremes. These are contingent upon the type of climatic hazards and geographic regions, e.g., inland flooding and windstorms are expected to amplify across the EU, while Southern Europe is likely to experience a rise in heat waves. Ageing infrastructure, growing energy demand, and population growth further escalate vulnerability and financial losses (OECD, 2018; WEF, 2023). Between 2010 and 2020, Eurostat estimated €14.5bn annual losses in the EU physical infrastructure due to climate hazards (Eurostat, 2022). According to Forzieri et al. (2018), it is predicted that the current €0.8 billion annual total (direct and indirect) losses to the transport sector due to natural hazards in the EU could reach €11.9 billion per year by 2100. These new demands underscore the urgency of bolstering the resilience and sustainability management of infrastructural assets and logistics operations. This urgency is reflected in the new EU directive on the resilience of critical entities (CER Directive, 2022), which stipulates that national authorities should identify critical entities, carry out resilience assessments, and embrace strategies that enhance resilience and climate adaptation.

Based on the preceding statements, the present deliverable reviews current resilience assessment models and disruption management strategies used in transport and logistics networks when exposed to natural and human-induced hazards.

The objectives of this deliverable, considering the roles defined in D1.2 (SARIL, 2024a), i.e., public authorities and operators involved in the development and maintenance of transport infrastructure, as well as management of traffic, ii) logistic companies involved in the long-term configuration of transport and logistics networks, and iii) stakeholders involved in the short-term management of transport and logistic operations, are summarised as follows:

1. **Obj.1**: A review of **current strategies and tools** employed by SARIL end-users to manage disruptions. This objective is grounded on the outcomes of a poll, wherein end-users were asked to indicate which strategies are critical for managing disruptions but are not addressed yet, and the findings on deliverables D1.3 (SARIL, 2024b).
2. **Obj.2**: A literature review of **current resilience assessment models** used for managing systems (e.g. infrastructure, traffic, transport, and logistic networks) based on the outcomes of a poll, wherein end-users indicated which tools are used to assess resilience components, i.e., preparedness, robustness, recovery and adaptative capacity.

3. **Obj.3**: A review of **resilience management strategies** adopted to enhance the resilience of logistics networks categorised by resilience component and the roles defined in the SARIL project.

The flow diagram of Figure 1 illustrates the structure and main objectives of D2.1. Section 2 addresses the Obj.1 by analysing key information from the previous deliverables (D1.1-D1.3) as well as the poll results. The results are analysed through the lens of each Role in order to identify gaps in the current strategies. Section 3 comprises the review of resilience modelling methods (Obj. 2) and management strategies (Obj. 3) proposed in literature and adopted by the Roles defined in the SARIL project. This section also includes the resilience modelling and management of the information system. Resilience modelling methods are reviewed for each component of resilience (preparedness, robustness, recovery capacity and adaptive capacity), and management strategies are proposed that can feed the identified gaps in the previous sections. Although the modelling methods are hazard-independent, references to specific hazards, such as flood, wildfire or pandemic, which are considered in each of the three scenarios of the SARIL project, are made. Information is handled by all Roles as a support tool, and therefore the information system is addressed separately. Finally, Section 4 summarizes the key findings and aligns the present deliverable with the deliverable D2.2, which presents the development of the SARIL integrated green resilience assessment framework, consistent across scales in terms of modelling, simulating, and evaluating impacts induced by disruptions.

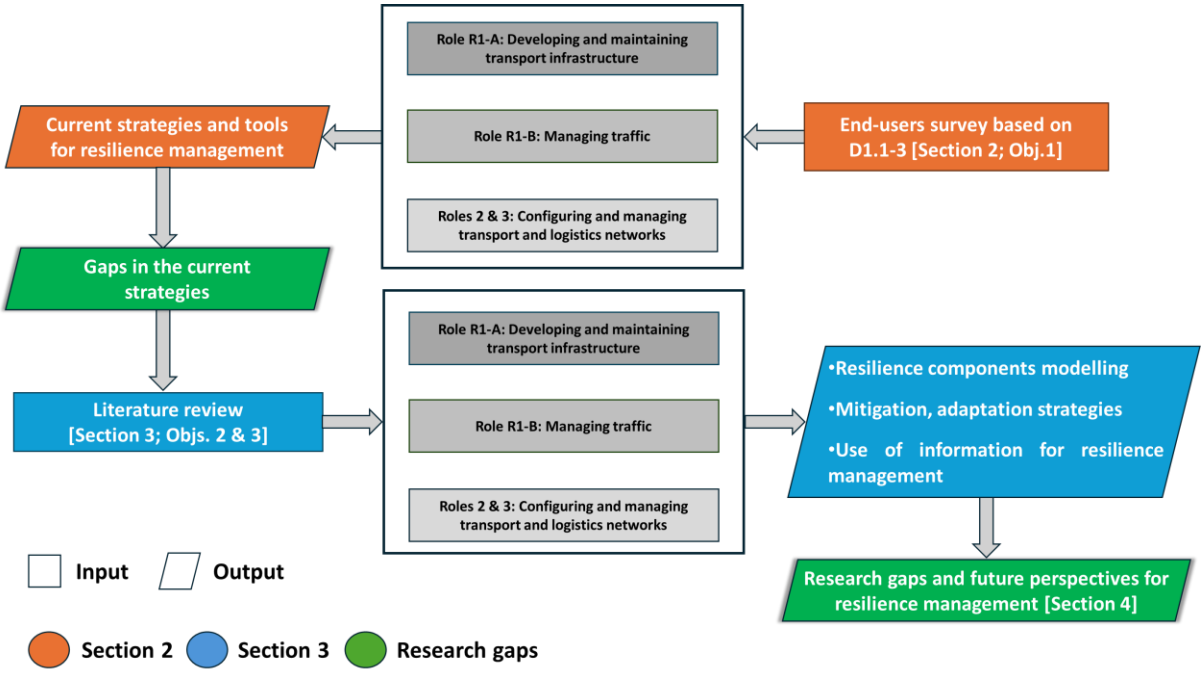

Figure 1: The flow diagram with the structure and main objectives of D2.1.

2. Current Strategies for Resilience Management

2.1 Summary of the End-User Poll

This section introduces the current resilience management strategies based on the outcomes reported in Deliverables D1.1 to D1.3 and on a poll carried out among the end-users of the SARIL project. This poll builds upon the survey of end-users carried out in D1.3 (SARIL, 2024b). In particular, in D1.1 (SARIL, 2023), three scenario cases (Regional, National, and European) were defined to represent disruptions at different geographical scales. D1.2 (SARIL, 2024a) established several logistic network roles to facilitate the development of a holistic resilience framework, identified the most relevant resilience and sustainability factors and proposed several KPIs to describe them. D1.3 (SARIL, 2024b) described the results of two types of stakeholders engagements; the first was interviews which identified the strategies end-users currently adopt to manage and mitigate disruptions affecting infrastructure and transport networks. In more details, end-users include:

- Public authorities and operators who are responsible for the construction and maintenance of transport infrastructure (Role 1-A).
- Entities responsible for the management of traffic (Role 1-B).
- Logistics companies who configure at long term the transport and logistic network (Role 2).
- Stakeholders managing and executing short term logistic operations (Role 3).

The second type of stakeholder engagement, online surveys, targeted a more comprehensive group by disseminating the questionnaire through direct email and social media platforms such as LinkedIn. It should be emphasised that the following sub-sections focus primarily on the strategies used by stakeholders to deal with disruptions and the challenges they face. The interested reader can find more information in the interviews and the surveys in Deliverable D1.3 (SARIL, 2024b).

The outcomes of the online surveys are summarised in Table 1 together with their description. The most influential disruption to responders' daily work relates to health emergencies, such as the COVID-19 pandemic which causes quarantines, closure of borders, and reduction of labour force to avoid personal contact. It is followed by regulatory changes related to pandemic or war, which can lead to trade restriction or embargos with prohibited goods lists or rerouting requirements to avoid conflict zones.

Further disruptions include extreme weather (or precipitation) ranked fourth, followed by disruptions due to a lack of workforce and strikes, cyberattacks, flooding, wildfires, and other natural disasters, which are expected to increase in some regions in the future due to climate change. Although heavy rainfall is closely linked with flooding events, the former is more frequent and less localized. For this reason, heavy rainfall was expected to affect the everyday life of respondents. However, flooding can be more damaging with respect to precipitation because of long-term recovery and damage to physical infrastructure, e.g. bridges. Therefore, the overall losses that heavy rainfalls cause can be lower in comparison to flooding. These events, which are commonly called high impact low probability events, are also related to global disruptions of supply chain, such as the Suez Canal blockage or Baltimore bridge collapse, which resulted in severe repercussions in the global supply chain (BBC, 2024). Other natural hazards, such as landslides, earthquakes, and tsunamis, appear less impactful. However, bias in the sample cannot be avoided given that natural hazards such as earthquake or tsunami are region-specific.

Disruption type	Description
Health Emergencies or pandemic	The COVID-19 pandemic caused significant impact, leading to increase/decrease of transport rates, driver shortage, oversupply issues in cargo terminals, fluctuations in cargo volumes and increase of energy costs.
Regulatory Changes	Often triggered by major disruptions like war and pandemics. Especially, war can lead to trade restrictions with prohibited goods lists or rerouting requirements to avoid conflict zones. Also, pandemics can cause quarantines, closure of borders and reduction of labour force to avoid personal contact.
War	War can result in congestion in ports, increase of transport rates and rise in energy costs.
Extreme Weather	Heavy rainfall and windstorms are expected to increase in some regions due to climate change.
Lack of workforce and strikes	Disruptions in the labour market leading to operational inefficiencies.
Cyberattack, flooding and wildfires	Flooding, wildfires or ice roads are expected to increase in some regions due to climate change.
Other natural disasters	Events like earthquakes, landslides, and sea storms.

Table 1: Main disruptions identified from the survey conducted in D1.3 (ranked from most to least impactful).

Additionally, D1.3 identified the following primary resilience factors of each Role:

- **Role 1-A** prioritises redundancy, which is closely followed by reliability, recovery, and learning. Visibility, collaboration, flexibility, and security hold moderate importance.
- **Role 1-B** values collaboration and learning the most, followed by visibility and flexibility. Redundancy is deemed the least important.
- **Role 2 and 3** prioritize reliability, flexibility, learning, collaboration, and recovery, with less emphasis on redundancy.

Table 2 collects the strategies that the different Roles adopt for dealing with disruptions and the resilience factors associated with these strategies. The most frequently adopted strategies comprise internal dialogue, adaptive strategies “as we go,” alternative transportation routes, and changes in internal processes. It is noteworthy that building collaboration by engaging new partners, and increasing redundancy by considering new business models, are among the least adopted strategies. Other uncommon practices involve using digital systems and tools to shut down processes, provide early warnings, and guide the prioritization of recovery actions during and after disruptions.

Several gaps in the management of the information system have been identified in the stakeholder online surveys and concern real-time data collection and communication tools used to manage disruptions.

- Outdated methods for information flow. Many stakeholders still rely on outdated systems, such as visual inspections for infrastructure managers (R-1A and B) or emails for logistic managers (R2 and R3), limiting their ability to respond efficiently during crises. There is a growing need for advanced digital tools that enable automated early warnings and real-time decision support. The surveys reported in D1.3 among end-users showed that, while some strategies —such as monitoring traffic demand and ensuring transparency in transport schedules— are widely addressed, real-time communication and collaborative decision-

making during disruptions should be enhanced. End-users recommended improving digital systems for early warnings and suggested the implementation of advanced analytics and monitoring tools.

- Cross-sector collaboration is needed to enhance coordination by Roles 2 and 3 – e.g. exchange of information - between public authorities, logistics companies, and infrastructure operators during crises.
- Measures to manage cyber-threats and climate change by all Roles, and especially Role 1. The evolving threats from climate change and cyber-attacks require resilience frameworks that are adaptable to emerging risks. Transmission of information is prone to cyberattacks, which thereby constitutes a further possible disruption for the system. Future research should prioritize developing flexible models that can evolve alongside new hazards, ensuring long-term resilience and sustainability.

Adopted strategy	Role(s)	Description	Associated Resilience Factor
Dialogue and information internally	R2,3	Emphasises the importance of communication within the organisation.	Collaboration
Adapting strategies “as we go”	R3	Flexibility in changing strategies based on the evolving situation	Flexibility
Changing transportation modes/routes	R2,3	Switching to alternative transportation methods or routes	Redundancy, Flexibility
Change internal processes	R2	Modifying existing procedures, e.g. standards, resources, and work practices	Flexibility, Preparedness
Continuous improvement or training measures	R2	Investing in ongoing training and improvements	Learning, Preparedness
Safety management systems and risk assessment	R1	Prioritising safety through structured systems and continuous risk assessments	Preparedness, Recovery, Reliability
Prevention protocols	R1	Implementing protocols like biomass management and action plans against specific threats such as snow	Preparedness, Reliability, Recovery

Table 2: Frequently adopted strategies by different Roles for dealing with disruptions (ranked from most to least used).

Based on the results of the surveys, and acknowledging the importance of information as a support tool, a poll on resilience modelling and management of the information system is performed and contained in this deliverable.

2.2 End-Users and Resilience Management Tools

This section builds upon the aforementioned end-users surveys by elaborating further on the resilience management strategies employed by the end-users, and associating these strategies with the four resilience components.

The poll, designed as a structured completion form for end-users, consisted of three sections. First, each end-user indicated which tools they employ for addressing disruption events and recovering the performance of their system. Subsequently, a list of handling strategies (see Annex I) was proposed for each resilience component (preparedness, robustness, recovery, and adaptive capacity). Respondents were asked to assign each tool listed in the first section to one of the handling strategies. Bearing in mind that some strategies may not have been addressed yet, end-users were asked to indicate "NA", which stands for "Not addressed", to those strategies they consider important to be addressed in the future. Handling strategies rated as "Not addressed" are discussed, building on a literature review and an analysis of whether other commercial tools account for these strategies. The poll concluded with a section dedicated to suggestions on how the project should contribute to specific handling strategies.

Based on the gaps identified in the strategies of the end-users, commercial tools are identified. For this purpose, machine learning has been trained based on the keywords and definitions of this study to identify commercial tools online.

2.2.1 Overview of the Results

End users identified 43 tools used for logistic and management purposes. These have been divided into three categories: *Website*, which refers to online resources; *Software*, which refers to computer programs; and *Documentation*, which refers to any document including guidelines and standards. 28 tools out of 43 correspond to *Webpage*, 13 to *Software*, and 2 to *Documentation*. Figure 2 illustrates the percentage distribution of the tool category reported by the end-users. Results indicate that *Website* is the leading tool category, followed by *Software* and, to a considerably lesser extent, *Documentation*.

Not all tools are used for managing disruptions. Those who have not been assigned to handle at least one strategy from the list are, within each category, shaded in Figure 2. Those consist, for example, of documents providing necessary actions in the event of an environmental emergency (e.g., oil spills), tools to manage traffic, real-time tracking tools, planning tools, and emissions calculators. Although certain tools are not used for any handling strategy (whether for mitigation or adaptation), analogous tools which provide similar data, such as real-time tracking, are used. This indicates that, when approaching a disruption event, certain tools are first sought, which may prove the efficiency and competence of one tool compared to another.

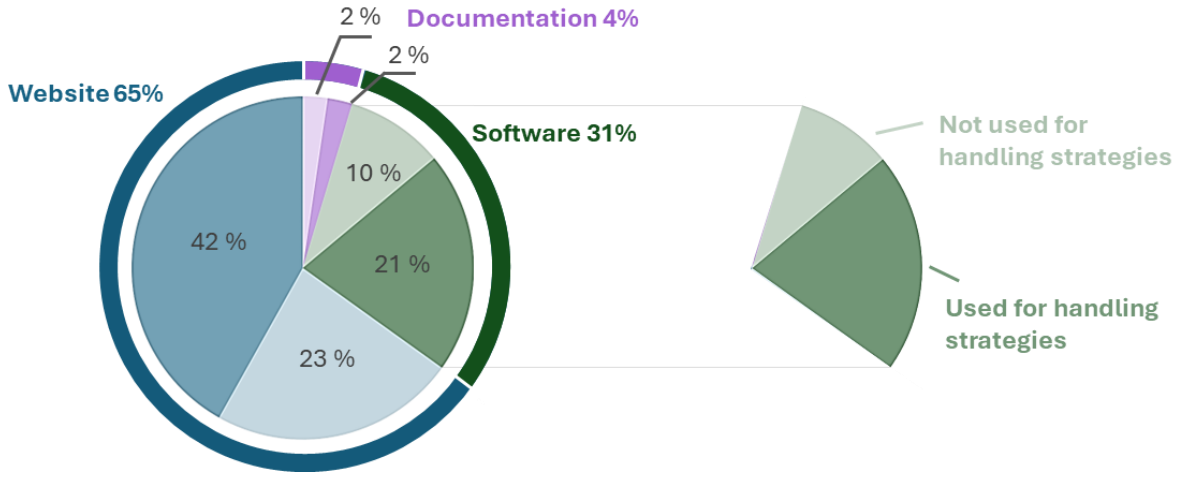

Figure 2: Percentage use of tool category (dark and light colour represent a tool used and not used for handling strategies, respectively).

Similarly, these tools have been divided into source categories (Figure 3): open source (free access), private (whenever a subscription is required), and internal (indicating that the end-user has defined its own tool). The figure also shows, as shaded, which percentage of the tools within each category has not been employed for managing disruptions. Results indicate that most tools come from private companies, i.e., a subscription is needed, followed by open source and internal.

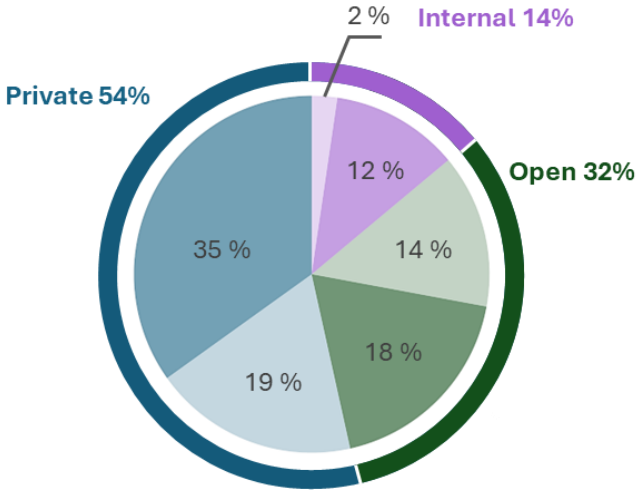

Figure 3: Percentage use of tool source category (dark and light colour represent a tool used and not used for handling strategies, respectively. See also Figure 2).

33 handling strategies were envisioned and presented to the end users (see Annex I), who had to relate which of their tools addressed which handling strategy. However, the stated tools only addressed some handling strategies.

Figure 4 illustrates the percentage of end users that have a tool to address (in green) or not yet (in red, standing for "Not addressed") each handling strategy. A handling strategy is characterised as important whether it is addressed or not addressed. If an end-user assigns a tool to a strategy, it means that it is important. Similarly, if an end-user characterises a strategy as "not addressed", it also means that the strategy is important; however, no tools are currently available for this specific strategy. Therefore, the larger the percentage, the more important the handling strategy. Each handling strategy is denoted by an ID named after the acronym of the resilience component (preparedness P,

robustness R, recovery capacity RC, adaptive capacity AC), followed by the position in the list (see Annex I).

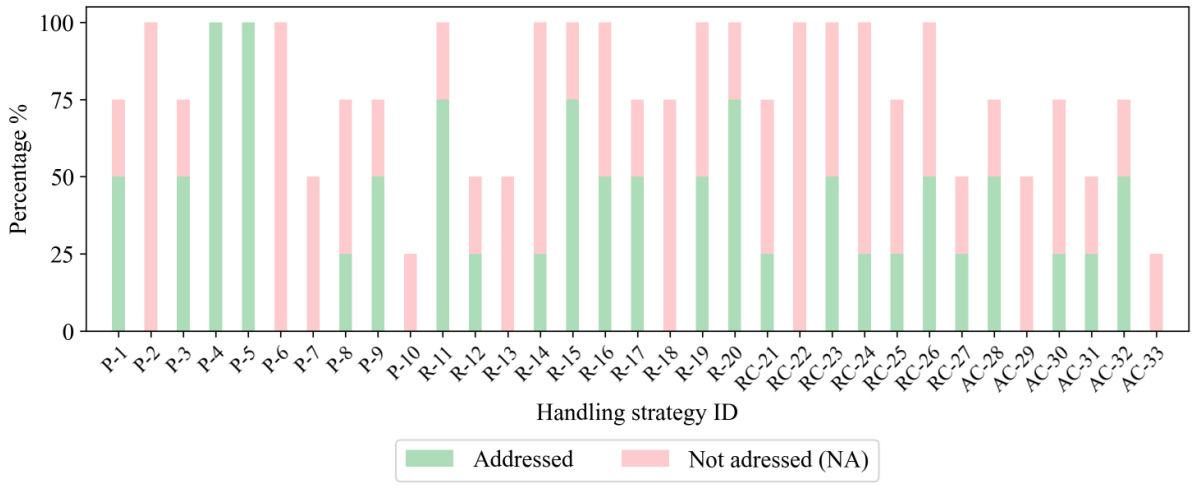

Figure 4: Results based on the SARIL project's end-users' outputs.

Figure 5 illustrates for each handling strategy how many tools fall into one of the three considered categories (*Website*, *Software*, *Document*). Results show how a unique tool category is employed for specific handling strategies (e.g., **P-1**, **P-5**, **P-9**, **R-14**, and **RC-21** are solely addressed by the tool category *Website*, **P-8**, **RC-25**, **RC-27**, and **AC-30** by *Software*, and **R-12** by *Document*).

Handling strategies **P-1**, **P-5**, **P-9**, **R-14**, and **RC-21** deal with external data such as train routes, ship schedules, weather forecasts, and partner collaboration. Given that this information is retrieved from external companies, the data is accessed through websites, and therefore, they are categorized as such. Handling strategies **P-8**, **RC-25**, **RC-27**, and **AC-30** deal with internal and private data. Therefore, in order to reduce vulnerability against cyberattacks, they are managed through internal software. Handling strategy **R-12** is a document focused on cooperation, communication, and information sharing between transport companies and authorities. Since only one end-user addresses **R-12** with the mentioned document, this handling strategy falls within the document category.

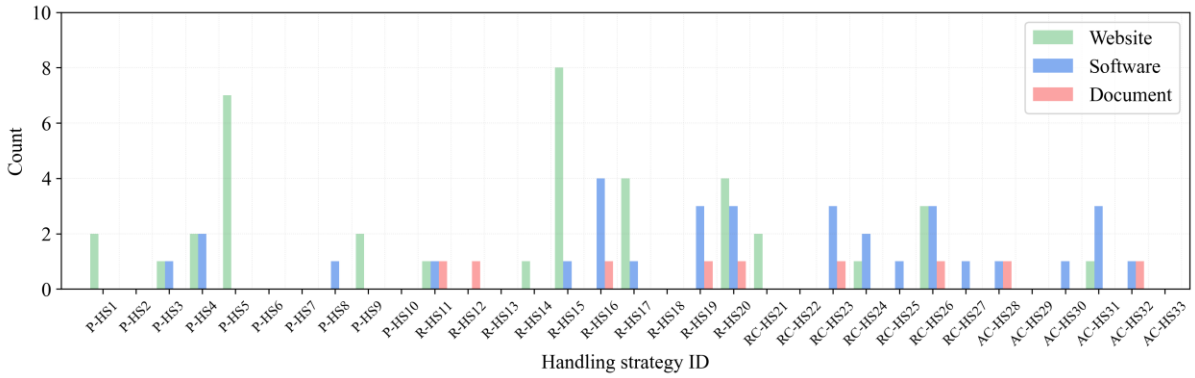

Figure 5: Tool category used for each handling strategy.

Similarly, Figure 6 illustrates for each handling strategy the number of tools that falls into one of the three source categories (*Open*, *Private*, *Internal*). Categories solely addressed by *Open* source tools encompass only **R-12**, by *Private* **P-3**, **R-14**, **RC-21**, **RC-24** and **RC-25**, and by Internal **P-8**, **RC-27**, **AC-28**, **AC-30**, and **AC-32.**

Handling strategy **R-12** falls within the first category, since the document used to address this disruption can be accessed through the end-user website. However, this document focuses on their infrastructure and might not apply to other scenarios. Handling strategies **P-3**, **R-14**, **RC-21**, **RC-24**, and **RC-25** fall within the private category, since all these strategies involve data analysis, numerical simulations, or data sharing among entities. These types of tools are generally not designed by end-users due to the increased computational and algorithmic required knowledge, which may be out of reach by end-users. Handling strategies **P-8**, **RC-27**, **AC-28**, **AC-30**, and **AC-32** fall within the internal category, since they all deal with internal processes and infrastructure management, which are explicitly designed for the end-user´s context.

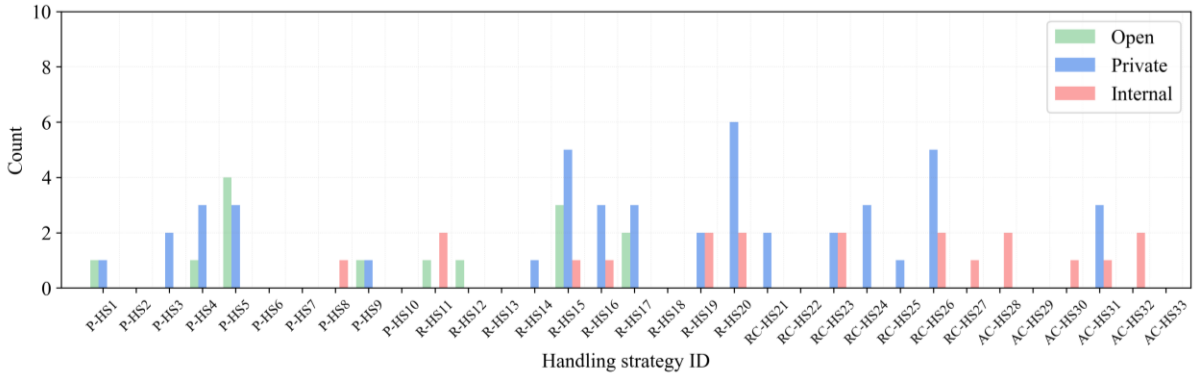

Figure 6: Tool source category used for each handling strategy.

Finally, end-users noted that during disruptions, they follow internal instructions based on management directives, though these may require further refinement. They suggested improving real-time data collection and communication among stakeholders, as current practices rely on email, even during disruptions. Additionally, they recommended implementing collective decision support strategies. No additional strategies were proposed by the end-users.

2.3 Role R1-A: Developing and Maintaining Transport Infrastructure

2.3.1 Analysis of Handling Strategies

Among all handling strategies, the following three are not covered by any tool from end-users:

- **P-2:** Continuous data collection that accounts for changes in the damage state of physical infrastructure (e.g., roads or bridges) and includes analysis to anticipate disruptions.
- **P-6:** Continuous resilience assessment and definition of critical points in a transport or logistics network due to deterioration and/or disruptive threats based on a resilience indicator.
- **RC-22:** Short- and long-term restoration plans to ensure rapid recovery.

End-users do not address handling strategies **P-2**, **P-6**, and **RC-22** due to the significant investment required in advanced technologies, data analytics, and the complexity of integrating continuous monitoring systems. Additionally, the immediate return on investment for such proactive measures is not always evident, making it challenging to prioritise them over more pressing operational concerns.

The following strategy is classified as important by all end-users; however, only one end-user currently addresses it:

- **R-14:** Digital tool giving a step-by-step plan and guidance during disruptions (e.g. alarm systems, sensors, cameras, etc.).

Strategy **R-14** is addressed by one of the end-users with the tool Avigilon. This private tool offers comprehensive security solutions integrating high-definition video surveillance, analytics, and access control systems. During disruptions, these tools enable real-time monitoring of critical infrastructure and assets, providing actionable insights and alerts to response teams. *Avigilon's* sophisticated analytics can detect anomalies and potential threats, facilitating rapid response and decision-making. *Avigilon* can serve organisations to manage disruptions, enhance situational awareness, and implement proactive measures to mitigate risks and minimise the impact on operations.

Most of the end-users have classified the following strategy as important (i.e., having a percentage of 75% in Figure 4):

- **AC-30:** Tool for updating risk, and recovery assessment methods to account for lessons learned e.g. from climate change or carbon emissions reduction.

This strategy is addressed by one end-user through internal software that manages all logistic and transport operations; however, it does not cover infrastructures.

Other strategies that **half** of the end-users have identified as important (i.e., having a percentage of 50% in Figure 4) but still need to be addressed are:

- **P-7:** Planning and executing timely interventions to prevent disruptions.
- **R-13:** Digital system automatically or manually shutting down processes to mitigate consequences.
- **AC-29:** Continuous improvement with disruption simulations and training of the population and logistical stakeholders.

These handling strategies are not yet addressed, since end-users frequently lack a preventive strategy to avoid or mitigate disruptions, yet they react once the disruption occurs. Therefore, a tool to address the handling strategy **P-7** must first simulate which disruptions can occur, and then prevention measures can be defined. Similarly, the handling strategy **R-13** relates to proactive actions, which are generally disregarded, although implementing mitigation strategies during a disruption event considerably increases the resilience of the system. Analogously, continuous improvement through simulations and training, i.e., **AC-29**, requires ongoing investment in training programs, technology updates, and stakeholder engagement, which many companies find difficult to justify without immediate and visible benefits.

Given that **none** of the end-users yet addresses strategies **P-7**, **R-13**, and **AC-29,** the three of them are addressed in the following sections.

The following strategies have been classified as the least important based on their percentage in Figure 4:

- **P-10:** Specific budget dedicated to disruptive events in contracts and projects administration and stakeholders.
- **AC-33:** Inclusion of educational subjects in young people's education to gain social resilience.

End-users may perceive strategy **P-10** as less immediately relevant, because it involves financial planning and allocation that may not directly impact their daily operations or personal experience. Also, strategy **AC-33** focuses on long-term benefits and societal changes, which might not resonate with end-users who prioritise immediate and tangible outcomes. The impact of educational changes

on social resilience is gradual and indirect, making it less compelling for those seeking quick and direct solutions to current problems.

2.3.2 Commercial Tools for Resilience Management

Strategy **P-2** of continuous data collection to monitor the state of the physical infrastructure is incorporated into various advanced tools. For example, SENSRnet provides real-time data and instant alerts for swift decision-making regarding the management of critical infrastructure. Trimble 4D Control integrates environmental and structural measurements into a single platform for comprehensive analysis and timely notifications. Also, ERDAS IMAGINE uses remote sensing to detect infrastructure damage over time with high-resolution imagery, and IBM SPSS Modeler employs machine learning to analyse SHM data, predicting failures and maintenance needs.

Furthermore, strategy **P-6** pertains to continuous resilience assessment and identification of critical points in a transport network based on a resilience indicator. Arguably, this strategy is critical to improve preparedness during the "before" phase, though very few tools are available that produce a single resilience indicator, and most of them do not account for all the components of resilience. For example, The R Score tool of Resilinc focuses on the resilience of systems by measuring their ability to withstand, absorb, and quickly recover from disruptive events. It considers various factors, including the age of infrastructure and potential threats, to define critical points in a network. By continuously assessing these elements, the tool helps in identifying vulnerabilities and making informed decisions to enhance resilience. However, a potential limitation of the tool is its limited emphasis on adaptive capacity, or the system's ability to evolve in response to long-term changes and emerging threats. A tool-kit with potential adaptation strategies, as required by legislations, could be added to cope with climate change effects.

Strategies **R-13** and **R-14** are about digital tools that enable automatic shutdown of the performance and provide guidance, e.g. closure of a bridge and information about alternative routes due to high risk induced by flooding water. The CAE tool integrates with sensors deployed across flood-prone areas in Sardinia, continuously monitoring crucial environmental parameters such as water levels, weather conditions, and ground saturation. It swiftly detects and alerts stakeholders to critical flood risks, enabling automated shutdown procedures for non-essential processes. This proactive approach aims to minimize potential damage and prioritize safety. Moreover, the tool serves as a communication hub, fostering collaboration among emergency responders, local authorities, and businesses. During disruptions, it provides step-by-step plans and guidance, coordinating responses and offering real-time updates to facilitate informed decision-making.

The strategy **RC-22**, which refers to "short- and long-term restoration plans, ensuring rapid recovery from disruptions" is not addressed by any of the tools of end-users. Esri's ArcGIS Roads and Highways tool allows authorities to manage road networks efficiently by integrating real-time data, assessing damage, and coordinating restoration efforts. It offers tools for monitoring road conditions, managing traffic disruptions, and planning repair projects. Additionally, the U.S. Climate Resilience Toolkit offers resources to manage the impacts of natural disasters like flooding and extreme weather on transportation networks. The toolkit helps planners create long-term restoration strategies for roads and bridges damaged by such events.

The U.S. Climate Resilience Toolkit can also address the strategy **AC-30**. In particular, the Sensitivity Matrix and indicator-based vulnerability screening process, along with the Guide to Assessing Criticality in Transportation Adaptation Planning, offers comprehensive resources for transport operators to evaluate and enhance resilience to climate stressors. Similarly, the open-source, Python-

based CLIMADA tool allows for the assessment of the economic impacts of natural hazards on infrastructure and evaluates the benefits of adaptation measures in planning for climate-related disruptions. These tools can be instrumental in updating risk and recovery assessment methods by incorporating lessons learned from climate change impacts.

2.4 Role R1-B: Managing Traffic

2.4.1 Analysis of Handling Strategies

Important strategies analysed above which are also relevant to Role 1-B refer to **P-6**, **P-7**, **R-13**, **R-14**, **RC-22**, **AC-29** and **AC-30**.

Additionally, all end-users have classified the following strategy, which is relevant to Role 1-B only, as important with a percentage of 100%, yet only one end-user currently addresses it:

- **RC-24:** Efficient road alternatives considering vulnerability and costs.

The end-user who addresses Strategy **R-24** with several tools, such as PTV Logistics, Routyn, and Mixmove, which are categorised as private tools. PTV Logistics Track Route Planning offers tools to optimise transport routes based on vehicle specifics, traffic conditions, and delivery schedules, ensuring efficient and resilient logistics management. Routyn optimises routes by analysing road conditions, traffic patterns, and logistical constraints with advanced algorithms and real-time data, minimising costs and vulnerability to disruptions. Mixmove streamlines transportation logistics through digital solutions that analyse route conditions and logistical constraints, recommending efficient routes that minimize delays and enhance resilience.

Strategy **R-18** is also relevant to Role 1-B and considered important by the end-users (i.e. 75% percentage), though none of the end-users currently address it:

- **R-18:** Efficient road alternatives considering vulnerability and costs.

2.4.2 Commercial Tools for Resilience Management

The selection of strategies to manage traffic during disruptions, such as wildfire, is based on their ability to comprehensively address the components or attributes of resilience. For these strategies, a number of commercial tools are proposed that combine continuous monitoring and predictive analytics to anticipate and prevent disruptions, assessment and strengthening of critical points in the transportation networks, and planning of timely interventions to ensure rapid recovery. In addition, they promote public education and effective coordination, as well as continuous improvement and adaptability through simulations and updates based on lessons learned. Together, these strategies and commercial tools ensure an effective response and a resilient transportation network to emergencies.

Regarding strategy **R-2** “Continuous data collection that accounts for changes in the damage state of physical infrastructure (e.g., roads or bridges) and includes analysis to anticipate disruptions”, Planet Labs is a satellite imagery provider offering high-frequency, high-resolution geospatial data. It provides near-daily imagery for continuous monitoring of areas affected by wildfires and assessing the impact on logistics infrastructure. It assesses damage to the logistics network, identifies critical points and provides mitigation plans in case of wildfires.

Regarding strategy number **R-6** “Continuous resilience assessment and definition of critical points in a logistics network due to ageing and/or disruptive threats based on a resilience indicator”, Interos is

a platform that provides continuous supply chain monitoring and risk assessment in real time. It uses artificial intelligence to assess the supply chain and predict disruptions due to wildfires, and also identifies critical points.

Regarding strategy number **R-7** “Planning and executing timely interventions to prevent disruptions”, Wildfire Analyst is a software that provides real-time analysis of forest fire behaviour. It simulates fire spread in seconds to support rapid decision making, especially in initial attack situations. It provides key information for resource allocation, generating maps and graphs that enable more accurate and faster decisions. Available in desktop, web and mobile applications, it ensures that results reach those who need them, without delay.

Regarding strategy **R-8** "Uniformity in the warning system, standardisation of data, accuracy of weather forecasts and public education in respecting rules and road safety", the European Union has EFFIS: European Forest Fire Information System. Its functionalities include a real-time viewer of forest fires, long-term fire weather forecasts, and a fire risk viewer, among others. EFFIS supports the services in charge of the protection of forests against fires in the EU and neighbour countries and provides the European Commission services and the European Parliament with updated and reliable information on wildfires in Europe. The fires mapped in EFFIS may include fires set intentionally for the purpose of vegetation management.

Regarding strategy number **RC-22** “Short- and long-term restoration plans to ensure rapid recovery” is addressed by IBM Environmental Intelligence Suite. This IMB suite uses artificial intelligence and data analytics to provide information on environmental risks. It offers real-time monitoring and vulnerability analysis of critical infrastructures. Applications include anticipating disruptions, optimising emergency response and developing medium and long-term recovery strategies. Resilinc is a provider of supply chain mapping and risk analysis solutions. It includes tools for continuous monitoring of supply chain resilience and long-term risk assessment. It develops handling strategies, recovery planning and long-term resilience.

A tool that can be used as an answer for the need of the fulfilment of strategies **RC-24** and **RC-25** is ArcGIS. ArcGIS is an advanced geoinformatics tool developed by the Environmental Systems Research Institute (Esri, 2024) for creating, managing, analysing, visualizing, and sharing spatial data and maps. It is widely used across various industries, including urban planning, natural resource management, environmental protection, urban development, logistics, and telecommunications. One of the components of ArcGIS - ArcGIS Pro is a modern desktop application that replaces ArcMap, offering a more integrated environment for handling both 2D and 3D data. It allows users to create maps and scenes, perform advanced analyses, and integrate with other ArcGIS services. ArcGIS Pro features a ribbon-based interface, supports multiple layouts, and enables direct collaboration with cloud services and databases. It can support the efficient designation of alternative routes for both road and rail transport. (**RC-24**), as well as it can support the designation of alternative routes while considering the special requirements of vehicles such as their length or weight (**RC-25**). What is more ArcGIS Enterprise is a server-based GIS platform that manages, processes, and distributes spatial data within an organisation, offering full control over GIS infrastructure, including security, scalability, and data access. It includes components like Portal for ArcGIS, ArcGIS Server, ArcGIS Data Store, and ArcGIS Web Adaptor, forming a comprehensive environment for large teams.

It is important to note, however, that the tool does not continuously collect real-time data, so while simulations conducted with it are very useful, they must be supported by data on routes (which are often already available from public entities or in private databases and disruptions that occur on railway lines.

Strategy **AC-29** "Continuous improvement with disruption simulations and training of the population and logistical stakeholders" can be addressed by SimTable. SimTable offers interactive wildfire modelling, allowing stakeholders to create training modules, plan mitigations and engage the community using local data. Its advanced simulations consider wind, terrain and fuels for a realistic experience. It facilitates planning, training and communication with stakeholders through dynamic scenarios using GIS data. It also publishes animated fire progression maps for active and historic fires, useful for review and reference.

For strategy number **AC-30** "Tool for updating risk and recovery assessment methods to account for lessons learned e.g. from climate change or carbon emissions reduction", Synergi Life risk and barrier management software automates processes, facilitates data management and analysis, and ensures regulatory compliance. The tool essentially establishing a view from corporate level to operational contexts, while complying with data privacy regulations. Features include the collection and centralisation of risk data, the implementation of actions and workflows to mitigate risk, instant alerts for new registrations or deviations, and the ability to analyse risk trends, integrating easily with other data visualisation tools for improved management and impactful results.

2.5 Roles 2 and 3: Configuring and Managing Transport and Logistics Networks

2.5.1 Analysis of Handling Strategies

Important strategies analysed above which are also relevant to Roles 2 and 3 refer to **P-6**, **RC-22**, **R-14**, **AC-30**, **P-7**, **R-13** and **AC-29**.

Other strategies, relevant to Roles 2 and 3 only, which all of the end-users have identified as important (i.e., having a percentage of 100% in Figure 4) but half of them still do not address them are:

- **R-16:** Specific tool to know the cost of transport, fuel, and changes in demand in freight transport
- **R-19:** Managing high shipping rates and fuel price increases
- **RC-23:** Changing transportation modes to avoid disruptions

Most of the end-users have classified the following strategies as important (i.e., having a percentage of 75% in Figure 4):

- **RC-21:** Collaborating with new partners to maintain operations when usual partners are affected

The following strategies are classified as important with a percentage of 75% or above, though half of the end-users address them, at least; therefore, they will not be examined further in the following subsection:

- **P-3:** Data integration and market analysis for future planning
- **R-15:** Specific tool to access data from shipowners for terminal and carrier planning
- **R-17:** Specific tool for container tracking and port entity occupation
- **R-20:** Managing sudden fluctuations in cargo volumes
- **AC:31:** Flexibility to find new partners and build redundancy at critical points

2.5.2 Commercial Tools for Resilience Management

Everstream analytics claims that 75% of supply chain companies do not have adequate preparedness for addressing disruptions, yet they focus on improving response and recovery efforts. These efforts may not be sufficient to deal with disruptions due to the sheer volume, variety, and novelty of disruptive events over the past few years, which exceeds the capacity of companies to respond and recover. This statement aligns with the results of the poll, since strategies referring both to preparedness (**P-6**, **P-7**) and recovery capacity (**RC-22**) are not addressed by the end-users.

In some cases, strategy **P-6** can be supported by the Project44 tool component as part of the monitoring and reporting of disruptions. This tool delivers the visibility of the whole supply chain with the ports, terminal capacity and gives information to the supply chain stakeholders if there is any disruption on the monitored transport route. On this basis, the goods owner can take further transport instructions. However, the tool does not predict the probability of disruption or its duration.

With regard to the "not addressed" strategies **P-2**, **P-7**, **R-13** and **R-14**, Everstream Reveal offers real-time global incident monitoring, such as natural disasters, cyberattacks, weather incidents, plant closures, workplace accidents, production halts, and 120 other incident categories that have the potential to slow or stop the supply chain. Powered by proprietary data feeds and the largest global supply chain intelligence network, Everstream Reveal accounts for advanced AI, machine learning, and human analysis to process data for preventing disruptions or mitigating losses in the "before" or "during" phases.

For logistics operators acting as stakeholders from Role 2 and Role 3, especially those operating in global logistics networks, handling transport rates, including sea freight, and fuel prices is an extremely important aspect. This is because the profitability of companies and their offers depend on these factors. These requirements fall within the managing strategy **R-19**, which is hardly addressed through the use of specialised tools by SARIL end-users. Commercial tools on the market that can secure these user needs are tools that collect and analyse data on transport rates from various global trades and further offer daily or weekly analyses and forecasts of these rates. Such instruments may include tools and paid subscriptions from providers such as Freightos, Alphaliner, Xeneta. These tools, available as online platforms, aggregate and provide up-to-date data, depending on the option chosen, monitoring the fluctuation of transport rates in maritime transport, but also analysing capacity at ports and marine terminals. Advanced versions of these tools, such as Alphaliner Predict API enables predictive analytics considering rate levels, port congestion data and other factors affecting cargo traffic.

Collaborating with new partners when usual partners are affected by crises is a very important managing strategy for stakeholders operating on logistics market as configuring and managing transport and logistics network entities. This **RC-21** factor similar to the **AC-31** factor of flexibility in finding new or replacement partners can be covered by the use of tools based on transport market exchanges. Tools such as Trans.eu, Timocom, or Teleroute operate on the basis of an online resource exchange platform structure. It is possible to make one's own consignments or vehicles available for use at a specific time and in a specific destination. This solution offers the opportunity to use resources in an agile manner, whether you want to increase the efficiency of your logistics network or acquire new business partners in the event of disruption to your existing business network. For the specific type of road freight that is containerised cargo, there are dedicated collaboration tools such as the e-containers.eu platform. This makes it possible to share or exchange containerised cargo or to cooperate with a cross-section of road and intermodal hauliers and forwarders in the area of cargo handling and the use of transport resources such as vehicles.

2.6 Commercial Tools for Resilience Management of the Information System

The stakeholders did not mention any cyber security or cyber resilience specific tool in the poll. However, multiple categories of effective tools have been designed to evaluate threats, handle cyber incidents, and overall increase the cyber security and cyber resilience posture of an organisation. Moreover, some of the questions that were identified as important by the stakeholders in the poll could be completely or partially covered by such tools. Here we proceed to present the most relevant commercial or open-source tools for cyber security and cyber resilience management, and discuss which elements of cyber resilience and which strategies of the poll they may address. Threat intelligence tools may help an organisation in handling strategies **AC-30**, **AC-32**, and **AC-33** (see Annex I). An important note is that such tools often require the presence of a SOC (Security Operation Center), CERT (Computer Emergency Response Team) or CSIRT (Computer Security Incident Response Team), since they require domain knowledge.

The first category of tools is that of SIEMs (Security Information and Event Management), which are frameworks which allow an organisation to detect threats and manage security incidents. Splunk is, amongst other things, a tool that can act as a SIEM. Splunk works by collecting data from various sources like logs and network traffic, then indexing it so it can be easily searched and analysed in real-time. Users can create queries and custom dashboards to monitor and visualise this data, helping in quickly detecting security threats and anomalies. Splunk also allows setting up alerts for specific conditions and can integrate with other tools to enhance its capabilities. Similarly, IBM QRadar collects and analyses data from across an organisation's IT infrastructure to identify potential security incidents. It also supports compliance reporting and forensic investigations by storing security event logs. Both these tools may be effective to increase preparedness and robustness phases of a cybersecurity event, allowing to block and detect attacks.

SOAR (Security Orchestration, Automation, and Response) solutions can then be used to react to the events recognised by SIEMs. A SOAR orchestrates and automates routine and repetitive tasks involved in incident response, such as data collection, threat intelligence gathering, and initial remediation actions, allowing to speed up response times and reduce the manual workload of the security team. Famous examples of such tools are Cortex XSOAR and Splunk Phantom. In relation to the poll, a combination of such tools may partially or completely answer to handling strategies **P-6**, **P-7**, **R-11**, **RC-22**, **RC-27**, **AC-28**, and **AC-30**.

At a higher level, SIRPs (Security Incident Response Platforms) are designed to help an organisation to manage and respond to security incidents, providing a collaborative environment for security teams to analyse, investigate, and resolve them. An open-source example of this category of tools is TheHive.

Another category of tools and services that is definitely useful for organisations managing their cyber risk and cyber resilience are threat intelligence tools, used to receive and analyse threat intelligence reports, indicators of compromise (IOCs), and that provide insights into threat actors tactics, techniques, and procedures (TTPs). Some famous, at a high level similar threat intelligence tools and services are Recorded Future, ThreatConnect, IBM X-Force Exchange, and Palo Alto Networks AutoFocus. Specific reference is made to MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), an open knowledge base of adversary tactics and techniques based on real-world observations.

2.7 Gaps in the Current Approaches and Tools

The analysis of the results of the end-user poll highlighted several critical gaps in resilience management strategies for transport and logistics networks. Notably, there is a need for a comprehensive resilience indicator that includes all components of resilience, such as infrastructure adaptability to changing conditions, climate-related risks, and long-term sustainability goals. Furthermore, the end-users highlighted several criticalities in the current approach to resilience management:

- **P-6**: Lack of tools for continuous resilience assessment and definition of critical points in a logistics network due to ageing and/or disruptive threats based on a resilience indicator
- **P-7**: Lack of tools for planning and executing timely interventions to prevent disruptions.
- **R-14**: Absence of digital tools that provide step-by-step guidance during disruptions, such as alarm systems or integrated sensor networks.
- **R-15**: No specific tools to access data from shipowners for improved terminal and carrier planning.
- **R-16**: Missing tools to assess the cost of transport, fuel, and demand changes in freight transport.
- **R-17**: Lack of tools for container tracking and monitoring port entity occupation.
- **R-18**: No specific tools to obtain real-time information from rail infrastructure managers regarding rail route capacity.
- **AC-29**: Missing systems for continuous improvement through disruption simulations and training for logistical stakeholders and the population.

For the information system, stakeholders did not specify tools but highlighted significant gaps in existing strategies for managing cyber threats and enhancing recovery capabilities. There is currently a lack of a unified approach to resilience, as current tools primarily focus on detection rather than holistic adaptability. Additionally, while some platforms automate response workflows, they lack comprehensive planning for timely interventions to prevent disruptions (**P-7**, **R-14**). There is also a need for better integration of threat intelligence to inform long-term resilience strategies (**AC-30**, **AC-32**) and a lack of focus on sustainability within cyber resilience tools.

3. Literature Review on Resilience Modelling and Management

The gaps identified through the end-user poll were the starting point for the literature review that is reported in this section. The review has been carried out in terms of the same resilience components (preparedness, robustness, recovery, and adaptive capacity) across the three Roles (infrastructures, traffic, transportation and logistics networks managers) and managed functionalities (load-carrying, transportation, logistics) described in the previous sections and deliverables.

In D1.2, “resilience factors” were defined as attributes that describe the capacity of the system to endure and recover from disruptions minimizing the reduction of its functionality or performance. For each resilience factor, “resilience sub-factors” and relevant “KPIs” were introduced as measurable resilience attributes within each resilience factor. These attributes describe generically diverse capacity of the system that can develop in different phases of resilience management. A further classification of resilience factors was performed in D1.2, clustering resilience factors that are mobilised in the different resilience phases. These clusters are defined as resilience components.

To each component correspond a number of resilience factors, sub-factors, and relevant KPIs. For example, in the “during” phase, performance is contingent upon robustness (component) which depends on reliability, visibility and redundancy, etc., (factors). As defined in deliverable D1.2, Key Performance Indicators (KPIs) are established to quantify the various resilience sub-factors. The factors, sub-factors and associated KPIs can be found in Appendix I and II of D1.2 for each Role. Therefore, resilience modelling requires the modelling of each KPI. In this respect, this literature review presents the resilience KPIs proposed in literature.

The resilience curve depicted in Figure 7 illustrates the performance (Q) of a generic system across the several phases of resilience management (“before”, “during”, “after”, and “beyond” a disruptive event). This curve emphasizes how resilience components affect the system performance during the phases of resilience management. A disruption is intended as a loss of performance of a system. In the case, for example, of a physical infrastructure, a disruption could be a natural or a man-made event that damages some of its part. Damage to the physical infrastructure disrupt the transportation performance which affects the transportation and logistics network. It is noted that the disruption for a transportation or a logistic network is any event that leads to a loss of transportation performance, irrespective of its source and nature, that is a natural or man-made local event, or a global event, such a war or pandemic.

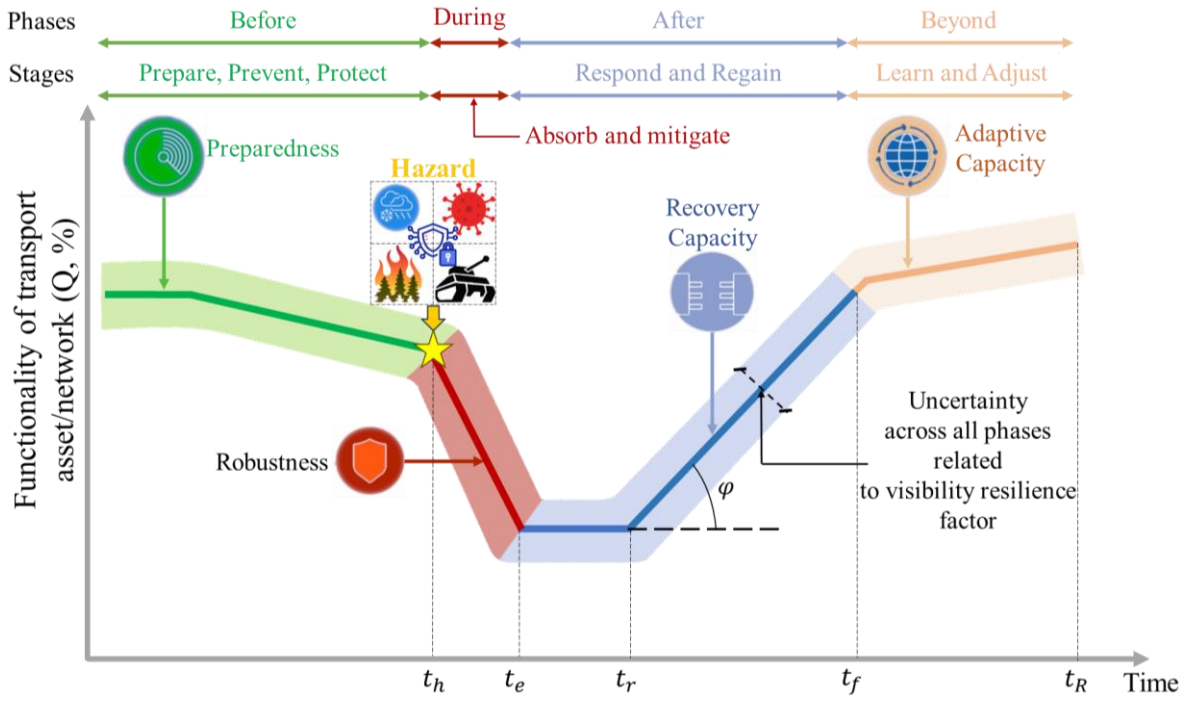

Figure 7: The resilience curve which describes the performance of a system with respect to time, including the different components of resilience, namely preparedness, robustness, recovery capacity and adaptive capacity as well as the phases of resilience (time points t_h and t_e refer to the start of hazard occurrence and emergency management; t_r and t_f refer to the start of recovery and full performance; t_R refers to the time of a new disruption) (after Karagiannakis et al. (2024).

Each of the four considered resilience components corresponds to one phase of resilience management: "before", "during", "after", and "beyond" the disruption.

In the "before" phase (until t_h), the performance is dependent on the preparedness measures and may increase, remain constant or even decrease due to deterioration.

During the event (from time point t_h until t_e), performance is tied to the system's ability to mitigate losses caused by the disruptive event—reflecting the system's robustness. The duration of this phase can vary considerably based on the nature of the hazard; for example, an earthquake might last seconds, while a flood or wildfire could persist for days or months, and war might extend over years.

Post-event, the system may not immediately recover its performance; there is often a delay before recovery commences, determined by the effectiveness of emergency management (period between t_e and t_r). When recovery begins, resource availability and preparedness significantly influence recovery time—more resources and better preparedness typically result in shorter recovery durations. This dynamic is illustrated by an increase in the angle ($\boldsymbol{\varphi}$) on the resilience curve. By the end of the recovery period (time point t_f), the system's performance may be greater than, equal to, or less than its pre-event level, depending on the recovery capacity. In the "beyond" phase, the variation of performance is influenced by the system's adaptive capacity, which refers to its ability to adjust to a new state informed by lessons learned from the disruptive event. The "beyond" phase corresponds with the "before" phase of a subsequent disruptive event, illustrated in Figure 7 by the time point t_R.

The review is presented for the three Roles described in D1.2. Each of this Role manages a different system performance and is interested in resilience with respect to different disruptions. For instance, R1-A is performed by Infrastructure Manager who oversees structural performance which might be affected by natural or man-made hazards. Role 1-B is performed by the Traffic Manager who manages the traffic performance which is affected by a disruption which is the lack of performance of the

physical infrastructure, irrespective of its nature and type. Transportation performance is managed by Roles 2 and 3 in long- and short-term, respectively and is affected by a disruption which is lack of traffic management and lack of performance of the physical infrastructure.

For all roles R1, R2, R3, resilience management consists of the implementation of handling strategies aimed to reduce the impact of disruptions on system performance. The impact of the disruption is measured in terms of cost functions that can be used to optimise resilience management. A review of the cost functions proposed in literature is reported for the three roles in the section on resilience management.

3.1 Role R1-A: Developing and Maintaining Transport Infrastructure

3.1.1 Resilience Modelling

Role R1-A focuses on developing and maintaining transport infrastructure, which includes roads, bridges, and railways that facilitate the movement of goods and people. Resilience components describe the capacities of the system (infrastructure) that affect its load-carrying performance. For role R1-A, resilience management consists of the implementation of handling strategies aimed at reducing the impact of disruptions, such as natural or man-made hazards, on the load-carrying capacity of the physical infrastructure. The impact of the disruption is measured in terms of cost functions.

Preparedness

The resilience component of preparedness involves identifying structural or functional deficiencies, prioritising strengthening actions, acquiring necessary resources, and strategically distributing them within the system before a disruptive event. Resilience is defined by two main system functionalities for transport infrastructures: structural or load-carrying capacity and transportation performance. Concerning structural performance, preparedness pertains mainly to measures intended to increase the structural capacity of the system to mitigate and absorb the actions during a disruptive event. Preparedness is also related to organisational aspects intended to increase the recovery capacity of the system in the immediate aftermath of the event, e.g. planning and prioritising the response to a disruption. For this reason, the concept of preparedness and, thereby, models and KPIs proposed in the literature for its description and quantification are usually related to robustness and recovery capacity (Karagiannakis et al., 2024). The same approach is used in literature to model resilience in terms of variation in transportation performance. For example, the seismic resilience of healthcare facilities was addressed, and the functional capacity of critical infrastructures was modelled, assuming a full traffic capacity before the disruptive event (Bruneau et al., 2003; Bruneau & Reinhorn, 2007; Cimellaro et al., 2009), where a unique resilience metric that considers the robustness and the recovery capacity was proposed. In the literature, robustness is often defined as the complement of fragility, i.e., the probability of exceedance of a certain damage state given an intensity measure of the disruption. The damage state is commonly associated with a reduced traffic capacity of the asset in the aftermath of an event.

However, the assumption of preserving full traffic or structural capacity before a disruptive event is not always valid. In fact, the capacity of a road network can decrease, remain constant or even rise before a disruptive event. For example, deterioration due to corrosion or fatigue can reduce the structural capacity of a bridge, and this can affect its traffic capacity due to the bridge partial or complete closure. In contrast, if retrofitting measures are taken, robustness with respect to a future disruption increases. According to Biondini & Frangopol (2016) and Ghosn et al. (2016), several deterministic and probabilistic performance indicators can be used to evaluate the structural capacity

of an asset, such as ductility, structural redundancy, load resistance factor or time-variant reliability index. The European standard (EN 16991, 2018) specifies a mathematical function (Eq. 1a) of structural capacity deterioration that can be used by engineers and infrastructure operators for risk-based inspection and maintenance within the life cycle of a structure. Recently, Domaneschi et al. (2024) investigated the change of robustness with deterioration by using a mathematical function (Eq. 1b) that accounts for investments, still at a conceptual level, such as structural health monitoring and/or structural control. Thus, if investments are made within the lifecycle of a structure, the function is modified to account for the capacity enhancement.

$$Q(t) = p_0 + p_1 \cdot t + p_2 \cdot t^2 + p_3 \cdot t^3 \quad \text{(Eq. 1a)}$$

$$Q(t) = Q_0 - \beta \cdot e^{(a \cdot t)} \quad \text{(Eq. 1b)}$$

Where $Q(t)$ describes the capacity curve; p_{0-3}, a & β are coefficients that regulate the intensity and velocity of deterioration, accounting for investments, Q_0 is the initial capacity, and t is the time.

The capacity curve of a structure or system is dynamically evolving during its service life by various conditions characterised by diffuse uncertainty, e.g., changes in loading conditions imposed by traffic or climate change. Therefore, the capacity curve as a function of time is given by the updated equation (Domaneschi et al., 2024):

$$Q'(t) = Q(t) + W(t) \quad \text{(Eq. 2a)}$$

$$W(t) = N\big(\mu_i(t), \sigma_i(t)\big) \quad \text{(Eq. 2b)}$$

The function $W(t)$ is a random function with normal distribution that accounts for the change in loading conditions and capacity. It is realised that the mean, μ, and standard deviation, σ, of the distribution are also time-dependent to account for the inherent uncertainty of the process.

Robustness

The second component of the resilience curve relates to robustness, defined as the ability of a system to withstand/absorb a disruption. During the disruption, the system may reduce its capacity, and depending on the type and severity of the disruption, the capacity loss can be significant and rapid. A common KPI to describe the robustness of a system is through its complement: fragility. A fragility function expresses the probability of exceedance of a certain performance level or limit state, e.g. serviceability or life safety, given an Intensity Measure (IM) of the disruptive event, e.g. flood or earthquake (Baker, 2015; Karagiannakis et al., 2022). The limit states, and subsequently the damage states (DSs), are defined in terms of Engineering Demand Parameters ($EDPs$), such as the drift ratio of a bridge pier or lateral displacement of a bridge deck, generically indicated as LS in Eq. 3a, for which threshold values LS_j corresponding to the considered limit states are defined. Lognormal probability distributions are commonly used to express a fragility function (Eq. (3a)).

$$P_j\big(LS \geq LS_j \big| IM\big) = \Phi\left[\frac{1}{\sigma_{tot}} \ln\left(\frac{IM}{IM_{m,j}}\right)\right] \quad \text{(Eq. 3a)}$$

$$P_j\big(DS \leq DS_j | IM\big) = 1 - P_j\big(DS \geq DS_j \big| IM\big) \quad \text{(Eq.3b)}$$

$P_j\big(LS \geq LS_j \big| IM\big)$ is the probability of exceeding the j-th limit state, Φ is the standard cumulative probability function, $IM_{m,j}$ is the median IM, that leads to the exceedance of j_{th} threshold of the EDP. Eq. 3b provides the complement of fragility, which is robustness. σ_{tot} represents the total lognormal standard deviation, considering uncertainty in IM-LS relationship, modelling of a system

and DS definition. Also, σ_{tot} is the total lognormal standard deviation, which is given by the following equation:

$$\sigma_{tot} = \sqrt{\sigma_{IM}^2 + \sigma_M^2 + \sigma_{LS}^2} \quad \text{(Eq. 4)}$$

where σ_{IM} is the uncertainty of the $IM - LS$ relationship (demand or input uncertainty), σ_M is the uncertainty in the modelling of a system, and σ_{LS} is the uncertainty in the LS definition. Additional uncertainties do exist but are less significant, as stated in Bakalis & Vamvatsikos (2018).

The level of damage that a system experiences can also be evaluated in terms of direct losses, which occur during a disruptive event. The indirect losses, which are related to the system loss of performance, depend on the recovery time, thus they are addressed in the recovery component of resilience. Within direct and indirect losses, there are also economic losses and casualties' losses. According to Cimellaro et al. (2010), the direct economic losses that refer mainly to physical and non-structural losses can be expressed as the ratio of the structure's repair and replacement costs as follows:

$$L_{DE}(IM) = \sum_{j=1}^{n} \left[\frac{C_{S,j}}{I_S} \cdot \prod_{i=1}^{T_i} \frac{(1+\delta_i)}{(1+r_i)} \right] \cdot P_j\left(LS \geq LS_j \middle| IM\right) \quad \text{(Eq. 5)}$$

where P_j is the fragility function as defined in Eq. (3); $C_{S,j}$ is the structure's repair costs associated with the j-damage state; I_S are the structure's replacement costs; r_i is the annual discount rate; T_i is the time range in years between the initial investments and the occurrence time of the extreme event; δ_i is the annual depreciation rate. Eq. (5) assumes that the initial value of an asset is affected by the discount rate, but the value also decreases with time according to the depreciation rate δ_i, which may vary with time. Losses due to direct casualties are evaluated as the ratio of casualties over the total number of people involved in the disruption, for example, the total number of patients that a hospital can host (Cimellaro et al., 2010). However, this definition cannot be easily adapted to transport infrastructures since bridges are not hosting facilities. Several studies on bridge loss assessment due to natural hazards do not consider casualties as a direct cost yet, only direct repair losses. Similar expressions to Eq. (5) for estimating direct losses can be found in the literature, especially due to earthquake hazard (Bradley et al., 2010; Dong & Frangopol, 2015; Xiang et al., 2020), among others. It should be emphasized that Eq. (5) provides the losses as a percentage, which can further be associated with the level of performance on the resilience curve. If direct losses need to be estimated in monetary terms, then Eq. (5) is modified as follows:

$$DC = L_{DE}(IM) \cdot c_{REB} \cdot W \cdot L \quad \text{(Eq. 6)}$$

where c_{REB} is the rebuilding cost per square meter (€/m^2); W & L represent the width and length of a bridge. More information about the repair costs with respect to each damage state can be found in HAZUS technical manual for flood hazard (FEMA-HAZUS, 2012).

Arguably, indirect losses are significantly higher compared to direct repair losses; however, they are not straightforward to estimate, and this is the reason that the literature has focused on this type of losses.

Recovery capacity

In the phase 'after' the disruption, the system starts restoring or regaining its performance. The recovery of the structural performance is denoted as 'restoration' process, while the recovery of the service performance (e.g. transportation for a bridge) is denoted as 'reinstatement' process. The type,

number, sequence, and duration of restoration tasks carried out by repair crews depend on the typology of the assets, damage state, available resources, and post-hazard idle time. These aspects strongly affect the recovery time of the asset (Mitoulis et al., 2021). The reinstatement process is described in terms of the increase of the traffic capacity. Restoration and reinstatement are intimately linked, since the gradual increase of the traffic capacity during the recovery process depends on the completion of the restoration tasks. The KPIs used to quantify the performance during the recovery process is denoted as restoration or reinstatement function, Q_{rec}, and usually modelled through the following three functions, depending on the level of preparedness (Cimellaro et al., 2010):

$$Linear: Q_{rec}(DS_i|T=t) = \alpha_2 \cdot \frac{t-t_r}{T_{rec}} + b_2 \quad \text{(Eq. 7a)}$$

$$Exponential: Q_{rec}(DS_i|T=t) = \frac{\alpha_2}{2} \cdot \left\{1 + \cos\left[\pi \cdot b_2 \cdot \frac{(t-t_r)}{T_{rec}}\right]\right\} \quad \text{(Eq. 7b)}$$

$$Trigonometric: Q_{rec}(DS_i|T=t) = \alpha_2 \cdot \exp\left[\frac{-b_2 \cdot (t-t_r)}{T_{rec}}\right] \quad \text{(Eq. 7c)}$$

where α_2 & β_2 are constants that depend on the preparedness level, t_r refers to the time point of recovery commencement and T_{rec} is the recovery time. When there is low level of preparedness of the transport operator, the linear function can be employed, whereas the trigonometric and exponential ones refer to medium and high level of preparedness. Mitoulis et al. (2021) carried out a survey and derived restoration and reinstatement functions based on the responses of operators, engineers, and experts in the field. In Figure 8, a representative sequence of restorations (R_i) tasks and reinstatement functions that describe the functional capacity for two damage states (moderate and severe) of a bridge are demonstrated. Unfortunately, restoration and reinstatement functions are difficult to be found in the literature, given that they are based on extensive surveys, and the voluntary effort of responders. Considering the fragility function of Eq. (3) and restoration/reinstatement function of Eq. (6), the capacity of a transport asset or system at a given time t after the commencement of the restoration works is given by:

$$Q_{rec}(t) = \sum_{i=0}^{n} Q_{rec}(DS_i|T=t) \cdot P(DS = DS_i|IM) \quad \text{(Eq. 8)}$$

where $P(DS = DS_i|IM)$ is the probability of being in DS_i for a specific IM. Based on the fragility function of Eq. 3, this is given by Eq. 8, for a number of damage states ($i = 0$, no damage):

$$P(DS = DS_i|IM) = P(DS \geq DS_i|IM) - P(DS \geq DS_{i+1}|IM) \quad \text{(Eq. 9)}$$

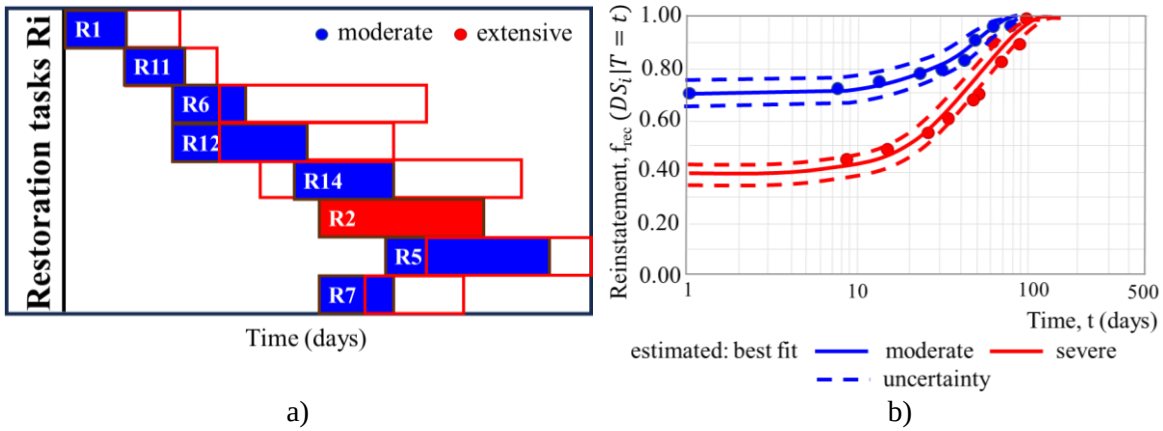

Figure 8: Recovery capacity component of resilience: a) restoration tasks and b) reinstatement functions for bridges.

When a bridge experiences damage due to a flooding event, and the operator decides to close the bridge, the vehicles are forced to follow an alternative path to their destination leading to indirect consequences. These consequences are associated with the running cost and monetary losses of vehicles detour, business interruption, relocation expenses, rental income losses, etc. In contrast with the direct losses, the indirect ones are dependent not only on the severity of the hazard but also on the recovery time. In the following, only indirect losses associated with the detour and time loss are estimated. The running cost of vehicles due to a detour on a bridge subjected to flood hazard can be expressed as (Stein et al., 1999):

$$C_{Run}(DS_j|T=t) = \left[c_{Run,car} \cdot \left(1 - \frac{ADTT}{100}\right) + c_{Run,truck} \cdot \frac{ADTT}{100}\right] \cdot D \cdot Q_{rec}(DS_j|T=t) \quad \text{(Eq. 10)}$$

where the cost of running cars and trucks per km (€/km) are denoted as $c_{Run,car}$ and $c_{Run,track}$ respectively; D is the length of the detour (km); and ADTT represents the average daily truck traffic ratio. The monetary value of time loss for both users and goods traveling along the detour and damaged link can be computed as (Stein et al., 1999):

$$C_{TL}(LS_j|T=t) = \left[c_{AW} \cdot O_{car}\left(1 - \frac{ADTT}{100}\right) + \left(c_{ATC} \cdot O_{truck} + c_{goods}\right) \cdot \frac{ADTT}{100}\right] \cdot \left[Q_{rec}(DS_j|T=t) \cdot \frac{D}{S} + ADE \cdot \left(\frac{1}{S_D} - \frac{1}{S_0}\right)\right] \quad \text{(Eq. 11)}$$

where c_{AW} is the average wage per hour (USD/h); c_{ATC} is the average total compensation per hour (USD/h); c_{goods} is the time value of the goods transported in a cargo (€/h); ADE is the average daily traffic remaining on the damaged link; O_{car} and O_{truck} are the average vehicle occupancies for cars and trucks, respectively; l is the route segment (i.e., link) containing the bridge (km); S_0 and S_D represents the average speed on the intact link and damaged link (km/h), respectively; and S represents the average detour speed (km/h). The expected economic indirect loss associated with each damage state is quantified by multiplying these outcomes by the probability of being at each damage state (from the fragility function). The total indirect losses are the sum over all damage states as these states form a set of mutually exclusive and collectively exhaustive events:

$$L_{IE}(IM) = \sum_{j=1}^{n} \left[C_{Run}(DS_j|T=t) + C_{TL}(DS_j|T=t)\right] \cdot P_j\left(DS \geq DS_j \middle| IM\right) \quad \text{(Eq. 12)}$$

The investigated time interval starts from the time when the repair/rehabilitation action is applied to the damaged bridge and ends at a given time point. As the performance of the bridge increases with time (e.g., days) due to repair/rehabilitation actions, the daily indirect loss associated with the damaged bridge decreases.

Adaptive capacity

The last phase of the resilience curve pertains to adaptation, which has received the least attention among all the phases in the literature. For example, climate adaptation is crucial for coping with the impact of climate change. The adaptive capacity refers to the systems' ability to learn from previous disruptive events, be flexible and adjust to deal with future disruptions. At the end of the "after" phase, a system may reach lower capacity than the "before" phase, which means that it was not resilient to cope with the disruption. In contrast, if the system is resilient, it may preserve the full capacity of the "before" phase, but lessons-learned might not be taken into account to address similar events in the future. In fact, the optimal scenario pertains to the increase of capacity above the

capacity level before a disruptive event, which means that the system will be capable to perform better when similar disruptions occur in the future (Karagiannakis et al., 2024).

Resilience components	KPIs	Equation	Modelling method
Preparedness	Capacity (structural or functional)	1a, b	Capacity curve and dispersion
	Uncertainty	2a, b	
Robustness	Robustness	3a, b	Fragility/vulnerability function
	Uncertainty	4	
	Direct financial losses	5 & 6	Loss function
Recovery capacity	Idle time	7 & 8	Restoration (structural) and reinstatement (traffic) functions
	Recovery time		
	Rapidity		
	Uncertainty		
	Indirect financial losses	10-12	Loss function
Adaptive capacity	Capacity (post-recovery)	13 & 14	Capacity curve and dispersion

Table 3: Resilience modelling methods, describing various KPIs for the flood hazard, are clustered based on the four different components of resilience.

The benefit of investments for adaptation is usually assessed within the life-cycle of an asset using fragility and risk functions (Mondoro et al., 2018; Pregnolato et al., 2017). Thus, for a hazard with the same intensity, there is a reduction in fragility (the curve shifts to the right) and risk, which can be expressed using Eq. 3, and the following expression applies:

$$P_{aj}\left(DS \geq DS_j \middle| IM\right) < P_j\left(DS \geq DS_j \middle| IM\right) \quad \text{(Eq. 13)}$$

where P_{aj} defined the fragility after adaptation, which is smaller than the fragility of an asset given the same intensity of a flooding event, for example. Considering Eqs. 5 & 12, the total losses after adaptation, L_{aT}, will also be less than the losses without adaptation, L_T, if the same disruptive event occurs, and the decrease in losses will be equal to capacity gain, G_{in}:

$$G_{in} = L_{aT} - L_T,\ L_T = L_{DE} + L_{IE} \quad \text{(Eq. 14)}$$

Table 3 summarises all the KPIs and modelling methods that are used to assess them. The KPIs are classified based on the resilience components as presented in the previous sections.

3.1.2 Resilience Management

This section contains a literature review on measures to manage resilience of transport infrastructures. Handling strategies may be taken to improve resilience, information from monitoring systems may be used as a decision support tool to improve resilience management. The impact of resilience management measures is quantified in terms of cost functions.

Handling (mitigation and adaptation) strategies

Mitigation strategies can be taken in the "before" phase to increase the robustness of the infrastructure to natural hazards and minimize the likelihood and severity of damage. These measures typically involve structural interventions or engineering solutions designed to strengthen the infrastructure and reduce its vulnerability to natural hazards. For example, one of the most common failure modes for riverine bridges, is linked to the reduction of the bearing capacity of the foundation, due to scour. An example of mitigation strategies consists in the installation of new, or in the enhancement of existing, protection systems such a sheet pile retaining walls, sloping-front structures, vertical pile foundation or submerged pipeline (Hung & Yau, 2017). When it comes to landslides, attention should be given to the construction of barriers, stabilisation measures, use of vegetation with deep rooting system and relocation of asset due to high risk (Winter, 2016).

Type of strategies	Resilience component	Adaptation strategies
Grey strategies	All	• Monitoring of structural response • Monitoring hazard-induced actions e.g. river water level, flow velocity, wind speed • Monitoring of operational factors, e.g., traffic
	Robustness	• Installation of new or improvement of existing scour protection system e.g. retrofitting of bridge foundations with additional piles • Bridge scour monitoring • Construction of dikes and creation of flood barriers for protection against water • Innovative materials resistant to corrosion • Elevation of roads • Construction of dikes and creation of flood barriers for protection against water • Need for improvement of drainage-sewer systems as well as for more roadside rain pits • New asphalt mixes that help in faster drainage of standing water • Enhancement of road layers to prevent washing off • Measures of protection against slope subsidence around road/rail network to avoid cut-off links Regular maintenance of rivers to avoid debris accumulation
	Recovery	• Design of and investment in new assets with "quick restoration" capability e.g. modular components, pre-fabricated elements, or standardized designs
Green strategies	Robustness	• Suitable vegetation at slopes and roadsides for soil stabilization, absorption of water and reduction of surface run-off
Soft strategies	All	• Policy recommendations for the usage of digital decision support tools, which are able to manage transport across their lifecycle • Frequent inspection and maintenance • Risk assessment models with multiple hazard scenarios and climatic projections for possible upgrading or redesign of transport assets

		• Land-use planning for relocation of transport paths • Communication channels between transport operators, stakeholders, local communities, and civil authorities to adjust and prioritise strategies • Insurance schemes that provide faster recovery and increase awareness • Campaigns to increase public awareness regarding local hazards • Setting and implementation of standards for emergency management (e.g., weather warnings). • Priority plans to maintain access to critical facilities e.g. hospitals, power plants • Definition of priority routes for road clearance in case of large-scale impacts • Coordination of emergency plans among transport modes and networks • Cost-benefit analyses for the best trade-off between resilience and cost in the long-term Early warning for shutting down flood-prone transport networks, activating surge mechanisms and staging repair capabilities at the edge of flood zone

Table 4: Adaptation strategies for transport assets against flood hazard.

On the other hand, adaptation measures for transport infrastructure focus on adjusting to the impacts of disruptions that cannot be entirely mitigated. The goal of adaptation is to "manage the unavoidable", enhance the resilience and minimize the negative consequences of climate hazards by improving preparedness, robustness and recovery capacity. The new CER Directive (CER Directive, 2022) and Adaptation strategy (EC, 2021) stipulate that National Authorities shall identify critical entities, receive EU support and embrace grey, green, and soft "investments" or strategies. Grey strategies are infrastructure-based (or technical) measures, green/blue strategies are ecosystem-based and soft pertain to policy, legal, social and financial measures. Such strategies are summarised in Table 4. It can be realized that grey and green strategies intend to increase mostly the robustness of transport assets, by using innovative materials, reducing exposure of assets, and improving maintenance practices. Grey strategies also incorporate monitoring strategies that reduce uncertainty across all the components of resilience. Also, the strategy to design assets with fast restoration capabilities e.g. modular/pre-fabricated components refers mostly to recovery capacity. Finally, soft strategies target all the components of resilience. For example, building a communication channel for collaboration among different actors involved in the resilience management of transport assets can prioritise retrofitting actions and help to build redundancy based on local needs as well as devise emergency plans. The lack of communication and road network redundancy was one of the main causes of road network disruption during the 2023 Emilia-Romagna floods (ReFLOAT-ER, 2023). Also, the policy to carry out frequent inspection and maintenance is an adaptation strategy that refer to the "beyond" phase of resilience.

Information-supported resilience management

The reduction of uncertainty can support resilience management. The uncertainty in the performance estimated across all the components of the resilience curve in Section 3 (represented by function W(t) in (Eq. 2b) is reduced thanks to the presence of SHM. Efficient structural health monitoring plays a crucial role in enhancing the knowledge of the capacity, and thereby of the performance of a system,

across all resilience management phases (before, during, after and beyond). For example, an SHM system can provide valuable information for maintenance and pre-emptive repair actions in the before phase (Limongelli et al., 2018, 2019; Prendergast et al., 2018).

Although the expressions of structural capacity enhancement due to investments in health monitoring still remains conceptual (Domaneschi et al., 2024), the benefits of structural health monitoring for the early damage detection, localization, estimation of degradation, and uncertainty reduction of structural capacity have been described by many researchers. Structural health information can serve to protect a bridge against further progress of structural deterioration, by triggering maintenance measures. (Morgese et al. (2021) proposed a two-stage monitoring methodology for damage detection, localization, and quantification, using fibre optics and a digital image correlation technique. Although the structural health monitoring is a powerful tool for well-informed decision-making, the current state of practice still relies in engineering judgment, empirical approaches and common sense. To address this limitation, (Giordano et al. (2020) developed a decision-making framework based on the value of information, and evaluated the benefits of structural health monitoring information. This information can assist transport asset managers to take proactive actions for bridge closure and repair due to scour erosion. For example Maroni et al. (2021) and Maroni et al. (2022) developed a probabilistic risk assessment framework for bridge damage due to scour, supported by real-time information on the scour depth measured by scour probe sensors. Sensors were installed in one bridge but the fragility of all the bridges along the river was updated by means of a Bayesian network approach. This probabilistic framework can be used during and in the exact aftermath of a flood event to detect damage in real-time. Another example of the use of monitoring information to support decisions is presented in reference (Zheng & Yu, 2015) where the fragility curves of scoured bridges ae assessed based on vibration measurements. A similar application of structural health monitoring in structural assessment can be found in Hann et al. (2009). Similar to the previous resilience components, the recovery capacity is strongly influenced by the availability of structural monitoring information. Through the facilitation of damage detection, localization, assessment of the damage state and effective use of available resources, the monitoring significantly reduces the idle and total recovery time (Giordano & Limongelli, 2020). Also, structural monitoring can potentially reduce the number of visual inspections and thereby restoration costs. Specifically, monitoring information can facilitate the prompt allocation of essential resources and the implementation of appropriate measures, leading to faster restoration performance of a system.

Despite the importance of information as a decision-support tool for resilience management, literature lacks metrics to quantify the impact of monitoring information on resilience management. Value of information from Bayesian decision theory appears as a suitable candidate, possibly able to also quantify environmental, beyond economic impact (Giordano & Limongelli, 2022).

Impact of resilience management measures

Resilience management entails the identification of optimal strategies to enhance resilience that is strategies able to minimize the impact of the disruption. Optimization is often defined in terms of life cycle cost-efficiency and indicators such as those included in Table 5 are defined to quantify it. Life-cycle cost assessment can be used to evaluate the efficiency of resilience enhancement strategies over the system service life For example, Mondoro et al. (2018) proposed as KPI the average annual losses to evaluate the benefit-cost-ratio of different retrofitting strategies. Similarly, Biondini & Frangopol (2016) identified an optimal resilience management approach based on the cost-reliability curve. The strategy that minimised the cost corresponded to the optimal reliability, and constrained to the minimum acceptable reliability value. Pregnolato et al. (2017) used a criticality index (CI) to prioritize adaptation strategies for a road network exposed to flooding. This index was based on two primary

factors: the depth of floodwater on a road segment (hazard) and the average daily traffic flow (exposure). The CI helped identify and rank road segments where both flood hazard and traffic exposure were highest, facilitating the evaluation of adaptation strategies such as hardening vulnerable sections of the road network. These strategies were assessed based on their net present value (NPV) and return on investment (ROI), considering a climatic projection for the year 2080. Adaptation engineering aims to protect infrastructure from climate change impact, as highlighted in the previous studies. Nevertheless, it should also intend to minimise the risk associated with incorrect climate predictions. This emphasizes the preference for flexible strategies that delay actions, allowing decision-makers to assess market and climate conditions further before committing to plans. To this effect, Mondoro et al. (2018) proposed the gain-loss-ratio which is defined as the ratio between the monetary gain and the reduction of losses due to the delay in taking a strategy to adapting to climate change.

Table 5 recapitulates all the aforementioned management indicators. It is important to emphasize that these indicators are mostly associated with the component of preparedness and robustness, since they account for the benefits of increasing the structural capacity of road network before or during the event. In case of Mondoro et al. (2018), the indicators can also be used to increase recovery and adaptive capacity, given that the reduction of losses may refer to strategies that prioritize the reduction of recovery time (indirect losses) over the reduction of vulnerability.

Most of the literature quantifies the impact of disruptions in terms of economic losses. Sustainability aspects are seldom tackled in literature (Aujoux & Mesnil, 2023; Raeisi et al., 2021).

Ref.	Management indicators	Description
(Mondoro et al., 2018)	$BCR = \frac{B_m}{C_m}$	BCR: benefit-to-cost ratio B_m: reduction of average annual losses or risk due to a strategy taken C_m: cost of this strategy
(Biondini & Frangopol, 2016)	$C_m = \sum_{k=1}^{n} \frac{C_k}{(1+v)^{t_k - t_0}}$ $\beta(t_k) = \frac{\mu_{R,k} - \mu_{S,k}}{\sqrt{\sigma_{R,k}^2 + \sigma_{S,k}^2}}$	C_M: Minimum-expected life cycle cost at the optimal reliability index β C_k: the cost of the k-th repair intervention taken at time point t_k and associated with the initial time point t_0 of reliability index measurement by considering a discount rate v n: is the total number of interventions μ, σ: mean and standard deviation of structural resistance and demand, respectively
(Pregnolato et al., 2017)	$NPV_r = \sum_{i=1}^{N} \frac{\int \rho(l_i) D(l_i) dx}{(1+r)^i}$	NPV_r: The Net Present Value of the benefit due to risk reduction is calculated by summing the disruption cost, $D(x)$, and likelihood, $\rho(x)$, of a range of flood events
(Mondoro et al., 2018)	$GLR = \frac{G_m}{L_m}$ $G_m = C'_m - C_m$	GLR: Gain-to-loss ratio G_M: the difference between the present value of the cost of the adaptation strategy m (i.e. C'_m) applied at time t_a and the present value of the cost (i.e. C_m) applied at the time t_0.

Table 5: A summary of cost-based resilience management indicators and their associated resilience components.

3.2 Role R1-B: Managing Traffic

3.2.1 Resilience Modelling of Traffic Infrastructure

There are some official studies that give insight into resilience modelling and management from the perspective of logistic infrastructures and forest fires. For example, wildfires represent one of the greatest threats to society and environment. These events not only cause environmental devastation by destroying ecosystems and their biodiversity but they can also affect critical infrastructure such as roads, causing a major socio-economic impact and affecting the safety of the population and access to affected areas (Sfetsos et al., 2021).

Preparedness

Following the discussion in the previous chapters, the component of preparedness mainly pertains to prevention actions so that both the infrastructure and the population are prepared to mitigate a disruptive event such as a wildfire, before it occurs. In this phase, the implementation of prevention plans that address vegetation management, ensure the performance of evacuation routes, and develop specific response protocols are necessary to mitigate the effects of a potential wildfire. In this regard, a fire risk map is essential to identify and assess those areas where there is a higher probability of fire. Arango et al. (2023) propose the use of KPIs as they present a more holistic approach by considering multiple dimensions of resilience, as well as offering long-term goals and sustainable development policies. However, the use of risk mapping as a resilience assessor for an area is not mutually exclusive with KPIs. Both can benefit from the information they provide.

For this phase, a fire risk map model is applied. The objectives of fire risk mapping are:

- Developing strategies to reduce the impact of wildfires.
- The identification and specific graphical representation of the most at-risk areas.
- Planning emergency protocols

In relation to this, Novo et al. (2020) defines fire risk as the probability of a wildfire occurring in addition to the damage it may cause given a location (vulnerability). The main factors contributing to the ignition and spread of a fire are vegetation, topography, climatic conditions, and human factors. In relation to human factors, Ganteaume et al. (2013) showed that 70% of forest fires are ignited near major roads. Given that the human and material resources of the administrations are limited, good management and optimisation of these resources has become a primary objective in the last decades to fight fires, trying to anticipate them by analysing the causes and conditioning factors.

To understand this, KPIs and models related to vegetation and its flammability have been developed over the last decades, as well as KPIs that measure risk as a function of climatic conditions. Some of these are the fuel models developed by Rothermel (1972), the Normalised Difference Vegetation Index (NDVI) (Rouse et al., 1973), or the Fire Weather Index (FWI) (Van Wagner, 1985).

(Novo et al., 2020) proposed the combination of all these KPIs with other aspects such as the morphometric properties of the terrain, the distance to roads and urban settlements, as well as the fire history of a region are key in the elaboration of a Fire Risk Map that allows us to know the resilience of the terrain by unifying these factors.

According to this, the forest fire risk map is composed of the combination of the following layers reclassified by risk index. That is, 1 very low, 2 low, 3 moderate, 4 high and 5 very high:

- Fuel type map

- Elevation map
- Slope map
- Aspect map
- NDVI map
- FWI map
- Historical fire map
- Road map
- Settlement map

Classifying the layers into groups and considering an Analytic Hierarchy Process (AHP) (Saaty, 1980), the final model with the following equation is obtained:

$$FR = b_1 \cdot V(a_1 \cdot NDVI + a_2 \cdot FMT) + b_2 \cdot T(c_1 \cdot A + c_2 \cdot S + c_3 \cdot E) + b_3 \cdot AI(d_1 \cdot DR + d_2 \cdot DS) + b_4 \cdot FWI + b_5 \cdot FH \quad \text{(Eq. 15)}$$

where FR is fire risk, V is vegetation type, $NDVI$ is normalized difference vegetation index, FMT is fuel model type, T is topography, A is aspect, S is slope, E is elevation, AI is anthropogenic issues, DR is road distance, DS is distance settlement, FWI is fire weather index, and FH is fire historical. The coefficients $a_i, b_j, c_k, d_l, i, j, k, l \in \mathbb{N}$ represent the weights of each term after applying the AHP process. By computing this equation, the forest fire risk map is obtained, in which each pixel will have an associated value from 1 to 5 according to the above classification.

This equation is presented in its most general form, with the coefficients for each term determined through a hierarchical process that incorporates a comprehensive literature review and expert advice from the field for context. For example, for the case study by Novo et al. (2020) of the region of the Iberian Peninsula, Eq. 21 takes the following values:

$$FR = 0.359 \cdot V(0.250 \cdot NDVI + 0.750 \cdot FMT) + 0.108 \cdot T(0.539 \cdot A + 0.297 \cdot AI(0.750 \cdot DR + 0.250 \cdot DS) + 0.298 \cdot FWI + 0.055 \cdot FH \quad \text{(Eq. 16)}$$

Looking at the values of the terms, the vegetation term and the FWI have a higher weight than the rest of the terms. It also coincides with the fact that the layers that compose both terms are those that can be updated more frequently. The morphometric properties of the terrain remain practically constant over time, although they still have a great influence on the spread of a fire, but less so than the aforementioned terms. As for the term related to Anthropogenic Issues, experience shows that a large proportion of intentional fires occur near roads and urban centres, as already mentioned at the beginning of this Section. Finally, fire history has little influence on the fire risk map. The fire risk map is therefore key in the preparedness phase, as it will help to advise administrations and managers in identifying risk areas to take preventive measures, as well as assist in the planning of evacuation routes to ensure that residents can leave risk areas quickly and safely.

Robustness

In contrast to risk maps, which focus on specific hazards and their geographical distribution, resilience KPIs offer a holistic view of a system's ability to cope with and recover from disasters. Risk maps provide probabilities of event occurrence, are specific and focused on particular hazards and their geographical distribution, while resilience KPIs, as advocated by Arango et al. (2023) and Novo et al. (2024), are more holistic, consider multiple dimensions, supporting long-term goals.

Risk maps and resilience KPIs, while distinct, complement each other and enhance overall accuracy. Risk maps identify specific hazards and their geographic distribution, whereas resilience KPIs offer a

broader view of a community's capacity to handle and recover from disasters. Combining these tools enables better planning and response (Holling, 1973; Nogal & O'Connor, 2018).

In forest management, a fire risk map provides a detailed geospatial view of fire risks, aiding in planning. For roads affected by fire, resilience KPIs offer a nuanced assessment of infrastructure's ability to withstand and recover from damage. KPIs include security, connectivity (Akbarzadeh et al., 2019; Liao et al., 2018), reliability (Lim et al., 2022), and efficiency.

Security and connectivity focus on infrastructure resilience, while efficiency addresses passenger needs and network performance. During a wildfire, the system's ability to maintain stable operation despite disturbances is crucial. Robust road networks support effective evacuation and emergency response, reducing wildfire casualties (Niu et al., 2022). High connectivity ensures route redundancy, and efficiency optimizes travel demand and resource use. This integrated approach provides a comprehensive view of fire resilience. The definitions of the discussed KPIs are set out in more detail:

Safety ensures that users are not exposed to hazards, maintaining safe road use and emergency response. The safety KPI (Eq. 23) evaluates this by comparing the travel time through a road link with the time it takes for a wildfire to reach that link. Specifically, the time needed to travel through the link should exceed the time for the fire to arrive.

The FIRE Approach Time ($FIRATi,c$) (Niu et al., 2022) measures this exposure. It represents the average time for a fire of category c to reach a road link i. FIRAT is calculated by dividing the Equivalent Fire Distance (EFD) by the Rate of Spread (ROS) for the fire category. The EFD accounts for all burning sources and fire suppression efforts, providing a distance equivalent to a reference burning source.

$$Safety_{i,c} = \begin{cases} 0\ (unsafe), & FIRAT_{i,c} > t_i \\ 1\ (safe), & FIRAT_{i,c} < t_i \end{cases}, \qquad \forall i \in N, \qquad \forall c \in C \qquad \text{(Eq. 17)}$$

where c indicates the wildfire category for which the safety KPI is assessed, of the set of wildfire categories to be evaluated, *C*. The link travel time, t_i, is compared with the corresponding $FIRATi,c$ for all the links of the set defining the network, *N.* Safety at a network level is assessed considering the portion of safe roads over the total roads in the network for each wildfire category (Arango et al., 2023), as expressed in Eq. 24.

$$Safety_c = \frac{1}{|N|}\sum_{i \in N} Safety_{i,c}, \qquad \forall c \in C \qquad \text{(Eq. 18)}$$

Connectivity target assesses users' ability to move and identifies if there are disconnected areas in the network. A route r consists of a set of links that connect an OD pair, pq. When an OD pair has different alternative routes, the network presents redundancy. The network is considered successfully connected if all the OD pairs of the network have at least one operational route. The connectivity of a given OD pq is assessed as expressed in Eq. 25,

$$Connectivity_{pq,c} = \begin{cases} 0\ (unconnected), & R_{pq,c} = \emptyset \\ 1\ (connected), & R_{pq,c} \neq \emptyset \end{cases}, \quad pq \in PQ, \qquad \forall c \in (\qquad \text{(Eq. 19)}$$

where $R_{pq,c}$ is the set of available routes connecting the OD pair pq under fire category c. When the safety condition is not fulfilled for a link, that is, $FIRAT_{i,c} \geq t_i$, it is assumed that the link is unavailable anymore, disabling the routes going through this link. The number of unsafe links tends to increase with each wildfire category, because of the increase in wildfire spread velocity, reducing the connectivity of the network. Connectivity at a network level is assessed considering the portion of active routes over the total routes of the network before the wildfire. That is,

$$Connectivity_c = \frac{\sum_{pq \in PQ} Connectivity_{pq,c}}{\sum_{pq \in PQ} |R_{pq,0}|}, \qquad \forall c \in C \qquad \text{(Eq. 20)}$$

Efficiency target gives a measure of the network service in terms of its demand capacity and mobility (Taylor & Susilawati, 2012). For this purpose, the efficiency of the available routes of each OD is calculated as a function of its distance and users associated with that OD pair. It is assumed that the shortest route between two points (an OD pair in this case) is the most efficient for users, because it allows faster trips. Thus, the closer the driving distance associated with an OD pair is to the minimum possible distance, the more efficient the route connecting the OD pair is. The minimum possible distance corresponds to the geometric distance, which means in a beeline. Considering the number of users of a route is also relevant, because even when a route is the shortest one, it is not efficient if it has no users. In many cases, there are several routes connecting an OD pair. In such cases, the efficiency associated with an OD can be calculated as the average of the efficiencies of the routes weighted by the portion of users choosing each route. To calculate the efficiency associated with an OD pair under a given fire category, the formulation of Eq. 27 is proposed.

$$Efficiency_{pq,c} = \frac{1}{|R_{pq,c}|} \frac{d_{pq}^{g}}{\sum_{r \in R_{pq}} X_r} \sum_{r \in R_{pq}} \frac{X_r}{d_r}, \qquad \forall pq \in PQ, \forall c \in C \qquad \text{(Eq. 21)}$$

If the value of the efficiency KPI is close to unity, it means that the OD pair is efficient; values close to zero mean that it is not efficient. Efficiency at a network level is assessed as the average value of the efficiencies of all the OD pairs. That is,

$$Efficiency_c = \frac{1}{|PQ|} \sum_{pq \in PQ} Efficiency_{pq,c}, \qquad \forall c \in C \qquad \text{(Eq. 22)}$$

Recovery capacity

Recovery capacity is the ability of a system to return to its original state. It can be evaluated through *Reliability*, which represents how quickly and effectively the network can recover from disruptive events while minimising waiting times. *Reliability* in transportation is defined as the feasibility of road users reaching a destination (Nogal et al., 2019). It is the ratio of minimum travel time within an OD pair under normal conditions $(R_{pq,o})$ to the minimum travel time during the disruptive event $(R_{pq,c})$.

$$Reliability_{pq,c} = \frac{min\{t_r;\ r \in R_{pq,o}\}}{min\{t_r;\ r \in R_{pq,c}\}}, \qquad \forall pq \in PQ, \forall c \in C \qquad \text{(Eq. 23)}$$

Reliability at a network level is assessed as the average of all OD pairs' reliabilities,

$$Reliability_c = \frac{1}{|PQ|} \sum_{pq \in PQ} Reliability_{pq,c}, \qquad \forall c \in C \qquad \text{(Eq. 24)}$$

where PQ denotes the number of OD pairs analysed.

Adaptive capacity

The impact of forest fires varies based on factors that influence control efforts. Key characteristics affecting social and environmental impact include Fireline Intensity (FLI), Rate of Spread (RoS), spotting, and sudden changes in fire behaviour. FLI, a primary factor in wildfire controllability, can be assessed through RoS and fuel consumption or estimated from flame length (FL). RoS, influenced by fuel and weather, affects the rate of spread and the resources needed for control. Spotting, where glowing fragments ignite new fires, increases the area affected and strains firefighting resources.

According to Tedim et al. (2018), controllability is a critical criterion for defining Extreme Wildfire Events (EWE). The current limit for effective fire control is 10,000 kWm-1; beyond this, even heavy firefighting aircrafts are ineffective. It is essential to differentiate between fires that are beyond

current control capabilities and those where control is hindered by resource limitations. EWEs pose significant risks to populations, assets, and infrastructure, potentially leading to fatalities. Post-wildfire experiences provide insights into the effectiveness of mitigation strategies, guiding future adjustments, such as expanding firebreaks and improving forest management. Software packages like Flammap and Farsite, based on Rothermel (1972) spread equations, model fire behaviour using detailed landscape files. These tools calculate parameters such as Flame Length (FL) and Rate of Spread (RoS), which help categorize fires by intensity. Tedim et al. (2018) offers a classification for extreme wildfires, detailed in Table 6.

Table 6 classifies forest fires into categories based on parameters, such as Fireline Intensity (FLI), Rate of Spread (RoS), and flame length. It assesses the type of fire and the difficulty of extinguishing it. From category 4 onwards, the fire's impact makes extinguishing extremely difficult, with higher categories exhibiting phenomena that render the fire uncontrollable. Tedim (2018) defines an Extreme Wildfire Event (EWE) as: "A pyro-convective phenomenon that exceeds controllability, characterized by high intensity, rapid propagation, long spotting distances, and unpredictable behaviour. It poses a serious threat to people, equipment, and socio-economic assets, with significant negative impacts.".

According to the Table 6, fires at level 3 and above become challenging to control. These parameters help identify regions that may be inextinguishable during a wildfire. To model the algorithm accurately, it's crucial to consider regional forest fire prevention and action plans (Técnica, 2020). For the Iberian Peninsula, the parameters accepted for the algorithm are detailed in Figure 9.

Real time measurable behaviour parameters					
	Fire Category	**Fireline Intensity (kWm^{-1})**	**Rate of Spread (m/min)**	**Flame Length (m)**	**Type of fire and capacity of control**
National wildfires	1	<500	<5 [a] <15 [b]	<1.5	• Surface fire • Fairly easy
	2	500-2000	<15 [a] <30 [b]	<2.5	• Surface fire • Moderately difficult
	3	2000-4000	<20 [c] <50 [d]	2.5-3.5	• Surface fire, torching possible • Very difficult
	4	4000-10000	<50 [c] <100 [d]	3.5-10	• Surface fire, crowning likely depending on vegetation type and stand structure • Extremely difficult
Extreme Wildfire Events	5	10000-30000	<150 [c] <250 [d]	10-50	• Crown fire, either wind or plume-driven • Chaotic and unpredictable fire spread • Virtually impossible
	6	30000-100000	<300	50-100	• Plume-driven, highly turbulent fire

					• Chaotic and unpredictable fire spread • Impossible
	7	>100000	>300	>100	• Plume-driven, highly turbulent fire • Area-wide ignition and firestorm development non-organized flame • fronts because of extreme turbulence/vorticity and massive • spotting • Impossible

Table 6: Wildfire events classification based on fire behaviour and capacity of control (adaptation from the original one). Note: a Forest and shrubland; b grassland; c forest; d shrubland and grassland.

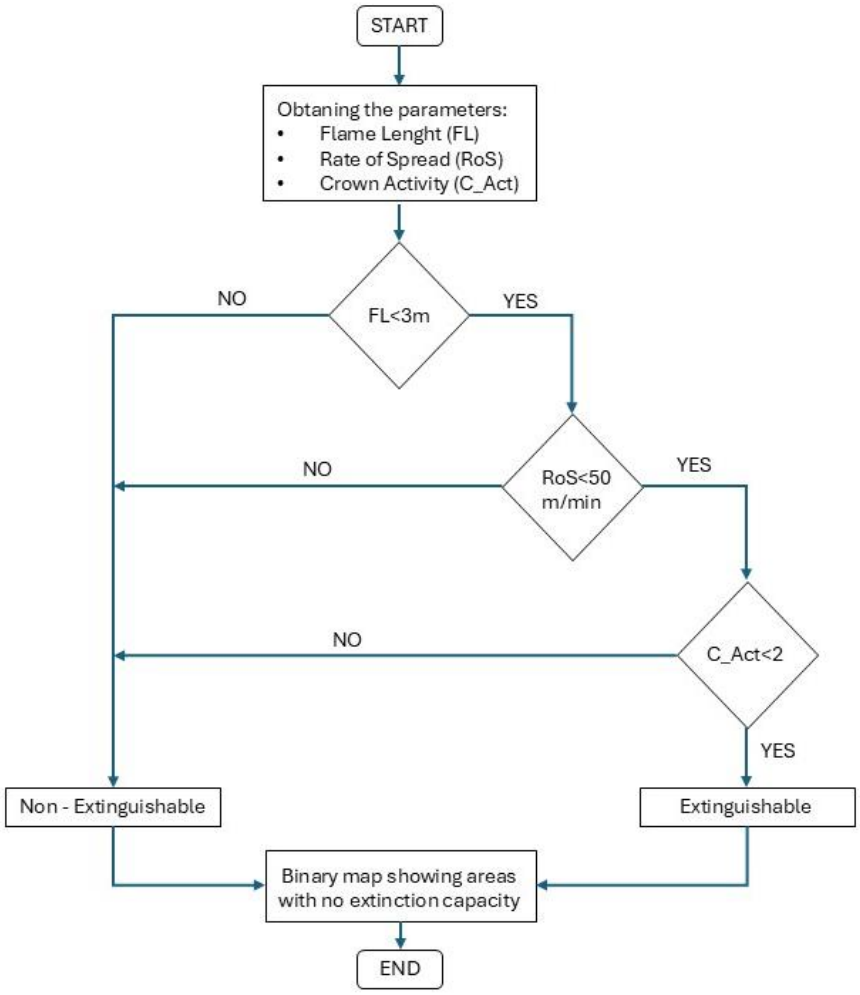

Figure 9: Flow chart for the determination of the Binary Map with the areas outside the extinguishing capacity (own elaboration). Note: C_Act values, 0 No fire behaviour characteristics, 1 surface fire, 2 passive crown fire (torching), 3 active crown fire (Técnica, 2020)

To develop the algorithm, parameters for category 3 are used as a reference: Flame Length (FL) of 3 m, Rate of Spread (RoS) of 50 m/min, and Crown Activity (C_Act) of level 2. Level 2 indicates flare-ups, which signal a transition from surface to crown fire (MFSL, 2023).

The algorithm evaluates each pixel based on these values, classifying areas as non-extinguishable if any parameter exceeds these thresholds, or extinguishable if all are below. The result is a binary map showing areas beyond extinction capacity.

In the beyond phase, it is crucial to ensure flexibility (or adaptability) in learning from previous wildfire events. Up-to-date prevention plans aid in resource allocation, such as acquiring advanced equipment for rapid deployment. Efficient planning and regular updates to firewalls and auxiliary belts enhance preparedness and adaptability, improving overall resilience. Effective forest management, which preserves biodiversity and reduces fuel can significantly lower critical parameters (FL, RoS, C_Act), thus reducing fire impact and ensuring continuous system improvement.

Table 7 outlines the indices and models related to each component of the resilience curve, as defined by SARIL project.

Resilience components	KPIs	Equation	Modelling method
Preparedness	Forest Fire Risk Index	21 &22	• Forest Fire Risk Map
Robustness	Connectivity Index	23 & 24	• Connectivity Function
	Safety Index	25 & 26	• Safety Function
	Efficiency Index	27 & 28	• Efficiency Function
Recovery Capacity	Reliability Index	29 & 30	• Reliability Function
Adaptive Capacity	Rate of Spread (RoS)	NA	• Algorithm for determining the extinguishing capacity of a forest fire
	Flame Length (FL)		
	Crown Activity (C_Act)		

Table 7: Resilience modelling methods, describing various RFs and KPIs for the fire hazard, are clustered based on the four different components of resilience (R1 role).

3.2.2 Resilience Management of Traffic Infrastructure

Handling (Mitigation and adaptation) strategies

Forest fires represent a growing threat. To address this challenge, various strategies have been developed to reduce the frequency and severity of fires, and also to strengthen the resilience of affected communities and ecosystems. Mitigation strategies include the reduction of vegetation fuels, sustainable forestry practices, creation of firebreaks, regulation and monitoring of land use and the development of early warning systems. On the other hand, adaptation strategies include the design of fire-resistant infrastructure, education and training of the population, restoration of affected landscapes, development of risk management plans and promotion of community resilience.

These strategies, when implemented together and in a coordinated manner, form a comprehensive approach to wildland fire management, reducing its impact and promoting the sustainability of ecosystems and the safety of communities.

Following the assessment of the impact of recent fires in the EU (2000-2017), the European Union faces the following policy challenges in the field of forest fires (EC, 2018):

- Promoting effective science-based forest fire management and risk-informed decision-making
- Shifting focus from suppression to prevention and increasing the awareness and preparedness of population at risk
- Developing synergies between EU and national policies to improve wildfire risk management
- Promoting resilience landscapes and communities through integrating fire management in the EU
- Improving firefighting and rescue capacities of first responders in crisis management

These new challenges seek to evolve towards a proactive approach that is based on the root of the problem and provides for long-term actions considering climate change. It is a holistic, resilience-based approach to fire management that encompasses the following stages (Arango et al., 2024) (see Figure 10):

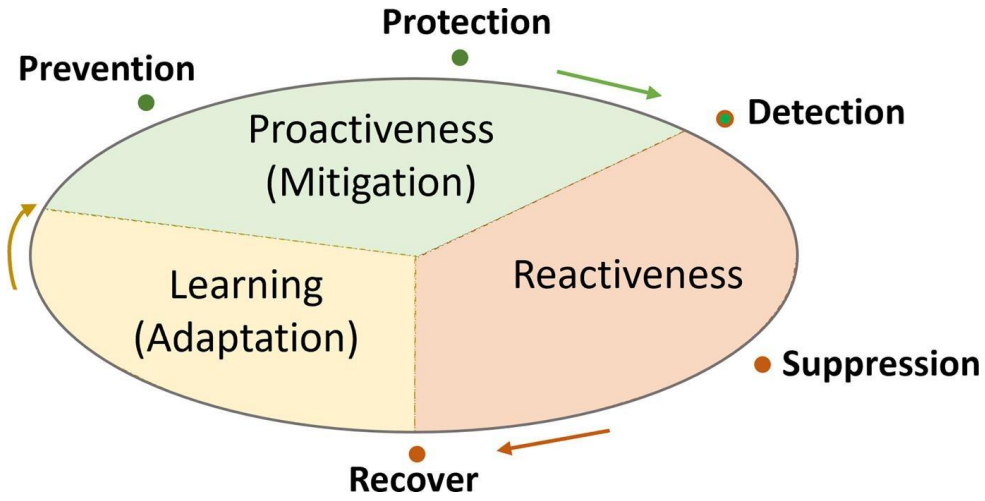

Figure 10: The holistic view of wildfire management based on resilience.

Figure 10 represents wildfire management based on resilience approach. Prevention aims to reduce the risk of wildfires by addressing the root causes, such as reducing fuel loads, managing forests, and implementing fire-safe building codes. Protection involves mitigating the potential damage from wildfires by creating defensible spaces around homes and communities and developing evacuation plans for residents. Detection is also an important aspect of wildfire management, as early warning systems can provide crucial information about the location, size, and potential impact of a fire. Rapid response is critical and suppression policies and resources such as firefighters, helicopters, and equipment are critical to this effort. Once a wildfire has been contained, recovery policies are necessary to help communities and ecosystems rebuild and heal. This includes supporting displaced residents, restoring damaged infrastructure, and rehabilitating affected ecosystems. Effective wildfire management requires a comprehensive and integrated approach that encompasses the five strategies from a resilience perspective. This resilience-based approach significantly impacts the traffic and transportation infrastructure. Prevention measures may lead to road closures or restricted access in

forest management areas to reduce fuel loads. Protection strategies could involve rerouting traffic to create defensible spaces and ensure safe evacuation routes for residents, thereby affecting normal traffic flow. Detection efforts may require the installation and maintenance of monitoring equipment along roadways and railways, influencing transportation schedules. Rapid response necessitates the unhindered movement of firefighting vehicles, helicopters, and equipment, which can lead to temporary road closures and prioritized access for emergency services. Recovery efforts often demand significant transportation of materials and personnel to restore infrastructure and rehabilitate ecosystems, impacting highways, railroads, and local roads. Thus, a resilient approach to wildfire management requires a dynamic and adaptable transportation network to support each phase effectively (Arango et al., 2023). This framework aligns with the Integrated Fire Management framework proposed in the European Commission report (EC, 2018).
The handling strategies proposed in this section mostly use tools based on Geographic Information Systems. These tools can play a crucial role in the EU's efforts to address these challenges. GIS-based tools allow the collection, analysis and visualisation of spatial data, thus facilitating the identification of high-risk areas, the planning of prevention strategies and the rapid and effective response to fires. In addition, GIS enables collaboration and information exchange not only between EU cross-border states, but also between stakeholders in the logistics chain.

Handling strategies for fire risk management are summarised as follows:

- **Forest planning, restoration and stand improvement through forest management:**
  Forest stand management, creation of firebreaks and implementation of sustainable practices reduce the accumulation of combustible materials and protect and conserve biodiversity. It helps to mitigate soil erosion and establish restoration strategies for post-fire recovery.
  Having a classification of indices that have a strong influence on the probability of occurrence of a forest fire, such as those managed in the fire risk map (see Section 3.2.1) is of great importance for disaster planning, prevention and management that can minimise the impact of fires.
  Considering the indices associated with the vegetation category (NDVI and fuel type model, which refers to the various types of vegetation that can ignite and sustain a fire), ecosystems with abundant scrub and dry grassland (models 6, 4 and 3) or dense forests (model 7) present a higher risk of ignition if they are neglected and do not have good management, restoration and conservation plans in place, thus detrimentally influencing the robustness of the region.

  For example, in southern Europe, which is heavily affected by the high frequency of forest fires and where Mediterranean climate and species prevail, it has been found that the endemic species that make up the forests have developed a certain resistance to mild or moderate fires, surviving them and having at their disposal a greater quantity of nutrients obtained from the ashes (Moya et al., 2011). However, the most common post-fire actions developed so far, such as salvage logging, do not positively influence the natural recovery and development of the forest (Bigs & Marquis, 2023). Early clearing treatments (before the 2nd year post-fire) induce lower mortality and improved species growth as shown by some authors (Martínez-Sánchez et al., 1999). Correct monitoring of the NDVI in this sense brings rigour to decision making, applying silvicultural works when the index shows low or moderate risk values and helps to prevent erosion and soil conservation.

- **Preparedness for road interventions in the event of forest fires:**
  Forest Planning, Restoration, and Stand Improvement through Forest Management:

Forest management practices, including firebreak creation and sustainable techniques, reduce combustible materials and protect biodiversity, aiding post-fire recovery and soil erosion mitigation. Classification of indices influencing forest fire probability, such as those in the fire risk map (see section 3.2.1), is crucial for disaster planning and management (Novo et al., 2020).

Indices like NDVI and fuel type models indicate higher fire risk in ecosystems with abundant scrub, dry grasslands, or dense forests if not properly managed. In southern Europe, endemic species exhibit some resistance to mild or moderate fires, benefiting from post-fire nutrients (Moya et al., 2011). However, common post-fire actions like salvage logging hinder natural recovery (Bigs & Marquis, 2023). Early clearing treatments can improve species growth (Martínez-Sánchez et al., 1999), and monitoring NDVI aids in decision-making, applying silvicultural works to prevent erosion and conserve soil.

The following table (Table 8) shows the classification of the most influential terms seen in (Eq. 15 of section 3.2.1 elaborated by Novo et al. (2020) and which compose the forest fire risk map.

- **Preparedness for road interventions:**

  Arango et al. (2024) introduces the GIS-FA tool, developed with a resilience-based perspective. This tool prioritizes the system's capabilities in the event of a fire rather than the probability of fire occurrence. The tool calculates intervention priority by assessing the infrastructure's exposure to wildfires and the criticality of an asset, using the Fire Arrival Time (FIRAT) metric to map exposure. It highlights the environmental impact on fire spread and reflects socio-economic-political activities' influence. The tool helps assess infrastructure resilience, revealing the need for improved management practices, such as better communication and adaptation over suppression. This enhances decision-making for wildfire management, potentially saving lives during events.

- **Improvement in the effectiveness of the initial attack by extinguishing teams:**

  Andrade & Hulse (2023) evaluates the performance and resilience of UAS and UTMs in wildfire response through dynamic simulations. Findings show that reducing communication delays and enhancing surveillance significantly improve fire crew responsiveness, enabling better planning. However, large-scale communication disruptions threaten resilience, necessitating robust UTM data link systems. UAVs and high-capacity data links can revolutionize wildfire response, but their effectiveness relies on a stable communication infrastructure.

- **Optimizing investments in forest fire mitigation:**

  Fire mitigation faces challenges such as capacity constraints, lack of collaboration, social support, and procedural delays. Yung et al. (2022) identifies three approaches to address these barriers:

  1. Increasing resources, simplifying procedures, limiting litigation, and public education.
  2. Organisational changes and capacity building for interagency collaboration.
  3. Public engagement to develop mitigation priorities.

  Investing in interagency capacity and public engagement can expedite fire mitigation, revealing more solutions to overcome key barriers.

- **Improved early warning and detection systems:**

  Early wildfire detection is crucial for minimizing impact and costs. Sensors and satellite tools (e.g., EFFIS, FIRMS) monitor variables like smoke, heat, and infrared radiation. These platforms

provide real-time data and historical fire regimes, aiding in understanding regions' susceptibility to future fires.

- **Optimization of fire-fighting resource deployment considering regional topography:** Sakellariou et al. (2023) emphasizes spatial fire resilience and adaptation strategies, highlighting topography's role in initial attack effectiveness. Ignoring topography allows faster vehicle movement and efficient coverage with fewer vehicles. However, integrating realistic topography reveals slower vehicle response times, necessitating more resources for effective coverage. This methodology offers flexible, optimized solutions for decision-makers, stressing the importance of geographical factors in emergency planning.

	Variables	Classes	Values	Relating Classes
Topography	Elevation (m)	>800	1	Very Low
		600-800	2	Low
		400-600	3	Moderate
		200-400	4	High
		≤200	5	Very High
	Aspect	South	5	Very High
		West	3	Moderate
		East	3	Moderate
		North	1	Very Low
		Flat	1	Very Low
		Northeast	2	Low
		Northwest	2	Low
		Southeast	4	High
		Southwest	5	Very High
	Slope (°)	>35	5	Very High
		25-35	4	High
		15-25	3	Moderate
		5-15	2	Low
		≤5	1	Very Low
Vegetation	NDVI	>0.67	1	Very Low
		0.54-0.67	2	Low
		0.40-0.54	3	Moderate
		0.27-0.40	4	High
		≤0.27	5	Very High
	Fuel type model	Fuel model 1	3	Moderate
		Fuel model 2	1	Very Low
		Fuel model 3	4	High
		Fuel model 4	5	Very High
		Fuel model 5	3	Moderate
		Fuel model 6	4	High
		Fuel model 7	5	Very High

Meteorological	Fire Weather Index	>28	5	Very High
		23-28	4	High
		13-23	3	Moderate
		3-13	2	Low
		≤3	1	Very Low
	Road distance (m)	>1200	1	Very Low
		1200	2	Low
Anthropogenic Issues		900	3	Moderate
		600	4	High
		300	5	Very High
	Settlement distance (m)	>2000	1	Very Low
		2000	2	Low
		1500	3	Moderate
		1000	4	High
		500	5	Very High
Historical Fires	Fire regimes	Fire regime 1	1	Very Low
		Fire regime 2	2	Low
		Fire regime 3	3	Moderate
		Fire regime 4	4	High
		Fire regime 5	5	Very high

Table 8: Values and relating classes assigned to variables of forest fire risk map.

The following Table 9 summarizes the handling strategies proposed in this section:

Reference	Resilience component	Strategies
(Martínez-Sánchez et al., 1999; Moya et al., 2011; Novo et al., 2020)	Preparedness, Adaptative Capacity	Forest Planning, Restoration, and Stand Improvement through Forest Management: • GIS (Geographic Information Systems) based forest planning. • Restoration of Degraded Forest Ecosystems. • Stand Improvement through Precision Silviculture. • Creation of Ecological Corridors. • Species Reintroduction Programmes.
(Arango et al., 2024; Arango, Nogal, Jiménez, et al., 2023)	All	Preparedness for road interventions: • Intelligent Traffic Management Systems. • Planning and Simulations of Road Interventions. • Identify critical points and potential bottlenecks that could arise during interventions. • Effective Coordination and Communication with Stakeholders. • Design and Construction of Resilient Roads. • Plan and build back-up infrastructure, such as alternative routes, to maintain traffic flow during a disruption.

(Andrade Sequoia R., 2023)	Robustness, Recovery Capacity	Improvement in the effectiveness of the initial attack by extinguishing teams: • Advanced Training and Drills for Response Teams. • Enhanced Communications Technology (UAS). • Collaboration with Local Teams and Volunteers.
(Laurie Yung, 2022)	All	Optimizing investments in forest fire mitigation: • Increasing resources, simplifying procedures, limiting litigation, and public education. • Organisational changes and capacity building for interagency collaboration. • Public engagement to develop mitigation priorities.
(EFFIS, 1998; NASA, 2012)	Preparedness	Improved early warning and detection systems: • Use of Drone Technology for Fire Detection. • Use thermal sensors and satellite tools to identify anomalous temperature rises and cameras to confirm the presence of fire. • Collect real-time data and analyse it to identify patterns that precede a fire. • Set up automatic alerts that are triggered when data indicates critical conditions, enabling rapid response.
(Sakellariou et al., 2023)	Preparedness	Optimization of fire-fighting resource deployment considering regional topography: • Integrate elevation and vegetation data into a GIS. • Develop a model that simulates fire spread considering topography. • Analyse access routes and available water points using GIS. • Plan strategic locations of fire stations, brigades and deployment routes based on topography. • Optimise routes to minimise total distance travelled and therefore fuel and time costs.

Table 9: Handling (mitigation and adaptation) strategies in the literature.

Information supported resilience management of traffic network

Remote sensing and satellite monitoring have become essential tools for disruption management and logistics chain optimisation. These technologies provide real-time data that are key to decision-making in adverse situations, enabling rapid detection of problems, facilitating damage assessment, identifying alternative routes and helping to implement measures to mitigate the impact of these disruptions. Critical infrastructures such as roads, railways and bridges are essential for economic development and mobility, which makes it imperative to ensure their resilience to natural disasters and unforeseen events. Earth observations play a crucial role in this context: from environmental monitoring to disaster management, the benefits are enormous (Spatineo Inc., 2024).

The Copernicus program, developed by the European Union and the European Space Agency (ESA), plays a pivotal role in providing Earth observation data through a fleet of satellites known as Sentinel. These missions deliver essential information for a wide range of applications, from environmental monitoring to disaster response (Copernicus, 2024). For example, Sentinel-1, with its Synthetic Aperture Radar (SAR), has been instrumental in enhancing road infrastructure safety in Italy by providing data on ground movements that affect critical infrastructure. The ground motion service,

supported by Sentinel-1, allows authorities to detect subtle shifts in infrastructure such as roads and bridges, enabling early interventions and reducing risks of failure due to structural weaknesses or natural hazards. This service ensures continuous monitoring of infrastructure in real-time, improving long-term safety and planning efforts (ESA, 2023).

Sentinel-2 provides high-resolution optical imagery, useful for monitoring land use, vegetation, and post-disaster landscapes, and is also critical for tracking wildfires. The Copernicus Climate Change Service (C3S) and Sentinel-2 play a vital role in wildfire monitoring, helping to track both fire intensity and burned areas. These satellites, combined with Fire Radiative Power (FRP) measurements, enable authorities to assess fire intensity in real-time. Additionally, this data is used to estimate carbon emissions and the scale of smoke plumes, contributing to understanding wildfire impacts on air quality and climate. This type of satellite monitoring is crucial for effective disaster management and resource allocation during wildfire events (ECMWF, 2024).

Sentinel-3 focuses on ocean and land monitoring, aiding in the assessment of water levels and temperature fluctuations, crucial for logistics and disaster preparedness. Sentinel-5P and Sentinel-6 further extend the program's capabilities by monitoring atmospheric pollution and sea level rise, respectively. Together, the Copernicus program and Sentinel missions offer vital geospatial information for efficient crisis management and the sustainability of logistics networks (Copernicus, 2024).

Maps, geospatial information, and thematic analysis derived from satellite imagery support decision-making and situational awareness throughout the disaster and crisis cycle, which includes preparedness, alertness, rapid analysis, response, recovery, and reconstruction. Fast delivery of accurate and comprehensive image-analysis products is essential, particularly during the analysis, response, and recovery phases, as they significantly aid in assessing large disaster situations, especially in remote areas where traditional assessment methods may fail.

The analysis of satellite images relies on rapidly available geoinformation and various techniques based on the type of disaster. Expertise in data sources such as Very High Resolution (VHR) optical data, thermal imagery, and Synthetic Aperture Radar (SAR) systems is crucial. Optical data are vital for planning relief efforts after events like earthquakes and tsunamis due to their intuitive interpretation. Thermal imagery is effective for detecting wildfires, with systems like MODIS being particularly useful for mapping fires and monitoring large-scale floods. SAR systems provide valuable mapping capabilities in adverse conditions, helping to assess floods, oil spills, and landslides, especially when comparing post-event images with reference data. Interferometrically derived digital elevation models are also critical for image processing and map generation (Voigt et al., 2007).

Through the integration of these technologies, decision-makers are equipped with the tools necessary to respond more effectively to crises, optimise logistics chains, and ensure the resilience of critical infrastructure, ultimately contributing to safer and more sustainable operations.

Impact of resilience management measures

Resilience management indicators provide a crucial framework for assessing regions' ability to withstand and recover from the impacts of wildfires. Meier et al. (2023) investigate the economic impact of wildfires in Southern Europe using detailed data on burned areas and economic variables for the period 2011-2018. An instrumental variables (IV) strategy is employed to address potential endogeneity of wildfires, using wildfire occurrence probability as an instrument based on relevant

climatic features. Additionally, it controls for fire risk indices and specific climate conditions that could directly affect regional economies.

The results show that wildfires have a significant negative impact on regional gross domestic product (GDP) growth, with estimated reductions ranging from 0.11% to 0.18% depending on whether fire numbers or burned area is used as a measure. In years with more severe wildfires, this reduction can be much more pronounced, reaching between 3.3% and 4.8%.

Regarding employment impact, heterogeneous effects are observed across economic sectors. Sectors such as wholesale and retail trade, transportation, accommodation, and food services experience a decrease in employment growth due to wildfires. In contrast, sectors like financial activities, insurance, real estate, and support activities experience an increase in employment growth, possibly due to risk management activities and real estate services.

To validate the robustness of the results, Fisher's randomisation tests are conducted (Fisher, 1937), and the sensitivity of spatial standard errors to different distance thresholds is evaluated. The results of these tests reinforce the statistical significance of the observed effects and the validity of assumptions regarding spatial effects of wildfires. Meier et al. (2023) provide substantial evidence that wildfires have significant and negative economic impacts on GDP and employment growth in Southern Europe (see Table 10). These findings underscore the critical importance of implementing effective wildfire management and prevention strategies to mitigate adverse impacts on regional economies.

Additionally, it is highlighted the need for adaptive public policies that consider both environmental risks and economic benefits in fire-prone regions, aiming towards more effective and sustainable management of these natural events in the context of global climate change.

Other indicators related to road networks and the impact on their use when affected by wildfires have been defined in sections 3.3.2 and 3.3.3 where the definitions of safety, connectivity, reliability and efficiency indices were proposed. Arango et al. (2023) propose the following guide (see Table 10) to help stakeholders define the level of importance of each KPI, as the more important it is, the stricter the threshold of the KPI applied to a road network or set of road networks. These KPIs can assume values between 0 and 1.

The following Table 10 summarizes the indicators proposed in this section:

Ref.	Management indicators	Description	Associated Resilience Components
(Sarah Meier, 2023)	$Y_{it} = \beta_0 + \beta_1 \cdot FIRE_{it} + \beta_2 \cdot BA_{it} + X_{it} \cdot \gamma + \epsilon_{it}$	Y_{it}: represents the GPD or employment growth in region I in year t. $FIRE_{it}$: is the number of wildfires in year t in region i. BA_{it}: is the burned area as a proportion of total area in year t in region i. X_{it}: is a vector of control variables including fire risk indices and climate conditions. $\beta_0, \beta_1, \beta_2$: are the coefficients of interest capturing the effects of wildfires on economic growth. ϵ_{it}: is the error term.	Robustness
	Safety (see 0, eq. 3 & eq. 4)	• 1: Ensures that all routes are out of fire range • 0.99-0.01: It is requested to maintain only a % of safe roads. This is recommended if other means of evacuation are available	Robustness

		• 0: No road is safe from wildfires.	
	Connectivity (see 370, eq. 5 & eq. 6)	• 1: Guarantees all routes are active, i.e., no OD pair of the network is disconnected • 0.99-0.01: Only a % of active routes are required, but disconnected OD pairs are not accepted. • 0: One or more OD pair is disconnected.	Robustness
	Reliability (see 0, eq. 9 & eq. 10)	• 1: Trips between all ODs are 100% reliable in terms of travel time. • 0.99-0.01: A % of travel-time reliability must be maintained, even if there are some delays. • 0: One or more ODs are not reliable at all in terms of travel time because they have been disconnected.	Recovery capacity
	Efficiency (see 0, eq. 7 & eq. 8)	• 1: All routes in the network transport are used in a fully efficient manner. • 0.99-0.01: A % of efficiency must be guaranteed. • 0: No road is safe from wildfires.	Robustness

Table 10: A summary of resilience management indicators.

3.3 Roles 2 and 3: Configuring and Managing Transport and Logistics Networks

3.3.1 Resilience Modelling

Recent global events, such as the COVID-19 pandemic and the Russo-Ukrainian war, impacted and continue to impact many aspects of daily life, scientific research, and business. Their course and effects have led scientists and logisticians from around the world to once again prioritize supply chain management. The concept of the supply chain is understood very heterogeneously in the literature. Different researchers emphasize different aspects of this phenomenon, often not limited to logistical concepts. The experience of recent events has questioned the previous hierarchy of features of a well-managed supply chain. In particular, there has been an increasing emphasis on the concept of resilience. Focusing on resilience has led researchers to expand its definitions. Riberio & Barbosa–Povoa (2018) emphasize critical aspects for a resilient logistics network. These encompass more than just responding to an event; they underscore the importance of adapting to it to restore the network to its pre-disruptive state or achieve a new equilibrium. The time taken to respond to and overcome disruptive elements is crucial, with a primary objective of minimizing the impact on network performance. Additionally, a variety of terms such as incident, disturbance, unexpected event, risk event, or disruption are used interchangeably. Moreover, resilience is a concept applicable across various stages, including strategic, tactical, and operational levels.

The literature presents and describes many ways to effectively and sensibly manage the supply chain. An approach to measuring, evaluating, and modelling resilience was presented by Pettit et al. (2010). They developed a tool for assessing supply chain resilience called “Supply Chain Resilience And Management”. This tool is based on two dimensions (Figure 11):

1. Supply chain vulnerability points - "fundamental factors that make the supply chain susceptible to disruptions"; based on expert research, the authors of the method identified seven vulnerability points:
    - Environmental variability (turbulence) - Degree of exposure to frequent changes in external factors

- Intentional threats - Intentional attacks aimed at disrupting operations or causing human, material, and financial harm
- External pressure - Occurrence of external tensions causing business barriers
- Resource constraints - Constraints arising from the lack of resource availability for production and distribution
- Process sensitivity - Importance of product and process integrity conditions
- Dependency on partners - Degree of dependence on external partners
- Disruptions from suppliers/customers - Vulnerability of suppliers and customers to external forces or disruptions

2. Supply chain capabilities - defined as "attributes that enable the supply chain to anticipate and counter disruptions". Based on expert research, the authors of the method identified fourteen supply chain capabilities:
   - Supply flexibility - Ability to quickly change supply sources
   - Order fulfilment flexibility - Ability to quickly change transportation means or other factors related to order fulfilment
   - Availability of production resources - Availability of resources to maintain a steady production level
   - Efficiency - Ability to produce with minimal required resources
   - Visibility - Awareness of the status of operational assets and environment
   - Adaptability - Ability to modify operations in response to threats and opportunities
   - Prediction - Ability to foresee potential future events or situations
   - Renewability - Ability to quickly return to a normal state after a disruption occurs
   - Dispersion - Wide distribution or decentralisation of assets
   - Collaboration - Ability to effectively work with external entities for mutual benefits
   - Organisation - Organisational structures, policies, skills, organisational culture
   - Market position - Company status in the market
   - Security - Defense against intrusions, thefts, attacks
   - Financial position - Ability to absorb fluctuations in cash flows

According to Pettit et al. (2010), individual elements of both dimensions are assessed on a scale from 1 to 5 using a survey study in which respondents answer several questions within each of the considered supply chain vulnerability points or capabilities. The respondents' answers are reflected in the scoring of individual vulnerability or capability elements. In the simplest variant of the discussed tool, the overall vulnerability score of the supply chain is the arithmetic mean of the scores of individual vulnerability points, while the overall supply chain capability score (for anticipating and countering disruptions) is the arithmetic mean of the scores of individual capabilities.

As the main basis for the described tool, three propositions/statements were considered (Figure 11):

- Proposition 1 – Excessive sensitivity of the supply chain relative to its capacity results in an increase in exposure to risk.
- Proposition 2 – Excessive increase in the assessment of the supply chain's capacity relative to its sensitivity results in a decline in profitability (excessively high costs) of the undertaken venture.
- Proposition 3 – The operation of the supply chain is more efficient when its capacities and sensitivity points are balanced.

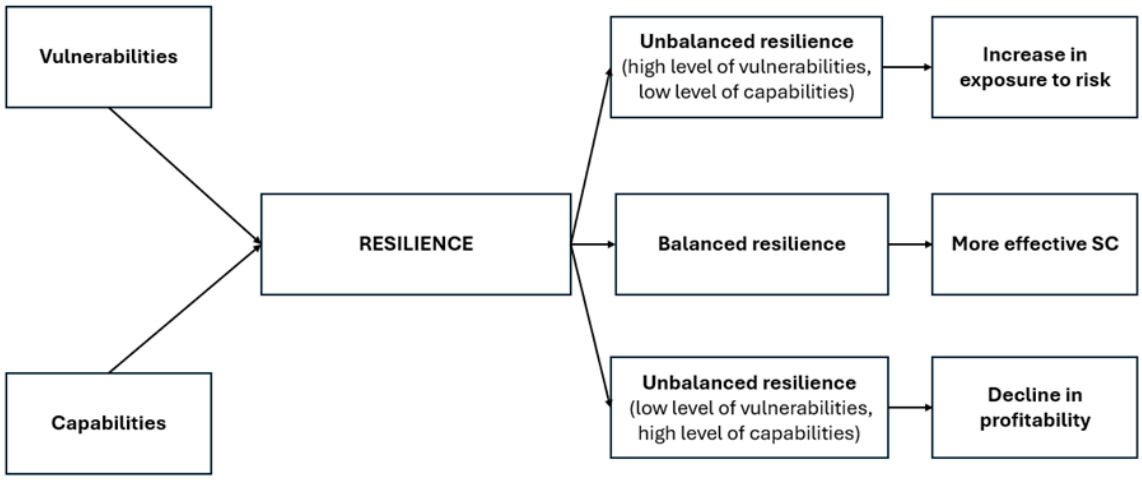

Figure 11: The dimensions of SCRAM methodology and the three main propositions.

However, the SCRAM methodology presents shortcomings. Its enhancement was aimed at by Lenort & Wicher (2013), who utilized a multicriteria method of hierarchical analysis of decision problems. Their developed supply chain resilience evaluation system is based on the decomposition of capabilities that influence resilience into a set of measurable KPIs. These indicators can have a qualitative nature. Each KPI is assigned appropriate weights that reflect its significance. The specific resilience KPIs and their weights (importance) were presented using the AHP method. It allows the decomposition of the decision problem into a hierarchical system of weighted goals, criteria, and measurable indicators. The proposed procedure consists of five steps:

1. Establishing the structure of the decision problem - The structure of the decision problem considers its hierarchy. The example presented in Figure 12 assumes a structure consisting of three levels, namely goal, criteria and KPIs.

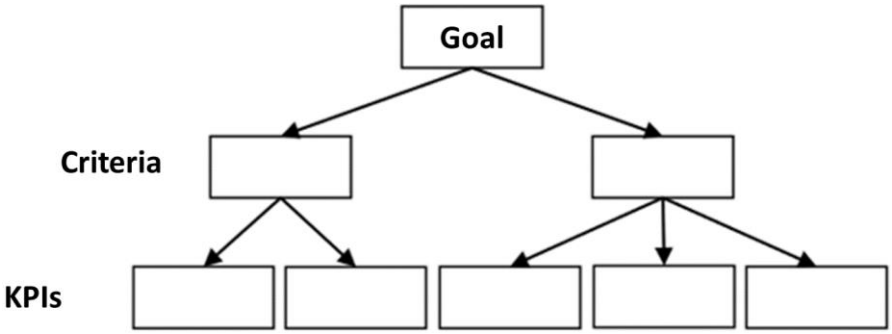

Figure 12: The structure with the hierarchical approach.

2. Construction of a set of pairwise comparison matrices - Each element in an upper level is used to compare the elements in the level immediately below. For three level hierarchy from Figure 12, it is necessary to create one matrix for criteria comparison from the viewpoint of the objective and two matrices for comparison of KPIs from the viewpoint of the criteria. Lenort & Wicher (2013) recommended using a nine-point scale to assess the significance of individual parameters, where 1 indicates negligible importance, and 9 indicates critical importance. Assuming *N* elements, pairwise comparison of element *i* with element *j* yields a square matrix *A* (of dimensions NxN), where a_{ij} denotes the "comparative" significance of element i relative to element j. In the matrix, a_{ij} equals 1 when $i = j$. Additionally, $a_{ij} = 1/a_{ji}$.

3. Determination of the relative normalized weight w_i of each element - This stage involves determining weights by calculating geometric means i and this row according to the formula:

$$w_i = \frac{\left[\prod_{j=1}^{N} aji\right]^{\frac{1}{N}}}{\sum_{i=1}^{N}\left[\prod_{j=1}^{N} aji\right]^{\frac{1}{N}}} \quad \text{(Eq. 25)}$$

4. Checking the consistency of the matrix - At this stage, the Consistency Ratio (CR) is calculated:

$$CR = \frac{CI}{RI} \quad \text{(Eq. 2}$$

CI is the consistency index, while RI is a random consistency index dependent on N (Table 11). The matrix is considered consistent when *CR* ≤ 0.1.

N	1	2	3	4	5	6	7	8	9	10
RI	0	0	0,52	0,89	1,11	1,25	1,35	1,4	1,45	1,49

Table 11: Random consistency index.

The consistency index is calculated according to the formula:

$$CI = \frac{\lambda_{max} - N}{N - 1} \quad \text{(Eq. 27)}$$

Where:

$$\lambda_{max} = \frac{1}{N}\sum_{i=1}^{N} \frac{A \cdot W}{w_i} \quad \text{(Eq. 28)}$$

A - pairwise comparison matrix,

W - normalized weight vector.

5. Calculating the global weights of all elements - The weights acquired so far from the individual pairwise comparison matrices are local ones. Global weights, which guarantee that the sum of weights at all levels will equal one, are determined using the formula:

$$gw_{ij} = w_i \cdot w_{ij} \quad \text{(Eq. 29)}$$

where gw_{ij} is the global weight of the j_{th} element of the i_{th} group; w_i is the local weight of the i_{th} group; and w_{ij} is local weight of the j_{th} element of the i_{th} group.

In the following sub-sections, different KPIs are proposed to assess each component of resilience. More information about the selected KPIs and their representative resilience factors and sub-factors can be found in deliverable D1.2.

Preparedness

In the Preparedness Phase of Supply Chain Resilience (SCR), various resilience factors and their representative KPIs are critical for ensuring that a supply chain can anticipate and respond to potential disruptions. This resilience components focuses on the proactive measures that organisations must take to safeguard their operations. Several methodologies, including Badhotiya's (2022) ISM-BN approach, SCRAM, and AHP, provide a framework to evaluate and enhance these KPIs.

- **Crisis Management Preparedness**: KPIs such as crisis management training sessions and emergency response training coverage (percentage of trained employees) assess the readiness of an organisation to handle disruptions. These can be evaluated using the AHP model to prioritize areas for improvement based on the relative importance of each KPI.

- **Information Quality**: it is measured as the "percentage of actual data with respect to all available data." This measures the reliability and accuracy of the information used in operations, ensuring that decision-making is based on real-time and accurate inputs. Key KPIs related to information quality include the percentage of first-hand data collected or forecast accuracy.
- **Situational Awareness**: Assessed using SCRAM, situational awareness involves the ability to predict and recognize vulnerabilities, improving visibility across the supply chain. Key KPIs include forecast accuracy and vulnerability assessment scores, which help identify gaps in preparedness.

Robustness

Robustness refers to the system's ability to absorb shocks without a significant loss of performance. It ensures that key operations can continue despite disruptions.

- **Reliability of activities**: it can be evaluated through two key performance indicators (KPIs): Shipping Accuracy, which measures the percentage of SKUs shipped without errors, ensuring the accuracy of product deliveries. Additionally, On-Time Delivery assesses the proportion of goods delivered to customers on schedule and in full, reflecting the organisation's ability to meet delivery commitments reliably.
- **Financial strength:** financial stability and its capacity to endure operational challenges, highlighting its ability to leverage resources effectively. The KPI of debt-to-equity ratio measures the proportion of a company’s financing that comes from debt relative to equity. Also, working capital ratio assesses the company’s ability to cover short-term obligations with its short-term assets.
- **Operational reliability**: A reflection of operational robustness, the KPI of customer retention index monitors the percentage of customers retained during disruptions, providing insights into the system’s capacity to meet demand despite challenges.

Incorporating the ISM-BN framework, robustness is connected to other KPIs, such as market position and financial stability, which collectively strengthen the system’s ability to absorb disturbances.

Recovery capacity

The Recovery Capacity corresponds to the ability of the supply chain to restore normal operations after a disruption. This phase emphasizes rapid recovery and minimizing downtime.

- **Recovery Time**: This KPI measures the time required to return to full operational capacity after an event, critical for minimizing downtime.
- **Rapidity**: The average rate of recovery, calculated as the percentage of performance restored per time unit. This is a critical metric in ISM-BN, where it helps model the interaction between other resilience factors, such as resource mobilization and recovery strategy efficiency.
- **Resource Mobilization**: The KPI of resource mobilisation efficiency evaluates how efficiently resources are deployed during recovery efforts, tracking the percentage of resources mobilized compared to what is needed. SCRAM helps assess this KPI by linking recovery efforts to real-time decision-making and resource availability.
- **Reserve capacity**: The reserved capacity or redundancy of a supply chain can be described by KPIs, such as inventory to sales ratio or backup storage ration. ISM-BN models reserve capacity

as a backup strategy that supports recovery by enabling alternative routes or suppliers, reducing reliance on any single point of failure.

Resilience components	KPIs	Modelling method
Preparedness	Crisis management training sessions	SCRAM, AHP or ISM-BN
	Emergency response training coverage	
	Percentage of first-hand data collected	
	Forecast accuracy	
Robustness	Reliability of activities	
	Customer retention index	
	Debt-to-equity ratio	
	Working capital ratio	
Recovery capacity	Recovery time	
	Rapidity	
	Resource Mobilization	
	Reserve capacity	
Adaptive capacity	Organisational Flexibility	
	Knowledge Management	
	Collaboration and Integration	
	Learning from Experience	

Table 12: Resilience modelling methods, describing various RFs and KPIs for global hazards, are clustered based on the four different components of resilience.

Adaptive capacity

Adaptive capacity reflects the system's ability to evolve and improve based on past disruptions:

- **Organisational Flexibility**: This KPI evaluates how well an organisation adapts its operations in response to challenges. Measured by the percentage of process changes implemented post-disruption, it is central to ISM-BN modelling, where flexibility drives long-term adaptation and resilience.
- **Knowledge Management**: A KPI that tracks the level of information sharing and lessons learned from past disruptions. This factor is central to enhancing future recovery efforts and forms part of adaptive learning.
- **Collaboration and Integration**: This KPI tracks the degree of coordination between supply chain partners, critical for ensuring adaptive capacity. SCRAM highlights the role of collaboration in enhancing resilience through shared resources and knowledge.
- **Learning from Experience**: Measured by the number of implemented lessons from past disruptions, this KPI evaluates how well an organisation adapts its strategy based on previous events. ISM-BN incorporates learning as a factor that enhances both adaptive and recovery capacities, helping organisations evolve post-disruption.

Table 12 shows the KPIs and models presented in the section associated with each phase of the resilience curve and associated with the Resilience Factors defined in SARIL project.

3.3.2 Resilience management

Handling (mitigation and adaptation) strategies

To effectively manage risks and their potential consequences, supply chains implement a range of risk mitigation strategies. These strategies are aimed at identifying, assessing, and managing risks in a coordinated manner among supply chain members to reduce the overall vulnerability of the supply chain. The ultimate goal is to ensure that the supply chain can quickly return to its pre-disruption state in the most efficient and cost-effective way possible.

1. Overview of Risk Mitigation Strategies

Risk mitigation strategies in supply chains are diverse and depend on the specific nature of the risk being addressed. These strategies can be broadly categorized into two types: preventive and reactive. Preventive strategies are proactive measures taken to avoid risks before they occur, while reactive strategies are implemented in response to a disruption to minimize its impact and facilitate recovery.

2. Preventive Risk Mitigation Strategies

Strategic Stock or Safety Stock:

One of the most commonly used preventive measures is the maintenance of strategic stock, also known as safety stock. This involves holding additional inventory in strategic locations, close to production facilities or distribution centres. By doing so, companies can buffer against supply chain disruptions and ensure that production can continue even if there are delays or shortages in the supply of raw materials or components. However, maintaining safety stock involves a trade-off, as it increases holding costs (ASCM, 2020).

Multiple Sourcing:

Another key preventive strategy is multiple sourcing, where a company sources its materials or components from several suppliers rather than relying on a single one. This diversification spreads the risk and improves service reliability (Min et al., 2019). However, this approach can lead to higher costs, as economies of scale might be lost when orders are split among multiple suppliers (Chopra & Sodhi, 2004).

Facility or Supplier Dispersion:

Geographical dispersion of facilities or suppliers is another effective preventive measure. By spreading operations across different regions, companies can reduce the risk of localized disruptions. For instance, if a natural disaster or political unrest affects one region, the company can continue its operations from other locations. However, this strategy requires significant investment in infrastructure and management across multiple sites (Pettit et al., 2010).

Flexible Transportation:

Incorporating flexible transportation options, such as multi-modal or multi-carrier systems, enhances a supply chain's resilience. This flexibility allows companies to switch transportation modes or carriers quickly if their primary logistics routes are disrupted. For example, if a particular shipping route

becomes inaccessible due to port congestion or natural disasters, the company can reroute shipments via alternative modes like air or rail transport (Ivanov & Dolgui, 2021).

Postponement:
The postponement strategy involves delaying the final customization or differentiation of products until closer to the point of sale. By standardizing production and holding off on specific customizations, companies can better manage demand uncertainty and respond more flexibly to changes in market conditions. This strategy is particularly useful in industries where demand is highly volatile (Pettit et al., 2010).

3. Reactive Risk Mitigation Strategies

Back-up Suppliers:

In the event of a disruption affecting the primary supplier, having back-up suppliers ready to step in can ensure continuity of supply. This strategy is crucial when dealing with critical components or materials that have few available substitutes (Min et al., 2019).

Rerouting:

When the main transportation route is disrupted—due to issues like traffic congestion, road closures, or port inefficiencies—rerouting shipments via alternative paths is a key reactive strategy. This requires a well-established logistics network that can quickly adapt to changing conditions (Ivanov & Dolgui, 2021).

Make and Buy Strategy:

Some companies adopt a hybrid approach of producing some components in-house (make) while outsourcing others (buy). This provides flexibility in scaling production and adjusting to supply chain disruptions. For instance, if an outsourced component becomes unavailable, the company might be able to increase in-house production temporarily to compensate (Chopra & Sodhi, 2004).

Revenue Management (Dynamic Pricing and Promotion):

Dynamic pricing, where the price of a product is adjusted in real-time based on supply and demand conditions, can be an effective way to manage the impact of disruptions. By raising prices during periods of scarcity or lowering them to clear excess inventory, companies can better control demand and supply alignment (Pettit et al., 2010).

Substitution:

In cases where specific raw materials become scarce or expensive, companies might opt to substitute them with similar alternatives until the situation normalizes. This requires flexibility in product design and production processes to accommodate different materials without compromising on quality (Pettit et al., 2010).

Assortment Planning:

Assortment planning involves strategically arranging products on store shelves to influence consumer purchasing decisions. During disruptions, this can be used to guide customers towards products that are more readily available, thereby managing demand for items that are in short supply (Ivanov & Dolgui, 2021).

4. Challenges in Implementing Risk Mitigation Strategies

While these strategies are essential for safeguarding supply chains, their implementation is not without challenges. According to Tang (2006), there are three primary challenges:

Return on Investment (ROI):

Assessing the ROI of risk mitigation strategies is difficult because disruptions may never occur. Companies must balance the costs of preparing for unlikely events against the potential losses if those events do happen.

Alignment with Corporate Strategy:

Risk mitigation strategies may conflict with a company's broader corporate strategy. For example, a company focused on cost reduction through supplier consolidation might find that it needs to diversify suppliers to enhance resilience, which could increase costs.

Strategy Suitability:

Not all strategies are suitable for every type of risk. A strategy that is effective for one type of disruption might be ineffective or even detrimental in another scenario. For instance, multiple sourcing might not protect against global disruptions like pandemics. Therefore, companies need to develop a portfolio of strategies that can address a wide range of risks.

In conclusion, while supply chain risk mitigation strategies are critical for managing disruptions, their successful implementation requires careful consideration of costs, alignment with overall business goals, and adaptability to different risk scenarios.

Information supported resilience management of logistic networks

Information plays a significant role in building the resilience of a logistics network. It helps logistics operators respond to supply chain disruptions and better manage risks. Additionally, it directly influences the decision-making process at various levels, including real-time decision-making, predictive analytics, and scenario modelling.

Real-time data provides information on the status of resources, enabling managers to make faster and more accurate decisions. With GPS vehicle tracking, companies can monitor transport routes and respond to delays caused by accidents or damage to logistics infrastructure. Moreover, thanks to sensor systems, operators can monitor the condition of transported goods, preventing product loss, which is particularly effective in the transportation of food or temperature-sensitive products (Juan et al., 2022).

In the context of decision-making, easy access to real-time data allows for rescheduling deliveries, changing routes, and improving resource management. This minimizes the risk of disruptions and enhances the smoothness of operations. Importantly, early warning of potential problems enables proactive measures, resulting in increased logistics network resilience (Hasan et al., 2024).

Another application of information in building resilience is its use in predictive analytics. Collecting and analysing historical data allows for the prediction of potential threats and disruptions in the future. Seasonal changes in demand may lead to stockpiling during key periods or relocating resources to areas with higher demand. Analysing past supply chain interruptions can help identify bottlenecks that may cause disruptions in the future.

Impact of resilience management measures for logistic networks

There is a wide range of methods and approaches in the literature for defining indicators of the impact of the disruption in supply chain resilience management. While some are quite similar to one another, others focus on distinct and divergent concepts. Regarding transportation, a notable modification to the model previously presented by Anand & Grover (2015) was introduced by Korneta et al. (2018). The modification primarily involved reducing the four critical areas to three by merging the resource management area with the inventory management area. This consolidation is justified not only by the simplification it offers but also by the fact that these areas are subject to very similar measurements. The structure of the model developed by Anand & Grover (2015) has been supplemented with other indicators and measures presented in the literature. The conceptual framework of this model is illustrated in Figure 13. It proposes the division of each of the three critical areas into four sub-areas, each associated with specific KPIs.

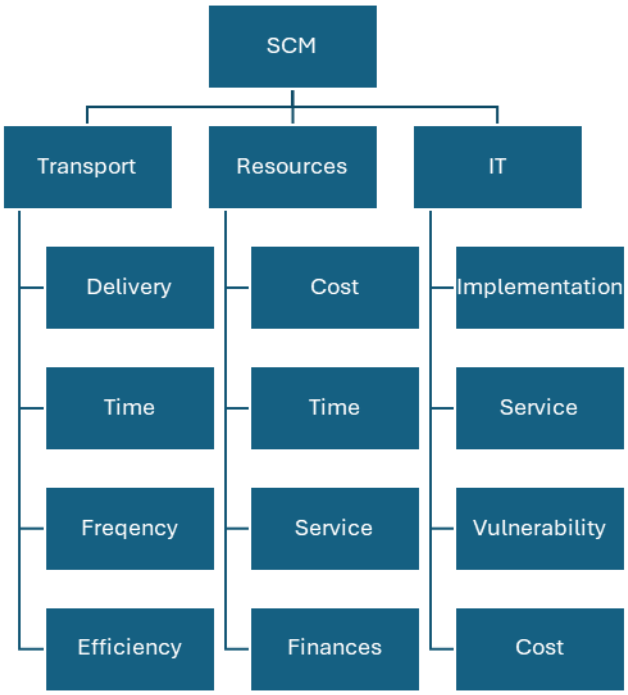

Figure 13 The conceptual framework of the modified supply chain performance model by Anand & Grover (2015).

The first critical area is transport optimization, which consists of four sub-areas: delivery, time, frequency, and efficiency. Measuring performance in the delivery domain can be supported by indicators such as:

- % on-time deliveries,
- delivery flexibility,
- erroneous deliveries,
- number of complaints as a % of total orders or sales,
- quality of transport documentation,
- temperature control during transport.

Time-related metrics include loading and unloading times, order preparation time, and the value of products expired due to transport delays.

For the frequency domain, suggested indicators include the number of road accidents and the daily number of routes.

Efficiency can be measured by:

- the amount of cargo transported over a given period,
- the efficiency of contracted subcontractors,
- the number of contracted or owned fleet vehicles,
- fuel consumption (in litres) per kilometre or ton.

The second critical area of the analysed model concerns resource optimisation. Cost measurement can be achieved using indicators such as:

- inventory turnover period,
- inventory value,
- inventory value as a percentage of sales,
- negative inventory discrepancies,
- personnel costs,
- material costs,
- product costs,
- IT systems costs,
- packaging costs,
- production costs,
- complaint costs.

However, resource optimization in supply chain management can indeed go beyond cost metrics. While cost is a primary focus, other non-cost factors, such as sustainability, risk mitigation, and service level improvement, are often included. More information can be found in EMF (2020), Tang (2006) and Wamba & Akter (2019).

Time measurement can involve indicators such as inventory replenishment time, time required for onboarding new employees, or time allocated for exploring new solutions.

Service measurement can be based on indicators such as:

- number of warehouses,
- service flexibility,
- certifications held (e.g., ISO),
- types of warehouses,
- energy consumption per square meter,
- customer satisfaction,
- packaging quality.

Key financial indicators may include:

- accounts receivable period,
- inventory turnover period,
- debt ratios,
- ROCE (Return on Capital Employed),
- EVA (Economic Value Added),
- profitability ratios (sales, assets).

The final critical area of the model pertains to IT optimization, comprising the following four sub-areas:

- level of IT implementation (e.g., WMS implementation level, IT implementation for tracking deliveries, integration of multiple systems, EDI usage level),
- service (data quality, system flexibility, IT compliance with current standards),
- sensitivity (number of complaints per customer, number of complaints per week, information reliability, speed of access to information),
- costs (IT investments as a percentage of sales revenue, IT maintenance costs).

3.4 Resilience of the Information System

The information system includes information that can support resilience management and the channels and tools that enable the information flow within the system, and communication among the actors involved in the system management. Resilience management must envisage handling strategies to face disruptions to the information system, such as cyber-attacks. In the next sections, a review on resilience modelling and management of the information system is reported through the description of resilience indicators and of handling strategies.

3.4.1 Resilience Modelling

Resilience in the cyber domain, often defined as cyber resilience, is a well-defined area mostly considered in the context of cybersecurity as the ability of systems and organisations to anticipate, absorb, respond and recover from, as well as adapt to cyber incidents when they occur (Bodeau et al., 2018). Given the dimensions of the field, the literature associated with cyber resilience and its KPIs is vast, and it is common to find formal models of KPIs that are associated with knowledge of a specific infrastructure or organisation under analysis. One of the most robust tools for understanding and categorising cyber threats is the MITRE ATT&CK framework (MITRE, 2015), a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The MITRE organisation defines cyber resiliency KPIs as challenging due, amongst other things, to their context "Cyber resiliency, like mission assurance, is meaningful in the context of the mission" (Bodeau et al., 2018). A good portion of the literature focuses on defining and adapting models to specific system categories or types, such as critical infrastructure or cyber physical systems (Barbeau et al., 2021; Murino et al., 2019; Smith et al., 2022).

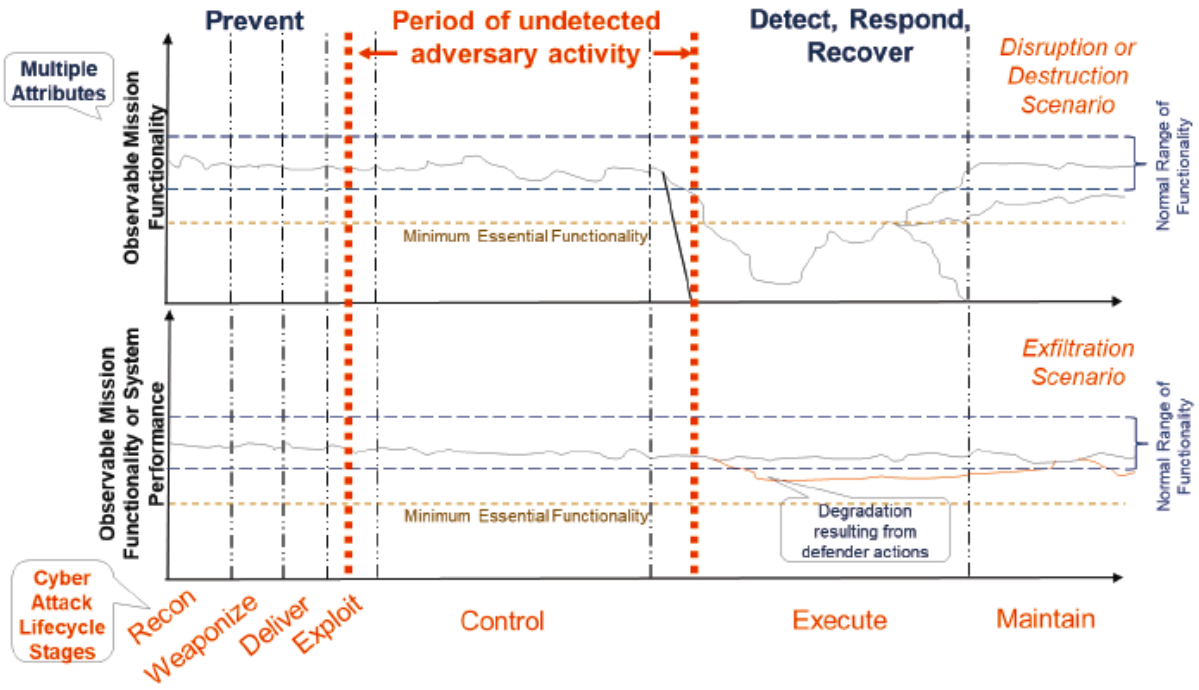

Figure 14: Cyber-attack lifecycle as presented in Bodeau et al. (2018)

Generally, a cyber-attack, or cyber incident, can be considered having a lifecycle composed of the phases presented in Figure 14, where in an initial stage the attackers are not necessarily executing their final disruptive goal but may manage to get access to the system (recon, weaponize, deliver, exploit, and control phases), in particular the control phase may or may not be present, depending on the attackers' objective. Next, the attackers execute the attack that degrades the performance of the system (execute phase), and potentially attempt to maintain control over the system (maintain phase).

It is possible to map such stages to the resilience phases of Figure 7. In the "before" phase, organisations implement preventive and detection measures to hinder attackers during reconnaissance and weaponisation and use threat modelling and risk analysis to understand potential vulnerabilities and attack paths to mitigate. In the "during" phase, systems are fortified to limit the impact of exploits, and monitoring mechanisms detect suspicious activities that could lead to attackers gaining control or executing malicious actions. In the "after" phase, restore processes, along with incident response plans, enable organisations to regain control and restore normal operations, even if attackers have executed their plans. Finally, the beyond phase involves continuously analysing incidents to improve defences against future exploits, and updating security protocols based on the latest threat intelligence to prevent attackers from maintaining control.

Preparedness

MITRE defines the 'anticipate' goal as "to maintain a state of informed preparedness in order to forestall compromises of mission/business functions from adversary attacks" (Bodeau et al., 2011; Bodeau & Graubart, 2017). The goal can be achieved through *predicting*, *preventing*, and *preparing* for attacks. To *predict* attacks, the organisation should focus on understanding whether there are attack groups, malwares, or other known threats that may aim at the organisation's assets. Commonly, this is achieved through obtaining and analysing threat intelligence. The best-case scenario for an organisation is to completely *prevent* an attack from being executed, through basic security hygiene (common security good practices, such as regular patching of systems, ensuring

strong password policies, etc…) and hardening of the organisation's attack surfaces (e.g., disabling unnecessary services and ports, implementing network segmentation, and applying the principle of least privilege). Finally, *preparing* means integrating in the organisation processes the so called cyber course of actions, or "a set of activities by cyber defenders [...] to confirmed, suspected, or predicted cyber-attacks." (Bodeau et al., 2011).

Threat Intelligence Coverage

An indicator of 'preparedness' with respect to cyber threats is the Threat intelligence coverage (TIC) which describes the collection, processing, and analysis of information about potential or current cyber threats. It provides insights into the tactics, techniques, and procedures (TTPs) used by adversaries, as well as their motivations and targets. TIC allows organisations to anticipate and prepare for potential attacks before they occur. By understanding the TTPs of threat actors, organisations can develop and implement mitigation strategies to protect against specific threats (Pascoe et al., 2024). TIC can be computed by Eq. 30 and describes the percentage of known threats for which mitigations are in place.

$$TIC = \left(\frac{NTM}{TNT}\right) \times 100 \quad \text{(Eq. 30)}$$

NTC is the number of threats with mitigations. This is the count of known threats for which the organisation has implemented preventive, detective, or corrective controls. TNT is the total number of known threats. This is the total number of threats that the organisation is aware of, based on its threat intelligence sources. To effectively measure the TIC, it is essential to have a comprehensive list of known threats that the organisation faces. There are several strategies and resources to achieve this. Beyond the MITRE, there are other more targeted but less accessible ways to obtain insights on the trends of cyber attackers and recognize vulnerabilities, such as using Threat Intelligence Platforms (TIPs), which aggregate data from various sources, providing comprehensive threat intelligence feeds that include information on vulnerabilities, exploits, and adversary behaviours, or conducting threat assessments and penetration testing to identify new threats and vulnerabilities specific to the organisation.

System Hardening Level

Vulnerabilities are weaknesses or flaws in a system that can be exploited by attackers to gain unauthorized access or cause harm. Removing vulnerabilities is crucial for several reasons. It prevents unauthorized access to systems and sensitive data, protects against malware, ensures compliance with regulatory standards, maintains system integrity, and improves system performance and stability. By addressing these weaknesses, organisations can prevent breaches, protect their information assets, and reduce the risk of security-related disruptions. Effective system hardening involves regularly applying patches and updates, properly configuring system settings, implementing strict access controls, and conducting regular security audits and assessments. The KPI that can be used for this phase is System Hardening Level (SHL), which provides the percentage of system vulnerabilities that have been addressed through patching or secure configuration (Eq. 31).

$$SHL\ (\%) = (NVA/TNV) \times 100\% \quad \text{(Eq. 31)}$$

NVA is the number of vulnerabilities addressed and represents the total count of system vulnerabilities that have been successfully mitigated. TNV is the total Number of Vulnerabilities and represents the sum of all identified vulnerabilities within a system. However, accurately determining this number requires vulnerability assessments, security scans, continuous security monitoring, and staying updated with the latest threat intelligence. Therefore, this KPI is only useful for organisations that have already implemented basic security analysis processes.

Robustness

In the "during" phase, the goal is to ensure the continuous performance of the organisation despite a successful execution of the attack. This implies mostly that there need to be predefined courses of action to ensure that operations continue, ideally in an alternative mode, or worst-case scenario in a degraded mode, but maintaining minimum performance.

Direct Static Economic Resilience

To assess the component of robustness, it is possible to use KPIs such as those mentioned in Section 3.1.2, specifically by Bruneau et al. (2003) and Bruneau & Reinhorn (2007). The KPI proposed by (Rose, 2007) (Figure 15) for economic resilience has been adopted and suggested for cyber resilience by Murino et al. (2019). This KPI accounts for the avoided drop in performance resulting from detection and response measures within the system. However, the context-dependent need arises to redefine KPIs initially considered economic in the original paper. In critical systems, where factors beyond economic impact are significant, a system-dependent redefinition of performance becomes essential, which can take into consideration not only the economic impact but also the effects of the attack on the targeted critical system functioning, such as the proportion of time the system has been operational over a specific period (uptime).

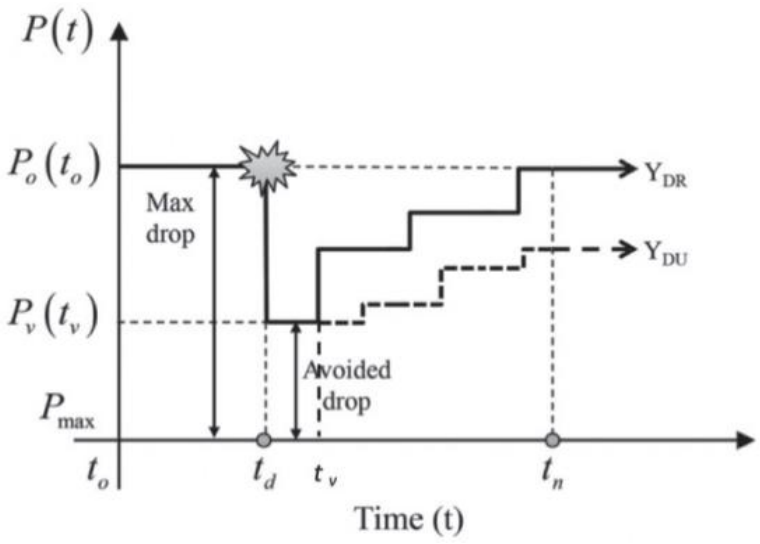

Figure 15: Formula for the estimation of resilience proposed by Rose (2007).

The KPI, ψ_c, which is given by Eq. 32, has the objective of representing the avoided loss of performances (or the robustness) due to detection and reaction measures, where $P_v(t_v)$ represents the minimum of the performances curve during the attack, $P_o(t_o)$ represents the performances (average) of the system previous to the attack, and P_{max} represents the estimated performance loss due to the attack if it was not detected or prevented by any measure. Therefore, it measures the ratio between avoided losses and the maximum potential losses.

$$\psi_c = \frac{Avoided\ drop}{Max\ drop} = \frac{P_v(t_v) - P_{max}}{P_o(t_o) - P_{max}} \quad \text{(Eq. 32)}$$

Recovery Capacity

The main scope of the "after" phase of cyber resilience is to restore mission or business functions to the maximum extent possible following a successful attack by an adversary. This phase in cyber resilience can be seen as partially overlapping with the "during" phase, particularly in the processes of detecting and reacting to a cyber-attack. These early detection and reaction steps are crucial not only for initiating defence mechanisms in the "during" phase but also for guiding the recovery process in the "after" phase. Timely identification of an attack is essential for both mitigating its impact and understanding its nature, which in turn informs the appropriate recovery actions. Therefore, while detection and reaction may be effective also in the "during" phase, for the sake of clarity, we will consider them as integral components of the "after" phase.

Mean Time To Detect (MTTD)

To assess the recovery capacity (neutralize and remove the attacker), security experts and organisations suggest to use a combination of two KPIs, the Mean Time To Detect (MTTD) and Mean Time To Respond (MTTR). For the MTTD, it holds that (Eq. 33):

$$MTTD = \frac{\sum_{i=1}^{N}(T_d - T_e)}{N} \quad \text{(Eq. 33)}$$

where T_d is the time of detection of a given attack or incident, T_e is the time of the actual event, either attack or incident, and N is the number of past cybersecurity incidents and attacks. MTTD measures the average time it takes to identify a cyber threat or security incident within a system. A shorter MTTD signifies a robust security posture and the ability to rapidly detect and successively respond to potential breaches, thereby minimizing the damage caused by cyberattacks.

Mean Time To Respond (MTTR)

To assess the effectiveness of the neutralisation and removal of a cyber threat or security incident, the Mean Time To Respond (MTTR) KPI is a valuable indicator, which is given by Eq. 34:

$$MTTR = \frac{\sum_{i=1}^{N}(T_r - T_d)}{N} \quad \text{(Eq. 34)}$$

where T_r is the time of recovery from a given attack or incident, T_d is the time of detection of a given attack or incident, and N is the number of past cybersecurity incidents and attacks. MTTR measures the average time it takes to control and mitigate a confirmed security incident from the moment it is detected. A shorter MTTR signifies a more agile and effective incident response capability, reducing the potential damage caused by the incident. While this KPI could be associated with both the "during" and "after" phases, it is often used to assess the efficiency of the recovery capacity ("after" phase).

Adaptive capacity

The main goal of the beyond phase of cyber resilience, also referred to as the "Evolve" phase in the MITRE framework, is to modify missions or business functions and/or their supporting cyber capabilities to minimise the adverse impacts of actual or predicted adversary attacks.

Key elements of the beyond phase include transforming existing processes and behaviours, as well as re-architecting systems and infrastructure. This process is driven by two main factors: the continuous evolution of the environment, including new technologies and emerging threat actors, and insights gained from post-incident analysis, which uncovers the origins, attack paths, and impacts of incidents.

The organisation's ability to adapt to the evolving environment can be evaluated as in the preparedness phase using KPIs such as threat intelligence coverage, provided that these KPIs are updated regularly. In this case, the increased percentage of known threats for which mitigations are in place can be estimated using Eq. 35, where TIC_a is the threat intelligence coverage after adaptation to the previous attack.

$$Inceased\ percentage = TIC_a - TIC \quad \text{(Eq. 35)}$$

The effectiveness of the post-incident process, the quality of the analysis, and the implementation of patches and countermeasures to prevent recurrence can be assessed using a combination of KPIs. Examples include "Length of time to determine the impact of a cyberattack on a mission" and "Elapsed time for system damage assessment" (from the MITRE cyber security metrics catalog). While neither KPI is formally defined in the literature, both can be measured as the time difference between the discovery of the attack and the conclusion of the assessment. Additionally, the completeness of the report should be considered, although there is no associated KPI in the literature, likely due to the subjective nature of defining a "complete" report. All the aforementioned KPIs and modelling methods for each resilience component are summarised in Table 13.

Resilience components	KPIs	Equations	Modelling method
Preparedness	Threat Intelligence Usage	15	• Threat Intelligence Coverage
	System Hardening against Vulnerabilities	16	• System Hardening Level
Robustness	Robustness	17	• Loss Function
Recovery capacity	Attack detection capability	18 & 19	• Mean time to detect • Mean time to respond
Adaptive capacity	Increased percentage of known threats for which mitigations are in place	20	• Threat Intelligence Coverage

Table 13: Resilience modelling methods, describing various KPIs for cyber-attacks, are clustered based on the four different components of resilience.

3.4.2 Resilience Management

Handling (mitigation and adaptation) strategies

Handling strategies for cyber resilience include continuous risk assessment and management, incident response planning, data backup and recovery processes, patch management, and continuous security awareness training for employees. Regular risk assessments and the implementation of risk mitigation strategies are crucial for identifying vulnerabilities and potential threats, not only in an initial stage but throughout the life of the organisation, especially upon considerable changes in the architecture, structure, or systems, allowing organisations to proactively address them (NIST SP 800-30, 2012). Data backup and recovery such as regular backups, offsite storage, and recovery testing safeguard critical data, ensure rapid restoration in the event of a breach (NIST SP, 2012b). Efficient, continuous, and

potentially automated patch management, involving the timely application of updates to software, hardware, and firmware, closes security gaps that could be exploited by attackers. Finally, considering that human is often the weak link in the cybersecurity chain, ongoing security awareness training, including phishing simulations, empowers employees to recognise and respond to threats, thereby increasing the overall security posture of the organisation (SANS Security Awareness). Similarly, developing and maintaining a detailed Incident Response Plan (IRP), coupled with regular testing and drills, ensures swift and effective response to cyber incidents, minimising their impact (NIST SP, 2012a).

Adaptation measures for cyber resilience mostly focus on integrating threat intelligence, adopting adaptive security architectures, and ensuring continuous improvement. Specifically, threat intelligence is the collection, analysis, and dissemination of information about current and most importantly potential cyber threats throughout time. It involves gathering data on threat actors, their tactics, techniques, and procedures (TTPs), as well as identifying vulnerabilities and attack patterns, knowing which are the most active attacker groups, their targets, and their modus operandi. Threat intelligence is fundamental for adaptive cyber resilience, since it enables organisations to proactively defend against emerging threats. Commonly, this implies subscribing to reputable threat intelligence feeds, sourced from cybersecurity firms and open-source platforms, which provide information that can be used to adapt and anticipate potential threats.

Secondly, to adapt and mitigate new vulnerabilities and threats, it is fundamental to design a security architecture that is adaptable and extensible. This involves implementing scalable security solutions that can adjust to changes, both in the IT environment and in the threat landscape, for example by using dynamic access controls to modify security policies based on the evolving threat assessments. Finally, more general effective policies for an adaptive and continuous improvement of an organisation's cyber resilience posture involve periodic security audits to ensure that the organisation is up to the current security standards. Fundamental is, finally, the implementation of a valuable feedback loop that allows an organisation to learn from previous cybersecurity incidents, identifying and solving missed vulnerabilities in the organisation’s infrastructure and procedures (NIST SP 800-53).

Impact of resilience management measures for cyber systems

While traditional cybersecurity aims to stop attacks, cyber resilience is about weathering the storm and quickly bouncing back when those attacks happen. It's a shift in mindset, recognising that it's not a matter of "if" but "when" cyber incidents will occur (World Economic Forum). To be cyber resilient, businesses need to have a plan in place to keep things running smoothly even when facing cyberattacks. This means preparing for the worst, making sure disruptions are minimal, and having a strategy that covers everything from risk management to incident response. It's a team effort that needs support from the top down, weaving resilience into the fabric of the organisation.

Achieving cyber resilience means finding the right balance between implementing measures to prevent attacks, detect them quickly, and taking effective actions to minimise damage. To achieve such balance, given that security measures carry direct and indirect costs, it is necessary to understand the return on investment for prevention, detection, and reaction measures implemented. Similarly to many other contexts, an excessive expense on one of the three elements may be less beneficial than distributing the investments. Gordon & Loeb. (2002) suggests that spending more than 37% of potential losses on security might not be the most efficient, though this idea has been debated.

That is where Return on Security Investment (ROSI) comes in ENISA (2012). It's a way to measure the financial value of your security efforts, showing how they can save money by preventing losses and keeping operations running. Return on Security Investment (ROSI) is key for organisations like CERTs to measure if their security spending is paying off. Unlike typical ROI, which focuses on making a profit, ROSI is about preventing losses. This is because security investments are more about reducing risk than directly boosting revenue.

Calculating ROSI basically implies evaluating how much potential loss could be saved by a security investment. The difference from the more common ROI stems from the fact that, generally, security investments do not result in profit, but in potential loss prevention. Therefore, ROSI focuses on calculating how much loss an organisation avoided thanks to a security investment.

To calculate ROSI it is first necessary to introduce two other metrics: Single Loss Expectancy (SLE) represents the expected amount of money that will be lost when a risk occurs. In the context of cyber resilience, SLE can be considered as the cost of an incident assuming a single occurrence. It is important to note that, especially in this phase, there is a lot of guesswork involved, since it's tough to pinpoint the exact cost and frequency of incidents, and past data is essential for making any reliable estimates.

Annual Rate of Occurrence (ARO) represents the probability that a risk occurs in a year. Of course, similarly to the previous metric, it is hard to predict something that may or may not happen, especially since it is dependent on existing security measures.

Finally, calculating ROSI involves figuring out the Annual Loss Expectancy (ALE) which represents the potential loss multiplied by its expected frequency on a given asset and is calculated as ALE = ARO * SLE. ROSI then compares the cost of security measures to how much those measures are expected to reduce that potential loss.

Following the ROI definition, ROSI can be calculated as:

$$ROSI = \frac{Monetary\ loss\ reduction - Cost\ of\ the\ solution}{Cost\ of\ the\ solution} \quad \text{(Eq. 36)}$$

where the monetary loss reduction can be defined by the difference of ALE pre- and post- security solution implementation ($preALE$ & $postALE$), and hence it holds:

$$ROSI = \frac{\text{preALE} - \text{postALE} - Cost\ of\ the\ solution}{Cost\ of\ the\ solution} \quad \text{(Eq. 37)}$$

Note that the same result can be obtained using the mitigationRatio, computed as

$$\begin{gathered} mitigationRatio * preALE = preALE - postALE \\ mitigationRatio = (preALE - postALE)/(preALE) \end{gathered} \quad \text{(Eq. 38)}$$

which results in the Eq. 39:

$$ROSI = \frac{preALE * mitigationRatio - Cost\ of\ the\ solution}{Cost\ of\ the\ solution} \quad \text{(Eq. 39)}$$

4. Conclusion, Research Gaps and Future Perspectives

The field of resilience management for infrastructure, transportation and logistics networks against disruptions has made significant strides, yet several gaps that revolve around KPIs and handling strategies are still missing.

With respect to **all Roles**, the poll of end-users and review of commercial tools yielded that a global indicator for continuous resilience assessment and identification of critical points in transport infrastructure or logistics networks due to disruptive threats is missing. This global indicator can enhance preparedness, by planning and executing timely interventions, and integrate different resilience factors that are critical for each Role. Additionally, tools that i) automatically shutting down processes for risk mitigation, ii) provide step-by-step guidance during disruptions, iii) offer short- and long-term restoration plans to facilitate rapid recovery, iv) provide road alternatives considering vulnerability and costs, v) allow sustainability integration in resilience management, vi) update risk and recovery assessment methods to account for lessons-learned e.g., from climate change, vii) integrate information for risk-informed decision-making are missing.

Based on the literature review of modelling and management strategies, a lack of KPIs to assess the impact of information on system management or to evaluate resilience and sustainability trade-offs was observed. This shortage of KPIs reflects the lack of strategies from the poll. While some end-users have employed tools like real-time tracking and traffic monitoring systems, many still rely on outdated methods like email for communication during disruptions. This presents a significant gap in real-time data collection and decision-making. Future research should focus on developing more integrated digital systems that streamline communication, automate early warnings, and guide recovery actions based on reliable KPIs, as those identified in the modelling Section.

With respect to **Role 1**, the poll identified that none of the end-users collects data systematically to account for changes in the damage state of physical infrastructure (e.g., roads or bridges) and includes analysis to anticipate disruptions. Additionally, efficient road alternatives avoiding constraints posed by road geometry need to be further explored.

Regarding **Role 2 and 3**, a tool that collects and analyses data regarding the capacity of train routes and ship schedules is needed. Collection of data regarding changes in traffic demand is sufficiently addressed by the end-users.

Furthermore, more research is needed to align cyber threat models with broader resilience assessments, particularly for non-digital infrastructures such as transport infrastructure systems. For this purpose, hybrid threats and cross-sectoral collaboration should be examined. Many resilience strategies, especially in logistics, lack mechanisms for cross-sector collaboration. As disruptions increasingly affect interconnected systems, research should focus on developing collaborative decision-making frameworks that bring together stakeholders from different sectors, ensuring comprehensive resilience management across entire networks.

Finally, strategies related to the continuous improvement of population and stakeholder engagement through disruption simulations, as well as the inclusion of educational courses for young people to build social resilience, were not considered important by all end-users in the poll. Nevertheless, these strategies can arguably enhance social resilience.

Annex I

Table 14, Table 15 and Table 16 collect the handling strategies contemplated in the poll, which are classified based on the Roles 1-3 and the resilience components (preparedness, robustness, recovery capacity, and adaptive capacity). Some strategies refer to more than one Roles. End-users were asked to indicate which of their tools addressed each handling strategy and, if they did not, whether they believed they should be addressed.

Resilience component	#	Handling strategies
Preparedness	P-1	Continuous data collection that accounts for changes in hazard and environmental conditions and includes analysis to anticipate disruptions
	P-2	Continuous data collection that accounts for changes in the damage state of physical infrastructure (e.g., roads or bridges) and includes analysis to anticipate disruptions
	P-6	Continuous resilience assessment and definition of critical points in a logistics network due to ageing and/or disruptive threats based on a resilience indicator
	P-7	Planning and executing timely interventions to prevent disruptions
	P-8	Uniformity in the alarm system, data standardization, weather forecast accuracy, and public education on respecting rules and road safety
	P-9	Efficient weather forecasts to anticipate and manage weather-related disruptions
	P-10	Specific budget dedicated to disruptive events in contracts and projects administration and stakeholders
Robustness	R-11	Prevention protocols and actions to follow during disruptions
	R-12	Cooperation, communication, and information sharing with transport companies and authorities during disruptions
	R-13	Digital system automatically or manually shutting down processes to mitigate consequences
	R-14	Digital tool giving a step-by-step plan and guidance during disruptions (e.g. alarm systems, sensors, cameras, etc.)
Recovery capacity	RC-22	Short- and long-term restoration plans to ensure rapid recovery
	RC-26	Availability of resources to ensure quick recovery
	RC-27	Quick recovery from cyberattacks, maintaining updated data for better predictive modelling
Adaptive capacity	AC-28	Storing incident data and lessons-learned
	AC-29	Continuous improvement with disruption simulations and training of the population and logistical stakeholders
	AC-30	Tool for updating risk and recovery assessment methods to account for lessons learned e.g. from climate change or carbon emissions reduction
	AC-32	Changing internal processes e.g. standards, resources, work practices to better handle and mitigate disruptions
	AC-33	Inclusion of educational subjects in young people's education to gain social resilience

Table 14: Handling strategies contemplated in the poll for Role 1A.

Resilience component	#	Handling strategies
Preparedness	P-1	Continuous data collection that accounts for changes in hazard and environmental conditions and includes analysis to anticipate disruptions
	P-4	Collection of data that accounts for changes in traffic demand
	P-5	Transparent data on train routes and ship schedules
	P-6	Continuous resilience assessment and definition of critical points in a logistics network due to ageing and/or disruptive threats based on a resilience indicator
	P-7	Planning and executing timely interventions to prevent disruptions
	P-8	Uniformity in the alarm system, data standardization, weather forecast accuracy, and public education on respecting rules and road safety
	P-9	Efficient weather forecasts to anticipate and manage weather-related disruptions
	P-10	Specific budget dedicated to disruptive events in contracts and projects administration and stakeholders
Robustness	R-11	Prevention protocols and actions to follow during disruptions
	R-12	Cooperation, communication, and information sharing with transport companies and authorities during disruptions
	R-13	Digital system automatically or manually shutting down processes to mitigate consequences
	R-14	Digital tool giving a step-by-step plan and guidance during disruptions (e.g. alarm systems, sensors, cameras, etc.)
	R-18	Specific tool to have information from rail infrastructure managers on the capacity of rail routes
	RC-22	Short- and long-term restoration plans to ensure rapid recovery
	RC-24	Efficient road alternatives considering vulnerability and costs
	RC-25	Practical road alternatives for larger trucks considering limitations posed by street geometry
	RC-26	Availability of resources to ensure quick recovery
	RC-27	Quick recovery from cyberattacks, maintaining updated data for better predictive modelling
Adaptive capacity	AC-28	Storing incident data and lessons-learned
	AC-29	Continuous improvement with disruption simulations and training of the population and logistical stakeholders
	AC-30	Tool for updating risk and recovery assessment methods to account for lessons learned e.g. from climate change or carbon emissions reduction
	AC-32	Changing internal processes e.g. standards, resources, work practices to better handle and mitigate disruptions
	AC-33	Inclusion of educational subjects in young people's education to gain social resilience

Table 15: Handling strategies contemplated in the poll (Role 1B).

Resilience component	#	Handling strategies
Preparedness	P-1	Continuous data collection that accounts for changes in hazard and environmental conditions and includes analysis to anticipate disruptions
	P-3	Data integration and market analysis for future planning
	P-6	Continuous resilience assessment and definition of critical points in a logistics network due to ageing and/or disruptive threats based on a resilience indicator
	P-7	Planning and executing timely interventions to prevent disruptions
	P-8	Uniformity in the alarm system, data standardization, weather forecast accuracy, and public education on respecting rules and road safety
	P-9	Efficient weather forecasts to anticipate and manage weather-related disruptions
	P-10	Specific budget dedicated to disruptive events in contracts and projects administration and stakeholders
Robustness	R-11	Prevention protocols and actions to follow during disruptions
	R-12	Cooperation, communication, and information sharing with transport companies and authorities during disruptions
	R-13	Digital system automatically or manually shutting down processes to mitigate consequences
	R-14	Digital tool giving a step-by-step plan and guidance during disruptions (e.g. alarm systems, sensors, cameras, etc.)
	R-15	Specific tool to access data from shipowners for terminal and carrier planning
	R-16	Specific tool to know the cost of transport, fuel, and changes in demand in freight transport
	R-17	Specific tool for container tracking and port entity occupation
	R-19	Managing high shipping rates and fuel price increases
	R-20	Managing sudden fluctuations in cargo volumes
Recovery capacity	RC-21	Collaborating with new partners to maintain operations when usual partners are affected
	RC-22	Short- and long-term restoration plans to ensure rapid recovery
	RC-23	Changing transportation modes to avoid disruptions
	RC-26	Availability of resources to ensure quick recovery
	RC-27	Quick recovery from cyberattacks, maintaining updated data for better predictive modelling
Adaptive capacity	AC-28	Storing incident data and lessons-learned
	AC-29	Continuous improvement with disruption simulations and training of the population and logistical stakeholders
	AC-30	Tool for updating risk and recovery assessment methods to account for lessons learned e.g. from climate change or carbon emissions reduction
	AC-31	Flexibility to find new partners and build redundancy at critical points
	AC-32	Changing internal processes e.g. standards, resources, work practices to better handle and mitigate disruptions
	AC-33	Inclusion of educational subjects in young people's education to gain social resilience

Table 16: Handling strategies contemplated in the poll (Role 2 and 3).

References

Akbarzadeh, M., Memarmontazerin, S., Derrible, S., & Salehi Reihani, S. F. (2019). The role of travel demand and network centrality on the connectivity and resilience of an urban street system. *Transportation*, *46*(4), 1127–1141. https://doi.org/10.1007/s11116-017-9814-y

Anand, N., & Grover, N. (2015). Measuring retail supply chain performance. *Benchmarking: An International Journal*, *22*(1), 135–166, p.21. https://doi.org/10.1108/BIJ-05-2012-0034

Andrade, S. R., & Hulse, D. E. (2023). Evaluation and Improvement of System-of-Systems Resilience in a Simulation of Wildfire Emergency Response. *IEEE Systems Journal*, *17*(2), 1877–1888. https://doi.org/10.1109/JSYST.2022.3169125

Arango, E., Jiménez, P., Nogal, M., Sousa, H. S., Stewart, M. G., & Matos, J. C. (2024). Enhancing infrastructure resilience in wildfire management to face extreme events: Insights from the Iberian Peninsula. *Climate Risk Management*, *44*, 100595. https://doi.org/10.1016/j.crm.2024.100595

Arango, E., Nogal, M., Jiménez, P., Sousa, H. S., Stewart, M. G., & Matos, J. C. (2023). Policies towards the resilience of road-based transport networks to wildfire events. The Iberian case. *Transportation Research Procedia*, *71*, 61–68. https://doi.org/10.1016/j.trpro.2023.11.058

Arango, E., Nogal, M., Yang, M., Sousa, H. S., Stewart, M. G., & Matos, J. C. (2023). Dynamic thresholds for the resilience assessment of road traffic networks to wildfires. *Reliability Engineering & System Safety*, *238*, 109407. https://doi.org/10.1016/j.ress.2023.109407

ASCM. (2020). *Association for Supply Chain Management, Supply chain risk management insights and innovations. APICS. Retrieved from https://www.apics.org*.

Aujoux, C., & Mesnil, O. (2023). Environmental impact assessment of guided wave-based structural health monitoring. *Structural Health Monitoring*, *22*(2), 913–926. https://doi.org/10.1177/14759217221088774

Bakalis, K., & Vamvatsikos, D. (2018). Seismic Fragility Functions via Nonlinear Response History Analysis. *Journal of Structural Engineering (United States)*. https://doi.org/10.1061/(ASCE)ST.1943-541X.0002141

Baker, J. W. (2015). Efficient analytical fragility function fitting using dynamic structural analysis. *Earthquake Spectra*. https://doi.org/10.1193/021113EQS025M

Barbeau, M., Cuppens, F., Cuppens, N., Dagnas, R., & Garcia-Alfaro, J. (2021). *Resilience estimation of cyber-physical systems via quantitative metrics. IEEE Access, 9, 46462-46475. https://doi.org/10.1109/ACCESS.2021.3066108*

BBC. (2024). *Baltimore bridge crash causes supply chain concerns [online]. Available: https://www.bbc.com/news/world-us-canada-68672373*

Bigs, G., & Marquis, K. D. (2023). *Perspective: Fire can be a nature-based solution. Gordon and Betty Moore Foundation. URL: https://www.moore.org/article-detail?newsUrlName=perspective-fire-is-a-nature-based-solution&tagToFilterBy=ab660061-a10f-68a5-8452-ff00002785c8*

Biondini, F., & Frangopol, D. M. (2016). Life-Cycle Performance of Deteriorating Structural Systems under Uncertainty: Review. *Journal of Structural Engineering*, *142*(9). https://doi.org/10.1061/(ASCE)ST.1943-541X.0001544

Bodeau, D., & Graubart, R. (2017). *Cyber resiliency design principles. The MITRE Corporation*

Bodeau, D., Graubart, R., Picciotto, J., & McQuaid, R. (2011). *Cyber resiliency engineering framework. MTR110237, MITRECorporation*

Bodeau, D. J., Graubart, R. D., McQuaid, R. M., & Woodill, J. (2018). *Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring, Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods, p. 8.*, https://www.mitre.org/sites/default/files/2021-11/prs-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf

Bradley, B. A., Cubrinovski, M., Dhakal, R. P., & MacRae, G. A. (2010). Probabilistic seismic performance and loss assessment of a bridge–foundation–soil system. *Soil Dynamics and Earthquake Engineering*, *30*(5), 395–411. https://doi.org/10.1016/j.soildyn.2009.12.012

Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O'Rourke, T. D., Reinhorn, A. M., Shinozuka, M., Tierney, K., Wallace, W. A., & von Winterfeldt, D. (2003). A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. *Earthquake Spectra*, *19*(4), 733–752. https://doi.org/10.1193/1.1623497

Bruneau, M., & Reinhorn, A. (2007). Exploring the Concept of Seismic Resilience for Acute Care Facilities. *Earthquake Spectra*, *23*(1), 41–62. https://doi.org/10.1193/1.2431396

CER Directive. (2022). *Directive of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC*

Chopra, S., & Sodhi, M. S. (2004). *Managing Risk to Avoid Supply-Chain Breakdown (available from https://sloanreview.mit.edu/article/managing-risk-to-avoid-supplychain-breakdown/)*.

Cimellaro, G. P., Fumo, C., Reinhorn, A. M., & Bruneau, M. (2009). Quantification of Disaster Resilience of Health Care Facilities. *Mceer-09-0009, https://www.eng.buffalo.edu/mceer-reports/09/09-0009.pdf*

Cimellaro, G. P., Reinhorn, A. M., & Bruneau, M. (2010). Framework for analytical quantification of disaster resilience. *Engineering Structures*, *32*(11), 3639–3649. https://doi.org/10.1016/j.engstruct.2010.08.008

Copernicus. (2024). *Sobre Copernicus, Retrieved from: https://www.copernicus.eu/es/sobre-copernicus*

Domaneschi, M., Cucuzza, R., Martinelli, L., Noori, M., & Marano, G. C. (2024). A probabilistic framework for the resilience assessment of transport infrastructure systems via structural health monitoring and control based on a cost function approach. *Structure and Infrastructure Engineering*, 1–13. https://doi.org/10.1080/15732479.2024.2318231

Dong, Y., & Frangopol, D. M. (2015). Risk and resilience assessment of bridges under mainshock and aftershocks incorporating uncertainties. *Engineering Structures*, *83*, 198–208. https://doi.org/10.1016/j.engstruct.2014.10.050

EC. (2018). *European Commission. Cardoso Castro Rego, F., Moreno Rodríguez, J., Vallejo Calzada, V., Xanthopoulos, G. Forest fires – Sparking firesmart policies in the EU, Publications. Office. DOI:10.2777/181450.* https://doi.org/10.2777/181450

EC. (2021). *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Forging a climate-resilient Europe - the new EU Strategy on Adaptation to Climate Change*

ECMWF. (2024). *ECMWF as part of The Copernicus Programme, 2024. Wildfire impact: How is it monitored & measured? Retrieved from: https://climate.copernicus.eu/wildfire-impact-how-it-*

monitored-measured

EFFIS, C.-E. U. (1998). *European Forest Fire Information System (EFFIS). URL: https://forest-fire.emergency.copernicus.eu/(EFFIS, Copernicus - European Union, 1998) European Forest Fire Information System (EFFIS). URL: https://forest-fire.emergency.copernicus.eu/*

EMF. (2020). *Ellen MacArthur Foundation. Circular Economy in Logistics and Transport*

EN 16991. (2018). *Risk-based inspection framework*

ENISA. (2012). *European Network and Information Security Agency. "Introduction to Return on Security Investment." (2012)*

ESA. (2023). *European Space Agency, Satellite data used for road infrastructure safety in Italy, Retrieved from https://www.esa.int/Applications/Observing_the_Earth/Copernicus/Sentinel-1/Satellite_data_used_for_road_infrastructure_safety_in_Italy#:~:text=A%20new%20gro*

Esri. (2024). *What is ArcGIS?. Retrieved from https://www.esri.com/en-us/arcgis/about-arcgis/overview*

FEMA-HAZUS. (2012). *Multi-hazard Loss Estimation Methodology, Earthquake Model, Technical Manual Hazus 2.1, https://www.fema.gov/sites/default/files/2020-09/fema_hazus_earthquake-model_technical-manual_2.1.pdf*

Fisher., R. A. (1937). *The Design of Experiments (second ed.), Oliver & Boyd, Edinburgh & London, https://mimno.infosci.cornell.edu/info3350/readings/fisher.pdf*

Ganteaume, A., Camia, A., Jappiot, M., San-Miguel-Ayanz, J., Long-Fournel, M., & Lampin, C. (2013). A Review of the Main Driving Factors of Forest Fire Ignition Over Europe. *Environmental Management*, *51*(3), 651–662. https://doi.org/10.1007/s00267-012-9961-z

Ghosn, M., Dueñas-Osorio, L., Frangopol, D. M., McAllister, T. P., Bocchini, P., Manuel, L., Ellingwood, B. R., Arangio, S., Bontempi, F., Shah, M., Akiyama, M., Biondini, F., Hernandez, S., & Tsiatas, G. (2016). Performance Indicators for Structural Systems and Infrastructure Networks. *Journal of Structural Engineering*, *142*(9). https://doi.org/10.1061/(ASCE)ST.1943-541X.0001542

Giordano, P. F., & Limongelli, M. P. (2020). Response-based time-invariant methods for damage localization on a concrete bridge. *Structural Concrete*, *21*(4), 1254–1271. https://doi.org/10.1002/suco.202000013

Giordano, P. F., & Limongelli, M. P. (2022). The value of structural health monitoring in seismic emergency management of bridges. *Structure and Infrastructure Engineering*. https://doi.org/10.1080/15732479.2020.1862251

Giordano, P. F., Prendergast, L. J., & Limongelli, M. P. (2020). A framework for assessing the value of information for health monitoring of scoured bridges. *Journal of Civil Structural Health Monitoring*, *10*(3), 485–496. https://doi.org/10.1007/s13349-020-00398-0

Gordon, L. A., & Loeb., M. P. (2002). *"The economics of information security investment." ACM Transactions on Information and System Security (TISSEC) 5.4: 438-457,* https://doi.org/*1094-9224/02/1100-0438*

Hann, C. E., Singh-Levett, I., Deam, B. L., Mander, J. B., & Chase, J. G. (2009). Real-Time System Identification of a Nonlinear Four-Story Steel Frame Structure—Application to Structural Health Monitoring. *IEEE Sensors Journal*, *9*(11), 1339–1346. https://doi.org/10.1109/JSEN.2009.2022434

Hasan, R., Kamal, M. M., Daowd, A., Eldabi, T., Koliousis, I., & Papadopoulos, T. (2024). Critical analysis

of the impact of big data analytics on supply chain operations. *Production Planning & Control*, *35*(1), 46–70. https://doi.org/10.1080/09537287.2022.2047237

Holling, C. (1973). *Resilience and stability of ecological systems. Ann Rev Ecol Syst, pp. 1-23, https://doi.org/10.1146/annurev.es.04.110173.000245*

Juan, S.-J., Li, E. Y., & Hung, W.-H. (2022). An integrated model of supply chain resilience and its impact on supply chain performance under disruption. *The International Journal of Logistics Management*, *33*(1), 339–364. https://doi.org/10.1108/IJLM-03-2021-0174

Ivanov, D., & Dolgui, A. (2021). A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0. *Production Planning & Control*, *32*(9), 775–788. https://doi.org/10.1080/09537287.2020.1768450

Karagiannakis, G., Giordano, P. F. and Limongelli, M. P. (2024). *Resilience components and metrics for transport infrastructure against natural hazards, IABSE congress 2024, San Jose, Costa Rica, 24-27 September, 2024 (https://www.iabse.org/Sanjose2024)*

Karagiannakis, G., Di Sarno, L., Necci, A., & Krausmann, E. (2022). Seismic risk assessment of supporting structures and process piping for accident prevention in chemical facilities. *International Journal of Disaster Risk Reduction*, *69*, 102748. https://doi.org/10.1016/j.ijdrr.2021.102748

Korneta, P., Krzyszkowski, A., & Chmiel, M. (2018). Performance measurement in supply chain. *AUTOBUSY – Technika, Eksploatacja, Systemy Transportowe*, *19*(4), 33–36. https://doi.org/10.24136/atest.2018.017

Lenort, R., & Wicher, P. (2013). *Concept of a system for resilience measurement in industrial supply chain. In METAL 2013: 22nd International Conference on Metallurgy and Materials TANGER, https://www.researchgate.net/publication/290184605_Concept_of_a_system_for_resilience_measurement_in_industrial_supply_chain*

Liao, T.-Y., Hu, T.-Y., & Ko, Y.-N. (2018). A resilience optimization model for transportation networks under disasters. *Natural Hazards*, *93*(1), 469–489. https://doi.org/10.1007/s11069-018-3310-3

Lim, S., Kim, T., & Song, J. (2022). System-reliability-based disaster resilience analysis: Framework and applications to structural systems. *Structural Safety*, *96*, 102202. https://doi.org/10.1016/j.strusafe.2022.102202

Limongelli, M. P., Chatzi, E., & Anžlin, A. (2018). Condition Assessment of Roadway Bridges: From Performance Parameters to Performance Goals. *The Baltic Journal of Road and Bridge Engineering*, *13*(4), 345–356. https://doi.org/10.7250/bjrbe.2018-13.421

Limongelli, M. P., Previtali, M., Cantini, L., Carosio, S., Matos, J. C., Isoird, J. M., Wenzel, H., & Pellegrino, C. (2019). LIFECYCLE MANAGEMENT, MONITORING AND ASSESSMENT FOR SAFE LARGE-SCALE INFRASTRUCTURES: CHALLENGES AND NEEDS. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, *XLII-2/W11*, 727–734. https://doi.org/10.5194/isprs-archives-XLII-2-W11-727-2019

Maroni, A., Tubaldi, E., McDonald, H., & Zonta, D. (2022). A monitoring-based classification system for risk management of bridge scour. *Proceedings of the Institution of Civil Engineers - Smart Infrastructure and Construction*, *175*(2), 92–102. https://doi.org/10.1680/jsmic.21.00016

Maroni, A., Tubaldi, E., Val, D. V, McDonald, H., & Zonta, D. (2021). Using Bayesian networks for the assessment of underwater scour for road and railway bridges. *Structural Health Monitoring*, *20*(5), 2446–2460. https://doi.org/10.1177/1475921720956579

Martínez-Sánchez, J. J., Ferrandis, P., De Las Heras, J., & Herranz, J. M. (1999). *Effect of burnt wood*

removal on the natural regeneration of Pinus halepensis after fire in a pine forest in Tus valley (SE Spain). Forest Ecology and Management, https://doi.org/10.1016/S0378-1127(99)00012-2

Meier, S., Elliott, R. J. R., & Strobl, E. (2023). The regional economic impact of wildfires: Evidence from Southern Europe. *Journal of Environmental Economics and Management*, *118*, 102787. https://doi.org/10.1016/j.jeem.2023.102787

MFSL. (2023). *Missoula Fire Sciences Laboratoy, Crown Fire (technical documentation). Flammap Help. URL: https://owfflammaphelp62.firenet.gov/#t=LegacyFARSITE%2FTech_Crown_Fire.htm*

Min, S., Zacharia, Z. G., & Smith, C. D. (2019). Defining Supply Chain Management: In the Past, Present, and Future. *Journal of Business Logistics*, *40*(1), 44–55. https://doi.org/10.1111/jbl.12201

Mitoulis, S. A., Argyroudis, S. A., Loli, M., & Imam, B. (2021). Restoration models for quantifying flood resilience of bridges. *Engineering Structures*, *238*, 112180. https://doi.org/10.1016/j.engstruct.2021.112180

MITRE. (2015). *MITRE ATT&CK®, https://attack.mitre.org/*

Mondoro, A., Frangopol, D. M., & Liu, L. (2018). Multi-criteria robust optimization framework for bridge adaptation under climate change. *Structural Safety*, *74*, 14–23. https://doi.org/10.1016/j.strusafe.2018.03.002

Morgese, M., Domaneschi, M., Ansari, F., Cimellaro, G. P., & Inaudi, D. (2021). Improving Distributed Fiber-Optic Sensor Measures by Digital Image Correlation: Two-Stage Structural Health Monitoring. *ACI Structural Journal*, *118*(6). https://doi.org/10.14359/51732994

Moya, D., Heras, J. D. las, Ferrandis, P., Herranz, J. M., & Martínez-Sánchez, J. J. (2011). *Fire resilience and Forest Restoration in mediterranean fire-prone areas. Technology and Knowledge Transfer e-Bulletin, Vol. 2, N. 3, http://hdl.handle.net/10317/1694*

Murino, G., Armando, A., & Tacchella, A. (2019). *Resilience of cyber-physical systems: an experimental appraisal of quantitative measures. In 2019 11th international conference on cyber conflict (CyCon) (Vol. 900, pp. 1-19). IEEE, https://doi.org/10.23919/CYCON.2019.8757010*

NASA, F. (2012). *Fire Information for Resource Management System (FIRMS). URL: https://firms.modaps.eosdis.nasa.gov/*

NIST SP, 800-30. (2012a). *"NIST special publication 800-30 risk management guide for information technology systems.", https://doi.org/10.6028/NIST.SP.800-30*

NIST SP, 800-34. (2012b). *"NIST Special Publication 800-34 Contingency Planning Guide for Federal Information Systems Revision 1.", https://doi.org/10.6028/NIST.SP.800-34*

Niu, C., Nair, D. J., Zhang, T., Dixit, V., & Murray-Tuite, P. (2022). Are wildfire fatalities related to road network characteristics? A preliminary analysis of global wildfire cases. *International Journal of Disaster Risk Reduction*, *80*, 103217. https://doi.org/10.1016/j.ijdrr.2022.103217

Nogal, M., Morales Nápoles, O., & O'Connor, A. (2019). Structured expert judgement to understand the intrinsic vulnerability of traffic networks. *Transportation Research Part A: Policy and Practice*, *127*, 136–152. https://doi.org/10.1016/j.tra.2019.07.006

Nogal, M., & O'Connor, A. (2018). *Resilience assessment of transport networks. Routledge handbook of sustainable and resilient infrastructure, Routledge, pp. 199-215, 1st Ed. ISBN: 9781315142074*

Novo, A., Dutal, H., & Eskandari, S. (2024). Fire susceptibility modeling and mapping in Mediterranean forests of Turkey: a comprehensive study based on fuel, climatic, topographic, and anthropogenic factors. *Euro-Mediterranean Journal for Environmental Integration*, *9*(2), 655–

679. https://doi.org/10.1007/s41207-024-00475-6

Novo, A., Fariñas-Álvarez, N., Martínez-Sánchez, J., González-Jorge, H., Fernández-Alonso, J. M., & Lorenzo, H. (2020). Mapping Forest Fire Risk—A Case Study in Galicia (Spain). *Remote Sensing*, *12*(22), 3705. https://doi.org/10.3390/rs12223705

Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Papers (CSWP) No. 29). National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.CSWP.29

Pettit, T., Fiksel, J., & Croxton, K. (2010). *Ensuring supply chain resilience: development of a conceptual framework. Journal of Business Logistics, Vol. 31, No. 1, 10.1002/j.2158-1592.2010.tb00125.x*

Pregnolato, M., Ford, A., Glenis, V., Wilkinson, S., & Dawson, R. (2017). Impact of Climate Change on Disruption to Urban Transport Networks from Pluvial Flooding. *Journal of Infrastructure Systems*, *23*(4). https://doi.org/10.1061/(ASCE)IS.1943-555X.0000372

Prendergast, L. J., Limongelli, M. P., Ademovic, N., Anžlin, A., Gavin, K., & Zanini, M. (2018). Structural Health Monitoring for Performance Assessment of Bridges under Flooding and Seismic Actions. *Structural Engineering International*, *28*(3), 296–307. https://doi.org/10.1080/10168664.2018.1472534

Raeisi, F., Algohi, B., Mufti, A., & Thomson, D. J. (2021). Reducing carbon dioxide emissions through structural health monitoring of bridges. *Journal of Civil Structural Health Monitoring*, *11*(3), 679–689. https://doi.org/10.1007/s13349-021-00474-z

ReFLOAT-ER. (2023). *Project on Resilient Reconstruction of Flooded Appenines Territories of Emilia-Romagna. Personal Communication during the mission in Modigliana municipality.* https://www.dabc.polimi.it/wp-content/uploads/2023/12/resilienza.pdf

Rose, A. (2007). *"Economic resilience to natural and man-made disasters: Multidisciplinary origins and contextual dimensions" Environmental Hazards, vol. 7, n. 4, pp. 383-398, https://doi.org/10.1016/j.envhaz.2007.10.001*

Rothermel, R. . (1972). *A mathematical model for predicting fire spread in wildland fuels. USDA Forest Service, Intermountain Forest and Range Experiment Station, available from https://research.fs.usda.gov/treesearch/32533*

Rouse, J. W., Haas, R. H., Schell, J. A., & Deering, D. W. (1973). *Monitoring vegetation systems in the great plains with ERTS, Paper A 20. In Proceedings of the Third Earth Resources Technology Satellite-1 Symposium, Washington, DC, USA, https://ntrs.nasa.gov/api/citations/19740022614/downloads/19740022614.pdf*

Saaty, T. (1980). *The Analytic Hierarchy Process: Planning, Priority Setting, Resources Allocation. Mcgraw-Hill, New York, ISBN 0070543712, 9780070543713*

Sakellariou, S., Sfougaris, A., Christopoulou, O., & Tampekis, S. (2023). Spatial Resilience to Wildfires through the Optimal Deployment of Firefighting Resources: Impact of Topography on Initial Attack Effectiveness. *International Journal of Disaster Risk Science*, *14*(1), 98–112. https://doi.org/10.1007/s13753-023-00464-3

SARIL, P. (2023). *D1.1 Scenario cases definition*

SARIL, P. (2024a). *D1.2 Framework for a sustainability and resilience evaluation of strategic logistics networks*

SARIL, P. (2024b). *D1.3 Strategies for improving resilience through participatory stakeholder practices - Delphi survey results*

Sfetsos, A., Giroud, F., Clemencau, A., Varela, V., Freissinet, C., LeCroart, J., Vlachogiannis, D., Politi, N., Karozis, S., Gkotsis, I., Eftychidis, G., Hedel, R., & Hahmann, S. (2021). Assessing the Effects of Forest Fires on Interconnected Critical Infrastructures under Climate Change. Evidence from South France. *Infrastructures*, *6*(2), 16. https://doi.org/10.3390/infrastructures6020016

Smith, S. C., Raio, S., Erbacher, R. F., Weisman, M., Parker, T. W., & Ellis, J. (2022). *Quantitative measurement of cyber resilience: A tabletop exercise. DEVCOM Army Research Laboratory (US): Adelphi, MD, USA, (availabe from https://apps.dtic.mil/sti/trecms/pdf/AD1158532.pdf)*

Spatineo, I. (2024). *How does earth observation benefit us? Retrieved from: https://www.spatineo.com/how-does-earth-observation-benefit-us/*

Stein, S. M., Young, G. K., Trent, R. E., & Pearson, D. R. (1999). Prioritizing Scour Vulnerable Bridges Using Risk. *Journal of Infrastructure Systems*, *5*(3), 95–101. https://doi.org/10.1061/(ASCE)1076-0342(1999)5:3(95)

Tang, C. S. (2006). *Perspectives in supply chain risk management. International Journal of Production Economics, 103(2), 451-488, https://doi.org/10.1016/j.ijpe.2005.12.006*

Taylor, M. A. P., & Susilawati. (2012). Remoteness and accessibility in the vulnerability analysis of regional road networks. *Transportation Research Part A: Policy and Practice*, *46*(5), 761–771. https://doi.org/10.1016/j.tra.2012.02.008

Técnica, I. (2020). *Manual de contenidos. Simulación de incendios forestales: Flammap y LIDAR aplicados a actuaciones de prevención. https://imasgal.com/curso/simulacion-incendios-forestales-flammap-lidar/*

Tedim, F., Leone, V., Amraoui, M., Bouillon, C., Coughlan, M., Delogu, G., Fernandes, P., Ferreira, C., McCaffrey, S., McGee, T., Parente, J., Paton, D., Pereira, M., Ribeiro, L., Viegas, D., & Xanthopoulos, G. (2018). Defining Extreme Wildfire Events: Difficulties, Challenges, and Impacts. *Fire*, *1*(1), 10. https://doi.org/10.3390/fire1010009

Van Wagner, C. E. (1985). *Equations and FORTRAN Program for the Canadian Forest Fire Weather Index System; Service Canadien des Forests, Gouvernement du Canada: Ottawa, ON, Canada. Forestry Technical Report 33, https://ostrnrcan-dostrncan.canada.ca/handle/1845/228362*

Voigt, S., Kemper, T., Riedlinger, T., Kiefl, R., Scholte, K., & Mehl, H. (2007). Satellite Image Analysis for Disaster and Crisis-Management Support. *IEEE Transactions on Geoscience and Remote Sensing*, *45*(6), 1520–1528. https://doi.org/10.1109/TGRS.2007.895830

Wamba, S. F., & Akter, S. (2019). *Impact of Big Data on supply chain management. Journal of Business Research, 70, 354-36, https://doi.org/10.1080/13675567.2018.1459523*

Waters, D. (2007). *Supply Chain Risk Management, Vulnerability and Resilience in Logistics*. https://eclass.unipi.gr/modules/document/file.php/BDT227/Υλικό Διαλέξεων/Supply Chain Risk Management_ Vulnerability and Resilience in Logistics-2007 %281%29.pdf

Xiang, N., Chen, X., & Alam, M. S. (2020). Probabilistic seismic fragility and loss analysis of concrete bridge piers with superelastic shape memory alloy-steel coupled reinforcing bars. *Engineering Structures*, *207*, 110229. https://doi.org/10.1016/j.engstruct.2020.110229

Yung, L., Gray, B. J., Wyborn, C., Miller, B. A., Williams, D. R., & Essen, M. (2022). New types of investments needed to address barriers to scaling up wildfire risk mitigation. *Fire Ecology*, *18*(1), 30. https://doi.org/10.1186/s42408-022-00155-2

Zheng, W., & Yu, W. (2015). Probabilistic Approach to Assessing Scoured Bridge Performance and Associated Uncertainties Based on Vibration Measurements. *Journal of Bridge Engineering*,

20(6). https://doi.org/10.1061/(ASCE)BE.1943-5592.0000683