www.piarc.org
2023R46EN

ROAD INFRASTRUCTURE AND TRANSPORT SECURITY

A PIARC TECHNICAL REPORT

TASK FORCE 3.1 *ROAD INFRASTRUCTURE AND TRANSPORT SECURITY*

PIARC

STATEMENTS

The World Road Association (PIARC) is a non-profit organization established in 1909 to improve international co-operation and to foster progress in the field of roads infrastructure and transport.

The study subject of this report was defined in the PIARC Strategic Plan 2020– 2023 and was approved by the Council of the World Road Association, whose members are representatives of the member national governments. The members of the Technical Committee responsible for this report were nominated by the member national governments for their special competences.

Any opinions, findings, conclusions and recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of their parent organizations or agencies.

This report is available from the internet site of the World Road Association (PIARC): http://www.piarc.org

World Road Association (PIARC)
Arche Sud 5° niveau
92055 La Défense cedex, France

International Standard Book Number: 978-2-84060-838-7

Front cover © iStock

ROAD INFRASTRUCTURE AND TRANSPORT SECURITY

A PIARC TECHNICAL REPORT

TASK FORCE 3.1 *ROAD INFRASTRUCTURE AND TRANSPORT SECURITY*

AUTHORS/ACKNOWLEDGEMENTS

This Report has been drafted by the Task Force 3.1 “Road Infrastructure sand Transport Security” of PIARC World Road Association. All information included in this report is correct to the best of the authors’ knowledge and therefore, they shall not in any case be held liable for any errors and omissions.

The Task Force 3.1 was chaired by Saverio PALCHETTI (Italy), Philippe CHANARD (France), Luz Angelica GRADILLA HERNANDEZ (Mexico) and Chris JOHNSON were the French, Spanish and English-speaking secretaries respectively.

The other members (M), associated (AM) and corresponding members (CM) of the Task Force 3.1 which were actively engaged in the work and also contributors to the preparation of this Report, were:

- Berthold BEST (Germany), (M)
- Michele BIANCHI (Italy), (AM)
- Boubacar DIALLO (Mali) (M)
- Paulin KOUASSY (Ivory Coast), (AM)
- Flavius PAVAL (Romania), (M)
- Ales PAVSEK (Slovenia), (M)
- Bine PENGAL (Slovenia), (M)
- Songsu SON (South Korea), (CM)
- UK Government Security Adviser, NPSA (United Kingdom), (M)
- Michal ZABOWSKY (Slovak Republic), (M)

Michele BIANCHI (Italy) and Paulin KOUASSY (Ivory Coast) joined the Task Force, formally appointed as associate members (AM).

The following Report was reviewed by the UK Government Security Adviser, the Centre for the Protection of National Infrastructure (CPNI now NPSA) for the English version, in collaboration with Alexandra LUCK (United Kingdom), Philippe CHANARD (France) for the French version and Luz Angelica GRADILLA HERNANDEZ (Mexico) for the Spanish version.

Also, a sincere thanks for their contribution to:

- Adalberto BIASIOTTI (Italy) and Anna VILLANI (Italy), Security managers;
- Fabio GARSIA (Italy), Professor of Security Engineering, University of Rome “La Sapienza”;
- Antonio SCALA (Italy), Senior Researcher, Institute for Complex Systems (ISC), CNR and Department of Physics of University of Rome “La Sapienza”;
- Balduino SIMONE (Italy), Professor of Traffic and Safety Law, University of Urbino;
- David WHITE (UK), Valerio PARISI (Italy) and Daniela PASTORE (Italy) for helping with the review of the English text throughout the development of this Report.

Shigeru KIKUKAWA, Jun TAKEUSHI and Kei SENOO (Japan) were respectively the Coordinator of Strategic Theme 3 "Safety and Sustainability" and the two Technical Assistants of the Coordinator.

EXECUTIVE SUMMARY

2023R46EN

ROAD INFRASTRUCTURE AND TRANSPORTATION SECURITY

A PIARC TECHNICAL REPORT

This report aims to provide elements for addressing security risks and risk management from criminal and terrorist threats in the various road topics affecting road infrastructure mentioned above, within the conceptual framework, definitions and terminologies provided by the international standards ISO 28000 and 31000. Among the techniques that can be used, risk assessment was chosen which includes risk identification, analysis and assessment phases, and selecting a consequence/liability pair and displaying them on a matrix according to the indications contained in the aforementioned international standards.

Once threats and risks from malicious acts are determined and prioritized, a common approach followed, aimed at mitigation strategy, accompanied by defence measures and proposals for specialized final recommendations for each addressed topic.

This document refers to the Report elaborated in the previous cycle by the PIARC Task Force C.1 "Security of Road Infrastructure", published in 2019.

This Report is also based significantly on a comprehensive Literature Review “PIARC TF 3.1 – Literature Review – Documents Relevant to Road Infrastructure and Transport Security”, developed by this Task Force and published by PIARC in 2022.

CONTENTS

PREAMBLE

The client should decide how much risk to accept.
No construction project is risk free.
Risk can be managed, minimized, shared, transferred or accepted.
It cannot be ignored.
The client who wishes to accept little or no risk should take different routes for procuring advice from the client who places importance on detailed, hands-on control.

The Latham Report, Constructing the Team", by Sir Michael Latham, 1994

Security. How can we define security and the means to defend ourselves from crime and terrorism, as well as theft and multiple damage during demonstrations or other malicious acts? Is it excessive to worry about security to this extent? The answer is that security affects all of us more and more. This has been the case since the tragic attacks of September 11, 2001 (New York), as well as many other tragic events such as January 2015 (Paris), March 2020 (Covid-19), February 24, 2022 (Ukraine - Russia), October 07, 2023 (Israel - Gaza), that have left a profound mark in our hearts and minds. Each one of us has unconsciously gone into a state of constant alert.

Especially 9/11 and November 13, 2015, when Paris was shaken by a group of terrorist attacks that culminated in the Bataclan massacre, left an indelible mark. It may happen to experience a remote psychological state of insecurity. We know we are exposed, in a city, in an airport or in a skyscraper. Physical and cyber threats may affect us directly and personally, immersed as we are in a sequence of geo-political, economic, energy, epidemic crises that have erupted in the last decade about which no one had worried us or warned us in advance.

It is prudent to be attentive observers, in order to anticipate threats beforehand. Simple citizens, employees, students, entrepreneurs, traders, retirees, restaurants, hotels, live in cities or the countryside, who hang out in shops, malls, offices, schools, and walk through the street. Many have businesses, some made investments, and suddenly their hard work can be wiped out by an unexpected crisis. Therefore, the need for greater awareness is growing in people, the desire to know and possibly to foresee events that can be decisive for our life and our activities. We find ourselves in an uncertain reality, and the need for security in growing. The word "security" comes from the Latin "*securus*" i.e., without worries. When we feel safe, we are, in fact, "without worries". But when do we feel safe? When are we really?

The list of current threats is long and a dramatic event that occurs anywhere in the world may affect virtually the entire planet. We have to defend ourselves against exceptional weather events and earthquakes as well as new threats originating from the use of internet (digital identity theft, cyber bullying, etc.) or home banking (phishing, pharming, etc.) as well as online shopping. We're dealing with issues concerning day-to-day life. All this is not paranoia, it is a reality to be faced with a clear mind and a good philosophical approach. This is proposed in this Report on "Road infrastructures and transport security", significantly based on international ISO standards.

We are aware of the challenge we face. The goal is complex and concerns the threats brought intentionally by malicious people: acts of violence to instill terror, commit attacks, robberies, or even to create fake news and carry out harmful actions on the internet. It's a task that we approach knowing its ever-morphing nature. The context of a project or an asset may change continuously and the next threat may not fall into the pool of previously observed phenomena.

The philosophy of improving security risk management serves to overcome this limitation. Continuous cyclical verifications serve to test the hypotheses adopted on the basis of the deduced facts, and critically rebuilding the choice made is imperative. It is a dialectical process between the complex reality - “chaos” - and order and reason - “logos” -, between irrationality and rationality, in a world which is chaotic, always in transformation and often also insecure.

1. INTRODUCTION

1.1. ACRONYMS - GLOSSARIES - TERMS – DEFINITIONS

Acronyms, glossaries, terms and definitions, are shown in chapters 1.4 and 1.5 of the Literature Review[1] which constitutes one of the basic references of this Report. They help significantly the reading of this document also in consideration of the specific vocabulary used in security matters. The list of the used acronyms is shown in Fig. 1.

Term	Definition
ADAS	Advanced Driver Assistance Systems
ADR	European Agreement concerning the International Carriage of Dangerous Goods by Road
AI	Artificial Intelligence
ANSI	American National Standards Institute
CAV	Connected Autonomous Vehicles
CBRNE	Chemical, Biological, Radiological, Nuclear, and high yield Explosives
CCTV	Closed-Circuit Television
CEN	European Committee for Standardization
CPNI	The Centre for the Protection of National Infrastructure (UK), now the NPSA
C-ITS	Cooperative Intelligent Transport Systems
DIV	Driver Infrastructure Vehicle (triangle)
EC	European Commission
ENISA	European Union Agency for Cybersecurity
EU	European Union
GDPR	General Data Protection Regulation
ISO	International Standard Organization
ICT	Information and Communication Technology
IMS	Integrated management system, integration within ISO of systems, processes and standards
IoT	Internet of Things
ISO	International Standard Organization
IT(S)	Information Technology (System)
IWA	International Workshop Agreement
LR	Literature Review
MS	Management System
NIST	National Institute of Standards and Technology
NPSA	The National Protective Security Authority (UK), formerly the CPNI

[1] "PIARC TF 3.1 – Literature Review – Documents Relevant to Road Infrastructure and Transport Security", 2022R07EN, ISBN 978-2-84060-682-6.

OECD	The Organization for Economic Cooperation and Development
PDCA	Plan-Do-Check-Act process or Deming's wheel or cycle
PIARC	World Road Association
RA(s)	Road Administration(s) and Authority(ies)
RSM	(PIARC) Road Safety Manual
SAE	Society of Automotive Engineers
SCADA	Supervisory Control and Data Acquisition
TC(s)	Technical Committee(s)
TF(s)	Task Force(s)
ToR	Term of Reference from PIARC Strategic Plan 2020-2023, update October 2020
UAV	Unmanned Aerial Vehicle
UN	United Nations
VAAW	Vehicle As A Weapon
VBIED	Vehicle Borne Improvised Explosive Device
VSB	Vehicle Security Barrier

Fig. 1 - List of acronyms

1.2. BACKGROUND

1.2.1. An overview on security in road infrastructure and transport

The **PIARC Report "Security of Road Infrastructure" of the Task Force C.1., published in 2019**[2] in the context of the PIARC 2016-2019 cycle (hereinafter Report TF C.1 2019), dealt with the basic issues of infrastructure security of interest to RAs also suggesting technical and operational recommendations to prevent physical and cyber threats in the road infrastructure sector. During the preparation and publication of such Report, several tragic events took place in Europe and around the world, highlighting the evolving threats from terrorism and criminality to infrastructure, public spaces and mobility. Accidental incidents also occurred, the most serious of which having the same tragic consequences.

Since **January 2015**, after the attack on the editorial office of the satirical newspaper Charlie Hebdo in Paris, an increased perception of security has been recorded globally and a profound cultural transformation has taken place. We are experiencing shocking changes on various levels: the physical, virtual, man-machine hybrid, informative one. The latter is a new theme to defend democracies from terror, to limit disinformation and manipulation. Intelligence, understood also in a general sense as tool to collect, store, evaluate and disseminate relevant information for the protection of the security of institutions, citizens and businesses, has become a fundamental tool for understanding the "truth" of reality, especially when a war or conflicts are involved.

[2] "Security of Road Infrastructure", Final report of the Task Force C.1., PIARC 2019, Paris, France. ISBN 978-2-84060-524-9. Available in English, French and Spanish
https://www.piarc.org/en/order-library/30826-en-Security%20of%20Road%20Infrastructure

Today, a new is being fought over the **manipulation of people's minds**. The possibility of internet, becoming accessible to the entirety of the world's population already around 2030, raises in particular the issue of **consumer manipulation**, including also road users, in the looming digital dimension where not only “true and false” but also “illegal and legal” become indistinguishable. **Social networks** have become not only a “virtual square” but also enormous factories for data alteration and mystification.

Furthermore, the potential **conflict between human intelligence and AI** and its potentially devastating consequences is an issue that has raised little awareness of the consequences in the public.

Globally, **threats have increased in their complexity**, where causes and effects intertwine. As noted in daily reports, security threats to the activities of an organization can be brought by foreign or internal state and non-state actors. We have dozens of different possible threats, ever-evolving and no longer targeting only government or public entities but a much wider range of objectives, such as private infrastructure, transport and also academic sector entities. These sectors present not only physical assets such as roads and communication networks, but also, as said, the informative and intellectual capital behind them. All these mean a broad, veritable, geopolitical battlefield in which, in particular, RAs must operate.

We have threats in the **external context** of an organization which can cause damage through crimes and violence against people and things and through physical and cyber-attacks of various kinds. On the other side, in the **internal context**, insider threats may involve deliberate actions by insiders with malicious or criminal motivations, such as working with intelligence entities or competing entities. Other actions by insiders can cause damage even through simple negligence, unpreparedness or under stress situations.

The Covid-19 pandemic has caused unprecedented crises in public health, public and private safety and security for countries around the world. The pandemic has brought new difficulties for businesses and people and new opportunities for physical and cyber-attacks[3]. Many people were working remotely or from home, and the pandemic has favoured the development of IT countermeasures in relation to not only a new mental approach to work but also of online shopping and meetings[4].

Strengthening existing **security measures** or creating new ones can objectively be costly. For economic reasons or superficiality, unfortunately, the answer of many organizations to security threats is low-level, often limited to the implementation of measures, for example, limited to the control of the access of people and vehicles. A common mistake is to look for solutions based on observing other companies or previous incidents without an outlined strategy for the future.

Another mistake is thinking that security is limited to the work of police and intelligence forces. They have a central and prevalent role, but must be assisted by other important figures, ranging from local police to mayors, up to **private security and corporate structures** in charge of security:

---

[3] “Covid-19 : Initial Impacts and Responses to the Pandemic from Road and transport Agencies”, PIAR Covid-19 Response Team, 2020, 2020BN03EN, ISBN 978-2-84060-628-4.

[4] “Security and Pandemic: Application of the Concepts of Resilience for Business Continuity”, S. Palchetti, R. Mastrangelo, M. Bianchi, PIARC XVI World Winter Service and Resilience Congress - Calgary 2022. See it in LR as Sheet n.3 in Appendix B.7.

none of them plays a marginal role, nor is to be considered "second-class". Each one is called to play a part of his own, in close collaboration with the others.

Just waiting for unexpected events and reacting as they happen allows undoubtedly immediate resolutions. However, in case of repeated emergencies, such strategy entails a greater expenditure of energy than a permanent and systematic effort for security. Best practices suggest that risk is a **condition of uncertainty** which is inevitable given the context in which we live. For this reason, given that budgets are not unlimited, pre-emptive actions such as investments in company awareness even without substantial investments can be useful in producing changes and adaptations before a grey or black swan (against the unpredictable unknown) force to do so.

In this perspective, one key concept is **to be resilient to risk**, i.e., to be able to resist the effects of an event and to recover from it.[5] This attitude can be characteristic of an organization, of a system, of a community, of even an individual and constitutes a competitive advantage. The events that have taken place in recent years teach us that this attitude is an opportunity. We have seen examples of this concept during the pandemic when some companies have shown resilience towards a global, unforeseen and dramatic event, managing right from the start to ensure continuity in their activity and in the services provided, as they had adequately prepared to face crises.[4]

Fundamentally, there are issues that business and government leaders cannot avoid[6]: **how secure is the organization** in relation to the current threat outlook? What are the organizational investments made in security and what should they have been? How do they correspond to current and emerging threats? What internal knowledge is there of security incidents?

If these **questions** cannot be answered by an organization, based on existing policies and practices, there is a clear need for implementing **a security risk management**. Considering that there are probably no satisfactory answers to those questions, TF 3.1 proposed to give answers to the following questions: *Which information would be most valuable for helping RAs be aware of its threats and risks and manage them? How can we help RAs to better manage security?*

This **Report** intends to provide some answers to such questions and advise in the different areas represented by the PIARC TCs and TFs interested in security. This will be provided through prioritization of risk and recommended mitigation strategy, as well as defence measures to support decision making.

1.2.2. The PIARC Task Force 3.1

According to the PIARC Strategic Plan 2020-2023[7], the Task Force 3.1 was created for **embedding security** into the output of other PIARC Technical Committees (TC) and Task Forces (TF) and provide recommendations to them. This task dealt with issues of various nature: some are infrastructure and projects, others are operations, services and settlements:

- Operation, services and settlements:

[5] In our previous 2019 Report the relationship between security and resilience was widely dealt with (chapter 6) and the critical issues in the resilience cycle (prepare, prevent, protect, respond, recover) were also analyzed in detail in seven security case studies (chapter 7 and appendices).
[6] See also a series of general questions on security implementation further ahead in **Appendix 2** to this Report.
[7] PIARC – The World Road Association, "Strategic Plan 2020-2023", Update October 2020, http://www.piarc.org

- *TC 1.1 Performance of Transport Administrations*
- *TC 1.4 Climate change and Resilience of Road Network*
- *TC 1.5 Disaster Management*
- *TC 2.1 Mobility in Urban Areas*
- *TC 2.2 Accessibility and Mobility in Rural Areas*
- *TC 2.3 Freight*
- *TC 2.4 Road Network Operation/ITS*
- *TF 2.1 New Mobility and its Impact on Road Infrastructure and Transport*
- *TC 3.1 Road Safety*
- *TC 3.3 Asset Management*
- Infrastructure and projects:
- *TC 4.2 Bridges*
- *TC 4.4 Tunnels*

Finally, a contribution of terms and typical expressions of the specialist security issue may be envisaged to the *Terminology Committee.*

To achieve its goals, the T.F. 3.1 referred to the work illustrated in the **Report TF C.1 2019** by emphasising some parts while keeping others. Chapters 1. "*Introduction*", 2. "*Understanding the Issue*", 3. "*Security-Minded Approach*" constitute an essential starting point. Chapter 4. "*Security Risk Management of Road Infrastructure*" has been developed and expanded by the TF 3.1, becoming Chapter 2. "*Security Risk Management*" and Chapter 3. "*The Process of Security Risk Management"*. It also constitutes the basic methodology for embedding security in the activities of the concerned PIARC TCs/TF by means of security risks prioritization developed here in Chapter 4. Finally, the chapters from 5 to 8 of the previous Report 2019 constitute the primary source for the chapters on risk treatment.

This Report is also significantly based on a comprehensive recently published Literature Review (LR) (see a summary in **Appendix 1**) which collected the main knowledge available in 8 source groups: legislations and policies, standards, studies and researches, PIARC reports, other reports, manuals and books, case studies and best practices, events and situations. Among all, the international standards and in particular the ISO standard families have been taken into consideration.

1.3. INTRODUCTION TO THE REPORT AND ITS METHODOLOGICAL APPROACH

In light of the global context of risks and the **PIARC Strategic Plan 2020-2023**, TF 3.1 team has pondered on a way for embedding effectively security in PIARC TCs and TF according to the ToR, starting with a common list of threats in terms of malicious and criminal attacks brought by voluntary acts. These have recently been joined by the effects of pandemic and worldwide geopolitical crises with the unleashing of all forms of cyber threats. Therefore, the first basic question to be answered as TF 3.1 is how to provide a common **security risk management** approach, given the great variety of topics, to contribute significantly to the improvement of security and consequently resilience both of an infrastructure, a service or a settlement.

A very authoritative and consolidated body has been found in the **ISO international standards**, which deal specifically with security risk management according to **ISO 28000:2007** and **ISO 31000:2018**, completed with their correlated ISO families. They propose a broad application of

the methodology of continuous improvement of production or operations based on the so-called Deming cycle (Plan-Do-Check-Act, PDCA) that assures also the necessary holistic attitude and no silos approach of the security issue considered the complexity of the road infrastructure and transport environment.

ISO 31000:2018 is applicable to any type of risk and can be used by any type of organization, group or individuals and is not specific to any industry or sector. It provides the organizational model that an organization should develop for an effective risk management process. The ISO 31000 standard states that the security risk includes: events mainly of a malicious and/or culpable nature that can damage material and intangible assets, organizational and human resources for which an organization has or needs to ensure adequate competitive capacity in the short, medium and long term. The proposed process aims to identify, analyse, understand, manage and prevent the effects of threats to bring back the security risk within an acceptable margin or "risk appetite". At the conclusion, the process leads to the identification of the priority risks and addressing them technically.

In this Report, it is pointed out that security risk management deals with **events that have not yet occurred** and consequently we have to deal with the continuous evolution of the security risks in a national and international context. As reminded, security must indeed face a constantly evolving framework of physical and cyber voluntary attacks and criminal actions in the context of possible but unforeseeable situations, as happened in the case of the Covid-19 pandemic. No security measure lasts forever and its effectiveness has a time limit. It must be continuously monitored and improved in its effectiveness and the aforementioned Deming cycle helps to address the problem of actualizing continuously evolving risks: identify the threats, analyse the risks, evaluate them, propose the necessary measures, and then start all over again. **Terrorists and criminals** (including scammers) are always on the prowl and are generally excellent "managers" themselves.

A core part of this Report is dedicated to the **security risk assessment process**. Many techniques are available, as explained in **ISO 31010:2019**, with different levels of scope, training, expertise, complexity, effort and also qualitative and quantitative approach. **The qualitative approach** follows criteria which we can define as more humanistic, the quantitative, more scientific. The quantitative approach is suitable for all those risks where you can get data from any source to enter in the analysis model (economic, financial, industrial risks). It leads to in-depth assessments but it needs reliable databases and sophisticated calculation models. The qualitative approach is, on the contrary, purely narrative and descriptive. A mistake is to believe that **the quantitative approach**, as it is based on data and on the statistical-mathematical model, is necessarily better than the qualitative one. It depends on the objectives to be achieved and the type of risks to be analysed. Qualitative approach is necessary in case of risk related to terrorism and crime, engineering disasters, corporate risk management and other applications with the presence of human variables that cannot be categorized in a mathematical model. It is the least complex and costly and can be used for the first classification of risks, for example to promote awareness and information on threats and risks.

A **semi-quantitative approach** based on rating scales for likelihood and consequences and a risk matrix are chosen to carry out an information and prioritization of the risks for embedding security in PIARC TCs and TFs. The reasoning and discussion within TF 3.1 have been used to identify risks and assess their impact. Among the various possible methodologies, the construction of the risk

matrix that multiplies likelihood and consequence was followed. It is preliminarily based on the evaluation of the vulnerabilities in the internal and external contexts defined by the more threatened assets, the choice of the priority threats and for each of them the likelihood L, the consequences C and therefore the risk as a result of the L x C product. The result is not a simple **two-ordinal risk matrix (likelihood and consequences)** because it incorporates a preliminary vulnerability assessment based on analysis of the **external and internal contexts**. This is an essential step in threat prioritization and it is "expert-judgement based" as founded on the evaluation of the expert who draws up evaluation sheets.

A complementary or in some cases third way, trusting the **resilience** of the system sometimes can be considered and it is the best choice made when the matter is too complicated and even expensive for the organization. It has its approximations, as well, and these must be taken into account since they may lead to shortcomings within the organization, acceptance of a high level of risk in general, and also economic waste.

In conclusion, security deals with the **world as an open system**. Something that cannot be predicted mechanically in the premises. The world is a creative and surprising organism in all senses, both positive and negative. In the latter case, it can bring damage, death and destruction in different ways. In light of the complexities and uncertainties to be considered, some errors of evaluation can be possible in our work as an empirical method based on the team perception of risks was followed. It would be outside the scope of this Report to make an exact measurement of its effectiveness and it would not have been possible to remove an existing source of error in the subjective judgment of likelihood and consequences.

The TF 3.1 team is aware of these limitations which are part of any method that uses subjective judgments in **risk analysis**, therefore risk matrices will be proposed with caution by providing an explanation of the judgments embedded in them. It is clear, that the results of the analyses carried out are indicative and should not be used to make decisions. However, the conclusions, also scrutinized by the competent TCs and TFs, appear to be ultimately at least reasonable and useful as information to improve awareness on security.

As well known, the **target** of this final Report is not to give answers to incidents that occurred but provide a reference for PIARC TCs and TFs to prioritize their security risks. However, the challenge is also to reach the PIARC public in general, consisting of administrations, organizations and professionals involved in road and road transport to be stimulated to assume a predictive posture for the protection of their infrastructures and transport activities from any kind of threats and risks. Our task was to convey clarity and stimulate the ability to react consciously, creatively and responsibly in the face of unforeseen or adverse events as an incident, catastrophic event or major natural disaster.

1.4. TARGET AUDIENCE

This **Report is addressed** to decision makers, road owners and managers, operators, security experts, risk analysis specialists interested in planning, design, implementation, operation, maintenance, refurbishment and supply related to road infrastructure and transport.

The **challenge** of this Report is reaching the audience of the road stakeholders which are very reluctant to take security risks into consideration, contrary to what other transport modes, such as air, maritime and rail transportation have been doing for decades.

1.5. Structure of the Report

This Report explains how to defend against criminal and terrorist activities in relation to various road issues proposing a methodology to prioritize threats and risks.

In **Chapter 1 – Introduction**, we provide basic definitions with the acronyms and terms used. Furthermore, a framework is outlined of the work in relation to the current state of the art, to the works already published on security within PIARC and to the methodologies relating to the security risk assessment process.

In **Chapter 2 – Security Risk Management**, we deal with the philosophy of security risk management in the light of international reference standards.

In **Chapter 3 - The process of security risk management**, we concretely address the design of security measures in the road sector with a series of in-depth studies.

In **Chapter 4 - Recommendations for PIARC TCs-TFs**, we apply the security risk management process to some specific issues within PIARC to learn how to protect ourselves from criminal and terrorist threats.

In **Chapter 5 – Conclusions**, we try to reflect on some evidence that has emerged from the work carried out, on the possible traps and ambiguities of security and explore some future perspectives on the subject.

In the **Appendices** we put together a series of helpful documents to complete the cognitive framework on security applied to roads.

In **Appendix 1**, we propose a synthesis of the Literature Review Report, "PIARC TF 3.1 – Literature Review – Documents Relevant to Road Infrastructure and Transport Security", developed by this Task Force and published in 2022 in the PIARC website.

In **Appendix 2**, we propose an interesting application of the ISO standard 28000 in the form of a checklist for a preliminary "in-house" assessment of the security level of an organization which can be useful in general.

In **Appendix 3**, we address the topic of road safety and security in developing countries with reference to the sub-Saharan area.

In **Appendix 4**, we propose a reasoned summary of the papers presented by the members of the T.F. 3.1 at T.F. 3.1 Technical Session at the 27th World Road Congress in Prague on October 6th, 2023.

In **Appendix 5**, we deal with cyber-attacks and IT systems and new risks coming from artificial intelligence in the field of road infrastructure with some examples and final recommendations.

2. SECURITY RISK MANAGEMENT

2.1. RISK AND RISK MANAGEMENT

The **concept of risk** is addressed in all fields, not only security but also finance, safety engineering, health, transport or supply chain management, etc. In any future activity such as the functioning of an organization or of a system (also in a broad sense including natural phenomena) there is a degree of risk, in relation to the negative and undesirable consequences of such activity. As shown in chapter 1.4 in the LR, risk is a broad concept summarized as follows:

a) the exposure to a context in which there are uncertainties;
b) the possibility of an unfortunate event happening;
c) the different level of intensity of the negative and undesirable consequences.

Among several alternatives, the **measurement of risk** (even intuitively) can be seen in terms of combination of likelihood and consequences that an undesired event may occur.[8] Probability can be the combination of threat and vulnerability. Consequences or effects can be determined in terms of human life, material damage, financial or reputational value.

Among the very many possible **definitions of risk**, we can summarize here the following:

"A potential loss, disaster, or other undesirable event measured with probabilities assigned to losses of various magnitudes. It is the product of the probability (that a threat occurs) and the impact/consequences (expected/calculated) if the threat occurs."

The **decision makers** of an asset, a settlement or an activity have the responsibility of eliminating and limiting the risks caused by threats, at least to the extent possible. This is the risk management activity for which, as the mentioned chapter 1.4 in the LR, we could consider the following definition: *"The identification, analysis and prioritization of risks followed by coordinated and economic application of resources to reduce, monitor, and control the probability and/or impact of unfortunate events. "*

2.2. INTERNATIONAL STANDARDS AND SECURITY

The sources of some **main international standards** have been taken into consideration and their impacts on security (from 1 - low to 5 - high) have been indicatively and tentatively evaluated in relation with the selected PIARC TCs and TFs in the following matrix (Fig. 2):

- ISO 9000 family on quality management
- ISO 31000 family on risk management
- ISO 14000 family on environmental management
- ISO 28000 on security management systems for the supply chain
- ISO 22300 on societal security and resilience
- ISO 27000 family on information technology
- ISO 28000 family on security of supply chain
- ISO 39000 family on driving

[8] The classic definition of triplet "scenarios, consequences and probabilities" (s_i, p_i, c_i), where s_i is the i^{th} scenario, p_i is the probability of that scenario, and c_i is the consequence of the i^{th} scenario, i =1,2, …N , has been founded by Kaplan and Garrick (1981) for the nuclear industry.

- ISO 45000 on personnel and labour
- IWA 14 family on vehicle security barriers
- CEN family on security

ISO & relevant Standards	9000	14000	27000	28000	31000	20858	22300	39000	45000	IWA-14	CEN/TR 16705	ADR	Envision
	Management	Environment	Informatic	Supply Chain	Risk Management	Perimeter	Security Resilience	Drive	Personnel and Labor	Crash testing	Perimeter	Dangerous goods	Sustainable infrastructure
TC 1.1 Performance of Transport Administrations	5	3	4	3	4	1	3	1	1	1	1	2	5
TC 1.3 Finance and Procurement	2	2	2	2	3	1	1	1	1	1	1	1	5
TC 1.4 Climate change and Resilience of Road Network	1	4	2	3	2	1	3	3	2	2	2	3	5
TC 1.5 Disaster Management	1	4	4	4	5	1	3	2	2	2	3	5	5
TF 1.1 Well-Prepared Projects	5	5	3	5	5	3	5	1	1	1	3	2	5
TC 2.1 Mobility in Urban Areas	4	1	5	4	2	1	3	1	1	1	1	1	3
TC 2.2 Accessibility and Mobility in Rural Areas	1	2	1	2	1	1	4	1	1	1	1	1	3
TC 2.3 Freight	3	3	4	3	2	3	3	5	5	2	3	5	2
TC 2.4 Road Network Operation/ITS	3	2	3	3	2	2	4	1	1	1	2	4	4
TF 2.1 New Mobility and its Impact on Road Infrastructure and Transport	2	1	5	2	4	1	2	1	2	2	1	2	1
TC 3.1 Road Safety	3	2	2	1	3	2	3	3	3	1	2	5	3
TC 3.3 Asset Management	3	2	3	3	2	2	2	1	3	1	2	4	3
TC 4.2 Bridges	3	4	3	1	3	2	5	1	3	1	1	3	3
TC 4.4 Tunnels	1	1	3	4	3	3	4	2	5	1	3	3	3
TF 4.1 Road Design Standards	3	3	3	4	4	5	5	1	1	5	5	2	5
Terminology	1	2	5	5	5	3	5	2	3	3	3	5	3

Fig. 2 - International Standards and impact on security towards the selected PIARC TCs-TFs

2.3. ISO 28000 AND THE SECURITY MANAGEMENT SYSTEM

International standards have been investigated starting from the standard for **security management** ISO 28000:2007[9]. It establishes the criteria by which an organization can manage the security environment and determines whether adequate security measures have been implemented. This security risk management methodology complies to the general quality and project management principles for ensuring continuous improvement of business results: plan, do, check, act **(Fig. 3)**. This process in four steps is commonly known as **PDCA cycle** (Plan-Do-Check-Act) or Deming's wheel or cycle[10] **(Fig. 4)**:

[9] ISO 28000:2007 – Specification for security management systems for the supply chain (revised in 2022). See in LR, Appendix B.2 "Standards", Sheets from n.66 to n.75.

[10] This process forms the basis of the international standards ISO 9001, 14001, 28000, 31000. The idea of a PCDA cycle uses the hypothesis-implementation-verification-new hypothesis scheme. This is a universally known methodology in order to achieve with success the objectives of quality improvement with tangible and lasting benefits. In the early 1950s, the American engineer W.E. Deming introduced this cyclical methodological approach according to which quality management means a commitment to the continuous improvement and innovation of products and processes (Deming, W. Edwards, Out of the Crisis, MIT Press, 1986).

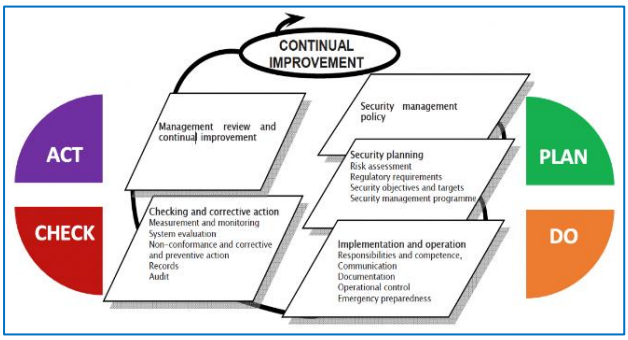


Fig. 3 - Concept of the continuous quality improvement associated with the application of the PDCA cycle in international standards

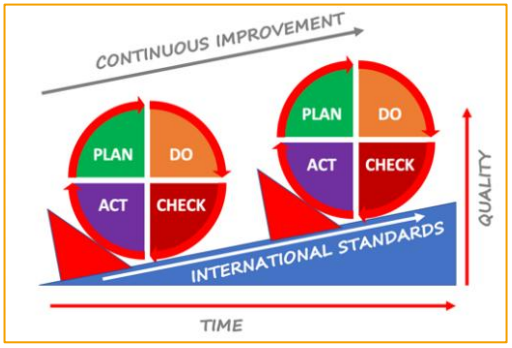


Fig. 4 - Security Management System (elaboration from ISO 28000:2007)

I. **PLAN** – Security management policy and planning: determine the goals and recipients. Determine methods for achieving goals. Starting from the knowledge of its status, the organization defines its security policy and establishes the objectives and processes necessary to obtain the expected results. This is normally the task of top management. Based on the policy view, this part of the process carries out the updating of the security policy and plans. This phase includes risk assessment.

II. **DO** – Implementation and operation: doing the job, training and education. During this phase, the organization assesses and manages security risks, organizes and implements the related processes for the mitigation and control of security risks, also communicating and involving staff and providing adequate resources and training.

III. **CHECK** – Checking and corrective action: check the effects of implementation. The organization monitors and measures the processes concerning the security policy, the risk control objectives, the legal aspects and other requirements, and reports on the results also through audit measures. The organization will review security breaches or gaps and ensure corrective actions.

IV. **ACT** – Management Review and Continual Improvement: take appropriate action. The organization reviews its performance enabling corporate management to take decisions to continually improve the performance of the security management system in response to lessons learned and data collected, with respect to both specific areas and the overall cycle.

In **Appendix 2**, an interesting application of the ISO standard 28000 is also proposed in the form of a checklist for a preliminary "in-house" assessment of the security level of an organization[11].

2.4. ISO 31000 FAMILY AND RISK MANAGEMENT

ISO 31000 is the international best practice guideline regarding risk management, which is widely accepted, generic and open to understand risk, manage any type of risk and in particular the one deriving from security. The application of this guideline can be customized to any organization and its context and be applied to any activity at all levels. Therefore, we will follow the process defined by ISO 31000 that takes place within what is defined in ISO 28000, which has a similar

[11] Based on the document "Protective Security Management Systems (PSeMS)", by the Centre for the Protection of National Infrastructure, CPNI (UK), 2018.

approach, as both follow the quality and project management field for ensuring continuous improvement established by ISO.

The structure of the risk management process is broken down into the following steps[12] (see Fig. 5):

- establishing the context (internal and external),
- risk assessment (identification, analysis, evaluation),
- risk treatment,
- risk monitoring and review.

Fig. 5 - The process of risk management (elaboration from ISO 31000:2018)[13]

One core concept in risk management is **uncertainty**. It can take on various aspects:

- it is inherent in the indefinite nature of phenomena (aleatory uncertainty);
- it is the effect of a lack of knowledge (epistemic uncertainty);
- it is linked to the evaluations of professionals, as experts' review are based on a combination of factual and experience-based considerations, or to organizational and business decisions (decisional uncertainty);
- it is consequent to the mutation of contexts (contextual uncertainty).

It must be recognized that uncertainties are an unavoidable reality. Consequently, risk management has to be **continuously corrected and updated**, following every change in the business or in the infrastructural context or in the organizational process or due to the grafting of technological innovations. Detecting timely change, including first of all threats, must generate reactions, which change the state of the organization, generating a mutation of vulnerabilities. This motivates the need to apply a **no-silo, holistic and security-minded approach** (see our previous Report 2019). Uncertainties make it necessary to build resilience to cope with unexpected circumstances. Also, uncertainties themselves make the decision-making process complex and, therefore, this latter is also clearly uncertain.

But it seems necessary to underline the fact that objective risk management is not eliminating risks, but only giving adequate information and possibly managing and preventing them. As outlined in ISO 31000 standard, the risk management process includes indeed, in addition to a

[12] See in LR, Appendix B.2 "Standards", Sheets from n.76 to n.70. In Sheet n.80 the ISO/Guide 73:2009 "Risk management – Vocabulary" became recently ISO 31073:2022 and provides the definition of terms related to risk management.
[13] ISO 31000:2018 - Risk management – Guidelines.

risk management plan, a plan for the **communication and consultation** of stakeholders to provide basic information on the priorities on threats even if no decision-making actions arise.

Risk management has become an integral part the **project management**. It appears clear that the implementation of a risk management process that integrates security is likely to have a direct impact on the general management processes and business of an organization.

ISO 31000 explicitly refers to the guidelines and general principles for setting up a system management based on quality according to the **ISO 9001** standard of 2008[14]. This voluntary standard, widely adopted and used by companies and organizations of various types, allows an organization to evaluate its ability to meet the requirements established by the customer, by the legal requirements and by the organization itself.

[14] ISO 9001:2008 - Quality management systems - Requirements. See in LR, Appendix B.2 “Standards”, sheet n.1.

3. THE PROCESS OF SECURITY RISK MANAGEMENT

In the process of security risk management, the structure established by **ISO 31000** (Security Management System) and **ISO 28000** (Security Risk Assessment) is followed. In this chapter 3 the basic principles of the process of Security Risk Management will be outlined which will be later be analysed further in the following chapter 4, in relation to the specific issues of interest of the PIARC TCs and TFs.

3.1. ESTABLISHING THE CONTEXT

Establishing the context is understanding the world in which an organization is located and dealing with the uncertainties generated by the interaction with the environment and, as far as possible, controlling the consequences. Any organization or asset, due to the fact of carrying out an activity or providing a service, is characterized by its **external context** in which it is located and its own **internal context**. From a security standpoint of view, it is necessary to study how the organization or asset interact externally and internally by dividing their activity into macro-areas of potential vulnerability where they can be subjected to threats which can materialize in both contexts of an asset or an organization.

Schematically, an external context can be made up of 5 macro-areas of potential vulnerability **(Fig. 6)**:

- geographical;
- infrastructural;
- socio-economic;
- political;
- territorial.

Likewise, the internal context can be characterized by 8 macro-areas of potential vulnerability **(Fig. 7)**, for example:

- external areas;
- external perimeter;
- internal areas;
- offices (staff included);
- production/operation facilities;
- control/data centre;
- storage;
- laboratories**.**

EXTERNAL CONTEXT		
	MACRO-AREAS OF VULNERABILITY	ELEMENTS OF VULNERABILITY
1	GEOGRAPHICAL	Locations exposed to any external action such as natural disasters (floods, earthquakes, tsunamis, hurricanes, volcanoes, etc.), pandemic and others for their security effects
2.1	INFRASTRUCTURAL	Proximity to sites of importance for security purposes (chemical centres, sites at risk of major accidents, fair and exhibition sites, etc.)
2.2		Proximity to hubs or networks of (inter)national importance (roads, motorways, railways, airports, ports)
2.3		Proximity to police forces sites, military settlements, fire brigades
3.1	SOCIO-ECONOMIC	Areas with a high unemployment rate and a high state of material and social need
3.2		Possibility of media attacks, by competitors or customers
4	POLITICAL	Unstable political context , political figures and V.I.P*
5.1	TERRITORIAL	Presence of micro-crime (theft, robbery, murder, fire, extortion, money laundering, usury)
5.2		Presence of organized crime, terrorism
5.3		Activism of anarcho-insurrectionist movements, condition of confessional or racial segregation

Fig. 6 - Areas and element of vulnerability due to the external context

INTERNAL CONTEXT		
	MACRO-AREAS OF VULNERABILITY	ELEMENTS OF VULNERABILITY
1	EXTERNAL AREAS	Roads, parking spaces, service vehicles, visitors and suppliers vehicles, variable message portals, people
2	EXTERNAL PERIMETER	Accesses, protections
3.1	INTERNAL AREAS	Structures (for tunnels: descendants, escape facilities, ventilation wells, for bridges: deck, hangers) and management system
3.2		Buildings (people, offices)
3.3		Roads (accesses, entrances, exits, parking spaces)
3.4		Vehicles (company, business, employees, visitors, suppliers)
4.1	OFFICES	Staff and managers
4.2		Visitors and suppliers
4.3		Computer systems and office equipment
4.4		Information/communication
5.1	PRODUCTION/OPERATION FACILITIES	Work areas (service stations, toll stations)
5.2		Installations (electrical power supply and distribution, lighting, signalling, over-weight vehicle detection)
5.3		Emergency (fire-fighting systems, smoke and hot gases control, air quality)
5.4		Consumables (dangerous)
6	CONTROL/DATA CENTRE	Server, SCADA systems
7.1	STORAGE	Raw materials (dangerous)
7.2		Finished products
8.1	LABORATORIES	Staff, specialists, experts
8.2		Offices
8.3		Computers and digital devices

Fig. 7 - Areas and element of vulnerability due to the internal context

3.2. RISK ASSESSMENT

3.2.1. General

According to the ISO 31000, the sub-process of risk assessment is composed by three subsequent steps (see **Fig. 8**).

Fig. 8 - Approach to risk assessment

Risk identification and analysis must be considered as a **continuously iterative process**: we identify threats and by analysing them in terms of likelihood and consequences, then we identify further threats and so on in a cyclic manner. Risk evaluation provides a rating of different risks.

The goal of **risk assessment sub-process** is to make an examination of all risks of the organization or asset and to recognize the most significant risks and threats. This output is fundamental to carrying out the following steps of the process: prioritization and definition of measures to cancel them or put them under control.

3.2.2. Risk identification

Since it is placed in an external context and consisting also of an internal context, any organization or asset is exposed to various types of **security threats**. These threats are the result of intentional acts, accidents, natural events due to their multiplier effect, that may cause damages.

Risk identification aims to **identify, classify and document** threats that can involve in general an infrastructure, an activity, a service provided in the external and internal contexts. The identification may be based on statistical data analysis or formulating a reasonable list of threats based on the experience and a subjective analysis of the security professional.

A comprehensive and commented checklist of 41 security threats is proposed in the **Figures 9-1, -2,-3,-4**:

Fig. 9-1 lists the crimes against only things or only people;

Fig. 9-2 lists the crimes perpetrated at the same time both against things and people;

Fig. 9-3 lists the crimes referable to acts of terrorism and/or organized crime aimed at people and things;

Fig. 9-4 lists the unattended and unforeseeable event or harmful voluntary acts causing terrorist or criminal attacks or disasters.

The proposed lists of threats are based on the experience of past and recent relevant critical events and on the TF C.1 2019 Report, where a first checklist of possible physical, cyber-physical and cyber threats from terrorism and crime was proposed, mentioning also the pandemic. [15]

[15] See "Security of Road Infrastructure", Final report of the Task Force C.1., PIARC 2019 and in the LR Appendix B.4 PIARC Reports, Sheet n.11 "Project Related Risks", output of Working Group A3.2, PIARC Technical Committee A.3 – Risk Management, 2019.

	SECURITY THREATS	DEFINITIONS	NOTES
	Crimes against people		
T 01	**Aggression**	*Spoken or physical behaviour that is threatening or involving harm to someone or something, without or with sexual implications.*	Aggression can be verbal and physical. Assault on employees. Violent activities in general. Intrusion of demonstrators. Armed intruders. Stabbings. Poisoning. Attack on security officers. Workplace violence. The aggression can also affect users of bridges and tunnels, passengers in automated vehicles and operating staff.
T 02	**Robbery**	*An act done by a single or small criminal gang of stealing from somewhere or someone with threat or use of force.*	It consists in the act or practice of stealing things, eg. keys, wallet, bags, vehicles.
T 03	**Mugging**	*A planned act implemented by an organized criminal gang of quick violent attacking and robbing an organization to steal valuables and money.*	It is a violent and quick attack, well planned and organised, carried out by an organized gang composed of various members and endowed with important means to steal significant amounts of money or valuables.
T 04	**Taking hostages**	*Someone being taken prisoner by hostiles in order to force the other people involved to do what the enemy wants.*	e.g. taking hostages in a bank or in a post office or school bus hijacking with children on board
T 05	**Kidnapping**	*To take a person away illegally by force, usually in order to demand money in exchange for releasing them but it may also not involve a request for money.*	Kidnapping of employers. Videocameras are very useful in case they are recorded.
T 06	**Mobbing**	*Systematic persecution of an individual within their own family, social, working context by family members, colleagues or superiors, usually consisting in acts of social exclusion, psychological violence, professional sabotage, groping which may extend to physical violence.*	Video recording can show mobbing acts on the street and identify car plates.
T 07	**Stalking**	*Repeated and intrusive persecutory behaviour, such as threats, harassment, phone calls, unwanted attention, or violence, by a person outside the victim's usual context.*	Person in charge of the procurement process may be nugged to divert the course of a work; stalking acts can be recorded as well as registration of car plates; a form of stalking are incorrect driving behaviors to disturb the driving of others eg. the use of high beams, overtaking or ramming attempts.
T 08	**Corruption**	*Illegal, vicious,or dishonest behaviour, especially by people in positions of power.*	
	Crimes against things		
T 09	**Theft**	*The act of dishonestly taking something that belongs to someone else, keeping it: things, vehicles, cargo, personal data, equipment.*	Theft of raw materials and finished products. Theft of machinery and equipment. Rest areas must be appropriately designed and controlled by RAs to prevent crime.
T 10	**Vandalism**	*The crime of intentionally damaging property belonging to other people or environment.*	Vandalism on the road eg. control unit, traffic light off in the tunnel due to the power being cut, fuel theft, damage to control sensors.
Til	**Graffiti**	*Words or drawings, especially humorous, rude, or political, on walls, buildings or transport means.*	
T 12	**Arson**	*The crime of intentionally starting a fire in order to damage or destroy thin gs, in particular a building (with or without involvement of people).*	It can also refer to the intentional burning of other things such as vehicles and woodland. An arson can destroy, seriously damage or just temporarily put a bridge or a tunnel out of action.
T 13	**Throwing objects to damage**	*To propel something with force through the air to damage people or things.*	Projection of objects from bridge parapets
T 14	**Violation of private property, unauthorized entry**	*Anyone who arbitrarily invades the land or buildings of others, public or private, in order to occupy them or otherwise make a profit.*	Unauthorized entrances to the central porter's lodge, to the vehicle guardhouse. Perimeter damage.
T 15	**Piracy**	*The act of attacking any means of transport (trucks, trains, ships) in order to steal goods from them.*	Video control for dissuasion purposes

Fig. 9-1 - Security threats caused by terrorism and crime

	SECURITY THREATS	DEFINITIONS	NOTES
	Crimes against people and things		
T 16	**Malicious or non-compliant personnel, sabotage**	*Malicious behaviour of personnel is intended to harm other people or cause physical damage to things as someone else's properties, assets or equipment.*	It includes : failure to comply with procedure and behaviors required by regulations, lack of compliance, doubtful professional ethics, managerial incapacity, theft of intellectual property, infidelity, secretly becoming part of a group in order to get information or to influence the way that a group thinks or behaves, troublemaker drivers in transport, mafia organization in subcontracting, unauthorized access, criminal infiltration, fraud, that is, an act aimed at harming a right of others by deceit. It should also be considered: the use of false policemen, false road accidents, false road detours, simulations of crime.
T 17	**Malevolent communications**	*It is the use of telecommunications products or services with the intention of reporting a bomb (real or false),or illegally acquiring money from, or failing to pay, a telecommunication company or its customers.*	It causes economic damage. They can be anonymous threatening phone calls or phone fraud, or more generally communications fraud, that is the use of telecommunications products or services with the intention of illegally acquiring money from, or failing to pay, a telecommunication company or its customers. To fight such crimes, certainly one of the most efficient methods is using telephone eavesdropping, which can prove very useful in gathering intelligence to fight tax evasion, scams and financial offences of several kinds.
T 18	**Disclosure of information, espionage**	*The act of making known (voluntarily or involuntarily) or steal sensitive information (e.g. confidential personal or commercial data, security measures or valuable goods being transported by personnel, operators, drivers).*	Theft of confidential information. Theft of know-how. Theft of PC. Dissemination of confidential information on asset management or on the movements of dangerous goods or valuables. Capture of information by activists. Military or police convoys captured by video cameras. Spying by competitors. The Ell's GDPR is a reference for the use, collection and protection of personal data with effects on the conduct of company affairs, on police activities, on the functioning of the internet.
T 19	**Misinformation**	*Incorrect or misleading information.*	Misinformation can relate to incorrect or misleading news of any nature, whether of journalistic origin, from social media or provided by the road mobility information system. For example, an untrue information about a compulsory exit from a motorway can be obtained to direct traffic in order to carry out a robbery or other crime. This can happen due to a hack and can also harm people. Misinformation can cause serious damages to reputation.
T 20	**Civil protests and strikes**	*A strong complaint expressing disagreement, disapproval or opposition and refusing to continue working due to social, political, environmental reasons or working conditions, wage levels or job loss.*	Civil protests can have consequences for people and things. Protest demonstrations. Intrusions of demonstrators. Demonstrations offsite. Blocking entry and exit flows. Disgrunled employee. It may be a choice to cause damage only to street furniture or vehicles to give strength to the protest but damage to people including members of the police can also happen accidentally. Protesters at toll booths or on the road can create blocks.
T 21	**Illegal transit**	*Prohibited access in certain areas or roads to specific categories of vehicles. Oversized vehicles.*	Electric kick scooter accessing to motorways, ring roads, prohibited urban areas can cause incidents. Oversized vehicles can provoke damages.
T 22	**Illegal transport**	*Prohibited transportation of persons or goods. Overloaded transportation.*	Prohibited transportation of persons or goods and overloaded transportation must be considered.

Fig. 9-2 - Security threats caused by terrorism and crime

	SECURITY THREATS	DEFINITIONS	NOTES
	Crimes referable to manifestations of terrorism and or organized crime aimed at people and things		
T 23	**Attack with vehicle used as a weapon (VAAW)**	*To try to injure or kill by means of a vehicle as a weapon, with or without the use of explosives .*	Terrorist attacks on powerplants, equipment, logistic facilities, employees. Included attack with vehicles carrying dangerous goods. Any attack can materialize in both external and internal contexts. Attacks can pose a threat to other modes of transport as well.
T 24	**Attack with parked vehicle borne improvised explosive device (VBIED)**	*To try to injure or kill using a VBIED parked close to an asset as target (internal or external to the site).*	Idem
T 25	**Attack with encroaching VBIED**	*To try to injure or kill using a VBIED exploiting gaps in perimeter protection or tailgating an authorized vehicle. Deception is used when the VBIED replicates a legitimate vehicle. Duress is used when a security officer is forced to open a vehicle access control point (VACP) or an authorized driver is forced to take an IED within his or her vehicle.*	Idem
T 26	**Attack with penetrative ram vehicle**	*To try to injure or kill using a ram vehicle (possibly a VBIED) breaching a building or physical perimeter.*	Idem
T 27	**Attack with suicide terrorist**	*To try to injure or kill using a person who has a bomb hidden on his or her body and who at the same time injures or kills himself or herself.*	Idem+E39:E48
T 28	**Attack with terrorist and/or threatening phone calls**	*To anticipate a real or presumed act aimed at injuring or killing one or more people, by a terrorist or threatening phone call.*	Idem
T 29	**Attack with envelope or letter bomb**	*To try to injure or kill using an envelope or letter bomb.*	Idem
T 30	**CBRNE attack**	*To try to injure or kill using a cargo, a package, an envelope, letter or other containing chemical, biological, radiological, nuclear substances, and high yield explosives (CBRNE).*	An attack CBRNE may require a bomb explosion (dirty bomb).
T 31	**Ballistic attack, bombing, blasting**	*To try to hit with objects that are shot or thrown through the air, such as a gun, missile, torpedo or airplane. Attacks on a place or area using bombs. To explode or destroy something or someone with explosives, or to break through or hit something with a similar, very strong force.*	Also airplane or ship (in case of a bridge) filled with explosives. Sniper. Blasting can have an impact outside a building, structure, or inside a tunnel.
T 32	**Cyber attack with malware infiltration**	*Attack involving, using, or relating to computers, especially the internet, through a computer software that is designed to damage the way a computer works.*	The attack can occur through internet-connected things that integrate digital elements (cyber-physical, IoT)
T 33	**Cyber attack with subtracting data for ransom**	*Attack involving, using, or relating to computers, aiming at taking away data in order to demand money in exchange.*	Idem
T 34	**Cyber attack with direct manipulation**	*Attack involving, using, or relating to computers, aiming at controlling or modifying data without anyone knowing it.*	Idem
T 35	**Cyber attack to the management system**	*Attack involving, using, or relating to computers, aiming at preventing a system or a process of a control centre of a tunnel, of a bridge, of urban mobility from continuing as usual or as expected .*	Cyber attacks can affect AI controlling vehicles resulting in the loss or manipulation of the vehicle itself.
T 36	**Attack with Unmanned Vehicles (UAV or drone; AUV or UUV)**	*Attack involving a military aircraft (Unmanned Aerial Vehicle) ora drone (hobbyst's aircraft) ; Autonomous or Unmanned Water or Underwater Vehicle which is guided autonomously by remote control to interfere with or destroy targets.*	Drones/UAV can be a threat to people and things, they can be armed with weapons and strike even in confined spaces such as through windows or ducts. They can cause damages through ventilation systems and windows with gas and a few kgs of explosives. UUV are used by drug traffickers to move goods autonomously ; they can be used to attack commercial shipping, oil platform, port logistic platforms or undersea communication cables.

Fig. 9-3 - Security threats caused by terrorism and crime

	SECURITY THREATS	DEFINITIONS	NOTES
	Unattended and unforeseeable event or harmful voluntary acts causing terroristic or criminal attacks or disaster		
T 37	**Pandemic, epidemic, epidemic outbreak**	*A disease due to a virus that exists in large areas of the world or in almost all of a group of people or in an area more or less delimited, causing serious illness and death of people. Terrorists or criminals can take advantage of it for their purposes such as cyber - cyber-physical - physical attacks.*	Covid-19 has revealed how pandemics, in addition to direct damage in terms of human lives, can sink the economies of the countries of the world by paralyzing in whole or in part, for a shorter or longer period, economic activities. The effect of pandemic on road network showed a strong initial impact on operations and construction. Afterwards, with specific training and adequate procedures the effects can be reduced. Financial risk can be caused to asset management due to the reduction of traffic. A higher threat can be the white war for the use of vaccines which, with an abuse of disinformation, fakes and social media, can create social instability and tensions between countries and within them.
T 38	**Natural disasters and climate**	*Events that can modify the enviroment and the social context in an area or in almost all the planet, for a time or permanently.*	These events can be threat multipliers. They can cause conflicts, social unrest and death of people of which terrorist or criminals can take advantage for their purposes such as cyber an physical attacks. A natural disaster can result in a blackout which creates the conditions for a criminal or terrorist attack. Climate change can create the conditions for a criminal or terrorist attack.
T 39	**Blackout**	*An electrical or radio power failure creates the possibility of a criminal or terrorist attack.*	Power failure or interruption. Data network interruption. Interruption of communication networks, jamming of radio networks.
T 40	**Disaster propagation from neighboring infrastructures**	*A disaster such as an explosion, a fire or even the diversion of a vehicle carrying dangerous goods can spread from the road to other infrastructures and vice versa.*	
T 41	**Geopolitical crises, armed clashes or combats, revolutions, uprisings**	*Condition that, for political or social reasons or due to criminal activity, causes tension in an area between opposing entities that can give rise to actions or clashes between armed groups up to the mobilization of national armies. The conflict can be conducted on two fronts: physical and virtual (hybrid war).*	The result is the change from a condition of political and social stability to one of instability which can lead to changes in the existing status quo. Each activity is perturbed for a more or less long time until a new equilibrium is reached which may differ from the initial one. The war fought on the web intends to steal information, tamper with systems, shut down vital infrastructures, and more. The consequences can have actors not directly involved in the conflict, including civilians.

Fig. 9-4 - Security threats caused by terrorism and crime

The **concept of threat to things or people is in itself abstract** if not contextualized, that is, related to the external and internal context of the property, the organization, the person. From the combination of the threat and the insecurity of the context arises the possible materialization of the effects in terms of damage according to the definition of risk illustrated in the previous chapter 2.1. Consequently, the common mistake of **confusing threat and risk**, which are two conceptually distinct terms, should not be made. To introduce the intrinsic characteristic of the context considered as criticality or weakness, the concept of vulnerability can be introduced which will be explained later (see next chapter 3.5.1.).

The identification of the risks to be assessed is an integral part of the risk management process: the **risks can be different** above all according to the type of organization or asset or infrastructure and to the internal and external context in which it operates and also in relation to the choices and behaviour of the attacker, criminal or terrorist.

Among the risks, the nuclear one is not considered since the resulting catastrophe would imply profound repercussions on a global scale, likely marking the end of modern civilization as we know it.

3.2.3. Risk analysis

Within the ISO 31000 family, ISO 31010:2019[16] provides guidance on the selection and application of **various techniques** which are used to analyse risk featured in ISO 31000. In ISO 31010 possible techniques, benefits, efforts, limitations are also described.

One of the most common methods in risk analysis uses the **likelihood/consequences matrix** (also known as risk matrix) and risk is represented by a single likelihood/consequences couple. It displays risks according to their likelihood and consequences and combines them to display a rating for the significance (magnitude) of risk.

The **risk matrix** is used to compare risks and has application at any level in an organization, asset or infrastructure. It is commonly used as a screening tool to examine the risks that have been identified, in particular to define which risks must be considered a priority and therefore highlighted at management level.

Qualitative, quantitative, semi-qualitative or **semi-quantitative approaches** for evaluating likelihood and consequences are illustrated in ISO 31010:2019. The semi-quantitative one is based on descriptive and ranking scales for likelihood and consequences. In the quantitative approach, measures of likelihood and consequences are expressed on numerical scales and processed on the basis of algorithms. This needs a scientific approach based on modelling, databases and statistics. The semi-qualitative and semi-quantitative techniques are intermediate processes.

The **qualitative method** is used in situations, as in security issues, where threats are not quantifiable in a deterministic way or in situations that do not justify the time and effort for a quantitative analysis based on computing models. It is simple but not trivial, however demanding professional competence, and its applications are widespread in almost any areas. In the approach of TF 3.1, we excluded to follow the quantitative solution due to its complexity, burden, and impracticability without the application of sophisticated models, but a semi-quantitative approach based on rating scales and risk matrix was therefore chosen for the prioritization of risks in the different PIARC TCs and TFs.

The two scales of **likelihood and consequences** are placed on the axes of the risk matrix. Scales can have any number of levels (three, four or five level scales are the most common) and the ratings can be given as numbers, words or letters which refer to numerical ranges. In the scope of this security Report, they are only qualitative. Numeric descriptions are commonly used to define the scale levels, and each level of the two scales shows a significant increasing magnitude than the one before.

The **scale likelihood** should span the range of the threats relevant to the risk analysis, as for example in **Fig. 11**[17]. In our case the **scale of consequences** reports only negative ones. It must be closely connected with the main concerns of the organization and should extend from the lowest to the highest credible consequence of interest. An example of adverse consequences rating is shown in **Fig. 12**[15].

[16] ISO 31010:2019 – Risk management – Risk assessment techniques. See in LR, Appendix B.2 “Standards”, Sheets n.78.
[17] Re-elaboration from ISO 31010:2019, Annex B chapter B.10.3.

	CONSEQUENCES			
RATING	Financial	Infrastructure	Mobility	Etc.
e	Max credible loss	Irreversible significant harm		
d				
c				
b				
a	Minimum of interest	Minor damage		

Fig. 11 - The likelihood rating

	LIKELIHOOD	
RATING	Descriptor	Descriptor meaning
e	Likely	Expected to occur within weeks
d		
c		
b		
a	Remotely possibile	Theoretically possible but extremely unlikely

Fig. 12 - The consequences rating

Fewer likelihood and consequences levels may be added and the scales may have even more than five points, depending on the context of the organization or asset.

In practice, for the purposes of TF 3.1, among different approaches, classifications based on **verbal expressions and related numeric values** are considered (**Fig. 13 and 14**). The likelihood and consequences scales must be developed by adapting them to the specific context of the organization, assets or infrastructure (typology and size) using appropriate levels to be verified with the stakeholders.

1.	RARE OR VERY UNLIKELY	>20 years	< 10% of cases
2.	UNLIKELY	every 10-20 years	< 33%
3.	MODERATE OR POSSIBLE	every 4-5 years	< 45 - 50%
4.	LIKELY	once a year	> 60%
5.	ALMOST CERTAIN OR VERY LIKELY	once a month	> 90%
6.	COMMON	every week	> 99%

Fig. 13 - Scale of likelihood of a threat

1.	INSIGNIFICANT OR NEGLIGIBLE	damage 1.000 € - 5.000 €
2.	MINOR	damage 5.000 € - 100.000 €
3.	MODERATE OR SIGNIFICANT	damage 100.000 € - 1 million €
4.	MAJOR OR SEVERE INTERNAL	damage 1 – 10 million €
5.	MAJOR OR SEVERE INTERNAL AND EXTERNAL	damage 10 – 50 million €
6.	CATASTROPHIC	damage above 50 million €

Fig. 14 - Scale of consequences of a threat

Regarding this latter, a description follows:

- **insignificant or negligible**: consequences are very low but it may be necessary to analyse situations where the likelihood is high since it can have cumulative and long-term effects; please note that in some cases it may be necessary to monitor an insignificant threat to avoid possible critical developments;
- **minor**: the organization, asset or infrastructure does not present a significant limitation to the activity; for example, the stop of the activity is less than four hours and there is no loss of important equipment;
- **moderate or significant**: the organization, asset or infrastructure is temporarily closed or unable to function, but can resume functioning after just over a day. A number of items of equipment could be damaged, but most of the equipment is not affected. Operations are reduced by up to, for example 25% for a certain period of time;
- **major or severe** (internal and/or external): the organization, asset or infrastructure is damaged or partially contaminated. There may be partial damage to some parts of the buildings, with possible internal flooding, smoke production and fires in some areas. Some goods and equipment inside could be irreparably damaged, but the rest of the equipment is mostly intact. Also, in relation to cyber-attacks, the operation is reduced between 25% to 50% for a few weeks to a few months and a portion of the organization, assets or infrastructure could be closed even for a longer period;
- **catastrophic**: the organization, assets or infrastructure is damaged or contaminated in such a way that it cannot be used in any way. Buildings are totally compromised and most of the goods and equipment that were inside and outside have been destroyed or damaged beyond any reasonable possibility of repair. Operations are reduced from 75% to 100% for a year or more. This category is usually considered in case of natural threats such as earthquakes, of ballistic attacks or bombings.

3.2.4. Risk evaluation

The combination of the two scales of likelihood and consequences creates the likelihood/consequences matrix or risk matrix. At their intersection there are cells to which an evaluation of risk is associated. In the following example, there are five ranges, indicated by Roman numerals18. Cells can be coloured to indicate the magnitude of risk. Depending on the definitions used for the scales, the matrix can give more weight to consequences or to likelihood,

[18] Ref. ISO 31010:2019, Annex B chapter B.10.3, Fig. B.17, p. 115.

or it can be symmetrical depending on the application (as in Fig. 15). To assess a risk, it is preferable first to describe the consequence best fitting the situation, then define the likelihood with which the consequences are believed to occur.

		Consequence rating →				
		1	2	3	4	5
Likelihood rating ↑	e	X	VI	IV	II	I
	d	XI	VIII	V	III	II
	c	XII	IX	VII	V	IV
	b	XIII	XI	IX	VIII	VI
	a	XIV	XIII	XII	XI	X

Magnitude
Extreme
High
Moderate
Low

Fig. 15 - Example of likelihood-consequences or risk matrix to evaluate the magnitude of risk[16]

A **score** can be assigned to obtain the product L (likelihood of threat) x C (consequences) = R (Risk). Numerical values are given to verbal labels and also different colours make better appreciate the level of risk (**Fig. 16**).

Probability		Consequences				
		Insignificant	Minor	Moderate	Major	Catastrophic
		1	2	3	4	5
Almost certain	5	5	10	15	20	25
Likely	4	4	8	12	16	20
Moderate	3	3	6	9	12	15
Unlikely	2	2	4	6	8	10
Rare	1	1	2	3	4	5

Extreme	15-25
High	8-12
Moderate	1-6
Low	

Fig. 16 - Number values in the risk matrix

In short, if the adverse event is even frequent but of little value, it can be of no interest (yellow/green ones); on the contrary, the most harmful and dangerous risks or the rare but potentially catastrophic (red ones) are those of greatest concern to decision makers and require treatment. Finally, risks evaluation can be divided into three categories:

- risks that are **not acceptable** due to the serious possible consequences on the organization, therefore corrective and mitigation actions are proposed and a priority scale can be drafted;
- risks that are **tolerable**, i.e., risks which involve possible negative effects on the organization that is willing to accept a degree of risk; eventually the decision to undertake corrective actions should be scrutinized, for example, with a cost-benefit analysis;
- risks that are **negligible**.

Strengths of the risk matrix technique include:

- relatively easy to use;
- quick classification of risks into different levels of significance;
- clear visual display of the level of risk;
- comparability of risks with different types of consequences.

Limitations include:

- likelihood/consequences scales and the consequent matrix are necessarily simplifications;
- validity of risk ratings depends on how well the scales have been developed and calibrated;
- combining likelihood/consequences as a simple product, some information may be lost, for example there is no distinction between risks with high consequences and low probability and those with low consequences that frequently occur; the reaction of an organization towards the former or the latter should differ;
- the same scales generally don't apply to different contexts;
- their use is very subjective and different experts can assign very different ratings to the same risk.

At the end of the risk evaluation phase, we are able to identify **the threats that involve risks to be considered a priority** for an organization.

3.3. RISK TREATMENT

Once the threats that pose priority risks to an organization have been identified, steps can be taken to deal with them **to mitigate the risks**.[19] Therefore, in relation to the **numerous risks and threats**, there are one or more potential risk mitigation strategies, always bearing in mind that the resources available are usually limited. But, before launching a mitigation strategy, some considerations about the possible courses can be made:

I. **doing nothing, accepting the risk as it is, and suffering the consequences**. This may be convenient if, for example, the risk is low and widespread (we are in the green boxes of the risk magnitude matrix in **Fig. 16** above) and, therefore, this could be reasonable for economic reasons;

II. **managing some extremely obvious risks,** without great effort by better developing company functions that are already operational (for example, implementing a backup and restore plan in a data centre that does not have any or installing a security system in a company transporting valuables, etc.);

III. **modifying corporate strategy by interrupting activities that generate an unsustainable risk** (e.g., if the activity is located in a place highly exposed to terrorist or criminal attacks and moving the business to another less dangerous location);

IV. **mitigating the risk by means of a mitigation strategy,** in order to implement defence measures or countermeasures.

3.3.1. Risk treatment for the mitigation strategy

Once one decides **to implement a mitigation strategy**, three different categories of defence measures can be considered: **protection, prevention, and transfer.**

A) Protection (PROT) concerns defence measures aimed at lowering the likelihood of occurrence and the consequences. They can be active, passive, procedural and organizational (**Fig. 17-1**) :

[19] The full chapter n. 5 has been devoted to this topic in Security of Road Infrastructure", Final Report of the Task Force C.1., PIARC 2019. A relevant reference is also the ENISA "Guideline on security measures under the EECC", July 2021.

A1) active, which are implemented to anticipate as much as possible an attack, to promptly detect it and react against the occurrence of a physical or cyber-attack (security controlled) in order to use the time (see further on, time factor and equation of defence) before the occurrence of the damage with countermeasures that avoid or reduce its might; the time factor is decisive for detecting the attack and transmitting the alarm as soon as possible (e.g., alarm systems);

A2) passive, which are implemented to stop and delay the occurrence of a physical or cyber-attack (static) to increase the time for the threat to occur in order to produce its consequences; in this case the time factor works to lengthen the timing of the attack (e.g., a perimetral fence);

A3) procedural-organizational, to integrate passive and active measures with the human factor in order to stop the attack.

B) Prevention (PREV), concerns corporate policy decisions aimed at stopping terrorist or criminal actions from happening through corporate decisions, intelligence activities (with national or private agencies); personnel training, meetings, debate, seminars on case studies, exercises, introducing or strengthening compliance with rules, procedures and standards, including non-binding ones also in terms of quality, reliability and reputation including adequate security risk assessment (**Fig. 17-2**).

C) Transfer (TRAN) is about action aimed to transfer or share all or part of the risk to third parties typically by means of contracts with private security services and insurance contracts (**Fig. 17-3**).

A1) PROTECTION ACTIVE	
PROACT 01: Physical access and intrusion detection	
a)	**implement physical access controls** (employees, vehicles, goods, third-party, contractors, suppliers, integrators, visitors, maintenance workers, in critical areas limited number of security-vetted, trained and qualified personnel etc.)
b)	**implement systems and procedures for intrusion detection and forwarding** timely to appropriate people, related to structures, main and secondary buildings, electrical substations (external-internal video-surveillance, person detectors, perimetral and burglar alarm, fire alarms, fire extinguishers, flooding

A2) PROTECTION PASSIVE	
PROTPAS 01: Physical and environmental security	
a)	**protect assets against unauthorized physical access** to facilities and infrastructure, set up adequate environmental and perimetral measures (fences and walls, portals, armored doors, doors and cabinet keys and locks, turnstiles and tripods, bars, external-internal and/or perimetral lighting, segmentation of spaces)
PROTPAS 02: Network and information security	
a)	**make sure software of network and information systems** are not tampered with or altered, for instance by using input controls and firewalls (NGFW-next generation firewalls, IDS-intrusion detection systems, encryption policy, signing, etc.)
b)	**check for malware** on internal network and information systems (malware detection and prevention software, secure segmentation and secure design of industrial networks, interaction with supply chain of parts, components and devices)
c)	**protect critical data** avoiding them from leaving the network or being haltered (network segregation, encryption of data, secret authentication information, user password, hashing)
d)	**direct manipulation protection** using network monitoring solutions (NMS-network management systems, SOCs-security operations centers, gateway devices such as IDS and NGFW, HMI-human-machine interface)
e)	**management system** protection based on MFA (Multifactor Authentication) and Zero Trust principles

A3) PROTECTION PROCEDURAL- ORGANIZATIONAL	
PROTPRO 01: Operational procedures	
a)	**set up and implement operational procedures** and assign responsibilities for operation of (critical) systems and for changes (change management)
b)	**set up and implement procedures for central reception**, vehicles and goods control (identity check for employees, third parties, truck drivers, keys management)
c)	**set up and implement procedures for security guard** (all entrances, day and night services)
d)	**set up and implement access to server rooms procedure**
e)	**set up and implement Internal postal service procedure**
PROTPRO 02: Asset management	
a)	**identify and update critical assets** and configurations (extended inventory, procedures, configurations)
PROTPRO 03: Incident management	
a)	**prepare staff to manage incidents** (policy, procedures)
b)	**establish incident reporting and communication procedures** (record, classification, entities involved)
PROTPRO 04: Business continuity management	
a)	**implement contingency and backup plans and strategies** for ensuring continuity of services provided (key sectors and services, recovery time)
b)	**implement a contingency plan** for related or dependent services
c)	**prepare for recovery and restoration of services following disasters** (policy, procedures, duplication, failover, backups)

v-2

Fig. 17-1 - Mitigation strategy: defence measures of protection

B) PREVENTION	
PRE 01: Information and security policy	
a)	**setting a security policy**
b)	**making key staff aware of the security policy**
PRE 02: Governance and risk management	
a)	**making a list of the main risks for security**, taking into account main threats for the critical assets
b)	**making key staff aware of the main risks and threats** and how they are mitigated
PRE 03: Human resources security	
a)	**assigning security roles and responsibilities** to staff
b)	**making sure the security roles are reachable** in case of security incidents
c)	**checking professional references of key staff** (security officers, system administrators, guards, etc.)
d)	**providing key staff with relevant training and material** on security issues
e)	**managing changes in staff and in their role and responsibilities** (revoke access rights, badges, equipment, training of new staff, etc.)
f)	**holding personnel accountable for security incidents** caused by policy violations (procedures, contracts, etc.)
PRE 04: Security of supplies	
a)	**backup to electrical power and/or fuel**
PRE 05: Monitoring, auditing and testing	
a)	**implementing monitoring, auditing and testing activities** (criticalities, priorities, standards-based continuous improvement policy)
b)	**implementing compliance and auditing to standards and legal requirements**
PRE 06: Security threats awareness	
a)	**performing regular threats monitoring** (intelligence, OSINT, studies)
b)	**establishing form of cooperation** with other parties
c)	**reviewing security threats and communicate** to those interested (appropriate time intervals, staff involvement)

v-2

Fig. 17-2 - Mitigation strategy: defence measures of prevention

C) TRANSFER	
TRA 01: Security of third-party dependencies	
a)	**including security requirements in contracts with third-parties**, including confidentiality and secure transfer of information
b)	**tranferring risk to an insurance company**, insurance solutions by contracts (physical losse, consequntial losse, legal, liabilities)

v-2

Fig. 17-3 - Mitigation strategy: defence measures of transfer

3.4. RISK MONITORING AND REVIEW

It is necessary to state categorically that it is not possible to create perfect defences and it is not possible to create satisfactory defences without the study of a **reasoned compromise** between measures of protection, prevention and transfer.

Priority risks and non-priority risks must be constantly updated and checked with the **cyclical repetition** of the risk management process. We need to assess not only the initial risks, but also how much the risk will change if various precautions are taken. Therefore, those risk mitigation efforts, once chosen, must be monitored in the same way and the risk management cycle must begin again.

Furthermore, methods such as the **risk matrix or the semi-quantitative scoring** adopted here make many simplifying assumptions. Therefore, it is necessary to consider the need for continuous monitoring and even simple self-examinations to make risk assessments more and more accurate and consolidate the choices in terms of mitigation strategy. According to the DCPA cycle, i.e., the iterative method of continuous improvement of ISO 28000 and 31000 proposed above, we have the possibility to re-evaluate decisions and the risk management process eventually leads to carrying out timely risk assessment sub-processes. Checklists as exemplified in **Appendix 2** are recommended at any stage.

A **minimal change** in one of the elements of the risk function (context, threat, probability, consequences) involves a change in the overall risk level. Changes occurring in the organization and in its processes, whether they are of an external nature or are the consequence or the interference of the measures implemented for the treatment of the previously identified risks, must be considered. This may also be achieved by the analysis of the incidents that have occurred but also from reports from institutional bodies or trade associations. Costs and also their evolution must be taken into account. Furthermore, the **factors** related to the possibility of failure of the electronic defences, the possibility of damage to the physical defences and the possibility of correct recognition of identification of the areas where the correct intervention on site is included, must be taken into account.

Finally, it should be considered that **criminals or terrorists** are usually excellent risk managers due to the perilous nature of such conducts potentially leading to long-term imprisonment or even death of the perpetrators. Therefore, the terrorist/criminal chooses his objective carefully and adapts his behaviour to the risks by deciding to attack in the most favourable moment. A constant verification and even adaptation of the defence measures can also help make dangerous individuals desist from their intent.

Summing up, **monitoring** is an iterative back and forth process, which tends to improve defences, implementing the PDCA cycle composed by some sub-process (an elaboration of a GANTT chart with tasks, milestones/times is necessary):

- continuous monitoring of risks and possible changes in the initial conditions, at appropriately established intervals through automatic measurements and checklists;
- some targeted checks can be carried out at short time intervals by internal structures on predefined risks;
- external or internal audits (e.g., penetration test) with frequency, for example, annually;
- comparing the results obtained with those expected by the stakeholders in the risk identification, analysis and evaluation phases;
- improving the assessments of some risks that have been considered critical in the previous phases, updating them through new inputs or news (e.g., by means intelligence information);
- in case of systemic risks that are shared between various organizations, exchanging sensitive information, considering that the risk can also affect others.

3.5. INSIGHTS INTO SECURITY RISK MANAGEMENT

3.5.1. On the difference between threat, vulnerability and risk

An asset or an organization is a complex material or immaterial object created by human intellect, born with its own intrinsic level of security (understood as the intrinsic ability to resist malicious attacks) in relation to the design principles adopted. This level cannot be measured in absolute terms, and it depends on the context in which it is placed, which may change.

The concept of threat is in itself abstract if it is not contextualized, while **vulnerability** is an intrinsic characteristic of the context considered as a criticality or weakness. From their combination arises the materialization of the damage and therefore **risk** arises. Weaknesses can be present in structures, procedures or technologies, physical and cyber assets, made up of real estate, machinery, people, know-how, information, data, knowledge, processes and systems. Therefore, **insecurity arises in relation to the internal and external elements** that have not been taken into consideration by the designer or by whoever created it. Unforeseen and unforeseeable events, not considered or underestimated during the design and implementation phase or even human errors, defects, black swans, climate change, geo-political and social mutations, or increasing traffic can determine the so-called vulnerabilities. An infrastructure can become vulnerable even if it hadn't been previously. For example, if a computer system is equipped with antivirus, which doesn't get updated, the computer will still be vulnerable to threads.

The effect of vulnerability is considered in the **risk assessment process** as a multiplicative factor (aggravating) of the likelihood of occurrence of the threat initially estimated:

$$Likelihood = Likelihood_{initial} \times Vulnerability\ (V > 1)$$

Since **in this Report we are not considering real cases but very broad and abstract categories of assets or organizations**, we will limit our analysis to obtaining the picture of the priority threats based on the calculation of the risk magnitude L x C = R. In a more refined process, vulnerability must be adequately considered as a function of the contexts (internal and external), procedures, technologies and human resources:

$$Vulnerability = f\ (contexts, procedures, technologies, human\ resources)$$

Therefore, risk should not be confused as threat since the risk exists because a threat is transformed in risk due to vulnerability.

ISO 28000 and 31000 suggest processes for controlling those threats and security risks. But also it should be remembered that **risk management concerns threats and events that have not yet occurred**, therefore the interactive process of analysis, evaluation, treatment, monitoring and reviewing is a challenging task that requires critical skills and non-conventional views.

Therefore, in the field of security, the so-called consolidated "good practices" should not be followed as they blind the decision maker, anesthetize them with respect to the ever-evolving context and determine fatal decision-making inertia.

3.5.2. On the risks of criminal and terrorist origin

With regard to **threats of criminal origin**, there is no doubt that an accurate assessment of the crime index of the area, in which the settlement is located, can already give a satisfactory indication of the type of criminal activity that may occur. A national statistical institute regularly

publishes tables, which are useful for acquiring **credible data of the crime level of an area**, for use in the evaluation. Local news information can also be very useful.

However, since thinking about risks means thinking about events that have not yet occurred, the information on criminal and terrorist facts that have occurred may be **anecdotal and therefore insufficient**. On the other side, the **probability of a terrorist attack cannot be quantified** in statistical terms because terrorism, by its very nature, is not governed by statistical or random factors. Consequently, this probability can be better understood from **geo-political analysis** which determines its occurrence. In general, when the threat of a terrorist or criminal attack is considered, it is suggested to work on a set of **possible attack scenarios**[20].

In this regard, **the attractiveness of the settlement as a target** is the primary consideration to be evaluated and the type of terrorist attack can vary according to the motivational and psychological profile of the terrorist (political motivation, religious motivation, social motivation, etc.) and, of course, the possible weapons. The most recent experiences demonstrate that **if firearms are not available, knives, axes or vehicles are used as weapons.**

3.5.3. On quantifying risk appetite of an organization

As explained in our first "Security of Road Infrastructure" Report drawn up in 2019 [21], **an organization will always have to bear a level of risk**, but how much capacity it has to do so will depend on the impact that a security breach or incident resulting in an asset's loss and compromise or failure could have on the organization and the organization's stakeholders. The countermeasures to be applied must be proportionate to each of the identified potential risks, according to pragmatic, appropriate, cost-effective measures and commensurate with the organization's risk appetite.

A very important aspect for the process of security risk management is **verifying the results of the risk assessment** in light of the quantification of the risk that the organization is willing to take in relation to the various threats. It applies to higher and moderate risks and requires an internal process involving the highest levels of management in the organization. Tolerance for higher risks (very rare) can yield savings while underestimating moderate ones (very frequent) can result in unexpected costs. We are within the **legitimate responsibility of the governance of an organization** and it is appropriate that their choices are accounted for in the process, keeping in mind the choices deliberately made from time to time and also correct them later if necessary.

In case of particular **risks relevant for both likelihood and consequences**, if it is not possible to reduce a risk (e.g., due to costs), an alternative may be to either eliminate or suspend the activity or the component subject to risk. Otherwise, one can try to change the consequences or likelihood. An alternative is to **transfer the risk to insurance companies**. It is also possible to opt for **solutions that strengthen the global resilience** of the organization or asset. Some can consider and **accept the risk by not intervening but continuing the activity** even if subject to risks. It is the ostrich policy!

---

[20] A difficulty in connecting the concept of probability to planned harmful actions arises considering the process "I know you know I know ....", that is the probability attributed to an attack totally changes if the attacker is rational and considers that the defender is aware.

[21] See it in ch. 3 "Security-minded approach" of the Report 2019, see note 2.

In addition to the scope of security, the risks that can impact an organization in carrying out their business, such as a company or an administration, can be different from the risks that can affect an asset. With regard to the former, it is clear that there are also **entrepreneurial risks, commercial risks and risks in general linked to the business of the economic entity** considered. In this case, an advisable strategy is to see the risks in an integrated strategic view and not take them into consideration and manage them individually. It **is preferable to focus on risk optimization**, while traditional risk management focuses on risk mitigation.

3.5.4. On the bias-induced risks for security experts

A major risk can be how experts assess the risk, that is, their point of view based on their professional aptitudes and knowledge. Risk management requires **the utmost attention to avoid arbitrary choices that can do more damage than doing nothing**.[22] For this reason, it is not recommended that the subjective evaluation of the success of the process based on the qualitative approach be made by the same managers who have planned it.

In various countries[23] there are **specialized professional figures for security corporate protection** i.e., *security manager*, with the main following functions:

- general definition of corporate security policies;
- implementation of policies within the individual organizational functions;
- risk management;
- crisis management and business continuity;
- terrorism, criminality, cyber-criminality and fraud mitigation.

The security manager or professional, together with the stakeholder of a company or an asset, must possess **a sense of awareness, intuition and creativity of their security risks** in the internal and external contexts in which they operate. We should not assume that simply applying the proposed process or any other will in itself lead to "wonderful" results. The process proposed here, however, provides a good starting point for assessing the risk arising from insecurity and helps us in the critical evaluation of priorities in the security domain.

3.5.5. On technology and cyber risks

In recent times there has been a significant growth in **cyber actions of a criminal nature**, above all through ransomware campaigns. Unlike the recent past, these attacks caused the **unavailability of data indefinitely** in addition to the threat of **disclosing said data**. Therefore, the attacker has the possibility of obtaining a more important ransom by also leveraging the damage deriving from the possible disclosure. Ransom attacks are also used to block production activities and also to hide traces of espionage activities[24]. The use of cybercriminal groups to delegate the execution of **espionage operations** is common practice. Digital attacks make it more difficult to pinpoint perpetrators.

---

[22] It is appropriate to mention some catchphrases by prof. Douglas W. Hubbard in "The Failure of Risk Management", Wiley, 2009, 2nd edition 2020: "a risk management that simply reacts to yesterday's news is not risk management at all" and "organizations in which a disaster hasn't occurred are just lucky and they may have been doing nothing substantially different from organizations in which disasters have occurred."

[23] In Italy, the UNI 10459:2017 standard on security professionals establishes both the functions and the academic profile and professional, necessary for the qualification of a security manager.

[24] I.e., in the hybrid war in Ukraine.

As regards the types of hostile actors, it must be noted that from 2021-22 onwards, excluding activist-related activities, there was an increase in **State-based actors**. Consequently, we are now dealing with of a **hybrid threat between States** and no longer only a physical threat. Considering the quick evolution of technology and the likelihood of incidents occurring also in war scenarios, **the use of technological and cyber systems presents a higher risk of uncertainties**. The estimated level of risk changes significantly over time. In this field, there may be difficulties to estimate the possible damage, while for likelihood we can estimate a high frequency of accidents.

Evaluating the risk of a loss of customer data to hacker, the potential loss could include costs of recovering said data, compensations to customers, legal costs, and/or the loss of customers. This could range from a trivial amount (e.g., if the hacker was internal and the damages were discovered before or after releasing the data). Among all, the cost of major mitigation and the loss of customers has to be considered.

A challenge also concerns **radicalization on the web**, which is confirmed as the main place of proselytism through the sharing of manuals and propaganda material.

Finally, it should be considered that **computer viruses have become part of our reality like biological viruses**[25] . It must be considered that, of the thousands of viruses created and released on the worldwide computer network, none really have gone extinct but all are under the control of their respective anti-viruses.

Concerning technological and cyber risks, it is also necessary that **security audit** be repeated periodically in consideration of the changes in the context (new activities, new threats, new organizations, new technologies, etc.).

3.5.6. On the geopolitical risks and armed clashes and conflicts

Currently several wars[26] **are unfolding in the world**, as well as riots, civil violence perpetrated variously by terrorist militias or by state security forces and military crises, some of which have been dragging on for years. Developing countries as well as third and fourth world countries are often the stage of such conflicts. The reasons are trafficking, economic interests, tempting natural resources, ethnic or political clashes, often happening between the poor. The **two biggest hot spots remain Africa especially in the sub-Saharan region and the Middle East**. Africa witnessed a sharp increase in instability under the covid-pandemic period that has halted over two decades of growth and fuelled latent crises in various regions of the continent. Conflicts involving gangs, armed forces affiliated to the Islamist network or regular armies. **The epicentre is the Sahel region**, the strip that runs along the southern borders of the Sahara, overwhelmed by the rise of violence already seen in the triangle between Burkina Faso, Mali and Niger. Africa is one of the most affected regions in the world with at least 15 ongoing conflicts (Rwanda, Congo, Kenya, Ethiopia-Eritrea, Mozambique, Mali, Niger, Guinea, Burkina Faso, South Sudan). Africa could be also influenced by the fallout of the war in Ukraine, exacerbating and multiplying tension within it. Some effects could be economic due to, for example, the interruption of wheat imports, rise in

[25] See at p. 104 “Biological and cyber viruses have a lot of common”, chapter 6.8 Security of the PIARC technical report “COVID-19: initial impacts and responses to the pandemic from road and transport agencies”, 2020BN03EN, ISBN: 978-2-84060-728-4.
[26] According to ACLED’s (The Armed Conflict Location & Event Data Project) site, one of the most up-to-date ones with disaggregated data collection, analysis, and crisis mapping, there are 59 ongoing conflicts of various kinds around the world: in Ethiopia, Yemen, Sahel, Nigeria, Afghanistan, Lebanon, Sudan, Haiti, Colombia, Myanmar, Brazil, Mexico.

energy costs, the growth of military influences from some non-African countries, migrants, weapons being spread from Ukraine itself to Caucasus, Afghanistan, Middle East and also the European Union.

The issue of **road security in low-income countries** is one of enormous concern (extract from **Appendix 3**). It is the cause of several losses of human life. It finds its source at various levels which are, in particular:

- the proliferation of acts of robbery by often armed individuals blocking the roads to strip users of all their belongings in slowdown areas with a poor state of the roads. These brigands are commonly called "road cutters";
- terrorist acts, especially in the Sahel region, consisting of placing explosive devices in crevices or potholes, causing several deaths, particularly in Burkina Faso during the year 2022;
- installation of explosive devices in crevices or potholes;
- banditry on the roads.

3.5.7. On the "black swan"

The expression "**black swan" is used to refer to an extremely rare event, very difficult to predict, sudden and devastating** which we think may occur by pure chance. In the book "The Black Swan"[27], it is argued with a metaphor that the events that have influenced the history of humanity were black swans because they were completely unpredictable and unlikely, like finding a black swan.

Catastrophes such as the attacks of September 11th, 2001 exemplify the impossibility of predicting the unpredictable. This has also happened in part more recently during the pandemic or the war in Ukraine (although both, if we look closely, could have been foreseen) and, more recently the Hamas attack to Israel (in this case the warning signs were probably overlooked). But, in reality they are a grey swan ...., in the sense that **we knew about the risk but we had likely lost perception of said risks**. And sometimes it is a kind of cultural blindness, i.e., it then turns out that that catastrophe was the result of events that were in front of everyone's eyes but which, for different reasons, were not perceived in their seriousness. This is the case of biological and cyber viruses that can't be considered as black swan.[28] In essence, the biggest threats are those we fail to consider. Since thinking about threats and risks means mostly trying to predict events that have not yet occurred, it is easy to picture the difficulty of the challenge. Moreover, the black swan is often in direct correlation to events that nobody accounted for in the system. This is the case of complex systems (see it the following paragraph and **Appendix 4.1**).

It is evident that **rare events are a problem for quantitative models**, that are probabilistic and require mathematical hypothesis; on the contrary, a **qualitative model**, that is humanistic - cultural, can broaden the view for which there is also the so-called "**lateral thinking"**, i.e. thinking

[27] In Nassim N. Taleb's book "The Black Swan: the Impact of the Highly Improbable", 2007, it is told the story of the turkey that thinks it will live forever because it is treated very well in the months leading up to the end of the year (inductive reasoning). It thinks this because it does not know about the end of the other turkeys that are fattened to be eaten at Christmas (deductive reasoning). This conscious evaluation is possible only by broadening the field of observation.

[28] In Appendix G of the LR, the extracts of paragraph 6.8 and 7.7 of the Final Report "Covid-19: Initial Impacts and Responses to the Pandemic from Road and Transport Agencies" elaborated by the members of TF, are retrieved.

creatively or in an unconventional way to solve a problem. Many future scenarios have been anticipated in literature.[29] The lesson is that it is recommended **to also refer to a broader context** and view than one's own company or category of companies to which one belongs, or even observing very different organizations, near-miss accidents and non-mathematical analyses based on non-logical thinking that is developed for example in games or puzzles.

3.5.8. On the interaction of threats and the concept of complexity

A complex system is defined as an **organic and structured aggregate of interacting parts**, whose global behaviour is not immediately attributable to that of the individual constituents, depending on the way in which they interact[30]. Threat complexity is a gigantic mosaic where tiles are continuously added (**Fig. 19**) and there can be many interactions and co-dependency amongst threats.

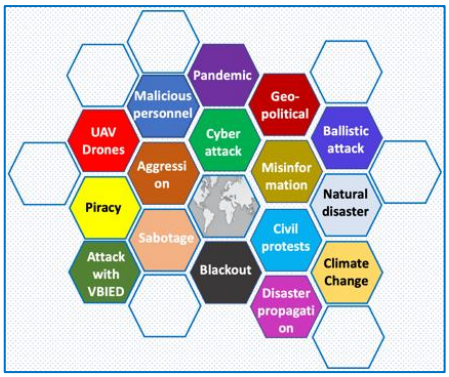


Fig. 19 – Threat complexity

Multiple consequences can result from a single cause, or a single consequence could have multiple causes. Some threats are organic and functional to each other. Some may act together, at the same time or at different times. Others can be interconnected and osmotic.[31] When an accident occurs, it can take on the dimension of a multi-factorial event such as chain of events (one after the other), cascading (relapses in various directions)[32] or casual links and loops.

Two important concepts must also be considered. The first is that **security deals with an open system, i.e., the world**. Something that cannot be predicted mechanically in the premises. The world is a creative organism in all senses, both positive and negative. In the latter case, it can bring damage, death and destruction in different ways. The second is that in the world, that is in real life, **the paradox of antinomy** exists. It means that at the same time both values of A and the value of non-A can be valid. So, a controversial reality can hide certainty, while something that appears absolutely certain may be wrong.[33]

[29] Among some it can be mentioned the 1948 novel "1984" by George Orwell, or "The Plague" by Albert Camus of 1947.
[30] See the paper: S. Palchetti and A. Scala "The Difficulties of Risk Assessments for Complex Network Infrastructure: Applications to the Security and the Resilience of Road Infrastructure", Prague PIARC WRC, 2023.
[31] An example is pandemic and cyber-attacks. Another example are cyber-attacks and physical effects such as closing doors or activating signals.
[32] It is the case of a disruption of the energy supply that could cause massive cascading effects.
[33] The philosopher G. W. Friedrich Hegel said in his Doctoral Dissertatio, 1801 : "Contradictio est regula veri, non contradictio, falsi".

Critical infrastructure and networks are complex and often interdependent systems i.e., systems of systems or even a network of networks (e.g., electricity networks, transport networks, etc.). In general terms, a complex system is characterized by an internal structure that can consist of many interacting components and by a network that regulates the ways in which the components of the system interact in space and time. This can lead to unpredictable behaviours.

3.5.9. On the concept of resilience

The term resilience, a word much abused in recent time, is defined as follows: given a system and a disturbance that acts upon such system, be it an accidental event, an attack of any kind or a pandemic, resilience is defined as the capability to regain its balance and return to its starting point. See also in our Report 2019 [2] how the critical issues in the resilience cycle (prepare, prevent, protect, respond, recover) were analysed in detail in seven security case studies (**chapter 7 and Appendices**).

A **full resilience-based approach is not concerned with causes but is concerned with effects**. It may not perform in-depth studies on the upstream threats, or on the various types of attacks, but it focuses on the ability to respond to critical events. As an example, smoke in a tunnel can originate from various causes while planning according to resilience, we don't care about the different causes but we look for the ability to react to smoke inside the tunnel. It's a simplification but it can work. However, **a strong limit of this approach is that is not easy to imagine security made up of a world of resilient cities, bridges, tunnels, roads, control centres, asset management, staff, users, etc**. Another limit of the resilient approach is that it does not know the true situation, and tends to incorporate all possible consequences. This can be particularly effective in cases of complex systems with possible multiple sources of risk leading to a single threat or multiple possible effects from a single threat such as chain events or cascading. **It can be also useful in case of unplanned and unforeseen events with major uncertainties.** But at the same time, it can be **very expensive** without certainty of achieving the objectives in term of security.

Anyway, the resilient approach can very helpful if **coupled with the process of security risk management**, integrating the mitigation measures with the four properties of resilience:

- **robustness**: the ability to withstand a given level of stress without undergoing degradation or loss of function (e.g., number of employees);
- **redundancy**: the extent to which the elements or systems are replaceable, i.e., capable of satisfying the functional requirements in the event of interruption, degradation or loss of functionality (e.g. number of IT hubs);
- **resourcefulness**: the ability to identify problems, set priorities and mobilize resources when conditions exist that threaten to destroy some elements, systems or other units of analysis (e.g., organizational capacity and self-organization);
- **rapidity**: the ability to satisfy priorities and achieve objectives in a timely manner in order to contain losses and avoid future disruptions (e.g., speed of recovery of business as usual).

Once the framework of the mitigation measures has been defined, it is possible to manoeuvre through **resilience engineering** by reinforcing, making redundancies, establishing priorities and making the system's responses faster in the event of an attack. These are estimates that everyone

can make related to own corporate policy as an integration of a threat protection framework, considering the complexity of the systems and the unpredictability of events. In this field an effort is still being made in **measuring resilience**.

3.5.10. On business continuity, corporate culture and crisis management

In addition to implementing a process of security risk management, an aspect of resilience is also the **establishment of a business continuity process.** It allows to face unexpected events without generating interruptions of service. Business continuity means the strategic and tactical capacity of an organization to continue its business in response to incidents that may affect it. It has evolved from disaster recovery, and it consists in defining **plans in which critical moments and recovery time objective are clear**. A support guide to managing operational continuity is the ISO 22301 standard[34] which refers to the continuous improvement process of the Deming cycle PDCA.

Two fundamental elements contribute positively to the management of business continuity in the field of security: the **culture and the awareness of the organization**. A specific chapter has been dedicated to the topic, in our previous Report of 2019 with reference to the integration of good security management practices. In order to increase the organization's awareness of business continuity, as in the field of security, it is necessary to:

- involve top management and the entire organization;
- assess the awareness gap and its potential impact on corporate strategies;
- set up, implement and monitor a corporate training, information and awareness campaign.

A topic in some ways complementary to risk management and business continuity is that of **crisis management**. The crisis determines the development of an emergency situation that has effects on the behaviour of people, who react in an often-unpredictable way both individually and as part of a crowd. The unleashing of fear, anguish and even panic is characteristic of this situation. They are non-rational reactions determined by the human sub-conscious.

Those familiar with emergency situations can imagine **what could happen when a critical situation** arises if no proper planning is done in advance and there is no clarity regarding to who is doing what, how and when. The effect of a more or less considered risk can cause total chaos. In fact, if operational activities already normally in ordinary conditions may face issues, even more so in extreme conditions, things may not work out as planned.

A crisis is basically characterized by:

- **surprise element**: there was no warning and the organization is already facing a crisis, hence reaction is late to arrive;
- **events follow one another in a cascade**: e.g., it is a scenario of a river in a flood;
- **lack of external communication, the absence of news on the crisis**, no answers to the requests for information and explanations by external parties, further fuel it;
- lack of internal communication.

[34] See in the LR Sheet n.15 in Appendix B.2 Standards.

Crisis management is strongly connected to resilience. An organization should develop a conscious approach to crisis management, with regard to both the direct management of the crisis and the preventive capacity of the pre-crisis phase. An organization should activate an internal structure in charge of crisis management as a Crisis Management Team that has the task of prevention, control and management of critical events, generally composed as in **Fig. 20**.[4]

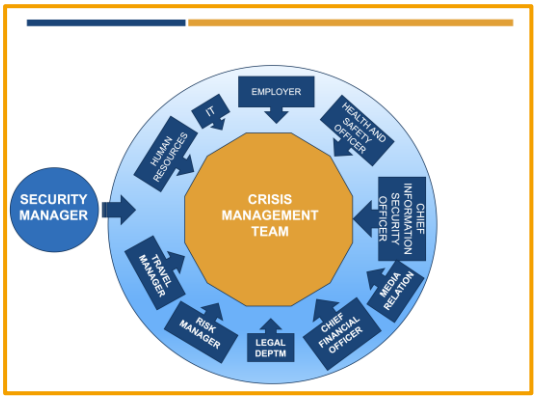


Fig. 20 - Crisis Management Team

In the pre-crisis phase an important role can be played by the **structures of risk management and experienced professionals** that have the task of monitoring risks in the internal and external contexts. They can act as an early measure to avoid a crisis or, at the very least, influence its development.

3.5.11. On transferring risk to an insurance company: fire and cyber-attacks

For every organization, **alternative solutions with different costs and effects on risks can be evaluated** on the basis of a calculation algorithm (**Fig. 21**)[35]. Based on the ratio of risk reduction and costs, a final balance must be obtained between the level of risk accepted and a residual risk not to be managed directly but transferred to an insurance company. The algorithm below is essential for this purpose. This happens typically in the case of fire and cyber-attacks.

Insurance solutions may concern: physical losses, consequential losses, legal liabilities (**Fig. 22**)[36].

Cyber insurance is a hot topic as the frequency and severity of cyber-attacks have increased dramatically in recent time. In this sector, specialized insurance policies essentially cover ransomware, data breaches and business interruption. New topics as artificial intelligence, robotics, virtual reality and the IoT risks, need evaluation of threat parameters.

Basic coverage typically covers the cost of incident investigations, loss of revenue due to business interruption, risk assessment for future cyber incidents and payment for direct damages from ransomware attacks - subject to coverage limits - and notifying affected customers. It is possible to also develop liability coverage to protect organizations from third-party lawsuits for damages: legal fees, compensation and fines for non-compliance. Often, disputes may arise with insurance companies and organizations discussing compensation.

---

[35] A wide-ranging approach is what has been proposed by Prof. Fabio Garzia in "An integrated multidisciplinary model for security management and related supporting integrated technological system", Proc. of IEEE International Carnahan Conference on Security Technologies, Orlando (USA), pp. 107-114, 2016, DOI: 10.1109/CCST.2016.7815690.

[36] From B. Gibbs, Willis Towers Watson, 2020.

The **implementation of good IT practices** reduces the insurance premium of cyber insurance, such as: encryption of sensitive data, installation of cybersecurity software and periodic staff training on cyber-attacks, data backup (to guarantee the operational continuity in the event of an attack and to prevent hackers from asking for ransom). Data backup must always be performed according to the rule that requires three copies of the data on two different media, one off-site and one offline, with a recovery system that does not contain faults.

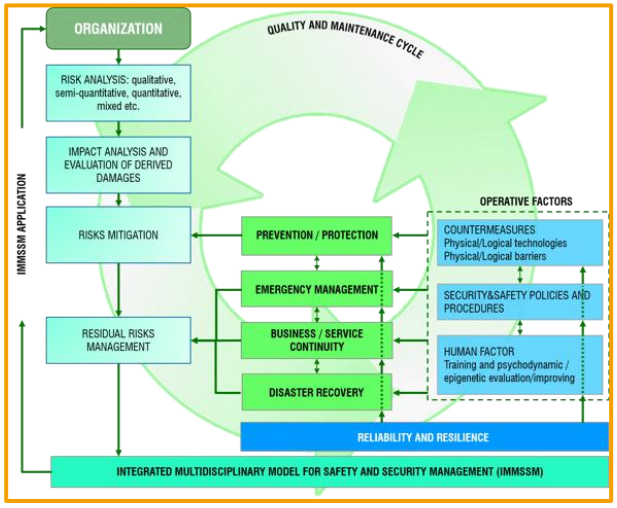


Fig. 21 - Scheme of the Integrated multidisciplinary model for security management

Fig. 22 – From risk origin to insurance solutions

3.5.12. On the time factor and the defence equation

A fundamental concept in security is the **time factor** which plays a decisive role in defining the most appropriate mitigation strategy. It is based on the fact that a criminal or terrorist act has its own development time for both physical and cyber actions. The ability to avoid the consequences or reduce their extent requires first of all estimating this time. Consequently, all protective measures must contribute to allowing the active protections to intervene. An example is that of the fire-fighting system in which the resistance time of the fireproof material must be greater than the alarm time and the emergency response time.

Concerning physical or cyber-attacks, the **time of penetration,** related to the attacker's objective and means, corresponds to the resistance time of the physical or cyber barriers. This must be greater than the sum of the times of detection of the attack and the time of communication of the alarm and the response to it. Therefore we have: $T_P > T_A + T_I$, called **defence equation**[37] where:

- T_P, is the time for the passive resistance with the contribution of all prevention and transfer measures;
- T_A, is the time required for an alarm to be detected and forwarded;

[37] Biasiotti, A, "Gli impianti di videosorveglianza" (Video surveillance systems), EPC, Italy, 2019.

- **T** $_{I}$, is the time required for the intervention on site of a first responder team from the moment the alarm is raised.

Some **uncertainties must be considered,** such as the attacker's objectives and the means or vehicles, which can be very different. For example, the destructive force of an attack carried out through a vehicle depends on its power and size, whether a truck, a 4x4 or a car, etc. Not surprisingly, some companies use **concentric layer defence** techniques including, for example, armoured gates or doors of varying resistance or obstacles on the ground for the sole purpose of slowing down the assault of criminals and thus adding useful time for the intervention patrol to react. This is also valid in the field of information technology.

3.6. THE PROCESS FOR EMBEDDING SECURITY IN PIARC TCS-TFS

The task assigned by the PIARC Strategic Plan to the Task Force TF 3.1 is embedding security in the TCs-TFs concerned. Some are focused on infrastructure and projects:

- TC 4.2 Bridges
- TC 4.4 Tunnels

Others are topics focused on operation and services:

- TC 1.1 Performance of Transport Administrations
- TC 1.4 Climate change and Resilience of Road Network
- TC 1.5 Disaster Management
- TC 2.1 Mobility in Urban Areas
- TC 2.2 Accessibility and Mobility in Rural Areas
- TC 2.3 Freight
- TC 2.4 Road Network Operation/ITS
- TF 2.1 New Mobility and its Impact on Road Infrastructure and Transport
- TC 3.1 Road Safety
- TC 3.3 Asset Management

The risk management model illustrated so far based on the ISO 31000 standard can be applicable to any TCs and TFs for the management of any type of risk and the process of security risk management will be carried out on their different topic.

The **first step** is to develop two chapters: one on the **general characterization** of the organization, asset or infrastructure and one on the **related security issues**. This is essential to frame the context in which we move. This activity required a literature review as already done in our recent Report on Literature Review[1], including significantly the main reports published in PIARC. Also, direct contacts with the TC - TF Chair and members for the acquisition of guiding elements were carried out.

The **second step** deals with the analysis of the **external context**, as schematically illustrated in the previous chapter 3.1 (**Fig. 6**), requiring a prior collection of data and information on the site, including the geographical location, the type of structure or infrastructure, socio-economic,

political and territorial issues.[38] Based on this information, the definition of areas, situations and critical assets are done.

The **third step** concerns the analysis of the **internal context**, as schematically also illustrated in the previous chapter 3.1. (**Fig. 7**). It concerns a series of spaces that can be interested by criticality such as external areas, external perimeter, internal areas, areas where relevant information, processes or activities are handled such as production, laboratories, control and data processing centres, operation facilities, storage and material handling areas (e.g., warehouses, etc.). The examination of contexts serves to identify vulnerabilities and threats.

The **fourth step** is **threats identification**, as the first phase of the risk assessment sub-process. The identification is based on a work of selection of a checklist of possible threats related to the specific topic between the 41 general threats listed in **Figures 9-1, -2, -3, -4**. Once the general list threats that could constitute possible security risk in the specific topic are identified, other more restricted checklists of threats must be developed in relation to the macro-areas of vulnerability in the external and internal contexts. This process is based on a series of reasoning based on experience and knowledge, following two typical investigative paths: inductive and deductive (**Fig. 18**). We talk about **inductive analysis** proceeding from detail to whole. For example, we think about the likelihood of an attack with explosives in the specific macro-area of vulnerability. On the contrary, a deductive analysis starts from a final event and then goes back to the events that may have caused it or from the failure to the component which caused it. As an example, if inside a building it is recognized to protect imperatively a laboratory, the question arises as to what threats should be considered in the specific macro-area of vulnerability? [39]

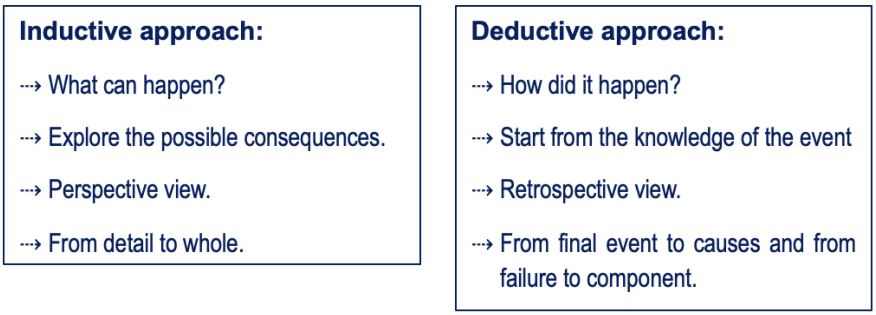


Fig. 18 – Investigative paths for risk identification

The **fifth step** is the second phase of the risk assessment sub-process finalized to **apply the scales of likelihood and consequences** (see previous chapter 3.2.3.).

In the **sixth step**, in relation to the areas of the internal and external contexts, possible major threats are identified based on the score levels defined for likelihood and consequences, as the multiplication between them provides the estimated values of the magnitude of the risk (third phase of the risk assessment sub-process).[40]

[38] For an effective study, photographs, geographical maps, plant layouts, type of site, as well as data, statistics and information would be needed.
[39] It is also useful to remind the English acronym WWWWWWH (who, what, where, when, why, with, how).
[40] Express in k€ or in other currency, the damage caused by the occurrence of the threat must consider both material and immaterial damages, such as damage to image, as well as the possible application of sanctions, such as could happen in the event of a violation of personal data. Security activities often involve the processing of personal data and / or sensitive data. A relevant example is information that is obtained from the management of access control systems, video surveillance, and so on. In EU, following the GDPR

In the **seventh step**, major threats are identified from the comprehensive examination of the highest risk values obtained in the different areas of vulnerability. Priority threats are then established based on this simplified process. Once the priority risks have been highlighted, some cycles of checks must follow on the basis of further evaluations of every possible and different nature (physical, economic, etc.). This according to the perspective of **continuous improvement proposed by the ISO standards** which also concerns the continuous identification of threats and risks.

Directive, it is imperative that all activities of security that involve the processing of these data are carried out in full compliance with the above legislation.

4. RECOMMENDATIONS FOR PIARC TCS-TFS

4.1. TC 1.4 CLIMATE CHANGE AND RESILIENCE OF ROAD NETWORK

4.1.1. Introduction

4.1.1.1. General

The purpose of this chapter is to study the relationship between **climate change and resilience of road network**, topic of TC 1.4, and security. For this, it is necessary to frame such issues in general and then focus on the relationship between climate change and resilience of road network and road security.

Climate change is a **complex issue** that involves physical consequences due to climate change caused by human activities which produced increasing emission of greenhouse gases, in particular CO_2 [41]. This has the effect of warming the planet by a few degrees affecting both the earth's atmosphere and seas[42]. This was accompanied, in the last thirty years, by a lack of recognition of the critical situation by national governments and inertia in the implementation of effective countermeasures. Not to mention the conflicts affecting the weakest and most vulnerable countries and also violent reactions from environmental activists. Climate change is a process of which mankind is increasingly aware of its self-destructive effects and is expected to become a major threat to humanity, for example by creating new and potentially lethal infectious diseases. Catastrophes that, until recently, were exceptional but have now instead become a reality.

The climate of the planet is becoming **unstable and unpredictable** in term of localization, intensity, duration and frequency of the phenomena. Climate change risks vary by country and region. Some regions tend to desertify, as in tropical and subtropical areas, and others to be flooded such as islands and coastal areas that were considered safe in the past. At the same time, some phenomena are modifying the landscape in a permanent way such as the ice caps at the poles and the glaciers on the mountains melting causing a global rise in sea level.[43] Heat waves cause drought and a reduction in crops, with possible famines and therefore a worsening of living conditions for the poorest nations and large migrations of populations.[44]

Global warming is a **threat multiplier**, causing damage to corporate assets, infrastructure, business continuity and supply chain.[45] **Companies and organizations** must face extreme

---

[41] CO2 (carbon dioxide) has a relevant role in the surface temperature of the earth because it absorbs the infrared radiation emitted by the earth's surface and an increase in its concentration in the atmosphere generates a warming of the earth's surface (greenhouse effect). CO2 levels are increasing annually in line with the emissions produced by human industrial activities: the current levels are unprecedented in the last one million years and are 30% higher than any other period in this time frame. At end 2021, CO2 concentration was 415 ppm (parts per million) and at the current rate it will be possible to reach the CO2 concentration of 450 ppm by 2050, with an increase of 3 degrees Celsius temperature of the planet. The previous peak of CO2 concentration occurred about 350 years ago with 300 ppm. Ref. Lawrence M. Kraus "The Physics of Climate Change", 2022, pages 31,37.

[42] The IPCC (Intergovernmental Panel on Climate Change, www.ippcc.ch) climate change projections indicate that the earth will become warmer, some regions will become wetter and some will become drier, sea levels will rise and storm surge height will increase, snow cover and extent of sea ice will reduce, and the frequency and severity of extreme weather events will increase.

[43] The global mean sea level timeseries is an indicator of climate change. From 1995 to 2016 there was an average increase in sea level of about 6,5 cm, a trend of 3.3 mm/year, that includes the ocean's thermal expansion, meltwater from mountain glaciers, and discharge from the Greenland and Antarctic ice sheets, https://climatedataguide.ucar.edu/climate-data/global-mean-sea-level-topex-jason-altimetry.

[44] In "UN Convention to Combat Desertification, Sustainability, Stability, Security", www.unccd.int/sustainability-stability-security

[45] Ref. Allianz Risk Barometer 2022, www.agcs.allianz.com. For 2021, global insured losses from natural disasters have far exceeded $ 100 billion, the fourth highest year on record. Hurricane Ida in the United States was the most expensive event, but more than half of the losses came from so-called secondary damage such as floods, heavy rains, thunderstorms, tornadoes and even winter frosts, which are often local but increasingly expensive. Examples include the winter storm Uri in Texas, the low-pressure phenomenon named

phenomena and corporate business continuity plans must be able to respond. It engages, on one side, **human ingenuity and the ability to adapt** with technical safety countermeasures and, on the other side, mobilizes the **political action of the States** needing to institutionalize the debate at the international level. **Within a short time**, sea level rise, flood risk, depletion of natural resources, land degradation, geological hazards can damage or disrupt infrastructure and affect the operating environment. Therefore, **Road Administrations** must take into account the effects of climate changes on road networks, to ensure their operational effectiveness in increasingly harsh conditions. This topic is covered in the report "Adaptation Methodologies and Strategies to Increase the Resilience of Roads to Climate Change – Case Study Approach", edited by PIARC TC E.1, 2019.[46]

Windier, wetter and wilder weather, greater extremes temperature, sea level rise, significant changes in precipitation patterns and extreme weather events test the **resilience of infrastructure and operational personnel**, suggesting the need for reinforced protection measures in relation to unforeseen and unforeseeable events and it has a significant impact on the design, construction, maintenance and operation of road infrastructure and transport. Moreover, many transport routes are located on coastal roads which are particularly vulnerable to extreme weather events and many pieces of critical infrastructure are exposed to rising sea levels as, for example, some major ports worldwide. In some areas of the world, flood dams are being built or planned; where possible, threatened structures are raised or settlements are moved inland and on higher ground, and the construction of new canals or better maintenance of existing ones is being considered. The transport network is also highly vulnerable to the impact of many external factors which can hinder its ability to provide its intended levels of services. **Operators and managers** are therefore called to address those threats by means of risk assessment and management for response measures based on the philosophy of prevention and resilience. Climate change considerations must be included when working on resilience and preparedness, defence planning, capability delivery, assets and installations, standards, innovation, training, exercises and disaster response.[47] In short, in a **local road network** it is necessary to take into account:

the working conditions of maintenance and operating personnel in hot weather, which may lead to changes in working hours;

the conditions for carrying out maintenance operations in high heat, which may require night work for concreting or laying asphalt;

the conditions of operations in very hot or very cold weather in case of traffic interruption and immobilization of users on the road network, which requires the provision of food and water or cold-resistant clothing;

Bernd, which resulted in catastrophic flooding in Germany and the Benelux, severe flooding in Zhengzhou, China, and heat waves and fires in Canada and California.

[46] "Adaptation Methodologies and Strategies to Increase the Resilience of Roads to Climate Change – Case Study Approach", PIARC TC E.1 Adaptation Strategies and Resiliency, 2019R25EN, 2019, ISBN 978-2-84060-524-9. See it in our LR sheet n.3 in Appendix b.4. It must also be considered the PIARC Report produced subsequently "Refinement of PIARC's International Climate Change Adaptation Framework for Road Infrastructure", 2019R30EN, 2019.

[47] In 2005, the hurricane Katrina, associated with global warming, had a devastating impact in South USA producing other local problems such as the draining of the wetlands, the extraction of groundwater, problems of levee design and maintenance standards, the failure of emergency services.

the conditions of surveillance of some earthworks during the change of precipitation-drought cycle;

the equipment particularly solicited in case of storms, such as road signs, which can lead to oversizing of foundations or to additional stocks.

In the last thirty years the countries in the world have tried to find an agreement on the **reduction of greenhouse gas emissions**. [48] These **negotiations on climate change** have proved very problematic because they ultimately require the transformation of a large part of the global economic structure and lifestyle. The contemporary way of life is causing environmental problems and the transport system is one of the main climate-altering factors. Its innovation according to **environmental sustainability**[49] criteria is the subject of action programmes in many parts of the world, assuming in this sense the more correct term of **ecological transition**.

It is not enough to simply focus on cutting emissions or switching toward non fossil fuel energy to solve the environmental crisis. There are also problems due to the impact of the **overuse of limited resources** of the earth, of **biodiversity reduction**, of **plastic waste**, etc. Each one interacts and accelerates another in a complex network of causes and effects. It is therefore important to avoid solutions that lead to different vulnerabilities. Some modern technologies applied to vehicles consume precious minerals extracted from mines.[50] These lead to other impacts and harmful consequences for the environment. The ecological problem is therefore not only a scientific, economic or political problem, but it is, above all and ultimately, an **ethical issue.**[51] Pollution and climate change threaten our health and **a global sense of responsibility** is needed towards present and future generations. [52]

Road Administrations (RAs) are engaged in prioritising sustainable technologies in procurement to deliver new climate-neutral capabilities and also integrate climate change into the design, construction, maintenance and operation of global road infrastructure. On this issue, the already mentioned PIARC Report of 2019 “Adaptation Methodologies and Strategies to Increase the Resilience of Roads to Climate Change – Case Study Approach”, based on the previous Report of 2015 “PIARC International Climate Change Adaptation Framework for Road Infrastructure” [53] were edited to provide a guide to RAs to increase the resilience of their networks and assets to climate change. The subsequent already mentioned Report of TC E.1, 2019, guides RAs through a

[48] In 1992, in Rio, the emergence of global environmental problems due to global warming and ozone depletion was the issue of the United Nations Framework Convention on Climate Change (UNFCCC). Other annual meetings of all States followed in Parties to the Convention (COP) to review the implementation of the above Convention and the Kyoto Protocol. The Paris Agreement is an international treaty reached on 12 December 2015 by the member states of the United Nations Framework Convention on Climate Change, regarding the reduction of greenhouse gas emissions which envisages limiting average global warming below 2 degrees Celsius compared to pre-industrial period, aiming for a maximum temperature increase of 1.5 degrees Celsius from 2020.

[49] Environmental sustainability means the condition of a development capable of ensuring the satisfaction of the needs of the present generation, without compromising the possibility of future generations to realize their own. The important concept of environmental sustainability requires in particular that the use of renewable resources must not be less than its reintegration and that the pollution of the environment does not exceed the carrying capacity of the environment itself.

[50] Lithium, cobalt, nickel, rare earths are considered "critical" raw materials.

[51] Albert Schweitzer (1875-1965), philosopher, theologian, physician and musician described in his book “Die Ehrfurcht vor dem Leben: Grundtexte aus fünf Jahrzehnten”, his attitude towards the world by speaking of “reverence for life”.

[52] The encyclical of Pope Francis “Laudato Si’”, published in 2015 with the subtitle “Care for Our Common Home,”, focuses on care for the natural environment and people, as well as broader questions on the relationship between God, humans, and the Earth. The humanity now represents a danger to nature and for the first time in history has the possibility of destroying the entire human race and nature itself. This responsibility extends not only to contemporaries but also to future generations. This requires the foundation of a new ethic, a planetary ethic, with the clear difficulty of convincing people to give up immediate advantages of various kinds and make sacrifices for those who are not yet there.

[53] “International Climate Change Adaptation Framework for Road Infrastructure“, PIARC 2015R03EN.

very comprehensive process, enriched by numerous case studies from various parts of the world, through the following steps:

- Identifying scope, variables, risks and data;
- Assessing and prioritizing risks (safety);
- Developing and selecting adaptation responses and strategies;
- Integrating findings into decision-making processes.

The **"Framework" of TC E.1** (2019) proposes a life-cycle and iterative approach to climate change adaptation which applies the general risk assessment process based on ISO 31000:2009[54] international standard and the definitions of ISO Guide 73. In particular, the following main natural parameters, hazards to road network and transportation are considered in the risk assessment process:

- temperature: extreme hot/low temperature, heat/cold waves;
- precipitation: rain, snow, drought;
- landslides: swelling and shrinking of clay soils, rock falls, mudslides;
- wind: extreme wind;
- flooding: sea elevation, fluvial flooding;
- wildfires.

In the mentioned Report of TC E.1 (2019) some **types and reasons for disruption** were considered as in **Figure 4.1.1**[55] . To those types of disruption, traffic restrictions and disrupted operations could also be added. Regarding adaptation measures, **Figure 4.1.2** shows the types of climate change events, impacts and consequences on roads, and adaptation strategies to decrease the likelihood and consequence of impacts.

In the recent PIARC internal document "Terminology on Resilience and Coordination with Related PIARC Technical Committees" of 2021, PIARC TC 4.1[56] informed of the **need to ensure consistency across TCs in the use of key definitions of resilience**[57] under two aspects: road networks and infrastructure. TF 3.1 shares this process and is totally aligned regarding the proposed definition.[58]

[54] ISO 31000:2009 international standard incorporates HB 167:2006 Security risk management standard edited by Australia and New Zealand.
[55] See in "Adaptation Methodologies and Strategies to Increase the Resilience of Roads to Climate Change – Case Study Approach", PIARC TC E.1 Adaptation Strategies and Resiliency, 2019R25EN, 2019, as in previous note.
[56] Report "Terminology on Resilience and Coordination with Related PIARC Technical Committees", PIARC TC 1.4 Climate Change and Resilience of Road Networks, 2021BN1.4EN, 2021.
[57] Resilience is : "The ability of a system, community or society exposed to a hazardous event, a trend or a disturbance, to resist, absorb, accommodate, adapt to, transform, learn and recover from the induced effects in a timely and efficient manner that maintain their essential function, identity and structure". Definition adapted from IPCC, 2019 and UNDRR, 2017.
[58] See paragraphs 2.3 and 8.2. in "Security of Road Infrastructure", Final report of the Task Force C.1., PIARC 2019, Paris, France.

Type of disruption	Reasons for disruption
Bridge closed Tunnel closed Ferry boat is not operating Road closed	Fire (on the road asset or close to the road) Vehicle in the road Drainage failure Accident with dangerous substances Flood Foundation failure Restrictions height – length – width – weight Landslide Quick clay slide Rockfall Avalanche Storm surge Electricity failure Accident point / stretch Wind Adverse weather

Figure 4.1.1 - Summary of the types and reasons for disruption

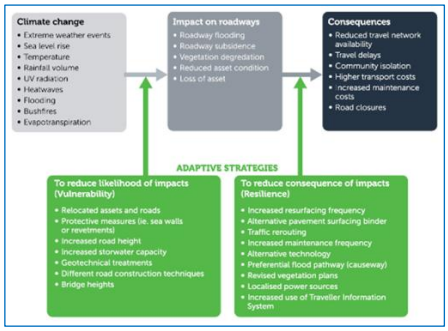


Figure 4.1.2. - Adaptation strategies to decrease the likelihood and consequences of climate change impacts.

4.1.1.2. Climate change and resilience of road network and security

Road networks and transportation are among the causes of climate change and environmental criticalities, and suffer at the same time their consequences. Climate change is a safety threat and also the cause of **security threats**[59] due to the connection between **environmental degradation** that results **and social tensions and possible consequent conflicts this could lead to.** These have various effects on the road infrastructure worldwide. The impact of climate change in term of security is called "environmental security"[60].

Climate change is considered a "**threat multiplier**" that affects human activities: the list of threats focuses on health, food, freshwater management and water scarcity, energy supply, infrastructure, transportation, biodiversity loss and demographic challenges. The consequences are human misery, hunger, desertification, and a substantial increase in migrants fleeing poverty aggravated by environmental degradation.[61] Floods and wild forest fires, droughts and famines devastate communities and increase competition for scarce resources and fuel tensions and conflict.

In road network and transportation, environmental degradation and calamities can be accompanied by an **increase in malicious acts**. An example is the case of forest fires, other forest fires are deliberately set for various reasons including along roads. Acts of vandalism and illegal trafficking may also happen in an area while the police and rescue services are involved in a rescue operation in another area where other disasters may have occurred. In the case of migratory flows, the presence of terrorists or criminals in the means of transport crossing borders cannot be ruled out.

The reaction to the climate crisis in a context of substantial political inertia pushes activists to opt for **more or less violent ecological opposition actions**. Beyond the non-violent one, a radically

[59] "Environmental security and climate change: analysing the discourse", Maria Julia Trombetta, Delft University of Technology, Cambridge Review of International Affairs, 2009.
60 See above studies in the Report on "Adaptation Methodologies …", 2019: as consequence of the lack of "conservation of the local and the planetary biosphere as the essential support system on which all other human activities depend".
[61] "0.6 billion people in Southeast Asia, Middle East, Central Africa and America will be forced to leave their cities by 2100 as the temperature in their urban centres will exceed 50 degrees Celsius for some months of the year." Press conference of 13 September 2022 of the International Federation of Red Cross and Red Crescent Societies (IFRC) and the International Committee of the Red Cross (ICRC), the world's largest humanitarian networks.

opposite approach is **ecoterrorism**[62]**,** which uses or threatens to use violence against innocent victims or property for political reasons related to the environment. The **Eco-war or aggressive non-violence** is when environmental activists reject violence against people and, only partially, against things. Destructions are finalized to stop a technical plant (from service station to a nuclear power plant), a motorway, any vehicles considered polluting (SUVs) or to remove activities or manufactures deemed harmful or illegal. In **bio-sabotage**, living species are used for destruction and sabotage such as in the case of wild boars destroying golf courses, rabbits in airports to damage aircraft, or mice to damage a powerplant.

Environmentally induced conflicts may appear likely in situations where fragility and conflict intersect as in the case of reduced fish stocks and forest destruction. Tensions can also follow the inability to adapt promptly to pressing and rapid environmental changes. This process is likely to occur along the fault-lines between developed and developing areas, national and sub-national. One example is the Mediterranean area, others are in the West and Central Africa and in America. An example is what happens in the **Sahel region**, where people are affected by armed conflict and violence, and the effect of climate change and the deterioration of the security situation can trigger unprecedented challenges for countries in the area.[63] Conflicts, weakened institutions and essential services, poor economies, growing population, lack of social cohesion, reducing biodiversity, affect the pastoralist way of life, agricultural producers, and the activity of fishermen. All of this is exacerbated by the Covid-19 pandemic and terrorism.[64]

Finally, it should be remembered that the worldwide crisis caused by the **Covid-19 pandemic** was not only a scientific and health problem, faced as an emergency or disaster, but above all an ecological issue. The behaviours that caused the climate crisis are the same that increase the chances of a virus to be transmitted from animals to humans. This occurs with the destruction of the environment and ecosystems which not only contributes to global warming but opens up the risk of new pandemics in the future. The deep relationship between environmental crisis and pandemics put us at risk of increased adverse events being multiplied by the intertwined consequences.

---

[62] In this regard, some environmentalists have claimed both the label and the violence it implies. This is in particular the case of the American eco-anarchist mathematician Theodore Kaczynski, nicknamed “Unabomber”, responsible for sixteen attacks. Total toll: twenty-three injured and three dead: a computer shop owner, an advertiser and the president of the California Forestry Association. The legitimacy of this violence - which in this case essentially targets the symbols of the "techno-industrial system" that Kaczynski holds responsible for the situation on the planet - takes two forms: symbolically, terrorism is a way of alerting public opinion by shocking it and, strategically, terrorism wants to respond to the violence of the system with counterviolence. Ecoterrorism can be, in some cases, improperly used to discredit illegal but not dangerous practices and actions. In recent weeks activists have put in place spectacular so called “art actions” in some museums in Europe trying to smear famous paintings still protected by glass. No substantial damage occurred. Another type of actions are roadblocks. In this case tragic consequences can occur as the case that occurred last November in Berlin (Germany) where a woman cyclist died because "Last generation" activists had blocked the A100 motorway causing a delay in the rescue of the woman who had been hit by a concrete mixer. Currently, it is being investigated whether a criminal offense has been committed, exceeding the limit of legitimate protest. Since this is the case of a blocked ambulance, at least the crime of assault is committed.

[63] That is the background of the conflicts unfolding the Sahel zone between peoples of the same country as for example in Mali where people don’t have any more access to fertile land, for example, or access to water. In Niger, land is being restored to counteract the loss of 100,000 hectares of land per year due to degradation and aridification thus countering the phenomena of destabilization and worsening of inter-community tension that all the Sahelian countries are experiencing. This has made results in terms of increased yield and production, agricultural growth and rural poverty reduction.

[64] See Appendix E “Illegal Freight Transport” and Appendix F “Terrorism in Sahel and West Africa” in our LR, 2022.

4.1.1.3. Specific requirements for TC 1.4 from PIARC ToR

The TC 1.4 is composed by two sub-themes:

- 1.4.1. Uniform and holistic methodological approaches to Climate Change and other hazard resilience;
- 1.4.2. Update of the PIARC Climate Change Adaptation Framework.

Security recommendations concern only the second sub-themes, as the first concerns an update of case studies coming from the previous Report of 2019, and the second concerns an update of the processes and methodologies of the PIARC Climate Change Adaptation Framework which includes the contribution of TF 3.1. in the security issue.

4.1.1.4. Methodology and International Standards

The consequences of climate change lead to extreme weather and natural events with **increasing risks** in particular to RAs. These are also pushed towards strategies for reducing the greenhouse effect gas emissions in their operations using new climate sustainable technologies and products. The works of the current TC 1.4 and the TC E.1 in the previous PIARC cycle on the topic of climate change have already developed a "Framework" based on the application of a risk management processes to road network and transportation threatened by such extreme weather and natural events. This is based significantly on the ISO 31000 standard and, as shown in **Figures 4.1.1 and 4.1.2**., a series of adaptation strategies to decrease the likelihood and consequences of climate change were considered.

In the previous paragraph it was highlighted that climate change is not a only security challenge but a **threat multiplier** that exacerbates existing threats and challenges. Therefore, organizations are not only dealing with the climate change challenge in their region, but they're also dealing with threat conflation with other threats such as terrorism, proliferation of weapons, border disputes, resource conflicts, pandemic.

These induced effects are important because they can prevent the **development of mitigation measures** themselves oriented to the safety of people threatened by the effects of climate change. Without environmental security, more conflicts can arise, more instability, more destruction of biodiversity, more pandemics and therefore less safety as well. Therefore, the issue must be considered circular.

ISO has developed **International Standards with guidelines** that provide a high-level framework for environmental management and for adaptation harmonizing the methodologies of the main families of standards [65]. They help organizations to identify, manage, monitor and control their environmental issues in a holistic manner and to understand how current and future climate challenges could affect them. Most of these standards don't have specific references for security but have an indirect influence for a correct corporate approach to security itself. However, they are proposed as a contribution to the work of TC 1.4.

The **ISO 14000 family** comprises a number of standards to manage environmental responsibilities of an organization. They can be applied to any organization engaged in adaptation activities regarding all environmental issues relevant to its operations, such as air pollution, water and

[65] See in this Report Ch. 2.2. "International Standards and Security".

sewage issues, waste management, soil contamination, climate change mitigation and adaptation, resource use and efficiency. These results can be certified. **ISO 14001:2015** *"Environmental management systems"* sets out the criteria for an environmental management system based on the continual improvement concept (PCDA cycle). Related to this topic, **ISO 14004:2016** provides the guidelines on the establishment, implementation, maintenance and improvement of an environmental management system and its coordination with other management systems. **ISO14006:2020** help integrate eco-design into other management systems. **ISO 14064-1:2018** specifies principles and requirements for the quantification and reporting of greenhouse gas (GHG) emissions and removal. **ISO 14050:2020** provides a vocabulary for environmental management.[66] **ISO 14055-1:2017** provides guidelines for combatting land degradation and desertification.[67] Other standards in the family focus on specific approaches such as audits, communications, labelling and life cycle analysis, as well as environmental challenges of climate change. **ISO 14080:2018** includes adaptation to the impacts of climate change and greenhouse gas mitigation in the process of sustainability. The **ISO 1409x series** is relevant for organizations involved in the fields of purchasing, investment and insurance when attempting to understand another organization's climate change adaptations. **ISO 14090** focuses on integrating adaptation within or across organizations by helping to understand the impacts and uncertainties of climate change and how these can be used to inform decisions. **ISO 14091:2021** provides guidance for assessing the risks related to the impacts of climate change. Its use is aimed at reducing vulnerability by addressing medium and long-term adaptation needs and will help all organizations to improve their understanding of system vulnerabilities and how critical these vulnerabilities might be to their operations. **ISO 14092:2020** offers specific guidance for local authorities and **ISO 14097:2021** considers the investments and financing activities related to climate change. In ISO, work is currently underway to develop future adaptation standards that fill gaps in urgent and strategic priority areas. In this regard, **ISO Guide 84: 2020** serves to take into account for climate change in ISO standards. It is aimed at helping to increase disaster preparedness, as well as impacting the resilience of organizations and their technologies, activities or products. Specialized terms and definitions were included. The most recent **IWA 42: 2022** "Net zero guidelines"[68] provides guiding principles and recommendations to enable a global and common approach to achieving net zero greenhouse gas emissions to help limit global warming to 1.5 ° C, reaching net zero by 2050.

Other ISO standards that look at different aspects of management systems are strictly integrated with ISO 14001, such as **ISO 9001** for quality management and **ISO 45001** for occupational health and safety, and **ISO 31000** for the management of the risks related to climate change (**Fig. 4.1.3**).

[66] See in our LR, Appendix B.2 "Standards", Sheet n.2.
[67] See in our LR, Appendix B.2 "Standards", Sheet n.3.
[68] IWA 42: 2022 "Net zero guidelines" was launched by ISO at COP27 Sharm El-Sheikh on November 2022.

	ISO family & relevant standards	Impact on security in climate change and resilience	Topics	Notes
1	9000	1	Specific requirements for quality management systems including security	Quality management has an indirect influence
2	14000	4	Specific requirements for environmental management including security	Specific application
3	27000	2	Specific requirements for information security management systems	General application, in particular for new technologies and for remote surveillance
4	28000	3	Specification for security management systems for the supply chain	Specific focus on the relationship between the supply chain and safety and security of transportation in environmentally critical areas
5	31000	2	Guidelines for managing risk	Basic methodology for risk management
6	20858	1	Framework to assist marine port facilities in security assessment and security plan	Valid for port areas and islands
7	22300	3	Vocabulary of security and resilience	For addressing the complex relationship between security and resilience
8	39000	3	Road traffic safety management systems	For training staff so that they are prepared for extreme events
9	45000	2	Guidance for occupational health and safety management systems	See above also for security aspects
10	IWA-14	2	Specification for vehicle security barriers	For vehicle security barriers
11	CEN/TR 16705	2	Classification for perimeter protection systems	For remote control of areas
12	ADR	3	Specification for the international carriage of dangerous goods by road	To better manage dangerous goods in climatic risk zones
13	ENVISION	5	Guidelines to implement more sustainable infrastructure, resilient and equitable projects	For design of infrastructures that are capable of sustaining climate change

Figure 4.1.3. - Impacts of ISO family & relevant standards on security in T.C 1.4 Climate change and resilience of road network

4.1.2. External and internal contexts

In the **external context**, climate change can also induce relevant security risks, as well as related resilience needs to infrastructure, building, vehicle or people mainly due to possible conflicts in poor and degraded countries or activist demonstration actions up to ecoterrorism in more advanced countries.

In the **internal context**, security risks induced to infrastructure, building, vehicle or people can be of a lower threat level. This is mainly because they have controlled areas and road and adequate levels of internal protection.

The macro-areas of vulnerability, the elements of vulnerability and the threatened assets, related to the security effects to road network and transportation caused by climate change in the external and internal contexts are identified are shown in **the first three columns MAV, EV, TA of Figures 4.1.2-1 and 4.1.2-2**

4.1.3. Risk assessment for TC 1.4 Climate change and resilience of road network

For risk assessment, its necessary a correlate reading between the following **Figures 4.1.2-1, 4.1.2-2, 4.1.3., 4.1.4., 4.1.5., 4.1.6., 4.1.7., 4.1.8. .**

4.1.3.1. Risk identification

In Figure **4.1.3**, we have:

- In **column GT**: security threats for climate change and resilience of road network, in general;

- In **column ST**: security threats for climate change and resilience of road network, specific for WG 1.4.2.

The difference between the two is that the specific security threats vs road network and transportation - in order to integrate the "Framework" of TC 1.4 - do not include natural disasters and climate change because they are not a security threat in themselves but, as explained, are threat multiplier. Safety threats deriving from natural disasters and climate change are the special concern of TC 1.4 (see **Figures 4.1.1 and 4.1.2**).

In **Figure 4.1.2-1 and 4.1.2-2** (column T), different possible threats are considered in the external and internal contexts.

		MAV	EV	TA	ST	L	C	R	
		MACRO-AREAS OF VULNERABILITY	ELEMENTS OF VULNERABILITY	THREATENED ASSET (Security induced effects caused by climate change)	SECURITY THREATS	LIKELI HOOD	CONSE QUENCES	RISKS	Notes
EXTERNAL CONTEXT	1	GEOGRAPHICAL	Locations exposed to any external action such as natural disasters (floods, earthquakes, tsunamis, hurricanes, volcanoes, etc.), pandemic and others for their security effects	Any infrastructure, building, vehicle or people located in an area interested by environmental degradation and subsequent possible social tension and conflict has a vulnerability.	1-5, 9-16, 20-26, 28, 31, 36-37, 39-41	4	4	16	Possible catastrophic effects If located in such areas
	2.1	INFRASTRUCTURAL	Proximity to sites of importance for security purposes (chemical centres, sites at risk of major accidents, fair and exhibition sites, etc.)	Idem, due to explosion or fire	40	1	4	4	Relevant effect but low likelihood
	2.2		Proximity of hubs or networks of (inter)national importance (roads, motorways, railways, airports, ports)	Idem, due to incident or accident	40	2	3	6	Not relevant
	2.3		Proximity to police forces sites, military settlements, fire brigades	Idem, due to protests	40	1	2	2	Not relevant
	3.1	SOCIO-ECONOMIC	Areas with high unemployment rate and a high state of material and social need	Idem, due to protests and crimes against people and things	1-5, 9-16, 19-26, 28, 31-37, 39-41	4	4	16	Extreme risk in case of ecoterrorism
	3.2		Possibility of media attacks, by competitors or customers						Not applicable
	4	POLITICAL	Unstable political context	The same as geographical	1-5, 9-16, 19-26, 28 31-37, 39-41	4	4	16	Extreme risk
	5.1	TERRITORIAL	Presence of micro-crime (theft, robbery, murder, fire, extortion, money laundering, usury)	Idem	1-5, 8-16, 19-22, 39	4	3	12	Moderate effect
	5.2		Presence of organized crime, terrorism	Idem	1-5, 9-16, 19-26, 28, 31-37, 39-41	4	4	16	Extreme risk
	5.3		Activism of anarcho-insurrectionist movements, condition of confessional or racial segregation	Idem		2	2	4	Low likelihood and effects

Figure 4.1.2-1 - External context, risk identification and analysis for TC 1.4 Climate change and resilience of road network

		MAV	EV	TA	ST	L	C	R	
		MACRO-AREAS OF VULNERABILITY	ELEMENTS OF VULNERABILITY	THREATENED ASSET (Security induced effects caused by climate change)	SECURITY THREATS	LIKELI HOOD	CONSE QUENCES	RISKS	Notes
INTERNAL CONTEXT	1	EXTERNAL AREAS	Roads, parking spaces, service vehicles, visitors and supplier vehicles, variable message portals, people	People, vehicles	1-5, 9-16, 20-26, 31, 36-37, 39-41	4	3	12	The consequences are not high because these areas are usually security controlled
	2	EXTERNAL PERIMETER	Accesses, protections	Security personnel, employers, doors and gates, control systems	idem	4	2	8	High likelihood, low effects
	3.1	INTERNAL AREAS	Structures	People, offices, buildings	23-26, 31, 36-37	2	2	4	Possible actions only carried by insiders, not relevant
	3.2		Buildings	Idem	Idem	1	2	2	Idem
	3.3		Roads	Idem	Idem	1	2	2	Idem
	3.4		Vehicles (company, business, employees, visitors, suppliers)	Idem	Idem	1	2	2	Idem
	4.1	OFFICES	Staff	The whole of the employees of an office, administration, company, service	1-5, 8-16, 19-20, 37, 39	1	3	3	For possible actions carried on by insiders
	4.2		Visitors and suppliers	External people who have to access for any reason	Idem	1	3	3	Idem
	4.3		Computer systems and office equipment	Computers and other digital devices, internal digital network	9-10, 16, 39	1	3	3	Idem
	4.4		Information/ communication	Corporate information and communication activities	19	1	3	3	Idem
	5.1	PRODUCTION/ OPERATION FACILITIES	Work areas	Control room, equipment, devices	9-10,12, 16,39	1	3	3	Only staff is allowed to enter, external people are admitted under control
	5.2		Installations	Control room, equipment, devices	Idem	1	3	3	Idem
	5.3		Emergency		Idem	1	3	3	Idem
			Consumable		Idem				Idem
	6	CONTROL/DATA CENTRE	Server	Platforms and data bases	Idem	1	3	3	Idem
	7.1	STORAGE	Dangerous raw materials	Buildings	Idem	1	3	3	Idem
	7.2		Finished products	Buildings	Idem	1	3	3	Idem
	8.1	LABORATORIES	Information/know-how	Computers and other digital devices		1	3	3	Idem
	8.2		Research programs and documents			1	3	3	Idem

Figure 4.1.2-2 - Internal context, risk identification and analysis for TC 1.4 Climate change and resilience of road network

		GT	ST
	Security threats	Climate Change and Resilience of road network in general	Sub-theme 1.4.2 Update of the PIARC Climate Change Adaptation Framework
	Crimes against people		
T 01	Aggression	X	X
T 02	Robbery	X	X
T 03	Mugging	X	X
T 04	Taking hostages	X	X
T 05	Kidnapping	X	X
T 06	Mobbing	0	0
T 07	Stalking	0	0
T 08	Corruption	X	X
	Crimes against things		
T 09	Theft	X	X
T10	Vandalism	X	X
T11	Graffiti	X	X
T12	Arson	X	X
T13	Throwing objects to damage	X	X
T14	Violation of private property, unauthorized entry	X	X
T15	Piracy	X	X
	Crimes against people and things		
T16	Malicious or non-compliant personnel, sabotage	X	X
T17	Communications	0	0
T18	Disclosure of information, espionage	0	0
T19	Misinformation	X	X
T20	Civil protests and strikes	X	X
T21	Illegal transit	X	X
T22	Illegal transport	X	X
	Crimes referable to manifestations of terrorism and or organized crime aimed at people and thing		
T23	Attack with vehicle used as weapon (WAAW)	X	X
T24	Attack with parked vehicle borne improvised explosive device (VBIED)	X	X
T25	Attack with encroaching VBIED	X	X
T26	Attack with penetrative ram vehicle	X	X
T27	Attack with suicide terrorist	0	0
T28	Attack with terrorist and/or threatening phone calls	X	X
T29	Attack with envelope or letter bomb	0	0
T30	CBRNE attack	0	0
T31	Ballistic attack, bombing and blasting	X	X
T32	Cyber attack with malware infiltration	X	X
T33	Cyber attack with subtracting data for ransom	X	X
T34	Cyber attack with direct manipulation	X	X
T35	Cyber attack to the management system	X	X
T36	Attack with Unmanned Vehicles (UAV or drone; AUV or UUV)	X	X
	Unattended and unforeseeable event causing terroristic and criminal attacks or disasters		
T37	Pandemic, epidemic, epidemic outbreak	X	X
T38	Natural disasters and climate change	X	0
T39	Blackout	X	X
T40	Disaster propagation from neighboring infrastructures	X	X
T41	Geopolitical crises, armed clashes or combats, revolutions, uprisings	X	X

GT : general threats for security of road network and transportation
ST : specific threats to integrate security in the "Framework" of TC 1.4 (natural disaters are not a security threat)

v-13, v-4

Figure 4.1.3. - Security threats for TC 1.4 Climate change and resilience of road network

4.1.3.2. Risk analysis

the columns L and C of Figures 4.1.2-1 and 4.1.2-2, show the assessment of the likelihood of the occurrence of threats and the evaluation of consequences. A rating of likelihood in five categories is shown in **Fig. 4.1.4 and** a rating of the potential consequences in five categories is shown as in the following **Figure 4.1.5**.

1.	Rare	>20 years	< 10% of cases
2.	Unlikely	every 10-20 years	< 33%
3.	Moderate	every 4-5 years	< 45 - 50%
4.	Likely	once a year	> 60%
5.	Almost certain	once a month	> 90%

Fig. 4.1.4 - Severity of likelihood for TC 1.4

1.	Insignificant	damage 1000€ - 5.000 €
2.	Minor	damage 5.000€ - 100.000 €
3.	Moderate	damage 100.000€ - 1.000.000 €
4.	Major	damage above € 1.000.000
5.	Catastrophic	extremely high

Fig. 4.1.5 - Severity of consequences for TC 1.4

4.1.3.3. Risk evaluation

In the column R of the Figures 4.1.2-1 and 4.1.2-2, the criticality of the risk is evaluated assigning the score derived from the product L x C = R (also called magnitude following ISO 31000). In it, only the most harmful and dangerous adverse event (extreme or red ones or magnitude 15-25 as shown in Fig. 16 of chapter 3.2.4 this Report) are considered.

The results obtained are summarized in the **Figure 4.1.6** in order to prioritize risks. It can be noted that in the case of tunnels **there are 4 major macro-areas of risks in the external and internal context and 26 priority threats**.

		MACRO-AREAS AND PRIORITY RISKS													
		EXTERNAL CONTEXT					INTERNAL CONTEXT								
		1	2	3	4	5	1	2	3	4	5	6	7	8	
		GEO	INFR	SOC-EC	POL	TERR	EXT A	EXT P	INT P	OFF	P/O	DAT C	STO	LAB	PRIOR
		16		16	16	16									
	Crimes against people														
T 01	Aggression	X		X	X	X									4
T 02	Robbery	X		X	X	X									4
T 03	Mugging	X		X	X	X									4
T 04	Taking hostages	X		X	X	X									4
T 05	Kidnapping	X		X	X	X									4
T 06	Mobbing														
T 07	Stalking														
T 08	Corruption														
	Crimes against things														
T 09	Theft	X		X	X	X									4
T10	Vandalism	X		X	X	X									4
T11	Graffiti	X		X	X	X									4
T12	Arson	X		X	X	X									4
T13	Throwing objects to damage	X		X	X	X									4
T14	Violation of private property, unauthorized entry	X		X	X	X									4
T15	Piracy	X		X	X	X									4
	Crimes against people and things														
T16	Malicious or non-compliant personnel, sabotage	X		X	X	X									4
T17	Communications														
T18	Disclosure of information, espionage														
T19	Misinformation			X	X	X									3
T20	Civil protests and strikes	X		X	X	X									4
T21	Illegal transit	X		X	X	X									4
T22	Illegal transport	X		X	X	X									4
	Crimes referable to manifestations of terrorism and or organized crime aimed at people and thing														
T23	Attack with vehicle used as weapon (WAAW)	X		X	X	X									4
T24	Attack with parked vehicle borne improvised explosive device (VBIED)	X		X	X	X									4
T25	Attack with encroaching VBIED	X		X	X	X									4
T26	Attack with penetrative ram vehicle	X		X	X	X									4
T27	Attack with suicide terrorist														
T28	Attack with terrorist and/or threatening phone calls	X		X	X	X									4
T29	Attack with envelope or letter bomb														
T30	CBRNE attack														
T31	Ballistic attack, bombing and blasting			X	X	X									3
T32	Cyber attack with malware infiltration			X	X	X									3
T33	Cyber attack with subtracting data for ransom			X	X	X									3
T34	Cyber attack with direct manipulation			X	X	X									3
T35	Cyber attack to the management system			X	X	X									3
T36	Attack with Unmanned Vehicles (UAV or drone; AUV or UUV)	X		X	X	X									4
	Unattended and unforeseeable event causing terroristic and criminal attacks or disasters														
T37	Pandemic, epidemic, epidemic outbreak	X		X	X	X									4
T38	Natural disasters and climate change														
T39	Blackout	X		X	X	X									4
T40	Disaster propagation from neighboring infrastructures	X		X	X	X									4
T41	Geopolitical crises, armed clashes or combats, revolutions, uprisings	X		X	X	X									4

v-13

Fig. 4.1.6 Major risk and priority threats for T.C 1.4 Climate change and resilience of road network

4.1.4. Risk treatment

In the **risk treatment** phase, it is necessary establish the mitigation strategy and countermeasures plan for **each 26 major security threats** in relation to the priority risks, as in **Figure 4.1.7**.

	MOST RECURRING SECURITY THREATS IN RELATION TO THE PRIORITY RISKS	GENERAL RECOMMENDATIONS
ST 01	Aggression	GR 1
ST 02	Robbery	GR 1
ST 03	Mugging	GR 1
ST 04	Taking hostages	GR 1
ST 05	Kidnapping	GR 1
ST 09	Theft	GR 1
ST 10	Vandalism	GR 1 – GR 2
ST 11	Graffiti	GR 1 – GR 2
ST 12	Arson without involvement of people	GR 1
ST 13	Throwing objects to damage	GR 1
ST 14	Violation of private property, unauthorized entry	GR 1 – GR 2
ST 15	Piracy	GR 1
ST 16	Malicious or non-compliant personnel	GR 2
ST 20	Civil protests and strikes	GR 2
ST 21	Illegal transit	GR 1
ST 22	Illegal transport	GR 1
ST 23	Attack with vehicle used as weapon (WAAW)	GR 1
ST 24	Attack with parked vehicle borne improvised explosive device (VBIED)	GR 1
ST 25	Attack with encroaching VBIED	GR 1
ST 26	Attack with penetrative ram vehicle	GR 1
ST 28	Attack with terrorist and/or threatening phone calls	GR 1
ST 34	Cyber-attack with direct manipulation	GR 1
ST 35	Cyber-attack to the management system	GR 1
ST 36	Attack with Unmanned Vehicles (UAV or drone; AUV or UUV)	GR 1
ST 37	Pandemic, epidemic, epidemic outbreak	GR 1
ST 39	Blackout	GR 1

Figure 4.1.7 – Security threats leading to priority risks in T.C 1.4 Climate change and resilience of road network

It can be noted that in the case of climate change and resilience **priority threats mainly occur in the external context**. This is because environmental criticality is linked to social and geopolitical problems, locally but also on a planetary scale, bringing about profound transformations.

Within the framework of a mitigation strategy **for all priority threats, the protection, prevention and transfer measures** for the climate change and resilience of road network security measures can be applied as shown in the **Figures 17-1,-2,-3** of chapter 3.3. Such measures must be detailed in relation to the specific contexts.

Regarding the measures for the protection, the subdivision of **active and passive measures and procedural-organizational measures** also apply.

It must be reminded that **any measure taken individually does not guarantee effectiveness** and a good professional must be capable of combining, mixing and dosing them.

4.1.5. Security recommendations

The future of Earth is in our hands. **The latest United Nations report on climate change** reminds us that greenhouse gas emissions in the last decade have been the highest in human history.

This situation results in **more frequent and more intense extreme weather events** resulting in increasingly dangerous consequences on people and things. Food and water insecurity is destined to increase with rising temperatures and consequent socio-political instability in many areas of the planet. It should be remembered that the transport sector is one of the major causes of national emissions of climate-altering gases.

In this critical situation of with an impending global catastrophe, the words of Pope Francis echo across the globe urging us all to take action: "*It is the time to act. We don't have time to wait anymore. Our concern is to see that the environment is cleaner, purer and that it is preserved. We must take care of nature so that it can take care of us.*"

In **Figure 4.1.7** some general recommendations related to the priority threats are proposed, as shown in **Fig. 4.1.8**.

GR 1	**On environmentally induced conflicts**
GR 2	**On action of activists**

Figure 4.1.8 – General recommendations for T.C 1.4 Climate change and Resilience of Road Network

GR 1 – On environmentally induced conflicts

Regarding the **environmentally induced conflicts**, countermeasures are more complex as they require government-level strategies. Two approaches can be considered: the first inspired by precautionary criteria, the second more traditionally oriented to reactive or defensive measures, following the two aspects of attack and defence.

The **reactive-defensive approach** is more military-oriented and comes into play, in particular, in case of terrorists aiming to take advantage of the climate crisis in various ways for their illicit profits and to destabilize a region in the process. It concerns actions of war against terrorists,

traffickers, etc. which leads to casualties and collateral damage. In some cases, the use of mercenaries and proliferation of weapons come into play.[69]

The **holistic and pragmatic attitude** of the precautionary approach oriented to the supervision of the territory and resources is more suitable to tackle complex problems. It seems to be more appropriate educating people to develop resilience if threatened by unsustainable development. It can prevent migration and conflicts. It has also consequences in new police and military practices including conflict prevention, peace-making, peacekeeping and peacebuilding. Regional cooperation, mitigation and adaptation measures are the best solution to fight climate change and insecurity. This is a new concept known as “securitization”, which means to promote a non-hostile approach, as an application of the “precaution through prevention” principle. We must therefore propose solutions to adapt to climate change and to prevent conflicts.

GR 2 – On activism

One security aspect of climate change and resilience, is facing the actions of activists**.** They can include **demonstration as well as acts of eco-terrorism** that are, in general, unpredictable. Particular circumstances such as the pandemic emergency, events such as congresses on climate change or international anti-globalization mobilizations are capable of sparking campaigns to fight against technological progress and climate change.

They require **localized and delimited responses** even if the difficulty in foreseeing where the actions will take place can create problems in particular for road and motorway administrations. On one hand, it’s a problem of preventive police and intelligence while, on the other, it needs a preventive attitude and reactive capacity by the administrations and organizations which are targets of these actions. In particular, after the events that took place in museums and places of historical and cultural heritage, vigilance has increased while bags and bag packs are no longer allowed to be brought inside.

[69] See Appendix E “Illegal Freight Transport” and Appendix F “Terrorism in Sahel and West Africa” in our LR, 2022.

4.2. TC 2.3 FREIGHT

4.2.1. Introduction

4.2.1.1. General

The purpose of this chapter is to study the relationship between TC 2.3 Freight and security**. Freight transport** is an immense and complex issue which affects every aspect of human life, and road freight transport is the simplest and most widespread means of transport in the world. To understand the relationship between **freight transport** and security it is previously necessary to frame briefly the process of **freight transport** in general and see how security comes into play, with particular attention to the application of current relevant topics in the interested sub-themes of TC 2.3.

The **transport of goods in large quantities - called "in bulk" -** concerns materials such as cereals, oil and fuels. Otherwise, the goods can be transported and handled individually within their packaging or with the various package assembly systems. This is especially true for goods that are not particularly bulky but, on the contrary, small, with value. The great variety of shapes and sizes of the **packaging** has led to solutions such as **pallets and containers**[70] to optimize loading and unloading operations and therefore optimize transport chain.

The concept of **logistics**[71] , together with its synonym **supply chain,** was born in industries such as consumer goods, retail, chemical, pharmaceutical, construction material, automotive, metal and steel, paper, packaging and printing. Logistics takes the shape of a real industrial chain with the aim of transporting goods around the world as economically and ecologically as possible. Freight transport and logistics as part of the global supply chain are the sum of **complex processes** with an endless world of combinations and possibilities. In brief, goods in the form of packages, pallets and containers are transported by all means of transportation (vans and trucks, trains, ships, airplanes) and handled in a **logistic centre** (whether a port, autoport, intermodal hubs and cargo hubs). Here, they are loaded and unloaded, opened and packaged by couriers, for new destinations reaching to the final customer.

The following **types of logistics** can be distinguished[72]:

bulk logistics, related to the handling of large quantities of bulk materials (usually raw materials);

industrial logistics, related to the activities of industrial companies and large-scale retail trade;

project logistics, for the management and coordination of major works and infrastructure;

support logistics, related to the management and maintenance, such as for high-tech products, military logistics within which the concept of logistics was born;

---

[70] The "pallets" are wooden platforms of standardized sizes, on which various goods are placed in boxes, bags and various packages, for a maximum capacity of 2000 kg. The “container” is a parallelepiped box in steel, of standardized sizes and capacities, generally equipped on the short side with a double-leaf door, and is capable of carrying up to approximately a maximum of 40 tons of goods. It is the most widespread system in the world for long-distance transport where the initial and final sections are travelled by road. Longer routes are carried out by train, ship or plane.

[71] According to the definition proposed by the Council of Logistics Management in 1986, logistics represents the process by which to plan, implement and control the flow of raw materials, semi-finished and finished products, and related information flows. It goes from the place of origin to the place of consumption, in order to make it as efficient as possible and compliant with customer needs.

[72] Translation from the entry "logistics" in the Dizionario della Logistica (Dictionary of logistics), by G. Leonida, 2023.

reverse logistics, which concerns the return of end-of-life products (or their parts or materials), returned by the customer for damage or change of mind, new re-uses, since waste can become raw material if recycled.

With the development of new information technologies, the concept of **integrated logistics** (or integrated supply chain management) has been able to spread. In it, all phases of the production process, internal and external to the company, are managed, in whole or in part, in a systemic vision. In the integrated logistics, a **physical flow and an information flow** can be distinguished (**Fig. 4.2.1**). The first goes from the producer/supplier to the consumer, the latter arises from the consumer and addresses the producer/supplier.

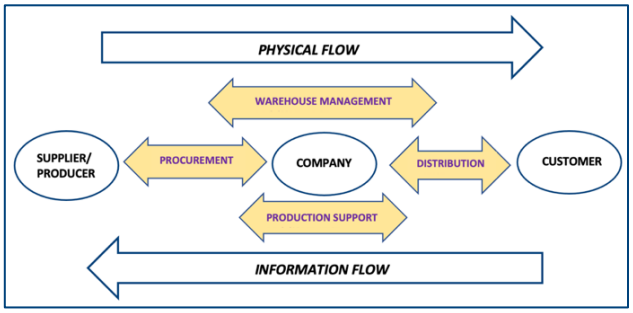


Figure 4.2.1 - Logistics flows

The **physical flow** is the operational aspect of logistics and includes the transport, handling in plants and storage of raw materials, semi-finished and finished products. Physical flow includes the different functions of:

- purchase and supply of raw materials;
- production support;
- warehouse and yard management;
- physical distribution to the final customer;
- recovery.

The **information flow**, on the other hand, includes direct communications between operators and drivers, vehicles and machinery, plants, warehouses, products and customers and concerns:

- information on demand (sales, products, markets);
- logistics planning;
- production programs;
- product requirements plan
- information for supply and delivery.

Optimizing and rationalizing these flows is essential in modern logistics to achieve the objectives of efficiency, rationality, profit and therefore competitiveness.

In the **integrated logistics**, a single transport company can play a bigger or smaller role in the whole logistic flows as a part of the global network of freight transport. In this network, a company can take advantage of **outsourcing** some non-core and specialized business activities (for example, transportation and handling of goods, digital platforms for managing and booking goods, etc.). Effective **infrastructure and communication network** are essential to integrated logistics. Some remarkable challenges in **road infrastructure** are: congestion, low capacity, deterioration,

critical last mile. We must pay close attention to the latter, because the first and last sector of the transport chain are carried out by road carriers. Overloading is a dangerous issue for infrastructure as it can cause damage to bridges and viaducts due to structure fatigue and environmental issues (decarbonization, shift towards lower greenhouse gas emissions modes). Regarding logistics vs **information technology**, adequate telecommunication equipment and networks are essential for the **digital transformation of freight transport and logistics companies** and for the applications of new technologies.

The concept of “Logistics 4.0”

Over the last few years there has been a shift towards a **greater level of automation** in integrated logistics regarding the supply chain, called Logistics 4.0 . A logistics company is therefore no longer limited to just a single part of transport, but has the task of coordinating, from a logistical point of view, the various functions and companies involved, along the entire supply chain with a wider planning and control on the distribution and delivery process. In this context, new information and communication technologies are at the basis of automated functions with a revolutionary impact on the physical and information flows. In this process some **critical issues** related to management of freight transport must be overcome, in relation to the various product categories, including dangerous goods:

- extensive use of automation, interconnection, digitization and cloud computing integration with the advent e-commerce (digitization of transport bills);
- automated scheduling of unloading/loading docks and their management in real time;
- confidentiality and respect for personal data of customers and drivers of all phases of transport and in particular of the delivery phase;
- certainty in delivery and collection times, optimizing loading and unloading times and vehicle routes, for ever faster delivery times starting from the purchase;
- optimal use of fleets and organization of loads to reduce empty runs;
- real-time visibility of the route of the goods;
- energy efficient and environmentally friendly freight transport choosing more sustainable transport mode with the integration of new modes of delivery in urban areas (driverless vehicles, unmanned aerial vehicles, electrification) [73] [74];
- ensuring and improving safety and security of all the steps related to the transport of especially the delivery phase.

Advanced technologies for vehicles management include some IT tools such as ICT, ITS, platooning, automated driving, intelligent roadways. Some applications of new technologies are:

[73] PIARC Report “Truck-Traffic on Highways for Sustainable, Safer and Higher Energy Efficient Freight Transport”, 2019R23EN. In the LR, Sheet n. 9 in Appendix B.4.
[74] PIARC Report “National Policies for Multi-Modal Freight Transport and Logistics”, 2019R24EN. In the LR, Sheet n. 10 in Appendix B.4.

Cooperative Intelligent Transport Systems (C-ITS)[75], Connected cooperative automated mobility (CCAM)[76], Mobility as a service (MaaS)[77] and Self organising logistics (SoI)[78].

The emerging technologies in the transport system [79] play a key role to the **IoT [80] that is boosting innovation in freight transport,** especially in **(Figure 4.2.2**[81]**)**:

data collection: smart sensors internal to the vehicle and also external like radars and cameras and lidar, with the purpose to detect the presence and behaviour of other transport users;

data storage and processing: short-range and long-range connectivity, blockchain to share ledger that everyone trust to be accurate, in particular containing the administration of transactions regularly maintained by a transport company, digital platform that serves as the backbone of the business for operations and customer engagement, taking care of the connected infrastructure and data that powers the services provided, big data to contain larger and complex data sets);

data driven analysis and decision making: artificial intelligence that concerns systems that display intelligent behaviour by analysing their environment and taking actions - with some degree of autonomy - to achieve specific goals**.**

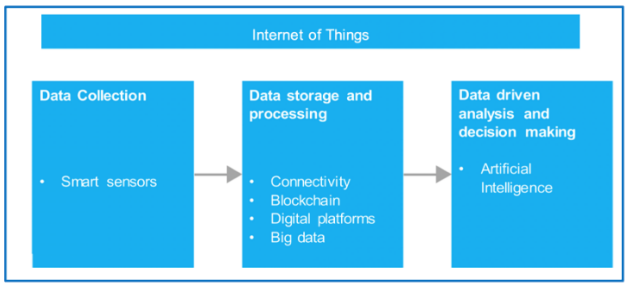


Figure 4.2.2 - Emerging technologies in freight transport

Autonomous driving in the freight sector is based on five levels: first level assisted driving, then semi-autonomous, highly automated driving, fully automated, up to the maximum level of automation with unmanned vehicles communicating with intelligent infrastructure. In an

[75] C-ITS are applications where Intelligent Transport Systems (ITS) e.g. vehicles, infrastructure equipment, traffic control centres, communicate and share information in order to improve road safety, traffic efficiency, comfort, sustainability, etc.. Therefore, even if not provided with intelligence in the strict sense, aim to integrate telecommunications, electronics and information technologies with transport engineering to provide innovative services to different modes of transport and traffic management as well as more information to users. In road transport, they include in particular two types of communication: V2V vehicle-vehicle and V2I infrastructure vehicle.

[76] CCAM is a subcategory of ITS related the networking, automation and coordination of vehicles (also in logistics). It comprises different levels of assisted and automated driving. It ranges from driver assisting features to fully automated vehicles.

[77] MaaS is a type of service that, thanks to a digital platform – in most cases a smartphone app – allows users to plan, book and pay for multiple types of mobility services. Therefore, is the integration of various form of transport services into a single mobility service accessible on demand. It offers transport users access to plan, book and pay for a range of transport services.

[78] SoL refers to decentral coordination of logistic chains, meaning that individual agents in the chain (e.g. companies, vehicles, containers) make autonomous decisions based on local intelligence and local data.

[79] European Parliament, Study requested by the TRAN committee, "The impact of emerging technologies on the transport system", Research for TRAN Committee, European Commission, Policy Department for Structural and Cohesion Policies Directorate-General for Internal Policies - November 2020. In the LR, Sheet n. 2 in Appendix B.5.

[80] In Dictionary of logistics (by G. Leonida, 2023), IoT, literally Internet "of things", or rather "of objects" is a term used for a concept of interrelated computer devices on the basis of which, through the Internet, every object - even of everyday experience - acquires its own identity in the digital world as it becomes "intelligent" and can connect with other objects to exchange the information possessed collected and/or processed. The Internet of Things is based on an interoperable communication protocol. The IoT uses the power of the Internet in a global network of dynamically configured web platforms for connected devices, things and people. In it, physical and virtual things have virtual identities, personalities and are perfectly integrated into the information network. In the transport domain, IoT devices are smart sensors, mechanical and digital machines, object, animals or people provide by unique identifiers.

[81] Ref. note 79.

intelligent infrastructure the so-called self-driving trucks could compensate for the future shortage of new drivers e.g., in closed areas (e.g. ports).

With autonomous driving, connected vehicles and intelligent infrastructures, **the world of transport is experiencing a rapid revolution in just a few years**. Technological innovation is outlining an increasingly efficient, sustainable and interconnected transport landscape. Increasingly digitalized and automated vehicles reduce the risk of human errors and improve fleet flow. It is expected that artificial intelligence (AI) solutions have the potential to support or even take the control to deal with the different vehicles, the large amount of data and the complexity of controlling real-time situations. With its ability to analyse large amounts of data, AI can help management decisions and give economic benefits by boosting the development of the goods sector increasingly in the direction of intermodality, i.e. the possibility of making goods travel using all modes of transport (road, railway, ship, plane), optimizing the routes of goods and reducing their environmental impact. **Some critical issues** in perspective: by 2040 a huge 45% increase in transported goods compared to 2010 is expected, with a decrease in the size of packages; it is clear that roads will not be able to handle this growth, also given the shortage of some million drivers worldwide.

4.2.1.2. Transport of dangerous materials

The **transport of dangerous goods by road** represents only a small percentage of total road transport, however the transport of such materials has a relevant impact on the transport chain related to safety and security issues. These special categories can have severe consequences of due to the leakage of dangerous material in the environment. The main legislation adopted **in Europe is the ADR**[82] that regulates the transport of dangerous goods by road. According to it, dangerous goods are materials and objects the transport of which is prohibited, and can only be authorized under certain conditions. Among these we have high-risk dangerous goods, i.e., goods potentially usable for terrorist purposes and which can therefore cause serious effects not only to environment but also as loss of human lives or mass destruction.

4.2.1.3. Freight and security

Road transport of freight and logistics have a strategical role in a country's economy as shown in the recent pandemic emergency. **Threats impact** strongly the world of freight, and risks can include anything that generates uncertainty related to an organization’s objectives or creates a deviation from the expected path. The strategical, political, social and economic roles of freight

[82] ADR Code (*European Agreement Concerning the International Carriage of Dangerous Goods by Road*) is based on the UN Recommendations and signed in 1957. It has been ratified by numerous European states including all members of the European Union (also extended to national transport). This regulation is applied also in other countries and similar regulation exists as well in other part of the world. In ADR, dangerous goods are divided into 9 classes and many subclasses ranging from explosive material to flammables to toxic, radioactive material and the so-called precursors, i.e., substances which when mixed with others give rise to an explosive. Starting from the 2005 ADR, an entire chapter was introduced in 2019, 1.10, on security to prevent theft, sabotage and attacks. In Europe, two documents have been approved, regulations and guidelines, with obligations for those who sell and obligations for those who buy:

- Regulation (EU) 2019/1148 of the European Parliament and of the Council of 20 June 2019 on the marketing and use of explosives precursors, amending Regulation (EC) No 1907/2006 and repealing Regulation (EU) No 98/2013;
- Communication of the European Commission, Guidelines for the implementation of Regulation (EU) 2019/1148 on the marketing and use of explosives precursors.

As the transport of dangerous goods by road represents only a small percentage of total road transport and the data are collected on the basis of sample surveys, the margins of error in any statistics will be substantial. Any figures for the transport of dangerous goods should be treated with caution. See on this topic the paper: F.Paval, S.Palchetti, “Current road security problems in the Romanian territory due to the illegal transport of dangerous goods”, PIARC WRC, Prague, 2023.

transport and logistic for a country, ignite the interest of crime and terrorism. Therefore, the whole issue of freight transport, since the goods produced are packaged, transported, stored and delivered, presents **physical and cyber security problems.**

Security threats concern not only the load transported, but also the staff (administrators, drivers, and workers), the vehicles, the facilities, the structure and infrastructure, as well as the docks, warehouses, intermodal centres and parking areas. Security incidents can occur in storage and transport with assaults, thefts and robberies. The strong technological component of IT issues with intelligent, connected, data-driven services, process automation and new intelligent digital solutions are vulnerable to security threats as well as procedural and organizational aspect. ITS systems and any platforms for managing supply chain are subjected to cybersecurity risks due to internet threats unless operating on a standalone digital environment.

The use of artificial intelligence (AI) on one hand improves services by making them more performing, on the other increases the likelihood of cyber-attacks as they are able to exploit the vulnerabilities of an information system by autonomously generating malware codes and also by increasing, for example, the capacity for phishing and therefore for scams. This increases the number of attacks and also the pool of potential possible hackers, allowing even the less experienced ones to commit such crimes. On the other hand, AI will facilitate cyber security processes because it will be able to understand, for example, whether an information system has been contacted by a real customer or supplier or not or whether an emergency signal from a driver is true or false.

For the mentioned innovative application C-ITS, CCAM secure communication is crucial since cybersecurity threats are relevant issues, particularly at higher levels of automation. Cyberattacks can be directed to the vehicle itself but also to the infrastructure. In the first case connectivity interfaces can be hacked to tamper the vehicle, potentially generating hazards. ln the latter case, infrastructure can be manipulated to send false information to the vehicle.

Following the digitalization, transport and logistics companies have adopted a business model capable to respond in real time to market needs and surprises that may also arise from security issues which can produce extensive damage and must be avoided. This requires improvements in the ability to forecast, prevent, and respond with agility, all resilient attitudes in the event of external shocks. Being agile and prepared for any kind of disruption, therefore, is an essential business activity in freight transport.

In some countries, transport security has become a big challenge in the trucking sector, due to huge losses to carriers, theft of trucks and cargoes [83]. Attacks on the storage of goods are common. Trafficking of stolen goods is most widespread in areas near the borders since the movement is facilitated from one country to another. Products and food can be distributed in the black market. The highest request is for high level technology merchandise: electronic components and drugs. New technologies can help transport companies in tackling this type of crime. Platforms have also been established for cooperation on investigations in collaboration with the local police forces.

[83] See the Appendix 1.5 “Freight theft” of PIARC Report “Security of Road Infrastructure”, PIARC 2019 EN.

Illicit trafficking is a very common problem in general for all countries, not only for those characterized by an unstable political situation or terrorist infiltration[84]. Crime groups are self-taught and are constantly improving their methodology, technology and infrastructure, resulting in an efficient operational approach. Besides, in some way, they get precise information about the cargo flows and exact time of trips.

Even dangerous goods can travel illegally in disguise across borders. Some transport operators do this by not displaying the appropriate signs on the vehicle, not declaring the origin, place of departure and destination of the load.

Other security problems arise from sabotage in the supply chain. Actions can be made by accident or theft of information or to facilitate hidden criminal activities, sometimes carried out by disloyal employees or drivers. Mafia and crime infiltrations are always possible in particular for the illicit trafficking of goods and migrants.

Contamination of trucks or warehouses when transporting food or containers intended for food can be accidental or voluntary as a form of sabotage. In these areas the control of the presence of pollutants and insects and mice is necessary.

Forms of espionage against customers or activities of a transport company are possible even inside the warehouses. A strict access control of people and vehicles is therefore mandatory.

For goods transport companies, insurance coverage against theft and robbery risk, and any sabotage of products that require quality control, are essential.

Today, transport companies have to be especially wary of global pandemics and cyber criminals aiming to steal sensitive data and information, who are particularly active against more developed countries, especially after the outbreak of the war in Ukraine. Companies also fear the risks to the operational continuity of their supply chain resulting from natural disasters, floods and earthquakes, extreme climate events and political instability with international conflicts and tensions. In this context, it is meaningless to think of acting in watertight compartments or “silos”, tackling one threat at a time alone, but it is necessary to share experiences among companies.

4.2.1.4. Specific requirements for TC 2.3 from PIARC TOR

The TC 2.3 is composed by three sub-themes[85] :

- 2.3.1 Best practices, monitoring and regulation to reduce overloading and associated pavement damage on road networks
- 2.3.2 Greening of freight transport
- 2.3.3 Application of new technologies on freight transport and logistics

Security recommendations concern two of them: 2.3.1 and 2.3.3.

4.2.1.5. Methodology and international standards

General ISO’s standard for risk management, ISO 31000, is the appropriate standard to counter effectively security threats impacting the world of freight, as explained in the previous chapters 2

[84] See Appendix E “Illegal freight transport” in “Road infrastructure and transport security – Literature review”, PIARC Report 2022R07EN.
[85] See PIARC, The World Road Association, “Strategic Plan 2020-2023”, update October 2020, http://www.piarc.org.

and 3 of this Report. ISO 31000 explains the fundamental concepts and principles of risk management, describes a framework, and outlines the processes of risk identification and management. The ISO 31000 family includes: IEC 31010:2019, Risk management – Risk assessment techniques and ISO 31073, Risk management – Vocabulary. A handbook[86], jointly published by the ISO and United Nations Industrial Development Organization (UNIDO), has been developed to support organizations' effort in creating and protecting their values to assist in realizing the multiple benefits offered by ISO 31000.

Transport and logistics companies can refer also to the basic standards ISO 9001 (quality management), ISO 14001 (environmental quality), ISO 27001 (information management systems), ISO family 28000 (supply chain security), where ISO 28001 is particularly devoted to supply chain and ISO 22301 (business continuity).

ISO 28000 encompasses to the various product sectors and establishes the requirements for managing safety along the entire supply chain and for identifying and controlling potential critically issues for people or goods and limiting their possible consequences. Among the crucial aspects taken into consideration are manufacturing, packaging and storage processes, the transfer of goods but also financial aspects, information management and human resources. It is aimed at all players in the supply chain and in particular at logistics companies. It allows you to improve the management of security threats (potential and known), the protection of assets and the reduction of losses related to theft. Among the advantages of ISO 28000 certification there is also the reduction of company insurance premiums through the demonstration of the commitment to guaranteeing the safety of personnel and the safety of goods and services. Finally, with the risk management-based approach, the implementation of ISO 28000 can be integrated with other management systems such as ISO 9001, ISO 14001, ISO 45001, ISO 27000 and Business Continuity.

ISO 22301 certification can verify the ability of organizations to give continuity to the activity in critical situations. It is relevant to any organisation, large or small, in any industry but particularly to freight forwarding and logistics companies operating in high-risk environments. Cyber-attacks, IT failures, but also floods, fires, epidemics and issues in the supply chain are examples of incidents that can pose a substantial threat to the management of any company. ISO 22301 Business Continuity Management System international standard provides the procedures to respond and handle every kind of situation, to have a better understanding of the organization, to implement strategies to ensure business continuity, using appropriate response tactics, to maintain the business continuity plan through exercises and corporate culture reviews. Audit processes help companies identify areas for improvement.

The recent **ISO 15408** (Information technology -- Security techniques -- Evaluation criteria for IT security)[87] is used for the evaluation of the security of IT products and systems, and for procuring them. The standard is used in risk assessment and risk and contains a set of requirements for the

[86] ISO 31000:2018 – Risk management – A practical guide.

[87] In three parts : Part 1: Introduction and general model (15408-1), Part 2: Security functional requirements (15408-2), Part 3: Security assurance requirements (15408-3).

security functions of IT products and systems, as well as assurance measures applied to them during a security evaluation.

A broad look at the international standards and their contents that can be considered as a reference in this context is shown in **Figure 4.2.2 .**

				Impact on security of the sub-themes of TC 2.3	
	ISO family & relevant Standards	Impact on security of freight transportation	Topics	2.3.1 Best practices, monitoring and regulation to reduce overloading and associated pavement damage on road networks	2.3.3 Application of new technologies on freight transport and logistics
1	9000	3	Specific requirements for quality management systems including security		general application
2	14000	3	Specific requirements for environmental management including security		general application
3	27000	4	Specific requirements for information security management systems		general application, in particular for new technology
4	28000	3	Specification for security management systems for the supply chain		general application, specific focus on supply chain
5	31000	2	Guidelines for managing risk		general application
6	20858	3	Framework to assist marine port facilities in security assessment and security plan		is an important reference for the safety of goods not limited only to port areas
7	22300	3	Vocabulary of security and resilience		general application
8	39000	5	Road traffic safety management systems	applies to overloads	general application
9	45000	5	Guidance for occupational health and safety management systems		applies for truck drivers
10	IWA-14	2	Specification for vehicle security barriers		applies to freight transport but not for new technology
11	CEN/TR 16705	3	Classification for perimeter protection systems		applies to the protection of areas affected by logistics and to areas of activity in general, guidelined to devices fro remote control
12	ADR	5	Specification for the international carriage of dangerous goods by road		relevant application for incident prevention
13	ENVISION	2	Guidelines to implement more sustanaible infrastructure, resilient and equitable projects		design of infrastructure, new technology, monitoring for freight transport

Fig. 4.2.2 - Impacts of International Standards for TC 2.3

4.2.2. External and internal contexts

In the **external and internal contexts,** the impact of security related to the application of new technology and the issue of overloading in the activity of freight transportation and logistics depend on the features and dimension of the transport and logistics company. Some of these features are:

- business areas;
- number of employees (level of turnover) and dimension of the vehicle fleet;
- level of innovation (automatization) in the integrated logistics;
- operational scope (local, national, international);
- tangible and intangible assets (physical infrastructure and digital platform for data management);
- interdependencies or correlations (level of outsourcing, use of various modes of transport in the supply chain);
- exposure to harsh external contexts (territorial crime, local conflicts, critical geographic borders).

As we can see, it is a very complex and diverse world of activities that can't be analysed here in general.

The vulnerability for sub-theme 2.3.1 is focused on the issue of security caused by overloading, while for sub-theme 2.3.3 the issues of security for the implementation of new technology in freight are ample and differentiated.

The macro-areas of vulnerabilities, the elements of vulnerability and the threatened assets, related to the security effects to freight transport in the external and internal contexts are shown in the **first three columns MAV, EV, TA of Figures 4.2.3-1 and 4.2.3.2**,

4.2.3. Risk assessment for TC 2.3 Freight

For risk assessment a correlate reading is necessary between the **figures 4.2.3-1, 4-2-3-2, 4.2.4, 4.2.5, 4.2.6, 4.2.7.**

4.2.3.1. Risk identification

As already described in the previous paragraphs, **security threats** concern the whole issue of freight transport. The threats may concern malicious personnel and people, even as an actor himself of the threat. The physical part that is structure, infrastructure, and vehicles, the IT and the procedural and organizational parts. The freight system as a whole is a complex system due to potential chains of events and cascade consequences reflecting on different operational contexts (local, national, international).

In **Fig. 4.2.4**., threats for freight transport and logistics are shown:

in column GT: **all security threats** are relevant for freight in general;

in column ST1: security threats in case of overloading including illegal oversized vehicles;

in column ST2: application of new technologies to freight transport and logistics must include malicious acts to people and things. Aggression and other crimes to people and things can be related to new technologies. In the external context, e.g., in case of aggression to drivers, a truck driver can be taken hostage. In the internal context, problems can arise with personnel or drunk drivers. Illegal transit can be a threat in an operating area causing an unexpected encounter or accident. Prohibited transportation of persons or goods and overloaded transportation must be considered in the implementation of new technology. All crimes referable to manifestations of terrorism and organized crime to people and things are relevant in new technology. Natural disaster and climate change are primarily relevant for safety of new technology in infrastructure such as logistic centres, offices, parking areas but can also produce effects on security.

in column T of Figures 4.2.3-1 and 4.2.3-2, possible threats in the external and internal context and in the different macro-areas of vulnerability are identified.

		MAV	EV	TA	ST	L	C	R	
		MACRO-AREAS OF VULNERABILITY	ELEMENTS OF VULNERABILITY	THREATENED ASSET	SECURITY THREATS	LIKELI HOOD	CONSE QUENCES	RISKS	Notes
EXTERNAL CONTEXT	1	GEOGRAPHICAL	Locations exposed to any external action such as natural disasters (floods, earthquakes, tsunamis, hurricanes, volcanoes, etc.), pandemic and others for their security effects	A logistics centre or any buildings and vehicles related to freight transport located in such an area has a vulnerability.	37, 38, 41	3	4	12	High risk If located in an exposed area
	2.1	INFRASTRUCTURAL	Proximity to sites of importance for security purposes (chemical centres, sites at risk of major accidents, fair and exhibition sites, etc.)	Idem, due to explosion or fire	30, 31	1	4	4	Effect can be relevant but low likelihood
	2.2		Proximity of hubs or networks of (inter)national importance (roads, motorways, railways, airports, ports)	Idem, due to incident or accident	40	2	3	6	Not relevant
	2.3		Proximity to police forces sites, military settlements, fire brigades	Idem, due to protests	20	1	2	2	Not relevant
	3.1	SOCIO-ECONOMIC	Areas with high unemployment rate and a high state of material and social need	Idem, due to protests, strikes and crimes against people and things	1-3, 7-36, 39	4	4	16	If freight transport and logistic centre have a strategic role, extreme risk
	3.2		Possibility of media attacks, by competitors or customers	Reputation	19	4	2	8	Not relevant
	4	POLITICAL	Unstable political context	The whole organization can be vulnerable	All except 4-7, 37, 38	3	4	12	High risk
	5.1	TERRITORIAL	Presence of micro-crime (theft, robbery, murder, fire, extortion, money laundering, usury)	Idem	1-4 7-26, 28, 39	4	3	12	High risk
	5.2		Presence of organized crime, terrorism	Idem	All except 37, 38	4	4	16	Extreme risk
	5.3		Activism of anarcho-insurrectionist movements, condition of confessional or racial segregation	Idem	9-15, 29, 31, 36	2	2	4	Low likelihood and moderate effect

Fig. 4.2.3-1 - External context, risk identification and analysis for TC 2.3 Freight

		MAV	EV	TA	ST	L	C	R	
		MACRO-AREAS OF VULNERABILITY	ELEMENTS OF VULNERABILITY	THREATENED ASSET	SECURITY THREATS	LIKELI HOOD	CONSE QUENCES	RISKS	Notes
INTERNAL CONTEXT	1	EXTERNAL AREAS	Roads, parking spaces, service vehicles, visitors and suppliers vehicles, variable message portals, people	Roads, vehicles, portals, people	1-4, 7-18, 20, 21-24, 30-31, 36, 40-41	3	2	6	Consequences are not high related to new technology
	2	EXTERNAL PERIMETER	Accesses, protections	Security personnel, employers, doors and gates, control systems	9-14, 20, 23-31 36, 39, 41	3	2	6	
	3.1	INTERNAL AREAS	Structures	Docks, warehouse	9, 12, 14, 31, 36, 39	1	4	4	
	3.2		Buildings	People, offices, buildings	9-14, 18, 31, 36, 39	1	4	4	Rare but high consequences to technological devices
	3.3		Roads	Accesses, entrances, exits, parking spaces, people	12, 21, 31, 36	1	3	3	
	3.4		Vehicles	Company, business, employees, visitors, suppliers	12-13, 31, 36	1	2	2	
	4.1	OFFICES	Staff and managers	The whole of the employees of an office, administration, services	1-4. 7-8, 16-18, 36-37	2	2	4	Access control
	4.2		Visitors and suppliers	Personnel, computers and other digital devices, information, buildings	1-3, 8-9, 16, 18, 32-35, 37	2	3	6	Visitors and suppliers are a risk, ex. stuxnet virus spread via a USB flash drive
	4.3		Computer systems and office equipment	Computers and other digital devices, cyberattacks	12, 16-18, 31-35, 39	4	4	16	Extreme risk for physical and cyber-attacks to offices
	4.4		Information/ communication	Internal digital network	17-18, 31-35, 39	4	4	16	Extreme risk for disrupting corporate functions
	5.1	PRODUCTION/OPERATIONF ACILITIES	Work areas	Docks, warehouses	16-17, 36, 39	2	3	6	Possibility of internal sabotage
	5.2		Installations	Equipment, devices (electrical power supply and distribution, lighting, signalling, over-weight vehicle detection, etc.)	16-17, 32-36	2	3	6	idem
	5.3		Emergency	Equipment, devices (fire-fighting systems, smoke and hot gases control, air quality)	16-17, 32-36	2	3	6	idem
	5.4		Consumables	Dangerous materials	16	1	2	2	idem
	6	CONTROL/DATA CENTRE	Server, SCADA systems	Platforms and data bases	16-18, 32-35, 39	4	4	16	Server disruption is an extreme risk
	7.1	STORAGE	Row materials	Dangerous goods	12, 16, 36, 40	1	2	2	
	7.2		Finished products	Dangerous goods	12, 16, 36, 40	1	2	2	
	8.1	LABORATORIES	Staff, specialists, experts	Research programs, documents Information/know-how					Not present
	8.2		Offices	structures					
	8.3		Computers and digital devices	Research programs, Information/know-how					

Fig. 4.2.3-2 - Internal context, risk identification and analysis for TC 2.3 Freight

The specific threats for both WG are also shown above in **Figure 4.2.4** . The aim is to provide a framework of recommendations for the effect of security threats with particular attention to the criticality of WG 2.3.1 and 2.3.3.

		GT	ST1	ST2
	Security hreats	Freight in general	Sub-theme 2.3.1 Best practices, monitoring and regulation to reduce overloading and associated pavement damage on road networks	Sub-theme 2.3.3 Application of new technologies on freight transport and logistics
	Crimes against people			
T 01	Aggression	X	0	X
T 02	Robbery	X	0	X
T 03	Mugging	X	0	X
T 04	Taking hostages	X	0	X
T 05	Kidnapping	X	0	X
T 06	Mobbing	X	0	X
T 07	Stalking	X	0	X
T 08	Corruption	X	0	X
	Crimes against things			
T 09	Theft	X	0	X
T10	Vandalism	X	0	X
T11	Graffiti	X	0	X
T12	Arson	X	0	X
T13	Throwing objects to damage	X	0	X
T14	Violation of private property, unauthorized entry	X	0	X
T15	Piracy	X	0	X
	Crimes against people and things			
T16	Malicious or non-compliant personnel, sabotage	X	0	X
T17	Communications	X	0	X
T18	Disclosure of information, espionage	X	0	X
T19	Misinformation	X	0	X
T20	Civil protests and strikes	X	0	X
T21	Illegal transit	X	X	X
T22	Illegal transport	X	X	X
	Crimes referable to manifestations of terrorism and or organized crime aimed at people and thing			
T23	Attack with vehicle used as weapon (WAAW)	X	0	X
T24	Attack with parked vehicle borne improvised explosive device (VBIED)	X	0	X
T25	Attack with encroaching VBIED	X	0	X
T26	Attack with penetrative ram vehicle	X	0	X
T27	Attack with suicide terrorist	X	0	X
T28	Attack with terrorist and/or threatening phone calls	X	0	X
T29	Attack with envelope or letter bomb	X	0	X
T30	CBRNE attack	X	0	X
T31	Ballistic attack, bombing and blasting	X	0	X
T32	Cyber attack with malware infiltration	X	0	X
T33	Cyber attack with subtracting data for ransom	X	0	X
T34	Cyber attack with direct manipulation	X	0	X
T35	Cyber attack to the management system	X	0	X
T36	Attack with Unmanned Vehicles (UAV or drone; AUV or UUV)	X	0	X
	Unattended and unforeseeable event or harmful voluntary acts causing terroristic or criminal attacks or disaster			
T37	Pandemic, epidemic, epidemic outbreak	X	0	X
T38	Natural disaster and climate change	X	0	X/0
T39	Blackout	X	0	X
T40	Disaster propagation from neighboring infrastructures	X	0	X
T41	Geopolitical crises, armed clashes or combats, revolutions, uprisings	X	0	X

v-13

GT : general threats for security of tunnels
ST : specific threats for security in the sub-themes

X is a threat
0 is not a threat
X/0 possible threat

Figure 4.2.4 - Security threats for TC 2.3 Freight

4.2.3.2. Risk analysis

In the risk analysis phase, the probability of the occurrence of threats (P) and the potential consequences that could derive from them in term of maximum possible damage or maximum probable damage (D) are evaluated as in Figure **4.2.4**

1.	Rare	>20 years	< 10% of cases
2.	Unlikely	every 10-20 years	< 33%
3.	Moderate	every 4-5 years	< 45 - 50%
4.	Likely	once a year	> 60%
5.	Almost certain	once a month	> 90%

Fig. 4.2.5 - Severity of likelihood for TC 2.3

1.	Insignificant	damage 1000€ - 5.000 €
2.	Minor	damage 5.000€ - 100.000 €
3.	Moderate	damage 100.000€ - 1.000.000 €
4.	Major	damage above € 1.000.000
5.	catastrophic	extremely high

Fig. 4.2.6 - Severity of consequences for TC 2.3[88]

4.2.3.3. Risk evaluation

In the column R of the figures 4.2.3-1 and 4.2.3-2, the criticality of the risk is evaluated assigning the score derived from the product L x C = R (also called magnitude following ISO 31000). In it, only the most harmful and dangerous adverse events (extreme or red ones or magnitude 15-25 as shown in Fig. 16 of chapter 3.2.4 this Report) are considered.

The results obtained are summarized in Fig. **4.2.7** in order to prioritize risks. It can be noted that in the case of freight **there are 4 major macro-areas of risks in the external and internal context and 8 priority threats.**

[88] It depends on the size of the company or infrastructure.

		VULNERABILITY AND MAGNITUDE													
		EXTERNAL CONTEXT					INTERNAL CONTEXT								
		1	2	3	4	5	1	2	3	4	5	6	7	8	
		GEO	INFRA	SOC-EC	POL	TERR	EXT A	EXT P	INT A	OFF	P FAC	DAT C	STO	LAB	PRIOR
				16		16				16		16			
	Crimes against people														
1	Aggression			X		X									2
2	Robbery			X		X									2
3	Mugging			X		X									2
4	Taking hostages														
5	Kidnapping					X									1
6	Mobbing					X									1
7	Stalking			X											1
8	Corruption			X		X									2
	Crimes against things														
9	Theft			X		X									2
10	Vandalism			X		X									2
11	Graffiti			X		X									2
12	Arson			X		X				X					3
13	Throwing objects to damage			X		X									2
14	Violation of private property, unauthorized entry			X		X									2
15	Piracy			X		X									2
	Crimes against people and things														
16	Malicious or non-compliant personnel, sabotage			X		X				X		X			4
17	Communications			X		X				X		X			4
18	Disclosure of information, espionage			X		X				X		X			4
19	Misinformation			X		X									2
20	Civil protests and strikes			X		X									2
21	Illegal transit			X		X									2
22	Illegal transport			X		X									2
	Crimes referable to manifestations of terrorism and or organized crime aimed at people and thing														
23	Attack with vehicle used as weapon (WAAW)			X		X									2
24	Attack with parked vehicle borne improvised explosive device (VBIED)			X		X									2
25	Attack with encroaching VBIED			X		X									2
26	Attack with penetrative ram vehicle			X		X									2
27	Attack with suicide terrorist			X		X									2
28	Attack with terrorist and/or threatening phone calls			X		X									2
29	Attack with envelope or letter bomb			X		X									2
30	CBRNE attack			X		X									2
31	Ballistic attack, bombing and blasting			X		X				X					3
32	Cyber attack with malware infiltration			X		X				X		X			4
33	Cyber attack with subtracting data for ransom			X		X				X		X			4
34	Cyber attack with direct manipulation			X		X				X		X			4
35	Cyber attack to the management system			X		X				X		X			4
36	Attack with Unmanned Vehicles (UAV or drone; AUV or UUV)			X		X									2
	Unattended and unforeseeable event or harmful voluntary acts causing terroristic or criminal attacks or disaster														
37	Pandemic, epidemic, epidemic outbreak														
38	Natural disaster and climate change														
39	Blackout			X		X				X		X			4
40	Disaster propagation from neighboring infrastructures					X									1
41	Geopolitical crises, armed clashes or combats, revolutions, uprisings					X									1

v-13

Figure 4.2.7 - Major risk and priority threats for TC 2.3 Freight

4.2.4. Risk treatment

In the risk treatment phase, it is necessary establish a mitigation strategy and countermeasures for **each 8 major security threats** related to the priority risks (**Fig. 4.2.8)**.

ST 16	**Malicious or non-compliant personnel**
ST 17	**Communications**
ST 18	**Disclosure of information, espionage**
ST 32	**Cyber-attack with malware infiltration**
ST 33	**Cyber-attack with subtracting data for ransom**
ST 34	**Cyber-attack with direct manipulation**
ST 35	**Cyber-attack to the management system**
ST 39	**Blackout**

Figure 4.2.8 – Major security threats leading to priority risks for T.C 2.3 Freight

In addition to such threats, **other 2 security threats are of particular concern** for possible evolutions in term of likelihood and consequences (**Fig. 4.2.9**).

ST 12	**Arson**
ST 31	**Ballistic attack, bombing and blasting**

Figure 4.2.9 – Other security threats of particular concern for T.C 2.3 Freight

Within the framework of a mitigation strategy **for all priority threats**, **the protection, prevention and transfer measures** for freight security issue apply as shown in the **Figures 17-1,2,3** of chapter 3.3. Such measures must be detailed in relation to the specific contexts.

Regarding the measures for protection, the subdivision of **active and passive measures and procedural-organizational measures** also apply.

It must be reminded that **any measure taken individually does not guarantee effectiveness** and a good professional must be capable at combining, mixing and dosing them.

4.2.5. Security recommendations

Countermeasures are needed at every segment of the supply chain from (automated) security controls to managing doors and portals, entrances and exit of trucks and vans. Special measures on the security of personnel (e.g., use of passwords) and of the entire IT sector in particular for storing data and for an effective strategy of corporate servers. An internal intelligence service and a strong cooperation with the police force are highly desirable.

General recommendations (GR) for the topic of security of freight transport are in **Fig. 4.2.10**.

GR 1	**Creating a culture of security, raise staff and drivers' awareness on general security issues and specific to the operational context, in order to promptly react to the ever increasing complexity of supply chain.**
GR 2	**Establish a sharing platform between companies regarding business risk, for the various categories of threats, to discuss and have support for priority actions regarding security both at the level of the individual company and at the level of the**

	individual company and the system of companies, always in full respect for the confidentiality of information.
GR 3	**Prepare integrated corporate security plans capable of guaranteeing the continuity of services based on international standards.**
GR 4	**Provide internal access restrictions to internal sensitive areas and prevent unauthorized persons or vehicles from accessing logistic assets (service building, parking areas, docks and warehouses).**
GR 5	**Provide special authorizations for subcontractors and suppliers involved in the supply chain.**
GR 6	**Provide standardized procedures for early detection of an incident, for alerting and for mitigating or neutralizing threats in collaboration with police forces.**
GR 7	**Organize early warning system to act in time in case of a security incident in a transport service abroad and domestically.**
GR 8	**Manage the flow of information, within transportation systems, being aware of sensitive private information: what private information is sharing, who is sharing it with and why they are sharing it. GDPR regulation of European Union helps to be aware about the data that are shared.**
GR 9	**In areas particularly at risk, it is necessary to consider the possibility of creating convoys of escorted trucks.**

Figure 4.2.10 – General recommendations for T.C 2.3 Freight

Further specific recommendations (SR) in relation to the priority threats are detailed below (**Fig. 4.2.11)** :

- SR 1 : On malicious or non-compliant personnel;
- SR 2 : On computer systems and office equipment, information/ communication and data centre;
- SR 3 : On disclosure of information, espionage;
- SR 4 : On black-out.

ST 16	**Malicious or non-compliant personnel**	**SR 1**
ST 17	**Communications**	**SR 2**
ST 18	**Disclosure of information, espionage**	**SR 1, SR 3**
ST 32	**Cyber-attack with malware infiltration**	**SR 2**
ST 33	**Cyber-attack with subtracting data for ransom**	**SR 2**
ST 34	**Cyber-attack with direct manipulation**	**SR 2**
ST 35	**Cyber-attack to the management system**	**SR 2**
T 39	**Blackout**	**SR 5**

Fig. 4.2.11 – Specific recommendations and major security threats for T.C 2.3 Freight

SR 1 - On malicious or non-compliant personnel:

- establish personnel responsibilities and liabilities based on procedures with regular updating and testing sessions,
- establish regular turnovers in key workstations.

SR 2 - On computer systems and office equipment, information/communication and data centre:

- provide staff at all levels with understanding of the technologies and techniques used to battle cyber threats in order to get some base line for cybersecurity to increase the mindfulness and focus towards this target;
- avoid that cybersecurity is a late afterthought that determines the vulnerability of systems and consider that there is an ever-widening gap between security and the dependence on IoT exemplified and amplified in transportation;
- provide autonomous communication and data network between computers and supply chain control systems without internet connection,
- restrict remote access to computer systems,
- use a secure remote-control tool for computer workstations,
- establish a protocol for the use of USB sticks and other data carriers,
- regularly change passwords and usernames connected to computers and control systems,
- systematically authenticate messages for variable message signs,
- provide anti-malware software and software updates,
- establish security requirements for the purchase of IT products and services and for all outsourcing activities;
- implement procedures and instructions for the management and maintenance of computers and control systems,
- do not allow the insertion of remote maintenance modems,
- disable unused ports on switches,
- implement ICT measures to detect anomalies and unauthorized access to communication or control systems,
- implement frequent and complete backups of data and software.

SR 3 - On disclosure of information, espionage:

- implement multilevel security, combining physical and logical defense lines (e.g.: physical barriers, natural surveillance and cameras) for operational areas, offices;
- have an internal intelligence unit.

SR 4 - On blackout:

- have redundant equipment for the supply of energy (electricity, water, fuel, batteries,) and the supply of radio and computer communication networks (copper and optic fibre network);
- alternatively, a minimum requirement is to have systems and equipment that enable to operate the logistic operator after a rupture in the energy or communication chain,

long enough to avoid shorter closure. Particular attention must be paid to the vulnerability of electrical substations.

Finally, in relation of the **2 security threats of particular concern, arson and ballistic attack, bombing and blasting** (**Fig. 4.2.9**), it should be emphasized that these threats have not been considered a priority in relation to the application of new technologies to freight transport as more related to the problem of physical damages. However, an arson or a ballistic attack, bombing and blasting can cause very serious destruction and damage to vehicles and goods warehouses in a logistic centre or at the headquarters of a transport company:

On arson: a deliberate fire or arson can destroy, seriously damage or even temporarily or partially put out of action a logistics centre, a warehouse, or a transport company including vehicles and goods;

On ballistic attack, bombing and blasting:

- it must be considered the possibility of a ballistic attack from the outside which could destroy the offices, as well as the vehicle fleet, the loading-unloading infrastructures and the warehouses where goods can be allocated not only in transit but also in custody;
- in the case of goods of particular importance, of economic or strategic value, it is necessary to establish an external security area adequately controlled and manned with video surveillance and alarm systems 24/24 h. In particular, close cooperation with the police forces is required in such cases;
- the physical location of the logistics plant is important to avoid facilitated access and also escape routes. It should also be considered that the same access routes must allow for the easy arrival of emergency vehicles by the forces of order and the fire brigade. Also pay close attention to buildings and surrounding areas that may be sources of possible threats.

4.3. TC/CT 3.1 Road Safety

4.3.1. Introduction

4.3.1.1. General

The purpose of this chapter is to study the relationship between TC 3.1 Road Safety and security. For this, it is necessary to frame such issue in general and then focus on the relationship between **road safety and road security** with particular attention to the contribution of security to the topics of TC 3.1 sub-themes.

The safety of people in road traffic is one of the primary social and economic aims pursued by a State as the road is a collective property and its safe and free use is a fundamental right of every civil society. Road safety is a very broad and multi-scientific topic and it deals with accidental, in-voluntary threats and also natural events. It includes **three general components (the triangle of road safety or DIV triangle)**: Driver behaviour, Infrastructure design, Vehicle engineering and the related interactions involving human, machine and physical factors (**Figure 4.3.1).**

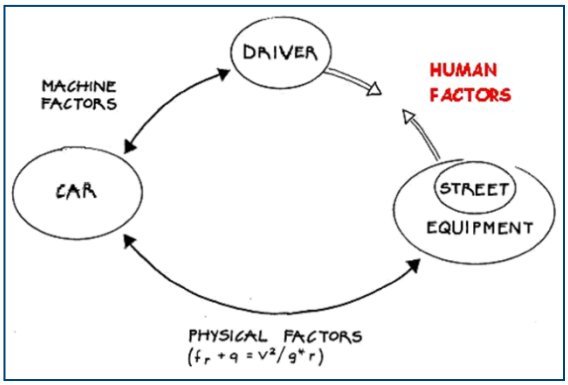


Figure 4.3.1 – The triangle of road safety and its relationships (human, machine, physical factors) (Source: PIARC Road Safety Manual, 2019)

Each driver has a particular perception of the vehicle and the road. A driver can travel by means of the physical relationships established with the vehicle (e.g., the steering wheel, pedals, gearbox, engine) and the information acquired from the vehicle itself and from the road, in a sequence of action and reaction dynamics. The information is acquired, in part, from the instrumentation, digital cockpits, infotainment systems and GPS devices, ADAS[89] equipment in a CAV. Other information is acquired from the road in the form of vertical road signs (e.g., speed limits) and horizontal signs, traffic lights, speed cameras, police check on the road.

Such perception of the driver is totally individual and works on the basis of an **already acquired knowledge** that allows the human brain to associate stored sensory signals (visual, acoustic) with information. Based on that, the brain of a driver can instantly elaborate a prediction which, once obtained, is continuously compared to reality in order to avoid errors. This real time processing is called **"prediction error minimization"** [90] and this action-reaction mechanism takes approximately two seconds.

The rules of the road

It would be advisable to drive anywhere in the world using basically the same rules but there are many differences from country to country in rules, road signs and recommended behaviours. In a country, but also on a continental level as in Europe, America, Oceania, common rules are essential. This makes driving around the world less difficult and unsafe. In a country, the essential set of rules is called "**the rules of the road"**[91], and it is composed by regulations which refer to the national laws that relate to road use. The rules of the road include legal requirements identified by the use of the words "must/must not" and anyone who disobeys these rules is committing an offense which may result in a fine, penalty points on the license or licence suspension and, in the most serious cases, imprisonment. The rules require the driver to stop if an "order" is notified by

[89] ADAS, Advanced Driver Assistance System, deals with electronic systems present on all modern cars and from July 2022 some of them are mandatory in EU even if in some cases they are not yet regulated in many States' rules of road. The ADAS systems allow you to be assisted in driving through active safety components, which work alongside the passive one (such as seat belts and airbags) and help the driver while driving by increasing the level of safety, the most important of which are: Cruise Adaptive Control, Collision Warning, Automatic Emergency Braking, Pedestrian Detection System, Lane Keeping, Traffic Sign Recognition, Night Vision, Driver Monitor System.

[90] See Ch. 4 in A. Seth, "Being you. A New Science of Consciousness", 2021

[91] Denominated in the UK: The Highway Code (see The Highway Code, 22, www.highwaycodeuk.co.uk 07/27/22); in USA: Traffic Code; in France: *Code de la route*; in Spain: *Código de circulación*; in Italy: *Codice della strada.*

police force, or equipped with a paddle or regular badge. Normally, the rules of the road include regulations for:

I. **Drivers:**

- driving any type of vehicle (e.g., cars, trucks, motorcycles, bicycles, powered wheelchairs and mobility scooters, animal-drawn vehicles);
- behaviour rules (e.g., speed, position, right of way, overtaking, level crossings, safe distance, crossroads stopping, parking, towing, use of helmets and chrono tachographs, use/prohibition of alcohol and drugs, adverse weather, sports competitions and pedestrians);
- road traffic in any type of roads, in and out of built-up areas, including single-track and rural or country roads;
- driving licenses and requirements;
- vehicle maintenance (safety and security);

II. **Infrastructure:**

- road definitions and classifications;
- powers and duties of RAs (owners and concessionaires);
- construction, protection of roads and public areas;
- organization of traffic, road signs, road markings, light signals controlling traffic, road works and information signs, signals by authorized personnel;

III. **Vehicles:**

- vehicle classification;
- construction and equipment standards including technical checks;
- vehicle circulation and registration, license plates;
- exceptional vehicles and transports.

Pedestrians must also abide by the rules of road:

- where a carriageway is bordered by spaces dedicated to pedestrians or normally walkable, such as sidewalks or shoulders, pedestrians are required to use them, excluding the carriageway;
- disabled people in wheelchairs can in all cases circulate on the roadway in the absence of suitable sidewalks;
- outside intersections, pedestrians are required to cross the roadway perpendicular to its axis;
- outside built-up areas and unless in situations likely to compromise their safety or special circumstances, pedestrians must stand near the right edge of the roadway in the direction of their travel;
- pedestrians must not stop on the carriageway dedicated to vehicles, except for necessity;
- in an area without pedestrian crossings, pedestrians must yield to drivers;
- pedestrians must not cross the road by passing before buses, trolleybuses and trams parked at stops.

The UN Decades of action in road safety (2011-2020)

Road safety is a serious problem in most countries of the world, from the most developed to the least developed[92]. All this translates into **deaths and injuries which are also an indication of the level of development of road rules** achieved. In some countries or regions of the world is difficult to enforce those rules and the lack of training of drivers, the bad condition and age of cars, the poor quality of roads and the shortage of horizontal and vertical signs, are fundamental causes of this dramatic scenario. It has therefore been suggested to the UN to launch the "Decade of Action in Road Safety" (2011–2020) with the goal of stabilizing and hopefully reducing the levels of global fatalities.

PIARC and road safety

PIARC has been committed to road safety for decades and has made this topic one of its main priorities. In its **Road Safety Manual** [93] (RSM), PIARC decided to provide a relevant contribution to the UN Decade of Action, integrating the Safe System approach [94] to managing road safety. The PIARC RSM was started in 2003, updated in 2015 and its last version was published in 2019. One pillar the RSM, is to encourage the development of comprehensive programs to improve road user behaviour, and sustained or increased enforcement of laws and standards"[95], combined with public awareness/education.

As more recent **PIARC references**, in addition to the on-line Road Safety Manual in its latest update 2019, the following PIARC reports can be mentioned: "Implementation of National Safe System Policies" [96] and "PIARC Road Safety - Case Studies Catalogue"[97].

The report titled **Implementation of national Safe System policies** (2019) deals with a survey of 31 national government agencies to get an understanding of current practices regarding the application of safe road infrastructure. The questionnaire includes progress in relation to national legislation, policies, road safety strategies, safety management systems, road infrastructure funding regimes and initiatives focused on Safe System outcomes. The Safe System approach has been recognized by the UN and other international bodies as a decisive component of improving road safety. It is dealt with in the chapter 4.5 in the PIARC Road Safety Manual[3] which will be referred to later.

The report titled **Road Safety - Case Studies Catalogue** (2019) contains the description of a set of interventions designed, implemented and operated worldwide to improve road safety, in three specific fields: vulnerable road users, human factors and interventions in low and middle-income countries. This report showcases 68 case studies provided by 21 countries and describes situations

---

[92] In a dated 2004 report of the World Health Organization on road traffic injury prevention, 1.2 million deaths and up to 50 million injuries were estimated worldwide each year and projections indicated that these figures would increase by about 65% over the next 20 years unless any commitment to prevention.

[93] PIARC, Road Safety Manual, October 2019, online on: https://roadsafety.piarc.org/en.

[94] See in PIARC RSM, chapter 4.5 : "The Safe System approach places some requirements on the road safety management system:
- recognition and acceptance of the concept of shared responsibility;
- recognition and acceptance of the role of system providers or designers;
- alignment with other policies (e.g., public and occupational health, environment, poverty reduction, mobility and accessibility, etc.), WHO (2004)."

[95] PIARC RSM Chapter 1 Box 2.1 The global plan pillars, Pillar 4: Safer Road users.

[96] PIARC, Implementation of National Safe System Policies, 2019, PIARC 2019R39EN.

[97] PIARC, Road Safety - Case Studies Catalogue, 2019, PIARC 2019R47EN.

in which a safety issue was caused by an incorrect interpretation of the road environment, a misunderstanding by the driver or an unexpected feature of the road or traffic conditions. In many situations, the road environment confused the driver and prevented the intended reaction from taking place. Consequently, operational errors may result in a possible driving mistake and lead to a collision. This catalogue of case studies describes how these critical situations were solved by means of targeted countermeasures, aimed at eliminating or reducing the misleading circumstances created by the road.

The update of the **PIARC Road Safety Manual** 2019 edition, available at PIARC website, was produced on the basis of the previous reports, consisting of three parts.

Part 1 on "Strategic global perspective", provides a description of the scope of the road safety topics and key developments which may influence current approaches to the objectives which are the foundation of RSM;

Part 2 on "Road safety management", provides guidance on the topic, including:

- **road safety management system**, with the guidelines for achieving results to reduce exposure to the risk of death and serious injury, highlighting the importance of leadership and the management capacity of governments and top management **(Fig. 4.3.2)**;
- **Safe System approach** aimed at the long-term goal (Vision Zero) of eliminating death and serious injury. It is based on the examination of contributing factors in road safety engineering and other interventions in order to move from a focus on accident prevention to a focus on death and serious injury prevention;
- **management and effective use of safety data** to address data requirements, the establishment, management and use of databases; data collected from accidents is considered a key source of information in risk assessment and treatment **(Fig. 4.3.2)**;
- **road safety objectives**, investment strategies, plans and projects to establish, grow and consolidate long-term results in road safety investment strategies.

Part 3 on "Planning, Design & Operation" demonstrates the safety impacts and value created by adopting the aforementioned strategies and in particular the Safe System philosophy:

- **role and responsibilities of RAs**, including safe road design for new roads, safety improvements of existing roads, safer outcomes from road maintenance and network operation activities;
- **interaction of human factors**[98] , operational mistakes in machine and vehicle handling, and technical standards and guidelines, for a safer road system (**Fig. 4.3.1**);
- developing policies, standards and guidelines;
- **assessing risks of death and serious injuries** and identifying issues, for example by diagnosing the contributing factors to crashes; road safety audit and reviews;
- intervention, selection and prioritization;

[98] Human Factors is the generic term for those psychological and physiological threshold limit values which are verified as contributing to operational mistakes in machine and vehicle handling (chapter 8.1 PIARC Road Safety Manual).

- **monitoring, analysis and evaluation** (economic, social, demographic, etc.).

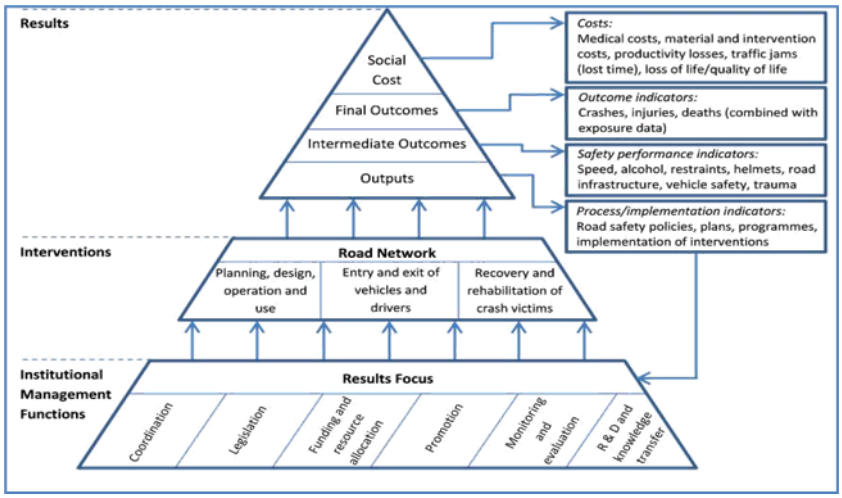


Figure 4.3.2 - Road safety management system and related data requirement
(Source: PIARC RSM adapted from WHO and GRSF)

PIARC's effort for road safety is relevant. The RSM represents an objective of high cultural and humanitarian value. It is a high-level approach, challenging for many countries but especially difficult for poorly developed countries to implement. The level of road safety is closely linked to the economic and social condition of an area and for this reason it can vary greatly within the same country.

Road infrastructure, new technologies and road safety

Road infrastructure refers to the physical structures and facilities that support road transportation, such as roads, bridges, tunnels, and signage. It plays a crucial role in facilitating the movement of vehicles and people.

In the most technologically advanced countries, **new technologies applied to roads and vehicles** can provide an opportunity to achieve relevant improvements in road safety. These concern planning, design, construction, and maintenance of transportation facilities that integrate advanced technologies and communication systems to optimize traffic flow, enhance safety, and improve overall transportation efficiency. These are the so-called Cooperative Intelligent Transport Systems and Services (C-ITS) [99] or simply ITS for roads and infrastructure and the Automated and Connected Vehicles (CAVs) equipped with Advanced Driver Assistance Systems (ADAS).

Road infrastructure is increasingly being equipped with C-ITS or ITS services to be capable to interact even more with the CAVs that will travel along them. A general list is as follows:

- roadside presence of a high bit-rate data communication (V2I);
- continuous coverage of the road axis through connection services;
- wi-fi hot-spots for the connectivity of personal devices;

[99] For example, in EU, European Commission Directive n.40 2010/22/EU of 15 March 2010 for the purposes of adaptation to technical progress and Communication from the European Commission (…) "A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility", COM/2016/0766 final.

- traffic control and management with forecasting models;
- providing travel information to users based on traffic data and forecasts;
- weather conditions monitoring;
- control and management of structures, infrastructure and transport;
- other information: car parks, energy supplies in particular for electric vehicles recharging.

In the era of artificial intelligence (AI), road infrastructure for ITS is becoming more and more important as it enables seamless integration of vehicles, infrastructure and data, to create a more intelligent and connected transportation network. This includes, beyond the use of sensors, cameras, and other monitoring devices to collect real-time data on traffic conditions, the implementation of systems analyzing these data and techniques such as adaptive traffic signal control, dynamic lane management, and intelligent transportation management systems.

The advent of ADAS (Advanced Driver Assistance Systems) and the new CAVs (Connected Autonomous Vehicles) is now a reality. It pushes RAs to make rapid progress in the field of road safety (C-ITS and more) and resolve the long-standing problems. As a direct consequence, while vehicle manufacturers appear to be ready or nearly so, the implementation of new technologies by the RAs will require a gradual improvement in term of rules, driver training, and investments.

Currently **6 levels of ADAS** can be considered[100]:

- Level 0 - No automation, the vehicle is fully controlled by the driver;
- Level 1 - Driving assistance, Adaptive Cruise Control and Lane Keeping;
- Level 2 - Partial automation, with some advanced functions in emergency conditions;
- Level 3 - Conditional automation, the vehicle is autonomously assisted in braking, accelerating and steering, the driver can take control at any time;
- Level 4 - High automation, artificial intelligence (AI) controls the vehicle, the driver supervises the vehicle and can intervene at any time;
- Level 5 - Full automation, the vehicle is fully controlled by AI and the driver becomes a mere passenger.

For example, **integrating vehicle-to-infrastructure (V2I) communication with a level 3 ADAS** enables real-time communication between vehicles and infrastructure to provide drivers with warnings and alerts about potential hazards, such as upcoming road works, accidents, or adverse weather conditions.

[100] Following SAE *Society of Automotive Engineering*, global association of engineers and experts in the aerospace, automotive and commercial-vehicle industries to advance mobility knowledge and solutions. https://www.sae.org

High-definition (HD) maps (**Fig. 4.3.3**), are an essential component of ITS in the era of AI. These maps are created and updated to provide detailed information about the road network to support ADAS systems. They depict the road geometry, lane markings, traffic signs, and other relevant details such as construction zones, accidents, hazards, or adverse weather conditions necessary for autonomous vehicles to navigate. Therefore, enabling CAVs to take decisions and respond to their surroundings in real-time.

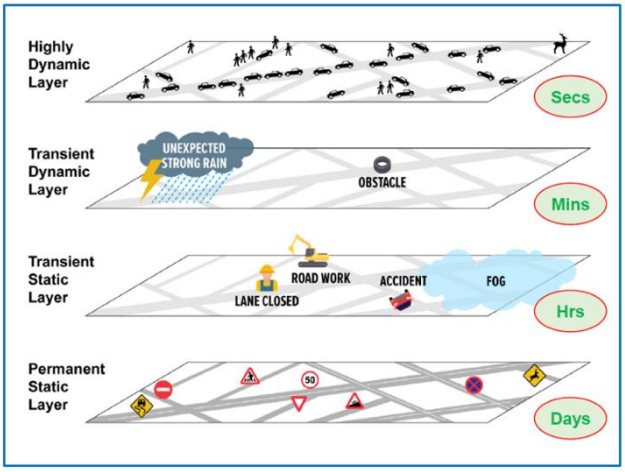


Figure 4.3.3 - HD map scheme with defined layers based on frequency of data change (source: Automotive Edge Computing Consortium)

RAs and road safety

Road signs are often problematic for RAs. Non-compliance of road signs with the highway code can be as high as 50% for vertical signs and over 90% for horizontal signs. **In more recent vehicles,** ADAS systems are currently being implemented starting from levels 1 and 2. As for level 3, CAVs are already operational and, at this level, the perfect legibility of the pictograms of the signals is essential.

Signal inconsistencies can inevitably lead the management software of an AI-driven vehicle to take incorrect decisions and consequently risk accidents. An ADAS automatically reduce the speed of vehicles when its optical device reads the speed limit signs. The question is: what happens when a device in unable to read the speed limit signs in the presence of atmospheric events, such as heavy rain, snowfalls or dense fog? The device will not reduce speed and the driver must react quickly against this unexpected behaviour and regain the control of the vehicle. The driver, in theory, might not be responsible for any negative consequences and might invoke the responsibilities of others according to the regulations currently in force. In the event of poorly-visible signals, the road owner or concessionaire will undoubtedly be held liable.

The application of new technologies requires solving the problems that afflict the road system and which make road safety still a goal to be achieved. Among these is the **chronic lack of road maintenance**, which is often attributed to economic difficulties. This falls under the responsibility of the RAs managing or owning the road but it is often overlooked due to economic difficulties.

The RAs often demonstrate that they neglect the needs of pedestrians (and also cyclists) by favouring vehicles. In many roads, pedestrians are not allowed and their mobility is not protected, since a separation between cars and pedestrians is not guaranteed. Pedestrian crossings should

have good visibility during day and night. But the walkways are often poorly visible and insidious or even non-existent, as well as sidewalks. In some countries, this can cause injuries and deaths. On the other hand, it should be noted that the pedestrians are more protected by road safety rules and in the event of a pedestrian being run over, the driver of the vehicle is responsible for almost all the accidents. If the pedestrian has violated the rules, it is possible to establish at most a contributory fault.

Road tenders and related contracts are fairly widespread problems which often do not guarantee good designs, administrative controls and crime infiltration protection. This leads to short-term solutions and poor-quality materials that do not guarantee due safety over time. This theme then leads back to poor road maintenance.

An epochal transition is taking place, determining a change in terms of responsibility in road safety. If the driver of a traditional vehicle is responsible for his conduct, in perspective, the driver of an ADAS equipped vehicle could not - in principle - be held totally responsible for driving and an assisted and automated driving based on an AI could not be blamed either in case of accidents![101] Regarding the infrastructure, a RA is responsible in their infrastructure domain, and must adapt themselves to these innovations since the perfect operation of road signs will be a functional need for CAVs. Regarding the drivers, the current regulations allowing ADAS vehicles at levels 3 and 4 prescribe that the driver must always be ready to regain at any moment the control of the steering wheel. For that, human reaction times become essential and driving will possibly need not only additional training but also a level of skill and attention even higher than that normally required in traditional vehicles. Furthermore, the coexistence between human-driven vehicles and those with autonomous (or partial) driving will have to be addressed with the related profiles of fault in the event of an accident.

The world of the roads still presents **many shortcomings, insufficiencies, errors and bad behaviours,** and the technological evolution can produce at the same time benefits and uncertainties. **Road safety is in a revolutionary transitional phase,** and in some respects, in unfinished or even unfamiliar land**,** given the current deficiencies both in infrastructure as well as in legal and also behavioural rules, involving particularly the RAs. This situation is becoming further complicated in the field of **road security** where infrastructural and legal technical deficiencies can be exploited by malicious parties to cause damage to people and things.

4.3.1.2. Road safety and security

The topic is that of **security threats to road safety**. Reality has already clearly highlighted how road traffic can be an area where it is possible to consume events that endanger the security of people. Examples are terrorist events have been carried out with the use of road vehicles thrown into the crowd as well as cases of criminals fleeing the wrong way on the highways, and also acts

[101] The OECD defines an Artificial Intelligence (AI) system as a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. The discussion on this point also concerns non-human-controlled combat drones, surgical robots and other AI subjects, i.e., the liability attributable to non-human-controlled AI-equipped machines for malicious intentional actions or negligence. The orientation on the matter is that artificial intelligences are not to blame and therefore cannot be the object of criminal punishment. It therefore appears clear how the development of new technologies generates a vacuum of penal protection than those offenses that cannot be attributable to the human programmer or user or to the machine itself. They must therefore be considered as fortuitous cases sources of an unpredictable and inevitable risk like natural ones which can never be completely cancelled but which can only be stemmed by decreasing their probability and ruinousness ("*Machina Delinquere Non Potest*. Brief notes on artificial intelligence and criminal liability" by Alberto Cappellini, Criminalia, 2019).

of vandalism committed to the detriment of infrastructure, places and public transport. The possibility of these scenarios happening must make grow awareness of RAs in order to be prepared in front of such events, prevent them and limit their effects.

In chapter 2.2 in our previous final Report "Security of Road Infrastructure" [102], published in 2019, **the difference between the two concepts of safety and security** is explained. Differently from safety, security deals with the prevention of risks related to crime, terrorism, and more generally malicious actions and is based on the likelihood and consequences of those intentional attacks. The essential element of security is the voluntary nature of a malicious act, with its harmful consequences to people and things.

Related to road, **security** concerns any action that wants to **disturb the driver-infrastructure-vehicle (DIV) triangle of safety** with the deliberate purpose of doing damage to people or things with as much as possible unforeseen incidental events. The unlawful behaviour of the driver or defaults of the RAs are a matter of safety while any deliberately harmful actions affecting the driver, infrastructure or vehicle and their interactions become a **matter of security**.

Some other considerations are useful to understand the complex relationship between **road safety and security**:

Safety is governed by the necessary binding national laws that have a certain uniformity worldwide; **security is not regulated by law but by the orders of the competent governmental authority** responsible for the security of a territory[103] whose enforcement is mandatory**;** there are also some **national and international standards containing technical guidelines and management patterns**, whose application is totally independent and voluntary.

Safety threats are far less subject to change and are totally regulated by national laws, while **security is vice versa open to an ever-evolving reality of threats**; security must face uncertainty and the complex reality involving adequate corporate strategies and minded-approach[104].

Safety **strategies** are mainly based on statistics of accidents related to the road sections, and security must predict and prevent threats as much as possible.

The **vision** of safety as a legal obligation means that there is a tendency on the part of the RAs to be limited to what is required by law and to neglect the rest; security needs embedding and managing as part of business as usual with a governance, accountability and responsibility, specific policies and processes, personnel training, awareness and security-minded behaviours.

From an **economic standpoint**, security can be considered an additional cost to road safety, but this must be evaluated in the light of the possible consequences; in complex assets such as tunnels and bridges it is even possible to adopt a resilient approach and a smart use of safety measures (e.g., in data collection and processing in control centres) also valuable for security. Examples are information technology and IoT, where safety and security are closely intertwined. Safety ratings can be potentially meaningless unless accompanied by security capabilities.

---

[102] "Security of Road Infrastructure", Final report of the Task Force C.1., PIARC 2019, Paris, France. ISBN 978-2-84060-524-9. Available in English, French and Spanish
https://www.piarc.org/en/order-library/30826-en-Security%20of%20Road%20Infrastructure

[103] For example, in France and Italy it is the Prefect of the Department (F) or of the Province (I).

[104] See the chapter 3 "Security-minded approach" in the above-mentioned Report 2019.

Safety measures can be a **first step in terms of security**, and an integrated and holistic vision suggests **to overcome any "silo" approach.** There is an ever-increasing overlap between safety and security also because in general the consequences of involuntary and voluntary acts may be the same.

A derived aspect of a vision limited to safety, is that it is static, well consolidated on the previous best practices to minimize safety risks and economic costs. So that RAs usually make projects that have proved to be successful in the past. On the contrary, **the vision of security is very dynamic** and is expected to change continuously and rapidly in particular regarding the intelligent transport systems (C-ITS) and automotive cybersecurity.

Conflicts between the needs of safety and security may arise. Control and monitoring systems are implemented for safety to detect hazardous conditions and take action to prevent hazards: i.e., close a tunnel, a bridge, or a section of a road, or evacuate people in the event of fire without obstacles. In a tunnel, it is necessary to allow the evacuation of drivers and passengers in the shortest possible time by using emergency exits. On the other side, security systems refer to the capability to provide adequate confidence that unauthorized persons and systems can neither access the structure or infrastructure nor gain access to system functions to alter or steal software or to cause damage or incidents. Therefore, the access to this type of infrastructure should allow for two-way operation.

Safety and security must also cooperate in **open-air public events**, on the street or in squares, from the village festival with 100 people, to the concert involving thousands of fans.

Safety and Security also overlap in case of **criminal actions, sabotage or vandalism**. These may require a specific design to better protect vehicles and drivers. Therefore, unless roads are designed and managed taking into account human factors, including terrorist, criminal acts and vandalism[105], it is unlikely that road safety can be completely achieved.

Unfortunately, safety and security design are **two engineering disciplines** which as of today still travel, in many cases, on separate paths. Safety standards and associated engineering work practices have substantial application in the civilian field and are mature and well-established, based on decades of learning. On the other hand, security design in the civil world has its roots in the military, police and intelligence fields. It must be considered that if a system is secure, it should be deemed safe. But, on the contrary, if a system is deemed safe then it may not be secure.

CAVs, C-ITS and security

The advent of new technologies of CAVs and C-ITS is **redefining the levels of responsibility.** The driver will become even more a supervisor of the vehicle but will still hold responsibility of commanding the vehicle in case of failure of the CAV. On the side of the vehicles, CAV are subject to specific authorisations by the competent Ministries or Public Authorities in charge, that must verify the technical suitability of the vehicle and suggest best practices in particular for automotive

[105] The effects on road security of vandalism are well explained in the works of Philippe Chanard such as in Appendix D of Literature Review (see previous footnote) “Fight Against Vandalism”, “Vandalism survey results”, PIARC 2021, and “Good Practices and Tips to Limit Theft and Vandalism of Road Assets”, PIARC World Road Congress, Prague, Czech Republic, 2023.

cybersecurity[106]. The RAs, both concessionaires and road owners, will probably carry the greatest burden of responsibility since they must give final authorization to circulate depending on the technical suitability of their infrastructure (as for exceptional transport). Regarding security threats of new technologies, it is evident that RAs will have the responsibility of their effects on road safety, and will have to answer to some relevant questions such as:

- **On the drivers:**
  - How to protect the driver from intentional fake communications on board the vehicle?
  - How to prevent the driver attacking others (by means of the vehicle)?
- **On the infrastructure:**
  - How to protect the infrastructure from being (cyber) attacked?
  - How to mitigate the consequences of an attack (physical or cyber) as fast as possible?
- **On the vehicles:**
  - How to prevent vehicles from being used as a weapon?
  - How to protect the vehicles from being cyberattacked?
- **On the pedestrians:**
  - How to protect the pedestrians from being attacked by users of CAVs and new soft mobility?
  - How to prevent the elderly population from being targeted on the road as pedestrians?

The advent of new technologies also affects the management of the many data that will be collected by these systems. The legal systems of many countries of the world are very sensitive to **personal data protection**, as in particular in the Europe Union[107]. The need to monitor drivers who may be involved in serious responsibilities and crimes can pose problems with regard to the manipulation of such data. CCTV systems that are installed in practically every municipality for safety/security reasons also fall under this legislation. The handling of personal information for these purposes must be done in compliance with the country's data protection law, including cross-border road safety offences investigation. Access to driving license data by public authorities should be properly defined and limited to what is strictly necessary.

Finally, it must be remarked that, **security is not currently adequately understood and considered** by the different entities involved in road management. It is also not usually mentioned in PIARC reports[108] and in the Road Safety Manual except for this Report and those that are

[106] As examples: PAS 1885;2018 "The fundamental principle of automotive cyber security. Specification", ISO/SAE International Standard 21434, "Road Vehicles – Cybersecurity engineering"; "A Code of Practice: Automated Vehicle Trialling – Guidance", UK Department of Transport, January 2022; "Cybersecurity Best Practices for the safety of Modern Vehicles", 2022, National Highway Traffic Safety Administration NHTSA, U.S. Department Administration.

[107] The acronym GDPR stands for General Data Protection Regulation, the regulation in force in the European Union which introduces strict rules on the protection of individuals with regard to the processing of personal data and the free circulation of the same.

[108] Only one mention of security in the PIARC reports was found in the Table 6b of the report "Implementation of national safe system policies", where, as a response to a questionnaire on strategies and policies, to target heavy vehicle collisions, it is noted that in France is mandatory, initial and continuous training including security features.

dedicated specifically to security. It also is a cultural, structural and awareness problem of the RAs. It often happens so that the competences on road safety and security are allocated to different administrations and in particular security is not usually dealt with by the RAs mostly involved in PIARC. Over time, security threats have grown and new forms of criminal and terrorist acts have raised that can involve road infrastructure and transport and necessarily require a different approach. Critical situations due to the pandemic and the current and future consequences of cyberattacks are increasing this awareness. It pushes more and more RAs to begin to actively get involved not only in the applications of new technologies but also in their even more increasing responsibilities regarding security.

4.3.1.3. Specific requirements for TC 3.1 from PIARC TOR

The TC 3.1 is composed by five sub-themes[109]:

- 3.1.1 Specific road safety issues for LMICs;
- 3.1.2 Implementation of proven countermeasures;
- 3.1.3 Update Road Safety Audit Guidelines;
- 3.1.4 Implications of connected and automated vehicles;
- 3.1.5 Update of the Road Safety Manual (for LMICS).

Considering PIARC ToR, security recommendations concern only the sub-theme 3.1.4. Regarding the sub-theme 3.1.5. “Update the Road Safety Manual”, security aspects are not considered in the Road Safety Manual and it would be desirable that security aspects be integrated in it.

4.3.1.4. Methodology and international standards

ISO 31000 is the general ISO’s standard for risk management, and it is also the appropriate standard to effectively counter the impact of security threats in road safety, as explained in previous chapters 2 and 3 of this Report. ISO 31000 explains the fundamental concepts and principles of risk management, describes a framework, and outlines the processes of risk identification and management also valuable in road safety contexts.

Other ISO Standards can be considered relevant for road safety as shown in **Fig. 4.3.4**.

[109] See PIARC, The World Road Association, “Strategic Plan 2020-2023”, update October 2020, http://www.piarc.org.

				Impact of security in the sub-themes of TC 3.1
	ISO family & relevant Standards	Impact of security in road safety	Topics	3.1.4 Implications of connected and automated vehicles
1	9000	3	Specific requirements for quality management systems including security	general application
2	14000	2	Specific requirements for environmental management including security	general application
3	27000	2	Specific requirements for information security management systems	relevant for V2V and V2I communications
4	28000	1	Specification for security management systems for the supply chain	general application, specific focus on supply chain
5	31000	3	Guidelines for managing risk	general application
6	20858	2	Framework to assist marine port facilities in security assessment and security plan	in relation to automatized and connected vehicles
7	22300	3	Vocabulary of security and resilience	general application
8	39000	3	Road traffic safety management systems	specific application for staff involved in operation
9	45000	3	Guidance for occupational health and safety management systems	relevant for road workers on the roads, setting up/repairing road safety furniture, and testing new vehicles in reality
10	IWA-14	1	Specification for vehicle security barriers	general application
11	CEN/TR 16705	2	Classification for perimeter protection systems	general application
12	ADR	5	Specification for the international carriage of dangerous goods by road	general application
13	ENVISION	3	Guidelines to implement more sustanaible infrastructure, resilient and equitable projects	general application

Fig. 4.3.4 - Impacts of International Standards for TC 3.1

ISO 39001 "Road traffic safety management systems — Requirements with guidance for use", defines the requirements aimed at reducing the number of deaths and injuries resulting from road accidents. It can be adopted by any type of organization: private companies, road network managers, public bodies, etc. The stakeholders for the implementation of such a system are companies that generate a large number of road trips for work reasons, companies that transport people or goods, companies that perform public services (e.g. road management, waste collection, companies of transport and logistics, etc.) or of companies that have a network of people on the road with tasks of commercial or operational nature. The standard is designed to adopt the Safe System goal and helps to conduct an assessment of risks from the "road" in such a way as to impose the adoption of all those "reasonably practicable measures" to manage this type of risk. This standard links to other ISO management systems standards.

ISO 45001:2018, and the related **45003:2021** and **45005:2020**, are the international standard for occupational health and safety and also security management in the workplace. It includes stronger leadership, better worker involvement and a focus on health, particularly mental health and allows the recognition of the company's exemption from criminal liability in the event of a serious or fatal injury. 45001 is based on the same structure as ISO 28000 and the other standards coordinated in the IMS group, and it is integrated with the ISO standards dealing with business continuity and disaster recovery. ISO 45001 requires the individual company to assess health and safety risks no longer limited to the internal context but also to consider the external context: territory, suppliers, subcontractors, insurance companies, the cultural factor (skills, knowledge, gender, culture that can influence risks or be influenced by them). This introduces the novelty of applying the PDCA cycle and the risk analysis to be carried out for workers, which puts 45001 at the forefront in the world.

The standard **IWA-14 -1:2013** is for impact testing and performance classification of VSBs also for the protection of sensitive targets and crowded areas. Impact performance deals with vehicle classification, impact speed, impact angle, penetration distance etc. As an example, the impact

testing may concern a 2500 kg vehicle travelling at 48 km/h or a 7200 kg vehicle travelling at 32 km/h a 90-degree angle. The vehicle categories assessed consider UK, European and North American vehicle types. Special tests can prove a twin attack situation, i.e., two vehicles one behind the other. The standard **IWA-14 -2:2013** is supporting the IWA 14-1 to provide guidance on the selection, installation and use of VSBs. **PAS 68:2013 (and PAS 69)** are impact test standard for the UK vehicle fleet (vehicle type and mass) derived from them the European standard **CEN CWA 16221:2010**.

4.3.2. External and internal contexts

The **impact of security in the external and internal contexts of road safety** must be considered in order to prioritize risks and ultimately propose recommendations. The components of the DIV triangle are regulated in each country by a "rules of road" code for which every infringement of these rules creates an unsafe condition for the traffic. It's a security issue to examine the willful damage caused by a physically or virtually harmful attacker on the DIV triangle and their interactions involving the human, machine and physical factors (**Figure 4.3.1)**.

In the **external context**, the DIV triangle can be subjected to various security threats caused by passing through critical areas. The infrastructure are various types of public and private roads: rural, municipal, departmental, national, highways, motorways, under the responsibility and competence of the specific RAs. As demonstrated in our 2019 Report[110], if there are large areas such as intermodal centres where traffic is if little or not controlled at all, this can be used for criminal or terrorist acts. Another possible case is that in which explosions or launch of explosive devices from outside the outer perimeter of a fenced and monitored area can strike inside buildings, persons or vehicles.

In the **internal context**, some security threats can affect the components of the DIV triangle in their internal activities.

The macro-areas of vulnerabilities, the elements of vulnerability and the threatened assets, related to the security effects to road security in its external and internal contexts are shown in the first three columns MAV, EV, TA of **Figures 4.3.4-1 and 4.3.4.2**.

4.3.3. Risk assessment for TC 3.1 Road safety

For risk assessment, a correlate reading between the following **figures 4.3.5-1, 4.3.5-2, 4.3.6, 4.3.7, 4.3.8, 4.3.9** is necessary.

4.3.3.1. Risk identification

The whole issue of road safety, in all its parts as described in the previous paragraphs, presents **security problems.** The threats can concern the drivers - which can become the perpetrators themselves of the threats - , the infrastructure, and the vehicles. Road safety as a whole is extremely complex due to the possible domino effects with cascading consequences. In **Fig. 4.3.6**., threats to road safety are shown:

in column GT: the security threats for road safety in general including malicious acts and those concerning the application of new technologies with more sophisticated acts;

[110] See the Appendix 1.1 "Explosion of a dirty bomb in an urban area" in the above-mentioned Report 2019.

in column ST1: threats related to CAV vehicles.

In the column ST of **Figures 4.3.5-1 and 4.1.5-2**, the possible security threats are considered.

		MAV	EV	TA	ST	L	C	R	
		MACRO-AREAS OF VULNERABILITY	ELEMENTS OF VULNERABILITY	THREATENED COMPONENT IN THE TRIANGLE OF SAFETY	SECURITY THREATS	LIKELIHOOD	CONSEQUENCES	RISKS	Notes
EXTERNAL CONTEXT	1	GEOGRAPHICAL	Locations exposed to any external action such as natural disasters (floods, earthquakes, tsunamis, hurricanes, volcanoes, etc.), pandemic and others for their security effects	Drivers as also pedestrians, infrastructure, vehicles	1-5, 9-13, 15-17, 19, 21-22, 37-39, 41	4	3	12	As derived security effects from natural disaster, and pandemic, crime can take advantage from critical situation to harm to the DIV triangle and CAV. Signs not readable by ADAS systems for adverse meteo. Threats from malicious or non-compliant personnel.
	2.1	INFRASTRUCTURAL	Proximity to sites of importance for security purposes (chemical centres, sites at risk of major accidents, fair and exhibition sites, etc.)	Idem	16, 23-27, 31-36	4	4	16	Traffic restrictions and different types of barriers are required in or near a fair and an exhibition area to avoid attacks from malicious drivers (criminal or terrorist) with vehicles or CAV. Possible negligence by malicious or non-compliant personnel.
	2.2		Proximity of hubs or networks of (inter)national importance (roads, motorways, railways, airports, ports)	Idem	16, 23-27, 30-36	2	5	10	Intermodal centres are a target for criminal or terrorist acts. In case of CBRNE attack, consequences could be catastrophic.
	2.3		Proximity to Police Forces sites, military settlements, Fire brigades	Drivers as also pedestrians, infrastructure, vehicles	23-27, 31, 36	3	3	9	Traffic patrolling required near such sensitive areas to avoid criminal and terrorist attacks with vehicles and CAV, drones, grenade or missile launches or explosions from outside the outer perimeter.
	3.1	SOCIO-ECONOMIC	Areas with high unemployment rate and a high state of material and social need	Idem	1-5, 9-13, 15, 21-27	4	3	12	Possibility of assaults to infrastructure and hijackings to private and public transport (buses, taxis). Threats from illegal transport and malicious or non-compliant personnel.
	3.2		Possibility of media attacks, by competitors or customers	None					
	4	POLITICAL	Unstable political context	Drivers as also pedestrians, infrastructure, vehicles	1-5, 9-13, 15, 16, 21-27	5	4	20	Possibility of assaults in private and public transport and infrastructure due to political riots can cause deaths. Malicious or non-compliant personnel.
	5.1	TERRITORIAL	Presence of micro-crime (theft, robbery, murder, fire, extortion, money laundering, usury)	Idem	1-5, 9-13, 15, 16, 21	5	3	15	Assaults in private and public transport and infrastructure. Threats to vehicles when parked (especially CAV and carrying dangerous goods). Threats from signs unreadable by ADAS vehicles due to tampering and malicious or non-compliant personnel.

	5.2		Presence of organized crime, terrorism	Idem	1-5, 9-13, 15, 21-27, 31, 36. 39-41	5	4	20	Same as above, aggravated by terrorism can cause deaths, as unregulated drone flight .
	5.3		Activism of anarcho-insurrectionist movements, condition of confessional or racial segregation	Idem	1-5, 9-13, 15, 21-27, 31, 39-41	5	3	15	As above

v-10

Fig. 4.3.5-1 - External context, risk identification and analysis for TC 3.1 Road Safety

		MAV	EV	TA	ST	L	C	R	
		MACRO-AREAS OF VULNERABILITY	ELEMENTS OF VULNERABILITY	THREATENED ASSET	SECURITY THREATS	LIKELIHOOD	CONSE QUENCES	RISKS	Notes
INTERNAL CONTEXT	1.1	DRIVER	Driver as a person	Physical person	1-5, 13, 37	5	3	15	Verbal aggression mugging, stabbing. In pandemic, attempt to induce contagion.
	1.2		Information/ communication	Driver's mobile phone and on-board info/communication system	32, 34	5	2	10	Included V2V and V2I, subtraction of the personal data
	2.1	INFRASTRUCTURAL	Structures	Communication network, C-ITS, digital message boards	9,10, 12, 13, 16. 32, 35	4	4	16	Any device or system if connected to interned by cable or wi-fi
	2.2		People, offices, buildings	traffic control centres, operators	1-5. 9-13. 16, 19, 21-22, 23-27, 31-36, 39	4	4	16	Idem
	2.3		Roads	Vertical and horizontal signs	9-13	5	3	15	Vandalism
	3.1	VEHICLE	ADAS system	Driving assistance, cruise adaptive control and lane keeping and all automations if connected to internet	32-35	5	4	20	Interference in the internal devices of a CAV, hijacking or remote theft by hackers can cause deaths

v-10

Fig. 4.3.5-2 - Internal context, risk identification and analysis for TC 3.1 Road Safety

		GT	ST1
	Security threats	Road safety in general	Sub-theme 3.1.4 Implications of connected and automated vehicles
	Crimes against people		
T 01	Aggression	X	X
T 02	Robbery	X	0
T 03	Mugging	X	0
T 04	Taking hostages	X	0
T 05	Kidnapping	X	0
T 06	Mobbing	0	0
T 07	Stalking	0	0
T 08	Corruption	0	0
	Crimes against things		
T 09	Theft	X	X
T10	Vandalism	X	X
T11	Graffiti	X	X
T12	Arson	X	0
T13	Throwing objects to damage	X	X
T14	Violation of private property, unauthorized entry	0	X
T15	Piracy	X	X
	Crimes against people and things		
T16	Malicious or non-compliant personnel, sabotage	X	0
T17	Communications	0	0
T18	Disclosure of information, espionage	0	X
T19	Misinformation	X	X
T20	Civil protests and strikes	0	0
T21	Illegal transit	X	0
T22	Illegal transport	X	0
	Crimes referable to manifestations of terrorism and or organized crime aimed at people and thing		
T23	Attack with vehicle used as weapon (WAAW)	X	X
T24	Attack with parked vehicle borne improvised explosive device (VBIED)	X	X
T25	Attack with encroaching VBIED	X	X
T26	Attack with penetrative ram vehicle	X	X
T27	Attack with suicide terrorist	X	X
T28	Attack with terrorist and/or threatening phone calls	0	X
T29	Attack with envelope or letter bomb	0	X
T30	CBRNE attack	X	0
T31	Ballistic attack, bombing and blasting	X	X
T32	Cyber attack with malware infiltration	X	X
T33	Cyber attack with subtracting data for ransom	X	X
T34	Cyber attack with direct manipulation	X	X
T35	Cyber attack to the management system	X	X
T36	Attack with Unmanned Vehicles (UAV or drone; AUV or UUV)	X	X
	Unattended and unforeseeable event or harmful voluntary acts causing terroristic or criminal attacks or disaster		
T37	Pandemic, epidemic, epidemic outbreak	0	0
T38	Natural disaster and climate change	X	X
T39	Blackout	X	X
T40	Disaster propagation from neighboring infrastructures	X	X
T41	Geopolitical crises, armed clashes or combats, revolutions, uprisings	X	X

GT : general threats for security related to raod safety
ST : specific threats for security in the sub-themes

X is a threat
0 is not a threat

v-13

Fig. 4.3.6 - Table of threats for TC 3.1 Road Safety

4.3.3.2. Risk analysis

In columns L and C of Figures 4.3.5-1 and 4.3.5-2, the assessment of the likelihood of the occurrence of security threats to road safety and the evaluation of consequences is made. A rating of likelihood in five categories is shown in **Fig. 4.3.7** and a rating of the potential consequences in five categories is shown in **Fig. 4.3.8**. Here consequences are defined in terms of damage cost. It can be considered or added the cost of the number of deaths (e.g., about 1.500.000 € per pers.), seriously injured (e.g., 150.000 € per pers.) and slightly injured (e.g., 5.000 € per pers.).[111]

1.	Rare	>20 years	< 10% of cases
2.	Unlikely	every 10-20 years	< 33%
3.	Moderate	every 4-5 years	< 45 - 50%
4.	Likely	once a year	> 60%
5.	Almost certain	once a month	> 90%

Fig. 4.3.7 - Severity of likelihood for TC 3.1

1.	Insignificant	damage 1000 € - 5.000 €
2.	minor	damage 5.000 € - 100.000 €
3.	moderate	damage 100.000 € - 1.000.000 €
4.	major	damage above € 1.000.000
5.	catastrophic	extremely high

Fig. 4.3.8 - Severity of consequences for TC 3.1

4.3.3.3. Risk evaluation

In column R of Figures 4.3.4-1 and 4.3.4-2, the criticality of the risk is evaluated assigning the score derived from the product L x C = R (also called magnitude following ISO 31000). In it, only the adverse event most harmful and dangerous (extreme or red ones or magnitude 15-25 as shown in Fig. 16 of chapter 3.2.4 this Report) are considered.

The results obtained are summarized in **Fig. 4.3.9** in order to prioritize risks. It can be noted that in the case of road safety **there are 6 major macro-areas of risks in the external and internal context and 13 priority threats**.

[111] It should be noted here that the security's events (like terrorist attack for instance) are not accidental but intentional. Therefore, they are not random events as the safety's ones (like fire in tunnels). So, in the security field, likelihood is not determined on classic a statistic approach but is assessed on a reasonable prediction of terrorist intentions and capabilities. The safety approach is based on statistics of accidents correlated with the road sections, the security must as far as possible anticipate the unpredictable.

		VULNERABILITY AND MAGNITUDE								
		EXTERNAL CONTEXT					INTERNAL CONTEXT			
		1	2	3	4	5	1	2	3	
		GEO	INFRA	SOC-EC	POL	TERR	DRI	INFRA	VEH	PRIOR
			20		20	20	15	16	20	
	Crimes against people									
1	Aggression				X	X	X	X		4
2	Robbery				X	X	X	X		4
3	Mugging				X	X	X	X		4
4	Taking hostages				X	X	X	X		4
5	Kidnapping				X	X	X	X		4
6	Mobbing									
7	Stalking									
8	Corruption									
	Crimes against things									
9	Theft				X	X		X		3
10	Vandalism				X	X		X		3
11	Graffiti				X	X		X		3
12	Arson				X	X		X		3
13	Throwing objects to damage				X	X	X	X		4
14	Violation of private property, unauthorized entry									
15	Piracy				X	X				2
	Crimes against people and things									
16	Malicious or non-compliant personnel, sabotage		X		X			X		3
17	Communications									
18	Disclosure of information, espionage									
19	Misinformation							X		1
20	Civil protests and strikes									
21	Illegal transit				X	X		X		3
22	Illegal transport				X	X		X		3
	Crimes referable to manifestations of terrorism and or organized crime aimed at people and thing									
23	Attack with vehicle used as weapon (VAAW)		X		X	X		X		4
24	Attack with parked vehicle borne improvised explosive device (VBIED)		X		X	X		X		4
25	Attack with encroaching VBIED		X		X	X		X		4
26	Attack with penetrative ram vehicle		X		X	X		X		4
27	Attack with suicide terrorist		X		X	X		X		4
28	Attack with terrorist and/or threatening phone calls									
29	Attack with envelope or letter bomb									
30	CBRNE attack									
31	Ballistic attack, bombing and blasting				X	X		X		3
32	Cyber attack with malware infiltration		X				X	X	X	4
33	Cyber attack with subtracting data for ransom		X					X	X	3
34	Cyber attack with direct manipulation		X				X	X	X	4
35	Cyber attack to the management system		X					X	X	3
36	Attack with Unmanned Vehicles (UAV or drone; AUV or UUV)		X			X		X		3
	Unattended and unforeseeable event or harmful voluntary acts causing terroristic or criminal attacks or disaster									
37	Pandemic, epidemic, epidemic outbreak						X			1
38	Natural disaster and climate change									
39	Blackout					X		X		2
40	Disaster propagation from neighboring infrastructures					X				1
41	Geopolitical crises, armed clashes or combats, revolutions, uprisings					X				1

v-13

Fig. 4.3.9 - Major risks and priority threats for TC 3.1

4.3.4. Risk treatment

In the risk treatment phase, it is necessary to establish the mitigation strategy and a countermeasure plan for **each 13 major security threats** related to the priority risks (**Fig. 4.3.10)**.

ST 1	**Aggression**
ST 2	**Robbery**
ST 3	**Mugging**
ST 4	**Taking hostages**
ST 5	**Kidnapping**
ST 13	**Throwing objects to damage**
ST 23	**Attack with vehicle used as weapon (VAAW)**
ST 24	**Attack with parked vehicle borne improvised explosive device (VBIED)**
ST 25	**Attack with encroaching VBIED**
ST 26	**Attack with penetrative ram vehicle**
ST 27	**Attack with suicide terrorist**
ST 32	**Cyber-attack with malware infiltration**
ST 35	**Cyber-attack with direct manipulation**

Figure 4.3.10 – Security threats leading to priority risks for TC 3.1 Road safety

In addition to such threats, **other 11 security threats are of particular concern** for possible evolution in term of likelihood and consequences (**Fig. 4.3.11**).

ST 09	**Theft**
ST 10	**Vandalism**
ST 11	**Graffiti**
ST 12	**Arson**
ST 16	**Malicious or non-compliant personnel, sabotage**
ST 21	**Illegal transit**
ST 22	**Illegal transport**
ST 31	**Ballistic attack, bombing and blasting**
ST 33	**Cyber-attack with subtracting data for ransom**
ST 35	**Cyber-attack to the management system**
ST 36	**Attack with Unmanned Vehicles (UAV or drone; AUV or UUV)**

Figure 4.3.11 – Other security threats of particular concern for TC 3.1 Road safety

Within the framework of a mitigation strategy **for all priority threats the protection, prevention and transfer measures** for road security issue apply as shown in the **Figures 17-1,2,3** of chapter 3.3. Such measures must be detailed in relation to the specific contexts.

Regarding the measures for protection, the subdivision of active and passive measures and procedural-organizational measures also apply. It must be reminded that any measure taken individually doesn't guarantee effectiveness and a good professional must be capable of combining, mixing and dosing them.

4.3.5. Security recommendations

General recommendations (GR) for the topic of security and road safety are in **Figure 4.3.12**:

GR 1	**Raise awareness of the RAs on the security issues.**
GR 2	**Train operation staff on security.**
GR 3	**Provide internal access restrictions to isolate control centre staff from other staff by securing entrances to these locations.**
GR 4	**Implement access restriction procedures.**
GR 5	**Organize formal powers to act in time in case of a security incident.**
GR 6	**Provide standardized procedures for early detection of an incident, for alerting and mitigating or neutralizing threats.**
GR 7	**Establish an internal security department or corporate protection office.**

Figure 4.3.12 General recommendations for TC 3.1 Road safety

A general security recommendation especially for RAs, valid for every company and organization is **to establish an internal security department** to fight against criminal and terrorist activities on the road, in the internal and external context of their institutional activity, establishing all the conditions for a collaboration with police forces and intelligence services[112] .

Further specific recommendations (SR) in relation to the priority threats are described below (**Fig. 4.3.13**):

- SR 1 : On urban areas;
- SR 2 : On controlled and fenced areas;
- SR 3 : On special events and exceptional transport;
- SR 4 : On information systems operators;
- SR 5 : On vehicles and CAV;
- SR 6 : On technological infrastructure, C-ITS and intelligent roads;
- SR 7 : On physical infrastructure;
- SR 8 : On circulation on the road of military, public safety and rescue vehicles or vehicles belonging to authorities;

SR 9 : On devices for protection from hostile or out-of-control vehicles in outdoor areas.

ST 1	**Aggression**	**SR 1, SR 3**
ST 2	**Robbery**	
ST 3	**Mugging**	
ST 4	**Taking hostages**	
ST 5	**Kidnapping**	
ST 13	**Throwing objects to damage**	
ST 23	**Attack with vehicle used as weapon (VAAW)**	

[112] S.Palchetti, R.Mastrangelo, M.Bianchi, "Security and Pandemic: Application of the Concepts of Resilience for Business Continuity, WWSRC Calgary, Canada, 2022.

ST 24	Attack with parked vehicle borne improvised explosive device (VBIED)	SR 1, SR 2, SR 3, SR 7, SR 8, SR 9
ST 25	Attack with encroaching VBIED	
ST 26	Attack with penetrative ram vehicle	
ST 27	Attack with suicide terrorist	
ST 32	Cyber-attack with malware infiltration	SR 4, SR 5, SR 6
ST 35	Cyber-attack with direct manipulation	SR 4, SR 5, SR 6

Figure 4.3.13 Specific recommendations and major security threats for TC 3.1 Road safety

SR 1 – On urban areas

Over the recent years, in **open-air public events**, on the street or in squares, from the Christmas market, to a village festival or a concert, there have been several examples of fatal tragedies caused by drivers running over event attendees or workers. In this case, some security measures are necessary to complement those for road safety. It is necessary to distinguish between stable solutions and temporary ones in relation to the permanent use of the public area or the short-term events. Any security solution has to be reached with the approval of the national public security authority which coordinates the activity of police forces and the departmental and local public security authority.

In case of **permanent measures**, a solution could be to expand and protect the pedestrian areas or urban sensitive sites, with limitation to traffic and interdiction to all or some means of transport, implementation of controlled access and fixed barriers for preventing access to uncontrolled or ill-intentioned vehicles. Retractable bollards can be used as permanent traffic barriers. In addition, surveillance systems with cameras are a tool that many cities have decided to invest in. Not only because they are useful for reconstructing crimes, but also for territorial control. In some countries facial recognition devices are already in use. The collection of traffic data is also useful for security. It allows supervision of vehicles in transit, in term of insurance verification as well as vehicle tax and inspection. It is also useful to pinpoint stolen vehicles and owners which are suspect in investigation. **Traffic surveillance systems** must also have the ability to detect vehicles traveling against traffic flow in order to be recognized as quickly as possible and stopped. Furthermore, vehicles with dangerous loads in transit or parked in sensitive areas must also be identified and monitored.

Concerning **temporary events**, the design of the event venue must be commissioned and a security plan must be drafted in advance in relation to road safety. A preventive and accurate technical analysis of the places and risks related to the event which, by its nature, always present particular characteristics, is essential. Regarding these events, the maximum level of risk is determined by the pop/rock concerts, followed by social political demonstrations, sport events and finally religious ceremonies.

Essential safety measures are the traffic management plans with road closures, parking bans, vehicle access control plan and checkpoints, emergency response plans and training for operators. The access gates must be guarded by qualified personnel for the entire duration of the event in collaboration with police forces. The duration and the number of people attending the event must be defined. These must be all strictly equipped with named tags as well as the insiders and the

protagonists of the event. Other safety measures can be foreseen to differentiate vehicle movements from pedestrian flows, for fire prevention and dedicated access to emergency vehicles, escape routes and clear paths of emergency vehicles, and the management of disabled people. No drinks must be sold or brought from outside in glass containers. Such safety measures can be also useful for security purposes. In addition, security procedures with protected communication between operators and intelligence are suggested and preventive activity in collaboration with police forces to collect information and give a quick response in case of emergency can be needed.

In case of threats in outdoor areas from **hostile vehicle or vehicles used as a weapon (VAAW),** a "last mile" security plan and controlled access areas are suggested. The area involved in the event must be totally closed to traffic also through the positioning of **vehicle security barriers** (VSBs) to mitigate the risks due to hostile or out of control vehicles. These must have the necessary requisites to fulfil their function: effectiveness (verified by full-scale tests at accredited bodies in accordance with international standards), flexibility of use and removal (mobile where necessary), modularity, resistance to manipulation, low maintenance requirements. Furthermore, the need to fit into a specific scenario without transferring a sense of insecurity and danger to the user of those spaces should be taken into account. It should be noted that the interference of these VSB devices with road traffic sometimes generates authorization problems. According some jurisdictions VSB are not yet recognized as security protection and instead are identified as common safety traffic barrier, and therefore traffic obstruction and dangerous obstacles.

The study of **crowd behaviour** (inflow, event, outflow) is also part of the security tasks. Furthermore, events often take place in a public area that is not confined or fenced, with non-exclusive but promiscuous access, being accessible throughout their duration also to residents and regular visitors of the area. With crowds comes the issue of access management to avoid injuries caused by panic and to prevent people from slipping and getting crushed.

Special attention must be paid to the **elderly people**: they are slower to move across crosswalks and less reactive when driving (fewer reflexes, reduced vision, particularly at night). In many countries, their number is growing and they are becoming increasingly vulnerable to aggression. Special rules at local level are often necessary to adapt to an aging population and the risks of insecurity.

The case of **new soft mobility**: in addition to bicycles, electric scooters (and, to a lesser extent, electric unicycles) have appeared on the market. These personal means of transport have given rise to road safety problems, often due to non-compliance with the rules as they can also be easily used to move around or to flee during malicious acts.

Regarding the **urban crossings for hazardous goods transport,** the European agreement on transport of dangerous goods (ADR) defines parking and movement rules, it does not apply in many countries. What's more, during the journey, the carrier may encounter several difficulties (traffic jams, hard-to-find parking, lack of secure facilities). The urban crossings of these type of vehicles must be planned taking into account safety and security risks.

SR 2 – On controlled and fenced areas

In a territory at risk for crime and terrorism, a compound comprising, for example, a hotel or offices is normally equipped with a controlled access security perimeter. Inside this perimeter is

a network of roads with green areas, parking and squares. In this context a possible threat is a vehicle loaded with explosives being detonated outside of the perimeter fence. To avoid damages to buildings, people and vehicles it is advisable that the distance of the building be at least 20 meters from the fence. It cannot be excluded a ballistic attack from the outside could destroy the access portals of the protected area and also cause very serious damage to the internal structures. As measures of protection of such areas it is necessary to establish an adequately controlled security area outside, and equip such area with 24-hour all-weather video surveillance and alarm systems.

SR 3 – On special events or exceptional transport

Some special events or circumstances can include sports competitions (rallies, marathons, bike rides, road racing, stage competition e.g., Tour de France, Paris-Dakar) or vehicles for special transport. Countermeasures can be planned for the protection of the participants to the races and spectators (e.g., distancing requirements for them and some considerations already made for the protection of urban areas may be valid here). An analogous case is that of transit of exceptional transport in terms of safety and security. For these events the definition of specific management models is required.

SR 4 – On information systems operators

It is recommended to **train employees on cyber security risks**. One option is to perform planned cyberattack simulation exercises as well as unexpected ones without warning. Carrying out unexpected audits should be carefully considered and discussed with the Staff Representative Committee and it should be made clear that a “successful” attack does not equate to a breach of trust. For example, one type of attack could be carried out by a simulated attacker who, after having collected the necessary credentials, successfully disguises himself-herself as a system manager, acquiring the ability to perform "trusted" operations that cannot be controlled or filtered by normal IT security systems. A simulated attack may involve the use of e-tolling or the personal data of users.

However, since a cyber-attack is an attack on all systems, it is necessary to protect: computers or servers, isolated or on the network, connected or not to the Internet, as well as peripheral equipment such as printers, communication devices such as smartphones or cellular devices and tablets. It is clear that methods of protecting each and every device can vary drastically in relation to the type and also to the technological level of said device and therefore an analytical list of security recommendations cannot be drawn up.

In case of **malicious or non-compliant personnel**, which can also involve espionage and sabotage, it may be advisable to adopt the following precautions:

- establish personnel responsibilities and liabilities based on procedures with regular updating and testing sessions;
- establish regular turnovers in key workstations;
- where necessary for security reasons, regular checks must be implemented compatibly with the protection of the freedom of personnel in his/her working activity and the protection of his/her personal data.

SR 5 – On vehicles and CAVs

Some basic security recommendations for drivers are that vehicles must be left locked, by removing the ignition key and engaging the steering lock, closing the windows completely, avoid leaving children, pets or any personal belongings inside or in the boot, and fitting anti-theft devices such as an alarm or immobilizer. At present, similar recommendations can be proposed for CAV vehicles, as issues of vehicle custody regarding stolen CAVs are considered to be much more relevant. At the moment there are no further specific security advices or procedures in the scientific literature and this can also be explained by the confidentiality of the topic. The responsibility of car manufacturers to provide a safe and secure vehicle should, in theory, prevent any form of cyber-attack. Therefore, recommendations for any user of automatic or automatized CAVs could be the same as for any internet-connected device. Although already present on the road at their first levels only future developments of CAVs will reveal the level of security that these vehicles will achieve.

SR 6 – On technological infrastructure, C-ITS and intelligent roads

While addressing **security issues of technological infrastructure**, it is necessary to consider the whole approach to information security as a coherent process of qualification, execution and continuous verification as mainly illustrated in ISO 27001. Often the knowledge of the specific risk is still restricted and therefore traditional approaches, i.e., the installation of "physical" countermeasures such as firewalls and end-point protection systems, are not sufficient. These systems can certainly be useful, but they cannot guarantee the most basic level of security as threats are constantly evolving. Creating a technological infrastructure, such as for example the secure and intelligent roads, essentially means guaranteeing the quality of the information that passes through it, which involves the security of:

- sources of information;
- transit of information.
- Recommendations for C-ITS and intelligent roads should concern:
- traffic control;
- mobility management;
- infrastructure control;
- improvement of road security.

Cyber and information security must be kept in mind by the procurement team in the organization who will need to define stringent requirements on the firmware and protocol quality of the devices that are going to be purchased. A guarantee on the after-sales support of the devices should also be required. In the most delicate cases it will be necessary to verify in advance, through internal or *ad hoc* structures, the quality of the device software and then create a list of criticalities that can cause exponential damage to the internal critical infrastructures.

A **risk assessment** can be effectively performed at various stages of the technology infrastructure life cycle. The objective is to assess the information security architecture and security controls in order to ensure that the system meets the necessary requirements. As is well known, the phases of a security risk assessment process are the following:

- define the organization's mission, governance and policies, reputational profiles;
- identify the technological assets/components;

- carry out a risk analysis based on impact and likelihood analysis;
- define an action plan based on priority risks;
- from the evidence of formal monitoring, create a follow-up on corrective actions for risk mitigation;
- additionally, provide resilience requirements to address unforeseen criticalities.

Security assessments should be performed periodically (possibly annually) in order to address and integrate any changes in offered services, new customers, new environment, etc., which could introduce new security risks to deal with. The risk assessment should also include personnel, contractors and the entire supply chain. At the same time, for specific services, the risk assessment process involves the following periodic technical checks:

- Vulnerability Assessment, every 3 months
- Penetration Test, every 6 months

Vulnerability assessment and penetration testing must be performed frequently as they allow an RA to obtain a list of the most identifiable vulnerabilities and to structure corrective actions in a relatively short period of time compatible with the rapid evolution of cyber threats. Once risks have been categorized as medium or high criticality, an organization can move into risk mitigation planning and implementation. The risk mitigation phase may involve developing mitigation plans designed to manage, eliminate, or reduce the risk to an acceptable level. Once implemented, the plan should be continuously monitored to assess its effectiveness, reviewing the course of action if necessary. Currently, insurance companies are able to cover the residual risk that may not be technically possible or convenient to counteract.

Some **other useful recommendations** on this topic can be found in our previous Report of 2019[113] in chapters 4.1.2 “Cyber and cyber-physical threats”, 5.2 “Mitigating cyber and cyber-physic attacks”, 8.3 “Improving security”.

SR 7 – On physical infrastructure

The concept of "physical security" refers to the awareness of the owners or managers of infrastructure of the security threats and risks to their infrastructure. These also include smart roads for the visible physical part: multifunctional stations and other technological installations such as, for example, traffic control centres and stations for energy distribution, production or transformation. Considerations on the protection of physical assets must be made from the early stages of designing a new building/structure. As with any other type of construction, adding new solutions and adaptations at a later stage of construction is - almost always - more expensive than incorporating them from the design stage.

Some general resilience principles for incorporating security measures into the design are:

- improving the ability to quickly react during an adverse event;
- adding redundancy and robustness to the system;
- having backup components to quickly replace damaged ones.

[113] See reference in previous note 14.

The first recommendation for prevention is to make access to the facility more difficult. Other countermeasures are designed to prevent malicious acts once the attacker is inside the premises or has gained access. The asset must possess multiple lines of defence or "levels of security" (as from a "military" perspective) (**Fig. 4.3.11**).

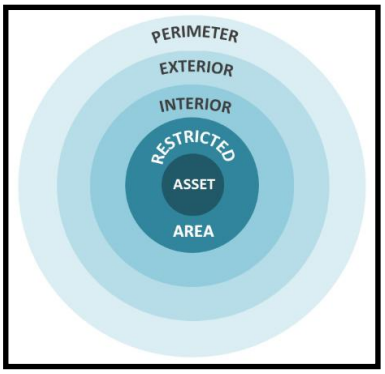


Figure 4.3.11 - Security levels, from PIARC TF C.1, 2019 [114]

A road infrastructure is also made up of a **series of auxiliary technological systems** characterized by the presence of an IT level responsible for their management and operation, which concern:

- systems used for infrastructure management: for example, lighting systems and ventilation systems for tunnels;
- traffic monitoring infrastructure and systems: cameras, cables, sensors on artefacts;
- atmospheric monitoring systems: anemometers, rain detectors, etc.;
- messaging systems: variable message signs;
- access and billing systems: toll systems

Furthermore, the physical infrastructure will be paired with **C-ITS information technologies** which will include, inter alia, the possibility for vehicles traveling on the road to exchange information with the road system, in order to:

- acquire travel information (road - vehicle flow);
- provide information to the road system on routes and on the status of traffic (vehicle - road flow);
- facilitate the exchange of information among vehicles (vehicle - road - vehicle flow).

The presence of such interconnections **increases vulnerable areas** and therefore the exposure and potential vulnerability of the road infrastructure to cyber-attacks. Therefore it is recommended to protect:

- the information flows used to manage traffic lights;
- the flow of information used to monitor tunnels and bridges;
- the flow of information to variable message signs;
- the flow of information from video surveillance and control systems.

[114] Ref. page 8 in AASHTO, Fundamental Capabilities of Effective All-Hazards Infrastructure Protection, Resilience, and Emergency Management for State Departments of Transportation. American Association of State Highway and Transportation Officials, Washington, 2015.

Other useful recommendations on this topic can be found in our previous Report of 2019 [115] in chapters 4.1.1 “Intentional physical threats”, 5.1 “Mitigating a vehicle borne attack”, 8.4 “Security in design”.

SR 8 – On circulation on the road of military, public safety and rescue vehicles or vehicles belonging to authorities

Vehicles supplied to the **Armed Forces and to Public Safety and Rescue Bodies** when circulating on ordinary roads receive special treatment for the purposes of infrastructure safety, traffic and road safety management. Some of these vehicles have constructive and functional characteristics that are out of the norm in terms of size, mass, speed and when in motion they require specific safety, security and confidentiality measures. Particular rules are issued for crossing urban areas and special countermeasures must be adopted in case of manoeuvres or parades by police/military forces such as the preliminary selection of suitable routes, distancing and mobile security barriers.

SR 9 - On devices for protection from hostile or out-of-control vehicles in outdoor areas

In recent years, the number of intentional or even **terrorist events linked to the use of vehicles as weapons (VAAW)** has increased worldwide. Consequently, in the case of temporary public events (concerts, parties, demonstrations, outdoor sporting activities, etc.) authorities and security professionals resort to the use of anti-terrorism structures to mitigate the risks caused by hostile or out-of-control vehicles. These devices, usually barriers capable of neutralizing these dangers, must interfere with road traffic. The **requirements necessary** to fulfill their function are: effectiveness - verified through full-scale tests at accredited bodies in accordance with international regulations -, flexibility of use and removal - mobile where necessary -, modularity, resistance to manipulation, low maintenance requirements. Furthermore, it is essential that these devices fit into a specific urban scenario without provoking a sense of insecurity and danger to the user of those spaces.

The interference of these devices with road traffic generates some problems for the **road regulations of some countries** as they are classified as a traffic obstacle and not as safety barriers (VSB) and therefore subject to specific approvals different from those of road safety barriers (RRS).

The new **ISO/FDIS 22342-2 “Security and resilience — Vehicle security barriers — Part 2: Application of car bomb arrestor standard”** covers guidance on the selection, installation and use of barriers against vehicles. It gives indications on how to create barriers, taking into account the type of vehicle, its mass and its speed, as well as the climatic conditions and soil conditions on which the barrier will be installed. The designer must also take into consideration:

- the threat profile,
- the assets to be protected,
- the site,
- the performance of the barrier,
- the purchasing strategy,

[115] See reference in previous note 14 already mentioned.

- the barrier installation strategy,
- the type of barrier needed, such as mobile barriers, useful for temporary high-risk events.

The standard suggests, among other recommendations, introducing curved paths immediately before accessing the barrier, so as to force the vehicle to significantly reduce its speed.

4.4. TC 4.2 BRIDGES

4.4.1. Introduction

4.4.1.1. General

The purpose of this chapter is to study the relationship between bridges, topic of TC 4.2, and security. For this, it is necessary to frame such issues in general and then focus on the relationship between bridges and road security.

The bridge design is a complex engineering problem and in various ages bridges were built often for more than one purpose. One basic motivation is to overcome, with a driveway or footpath**,** a stretch of water, a water course, a valley, or any natural obstacle, road or railway, and allowing for uninterrupted passage of highway and/or railway traffic. The goal is to facilitate travel, contacts with neighbouring peoples, trade and commerce. Bridges can also be used as defence structures, monuments to commemorate events – achievements - important persons or national heroes, as well as outdoor space for leisure activities, sports or markets and as ecological structures (footbridges for pedestrians or soft transport modes, wildlife crossings). Some bridges are outstanding buildings, famous for their magnificent architecture and technical innovations, structural strength, authentic works of "Land Art"[116]. Aesthetics in bridge engineering is an important topic that concerns to a certain extent also small bridges on roads and highways, whose basic function is to serve transport. If they are located in urban centres, good characteristics of landscape inclusion and day and night visibility are especial essential.

The bridge system

The **conceptual analysis in bridge-designing problems is of the utmost importance** in order to fulfill its fundamental function and performance. Generally, the **design of a bridge**[117] is determined by the span and height of the crossing, the foundations and abutments, the hydraulic and wind resistance requirements if it crosses a river, inland waterway or valley, and the traffic that will cross it. The increase in the size of vessels and in the density of marine traffic, and therefore in the passing clearance required for navigation under bridges, determine the need to build bridges with ever greater clearance and spans. The designer's ideas must integrate the technical concept, surrounding conditions and environmental impacts[118].

[116] *La obra de ingenierìa como obra de arte*, Javier Manterola, Fundacion Arquitectura y Sociedad, Ed. Laetoli, Pamplona, 2010.
[117] Ref. "CD 350 The Design of Highway Structures", Design Manual for Roads and bridges, Highways England, Rev. 0, 2020.
[118] See Chapter 1 "Conceptual Bridge Design" in Bridge Engineering Handbook, edited by Wai-Fah Chen and Lian Duan, Boca Raton: CRC Press, 2000. A relevant reference for highway bridges is provided by the American Association of State Highway and Transportation Officials (AASHTO) in "Standard Specifications for Highway Bridges", Washington, D.C., 18th Ed. 2014.

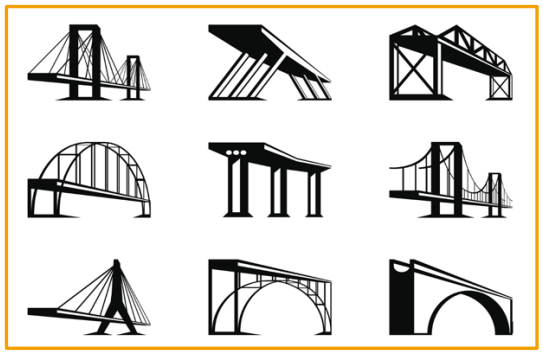


Figure 4.4.1 - Typologies of bridges (iStock)

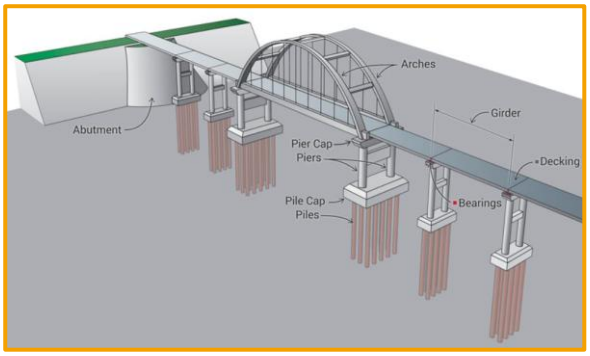


Figure 4.4.2 – Main parts of a bridge (EngineeringClicks)

The design process for bridges needs to include consideration of many factors, such as choice of bridge system, construction methodologies and techniques, materials, dimensions (span, clearance, loads and carrying capacity, longitudinal profile, cross profile, road plan layout), foundations and geological aspects, aesthetics and local landscape, environment (particularly wind strength, thermal gradient, soil type and earthquake risk), any kind of structural and navigational risk if crossing a waterway, and overall cost. As a general rule, the width of the roadway on the bridge has to be at least equal to the width of highway as it connects to the bridge and, especially in long bridges, emergency lanes and parking places in order to allow emergency stops are needed.

Bridges are part of a land transport network and they allow the crossing of stretches of water, valleys or any natural obstacle. A structure made up of multiple bridges connected into one longer structure, only on land: this is called viaduct. In case of large unique structure formed by one or more bridges or viaducts, as for example the crossing of a strait, the more general term of **fixed link**[119] can be used.

Bridges are characterized by **different materials, structure and appearance**[120] and the description of these aspects is relevant from the point of view of safety and security for the purposes of their protection from voluntary attacks. The most currently used materials are reinforced concrete, pre-stressed concrete and steel. There are also bridges built in masonry, stone and wood, although nowadays the latter are mostly for pedestrians only, and the former are usually historic bridges. It is possible to identify six basic long and middle span bridge types: beam, truss, arch, cantilever, cable-stay, suspension, (**Figure 4.4.1**), as well as three types of short-span structures: frame and gantry bridges, slab bridges and reinforced concrete girder bridges. There are also revolving bridges, drawbridges, sliding, floating, removable and horizontally curved bridges such as the military ones.

In summary, the following **parts for a bridge structure** can be identified (**Figure 4.4.2**):

- the **piers** with their parts (bearing, cap, stem), their supports and foundations, which can be normally highly visible elements with many possible forms (most frequently columns or frames either in the median or outside the shoulders);

[119] See Chapter 4 “Planning of Major Fixed Links” in Bridge Engineering Handbook, edited by Wai-Fah Chen and Lian Duan, Boca Raton: CRC Press, 2000.
[120] Ref. “CD 351 The Design and Appearance of Highway Structures”, Design Manual for Roads and bridges, Highways England, Rev. 0, 2020.

- the **abutments** with their foundations and the support devices, are also highly visible parts of the bridge, which include bearings, cantilever walls, cheek walls, and wing walls;
- the **superstructure** of the bridge, including the horizontal spans such as continuous girders, arches, trusses, etc.; all highly visible elements that can have many possible forms;
- the **deck**, including the concrete slab or the steel orthotropic deck, protrusions, railings, parapets, drainage devices, all of which have an influence on road traffic performance and safety as well as on the appearance either when seen in profile or from beneath the bridge.

A **bridge system** includes, other than the bridge in the strict sense (the structure), the technological and organizational parts which are necessary to manage the bridge in ordinary operation and in critical situations such as the case of incident/accident:

- the roads for service and emergency intervention;
- the **bridge supervision centre** (on site or remote) from which the traffic on the bridges is managed including technical installations and the telecommunication network (optical fibre, etc.) with the capability of handling hundreds of points to be controlled and managing sophisticated scenarios;
- the **organization** (staff) and the processes for the management of the bridge itself, including resource mobilization;
- the **traffic management measures** for the road network at the two ends of the bridge, the traffic management centre (if different from the bridge control centre), interactions with other systems;
- the **emergency management**, including coordination with many partners in a timely manner to contain losses and avoid future disruption: public services (Fire Fighters, Police), subcontractors (cleaning and breakdown services).

Materials

Diving more in detail, **bridges have been built in past ages**, and in some areas of the world they still are, in natural fibres, timber (as temporary structures), stone (arched) and masonry. Since the 19th century, **reinforced concrete bridges** have been developed. They consist of precast concrete elements or cast-in-place concrete. The former is fabricated at a production plant and then transported and assembled at the construction site. The latter are constructed “monolithically” and according to a continuous casting program.

Pre-stressed concrete bridges, are built for longer crossings than reinforced concrete bridges, using high-strength concrete, steel and steel cables. Two technologies exist for pre-stressing: pre-tensioning and post-tensioning systems. Section types are void slabs, i-girders and box girders. As an alternative to concrete bridges made up of several prefabricated beams placed side by side and parallel to the longitudinal axis of the bridge, a deck can be built by concrete slices connected by joints perpendicular to the longitudinal axis of the structure. **Steel beam bridges** are widely used in consideration of the problems of durability and therefore of long-term maintenance of pre-stressed reinforced concrete. **Truss steel bridges** have been built for over 150 years with different truss configuration. The deck is supported by a reticular structure made up of steel

elements placed to form triangles and can reach a span of approx. hundred meters. Their resistance to damage, and above all to fire, is lower than that of reinforced concrete bridges. Nowadays only a few single span trusses are used as highway bridges, but many are still used for railroad bridges. Modern highway trusses are usually either continuous or cantilever bridges. In the **mixed or composite bridges**, the deck is composed of steel beams (deck girders or box girders) linked to reinforced concrete slab or pre-stressed slab by metal connectors.

Structural typologies

As said, there are six basic **structural typologies of bridges** (**Figure 4.4.1**): beam, truss, arch, cantilever, cable-stay, suspension and those made of new materials; technology has allowed to overcome ever greater spans with ever more sustainable costs. The isostatic structural scheme of **girder system in reinforced concrete** consisting of slabs and T-beams (deck girders) resting on vertical piers is normally used for spans up to 20-25 meters.

In the pre-stressed reinforced concrete girder or the mixed steel-concrete system, different solutions can be applied to pre-stretched or post-stretched cables. Firstly, the deck can be made of beams (open section), formed by a set of longitudinal beams connected by transverse ribs and an upper slab, which houses the road platform, secondly, a closed (box) or multi-connected section possibly with a protruding upper slab, to house the road platform. In the open section, the effect of the torsional actions due to off-axis loads translates into an increase in bending of the edge ribs (secondary torsion). In the closed section, the torsional effects are absorbed by the whole beam thanks to its primary torsional stiffness.

Both the pre-stressed reinforced concrete solutions make it possible to overcome greater spans, but after some decades decisions must be taken for durability problems due to the corrosion of cable ends, of the concrete and of the yielding of the cable tension. The continuous beam scheme, with more than two supports, allows for the creation of spans greater than those of simply supported beams, as each span exerts a "counterweight" action on the adjacent ones. In this case, spans of 100-150 meters can be reached. The isostatic structural scheme of **girder system, the use of steel truss beams** is an alternative for spans ranging between 30 and 250 meters with remarkable advantages over normal or pre-stressed reinforced concrete for greater durability and minimum maintenance.

Cantilever bridges are generally built with three spans on two piers placed in the valley to be crossed. Two cantilever girders, serving as two arms, are built symmetrically on these, joining in the middle of the span with the other adjacent one. In this way, the structure is in equilibrium and the piers are stressed only axially and therefore the construction can progressively advance from one side to the other of the pier up to the centre line without temporary structures. The two outer spans are made by the two cantilevers extending to the banks or by joining in the central span with similar cantilevered beams anchored to the banks of the gap to be crossed. Cantilever bridges can be built using either steel or concrete. Two main types of deck can be used: the reinforced concrete box girder pre-stressed, the steel truss beam.

For bridges with greater spans, other static schemes than beam must be used: the arch, the cable-stayed bridge and the suspension bridge. In **arch bridges,** the most efficient system is the reticular one in steel. In it, the arch always needs a girder, connected to it by vertical elements (pillars or rods), which house the road platform and contribute to the functioning of the arch-beam

structural system. The deck supported by the arched structure can be placed above or below it and is connected with vertical hangers. It can be made of concrete or steel truss and can reach spans of about 500 m.

In the **cable-stayed bridges,** the static scheme is direct suspension, where the deck is directly supported by a series of almost rectilinear tensile elements that branch off from one intermediate tower also called antenna. The cables that support the deck can be made of stranded steel or pre-stressed concrete. They can be used for spans up to about 1000 m. **Suspension bridges** are the most suitable for very long-span bridges and actually hold the record of the longest span in the world with about 2000 m. The static scheme is indirect suspension, in which the deck is hung with hangers to the main tensile structures made up of linear elements (bars or chains or steel cables) hung between towers and abutments and bent by their own weight according to a funicular configuration of applied loads. Usually, two parallel steel cables are extended over three spans, one main and two laterals (shore spans) and the deck (in steel or reinforced concrete) houses the roadway. At the ends of the lateral spans, the cables are anchored at the foundation blocks capable of transferring horizontal tensions to the ground. The towers transfer to their foundations the vertical load of the supporting cables on which the deck is hung. The considerable wind exposure makes suspension bridges extremely vulnerable to the dynamic flexo-torsional actions induced by the wind (wing effect), while the effects of an earthquake are damped by the very high vibration period of bridges, which are outside the range of seismic interest. Nowadays, suspension bridges crossing navigable stretches of sea must have deck at least 70 meters above sea level due to the size of modern ships.

Bridges fire safety

As highlighted by scientific literature, **the fire risk for bridges is not negligible.** A bridge or fixed link can be severely damaged or even destroyed by vehicles colliding with it, intentionally or accidentally. Bridge fires have increased in recent years causing **severe structural damage and significant economic losses** in the order of tens millions of dollars worldwide [121] [122] and structural collapses of bridges have occurred with a frequency comparable to other extreme events such as earthquakes and winds [123].

---

[121] Garlock, M., Paya-Zaforteza, I., Kodur, V., and Gu, L., "Fire hazard in bridges and repair strategies, Engineering structures", 35, pp. 89-98, 2012; Hu, J., Carvel, R. and Usmani, A., "Bridge fires in the 21st century: A literature review", Fire safety journal, 126, 2012; Lee, G.C, Mohan, S., Huang, C. and Fard, B.N., "A study of US bridges failures (1980 – 2012), 2013, Buffalo, NY.

[122] Vehicles carrying explosives or flammable cargo can also be extremely dangerous to the facility in the event of an accident, as demonstrated in Mexico in January 2018 and Italy in August of the same year. In both cases the bridges were closed for a few months (in the second case in one direction only), due to the serious damage caused to the deck by the fire. January 12, 2018, on the Durango-Mazatlán highway (Mexico) near the El Carrizo bridge, a truck with two diesel-type tube containers suffered the detachment of the second trailer inside the Carrizo II tunnel and stopped, burning on the bridge. The fire, which lasted for about 4 hours before being suffocated, caused serious damage due to exposure to high temperatures: asphalt, concrete slabs, metal structures and damaged and disrupted operational, communication, electrical and other systems. optical fiber of the structure, as well as those that pass over it. Several punctures formed in the asphalt and concrete slabs, as well as leaving the reinforcing steel exposed. It resulted in the complete closure to vehicular traffic of the four lanes in both directions of traffic. On 6 August 2018, on a motorway viaduct, near Bologna (Italy), a tanker carrying LPG collided violently with a truck stopped behind a column of vehicles. A fire started, then the LPG tank exploded from overheating. The tremendous explosion brought down the motorway bridge that runs parallel to the ring road in a suburban but very populous part of the city. The tanker's explosion set fire to and blew up some cars parked in two car showrooms under the bridge. One carriageway on the highway was closed for about a year.

[123] At the San Francisco-Oakland Bay Bridge in California, a tanker truck carrying over 32 cubic feet of gasoline overturned and caught fire while traveling at high speed on April 29, 2007. The fire caused two spans of the I-580 freeway to collapse. These spans consisted of six girders welded and supporting a reinforced concrete slab roadway. The collapse occurred about 22 minutes after the start of the fire. The federal government spent more than $9 million to repair the damage, including $4.3 million for demolition and removal of the damaged section of highway and approximately $2 million for traffic control. Other incidents involving cable-stayed bridges and

The most common causes for fires, along the infrastructural network and particularly on bridges, are heavy vehicle or tankers collisions with combustible materials and the ignition of leaked flammable liquid. Even arson can act as a trigger. It affects mainly the deck, where the spread of the liquid and of fire is highly unpredictable so that the location of the fire cannot be determined a priori. Also, the structure can be affected if, as an example, it is hit by a gas explosion from a leaking pipeline attached to the bridge structure. [124]

A fire depends on the amount of fuel spilled and in case of hydrocarbons, those can have a high and rapid heat release and, being in the open air, benefit of an unlimited amount of oxygen. Therefore, the intensity of the fire can be exceptionally high. Also, the characteristics of a bridge can influence the growth, spread and decay of a fire, reducing or amplifying the transmissibility of the heat flow towards the supporting structure.

Despite the serious consequences, and unlike most structures and infrastructure as buildings and tunnels [125], there is **no specific regulatory obligation** that requires the designer to test a bridge according to fire resistance criteria and fires are often neglected in the design of bridges. As a consequence, in a bridge there are generally no fire extinguishing systems. This aspect can lead to a high vulnerability to fires bridges and in the event of a fire, a significant impact on the functionality of the infrastructural network must therefore be expected.

Bridges, on the other hand, can benefit from the positive effect of wind that cools the hot gas that spread during the fire, but it is often essential to check the extent of the deformations of the structure. Extreme deformations may not only cause the loss of functionality of the bridge, with severe repercussions for vehicular traffic, but also damage systems and underground services, both within and outside cities, often incorporated into the structure, with even more severe consequences.

In case of fire, the **most critical structural parts for bridges** are the deck beams due to local buckling and shear failure [126]. Fire alters the composition of materials as well as the geometry of the structure and consequently the behaviour of a bridge structure. The structure and the fire are strictly interdependent as the former influences of the development of the fire and therefore the development of combustion.

In terms of consequences, the victims of a fire on a bridge normally succumb at the beginning of the event, following the road accident and the fire with explosions resulting from it. This usually

---

suspension bridges have been investigated in the literature. For example, on 23 July 2013 a truck loaded with paper and electronic equipment collided with a vehicle and caught fire while crossing the New Little Belt suspension bridge in Denmark. The consequences were not serious and there was no permanent damage to the main cables and hangers. The bridge was checked, repaired and reopened to traffic. Since it was realized that the consequences could have been much more serious in the case of larger trucks or a tanker with a flammable liquid spill, it was decided to increase the passive protection layer of the steel cables in thickness and height up to 10 meters above the deck.

[124] On June 11, 2023 at 6:15 a.m., the driver of a tanker truck filled with eighty-five hundreds of gallons, lost control of his vehicle after taking an exit ramp below Interstate 95 in Philadelphia (USA) and struck a wall. The truck tipped and exploded, setting off a fire that melted the support structure of the road above, causing it to collapse. Pennsylvania Governor issued a proclamation of disaster emergency and acknowledged at a press briefing that that section of I-95, which carries an average of 160,000 vehicles per day, would be closed for some number of months with ripple effects along I-95, a 1,927-mile roadway that runs from Florida to Maine.

[125] In these cases, the fire takes place indoors and the buildings and tunnels can be equipped with active (sprinklers) and passive (fire-fighting materials) fire protection. Evacuation measures are also planned. In the case of buildings, the fire is initially localized due to the combustion of materials inside (mainly wood, paper and plastic materials) and has the possibility of expanding in relation to thermal inertia and quantity of materials and ventilation. On the contrary, on a bridge or a tunnel the fire spreads in relation to the spread of the fuel spill.

[126] The most critical structural parts for or buildings are the beams and pillars due to collapse under fire. Another substantial difference is that for buildings, the goal is to safeguard the lives inside, as victims can be numerous.

results in damage to the structures and, in extreme cases, the loss of the bridge or part of it in addition to the temporary or prolonged interruption of road traffic.

In conclusion, bridge structures are built for different purposes. To meet them, a bridge may have a large number of different structural types or combination of them: beams, arches, towers, cable-stayed, suspensions, constantly evolving in relation to the development of new materials especially in the steel manufacturing field. The structure must stand out and impart a feeling of stability, safety and security. A basic principle is that the form of the structure must correspond to the functions and, primarily, the technical requirements in term of load-carrying capacity must be fulfilled as well as strong guarantees for safety of drivers and people exposed to different environmental conditions and traffic situations. High-level safety measures can represent also basic protection for security.

Both **safety and security are factors affecting the design of a bridge** also in consideration of the need to contain the spread of a fire in the open air. A bridge is an extraordinary structure in which visual harmony between technical complexity and aesthetics must be obtained, placing itself in a landscape that will be modified by the structural itself both in a physical appearance and in its functioning. At the same time, the bridge is a structure that can become fragile due to the transit of vehicles carrying dangerous, flammable and explosive goods in the event of a fire resulting from an incident or accident or arson. Fires can severely damage bridge structures and can lead them to structural collapse, since they are not generally designed with fire resistance criteria. It can be noted that **vandalism** is a lower thread but its frequency can be a real issue for the managers and It can be unacceptable that **s**ome bridges are covered in **graffit**i.

4.4.1.2. Bridges and security

For their external exposure**, any bridge constitutes a critical element** within an infrastructure of land transportation[127] since it can be considered an objective given its visual significance and structural impressiveness, its transport and military functions, and also its symbolic value, especially in the case of commemoration of an event or an illustrious individual. A bridge produces strong emotions and can be considered a work of art with many meanings, including that of binding a person to a place. At the same time, a bridge has a function for the territory, as it provides a service to the population living there and beyond, to the region and to the country. All this gives the bridge a value as a public work that other works, especially road works, do not have. Therefore, a bridge can be destroyed by terrorists or criminals to send a clear message with many meanings and as well as cause physical damages.

In reality, damages caused by criminal or terrorist acts to a bridge are extreme events with a very low likelihood of occurrence but with devastating consequences [128]. Reinforced concrete and steel structures are in fact built to support considerable loads and environmental stresses. Therefore, explosions must be extremely strong, much more than that required to demolish a normal building, to have some effect. And, such quantities of explosives are difficult to get onto a bridge without arousing suspicion. Even if we exclude the possibility of knocking down a bridge

[127] The Member States of the EU are engaged in the process of applying the European Council Directive 2008/114/EC, containing the procedures for the identification and designation of European Critical Infrastructure, and a common approach to assessing the need to improve their protection in order to contribute to the protection of relevant persons and assets.
[128] The fact that no voluntary acts of this kind have ever occurred does not justify a lack of attention to the problem and in any case the damages that would be caused by such an act are comparable to those deriving from an accident or an earthquake.

and destroying it completely (unless it is due to wars), the partial loss of functionality of a bridge still constitutes a great damage. In this sense vandalism can also be an issue of concern. Therefore, a bridge lends itself to being a terrorist target rather than a war target. Its decommissioning creates damages to the territorial economy because bridges often provide vital links in a local transportation network. This situation mainly affects civilians, generating fear and lack of security in the inhabitants.

The **conceptual analysis in bridge-designing** must take into account that in the event of an accident (up to a certain defined level) the structure must maintain its integrity, the risks of traffic interruption should be minimized and repairs must be carried out in an acceptable timely manner. Hence structural resistance to accidental events, redundancy and ductility are overall important criteria for bridges.

Bridge's design weaknesses can be taken into account by those who want to carry out an attack. Therefore, for security purposes, it is necessary to conceive structures for bridges capable of withstanding threats related to its physical parts such as the structure, vehicles, traffic typologies (including dangerous goods transportation), materials, dimensions and also the operational personnel, as well as users of the bridge - who may also become perpetrators of damages themselves - , other parts such as the IT, control centres as well as the procedural/organizational aspects. As a designer and project manager it is therefore necessary to be open-minded, taking into account the degradation over time of the architectural characteristics of a structure, which, over time, worsens vulnerability elements eventually already present in the design and construction phases.

If neither **prevention nor protection** succeed in hindering an attack[129], it will be necessary to envisage a **business continuity plan at road network level** which precisely characterizes the resilient approach to the road network, which must mitigate the repercussions of a successful attack. **Since the economic impact of closing a bridge** increases over time, and therefore, given the existing risks, it is a good rule to plan alternative routes in advance.

Structural vulnerability

The vulnerability of a bridge to a malicious attack varies over time from the construction of the work, up to the natural degradation of performance over the useful life of the structure. This last point can be remedied through good maintenance planning, or structural interventions that manage to restore the building. **In the construction phase**, the risk of a successful attack on a bridge is high at the beginning (but the economic damage is lower) and is minimal when the structure is completed as its structural performance is at its peak (although a possible attack can provoke greater economic damage).

The **support piles of bridges** are critical to the structural integrity of the bridge and these must be designed with specific characteristics of strong structural robustness. Therefore, normally, these can only be damaged as the result of a significant explosion taking place in specific locations in relation to the piles [130] . The fact that there are **hidden areas** around the bridges, with often freely

[129] This can also be the result of a deliberate choice by the designer in agreement with the Road Administration.
[130] In some countries, it is considered at the design stage that for strategic land protection purposes a bridge could be demolished in the event of an attack, and specific provisions are incorporated to successfully perform a controlled explosion to achieve effective destruction.

accessible piers and abutments, means that they can be used as a venue for various illegal behaviour. In order to limit this and to ensure the safety of the public, areas which should not be accessible to unauthorized personnel must be usually fenced or otherwise protected and, in some cases, monitored. In particular instances, the piers themselves can be protected with bumper structures. In the event of a simple warning of the threat of explosives placed under the bridges, an interruption in traffic to verify the threat must still take place.

In the event of an **explosion or fire on the deck** of a bridge, a box-beam reinforced concrete bridge is more vulnerable than a bridge with a deck consisting of juxtaposed beams, as in the former the structure is thinner and stability is ensured by the resistance to deformation of the closed structure. In this case, the damage to one or more beams can be repaired more easily by replacing the damaged beams, while in the box-beam bridge the damage makes the structure brittle in a way that is difficult to remedy.

Expansion joints malfunctioning introduce a structural irregularity and vulnerability that can have catastrophic consequences. Such joints are commonly used in bridges to alleviate stresses associated with volume changes that occur as a bridge age and as the temperature changes. These joints can be placed within a span (in-span hinges), or at the supports, as is the case for supported beam bridges.

The spans made up of a series of beams placed side by side and supported by bearings can be vulnerable in the event of an explosion due to the beams getting out of their support guides. The interruption of road traffic however would be for a short period of time given the reduced likelihood of the explosion damaging both carriageways.

The **superstructures** are designed to elastically support the service gravitational loads. Consequently, superstructures tend to be strong enough to remain essentially elastic when subject to strong external impulse, but they can suffer greatly from the high temperatures of a fire which can be caused by an explosion of a tanker. However, damage to the superstructure is unlikely to be the primary cause of a span collapse. Conversely, damage can be concentrated on bearings and substructures. The superstructure may rest on elastomeric bearings, pivot bearings, or it may be integrated with the substructure. If the bearings and substructures are damaged and, in some cases, fail, a wide range of superstructure damage and failures can occur, although these failures are usually secondary.

A **metal bridge or mixed structure bridge**, composed of beams or box girders, can be, in principle, damaged by a bombings or demolition charges with greater ease than a reinforced or prestressed concrete bridge due to the reduced thickness of the structures. A truss bridge structure allows for a certain degree of resistance of the structure even in the presence of significant damage. As for cable bridges, they have a specific vulnerability in external cable anchors. This vulnerability can also be found in prestressed bridges with exposed cables in box girders.

The vulnerability of a bridge in terms of security depends not only on its dimensions or its span, but also on its location (urban or non-urban area, commercial area, tourist area, tunnel access, intermodal areas, strategic access, etc.), its traffic (pedestrians, cyclists, lorries, etc.), its use (frequent crossings by large numbers of people, transport of dangerous or high-value goods, etc.), its security/safety equipment (cameras, traffic lights, easy and discreet access, etc.) and the proximity or otherwise of local emergency services (nearby police, emergency services,

etc.). safety equipment (cameras, traffic lights, easy and discreet access, etc.) and the proximity of local emergency services (nearby police, emergency services, etc.). So it's not just long-span structures that are vulnerable to malicious acts.

Risk studies and risk management

Risk studies and risk management have gained a widespread application within planning, design, and construction of fixed links. Risks are inherent in major transportation links, and therefore it is important for the owner and society that risks are identified and included in the project together with the technical and economic aspects. Risks are often studied separately according to the consequences of concern:

Economic risks (rate of interest, inflation, exceeding of budget, changing traffic patterns);

Operational risks (accidents, incidents, loss of lives, impact to environment, disruption of the traffic, loss of assets, loss of income) and they may have important implications on the selection of the structural concept.

Construction risks (accidents, failure to meet time schedules or quality standards, unexpected ground conditions).

From the security standpoint a bridge is generally deemed to be a critical infrastructure, in particular if there are no alternatives paths and therefore a likely target for terrorists and criminals. A security risk management process is therefore necessary for the bridge to be placed in a road network in order to give specific protection measures which must be higher than those taken on roads or high/motorways. For the purpose of this chapter only the risks related to security will be considered.

A **risk management process for bridges** should follow the general flow based on ISO standard 31000 previously shown in **Figure 5** in chapter 2.4 with the risk analysis consisting of a systematic identification of threats and an assessment of the two components of the risk: the likelihood and the consequences. A prioritization of risks can be roughly performed using a qualitative assessment methodology (as in the development of this chapter) but an investigation into specific risks may be undertaken in order to establish a basis for a more-detailed work.

The risk management strategy for a bridge can be initially developed in each phase of the project: **conceptual study, preliminary design, final design, and operation**. It is highly important that in the conceptual study the highest risks and risks with potential impact on geometry (safety, rescue operations, span width) are especially accounted for. In the tender design phase, the main risks should be examined in more detail, and in the detailed design phase it is necessary to understand whether some components should be designed to mitigate specific security risks. At each stage of the risk management process, the outcome should be documented and stored in the archives. Consequent operational procedures should include a regular security review to ensure the ongoing safety and security of the bridge with operating and maintenance procedures supporting measures introduced to mitigate security risks.

In the scientific literature, three risk assessment methods are generally considered for bridges: fixed limits, cost efficiency, and ALARP (as low as reasonably possible). **Fixed limits** involve determining a risk acceptance threshold. In **cost efficiency**, no upper limit is defined and all risk reduction measures are present. The **ALARP method** applies a cost-benefit consideration in which

it is stated that the risk must be reduced as long as the cost of the reduction measures is proportionate to the risk-reducing effect. Usually, an upper limit beyond which the risk is unacceptable is introduced.[131] It is clear that in the event of unforeseen or non-statistically predictable events such as terrorist or criminal attacks, the possibility of an advanced risk assessment is uncertain. In this case, it is important to consider the criticality of the geo-political context.

4.4.1.3. Specific requirements for TC 4.2 from PIARC ToR

The TC 4.2 is composed by five sub-themes and security recommendations don't concern any of them.

4.4.1.4. Methodology and international standards

Many general ISO standards for reliability of structures can be applied to bridges:

- ISO 2394:2015 General principles on reliability for structures;
- ISO/TR 4553:2022 Deformations and displacements of buildings and building elements at serviceability limit states;
- ISO 10137:2007 Bases for design of structures - Serviceability of buildings and walkways against vibrations;
- ISO 12491:1997 Statistical methods for quality control of building materials and components
- ISO 13822:2010 Bases for design of structures — Assessment of existing structures
- ISO 13823:2008 General principles on the design of structures for durability
- ISO 13824:2020 Bases for design of structures — General principles on risk assessment of systems involving structures
- ISO 22111:2019 Bases for design of structures — General requirements
- ISO 23618:2022 Bases for design of structures — General principles on seismically isolated structures

In particular, ISO 2394:2015 General principles on reliability for structures at chapter 7 "Risk-informed decision making", deal with risk quantification, decision optimization and risk acceptance for consequences of both a direct and indirect nature with emphasis on robustness, at three levels: risk informed, reliability based, semi-probabilistic.

- ISO 22111:2007 specifies the general requirements for the structural design of buildings, industrial and civil engineering structures using reliability-based concepts. It is applicable to the design of complete structures, the structural elements making up the structure and the foundations.
- Many ISO standards apply to bridge design and construction, not dealing with security:

[131] In the Øresund Link, the 16-km fixed link for combined railway and highway traffic between Denmark and Sweden consists of three major projects: an immersed tunnel, a suspended bridge and an artificial island connecting the tunnel and the bridge, risk acceptance criteria were developed such that the individual user risk for crossing the link would be equal to the average risk on a highway and railway on land of similar length and traffic intensity. The ALARP-principle was applied to reduce consequences from risks within a cost–benefit approach. Risk-reducing measures were studied to reduce the frequency and consequences of hazardous events, such as fire, explosion, toxic releases, vessel collision and grounding, flooding, aircraft crash, and train derailment.

- ISO 6446:1994 Rubber products — Bridge bearings — Specification for rubber materials;
- ISO/PRF 6819 Steel wire rod for bridge cable wire;
- ISO 14963:2003 Mechanical vibration and shock — Guidelines for dynamic tests and investigations on bridges and viaducts;
- ISO 18649:2004 Mechanical vibration — Evaluation of measurement results from dynamic tests and investigations on bridges;
- ISO 19203:2018 Hot-dip galvanized and zinc-aluminum coated high tensile steel wire for bridge cables — Specifications;
- ISO 19427:2019 Steel wire ropes — pre-fabricated parallel wire strands for suspension bridge main cable — Specifications;
- ISO 21725-1:2021 Simplified design of pre-stressed concrete bridges — Part 1: I-girder bridges;
- ISO 21725-2:2021 Simplified design of pre-stressed concrete bridges — Part 2: Box-girder bridges;
- ISO 22762-2:2018 Elastomeric seismic-protection isolators — Part 2: Applications for bridges — Specifications.

In the general scheme of the ISO families, 14000 standard is important for bridges as well as the 27000, 31000, 22300, 45000, as well as ADR and Envision. In particular, the 22300 family is important for security and resilience aspects. On this subject, the considerations made for tunnels apply to bridges. The ISO standard for risk management ISO 31000 with related concepts and fundamental principles of risk management as well as risk identification also applies to bridges.

	ISO family & relevant Standards	Impact on security of bridges	Topics	Notes
1	9000	3	Specific requirements for quality management systems including security	general application
2	14000	4	Specific requirements for environmental management including security	general application, importance of the environment for bridges
3	27000	3	Specific requirements for information security management systems	general application, relevant for bridges
4	28000	1	Specification for security management systems for the supply chain	general application
5	31000	3	Guidelines for managing risk	important application
6	20858	2	Framework to assist marine port facilities in security assessment and security plan	no application
7	22300	5	Security and resilience	relevant application
8	39000	1	Road traffic safety management systems	general application
9	45000	3	Guidance for occupational health and safety management systems	is applied for bridge operators
10	IWA-14	1	Specification for vehicle security barriers	is applied for bridge operations
11	CEN/TR 16705	1	Classification for perimeter protection systems	application for the protection of bridges and control centres, guidelines to devices for remote control
12	ADR	3	Specification for the international carriage of dangerous goods by road	relevant application for incident prevention
13	ENVISION	3	Guidelines to implement more sustanaible infrastructure, resilient and equitable projects	design of bridge system, new technology

Fig. 4.4.3 - Impacts of ISO family & relevant standards on security for TC 4.2

4.4.2. External and internal contexts

The impact of security – with regards to criminality, terrorism, vandalism and cyberattacks – in the **external and internal contexts** of a bridge must be considered in order to prioritize risks and ultimately propose recommendations.

The macro-areas of vulnerabilities, the elements of vulnerability and the threatened assets, related to the security effects to road bridges in their external and internal contexts are shown **in the first three columns MAV, EV, TA of Figures 4.4.4-1 and 4.4.4.2**.

4.4.3. Risk assessment for TC 4.2 Bridges

For risk assessment, a correlated reading between the following **figures 4.4.4-1, 4.4.4-2, 4.4.5, 4.4.6., 4.4.7, 4.4.8** is necessary.

4.4.3.1. Risk identification

As described in the previous paragraphs, bridges in all their components present **security problems.** Threats can concern personnel, users of the bridge – who may also become perpetrators of damages -, the physical part i.e., structure, infrastructure, complementary elements and vehicles, the IT and the procedural/ organizational parts. The bridge system as a whole is a complex infrastructure due to possible domino effects with cascading consequences.

In **Fig. 4.4.5**., **the general threats for the bridges are shown in column GT**: the security threats for bridges and bridge management in general include physical and cyber malicious acts and the ones concerning the application of new technologies with more sophisticated attacks including the instances of bridges being used as geopolitical weapon.

In column T of Figures 4.4.4-1 and 4.4.4-2, the possible security threats are considered.

		MAV	EV	TA	ST	L	C	R	
		MACRO-AREAS OF VULNERABILITY	ELEMENTS OF VULNERABILITY	THREATENED ASSET	SECURITY THREATS	LIKELI HOOD	CONSE QUENCES	RISKS	Notes
EXTERNAL CONTEXT	1	GEOGRAPHICAL	Locations exposed to any external action such as natural disasters (floods, earthquakes, tsunamis, hurricanes, volcanoes, etc.), pandemic and others for their security effects	Structures of the bridge, cable anchors, users, staff, vehicles, parking, accesses, toll barriers	38	4	4	16	Strong natural events and environmental degradation can be threats multipliers for a bridge located in such an area, e.g., a vehicle transporting dangerous goods crossing during a storm
	2.1	INFRASTRUCTURAL	Proximity to sites of importance for security purposes (chemical centres, sites at risk of major accidents, fair and exhibition sites, etc.)	Idem, due to explosion or fire near	30, 31	4	4	16	Possible catastrophic effects
	2.2		Proximity of hubs or networks of (inter)national importance (roads, motorways, railways, airports, ports)	Idem, due to incident or accident	12, 40	4	4	16	Possible catastrophic effects and high likelihood
	2.3		Proximity to police forces sites, military settlements, fire brigades	Idem, due to protests	12, 13, 20, 31, 39	3	4	12	Temporary blockade of the bridge, moderate attacks
	3.1	SOCIO-ECONOMIC	Areas with high unemployment rate and a high state of material and social need	Idem, due to protests, strikes and crimes against people and things	1-3, 9-13, 16, 19-22, 23-36, 39	3	3	9	Temporary blockade of the bridge, heavy attacks
	3.2		Possibility of media attacks, by competitors or customers	Reputation	19	1	2	2	Not relevant
	4	POLITICAL	Unstable political context	Crimes against people and things	12, 16, 19, 23-27, 31, 36, 39, 41	4	4	16	High risk in case of militarily strategic location with the involvement of civilians
	5.1	TERRITORIAL	Presence of micro-crime (theft, robbery, murder, fire, extortion, money laundering, usury)	Idem	1-3, 9-13, 15, 16, 19-36, 39	3	2	6	Moderate likelihood, not relevant consequences
	5.2		Presence of organized crime, terrorism	Idem	12, 16, 23-27, 30-31, 36, 39	4	4	16	Extreme risk, possible symbolic target
	5.3		Activism of anarcho-insurrectionist movements, condition of confessional or racial segregation	Idem	1-3, 9-13, 15, 16, 19-36, 39	2	3	6	Low likelihood and moderate effect, difficult target

Fig. 4.4.4-1 - External context, risk identification and analysis for TC 4.2 Bridges

		MAV	EV	TA	ST	L	C	R	
		MACRO-AREAS OF VULNERABILITY	ELEMENTS OF VULNERABILITY	THREATENED ASSET	SECURITY THREATS	LIKELI HOOD	CONSE QUENCES	RISKS	Notes
INTERNAL CONTEXT	1	EXTERNAL AREAS	Roads, parking spaces, vehicles of visitors and suppliers, portals for message panels	Roads, parking spaces, service vehicles and of visitors and suppliers, portals, variable message panels, people	1-3, 9-13, 20-22, 23-31, 36, 39-41	3	3	9	Moderate consequences in case of penetrative vehicle and ballistic attack
	2	EXTERNAL PERIMETER	Accesses, protections	Security personnel, employers, doors and gates, control systems	9-13, 20, 23-31, 36, 38-41	3	3	9	Moderate consequences
	3.1	INTERNAL AREAS	Structures	Deck, hangers, escape facilities	12, 23-24, 31, 36	4	5	20	Arson or ballistic attack to the structures of the bridge can be catastrophic
	3.2		Buildings	People, offices, buildings	12-13, 36, 39	3	3	9	Moderate consequences if inside the bridge
	3.3		Roads	Road's platform, emergency lanes, parking places, people	12-13, 23-27, 31, 36	4	4	16	Closure or limitation of exercise due to fire/explosion/ bombing on the deck
	3.4		Vehicles	Company, business, employees, visitors, suppliers	12-13, 23-24, 31, 36	1	2	2	Not a target
	4.1	OFFICES	Staff and managers	Normally, there are no offices with employees inside a bridge					
	4.2		Visitors and suppliers	Idem					
	4.3		Computer systems and office equipment	Idem					
	4.4		Information/ communication	Idem					
	5.1	PRODUCTION/ OPERATION FACILITIES	Work areas	Service stations, toll stations control room, people	12, 16, 18, 31, 36, 39	4	4	16	Toll station and control room are physical and digital targets
	5.2		Installations	Equipment, devices (electrical power supply and distribution, lighting, signalling, over-weight vehicle detection, etc.)	16, 31-36, 39	3	3	9	Technical facilities can be a target but with not heavy consequences
	5.3		Emergency	Equipment, devices (fire-fighting systems, smoke and hot gases control, air quality)	16, 32-36. 39	2	3	6	idem
	5.4		Consumables	No dangerous materials					
	6	CONTROL/DATA CENTRE	Server, SCADA systems	Platforms and data bases to ensure road and bridge safety and staff management	16, 18, 31-36, 39	2	3	6	This technical facilities can be a target but low consequences
	7.1	STORAGE	Raw materials	Normally, there are no raw materials in a bridge					
	7.2		Finished products	Idem					
	8.1	LABORATORIES	Staff, specialists, experts	Normally, there are no laboratories in a bridge					
	8.2		Offices	Idem					
	8.3		Computers and digital devices	Idem					

Fig. 4.4.4-2 - Internal context, risk identification and analysis for TC 4.2 Bridges

		GT
	Security threats	Bridges
	Crimes against people	
T 01	Aggression	X
T 02	Robbery	X
T 03	Mugging	X
T 04	Taking hostages	0
T 05	Kidnapping	0
T 06	Mobbing	0
T 07	Stalking	0
T 08	Corruption	0
	Crimes against things	
T 09	Theft	X
T10	Vandalism	X
T11	Graffiti	X
T12	Arson	X
T13	Throwing objects to damage	X
T14	Violation of private property, unauthorized entry	0
T15	Piracy	0
	Crimes against people and things	
T16	Malicious or non-compliant personnel	X
T17	Communications	0
T18	Disclosure of information, espionage	X
T19	Misinformation	X
T20	Civil protests and strikes	X
T21	Illegal transit	X
T22	Illegal transport	X
	Crimes referable to manifestations of terrorism and or organized crime aimed at people and thing	
T23	Attack with vehicle used as weapon (WAAW)	X
T24	Attack with parked vehicle borne improvised explosive device (VBIED)	X
T25	Attack with encroaching VBIED	X
T26	Attack with penetrative ram vehicle	X
T27	Attack with suicide terrorist	X
T28	Attack with terrorist and/or threatening phone calls	X
T29	Attack with envelope or letter bomb	X
T30	CBRNE attack	X
T31	Ballistic attack, bombing and blasting	X
T32	Cyber attack with malware infiltration	X
T33	Cyber attack with subtracting data for ransom	X
T34	Cyber attack with direct manipulation	X
T35	Cyber attack to the management system	X
T36	Attack with Unmanned Vehicles (UAV or drone; AUV or UUV)	X
	Unattended and unforeseeable event causing terroristic and criminal attacks or disasters	
T37	Pandemic, epidemic, epidemic outbreak	0
T38	Natural disasters and climate change	X
T39	Blackout	X
T40	Disaster propagation from neighboring infrastructures	X
T41	Geopolitical crises, armed clashes or combats, revolutions, uprisings	X

GT : general threats for security of bridges

X is a threat
0 is not a threat

v-13

Fig. 4.4.5 Security threats for T.C. 4.2 Bridges

4.4.3.2. Risk analysis

In columns L and C of the Figures 4.4.4-1 and 4.4.4-2, the assessment of the likelihood of the occurrence of threats and the evaluation of consequences is made. A rating of likelihood in five categories is shown in **Fig. 4.4.6** and a rating of the potential consequences in five categories is shown in **Fig. 4.4.7**. Consequences is here defined in terms of damage cost. It can be considered or added to the cost of the number of deaths (e.g.: about 1.500.000 € per person), serious injures (150 000 € per person) and minor injuries (5 000 € per person).[132]

1.	Rare	>20 years	< 10% of cases
2.	Unlikely	every 10-20 years	< 33%
3.	Moderate	every 4-5 years	< 45 - 50%
4.	Likely	once a year	> 60%
5.	Almost certain	once a month	> 90%

Fig. 4.4.6 - Severity of likelihood for TC 4.2 Bridges

1.	Insignificant	damage 1.000 € - 5.000 €
2.	Minor	damage 5.000 € - 100.000 €
3.	Moderate	damage 100.000 € - 1.000.000 €
4.	Major	damage above € 1.000.000
5.	Catastrophic	extremely high

Fig. 4.4.7 - Severity of consequences for TC 4.2 Bridges

4.4.3.3. Risk evaluation

In column R of Figures 4.4.4-1 and 4.4.4-2, the criticality of the risk is evaluated assigning the score derived from the product L x C = R (also called magnitude following ISO 31000). In it, only the most harmful and dangerous adverse events (extreme or red ones or magnitude 15-25 as shown in Fig. 16 of chapter 3.2.4 of this Report) are considered.

The results obtained are summarized in **Fig. 4.4.8** in order to prioritize risks. It can be noted that in the case of bridges **there are 6 major macro-areas of risks in the external and internal context and 1 priority threat**.

[132] It should be noted here that the security's events (like terrorist attack for instance) are not accidental but intentional. Therefore, they are not random events as the safety's ones (like fire in tunnels). So, in the security field, likelihood is not determined based on a statistic approach but is assessed on a reasonable prediction of terrorist intentions and capabilities.

		MACRO-AREAS AND PRIORITY RISKS													
		EXTERNAL CONTEXT					INTERNAL CONTEXT								
		1	2	3	4	5	1	2	3	4	5	6	7	8	
		GEO	INFR	SOC-EC	POL	TERR	EXT A	EXT P	INT A	OFF	P/O	DAT C	STO	LAB	PRIOR
		16	16		16	16			20		16				
	Crimes against people														
T 01	Aggression														
T 02	Robbery														
T 03	Mugging														
T 04	Taking hostages														
T 05	Kidnapping														
T 06	Mobbing														
T 07	Stalking														
T 08	Corruption														
	Crimes against things														
T 09	Theft														
T10	Vandalism														
T11	Graffiti														
T12	Arson		X		X	X			X		X				5
T13	Throwing objects to damage								X						1
T14	Violation of private property, unauthorized entry														
T15	Piracy														
	Crimes against people and things														
T16	Malicious or non-compliant personnel				X	X					X				3
T17	Communications														
T18	Disclosure of information, espionage										X				1
T19	Misinformation				X	X									2
T20	Civil protests and strikes					X									1
T21	Illegal transit					X									1
T22	Illegal transport					X									1
	Crimes referable to manifestations of terrorism and or organized crime aimed at people and thing														
T23	Attack with vehicle used as weapon (WAAW)				X	X			X						3
T24	Attack with parked vehicle borne improvised explosive device (VBIED)				X	X			X						3
T25	Attack with encroaching VBIED				X	X			X						3
T26	Attack with penetrative ram vehicle				X	X			X						3
T27	Attack with suicide terrorist				X	X			X						3
T28	Attack with terrorist and/or threatening phone calls														
T29	Attack with envelope or letter bomb														
T30	CBRNE attack		X			X									2
T31	Ballistic attack, bombing and blasting		X		X	X			X		X				5
T32	Cyber attack with malware infiltration				X						X				2
T33	Cyber attack with subtracting data for ransom				X						X				2
T34	Cyber attack with direct manipulation				X						X				2
T35	Cyber attack to the management system				X						X				2
T36	Attack with Unmanned Vehicles (UAV or drone; AUV or UUV)				X	X			X		X				4
	Unattended and unforeseeable event causing terroristic and criminal attacks or disasters														
T37	Pandemic, epidemic, epidemic outbreak														
T38	Natural disasters and climate change	X													1
T39	Blackout				X	X					X				3
T40	Disaster propagation from neighboring infrastructures		X												1
T41	Geopolitical crises, armed clashes or combats, revolutions, uprisings				X										1

v-13

Fig. 4.4.8 - Major risks and priority threats for TC 4.2 Bridges

4.4.4. Risk treatment

In the **risk treatment** phase, it is necessary to establish a mitigation strategy and countermeasure plans for **each 2 major security threats** related to the priority risks (**Fig. 4.4.8**).

ST 12	**Arson**
ST 31	**Ballistic attack, bombing and blasting**

Figure 4.4.8 – Security threat leading to priority risks in T.C 4.2 Bridges

In addition to such threats, **other 8 security threats are of particular concern** for possible developments in term of likelihood and consequences **(Fig. 4.4.9**).

ST 16	**Malicious or non-compliant personnel, sabotage**
ST 23	**Attack with vehicle used as weapon (WAAW)**
ST 24	**Attack with parked vehicle borne improvised explosive device (VBIED)**
ST 25	**Attack with encroaching VBIED**
ST 26	**Attack with penetrative ram vehicle**
ST 27	**Attack with suicide terrorist**
ST 36	**Attack with Unmanned Vehicles (UAV or drone; AUV or UUV)**
ST 39	**Blackout**

Figure 4.4.9 – Security threat of particular concern for T.C 4.2 Bridges

Within the framework of a mitigation strategy for all priority threats, **the protection, prevention and transfer measures** for bridges security issues apply as shown in **Figures 17-1,-2,-3** of previous chapter 3.3. Such measures must be detailed in relation to the specific contexts.

Regarding the measures for protection, the subdivision of **active and passive measures and procedural-organizational measures** also apply.

It must be reminded that **any measure taken individually do not guarantee effectiveness** and a good professional must be capable of combining, mixing and dosing them.

4.4.5. Security recommendations

Bridges are strategic infrastructure and must be designed to withstand exceptional load conditions. Among all the **criminal and terrorist actions** that can damage a bridge the ones that present the greatest risks are arson, ballistic attacks and bombing. All other types of threats including physical attacks with vehicles and even explosives may not compromise the structure integrity given the large size and strength of the structure which is already designed to withstand considerable loads unlike a traditional building. Furthermore, an attack would require large quantities of explosives which are difficult to carry on a bridge without alerting police forces due to bridges usually being heavily monitored structures.

It should be noted that all these serious acts have a very low probability of occurring. On the other hand, acts of vandalism cause minor but repeated damage; their frequency can therefore be a real problem for managers, as it is unacceptable for some bridges, large or small, to be covered in graffiti and to have equipment that has been deliberately damaged.

Cyber-attacks may have consequences for the operation of the bridge but they cannot damage its structure.

The damages usually arise from a complex and interacting set of contributing variables. Common knowledge indicates that a bridge is most likely to be vulnerable in case of:

- lack of fire resistance criteria design;
- sensitivity to fire;
- excessive deformability or lack of redundancy of structural elements;
- lack of adequate protections;
- easy access to the structures;
- complex structural configuration;
- lack of video surveillance, road traffic control systems and vessel traffic systems;
- being built over waterways or near coastal areas;
- proximity to other infrastructure and airports.

Some **general recommendations (GR)** for the security of a bridge are shown in **Fig.4.4.10**.

GR 1	**Train bridge system personnel on security matters**
GR 2	**Raise staff awareness on information system security**
GR 3	**Implement access restriction procedures to prevent unauthorized persons or vehicles from accessing bridge system assets (service buildings, external areas, control centre)**
GR 4	**Provide special authorizations for subcontractors and suppliers likely to be involved in the maintenance of bridge control and traffic control centres**
GR 5	**Provide internal access restrictions to isolate control centre staff from other staff by securing entrances to these locations**
GR 6	**Organize formal powers to act in time in case of a security incident**
GR 7	**Provide standardized procedures for early detection of an incident, for alerting and for mitigating or neutralizing threats**

Figure 4.4.10 – General recommendations for T.C 4.2 Bridges

Further specific recommendations (SR) as related to the priority threats are proposed below (**Fig. 4.4.11):**

- **SR 1 : On fire resistance;**
- **SR 2 : On structural resistance;**
- **SR 3 : On geo-political context;**
- **SR 4 : On video surveillance, road traffic control system and vessel traffic service;**
- **SR 5 : On international navigation rules;**
- **SR 6 : On strategic defence.**

ST 12	**Arson**	**SR 1, SR 2, SR 4**
ST 31	**Ballistic attack, bombing and blasting**	**SR 1, SR 2, SR 3, SR 4, SR 5, SR 6**

Figure 4.4.11 – Most recurring threats and specific recommendations for T.C 4.2 Bridges

SR 1 – On fire resistance

A deliberate fire or arson can **destroy, seriously damage or even temporarily or partially put a bridge out of order**. As we have previously discussed on the subject of safety, the current structural standards of bridges do not explicitly consider fire actions. A fire can be caused by a road accident and it can develop on large surfaces on a bridge. The scientific literature indicates that this type of accident is becoming increasingly common. The most common causes of bridges fires are vehicle collisions or activities carried out near or below the structure, with the flammable

liquid leaks triggering fires, and arson. **The spread of the liquid** and therefore of the fire is highly unpredictable and the spread of the heat flow towards the supporting structure is strictly tied to the structural characteristics of the bridge.

Given the great variety of possible types of bridges, it is impossible to define criteria that are valid for all. Consequently, in the case of strong exposure to the risk of arson and terrorist attacks, it is first of all recommended to consider the **fire design of a bridge** which, unlike buildings and tunnels, should be based on the performance of the structure as a whole rather than on individual parts [133].

The possible evolution of the structure's behaviour in the event of fire with the deformation of the materials and geometry of the structure itself must also be considered. Particular attention in the **design phase** must be devoted to the deck, in particular in case of beams or steel reticular structures, due to local instability and shear failures. It is recommended to build fire resistant decks in relation to different fire intensity. Real or modelled fire scenarios should be carried out to study how to reduce the growth, spread and decay of a fire.

A fire can also be ignited as a result of a **ballistic attack or bombing** to a bridge, destroying or very seriously damaging the deck or a pier.

SR 2 - On structural resistance

Structural resistance is a trait normally already present in bridges as they are particularly resistant structures. But **resistance to the impact of an aircraft or ship** is not always considered. Bridges and overpasses with girders and with cables / stays made of steel and steel-concrete are particularly vulnerable due to being in most cases not designed with fire resistance criteria in mind, therefore being subject to a decrease of load-bearing capacity in the event of rapid heating of the steel structural elements as well as often being built using static schemes with low resistance to fire. With regard to the decks made with side-by-side and supported beams, particular attention must be paid to the design of the supports with elastomeric bearings which can be destroyed by fire or can come out of their positions even in the event of small impacts or explosions.

In this respect, **suspension bridges** are less at risk as they are less subject to damage by design given the difficulty of hitting a load-bearing cable and also the great strength of the load-bearing towers. On the contrary, a cable-stayed bridge can prove to be more vulnerable in case of damage to the tower or antenna, which are only stressed axially by the stays which acting in a balanced way and in case of absence or damage to one of the stays the antenna would not be able to bear strong bending moments.

SR 3 - On geo-political context

A ballistic attack can occur in **proximity to sites of importance** such as chemical facilities, sites at risk of major accidents, fairs and exhibition sites, and hubs of (inter)national importance (roads, motorways, railways, airports, ports) bringing consequences all around. Such typology of attacks can also be carried out by an airplane or a ship filled or not with explosives.

[133] Franchini A, “Sicurezza antincendio di ponti: perché conta e come ottenerla” (Fire safety of bridges: why it matters and how to get it), Antincendio, EPC Editore, Roma, Italy, 5, 2023.

It is also recommended to pay particular attention when **crossing waterways or passing near coastal areas** as from there a threat can be brought by a boat or a ship with explosives under or laterally to the bridge.

With regard to the risk of **ship collision**, protection with adequate fences must also be provided for the piers of the bridge if they are laid in the watercourse.

Everything becomes more complex in an **unstable political context**.

SR 4 – On video surveillance, road traffic control system and vessel traffic service

It is recommended to plan a **video surveillance and monitoring of the areas** close to the structures and implement an efficient and prompt firefighting capability. A **traffic control system** for timely regulation of traffic is also recommended, to control not only the type of vehicles but also the loads in such a way as to be able to stop dangerous vehicles from accessing the bridge and be prepared for any situation. Such systems can also be useful for predicting particularly unfavourable weather conditions that can affect the safety of the bridge deck and the towers or piers. Those systems are relevant for operation continuity of the route and vandalism prevention.

What's more, after a major incident, managers must quickly guarantee the continuity of the route. They must propose alternative routes and, in the worst case, quickly call in companies capable of temporarily installing a temporary or emergency bridge.

With regard to the risk of **ship collision**, in addition to adequate protection, a **vessel traffic service** (VTS) is recommended to control the risk of direct impact of ships against structures of the bridge, also including ships with a mast exceeding the clearance of the deck above the sea level.

SR 5 – On international navigation rules

In the case of **bridges of particular strategic importance**, international navigation rules are recommended to avoid accidents caused by impacts of airplanes or ships and ships with a very tall mast. A controlled security area around the bridge with 24-hour all-weather radar, video surveillance and alarm systems can provide information on the immediate context. It can be useful to check non-compliant aircraft and ships in order to provide information to avoid a collision.

SR 6 – On strategic defence

A ballistic attack can be carried out from a **long distance**. In this case the infrastructure protection systems must act on a much larger scale than the local one and should, if possible, benefit from military defence systems. In this case the security plan takes on a national strategic defence level. It is obviously recommended that a structure of strategic importance as a bridge be included in the national military defence system.

4.5. TC 4.4 TUNNELS

4.5.1. Introduction

4.5.1.1. General

The purpose of this chapter is to study the relationship between **tunnels**, topic of TC 4.4, and security. For this, it is necessary to frame such issues in general and then focus on the relationship between tunnels and road security.

Tunnels are engineering structures aimed at crossing an obstacle as mountains or waterways or to pass under inhabited areas. Together with bridges they constitute the **most expensive and risky works** in a road network and can last for centuries. In recent years the use of road tunnels has become very common as this type of infrastructure allows the roads to be hidden underground, solving in particular urban, environmental and landscape problems.

Tunnels have become increasingly expensive and complex[134] over the years, in particular due to growing levels of safety required in the event of a fire. Incidents and collisions are probably not more frequent in road tunnels than on open roads, as road tunnels can provide a safer and more controlled driving environment for road users. However, the consequences of serious accidents such as fire and leaks of dangerous substances are potentially more severe in the confined environment of a tunnel than on open roads[135].

The tunnel system

A tunnel system[136] includes the tunnel in the strict sense (the structure) and some complementary elements which are necessary to manage the tunnel especially in the case of incident/accident:

- the **road in and outside the tunnel**, including an alternative route in case the tunnel is closed for traffic or certain vehicles;
- the **tunnel control and supervision centre** (on site or remote) from which the tunnel is operated including technical installations and the telecommunication networks (optical fibre, etc.) with the capability of handling hundreds of points to be controlled and managing sophisticated scenarios;
- the **organization** (staff) and the processes for the management of the tunnel itself, including resource mobilization;
- the **traffic management measures** for the road network, the traffic management centre (if different from the tunnel control centre), interactions with other systems (e.g. : when the tunnel is part of an interconnected underground infrastructure or when another organization operates the road network outside the road tunnel);
- the **emergency management**, including a coordination with many partners in a timely manner to contain losses and avoid future disruption: public services (Fire Fighters, Police), subcontractors (cleaning and demolition services).

The lifespan of a tunnel is divided in different phases: design, construction, commissioning, operation and restoration/upgrading/replacement. In general, the **design of a tunnel**[137] includes the following points:

---

[134] See on the topic of complexity and tunnels the paper: S. Palchetti and A. Scala, “The difficulties of risk assessments for complex network infrastructure: applications to the security and the resilience of road infrastructure”, PIARC WRC, Prague ,2023, where the case of critical infrastructure is mentioned such as tunnels, where self-organization and human resource capacity are essential to dealing with complex situations such as fires.

[135] As accidents occurred in road tunnels with many dead can be mentioned: Mont Blanc (Italy-France) 1999, Tauern (Austria) 2001, San Gottardo (Switzerland) 2001, Frejus (Italy-France) 2005.

[136] Ref. “Improving Road tunnel resilience, considering safety and availability. A PIARC briefing note including a collection of case studies”, PIARC TC 4.4 Tunnels, 2022R04EN, 2022.

[137] Many PIARC publications on the issue of tunnels are available on the PIARC website, we can mention here in addition to those explicitly referred to in the text:

- “Road tunnels: complex underground road networks”, 2016R19EN, with the objective to make a point of the current situation around the world and the particularities of the underground networks;

- **the horizontal and vertical alignment**, which involves the design of the geometry of the underground interchanges or connections (in particular exits or merging areas). Particular elements of the project are the service tunnels that allow access during the work phase, the evacuation or escape routes in the event of fire, emergency team accesses and possible ventilation wells. In mountain tunnels, protective measures are planned against rocks slides, snowfalls and ice;
- **the functional transverse profile**, which must be designed on the basis of some parameters such as: traffic volume, type of vehicles allowed in the tunnel, organization of operations, urban or rural areas, number and width of the lanes, clearance (depending on the type of vehicle), emergency lanes, emergency stop lanes or the lay-bys, traffic dividers and their width in case of bidirectional operation, spaces for ventilation ducts. Relevant for safety/security are also escape structures for the evacuation of people in the event of fire (safe zones, corridors, passages, stairs, panic doors, routes for evacuating users and access for emergency and rescue teams, exits leading out of the tunnel, safety lighting, escape signs, anti-intrusion security devices). Numerous functional networks and equipment for operation pass through a tunnel: the sewer system also for collection of polluted liquids from the carriageways, the water supply network for the fire-fighting system with hydrants, the electrical networks with low, medium and high voltage cables. These systems must be adequately protected to ensure the tunnel's operating safety and in particular their protection against fire, theft and sabotage, as well as the possibility of carrying out maintenance and modifications throughout the lifespan of the tunnel. In terms of signals and signs, we have: lane signs, variable message panels, directional indications. Rest areas are needed for maintenance and safety of the operating teams.
- **the operating equipment and facilities**, which must allow the tunnel to fulfill its function, and in particular to ensure the flow of traffic, providing users with appropriate level of safety/security and comfort while crossing the tunnel. Lack of maintenance and human intervention may lead to a reduction in the reliability of

---

- "Design fire characteristics for road tunnels", 2007R01EN, to provide guidance and recommendations on the choice of design fire for road tunnels;
- "Experience with significant incidents in road tunnels",2017R35EN, on lessons learned from incidents and developments in safety management and risk analysis.
- "Large Underground Interconnected Infrastructure", 2019R42EN, (also in our LR, chapter B.4, Sheet n.4), this report is the continuation of the previous one of 2016 and analyze in a much details the particularities of these infrastructure;
- "Prevention and mitigation of tunnel-related collisions", 2019R03EN: the report presents and recommends possible organizational and technical measures one can implement to lower the probability (prevention) or the mechanical consequences (mitigation) of tunnel-related collisions.

Other PIARC reports on tunnels are also cited in our LR, in chapters 3.4 and 4.4.:

- "Introduction to the RAMS concept for road tunnel operations", 2019R05EN,
- "Road tunnel operation: first steps towards a sustainable approach", 2017R02EN,
- "Best practice for life cycle analysis for tunnel equipment", 2016R01EN,
- "Recommendations on management of maintenance and technical inspection of road tunnels", 2012R12EN,
- "Good Practice for the Operation and Maintenance of road Tunnels" 2004/05.13.EN.

the tunnel and its level of safety/security.[138] The main facilities relevant to safety/security issues are:

- **electricity supply**: redundant and protected distribution system from fire and other hazards that can cut power supply; electric cabins, immediate emergency supply UPS systems, or diesel generators that prevent the interruption of all of the safety equipment during a period of about half to one hour to guarantee minimal operation conditions; internal and external electric cabins;
- **ventilation equipment**: to guarantee the health, comfort and safety of the users and to control air pollution in an enclosed environment like a tunnel; it can reduce the spreading of a fire, until the complete evacuation of the tunnel as well as reduce thermal radiation and temperature, and the development and the propagation of toxic gases and smoke;
- **additional equipment** for ventilation such as air treatment or air cleaning and fixed fire suppression systems;
- **lighting**: to ensure safety and comfort of the users in a tunnel;
- **data transmission and SCADA**: they must have the full supervision of the tunnel in any critical condition, permitting the collection, transmission and treatment of information, and then the transmission of the equipment's operating instructions;
- **radio communications**: there are addressed to users and include also remote monitoring, data detection, traffic management, control and supervision, as well as the organization of evacuation; it includes emergency phone and radio networks for the operation teams, the emergency services and tunnel users;
- **signalling**: essential in all critical operations, it includes among all fixed sign panels, traffic lanes signals, variable messages signals, traffic lights and stopping lights;
- devices for **firefighting** localized and along the traffic lanes;
- **other equipment** for safety is luminous beacons, "lifelines" fixed on the side wall.

Road tunnels can be also part of **complex underground infrastructure**[139] as:

- a sequence of successive tunnels;
- multimodal tunnels: shared usage between buses, pedestrians, bicycles and trams;
- tunnels giving access to business and commercial centres for public access and freight delivery;
- tunnels with a dual function as transit and access to underground car parks;
- tunnels with reduced vertical clearance;
- underground infrastructure with numerous entrances and exits, as well as underground interchanges.

Tunnels safety

Safety is the major concern in tunnel planning, design, implementation, operation, maintenance, and refurbishment. Following several major tunnel fires in the years 1999 and 2000 [2], considering

[138] See PIARC reports 2012R14EN "Life cycle aspects of electrical road tunnel equipment" and 2016R01EN "Best practice for life cycle analysis for tunnel equipment"

[139] See the PIARC technical report Road Tunnels: Complex Underground Road Networks 2016R19EN

the relevant risks of loss of human lives, governmental bodies, road authorities, owners and designers are channelling resources on improving safety levels in new and existing tunnels. Therefore, even more stringent safety regulations, construction standards and measures have been developed and implemented [140].

Current risks on road tunnels are related to incidents/accident, visibility, traffic congestion and jams, breakdown vehicles, hazards in case of fire, dangerous goods transportation. In perspective, other risks can be brought about by technological innovations, in particular, alternative fuels and autonomous vehicles.

Transport of hazardous materials has a relevant impact on safety and security. In this type of transport, the particular environmental conditions that occur in road tunnels can lead to variations both in the accident rate and in the severity of the possible consequences of the leakage of dangerous material. Therefore, considering the consequences of accidents in tunnels, it is necessary to take into account an increase in the effects compared to other structures in the open. The main legislation adopted in Europe is the ADR[141] that regulates the transport of dangerous goods by road. According to it, dangerous goods are materials and objects the transport of which is prohibited and can only be authorized under certain conditions. Among these we have high-risk dangerous goods, i.e., goods potentially usable for terrorist purposes and which can therefore cause serious effects such as loss of human lives or mass destruction. The ADR Code provides a five-category classification of tunnels from no transit restrictions to restrictions for all categories of dangerous goods in relation to the characteristics of the tunnel and certain hours of the day or days of the week.

We can consider two different aspect concerning tunnel safety: an **active** one**,** to prevent accidents, and a **passive** one, to contain the consequences of the accident. Active safety depends on the already mentioned technical factors such as length and geometric characteristics as well as on traffic, vehicles and transported goods. Passive safety requires awareness from road users, attention to driving, compliance with traffic rules, effectiveness of signs and emergency measures, lighting system.

Consequently, the main **focus of road tunnels safety** deals with accident/incident characteristics, fires, smoke propagation and management, egress behaviour and escape routes, signs to provide evacuation of the able-bodied and disabled people, lighting, fixed fire-fighting systems and possible alternatives, managing efficient emergency response with private or public fire brigades, developing codified operating and intervention procedures and training for all stakeholders. In this respect, a distinction con be made between short, medium and long tunnels (under 500 m, 500 – 2500 m, over 2500 m), monodirectional or bidirectional (single or twin tube). In synthesis, the safety conditions in a tunnel result from the combination of factors such as the infrastructure,

[140] In European Union countries, Directive 2004/54/EC is applied which establishes minimum safety requirements relating to the infrastructure and operation of road tunnels of the trans-European network longer than 500 meters.

[141] ADR Code (*European Agreement Concerning the International Carriage of Dangerous Goods by Road*) is based on the UN Recommendations and signed in 1957. It has been ratified by numerous European states including all members of the European Union (also extended to national transport). This regulation is applied also in other countries and similar regulation exists as well in other part of the world. In ADR, dangerous goods are divided into 9 classes and many subclasses ranging from explosive material to flammables to toxic, radioactive material and the so-called precursors, i.e., substances which when mixed with others give rise to an explosive. See on this topic the paper: F.Paval, S.Palchetti, "Current road security problems in the Romanian territory due to the illegal transport of dangerous goods", PIARC WRC, Prague, 2023.

operation, interventions, vehicles and users (**Fig. 4.3.1**). Today, tunnel safety in most new tunnels meets the highest standards ever achieved in the industry.

Fig. 4.5.1 - Factors affecting safety in a tunnel [142]

Prescriptive design codes are causing **ever-increasing requirements**, new technological equipment, increasing number of data points for system monitoring with decreasing the life cycle of systems. The challenge lies in the complexity of safety measures which can have negative impacts on safety and security [1].

Past **PIARC work on risk assessment and risk management** includes reports such as e.g., "Risk analysis for road tunnels (2008R02)" and "Risk evaluation, current practice for risk evaluation for road tunnels" (2012R23EN)". As requested by the 2004 EU Directive on the minimum safety requirements for tunnels in the trans-European road network, risk analysis has become a common tool for assessment of tunnel safety in several countries. A broad spectrum exists when it comes to qualitative and quantitative risk analysis [143] for each step of the risk assessment process to estimate the safety/security level of a given tunnel (incidents/accidents, fires, dangerous good transportation). In particular, in the scenario-based approach, different scenarios and possible subsequent events can be analysed in a detailed time-dependent analysis of sequences of events or a realistic planning of emergency response. Consequently, for each path of subsequent events, likelihood and consequences can be estimated. By summarizing the partial risks of all scenarios, the overall risk of a tunnel can be evaluated [144]. This approach also includes scenarios which may not yet have occurred.

4.5.1.2. Tunnels and security

The whole issue of tunnels, as described in the previous paragraph, presents **security problems** depending on whether the tunnel is monodirectional or bidirectional, its length, traffic typology. The threats concern the personnel, users of the tunnel who may themselves become perpetrators of a threat, the physical part i.e., the structure, infrastructure, and vehicles, the IT and the procedural and organizational parts. Terrorist and criminal acts could happen in a tunnel, as terrorists are likely to target objectives with higher potential impact on society and in terms of media coverage. This is the case of objectives with potentially high number of deaths and/or that are emblematic as for long road tunnels (e.g., base tunnels under the Alps in Europe, some of which are considered critical infrastructure). Particularly for these, special security (and safety) measures are necessary.

---

[142] PIARC "Road Tunnels Manual", version 2, October 2019, http://www.piarc.org
[143] "Risk analysis for road tunnels", report PIARC 2008R02.
[144] "Current practice for risk evaluation for road tunnels", report PIARC 2012R23EN, which incorporates the outputs of the previous report of 2008 on the same topic.

Contrary to safety, **security measures** are not regulated by laws but only by standards, guidelines and recommendations. Advanced safety measures can also provide some effectiveness in security. The consequence is that while a tunnel project is being developed it is unclear whether and where security devices will be installed.

In general, the **effects of a random accident** for safety reasons and a deliberate attack can be the same, but in tunnels, **safety and security** sometimes come into conflict [145]. One example is fires or toxic gas release (which could be accidental or intentional) for which safety management system must provide for a reliable, immediate and easy opening of doors in the event of an emergency. As a consequence, escape routes or emergency exits in the tunnels must be free and easily accessible but, in the framework of security, it is also necessary to prevent the use of emergency exits from outside the tunnel as access routes by malicious persons to cause potential damage inside the tunnel. Compatibility of door opening devices for fire safety purposes with door closing devices for anti-intrusion purposes it is not a widespread practice and is an important topic yet to be fully explored.

The risks of physical security are associated with those of **cyber security** given that, in recent years, there has been a rapid evolution of cyber threats which have often exceeded the criticalities of physical security for the relevant cases. Tunnel control systems, based on SCADA systems, are particularly exposed to cyber-attacks. In perspective, the **new technologies of connected cars and automated driving**, as well as the so-called "smart" roads where the management platforms are not adequately protected, represent potential targets for cybercrime, also in relation with tunnels. However, likelihood of a self-driving car being used by a cybercriminal to target a tunnel seems currently very low[146].

As regards road tunnel systems, **case studies** concern documented hacking attempts that modified information panels by providing misleading information to drivers or that interrupted the operation of lighting and ventilation systems. In this sense, the vulnerability of the systems - cabins, ventilation, cameras, fire-fighting, emergency call stations - also constitutes a major threat to the entire corporate network as access points for a possible cyber-attack. The threat of cyber-attacks is real [147] and an organization must be prepared to deal with it. Research carried out in Germany by the BASt (Federal Roads Research Institute) in Bonn has shown the possibility for an attacker to take full control of the control centre of a tunnel, without the operators of the centre even noticing.[148]

Due to difficulties of adopting integral security measures right from the design stage, security prevention measures are currently not foreseen in national, regional and local road networks. Therefore, it is widespread practice to **strengthen the safety measures** as traffic control and surveillance systems, with better company organization, training and awareness-raising interventions for personnel in terms of security. It can be a start, even for economic reasons, but it comes with obvious limitations.

---

[145] See in this report chapter 4.10 on TC 3.1 Road Safety.

[146] Autonomous vehicles are mainly subjected to cyber-attacks that will decrease the security level of their car (ghost objects, breaks less efficient) according to ENISA.

[147] In 2015, the Carmel Tunnel, in Haifa (Israel) crossing the Carmel Mountains, had to be closed for eight hours due to a physical cyber-attack, resulting in severe traffic congestion (The Associated Press, 2015).

[148] See Appendix 1.2 in our previous final Report of PIARC TF C.1 "Security of Road Infrastructure", 2019.

Tunnel control centres

The control centres of the tunnels deserve particular attention since they are responsible for **monitoring and controlling the traffic inside and at their entrances**, for maximum operational safety. They always operate remotely even when built near the tunnel. They are mostly integrated into IT communication networks through different interfaces and in the absence of effective protections it is possible to carry out manipulations in the control units of the systems. There is also the possibility of manipulating sensor data, blocking control commands and altering standard safety controls which can cause:

- closure of the tunnel;
- damage to tunnel systems;
- interruption of the safety devices;
- data theft and ransomware.

Tunnel as critical infrastructure[149]

It is worth mentioning the case of the **Frejus road tunnel between Italy and France**, about 13 kms long, recognized by two governments as critical infrastructure in the framework of a Directive of the European Union. The protection of a critical infrastructure poses the question of priority interventions during operations. Some critical scenarios for security have been defined:

- explosion in a zone near the tunnel, therefore actions not directly aimed at the tunnel but which block access to it;
- simultaneous explosions of vehicles loaded with explosive at both entrances of the tunnel;
- explosion of car bombs in proximity of the central operations control that manages all the security system;
- launch of particular objects from ventilation ducts above the road surface;
- injection of a toxic gas in the air ventilation system through a well or an external air vent;
- malfunctioning of coordinated radio control rooms (twin rooms in stand-by that are activated in case of emergency on both sides);
- loss of high-tension electricity lines that run under the tunnel;
- loss of communication of the computer systems.

[149] it is a road infrastructure considered strategic for the transport of a country, see also paragraph 1.1.2 “An outlook on road infrastructure and transport security” in this Report.

Complexity and resilience

Tunnels are **complex [150] systems** as they are made up of different parts that can interact in different ways. In general, within the normal operation of an infrastructure, all the parts act individually according to the criteria with which they were designed and built for, i.e., separately and in a pre-established order. On the other hand, during a crisis, disorder and complexity can arise which must be taken into account. This can occur in particular in the face of the non-linear dynamics of a fire, people fleeing, or terrorist attacks. It is not possible to fully predict the behaviour of people inside a tunnel during a fire. It is determined by internal and external factors and sometimes by chance. A fire in a tunnel can destroy the power lines and other systems that pass through it. It can cause structural failures and can generate polluting and toxic fumes which can spread outside from the aeration shafts with consequences on the natural or urban environment, depending on the location of the tunnel.

Tunnels behave as a complex system during critical phases (e.g., fire). Security events in which a resilience-oriented approach can be useful, are: fires, disasters involving dangerous goods, failure of the tunnel system [3,9]. This means non-linear dynamics that are not based on the classic "analysis-planning-implementation" managerial scheme. In such cases, predictive models may not prove helpful and knowledge of the phenomena as well as the ability to react correctly to every critical situation can be necessary. Resilient engineering by self-organization and self-leadership are more suitable in a tunnel during a critical phase, with operators showing a high aptitude for responsibility and critical decisions following the model "action-learning-adaptation". Resilience also can be improved with on-site traffic officers and/or service contracts with a company to manage fires or leaks when they occur. In other words, during a critical phase it can be more effective to deal with the consequences as opposed to the causes.

Many definitions of resilience can be found in scientific literature, as it is a cross-cutting issue: in essence, when talking about resilience, we mean the ability of a subject - e.g., asset, organization, community, region - to anticipate, resist, absorb, respond, adapt and recover from a disruptive action. Resilience consists in the following properties[151]:

- robustness: the ability of the tunnel to withstand a given level of stress without undergoing degradation or loss of function;
- redundancy: the extent to which the elements or systems of the tunnel are replaceable, i.e., capable of satisfying the functional requirements in the event of interruption, degradation or loss of functionality;
- resourcefulness: the ability of tunnel management to identify problems, set priorities and mobilize resources when conditions exist that threaten to destroy some elements, systems or other units of analysis; self-organization of the operators;

[150] The definition of complexity provided by the ISO 22300, Security and Resilience – Vocabulary, is "the condition of an organizational system with many diverse and autonomous but interrelated and interdependent components or parts where those parts interact with each other and with external elements in multiple and non-linear ways".
[151] See the reference at previous note 3 at page 37.

- rapidity: speed of recovery of the tunnel operations, ability to satisfy priorities and achieve objectives in a timely manner in order to contain losses and avoid future disruptions.

In this regard, an ongoing debate is how to measure resilience, i.e., the level of resilience available and necessary. Certainly, more resilient from a security standpoint: a dual tube tunnel is more resilient than a single tube, as it allows specialized teams to intervene within a few minutes. They are also more resilient if entirely fire resistant, or if they allow orientation inside in total darkness before evacuating people and lead the evacuation. A detailed technical knowledge of the tunnel and the traffic inside it also necessary.

4.5.1.3. Specific requirements for TC 4.4 from PIARC ToR

TC 4.4 was conceived with seven sub-themes and security recommendations may concern three of them:

- 4.4.1. Measures for increasing resilience of tunnels, since security can contribute on increasing the resilience of the tunnel system;
- 4.4.2. Best practices in management (maintenance and traffic operation) in urban and heavy traffic tunnels, as security is one of these best practices particularly in urban tunnels and in case of heavy traffic tunnels;
- 4.4.4. Intelligent Transport Systems on tunnels, considering that security must be integrated in Intelligent Transports Systems (ITS); safety distance control, lane departure warning systems, heavy vehicle guidance systems, vehicle localization and counting systems, identification of hazardous goods vehicles.

It should be noted that, regarding the sub-theme 4.5.5. “Update of the Tunnels Manual”, security aspects are not considered in the manual and it would be advisable that security aspects be integrated in it.

4.5.1.4. Methodology and international standards

Risk analyses of security threats according to the classic method can be insufficient in a complex context and resilience allows us to be prepared beyond the present and for predictable events[152]. However, it is hard to imagine a world where resilience is applied everywhere: to tunnels, roads, control centres, asset management, staff and road users…etc. The limit of the resilient approach is that it does not know reality, but tends to incorporate all possible consequences[153]. It therefore does not deal with the new, possible threats, because it tends to encompass them all. A threat framework is used to have the vision in the internal and external context of a tunnel, and it is advisable to always keep an eye on latest developments. Resilient engineering and classic risk

[152] Park, Jeryang, et al. "Integrating risk and resilience approaches to catastrophe management in engineering systems." Risk analysis 33.3 (2013): 356-367. This paper tells that in risk analysis of complex systems, resilience engineering must be taken into consideration especially when considering catastrophic events.

[153] E.g., the failure of a CCTV camera system requires routine maintenance and the resilience of the tunnel system should not be invoked for this.

management are complementary, integrating resilience into risk management through improvement processes envisaged by ISO standards [154] [155].

ISO's standard for risk management, **ISO 31000**, is the appropriate standard to support this, as explained in previous chapters 2 and 3 of this report. ISO 31000 explains the fundamental concepts and principles of risk management, describes a framework, and outlines the processes of risk identification and management. In the ISO 31000 family is particularly relevant for tunnels: IEC 31010:2019, Risk management – Risk assessment techniques and ISO 31073, Risk management – Vocabulary. A handbook[156], jointly published by the ISO and United Nations Industrial Development Organization (UNIDO), has been developed to support organization's effort in creating and protecting corporate value to assist in achieving the multiple benefits offered by ISO 31000. The ISO family 28000 must also be taken into account, and ISO 28001 is particularly focused on supply chains.

A useful reference can be found in **ISO 22301:2019**, "Security and resilience – Business continuity management systems – Requirements", which specifies the structure and the requirements for the design, implementation and maintenance of a resilient management system, aimed at developing business continuity. It incorporates the principles of ISO 31000 on risk management. With regards to the system and organization of road tunnels, the aim is to always provide a safe traffic route through the tunnel. The standard provides a framework to support this objective with technical means and operational procedures. A broad look at the international standards and their contents can be considered as a reference in this context is shown in **Fig. 4.5.2.**

It should be noted that under the chairmanship of INTERPOL and UNOCT (United Nations office of counter-terrorism), a compendium of good practices for the protection of critical infrastructures against terrorist attacks was developed. It contains insights concerning risk analysis that have been taken into account in chapter 4.2.3.

[154] F. Flammini, R. Setola, and F. Lollini, "Resilience Engineering and Risk Management," in Resilience Assessment and Evaluation of Computing Systems, Springer, 2012, pp. 35-52. This paper discusses the relationship between resilience engineering and classic risk management, noting that they are complementary and can be integrated through the improvement processes outlined by ISO standards. The authors argue that resilience engineering emphasizes the importance of understanding how complex systems respond to unexpected events and disturbances, and that it can help organizations to improve their risk management processes by incorporating this understanding into their risk assessments. The paper provides an overview of the key principles and practices of resilience engineering and their implications for risk management in the context of complex systems such as road infrastructure.

[155] Yu, David J., et al. "Toward general principles for resilience engineering." Risk Analysis 40.8 (2020): 1509-1537. This paper states that in the search for tools and methodologies for risk analysis of complex systems, resilience engineering must be considered to manage complexity.

[156] ISO 31000:2018 – Risk management – A practical guide.

				Impact on security of the sub-themes of TC 4.4		
	ISO family & relevant Standards	Impact on security of tunnels	Topics	4.4.1 Measures for increasing resilience of tunnels	4.4.2. Best practices in management practices (maintenance and management)	4.4.4 ITS in tunnels
1	9000	1	Specific requirements for quality management systems including security	general application		
2	14000	1	Specific requirements for environmental management including security	general application		
3	27000	3	Specific requirements for information security management systems	general application		general application, for new technologies
4	28000	4	Specification for security management systems for the supply chain	general application, specific focus on material supply chain for tunnel		general application
5	31000	3	Guidelines for managing risk	general application		
6	20858	3	Framework to assist marine port facilities in security assessment and security plan	no application		
7	22300	4	Vocabulary of security and resilience	general application		
8	39000	2	Road traffic safety management systems	general application		
9	45000	5	Guidance for occupational health and safety management systems	is applied for tunnel operators		
10	IWA-14	1	Specification for vehicle security barriers	is applied for tunnel operations		
11	CEN/TR 16705	3	Classification for perimeter protection systems	application for the protection of tunnels and control centres, guidelines to devices for remote control		
12	ADR	3	Specification for the international carriage of dangerous goods by road	relevant application for incident prevention		
13	ENVISION	3	Guidelines to implement more sustainaible infrastructure, resilient and equitable projects	design of tunnel system		design of tunnel system, new technology

Fig. 4.5.2 - Impacts of ISO family & relevant standards on security for TC 4.4 Tunnels

The **compatibility of door opening devices** for fire safety purposes (safety) with door closing devices for anti-intrusion safety purposes (security) is a topic on which many international organizations are working. In particular, the Confederation of Fire Protection Associations Europe (CFPA E), which deals with fire safety, natural disasters and security with the aim of facilitating and supporting the commitment to fire protection measures in the European countries, produced in 2013 the Guideline 2:2018 F "*Panic & Emergency Devices*" on exit devices. It complies with the European standards for panic and emergency exit devices, EN 1125 and EN 179. The guideline applies where the activity imposes demand for doors which shall normally be kept locked from the outside and/or prevent the passage of unauthorized persons, and shall also be used as escape routes.

Regarding the **signs necessary for emergency purposes**, especially in presence of disabled people, according to the Swedish Fire Protection Association (*Brandskyddsföreningen*), member of CFPA E, approximately 25% of the entire population is considered disabled in various ways. These also include non-self-sufficient children, elderly people, pregnant women, etc. It is therefore essential to account for such individuals during the fire and security planning and designing stage of escape signs and routes. On this topic, the Guidelines CFPA-E 5: 2016 F "*Guidance signs, emergency lighting and general lighting"*, and CFPA-E 33: 2015 F "*Evacuation of people with disabilities"* are available. In relation to the various disabilities, different approaches are needed to signal an emergency and the need for evacuation. This requires real evacuation planning and must also include specific devices such as wheel chairs, rescue lifts, safe zones, etc., in the various living and operational contexts (hotels, hospitals, churches, shopping centres, restaurants, bars and nightclubs, museums, theatres, schools, offices, etc.) including tunnels.

4.5.2. External and internal contexts

The impact of security - regarding criminality, vandalism and cyberattacks – in the **external and internal contexts** of a tunnel must be considered in order to prioritize risks and ultimately propose some recommendations.

The macro-areas of vulnerabilities, the elements of vulnerability and the threatened assets, related to the security effects on road tunnels both in their external and internal contexts are shown **in the first three columns MAV, EV, TA of Figures 4.5.3-1 and 4.5.3.2**.

4.5.3. Risk assessment for TC 4.4 Tunnels

For risk assessment, a correlated reading between the following **figures 4.5.3-1, 4.5.3-2, 4.5.4, 4.5.5., 4.5.6, 4.5.7** is necessary.

4.5.3.1. Risk identification

The whole issue of tunnels, in all its parts as described in the previous paragraphs, presents **security problems.** Threats can concern personnel, user of the tunnel – who may also become perpetrators of damages - , the physical part i.e. structure, infrastructure, complementary elements and vehicles, the IT and the procedural and organizational parts. The tunnel system as a whole is a complex infrastructure due to the possible domino effects with cascading consequences.

In **Fig. 4.5.4**., threats for the tunnels are shown:

- **in column GT**: security threats for tunnels and tunnel management in general include classic malicious acts and the ones concerning the use of new technologies with more sophisticated attacks as well as the use of tunnels as geopolitical weapons;
- **in column ST1**: threats in relation to resilience also include criminal and terrorist actions;
- **in column ST2**: regarding maintenance and traffic operations we need to also consider the ones that can cause deaths or claim lives of people at work;
- **in column ST3**: misinformation in intelligent transport can also be a major threat for tunnels.
- In **column T of Figures 4.5.3-1 and 4.5.3-2**, the possible security threats are considered.

		MAV	EV	TA	ST	L	C	R	
		MACRO-AREAS OF VULNERABILITY	ELEMENTS OF VULNERABILITY	THREATENED ASSET	SECURITY THREATS	LIKELI HOOD	CONSE QUENCES	RISKS	Notes
EXTERNAL CONTEXT	1	GEOGRAPHICAL	Locations exposed to any external action such as natural disasters (floods, earthquakes, tsunamis, hurricanes, volcanoes, etc.) and pandemic	In general, any relevant external structure or areas such as portals, control areas, material storage areas, construction sites, toll barriers, control centres, power stations	37, 38	2	4	8	If located in such an area
	2.1	INFRASTRUCTURAL	Proximity to sites of importance for security purposes (chemical centres, sites at risk of major accidents, fair and exhibition sites, etc.)	Idem, due to explosion or fire	12, 30, 31	1	4	4	Relevant effect but low likelihood
	2.2		Proximity of hubs or networks of (inter)national importance (roads, motorways, railways, airports)	Idem, due to incident or accident	40	2	3	6	Not relevant
	2.3		Proximity to police forces sites, military settlements, Fire brigades	Idem, due to protests	20	1	2	2	Not relevant
	3.1	SOCIO-ECONOMIC	Areas with high unemployment rate and a high state of material and social need	Idem, due to protests, strikes and crimes against people and things	1-3, 7-22, 23-36, 39	4	4	16	Extreme risk
	3.2		Possibility of media attacks, by competitors or customers	Reputation	19	2	2	4	Not relevant
	4	POLITICAL	Unstable political context	The whole organization can be vulnerable	All except 4-7, 37, 38	3	4	12	Possible moderate risk in case of strategical location
	5.1	TERRITORIAL	Presence of micro-crime (theft, robbery, murder, fire, extortion, money laundering, usury)	Idem		4	3	12	Moderate likelihood, not catastrophic consequences
	5.2		Presence of organized crime, terrorism	Idem		4	4	16	Extreme risk
	5.3		Activism of anarcho-insurrectionist movements, condition of confessional or racial segregation	Idem		2	3	6	Low likelihood and moderate effect

Fig. 4.5.3-1 - External context, risk identification and analysis for TC 4.4 Tunnels

		MAV	EV	TA	ST	L	C	R	
		MACRO-AREAS OF VULNERABILITY	ELEMENTS OF VULNERABILITY	THREATENED ASSET	SECURITY THREATS	LIKELI HOOD	CONSE QUENCES	RISKS	Notes
INTERNAL CONTEXT	1	EXTERNAL AREAS	Roads, parking spaces, vehicles of visitors and suppliers, portals for message panels, people	Roads, vehicles, portals, people	1-4, 9-15, 20, 23-24, 27-28, 30-31, 36, 38-41	3	3	9	Moderate consequences in case of penetrative vehicle and ballistic attack
	2	EXTERNAL PERIMETER	Accesses, protections	Security personnel, employers, doors and gates, control systems	9-15, 20, 21-31, 36, 38-41	3	3	9	
	3.1	INTERNAL AREAS	Structures	Inside a tunnel, descendants, escape facilities, ventilation wells	9-15, 21-30-31, 36, 39	1	5	5	A ballistic attack to the structures of the tunnel can be catastrophic, but low likelihood
	3.2		Buildings	People, offices, buildings	9-14, 18, 21-31, 36, 39	1	4	4	More consequences if inside a tunnel
	3.3		Roads	Accesses, entrances, exits, parking spaces, people	12, 18, 22-23, 31, 36	1	3	3	More consequences if inside a tunnel
	3.4		Vehicles	Company, business, employees, visitors, suppliers	12-13, 21-24, 31, 36	1	2	2	
	4.1	OFFICES	Staff and managers	The whole of the employees of an office, administration, services, toll stations	1-4, 7-8, 16, 18, 20-21, 37	2	2	4	Access control
	4.2		Visitors and suppliers	Personnel, computers and other digital devices, information, buildings	6-12, 14, 16, 18, 20-21, 32-35, 37	2	3	6	Visitors and suppliers are a risk, ex. virus spread via a USB flash drive
	4.3		Computer systems and office equipment	Computers and other digital devices, cyberattacks	12, 16-18, 31-35, 39	4	4	16	Major risk for physical and cyber-attacks to offices
	4.4		Information/ communication	Internal digital network	12, 17-18, 31-35, 39	4	4	16	Major risk, e.g., setting misinformation on panels
	5.1	PRODUCTION/ OPERATIONF ACILITIES	Work areas	Service stations, toll stations control room, people	16-17, 36, 39	2	3	6	Only internal people are allowed to enter
	5.2		Installations	Equipment, devices (electrical power supply and distribution, lighting, signalling, over-weight vehicle detection, etc.)	16-17, 32-36, 39	2	3	6	If external people not admitted
	5.3		Emergency	Equipment, devices (fire-fighting systems, smoke and hot gases control, air quality)	16-17, 32-36, 39	2	3	6	idem
	5.4		Consumables	Dangerous materials	16	1	2	2	idem
	6	CONTROL/ DATA CENTRE	Server, SCADA systems	Platforms and data bases to ensure road and tunnel safety and staff management	12, 16-18, 31-35, 39	4	4	16	Extreme risk
	7.1	STORAGE	Row materials	Dangerous goods	12, 16, 36, 40	1	2	2	
	7.2		Finished products	Dangerous goods	12, 16, 36, 40	1	2	2	
	8.1	LABORATORIES	Staff, specialists, experts	Research programs, documents Information/know-how	1-9, 16-19, 37	1	4	4	Staff can have confidential information
	8.2		Offices	Structures	23-36, 39	1	4	4	A laboratory can be physically inside the tunnel
	8.3		Computers and digital devices	Research programs, Information/know-how	16-18, 32-35, 39	1	2	2	know-how can be remotely

Fig. 4.5.3-2 - Internal context, risk identification and analysis for TC 4.4 Tunnels

		GT	ST1	ST2	ST 3
	Security threats	Tunnels in general	Sub-theme 4.4.1 Measures to increase the resilience of tunnels	Sub-theme 4.4.2 Best management practices (maintenance and traffic operation) in particular in urban and heavy traffic tunnels	Sub-theme 4.4.4 Intelligent transport systems in tunnels
	Crimes against people				
T 01	Aggression	X	0	X	0
T 02	Robbery	X	0	X	0
T 03	Mugging	X	0	X	0
T 04	Taking hostages	0	0	0	0
T 05	Kidnapping	0	0	0	0
T 06	Mobbing	0	0	0	0
T 07	Stalking	0	0	0	0
T 08	Corruption	0	0	0	0
	Crimes against things				
T 09	Theft	X	X	X	X
T10	Vandalism	X	X	X	X
T11	Graffiti	X	X	X	X
T12	Arson	X	X	X	X
T13	Throwing objects to damage	X	X	X	X
T14	Violation of private property, unauthorized entry	0	0	0	0
T15	Piracy	0	0	0	0
	Crimes against people and things				
T16	Malicious or non-compliant personnel, sabotage	X	X	X	X
T17	Communications	0	0	0	0
T18	Disclosure of information, espionage	0	0	0	0
T19	Misinformation	X	X	X	X
T20	Civil protests and strikes	X	X	X	0
T21	Illegal transit	X	X	X	X
T22	Illegal transport	X	X	X	X
	Crimes referable to manifestations of terrorism and or organized crime aimed at people and thing				
T23	Attack with vehicle used as weapon (WAAW)	X	X	X	X
T24	Attack with parked vehicle borne improvised explosive device (VBIED)	X	X	X	X
T25	Attack with encroaching VBIED	X	X	X	X
T26	Attack with penetrative ram vehicle	X	X	X	X
T27	Attack with suicide terrorist	X	X	X	X
T28	Attack with terrorist and/or threatening phone calls	X	X	X	X
T29	Attack with envelope or letter bomb	X	X	X	X
T30	CBRNE attack	X	X	X	X
T31	Ballistic attack, bombing, blasting	X	X	X	X
T32	Cyber attack with malware infiltration	X	X	X	X
T33	Cyber attack with subtracting data for ransom	X	X	X	X
T34	Cyber attack with direct manipulation	X	X	X	X
T35	Cyber attack to the management system	X	X	X	X
T36	Attack with Unmanned Vehicles (UAV or drone; AUV or UUV)	X	X	X	X
	Unattended and unforeseeable event or harmful voluntary acts causing terroristic and criminal attacks or disasters				
T37	Pandemic, epidemic, epidemic outbreak	X	X	X	0
T38	Natural disasters and climate change	X	X	X	X
T39	Blackout	X	X	X	X
T40	Disaster propagation from neighboring infrastructures	X	X	X	X
T41	Geopolitical crises, armed clashes or combats, revolutions, uprisings	X	X	X	X

GT : general threats for security of tunnels
ST : specific threats for security in the sub-themes

X is a threat **0** is not a threat
X/0 possible threat

v-13

Fig. 4.5.4 Security threats for TC 4.4 Tunnels

4.5.3.2. Risk analysis

In columns L and C of Figures 4.5.3-1 and 4.5.3-2, the assessment of the likelihood of the occurrence of threats and the evaluation of consequences is made. A rating of likelihood in five categories is shown in **Fig. 4.5.5** and a rating of the potential consequences in five categories is shown in **Fig. 4.5.6**. Consequences are here defined in terms of damage costs, which can be added

to the cost of the number of deaths (e.g.: about 1.500.000 € per pers.), serious injures (150.000 € per pers.) and minor injures (5.000 € per pers.).[157]

1.	Rare	>20 years	< 10% of cases
2.	Unlikely	every 10-20 years	< 33%
3.	Moderate	every 4-5 years	< 45 - 50%
4.	Likely	once a year	> 60%
5.	Almost certain	once a month	> 90%

Fig. 4.5.5 - Severity of likelihood for TC 4.4 Tunnels

1.	Insignificant	damage 1000€ - 5.000 €
2.	Minor	damage 5.000€ - 100.000 €
3.	Moderate	damage 100.000€ - 1.000.000 €
4.	Major	damage above € 1.000.000
5.	Catastrophic	extremely high

Fig. 4.5.6 - Severity of consequences for TC 4.4 Tunnels

4.5.3.3. Risk evaluation

In column R of Figures 4.5.3-1 and 4.5.3-2, the criticality of the risk is assessed assigning a score derived from the product L x C = R (also called magnitude following ISO 31000). In it, only the adverse event most harmful and dangerous (extreme or red ones or magnitude 15-25 as shown in Fig. 16 of chapter 3.2.4 this Report) are considered.

The results obtained are summarized in **Fig. 4.5.7** in order to prioritize risks. It must be noted that in the case of tunnels **there are 5 major macro-areas of risks in the external and internal context and 9 priority threats**.

[157] It should be noted here that the security's events (like terrorist attack for instance) are not accidental but intentional. Therefore, they are not random events as the safety's ones (like fire in tunnels). So, in the security field, likelihood is not determined based on a statistic approach but is assessed on a reasonable prediction of terrorist intentions and capabilities.

		MACRO-AREAS AND PRIORITY RISKS													
		EXTERNAL CONTEXT					INTERNAL CONTEXT								
		1	2	3	4	5	1	2	3	4	5	6	7	8	
		GEO	INFR	SOC-EC	POL	TERR	EXT A	EXT P	INT A	OFF	P/O	DAT C	STO	LAB	PRIOR
				16		16				16		16			
	Crimes against people														
T 01	Aggression			X		X									2
T 02	Robbery			X		X									2
T 03	Mugging			X		X									2
T 04	Taking hostages														
T 05	Kidnapping														
T 06	Mobbing														
T 07	Stalking			X		X									2
T 08	Corruption			X		X									2
	Crimes against things														
T 09	Theft			X		X									2
T10	Vandalism			X		X									2
T11	Graffiti			X		X									2
T12	Arson			X		X				X		X			4
T13	Throwing objects to damage			X		X									2
T14	Violation of private property, unauthorized entry			X		X									2
T15	Piracy			X		X									2
	Crimes against people and things														
T16	Malicious or non-compliant personnel, sabotage			X		X				X		X			4
T17	Communications			X		X				X		X			4
T18	Disclosure of information, espionage			X		X				X		X			4
T19	Misinformation			X		X									2
T20	Civil protests and strikes			X		X									2
T21	Illegal transit			X		X									2
T22	Illegal transport			X		X									2
	Crimes referable to manifestations of terrorism and or organized crime aimed at people and thing														
T23	Attack with vehicle used as weapon (WAAW)			X		X									2
T24	Attack with parked vehicle borne improvised explosive device (VBIED)			X		X									2
T25	Attack with encroaching VBIED			X		X									2
T26	Attack with penetrative ram vehicle			X		X									2
T27	Attack with suicide terrorist			X		X									2
T28	Attack with terrorist and/or threatening phone calls			X		X									2
T29	Attack with envelope or letter bomb			X		X									2
T30	CBRNE attack			X		X									2
T31	Ballistic attack, bombing and blasting			X		X				X		X			4
T32	Cyber attack with malware infiltration			X		X				X		X			4
T33	Cyber attack with subtracting data for ransom			X		X				X		X			4
T34	Cyber attack with direct manipulation			X		X				X		X			4
T35	Cyber attack to the management system			X		X				X		X			4
T36	Attack with Unmanned Vehicles (UAV or drone; AUV or UUV)			X		X									2
	Unattended and unforeseeable event or harmful voluntary acts causing terroristic and criminal attacks or disasters														
T37	Pandemic, epidemic, epidemic outbreak														
T38	Natural disasters and climate change														
T39	Blackout			X		X				X		X			4
T40	Disaster propagation from neighboring infrastructures					X									1
T41	Geopolitical crises, armed clashes or combats, revolutions, uprisings					X									1

v-13

Fig. 4.5.7 - Major risks and priority threats for TC 4.4 Tunnels

4.5.4. Risk treatment

In the **risk treatment** phase, it is necessary establish the mitigation strategy and the countermeasures plan for **each 10 major security threats** related to the priority risks (**Fig. 4.5.8**).

ST 12	**Arson**
ST 16	**Malicious or non-compliant personnel**
ST 17	**Communications**
ST 18	**Disclosure of information, espionage**
ST 31	**Ballistic attack, bombing, blasting**
ST 32	**Cyber-attack with malware infiltration**
ST 33	**Cyber-attack with subtracting data for ransom**
ST 34	**Cyber-attack with direct manipulation**
ST 35	**Cyber-attack to the management system**
ST 39	**Blackout**

Figure 4.5.8 – Security threats leading to priority risks in T.C 4.4 Tunnels

In addition to such threats, **other 24 security threats are of particular concern** for possible developments in term of likelihood and consequences (**Fig. 4.5.9**).

ST 02	**Robbery**
ST 03	**Mugging**
ST 04	**Taking hostages**
ST 07	**Stalking**
ST 08	**Corruption**
ST 09	**Theft**
ST 10	**Vandalism**
ST 11	**Graffiti**
ST 13	**Throwing objects to damage**
ST 14	**Violation of private property, unauthorized entry**
ST 15	**Piracy**
ST 19	**Misinformation**
ST 20	**Civil protests and strikes**
ST 21	**Illegal transit**
ST 22	**Illegal transport**
ST 23	**Attack with vehicle used as weapon (WAAW)**
ST 24	**Attack with parked vehicle borne improvised explosive device (VBIED)**
ST 25	**Attack with encroaching VBIED**
ST 26	**Attack with penetrative ram vehicle**

ST 27	**Attack with suicide terrorist**
ST 28	**Attack with terrorist and/or threatening phone calls**
ST 29	**Attack with envelope or letter bomb**
ST 30	**CBRNE attack**
ST 36	**Attack with Unmanned Vehicles (UAV or drone; AUV or UUV)**

Figure 4.5.9 – Other security threats of particular concern for T.C 4.4 Tunnels

Within the framework of a mitigation strategy for all priority threats, **protection, prevention and transfer measures** for tunnels security issues apply as shown in **Figures 17-1,-2,-3** of chapter 3.3. Such measures must be detailed in relation to the specific contexts.

Regarding the measures for protection, the subdivision of **active and passive measures and procedural-organizational measures** also apply.

It must be reminded that **any measure taken individually does not guarantee effectiveness** and a good professional must be capable of combining, mixing and dosing them.

4.5.5. Security recommendations

Some **general recommendations (GR)** for the security of a tunnel are shown in **Fig. 4.5.10**.

GR 1	**Train tunnel system personnel on security matters**
GR 2	**Raise staff awareness on information system security**
GR 3	**Implement access restriction procedures to prevent unauthorized persons or vehicles from accessing tunnel system assets (tunnel, service buildings, external and internal areas, control centre)**
GR 4	**Provide special authorizations for subcontractors and suppliers likely to be involved in the maintenance of tunnel control and traffic control centres**
GR 5	**Provide internal access restrictions to isolate control centre staff from other staff by securing entrances to these locations**
GR 6	**Organize formal powers to act in time in case of a security incident**
GR 7	**Provide standardized procedures for early detection of an incident, for alerting and for mitigating or neutralizing threats**

Figure 4.5.10 – General recommendations for T.C 4.4 Tunnels

Further specific recommendations (SR) related to the priority threats are shown below (**Fig. 4.5.11)**:

- **SR 1 : On fire resistance;**
- **SR 2 : On malicious or non-compliant personnel, sabotage;**
- **SR 3 : On computer systems and office equipment, information/communication and data centre;**
- **SR 4 : On disclosure of information, espionage;**
- **SR 5 : On ballistic attack, bombing, blasting;**
- **SR 6 : On blackout.**

ST 12	**Fire resistance**	**SR 1**
ST 16	**Malicious or non-compliant personnel**	**SR 2**
ST 17	**Communications**	**SR 3**
ST 18	**Disclosure of information, espionage**	**SR 4, SR 2**
ST 31	**Ballistic attack, bombing, blasting**	**SR 5**
ST 32	**Cyber-attack with malware infiltration**	**SR 3**
ST 33	**Cyber-attack with subtracting data for ransom**	**SR 3**
ST 34	**Cyber-attack with direct manipulation**	**SR 3**
ST 35	**Cyber-attack to the management system**	**SR 3**
ST 39	**Blackout**	**SR 6**

Figure 4.5.11 – Most recurring threats and specific recommendations for T.C 4.4 Tunnels

SR 1 - On fire resistance

Some recommendations are:

- Study of **solutions to evacuate and protect people in relation to technological progress**. Regulatory solutions already implemented in the field of safety can be considered a first step also for security. It should be noted that the majority of fires in tunnels are attributable to the failure of a vehicle which catches fire spontaneously and therefore not following an accident with collisions between vehicles or voluntary criminal or terrorist actions. In the safety field, this leads to the need a particular attention to interventions aimed at limiting fire outbreaks on vehicles and particularly on heavy vehicles, limiting the importance (and costs) of large interventions in tunnels;
- the **technological evolution of vehicle propulsion systems** including electric, hybrid, gas or fuel cell (alcohol or hydrogen) could cause safety and security risks in tunnels. To combat these, methods of prevention and mitigation of arson are yet to be explored;
- an area of technological development which is receiving a lot of attention is also that of **automatic fire mitigation water systems**, of the "deluge" or "water-mist" type with atomized water;
- an area of in-depth study concerns **human behavior** both in operation and with reference to the behavior of users in emergencies and crisis situation (see **Appendix 4.1 - Complexity**), aimed at the optimal use of modern communication technologies;
- a particularly significant field is the **management of the evacuation processes in long tunnels** similarly to what occurs during terrorist or criminal attacks in theaters or sports facilities. Evacuations require people to be directed to exits and an active role of the personnel assisting them directly or indirectly. In the road sector, critical issues may emerge such as, for example, the difficulty of communication due to the different languages used for communications with people in the tunnel or the

difficulty of recognizing security personnel (with the use of color jacket for example orange). In the field of safety and security it is necessary to allow instant orientation to guarantee the correct behavior of people and personnel. For this reason, the new forms of technological innovations linked to artificial intelligence can provide interesting developments for the prevention and management of emergencies, the management of masses and also ventilation management methods.

SR 2 - On malicious or non-compliant personnel, sabotage

Some possible recommendations are:

- establish personnel responsibilities and liabilities based on procedures with regular updating and testing sessions,
- establish regular turnovers in key workstations.

SR 3 - On computer systems and office equipment, information/communication and data centre

Some recommendations:

- provide a **self-contained communication and data network** between the tunnel control computers and systems and the traffic control centre, without connection to Internet,
- **limit remote access** to computer systems,
- make sure a remote-control tool for computer workstations is available,
- establish a protocol for the use of USB sticks and other data carriers by personnel,
- **regularly change passwords and usernames** linked to computers and control systems,
- systematically authenticate messages for variable message panels,
- provide anti-malware software and software updates,
- **set security requirements** for the purchase of IT products and services,
- **implement procedures and instructions** for the management and maintenance of computers and control systems,
- do not allow all-time connection of remote maintenance services,
- disable unused ports with the use of switches,
- **regularly monitor the air conditioning** of computer server rooms and provide redundancy,
- **implement ICT measures** to detect anomalies and unauthorized access to communication or control systems,
- implement frequent and complete backups of data and software,
- **properly separate the (optical fibre) network** of the road operator from the (fibre optic) network delegated to serve the territory in the public domain. All interventions on this network must not pose operating problems.

Other suggestions:

- install alarm sensors on the emergency exit doors of a tunnel, taking into account the **two different needs of allowing exit without obstacles and preventing unauthorized access;** there is a need for compatibility of door opening devices for

fire safety purposes (safety) with door locking devices for anti-intrusion purposes (security) due to the danger posed by terrorism;

- Inside a tunnel, knowing that an excess of sensors can cause issues, it is important to **choose an appropriate sensor network** which, to be effective, must be essential in relation to the type and state of the tunnel;
- **fixed call stations in tunnels (SOS columns) are fundamental,** as they allow the unambiguous localization of the caller and the possibility of sending "handsfree" messages in the tunnel directly to the operator of the control center. The SOS columns could be transformed into potential repeaters for wireless networks in tunnels, to ensure the user's contact with the outside via their smartphone or other fixed technological systems on-board;
- **luminous signs in a tunnel** must be included in the design of the electrical system and must be aligned with the ideas of the fire safety designer and the security manager; safety signs are very important in particular for security and should be the subject of specific design - as in the case of a plant - by specialist technicians; it is necessary to determine the type of sign (whether luminous or not), colour, size, orientation (whether it is a flag, hung from the ceiling, on the wall...), material (plastic, aluminium...), reference legislation, presence or absence of writing, language or languages of writing.

With the **implementation of ITS** (such as sensors, cabling, sensitive cameras, wi-fi hot spots...), road infrastructures will be equipped with extremely rapid and efficient information acquisition and transmission support. Looking ahead, the possibility for the user to send emergency communications and the possibility for the RA to send communications to users or to acquire real-time information on the operating status of the tunnel is desirable. With the **technological development of vehicles**, the dialogue between the vehicle and the infrastructure will also increase in tunnels, and in the event of a safety and security emergency, it will allow to immediately and, above all, **automatically send information directly on board to users in transit**, even in the absence of a control centre.

SR 4 - On disclosure of information, espionage

A recommendation:

- Implement multi-level security, combining physical and logical lines of defence (e.g.: physical barriers, surveillance and cameras) for the centres but also for technical rooms.

SR 5 - On ballistic attack, bombing, blasting

Some recommendations:

- a **ballistic attack or bombing** from the outside could destroy the access portals of the tunnel and also very seriously damage the internal parts, the control and SCADA systems. In the case of tunnels of particular strategic importance, in order to avoid such threat, it is necessary to establish outside an adequately controlled security area and equipped with 24-h all-weather video surveillance and alarm systems;
- regarding **blasting threats**, an analysis needs to be carried out taking into account a variety of explosive sizes, location and delivery methods. Furthermore, it is

necessary to assess induced overpressure by blast on external, internal and neighbouring facilities or adjoining structures. A typical study and analysis will identify the damage level of the tunnel lining in the vicinity of the explosion, as well as the consequential damage in the liner in any adjacent tunnel or other subsurface infrastructure located close to the impacted tunnel. Any possible local failure in the tunnel lining and their consequence on the level of service of the facilities must be also identified.

SR 6 - On blackout

It is recommended to have redundant equipment for the supply of energy (electricity, water, fuel, batteries,) and the supply of radio and computer communication networks (copper and optic fibre network) in or nearby the traffic management centres and tunnel control centres. Alternatively, it is necessary to at least have systems and equipment that enable to operate the tunnel after an interruption of the energy or communication system, long enough to avoid an immediate closure. Particular attention must be paid to the vulnerability of electrical substations.

5. CONCLUSIONS

- **The purpose of security risk management** is to create and protect the value of an organization, an asset, and in particular of a road administration. It strengthens performance, stimulates innovation and supports the achievement of corporate objectives.
- In an objective way, **security measures** consist in the reduction of threats towards values considered important or even essential, and, from a subjective standpoint, the elimination of fear of possible attacks to those fundamental values.
- We all know that the **world has never been a peaceful place and most likely will never be.**
- The **new millennium** started with the apocalyptic event of September 11, **2001** followed by the economic crisis of **2008**, the Fukushima nuclear disaster in **2011**, the Islamist terrorist attacks of **2015**, and the first global pandemic in **2020**. All these without even mentioning **climate change** which - despite becoming relevant only a few decades ago - poses an exponentially growing threat on the future of humanity.
- There are actually over sixty ongoing armed conflicts in the world and in particular two wars which could destabilize the world: since **2022**, the war in the heart of Europe between Ukraine and Russia, and recently, starting from October **2023**, the war in Israel and Gaza.
- All these events and the threat of terrorist and cyber-attacks in democratic countries, including the potential effects of the incorrect use of artificial intelligence, have **direct or indirect effects** on our lives and on the business continuity of our organizations and companies including Road Administrations (RA).
- The current situation is fuelling **collective insecurity**.
- One of the effects of this is the **all-round expansion of surveillance and prevention**. In cities, in particular, increasing surveillance raises the question of whether it is really worth to forego privacy and individual freedom to increase security.
- It seems that even more security can actually lead to even more insecurity, according to a **perverse mechanism**. Risk aversion creates new threats: more and more surveillance, more and more technology, more and more cyber threats. This field is defined by a continuous attack - response cycle.
- Security project can disrupt due to its internal contradictions because those who seek excessive security are destined to a never-ending feeling of danger and security can become **a sort of trap**.
- Given all these factors, **the absence of threats is to be considered an anomaly but also the excess of security**. Therefore, **it is necessary to work with the purpose of transforming threats into risks**, pondering on the latter as a result of the threat management action.
- The **process of risk management,** as proposed in the international standards, is a basis that provides an excellent starting point for assessing risks arising from insecurity and helps us in the critical evaluation of priorities in the security domain.
- We should not assume that **simply applying the proposed process or any other will in itself lead to wonderful results**. The security manager or professional, together with the

stakeholder of a company or an asset, must possess a **sense of awareness, intuition and imagination** of their security risks in the internal and external contexts in which they operate.

- The world is a **complex system** made up of parts that mutually interact with each other so that it no longer makes sense to study an event on its own, overlooking interactions it may have with other events according to a systemic vision.
- In some cases, the **complexity of the threats and the consequent events** make very complicated and sometimes impossible to apply a risk assessment methodology.
- In these cases, it is possible to address complexity by **integrating security management processes with resilient approaches**.
- The approach aimed at developing resilience must be oriented towards **planning the ability to react in relation to every possible event and not individual causes** (who or what caused it), overcoming the classic linear schemes such as arborescence of harmful events and the related responses.
- However, **it is hard to imagine a world where resilience is applied everywhere**: to tunnels, roads, control centres, asset management, staff and road users…etc. The limit of the resilient approach is that it does not know reality, but tends to incorporate all possible consequences. It therefore does not deal with the new, possible threats, because it tends to encompass all possible consequences, and the resulting costs would be impracticable.
- Since **resilience engineering does not conflict with risk management process** it can complement it by integrating resilience into risk management through the improvement processes envisaged by the ISO standards.
- The **COVID-19 pandemic**, in the form of an unintentional and unpredictable threat, was an extraordinary lesson learned in managing security events for the application of the concepts related to resilience: prepare, prevent, protect, respond, recover.
- In particular, it has questioned the **operational management of roads and/or transport agencies or administrations** in order to ensure the performance of activities in a critical context. The emergency has highlighted the importance of the ability of RAs to deal with complex situations which require a multidisciplinary approach.
- New challenges for the world and also for RAs come from dealing with cyber security that has increased drastically following the pandemic and following a shift of current wars from the field to a **hybrid warfare**.
- The strong increase in cyber-attacks in recent times underlines the decisive importance of a security-oriented corporate approach to integrated organizational processes, protocols and resources in order to react to **complex cyber incidents**.
- **Biological and cyber viruses** have a lot in common and a cybernetic pandemic scenario must be taken into consideration for the future. Cyber viruses must be taken seriously as they have the potential to cause disruption at the most inappropriate time.
- **Security managers and departments of corporate protection of an organization** are of primary importance for the application of the process of risk assessment and the concepts related to resilience.

In summary:

- **We need to establish a distinction between the things that depend on us from those that do not.**
- **The security "game" is played with the things that depend on us, avoiding wrong thoughts.**

Some of these wrong thoughts are:

- thinking about security in an egocentric and self-referential way,
- depending on common or other people's opinions,
- seeking dominance, power, visibility, personal ambition,
- being limited to a "reactive" approach.

Some **right thoughts are instead**:

- thinking about security in an open and interactive way,
- cultivating one's thoughts in a free and conscious way,
- governing the mind by learning to improve our security-minded approach,
- moving to a "proactive" approach, involving the whole organization: each component must be an active, accountable, responsible and aware part of the security process.

Let's spread a correct security culture!

Remove barriers that hinder collaboration and communication between team members as well as reduce efficiency and obstruct the flow of information (no "silo" approach).

Be independent, always review carefully, perceive future problems, trends or changes in advance, in order to plan for appropriate security measures in time.

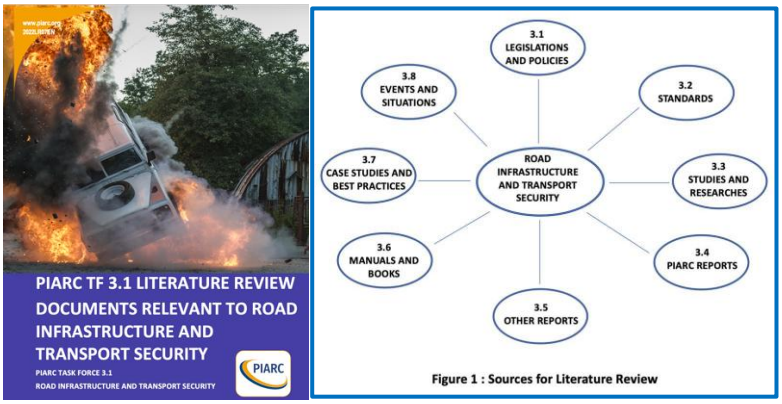
The lesson is:

DO NOT WAIT FOR IT TO HAPPEN.

DO IT NOW!

6. APPENDICES

APPENDIX 1 - SYNTHESIS OF LITERATURE REVIEW REPORT



PIARC TF 3.1 – Literature Review – Documents Relevant to Road Infrastructure and Transport Security", 2022R07EN, ISBN 978-2-84060-682-6.

The Literature Review (LR) is the preparatory work of TF 3.1 Road Infrastructure and Transport Security for the accomplishment of its final Report, according to the provisions of the Term of References (ToR) of the Task Force (TF) 3.1 "Road Infrastructure and Transport Security", as included in the PIARC Strategic Plan 2020-2023[158]. The work of TF 3.1 is the continuation of the last cycle 2016-2019 in which PIARC TF C .1 focused on security of road infrastructure, publishing its final Report[159]. Meanwhile, the awareness for physical and cyber security issues in logistics chains, personal and public transport and vulnerable infrastructure in general has grown. In its Strategic Plan 2020-2023, PIARC decided to broaden the security view in the infrastructure component and in transport and mobility. Later, the pandemic Covid-19 that has flared up in last years has reinforced this need. The TF 3.1 has carried out the task to collect literature sources dealing with road infrastructure and transport security in 8 source groups: legislations and policies, standards, studies and researches, PIARC reports, other reports, manuals and books, case studies and best practices, events and situations. Among all, the international standards and in particular the ISO standard families have been taken into consideration.

The scope of this LR is to collect the documents useful to provide recommendations on security matters within the mentioned PIARC Strategic Plan 2020-23, based on the 4 Strategic Themes, the 17 TCs and the 4 TFs included the Terminology Committee. TCs and TFs were selected in relation to the possible impact of security on them, both physical and cyber, for a total initially of 15 in all.

The LR also contains the synthesis of a survey about vandalism ("Fight against vandalism"-appendix 1).

In the Strategic Theme 1 "Road Administration", it was considered that security issues have an impact on the performance of transport administrations in all stages of infrastructure planning, design, building, operating and maintaining. Climate change poses urgently new challenges in terms of security linked to environmental disasters that can destabilize the social and economic

[158] PIARC – The World Road Association, "Strategic Plan 2020-2023", Update October 2020, http://www.piarc.org
[159] "Security of Road Infrastructure", Final report of the Task Force C.1., PIARC 2019, Paris, France. ISBN: 978-2-84060-524-9. Available in English, French and Spanish.
https://www.piarc.org/en/order-library/30826-en-Security%20of%20Road%20Infrastructure

life of an area and create serious problems in a population. Therefore, in Strategic Theme 1 the following TCs were selected:

- TC 1.1 Performance of Transport Administrations;
- TC 1.4 Climate Change and Resilience of Road Network;
- TC 1.5 Disaster Management.

In the Strategic Theme 2 "Mobility", it was considered that security has an impact on the transport services and the infrastructure included in the urban mobility and the rural areas are also threatened: this is mainly because, being larger territories, they are subject to fewer controls.

Since secure and reliable transport of people and goods are essential for a healthy economy and a safe social life, it is quite obvious to protect these activities from critical conditions caused by security risks that can destabilize a civil society. Transport security covers also physical and cyber security in every logistic chain. For the security of service, the physical security of all personnel involved within transport and logistic operations becomes vital. In relation to new technological developments, a particular attention must be paid to security considerations in the domain of automated vehicles, smart roads and ITS applied to road network operation. Therefore, in Strategic Theme 2 the following TCs and TF were selected:

- TC 2.1 Mobility in Urban Areas;
- TC 2.2 Accessibility and Mobility in Rural Areas;
- TC 2.3 Freight;
- TC 2.4 Road Network Operation/ITS;
- TF 2.1 New Mobility and its Impact on Road Infrastructure and Transport.

In the Strategic Theme 3 "Safety and Sustainability", it is well known that safety and security[160] are strongly linked in relation to road issues and both contribute to the resilience of a system and of an organization. This involves a vision to the overall aspect of asset management and the overall resilience of a road network. Therefore, in Strategic Theme 3 the following TCs were selected:

- TC 3.1 Road Safety;
- TC 3.3 Asset Management.

In the Strategic Theme 4 "Resilient Infrastructure", it was considered that historically bridges and tunnels, due to their relevance as nodes of transport networks and also for their visual impact, are the main infrastructure exposed to attacks and sabotage. Therefore, in Strategic Theme 4 the following TCs were selected:

- TC 4.2 Bridges;
- TC 4.4 Tunnels.

In consideration of the various application fields, this has led to semantic problems. In the LR there are a many references and definitions concerning the term of security[161] (and also safety) in the ISO glossary and also other terms. The terminological aspects are therefore very relevant

[160] See chapter 2.2 "Safety vs. Security" in "Security of Road Infrastructure", Final Report of Task Force C.1., PIARC 2019.
[161] In "Security of Road Infrastructure", Final report of the Task Force C.1., PIARC 2019, security was defined as the state of relative freedom from threat or harm caused by intentional, unwanted, hostile or malicious acts, including sabotage and espionage. But, as highlighted in the present Literature Review, many other expressions are available.

because they contribute to spreading a very specialized vocabulary, sometimes new and unknown. Therefore, the Terminology Committee was selected to provide its contribution in the field of security. Finally, it was recognized that other TCs and TFs could also benefit from TF 3.1 work. Consequently, three other TC and TFs were considered eligible to receive a contribution in terms of security:

- T.C 1.3 Finance and Procurement;
- TF 1.1 Well-Prepared Project;
- TF 4.1 Road Design Standards.

APPENDIX 2 - CHECKLIST IMPLEMENTING ISO 28000:2017[162]

1. PLAN – Security management policy and planning

PLAN phase corresponds answering the following questions:

1. Corporate management endorse and therefore support the security management policy?
2. Is the company policy based on a credible assessment of the security risks in relation to the overall activities?
3. Does the security management policy enable specification of security objectives, performance measures and mitigation requirements?
4. Does the security management policy take regulatory, legal and statutory requirements into account?
5. Is security management policy regularly maintained and updated in conjunction with corporate management?
6. Are security objectives and targets communicated and understood throughout the organization and applicable third parties, suppliers, etc.?
7. Is there established process for ongoing security risk identification, assessment and management?
8. Do security risk assessments include physical, cyber, and personnel domains?
9. Do security risk assessments include issues related to assets, technology, people, processes and environment?
10. Do the outputs from security risk assessments inform the design, management, and control of operational security processes?
11. Are security management plans for achieving objectives and targets implemented and maintained?
12. Have all the security processes and procedures defined in the management plan been clearly defined in terms of performance measures?
13. Are the security performance measures specific, measurable, achievable and relevant?

2. DO – Implementation and operation

DO phase corresponds to answering to the following questions:

14. Is corporate management formally accountable for the design, maintenance, documentation and improvement of the organization's security management system?
15. Is the security management system reviewed and updated in relation to any significant organization change?
16. Are changes to the organization documented and reflected as part of the security risk assessment process?
17. Does corporate management provide adequate financial resources to support the security management plan of the organization?
18. Are roles and responsibilities defined in relation to security management throughout the organization?

[162] Ri-elaboration from the document “Protective Security Management Systems (PSeMS) - Guidance, Checklist, and Case Studies, CPNI, 2018.

19. Are organization operations necessary for achieving the security policy, objectives and plans, identified and controlled?
20. Is a documentation system established and maintained that includes the security policy, target, risk management data, plans, procedures and performance records?
21. Are plans and procedures established and maintained for detailing the responses and mitigations for security incidents and emergencies?
22. Are controls in place to ensure facilities, equipment, and are supporting services effective in achieving the security objectives?
23. Is the security policy communicated to all the staff, third parties, and suppliers?
24. Does corporate management regularly communicate the importance of meeting security management requirements related to all relevant stakeholders?
25. Are security matters communicated regularly with effective corporate management and staff involvement?
26. Is security awareness training provided to all staff, relevant third parties, and suppliers?
27. Are specific security training requirements assessed in accordance with security roles and responsibilities?
28. Does security training provide all relevant personnel with the necessary operation skills, knowledge, and abilities?
29. Are exercises and training for emergency preparedness completed regularly?

3. CHECK – Checking and corrective action

CHECK phase corresponds to answering to the following questions:

30. Are procedures to monitor and measure organizational security performance established and maintained?
31. Are procedures to monitor and measure the performance of the security management system established and maintained?
32. Is the frequency from measuring and monitoring the performance measures proportional to security risks and threats?
33. Is performance monitoring and measurement to facilitate subsequent corrective and preventive action analysis?
34. Is security data traceable, retrievable and accessible?
35. Are there controls in place to ensure the quality of the performance data is assured?

4. ACT – Management Review and Continual Improvement

The organization reviews its performance enabling corporate management to take decisions to continually improve the performance of the security management system in response to lessons learned and data collected, with respect to both specific areas and the overall cycle.

ACT phase corresponds to answering to the following questions:

36. Is there an established plan to help ensure the security management system is efficient and effective?
37. Are security related failures, non-conformances, incidents and audit findings reviewed in a timely fashion?
38. Are security and corporate risk registers reviewed and updated following security-related failures, non-conformances, incidents and audit findings?

39. Are proposed corrective and preventive actions assessed and implemented in a timely manner?

APPENDIX 3 - ROAD SAFETY AND SECURITY IN DEVELOPING COUNTRIES AND PREVENTION MEASURES AGAINST TERRORIST ATTACKS DIRECTED AT CROWDS.

ROAD SAFETY AND SECURITY IN LOW-INCOME COUNTRIES

The issue of road safety and security in some low-income countries is an issue of big concern. It is the cause of several losses of human life. Today, it finds its source at various levels which are, in particular:

- the absence of signage of potential dangers on the roads (heavily eroded roads in the work areas) resulting from a lack of road maintenance; to this must be added the absence of reporting when broken down vehicles are on the road;
- the proliferation of acts of robbery with often armed individuals blocking the roads to strip users of all their belongings in slowdown areas due to the poor state of the road. These brigands are commonly called "road cutters";
- the terrorist acts, with mass attacks on the public motivated by personal or ideological or religious reasons, possibly with the placing of explosive devices in crevices or potholes or assaults with all kinds of firearms and non-firearms causing several deaths [163].

In several capital cities, the safety of roads is put to the test with the **theft of manhole covers** often located in the middle of the road. The gaping opening left by the theft of these buffers is a real danger for road users. This danger is more real for pedestrians in the rainy season, when the roads are flooded due to the climatic changes observed in recent times. To react to the theft of cast iron manhole covers, consideration should be given, in addition to the penalties that may be imposed on the culprits, to the possibility of using buffer solutions with other less popular materials. This is the case of fibreglass or any other material that may help to protect users, especially children who can more easily fall and die there. It is important for RAs in these countries to be more inventive in finding the best answers to this question. It will be a question of finding signalling equipment adapted to the different contexts and warning users of the danger.

Regarding the **installation of explosive devices in crevices or potholes**, the best response is to undertake maintenance work on time. RAs authorities are trying to find solutions for quick and durable pothole repairs for paved roads. To this end, resorting to cold mixes seem to be a good solution.

For **banditry on the roads**, a regular deployment of law enforcement is an essential solution. However, it seems necessary to adopt a participatory approach, favouring collaboration with the localities closest to the areas concerned (camp, village, sub-prefecture, etc.).

Support from community leaders coupled with law enforcement proximity to populations through increased population sharing can help anticipate threats. The resolution of these safety and security problems requires more responsible governance of the road sector and greater synergy of actions between the various stakeholders (Ministries in charge of roads, Ministry in charge of transport, Ministry of Security, Ministry of interior or territorial administration).

[163] See for example in the Sahel region, Burkina Faso during the year 2022, but also in Europe in 2015 and following years.

PREVENTION MEASURES AGAINST TERRORIST ATTACKS DIRECTED AT CROWDS

To take actions that can help prevent, defend and respond to mass attacks on the public, five points can be highlighted [164]:

1. Proactively prevent mass attacks.

Reporting by the public helped block nearly two-thirds of the attacks. Warning signs should be identified early:

I. Reason:

- inspiration from previous attacks;
- desire to satisfy an extremist cause as a reaction to a situation, an event, a perceived threat.

II. Preparation by the criminal/terrorist:

- write a plan or improvise;
- look for information on how to maximize the impact of the attack and explore websites;
- communicate to coordinate with other violent extremists including to recruit others;
- search for weapons, ammunition and equipment;
- travel frequently (for training or targeting).

2. Local communities need multidisciplinary teams to follow and evaluate warning signs and determine what to do after the attack.

In particular:

- the organization of a public event requires the figure of a responsible for security (security manager) for the organization of the event (for example the identification of control points that can guarantee an appropriate and dynamic examination of the situation);
- threat assessment is not just about the possibility of an attack, it also requires determining the next steps to take to deal with the subject and to direct the necessary follow-up.

3. Adequate preparation reduces casualties in the critical initial stages of an attack, before responders arrive on the scene.

From the point of view of site security management, it is necessary to:

- prevent shooters from surprising crowds at close range and block escape routes;
- create buffer zones (in the surrounding area);
- facilitate crowd rapid movement away from shooters (to emergency exits or known protected rooms);

[164] The National Institute of Justice (USA) has developed the Mass Attacks Defence Toolkit 2 (https://www.rand.org/pubs/tools/TLA1613-1.html), an online IT tool with strategies and indications that allows you to frame the risk of terrorist attacks directed at groups of people, also offering indications on possible mitigation and control strategies. It drew on more than 600 mass attack scenarios, hundreds of articles and resources, and dozens of expert interviews.

- place physical barriers (walls, locked doors, secure windows) between shooters and crowds

From the training of the potential victims, it is recommended to be prepared to adopt the strategy of “run, hide and confront” the criminal:

- be prepared to run if you can safely escape the scene;
- it may be safer to hide in a safe place, rather than try to escape safely from the scene;
- confront the criminal only when you cannot escape or hide; use distraction tools (e.g. throwing shattering bottles), use anything that can serve as a weapon and move at an angle to the shooter.

4. An effective joint response to a mass attack requires planning and training, which must include all those who will be involved in response and counter-attack strategies.

In particular:

- effective responses to attacks include coordination among law enforcement, fire, and emergency medical services, as well as hospitals, victim support providers, site security officers, and site personnel. For this to happen, managers must provide adequate support and guidance for planning and training;
- the Mass Attacks Defense Toolkit also provides skills and resources to assist all responders with planning and training. For example, it is essential that all operators involved are aware of the command and communications techniques to be adopted during an attack;
- planning and training must cover communications – including common radio frequencies – as well as strong radio discipline, to avoid overloading communications channels. They must also include traffic management and control, to ensure that vehicles and personnel do not clog the scene and impede others involved in the response (for example, leaving no room for ambulances).

5. The recovery plan must include planning and training for recovery activities.

Actions immediately following the attack include identifying and arresting the attackers (where applicable), investigating the attackers and potential conspirators, and providing mental health and emotional support procedures, such as creation of family assistance centres and provision of assistance to victims.

In particular:

- short-term actions include mental health and emotional support for victims, survivors and workers, together with debriefing sessions to record and analyse critical information regarding responses and review resources available to victims;
- long-term actions for first responders include providing ongoing emotional and mental health support to survivors and caregivers, monitoring the recovery process of victims, and engaging in recognition of worthy behaviours, such as rewards for acts of valour, ceremonies for victims and heroes, commemorations and commemorative events and after-action reports.

APPENDIX 4 - PAPERS PRESENTED AT T.F. 3.1 TECHNICAL SESSION AT THE 27TH WORLD ROAD CONGRESS IN PRAGUE ON OCTOBER 6TH, 2023

APPENDIX 4.1 - COMPLEXITY

THE DIFFICULTIES OF RISK ASSESSMENTS FOR COMPLEX NETWORK INFRASTRUCTURE: APPLICATIONS TO THE SECURITY AND THE RESILIENCE OF ROAD INFRASTRUCTURE

Authors: **Saverio PALCHETTI**[165] and **Antonio SCALA**[166]

1. SECURITY, COMPLEXITY AND ISO STANDARDS

The international standard **ISO 22300**[167] defines complexity as "the condition of an organizational system with many diverse and autonomous but interrelated and interdependent components or parts where those parts interact with each other and with external elements in multiple and non-linear ways". Some basic concepts of complexity are:

- **complexity is an intrinsic property** of an organization or asset or of a system in general which is determined as they are enriched with processes, technologies, organizational structures, personnel, often with the aim of improving performance;
- an organization or an asset is a **complex system** because made up of many interrelated and interdependent parts that interact with each other and with the outside world, and these parts cannot than to be seen in their complexity[168] [169]; any simplification or reduction of complexity can become a risk factor in itself, often overlooked, when dealing with the issue of risk management, especially in the security domain;
- the complexity of a system[170] is determined by external and internal factors, both related to security[171]; among the **internal complexity factors** can be considered technological innovations, the application of new regulations and also any decision concerning the management of the organization; the **external complexity factors** are linked to the threats and risks that may loom over an organization or an asset, i.e. to the actions taken intentionally that give rise to violence, attacks, robberies, terrorist acts, intimidation, mobbing, fake, and more, also affecting the world of the web;
- a complex system **responding to critical security situations** reacts by increasing its functional and structural complexity and, at the time of the critical event, the intrinsic complexity of the organization or asset combines with the complexity determined by the incident itself; the outcome of the response can take on the dimension of a **multifactorial event**, triggering ripple-like effects (one after the other) or cascade effects (repercussions in various directions) [172]. They are the so-called systemic risks, because they involve the interdependencies between systems or subsystems and networks [173], in which, in a critical

---

[165] S. Palchetti, PhD, Senior Security Manager, Chair PIARC TF 3.1 "Road Infrastructure and Transport Security", Italy.
[166] A. Scala, PhD, Senior Researcher, Institute for Complex Systems (ISC), CNR and Department of Physics, "La Sapienza", Rome, Italy.
[167] ISO 22300, Security and Resilience – Vocabulary.
[168] A. Gandolfi, Formicai, imperi, cervelli - Introduzione alla scienza della complessità (Anthills, empires, brains - Introduction to the science of complexity), Bollati Boringhieri, 1999, pag. 231.
[169] G. Parisi, Nobel Prize for Physics 2021, in his book "In un volo di storni. Le meraviglie dei sistemi complessi (In a flight of starlings. The wonders of complex systems), Rizzoli, 2021, provides an important contribution on the theme of complexity.
[170] General definition of a system: "Sets of elements standing in interaction" in L. von Bertalanffy, Teoria generale dei sistemi (General System theory: Foundations, Development, Applications), ILI, Milano, 1971 1968.
171 See Fig. 9 in chapter 3.2.2 of this Report.
[172] S. Pahwa, C. Scoglio, A. Scala, Abruptness of cascade failures in power grids, Scientific reports, 2014.
[173] G. Caldarelli, Without equal. Understanding with networks a world that has no precedent, Egea, 2022.

condition, the overall effect on the components of the system can be greater than the sum of the effects on the components taken individually.

Studying the security risks as in the purposes of the Task Force 3.1 in the various issues of the road world from climate change, to the resilience of networks, to infrastructural issues[174] including tunnels, **aspects of internal and external complexity** have emerged that need to be taken into account[175] which essentially refer to functions, structures, personnel and technologies. Some issues such as urban mobility have characteristics of complexity that make them similar to ecosystems or even living organisms [7]. **Traditional risk management** tools and techniques can be in some cases inadequate and risk analysis cannot can't be limited to **linear cause-effect thinking (Fig. 1 and 2)**. Therefore, the international standards **ISO 31000 and ISO 28000** specialized in security risk assessment, are based on the Deming Cycle Continuous Improvement method or DCPA and the defence measures must be verified and cyclically rethought [176]. In complex contexts, continuous control and corrective actions, protection and resilience measures must therefore be continuously monitored both according to the linear cause-effect-defence measure scheme and according to resilience analyses.

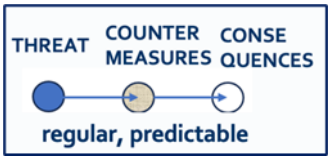


Fig. 1 - Linear cause-effect thinking

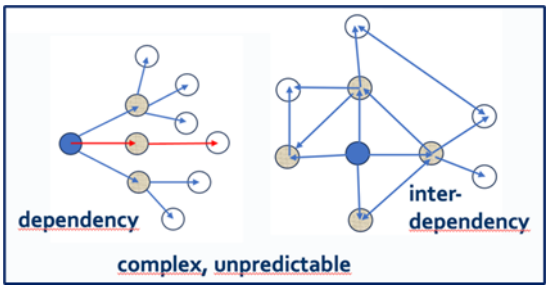


Fig. 2 – Non-linear cause-effect thinking

2. THE FOUR DIMENSIONS OF A COMPLEX SYSTEM

Examples of complex systems in nature are the human mind, ecosystems and the earth system as a whole, living organisms, financial markets, social and economic systems. These complex systems are capable of generating crisis situations from which conflicts and security problems arise. **Infrastructure and transport networks** have characteristics of complexity that affect their security, due to the many components (both physical and human) that can interact differently in space and time with non-linear dynamics. For such networks, aspects of complexity are also present in sub-components such as road networks, underground road sections and tunnels. Furthermore, the infrastructure and transport networks intersect with the **water, gas, electricity and telecommunications supply networks**, therefore, today's reality consists of a system of interdependent critical infrastructures, endowed with their own internal complexity, whose failures can propagate from one infrastructure to another with unpredictable domino effects[177].

In particular, **Road tunnels** have their own complexity from the point of view of both safety and security, as made up of technical components (structure, systems, personnel, traffic passing through them) but it is also a system in which the various parts can interact in various ways. In

[174] See the Ref. in note 9.
[175] See chapter 4.13 in this Report.
[176] See in this Report Fig.3 on PDCA cycle in chapter 2 "Security Risk Management" and in chapter 3 "The process of Security Risk Management".
[177] G. D'Agostino, A.Scala, Networks of networks: the last frontier of complexity, Vol. 340. Berlin: Springer, 2014.

general, **in the normal operation**, all the parts act individually according to the criteria with which they were designed and built, i.e., separately and in a pre-established order. **In a crisis situation**, disorder and complexity can arise. This can occur in particular in the face of the **non-linear dynamics of a fire, of people fleeing, of a terrorist action**. It is not possible to fully predict the behaviours of people inside a tunnel during a fire. It is determined by internal and external factors and sometimes by chance. It is constantly evolving and you can create the so-called **"group dynamics"**, which is influenceable but not predictable [178]. If a fire in a tunnel destroys the power lines and other systems that pass through it, it can cause structural failures, generate polluting and toxic fumes which can spread outside from the aeration shafts with also consequences on the natural or urban environment.

The definition of complexity provided by **ISO 22300** can be seen providing **four dimensions of complexity** in the organizational field [179] [180] **(Fig. 3)**:

- **variety** (or diversity): the number, diversity and heterogeneity of the elements (subsystems) constituting the system and the context with which it relates;
- **variability** (or dynamism): rate of change of the co-evolution between the system and its context;
- **interdependence**: level of interaction, the elements/subsystems of the system are strongly interconnected and interacting with each other and with the environment with which they relate so, on the one hand, they maintain a certain autonomy of behaviour but are connected to each other and influence each other;
- **uncertainty** (or indeterminacy): degree of unpredictability and ambiguity of the system also due to the presence of non-linear relationships for which individual knowledge of each of the subsystems is not sufficient to establish the overall evolution of the system over time.

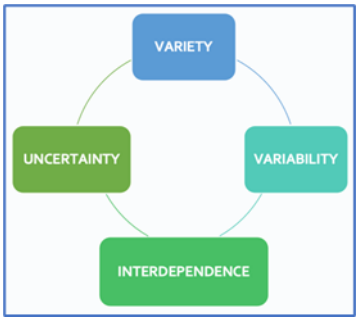


Fig. 3 – The four dimensions of complexity

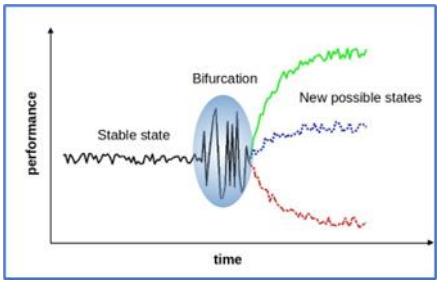


Fig. 4 - Phases of a catastrophic bifurcation system [181]

3. THE CATASTROPHIC BIFURCATION IN THE BEHAVIOR OF A COMPLEX SYSTEM

The behaviour of a complex system is defined as **"emergent" behaviour** [182] because it exhibits properties that are difficult to predict on the basis of the laws that govern its components taken

[178] See the Ref. in note 4 at pag. 236.
[179] Reworking of "Complessità e Management - Intervista con il prof. Alberto Felice De Toni" di Enrico Laurenti, Luglio, 2021 (Complexity and Management – Interview with prof. Alberto Felice De Toni di Enrico Laurenti, July, 2021).
[180] See the Ref. in note 4 at pagg. 97-98.
[181] Personally elaborated by Prof. Antonio Scala.
[182] It can be simulated with computational models, see the Ref. in note 15.

individually, deriving from the interactions between the components themselves. This behaviour **(Fig. 4)** generally consists of a stability phase, during which the perturbations have been neutralized and the system remains stable. This phase can also consist of discontinuous and unpredictable behaviour, even in the face of continuous input. If, on the other hand, the system is subjected to too strong an external perturbation or has its own spontaneous evolution, a phase of instability can be determined, called **"catastrophic bifurcation"** in which the system enters an unstable state from which it emerges modified.

The catastrophic bifurcation has no particular negative or positive meaning. In other words, a fork can lead the system to higher levels of organization and effectiveness. A crisis can give rise to a more complex and more efficient system in the management of energy, material and information flows or it could, on the contrary, drag the system towards a situation of chaos and degradation and therefore towards lower organizational levels [183]. In this sense, the catastrophic bifurcation can correspond to the **resilience threshold** of a complex system. Once this has been overcome, one can return to a new stable phase which can be more or less complex than the previous one. This can give rise to new emergent behavior and so on.

Criminal or terrorist actions can bring a complex system close to the critical threshold **of bifurcation** [184], resulting in an unstable system condition. If not absorbed by the resilience of the system, they are capable of triggering the aforementioned critical unstable situation which tends to a new equilibrium, which if worse (which often happens if the external action is harmful) leads to a state of less complexity, i.e., less people (more dead), less infrastructure and equipment (destruction and damage).

4. SOFTWARE COMPLEXITY AND SECURITY

Cybercrime is becoming even more profitable in the monetary aspects; therefore, cybercriminals are looking for new opportunity for their attacks and the growing number of threats in these last years show that there is a specific vulnerability in the informatic area. The international standard ISO 22375 on software complexity declares that the greater the complexity of a software system, the greater the chances of security holes.

The incessant implementation of an increasing number of **new technology services and products** on the market can lead to an increase in the number of vulnerabilities. Cloud computing, social media, mobile devices, the Internet of Things (IoT), mobile applications, integration, interconnectivity and platform compatibility[185] have created many opportunities for cyber criminality. Some producers are also involved in vulnerability leaving deliberately backdoors in hardware and software for different purposes such as malicious intentions, surveillance programs or covert commercial agendas.

---

[183] See the Ref. in note 4 at pagg. 213-215

[184] The critical threshold for a complex system marks the switch between qualitatively and quantitatively different ways of operating of the systems. As an example, the critical stress for a bridge marks the point at which the bridge collapses, i.e., goes from an operative to a non-operative state. In this case, the critical threshold marks an irreversible switch, i.e., relieving the stress does not make a collapsed bridge functional. In other cases, like traffic jams, if the density of cars goes below the critical threshold the jam is resolved; in such a case we speak of reversible transitions.

[185] C. K. Chang and R. C. Chang, "An Overview of Vulnerability Analysis in the Field of Cybersecurity," Journal of Information Security, vol. 10, no. 5, pp. 279-291, Sep. 2019. This paper discusses the various reasons for the continuous increase in the number of disclosed vulnerabilities, including the rapid pace of technological innovation and the increasing complexity of software products. The authors also discuss various approaches to vulnerability analysis and provide an overview of the current state of the field of cybersecurity.

5. RESILIENCE, SECURITY AND COMPLEXITY

The approach that develops resilience[186] must be **oriented towards planning the ability to react in relation to every possible event (e.g., fire) and not on individual causes** (who or what caused it), overcoming the classic linear schemes such as arborescence of harmful events and the related responses. This allows to face uncertainties, surprises, and significantly the risks due to complexity. Resilience consists of the four properties shown in the following **Fig. 5**.

Rapidity: the ability to satisfy priorities and achieve objectives in a timely manner in order to contain losses and avoid future disruptions (e.g., speed of recovery of business as usual).	 Fig. 5 – The properties of resilience	**Robustness:** the ability to withstand a given level of stress without undergoing degradation or loss of function (e.g., number of employees).
Resourcefulness: the ability to identify problems, set priorities and mobilize resources when conditions exist that threaten to destroy some elements, systems or other units (e.g., organizational capacity and self-organization).		**Redundancy:** the extent to which the elements or systems are replaceable, i.e., capable of satisfying the functional requirements in the event of interruption, degradation or loss of functionality (e.g. number of IT hubs).

A fundamental assumption is that is not possible to imagine security made up of a world of resilient buildings, resilient bridges, resilient tunnels, resilient asset management and resilient staff and users…etc. The limit of the resilient approach is that it does not know reality, but tends to incorporate all possible consequences. It therefore does not deal with a possible threat, because it tends to encompass them all. Since **resilience engineering does not conflict with classic risk management,** it can complement it. The **dimension of resilience can be integrated into risk management** through the improvement processes envisaged by the ISO standards [187] [188]. **In a complex context, resilience allows to be prepared** beyond the actuality and the predictable [189]. In cases such as preparing for climate change, dealing with a new disease or a terrorist attack in a new way, traditional statistical methods and techniques are not suitable, as they cannot be modelled and relevant data are missing. **In the face of complexity, the answer is therefore in improvement processes together with resilient approaches**.

Self-organization, that is the ability of people to self-organize, is the organization that emerges in the absence of a plan, which is of particular importance in situations where, to deal with the unpredictability of cases, it is necessary to rely on the organizational qualities of the operators.

---

[186] Resilience can be defined as the ability of a subject - e.g., asset, organization, community, region - to anticipate, resist, absorb, respond, adapt and recover from a disruptive action (see chapter 6 in PIARC TC C.1 “Security of Road Infrastructure,” 2019R12EN)

[187] F. Flammini, R. Setola, and F. Lollini, "Resilience Engineering and Risk Management," in Resilience Assessment and Evaluation of Computing Systems, Springer, 2012, pp. 35-52. This paper discusses the relationship between resilience engineering and classic risk management, noting that they are complementary and can be integrated through the improvement processes outlined by ISO standards. The authors argue that resilience engineering emphasizes the importance of understanding how complex systems respond to unexpected events and disturbances, and that it can help organizations to improve their risk management processes by incorporating this understanding into their risk assessments. The paper provides an overview of the key principles and practices of resilience engineering and their implications for risk management in the context of complex systems such as road infrastructure.

[188] Yu, David J., et al. "Toward general principles for resilience engineering." Risk Analysis 40.8 (2020): 1509-1537. This paper states that in the search for tools and methodologies for risk analysis of complex systems, resilience engineering must be considered to manage complexity.

[189] Park, Jeryang, et al. "Integrating risk and resilience approaches to catastrophe management in engineering systems." Risk analysis 33.3 (2013): 356-367. This paper tells that in risk analysis of complex systems, resilience engineering must be taken into consideration especially when considering catastrophic events.

Self-organization does not mean lack of rules or procedures since the behaviour of the actors is not completely free, but is subject to constraints. The control is delegated in a widespread way while the centre takes care of the development, passing from a "planning and control" role to a one of "creation and protection of the context" from a role of "controller" to one of "builder". The organization must become “a team of teams”. The management of complex systems is "of many minds" while the traditional one is "of a few minds", only those of the top, with a leadership that therefore simply controls. To manage a situation of increasing complexity, it is necessary to focus on everyone's participation and assumption of responsibility.

This applies to the case of **tunnels**, which have a model in normal conditions and a model which only in a critical phase (e.g., fire) becomes a complex system. In a tunnel, hierarchy and self-organization in terms of security can coexist. Models of self-organization and leadership styles of "construction and supervision of the context" and self-leader behaviours occur in highly complex contexts, as happens in a tunnel in a critical phase, and with people who show a high aptitude for responsibility and decisions. **The tunnel complex system is a dynamic system,** which evolves over time and the most suitable scheme for **governing security in tunnels** is "action-learning-adaptation"[190].

The **glider analogy** can be used to explain this approach [191]. To fly with a glider, you need to rely on the currents and the pilot's ability to exploit them adequately, but it is said that he will not be able to get right to the goal since he does not have complete control of the aircraft. The following strategy is a mix between intentional strategy and emergent strategy, essentially one does not need to plan, preparing oneself not in a preordained way. So, knowing how to read the situation according to an approach defined as **"evaluation & exploitation", as opposed to the traditional "design & implementation"** and the behaviour is defined *in itinere* (ongoing). **In the security of complex systems, solutions cannot be planned and the situation must be read at the moment.**

6. THE QUESTION OF THE MEASURE OF RESILIENCE

A possible measure of resilience is based on **four interdependent dimensions (Fig. 6)**: technical, organizational, social and economic, to be represented with different performance indicators, interrelated with the four properties of resilience:

- the **technical** dimension of resilience refers to the ability of physical systems (including components, their interconnections and interactions and entire systems) to operate at acceptable/desired levels when subjected to perturbative forces;
- the **organizational** dimension refers to the ability of organizations that manage critical facilities and have responsibility for performing critical disaster-related functions to make decisions and take actions that contribute to the achievement of the resilience properties outlined above, i.e. that help achieve greater robustness, redundancy, availability of resources and speed;
- the **social** dimension of resilience consists of measures specifically designed to reduce the extent to which affected communities and governmental jurisdictions are negatively impacted by the loss of critical services following disasters;

[190] This is the training philosophy of the special teams of the Italian Firefighters called USAR (Urban Search And Rescue) created to improve rescue activities in rubble, deriving from seismic events, explosions, collapses or static and hydrogeological instability.
[191] In H.Mintzberg, The structuring of organizations, Prentice-Hall, 1979.

- the **economic** dimension of resilience refers to the ability to reduce both direct and indirect economic losses deriving from events.

System Engineering[192] proposes an empirical method to solve engineering problems of complex systems. It is composed of four phases for the search for optimal solutions and each phase includes different operational tools **(Fig. 7)**.

PERFORMANCE MEASURES	Robustness	Redundancy	Resourcefulness	Rapidity
TECHNICAL	**Damage** avoidance and continued service provision	**Backup/duplicate system**, equipment and supplies	**Diagnostic and damage detection** technologies and methodologies	**Optimizing time** to return to pre-event functional levels
ORGANIZATIONAL	**Continued ability** to carry out designated functions	**Backup resource** to sustain operations (e.g., alternative sites)	**Plan and resources** to cope with damage and disruption (e.g., mutual aid, emergency plans, decision support systems)	**Minimize time** needed to restore services and perform key response tasks
SOCIAL	**Avoidance of casualties and disruption** in the system	**Alternative means** of providing for community needs	**Plan and resources** to meet community needs	**Optimizing time** to return to pre-event functional levels
ECONOMIC	**Avoidance of economic losses** (direct and indirect)	Untapped or excess **economic capacity** (e.g., inventories, suppliers)	**Stabilizing measures** (e.g., capacity enhancement and demand modification, external assistance, optimizing recovery strategies)	**Optimizing time** to return to pre-event functional levels

Fig. 6 - Possible measures of resilience through performance indicators[193]

Phase	*Instruments*
Analysis of the current situation and future scenarios	Systemic analysis Correlation matrices Flow charts, templates Statistical tools (e.g., Pareto analysis) Simulations Creating scenarios Information gathering techniques Analysis of strengths and weaknesses, opportunities and risks (SWOT analysis)
Definition of objectives	Objectives tree
Creation of solution variants	Creativity techniques Brainstorming Parallel (lateral) thinking
Choosing the optimal solution	Utility calculation tables (value analysis) Consequence analysis Simulations Delphi technique

Fig. 7 – System Engineering method

Brainstorming is very important to consider some combinations of threats as, considering all combinations, is not feasible. Furthermore, combinations of the most probable events could lead to other risks and, since these are complex systems, one must ask how the occurrence of one event increases the probability or impact of another event.

The **Delphi technique** is essential to acquire the opinions of a panel of experts and to collect and compare the judgments on a topic through a set of coordinated questions. It is used for complex problems about which uncertainty exists and for which expert judgment needs to be acquired. In our case it can be used to identify threats and assess risks by seeking consensus on the probabilities and consequences of possible events and their combinations. It can be repeated over time every day, week, month or even year and does not require physical presence on site, as it can also be distributed, processed and returned remotely.

[192] See in AA.VV., Caos e complessità, Laboratorio interdisciplinare laboratorio dell'immaginario scientifico, CUEN, 1996. pag. 284.
[193] See in F.Borghetti, G. Marchionni, L. Studer, Il concetto di resilienza delle infrastrutture di trasporto. Quadro delle ricerche e metodi quantitativi di analisi, Laboratorio di Mobilità e Trasporti, Politecnico di Milano e Dipartimento di Design, 2019, Milano.

APPENDIX 4.2 - TUNNELS

THE DIFFICULTIES OF RISK ASSESSMENTS FOR COMPLEX NETWORK INFRASTRUCTURE: APPLICATIONS TO THE SECURITY AND THE RESILIENCE OF ROAD INFRASTRUCTURE

Authors: **Philippe CHANARD**[194] and **Christofle WILLMANN**[195]

1. Introduction

Tunnels are covered structures designed to allow the underground passage of a road, railway or waterway. They can be short, medium or long (over 2500 m), one-way or two-way. They may be successive; they may be small gauge; they may be intermodal; they may serve car parks in urban areas; they may also have multiple underground entrances and exits.

2. Tunnels became complex structures [196]

2.1 Isolated tunnels: an intrinsic complexity

Tunnels, whose sole function initially was to cross an obstacle (usually a mountain), have become increasingly complex over the years, with the inclusion of more and more complicated operating equipment and ventilation systems, control and supervision systems capable of handling tens of thousands of points to be controlled and of proposing increasingly sophisticated management scenarios.

The conditions for operating a tunnel are complicated because of the number of actors involved and the numerous and specific tasks of the operating bodies.

Thus, the following actors must cooperate: the tunnel owner and operator himself, other road network operators, the national and local administrative authorities, public services such as fire and rescue services, traffic police, medical services and other subcontractors (cleaning, maintenance, breakdown services, etc.).

The usual tasks of tunnels' operating bodies are: Traffic monitoring and operation of tunnel equipment, Surveillance by patrols, Civil engineering management, Equipment management, Emergency management, Technical and administrative management.

A peculiar safety management is compulsory: because a tunnel is an enclosed space, safety management focuses on controlling the risks associated with fires and the transport of dangerous goods.

Managers' attention is drawn to the following main points:

- The tunnel control centre must have the possibility to interrupt the broadcasting of user radios in order to broadcast emergency messages. Sirens and audible beacons may also be useful especially in tunnel with important issue in terms of risks;
- A tunnel closure system, if possible combined with variable message signs, is a useful safety feature in the event of a serious incident;

---

[194] P. Chanard, PIARC-FRANCE, Former director deputy DIR Massif Central, France.
[195] C. Willmann, CETU, Director of research and studies safety and security, France.
[196] Ch.Willmann and all; Breakdowns, accidents and fire in road tunnels – statistics; CETU information document – 24 p - February 2022

- Emergency exits should be signalized and visible (for example with flashing location point) and may be equipped with audible beacons depending on the issue of the tunnel in term of risks. Flashing exit path indicators can be useful;
- The regular checking and maintenance of this equipment is imperative for the operating teams who must be able to intervene in real time.

All the measures mentioned above should be used consistently within organizational procedures developed with the participation of all the operating body team members and all stakeholders involved in the safety management. Regular training sessions and exercises are required to ensure the smooth appliance of these measures and the good coordination of stakeholders.

2.2 Tunnels in an underground road network: an overall complexity

To illustrate the complexity of some "**Underground Road Networks**", these can be defined by the following infrastructures quoted as examples: sequencing of several successive tunnels close together, service tunnels serving business and commercial centres or parks (users and freight), underground infrastructure with multiple entrances and exits, as well as underground interchanges. This category of tunnels is the most crowded.

3. Tunnel security, a complex approach

As explained above, tunnels are complex infrastructure with various organisational and technical measures developed for safety reason. Safety deals with the incidents that happens accidentally and are random events like breakdown, collisions and fires. In addition, security deals with events that are not accidental but intentional like terrorist attack. Fortunately approaches, methods and measures developed for safety reasons can be useful and effective in the framework of security.

3.1 The tunnel system: a broad range of structures, assets, measures, organization and processes

The structure complexity is an element that increases security risks but the security issue is more complicated.

In reality, as done for dozens of years in safety' field, it is necessary to consider the tunnel as a system in order to deal effectively with 'security' issues The system includes several elements:

- The tunnel in the strict sense;
- The tunnel control centre (on site or remote) from which the tunnel is operated including the telecommunication network (optical fiber, etc.);
- The organization (staff) and the processes for the management of the tunnel itself, including resource mobilization;
- The traffic management measures for the road network, the traffic management centre (if different from the tunnel control centre), interactions with other systems (e.g.: when the tunnel is part of an interconnected underground infrastructure or when another organization operates the road network outside the road tunnel);
- The road in and around the tunnel, including an alternative route for occasions when the tunnel is closed and when a coordination with local administrative authority is needed;
- The emergency management, including a coordination with many partners in a timely manner to contain looses and avoid future disruption: public services (fire and rescue services, Police), subcontractors (cleaning and breakdown services).

All elements of the tunnel system are affected by safety and security, which makes it, in reality, a complex infrastructure to deal with in terms of security.

3.2 The security risk assessment[197]

According to the ISO 31000, the process of risk assessment is composed by three subsequent steps:

To simplify, only a few key points are highlighted below:

3.2.1 Threats

In the framework of security, threats concern people, the staff of operating body, the physical part that is structure, infrastructure, and vehicles, the information technology (IT) and the procedural and organizational parts. The tunnel system as a whole is a complex infrastructure to deal with in terms of security.

Since roads are the site of various types of criminal acts and illicit traffic and may also be the site of acts of a terrorist or criminal nature, the tunnel is one of the most exposed parts of the road network. It is due to the fact that inside, as a confined environment in which road traffic develops, human life is more at risk.

The effects of an incident occurring accidentally and a deliberate attack can be the same.

The risks of physical security are associated with those of cyber security given that in recent years there has been a rapid evolution of cyber threats, which have often exceeded the criticalities of physical security. Tunnel control systems, based on Control and Data Acquisition Systems, are exposed to cyber-attacks.

The threat of cyber-attacks is a reality and in the event of an intentional malware action, the organizations in charge of operating a tunnel system must be prepared.

3.2.1.1 Specific threats related to tunnel control centres

The control centres of the tunnels are responsible for monitoring and controlling the traffic inside and at their entrances, for maximum operational safety. They are mostly integrated into IT communication networks through different interfaces and in the absence of effective protections, and in them it is possible to carry out manipulations in the control units of the systems. There is also the possibility of manipulating sensor data, blocking control commands and altering standard safety controls.

---

[197] *Ph. Chanard, French-speaking secretary of Task Force 3.1: 2023 Report "Road Infrastructures and Transport Security" - PIARC*

3.3 The risk analysis and the risk evaluation

To define and prioritize the measures to be taken in order to handle the threats, some critical scenarios in the field of security can be defined and taken into account in a risk analysis:

- Explosion in a zone near the tunnel (therefore actions not directly aimed at the tunnel but with consequences in accessing it);
- Simultaneous explosions of vehicles loaded with explosive at both entrances of the tunnel;
- Explosion of a vehicle loaded with explosive against the site where the central control operations that manage all the security system is located;
- Launch of particular objects from ventilation ducts above the road surface;
- Input of a toxic product in the air ventilation system through a well or an external air vent;
- Loss of coordination of radio control rooms (twin rooms in stand by that are activated in case of emergency);
- Loss of electricity line;
- Loss of communication by the computer systems,
- Violent demonstrations and movements

The risk analysis leads to an estimation of the risk. This estimation is mainly based on the following principle:

R (Risk level) =P (Probability of the occurrence of the threat) x D (damages)

Depending on the methodology used, risk estimation and evaluation can take many forms. The risk estimation could be achieved in a qualitative or a quantitative way.

If the estimation is qualitative, the evaluation will also be qualitative.

If the estimation is quantitative, it can result from a matrix or an expected value of deaths or an F/N curve (F: frequency, N: number of deaths).

Then evaluation could be achieved by using a reference curve or number, or the ALARP principle (As Low As Reasonably Practicable) or the GALE principle (Globally At Least Equivalent).

3.4 The security measures

The risk analysis and the risk evaluation should lead managers to priorize and to plan:

- Preventive security measures: access controls, physical security of premises, structures and equipment, organization and processes, security training, etc.
- Information security measures: autonomy of information systems, limitation of remote access, regular updating of software and passwords, etc.
- Mitigation measures for example against fire.

A selection of safety and security measures is listed below:

Top 5 of preventive security measures:

- prevent unauthorized persons or vehicles from accessing tunnel system assets
- provide special authorizations for subcontractors and suppliers
- isolate control centre staff from other staff during their operation by securing entrances
- implement multi-level security, combining physical and logical lines of defence

- have redundant equipment for the supply of energy, radio and communication networks (copper, optical fibre networks) in or nearby the traffic management centres and tunnel control centres.

Top 5 of Information security measures:

- regularly change passwords and usernames linked to computers and control systems
- set security requirements for the purchase of information products and services
- limit remote access to computer systems and disable unused ports on switches
- provide a self-contained communication and data network between the tunnel control computers and systems and the traffic control centre, without connection to the Internet
- systematically authenticate messages for variable message panels and do not let tele maintenance modems be plugged in.

APPENDIX 4.3 - VANDALISM

GOOD PRACTICES AND TIPS TO LIMIT THEFT AND VANDALISM OF ROAD ASSETS

Author: **Philippe CHANARD**[198]

1. INTRODUCTION

Road managers are confronted daily with theft and vandalism. Very often, the consequences are significant because, in addition to the damage to material goods which are not always quickly repaired, the image of the road service is damaged and the morale of maintenance staff is affected. Given the importance of the subject, the PIARC experts of Task Force 3.1 Infrastructure and Transport Security launched a survey in 2020 on good practice in anti-vandalism measures and devices. The purpose of this article is to simplify the presentation by devoting a first part to anti-graffiti measures and a second to anti-theft measures.

2. ANTI-GRAFFITI MEASURES

The most common cases of vandalism are graffiti on structures, but also on signs and even on speed cameras.

Few road managers have a specific policy on the subject. The Federal Roads Office (Switzerland) is one of them, and has given a precise definition of the term "graffiti" and established practical intervention criteria depending on the messages and locations of the graffiti.

2.1 Definition of the term "graffiti"

Graffiti is calligraphic inscriptions or drawings, written, painted or engraved on a surface not normally intended for that purpose. Graffiti is sprayed with aerosol cans, scribbled with felt pens or scratched with sharp objects. Simple inscriptions or logos are called "tags". Graffiti consists of a combination of stylized letters or drawings.

2.2 Nature of graffiti

Three types of graffiti are considered:

1. Political, racist, anti-religious messages: not acceptable - remove immediately.
2. Stylized graffiti with pornographic content: not acceptable - remove immediately.
3. Tags: acceptable - to be removed periodically (immediately or not, but regularly) - or to be retained depending on its location or artistic value.

Graffiti that could be retained FEDRO photos

Graffiti that needs to be removed FEDRO photos

[198] P. Chanard, PIARC-FRANCE, Former director deputy DIR Massif Central, France.

2.3 Graffiti location criteria: case of engineering structures in Switzerland

Graffiti should be removed from:

Structures along or over roads with heavy daily traffic -> to be treated immediately

Exceptional engineering structures -> to be treated periodically

Structures in urban areas and on bypasses of major cities [199] -> to be treated periodically

Structures supporting traffic signs -> to be treated immediately

Tunnels (inner walls and portals) > to be treated immediately

2.4 Graffiti treatment techniques

While preventive techniques (anti-graffiti paint, fencing, planting) exist, curative techniques (graffiti removal, paint coating) require the will of managers and the availability of maintenance staff. Many local authorities hire specialized companies to remove graffiti. Among the anti-graffiti paints are distinguished:

- *Temporary anti-graffiti systems.* These are usually an invisible protective layer (products based on acrylates, biopolymers, waxes or waxy products) that prevents graffiti from penetrating the concrete.
- *Semi-permanent anti-graffiti systems.* These are two-layer systems (the top layer, called the sacrificial layer, consists of waxes or waxy products, and the bottom, permanent layer consists of silanes, siloxanes or acrylates).
- *Permanent anti-graffiti systems.* The products most often consist of polyurethanes or epoxy resins as chemical resistant layers. But products based on silanes/siloxanes and acrylates are also used

Through these preventive techniques, the removal of graffiti is greatly facilitated and usually requires a simple hot water jet under pressure with some chemical cleaning products. In the absence of preventive techniques, cleaning is more complex and involves either chemical or mechanical methods (pressurized water jetting, hydro gumming, etc.) or covering paints.

2.5 Some practical examples

2.5.1 The case of the Quebec Ministry of Transport

Testing the effectiveness of anti-graffiti paints on metal walls.

[199] In certain cases, and in collaboration with the local authorities, certain surfaces may be made available for artistic graffiti. An agreement on the location, style and colors to be used must be made in advance with the relevant Works Manager.

2.5.2 The case of the French Ministry of Transport -A75

Covering graffiti with artistic paint in a rest area sanitary room-Photo 4 DIRMC

2.5.3 The case of the French Ministry of Transport/A6[200]

Gabion in front of concrete abutment of a mixed bridge

Fencing and planting in front of the noise barrier

3. Anti-theft measures

As far as theft is concerned, underground cables, materials and equipment in technical premises, photovoltaic panels close to the road, construction site batteries and even some traffic signs are targeted.

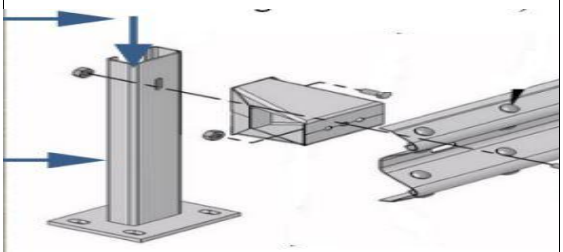
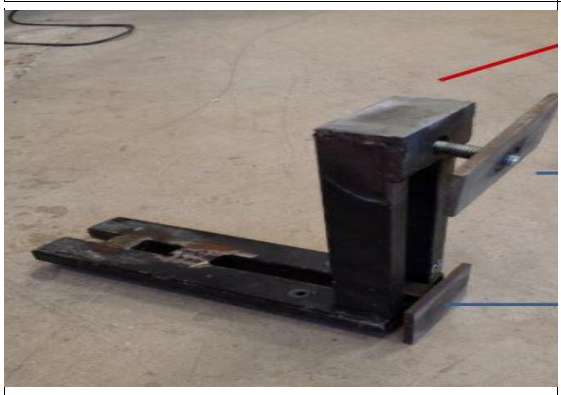
3.1 "Home-made" tricks

In addition to the classic anti-theft techniques (intrusion detectors, surveillance cameras, etc.), some French road workers have cleverly created "home-made" devices for hanging batteries on guardrail posts, for locking manhole covers.

3.1.1 Anti-theft of construction batteries

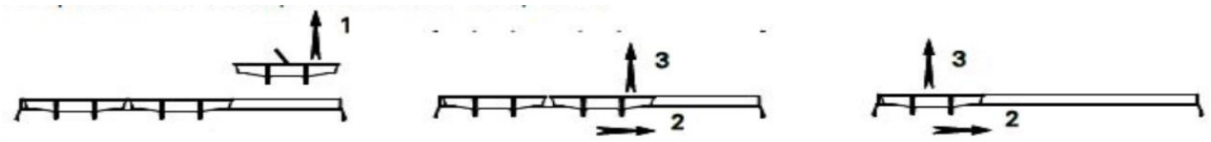
The A75/A750 maintenance and operations centre in Montarnaud, which is particularly affected by repeated battery thefts, has designed an effective anti-theft device. It is a system comprising a battery and a specific box with visible connections. The whole system is fixed to a C100 slide support and cannot be dismantled without special tools.

[200] Pictures by Philippe Chanard

Support with spacers that slide into the post of the slides => Battery assembly and fixing before installation Battery in its adapted case Initiative centre A75 Montarnaud DIR Massif Central – *Schemes- Photos 9-10 -11 DIRMC*	Post C100 without spacer removal 
	

3.1.2 Anti-cable theft: lockable chamber buffer

DIR Centre Est staff have designed lockable and interlocking cable chamber buffers from standard products to deter thieves.



3.2 Drones

Other managers (Brazil) do not hesitate to mobilize drones and observation towers in sensitive areas and to equip equipment with chips. Theft of vehicles and fuel is also possible but not specific to road managers. In general, dual-use technologies (integrated safety and security) should be sought. Specifically in Brazil, it was necessary to create models of the type of surveillance according to the degree of violence identified for a given region.

Thus, for regions where there is more violence and crime, the type of model will be adopted with more or less devices or measures:

- for areas with a high level of vehicle theft: drones + watchtowers with drone battery charging + GPS trackers (geo-trackers or GPS trackers);
- for areas with a high rate of sign theft: locator chips;
- for regions with high levels of vandalism on road assets: drones + watch towers.

Drone on its charging tower[201]

[201] From Departamento Nacional de Infraestructura de Transportes/DNIT

APPENDIX 4.4 - DANGEROUS GOODS

CURRENT ROAD SECURITY PROBLEMS IN THE ROMANIAN TERRITORY DUE TO THE ILLEGAL TRANSPORT OF DANGEROUS GOODS

Authors: **Flavius PAVAL**[202] and **Saverio PALCHETTI**[203]

1. GOODS AND SECURITY IN LAND TRANSPORT

Security measures were introduced by the United Nations following the events of 11 September 2001, with the aim of defence against terrorism and to prevent attacks in which dangerous goods could be used. By its nature, the transport of dangerous goods involves materials, objects or articles which are characterized by their dangerousness (explosives, flammable liquids and gases, toxic products, etc.) and by their possible use in terrorist actions.

The **ADR regulation** [204] is the European regulation that regulates the transport of dangerous goods by road. According to it, dangerous goods are materials and objects, the transport of which is prohibited but which can only be authorized under certain conditions. Among these we have high-risk dangerous goods, i.e., goods potentially usable for terrorist purposes and which can therefore cause serious effects such as loss of human lives or mass destruction. In 2005, the aspects relating to security, because they can result in numerous losses of human lives, mass destruction, environmental impacts and socio-economic upheavals, were introduced in the **Chapter 1.10** of the Technical Annex "A". They are addressed to all parties involved in the transport chain: staff of the sending, loading, carriers, unloading companies, receiving companies. The regulation, ratified not only by all members of the European Union but also by various countries, is divided into technical annexes and updated every two years.

ADR defines "security" measures to be adopted also to reduce the potential risks of theft or improper use of dangerous goods. Such rules involve operators whose activity affects the transport and/or storage of dangerous goods and provide for the obligation for transport companies to draw up and implement a security plan, according to risk management processes, identifying: responsibility, with qualifications and skills, typology of dangerous goods, assessment of the security risks associated with the transport of dangerous goods, definition of the measures to adopt to reduce security risks, measures taken to deal with threats, procedures for verifying and evaluating security plans, dissemination of the necessary information.

The classification of a dangerous goods or preparation (**Fig. 1**[205]) determines:

- the type of transport and the types of packaging that can be used for transport in parcels;
- danger indications, stowage and segregation methods;
- the information and documents to be given to carriers, operators and authorities.

---

[202] F. Paval, PhD, Associate Professor UTM – DIIT, Head of Traffic Safety Service - CNAIR Bucharest, Romania.
[203] S. Palchetti, PhD, Senior Security Manager, Chair PIARC TF 3.1 “Road Infrastructure and Transport Security”, Italy.
[204] ADR Regulation, European Agreement Concerning the International Carriage of Dangerous Goods by Road
[205] Classification criteria according to the provision of ADR, Ref. ADR - Part 2.

Class	Description	Main danger
1	Explosive materials and objects	Explosion
2	Gas	Gas emission resulting from pressure or chemical reaction
3	Flammable liquids	Flammability and/or explosivity
4.1	Flammable solids, self-reactive substances, substances subject to polymerisation and solid desensitized explosives	Flammability and/or explosivity
4.2	Substances subject to spontaneous ignition	Flammability without the presence of ignition or self-ignition
4.3	Substances which, in contact with water, emit flammable gases	Flammability and/or explosivity due to release of flammable gases
5.1	Oxidising substances	Perchlorates, ammonium nitrate, fertilizers, emulsions and suspensions or gels
5.2	Organic peroxides	Instability with accelerated decomposition
6.1	Toxic substances	Toxicity by inhalation, ingestion and skin contact
6.2	Infectious substances	Contagion by viruses, bacteria, parasites, fungi
7	Radioactive materials	Radioactivity, radio toxicity, radiation contamination
8	Corrosive substances	Corrosion of human tissue and metals, production of corrosive mists and vapours
9	Various dangerous materials and objects	Various environmental hazards

Fig. 1 - Classification of goods in ADR

PRODUCTS	Agriculture	Car factory	Plastic factory	Pottery factory	Insecticide factory	Rubber factory	Paint factory	Solvent factory	Textile factory	Chemical laboratories	Manuf. electrical components	Manuf. synthetic products	Pharmacy - grocery	Hospitals	Typography	School	Armories	Construction sites	Building materials
	SOURCES FOR SUPPLY (Manuf. = Manufacture)																		
Ammonium nitrate	■	■			■			■		■	■	■	■	■					
Aluminium																			■
Iron oxide				■	■	■	■	■		■			■			■			
Linseed oil	■														■	■			
Magnesium						■		■	■	■		■				■			
Phosphorus	■														■	■			
Potassium												■	■			■			
Potassium chlorate				■	■			■		■		■			■	■			■
Potassium nitrate	■				■		■		■	■	■					■			
Potassium permanganate				■	■							■	■			■			
Sodium chlorate				■	■		■					■	■		■				
Sodium nitrate	■			■		■			■			■	■		■				■
Sulfur	■	■		■	■	■	■		■	■		■	■		■	■			
Sulfuric acid	■	■							■				■						
Black or gunpowder																	■	■	
Carbon tetrachloride	■									■			■						

Fig. 2 - Table of sources for supply of products called precursors

2. THE PROBLEM OF PRECURSORS

Many common ADR dangerous goods have become precursors to explosives, i.e., substances which when mixed with others give rise to an explosive. Among these substances there are, for example, common fertilizers[206] (**Fig. 2**). In Europe, regulations and guidelines have been approved with obligations for those who sell and obligations for those who buy:

- Regulation (EU) 2019/1148 of the European Parliament and of the Council of 20 June 2019 on the marketing and use of explosives precursors, amending Regulation (EC) No 1907/2006 and repealing Regulation (EU) No 98/2013;
- Communication of the European Commission, Guidelines for the implementation of Regulation (EU) 2019/1148 on the marketing and use of explosives precursors.

Main points of awareness are:

- **knowledge and aware of the risk** of improper use of dangerous goods;
- **security measures** against the theft or misuse of dangerous goods;
- **procedures** for applying security measures;
- **staff engaged** in the transport of commonly used goods should consider the security provisions for ground transportation of dangerous goods (commensurate against their responsibilities).

For the precursors the risks are not so much of transport but of **theft or disappearance**. Theft is a criminal act while the disappearance can be a material error or carelessness and can occur within the production site and also during transport. All this can occur within the context of the seller, but also in that of the buyer. It is important for the seller to check the labels, keep the documents for 18 months, carry out a psychological evaluation on the buyer and report suspicious behaviour[207] or transactions or thefts and disappearances within 24 hours. **Training is essential**

[206] For example, ammonium nitrate can be used as a fertilizer but also as an explosive precursor and is normally sold in 25 kg bags in any agricultural cooperative; potassium nitrate, available in sacks, is used as a fertilizer, food preservative (e.g. cured meats) and to produce gunpowder; potassium chloride supplements, usually in tablets, are usually taken during or after meals to reduce gastrointestinal irritation and laxative effect.

[207] Suspicious behavior of a buyer: appears nervous, avoids questions, is not a regular customer, tries to buy products in anomalous quantities, combinations and concentrations, does not know the uses of the product well, is reluctant to give clarifications, refuses to answer.

for those who produce, sell, transport and buy, as well as the preparation of physical defence measures and a frequent periodic check of warehouse stocks.

The **inspections are done by the national supervisory authority** which is the criminal police body of the Ministry of the Interior of the European country concerned which is also in charge of receiving reports. [208] The checklist is confidential and applies to: storage activities, control activity on the buyer, method of marking the goods, mode of transport.

3. ROAD TRANSPORT OF DANGEROUS GOODS AND SECURITY

In the Chapter 4.2 of this Report, it was highlighted that the **whole issue of the transport of goods**, since the goods produced are packaged, placed in any kind of container and placed on a transport carrier until reaching their destination, presents security problems. The **threats** concern the personnel, people in general even as an actor himself the threat, the physical part that is goods, containers, means carrying the object, structure and infrastructure, as the intermodal centres or parking areas, and the IT and the procedural and organizational parts.

The **security threats for freight transport** concern not only the load transported, but also the staff (drivers, administrators and workers), the means and logistics facilities and the supply chain as a whole. All this is linked by procedures that have important role in security. As a necessary response to the **new operational scenarios** resulting from the pandemic emergency, a widespread awareness has been further consolidated regarding the strategic role of road transport and logistics as essential services in a country's economy.

The **transport of dangerous goods on the road network** is the object of particular attention both in terms of accidents and in the seriousness of the possible consequences of the leakage of dangerous materials.[209]

As shown, the problem of risk in the transport of dangerous substances is addressed by the **ADR regulation** which divides the products into homogeneous categories and establishes the conditions of transport, the characteristics of the containers, the periodic inspections, etc. . But, with the **aim of preventing the release of the product in the event of an accident,** compliance ADR does not guarantee that the risk to which the population is exposed is negligible. By way of example, for the same type of product transported and means of transport used, **the risk can be very different** depending on the itinerary chosen, the number of journeys made along the same route, etc.

Furthermore, taking into account the **cumulative risk** due to the possible overlap in the same area of different dangerous activities deriving from transport from loading and unloading operations and from the presence of industrial settlements. **This assessment needs to be done at the local level and its accuracy depends on detailed knowledge of the situation in the area**.

The **risk assessment in the transport of a dangerous substance**, even if similar to that relating to an industrial activity, is more demanding, and requires the knowledge of a greater amount of

[208] According to the Regulation, an inspection in a factory involves the verification of a hundred control points.

[209] The main reference is represented by the application of the international standards ISO 31000 and ISO 28000 specialized in security risk assessment. As is known, these are families of standards based on the Deming Cycle Continuous Improvement method or DCPA. Based on it, the defense measures must be verified and cyclically rethought, proposing different ways in which this cyclical adaptation or improvement can be achieved.

information. In fact, in the case of transport, both the probability of an accident and its consequences vary continuously along the itinerary and this forces us to examine a much larger number of cases. Risk analyses must therefore be repeated every time the relevant parameters change along the route. The **information needed to assess risk** can be classified as follows:

a) **specific to the case in question**: substance transported, means of transport, number of journeys, itinerary followed, etc.:
b) **obtainable from the collection of data and statistics**: accident rates; quantities released following an accident, weather conditions. resident population, etc.;
c) **obtainable from information available in the scientific and technical literature**: flammability limits, dispersion methods, trend of the overpressure field, effects on the human body, etc.

The **most critical point** is generally constituted by the availability of the information referred to in point b) which is difficult to find and very often not directly applicable to the transport of dangerous substances. Strictly speaking, in fact, the data should refer to the type of vehicle used, the product being transported and the itinerary followed. However, since fortunately the number of accidents that actually occurred is limited, it is generally not possible to have specific and at the same time statistically significant data available. Some problems may also arise in the retrieval of information from the literature referred to in point c) in the case of particular products or mixtures of products, this occurs for example for the aforementioned precursors.

Once the above information is available, the **transport risk assessment follows the procedures similar to those normally used P X D = R** taking care to apply them for each of the homogeneous sections into which the itinerary can be considered divided and then recombine the contributions of the single sections in order to obtain the global risk relating to the entire route. As a measure of risk, social risk seems to be preferred since it takes into account both the probability that a dangerous event will occur in the reference time interval and the number of people who could suffer the consequences. Therefore, the risk is obtained as a product of the probability of accidents per year capable of causing a number of deaths a certain number of deaths including possibly that of the driver.

In essence, a procedure for risk assessment in the transport of dangerous goods could be composed as follows:

- **definition of the dangerous substances** to which the procedure is to be applied;
- **census of the transport of dangerous substances** on the national territory;
- **retrieval of data on the accident** rate;
- **accident scenarios** and their evolution;
- **meteorological data**;
- **resident population and in transit** along the road network expressed as the number of people per km^2.

4. ROAD TRANSPORT NETWORK IN ROMANIA

Romania is part of the European Union, and its **geographical location** is in the Eastern part, being a country with access to the Black Sea and therefore into the Mediterranean Sea (**Fig. 3**) . The **port of Constanta** is the fourth largest in Europe and is located on the routes of the Pan-European Transport Corridors “IV” that connect the North Sea to the Black Sea. Between the port of Constanta and the port of Rotterdam there are both the Rhine-Main-Danube rivers connection

and the road-highways-motorways network crossing Europe. Two other **EU Transport corridors** cross in Romania: "VII" and "IX" (**Fig. 3**). Constanta port is also located at the intersection of commercial routes that connect the markets of landlocked countries in Central and Eastern Europe with the Transcaucasia region, Central Asia and the East.

Most volumes of goods are transited on Romanian territory from East to West, respectively from the port of Constanta, to the border with Hungary (west) (**Fig. 4**). Regarding the transport of dangerous goods, the largest traffic volumes are registered on the route on the territory of Romania, that starts in Constanta port and leads to the border with Hungary (in the west).

Fig. 3 – Romania and its positioning in relation to Europe and Constanta port – Rotterdam port relationship

Fig. 4 – Main road transport network (European corridors) in Romania

With the **conflict in Ukraine**, the volumes of goods transport increased exponentially, and the route to be followed from the border with the Republic of Moldova and the border crossing point with Hungary, to cross Romania from east to west or from N or NE to West, is of approx. 750 - 800 km.

5. TRANSPORT OF DANGEROUS GOODS IN ROMANIA

In the **tables published by Eurostat** the increase of 32% in traffic of dangerous goods in 2021 on 2020 is shown[210]. Considering the fact that after the outbreak of the conflict in Ukraine, at customs of the Republic of Moldova and Ukraine, on the entry into Romania, the **queues of goods vehicles** measured impressive lengths tens of kilometers and long waits of up to a week, it is easy to understand that in these conditions, due to the pressure and the high volume of activity, it is very likely for customs inspection bodies to make errors, thus, entering the country, vehicles transporting illegal goods, the most dangerous for the state and infrastructure being those transporting dangerous goods.

Regarding the verification of the transport of dangerous goods, in Romania is operating the **State Inspectorate for Control in Road Transport - I.S.C.T.R.** which is the permanent technical body specialized under the Ministry of Transport and Infrastructure, ensuring at the national level the inspection and control of compliance with national and international regulations in the field of road transport. In 2021, a **report on contraventions and sanctions** was issued as a result of

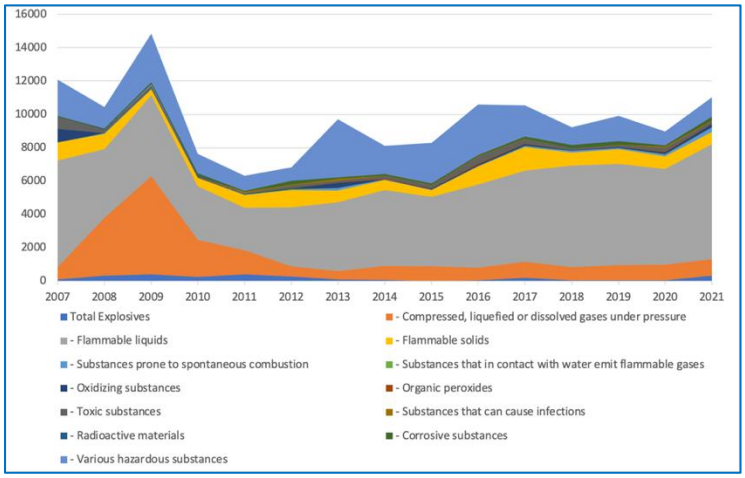
[210] Road freight transport of dangerous goods 2017-2021, EUROSTAT (online data codes : road_go_ta_dg; road_go_ta_tott)

controls carried out on the road transport of dangerous goods, from which the results emerged as in **Fig. 5** [211].

		Place of vehicle registration			Total number
		Romania	Other EU member states	Third countries	
The number of controlled transport units depending on the load content (and ADR)		2609	119	180	2908
The number of transport units not complying with ADR provisions		94	3	1	98
The number of immobilized transport units		34	1	0	35
The number of violations found, depending on the risk category	Category I of risk	34	1	0	35
	Category II of risk	41	1	1	43
	Category III of risk	19	1	0	20
The number of sanctions imposed, depending on the type of sanction	Warning	0	0	0	0
	Fine	94	3	1	98
	Criminal offence	0	0	0	0

Fig. 5 – Contraventions issued as a result of controls carried out on the road transport of dangerous goods

The trend of the data on road transport (2007-2021) are presented in **Fig. 6**, including the goods transported by vehicles for the road transport of goods, registered in Romania, with a maximum authorized payload of at least 3.5 tons, operating on the basis of a valid goods transport license. The total of dangerous goods transported in 2021 was equal to approximately 11 million tons for approximately 2.3 billion tons-km. The control of dangerous goods transported on road infrastructure was extremely important, because they can lead, intentionally or unintentionally, to the occurrence of unfortunate events, with extremely serious consequences for the infrastructure and for the country.



ESTIMATED TOTAL QUANTITY OF DANGEROUS GOODS CARRIED BY ROAD	11.024 thousands of tons	2.265.070 thousands of tons - km

Fig. 6 - Transported goods, by categories of dangerous goods and types of road transport (2007-2021)

[211] Anexa III, DIRECTIVA 1995/50/CE, RAPORT CU PRIVIRE LA CONTRAVENŢII ŞI SANCŢIUNI, Instituţia: INSPECTORATUL DE STAT PENTRU CONTROLUL ÎN TRANSPORTUL RUTIER – I.S.C.T.R., 2021, CONTROLUL TRANSPORTURILOR RUTIERE DE MĂRFURI PERICULOASE. (Appendix III Directive1995/50/EC, Report Regarding Offenses and Sanctions, Institution: STATE INSPECTOR FOR ROAD TRANSPORT CONTROL – I.S.C.T.R., 2021, CONTROL OF ROAD TRANSPORTATION OF DANGEROUS GOODS.)
For the purposes of this annex, the country of registration is the country of registration of the motor vehicle.

6. ACCIDENTS INVOLVING DANGEROUS GOODS IN ROMANIA

Road transport accidents involving dangerous goods happened in 2016 in Romania mainly in National roads (52 with 37 deaths). In 2016, 3 road accidents involved vehicles carrying very large quantities of dangerous goods, without explosions, as these substances were neutralised by the emergency crews that arrived at the scene. **Fig. 7** shows the results of the accidents happened in Romania related to the substances transported.

Type of substance transported	No. accidents	Dead	Seriously injured	Slightly injured
Flammable liquids	48	23	35	18
gas	21	12	18	9
Oxidizing substances	11	8	8	4
Substances that generate flammable gases in contact with water	6	2	4	1
Organic peroxides	2	2	2	1
Flammable solids	2	3	1	1
Explosive substances	2	1	1	4
Substances subject to spontaneous combustion	2	1	1	0
Toxic substances	2	1	2	1
Self-reactive substances	1	0	1	0
Corrosive substances	1	1	0	0
TOTAL	98	54	73	39

Fig.7 - Accidents in Romania involving dangerous goods

These kind of events can have devastating results for the country's economy, especially in case of international malicious events (terrorist attacks, war, etc.) since other than the road network, the electricity distribution network, the telecommunications network, the public lighting system can be involved. This is an extremely important issue for road infrastructure managers when tragic international events (such as the war in Ukraine) destabilize routine checks on international transport, putting extreme pressure on the personnel involved in checks and controls, making the road network vulnerable for anti-social actions, terrorist attacks or thefts also through the transport of dangerous goods.

APPENDIX 4.5 - INFORMATION TECHNOLOGY AND ARTIFICIAL INTELLIGENCE

NEW SAFETY AND SECURITY REQUIREMENTS FOR ROAD INFRASTRUCTURE IN THE AI ERA

Authors: **Flavius Michal ZABOVSKY, Eva LIESKOVSKA, Katarina ZABOVSKA**[212]

1. ARTIFICIAL INTELLIGENCE AND ROAD TRANSPORT

In the **Figure 1** the overview of the core components of transportation are shown. Related to that, **artificial Intelligence (AI) techniques** used in the road transportation include [213]:

- **vehicles automation** - automated/autonomous driving, assisted driving, platooning;
- **operational intelligence** – ITS, traffic management, solutions for optimization and capacity platting, multi-modal transportation, critical infrastructure monitoring, infrastructure forecasting, maintenance costs reduction, passengers' satisfaction;
- **asset intelligence** - AI is helping to assess the performance of an infrastructure and support design, planning and management of it. This kind of application is tightly connected to "digital twin" concept which can be applied on different levels of intelligent systems for transportation.

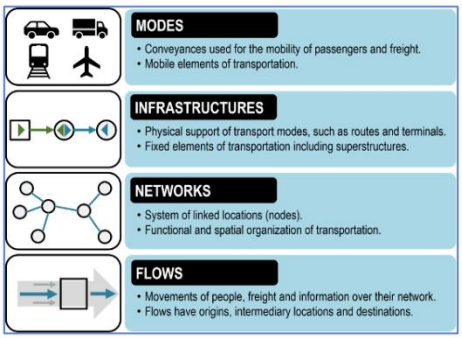


Figure 1: Core components of transportation [3]

AI **works with large datasets, data streams, images, video data, and weakly structured data** and these data are obtained from IoT sensors, traffic counters, toll systems, and machine vision equipment.

In traffic and transportation research, **AI models are basically of two kinds** depending on their intended use: **predictive models**, are mostly motivated by economic factors, **interpretative models**, used in understanding complex systems, such as ITS, traffic systems, passengers' behaviour and others.

Some critical aspects of AI are that the learning process for **advanced processing and predictive models** do not require supervision by data analysts or engineers and the resulting applications can use learning patterns observed automatically from data. Furthermore, one of the critical points of the application workflow for AI-based solutions is that they can be influenced by data during the learning and operational phases. For this reason, the **sole implementation of an artificial intelligence model is not possible but applications by their nature require constant improvement and adaptation to new inputs/data**. This improvement process is essential for the overall security and resilience of AI-based transportation solutions.

---

[212] University Science Park, University of Zilina, Slovak Republic

[213] M. Niestadt, A. Debyser, D. Scordamaglia, and M. Pape, "Artificial intelligence in transport: Current and future developments, opportunities and challenges," 2019.

A characteristic of the applications of AI in transportation is that they concern **real-life scenarios**. Relevant applications are dealing with public transport (travel times, off-peak vs crowding), traffic flow analysis, parking management, pedestrians' mobility. Applications in this group are strongly connected to **machine vision and IoT technologies** and both, predictive and interpretative approaches. Machine vision solutions are used for **plate and signs recognition and object detection**. They are implemented in infrastructure (cameras) and in the cars for driver's assistance and monitoring. Regarding the **infrastructure** itself, AI based solutions concern road condition monitoring systems and includes points cloud processing (lidar data), sensors data analysis. Other topics are accidents and safety, freight distribution and logistics, security and resilience.

2. AI ALGORITMS IN TRANSPORTATION

AI algorithms are distinguished by their use of existing data, which contains the resulting decisions based on inputs/factors. Large datasets are almost always used as input data, and the ability to acquire and process large amounts of data has led to massive advancements in the field of AI. Thus, in principle, collecting and storing large amounts of data is a prerequisite for deploying AI-based solutions, as is the process of analysing and then processing it into a form suitable for a given AI algorithm or group of algorithms. Currently, the main areas of deploying AI algorithms in transportation are:

vehicle control: related to automated (semi-autonomous) or autonomous driving.

ITS: predicting future traffic conditions based on data processing from sensors located in the infrastructure;

public transport: for sustainable mobility given the universe of behavioural inputs;

planning, decision-making, and management: for a more efficient use of existing infrastructure to respond to traffic demand.

Automated and autonomous driving is tightly connected to AI. The goal is to improve the overall productivity of transport/transportation and at the same improve safety.

For **the field of ITS**, the combination of technologies and communication systems is specific. Algorithms lead to prediction and detection models aimed at better predicting traffic density, traffic conditions and incidents to solve problems that are difficult to solve with classical methods of optimization, planning and management. Due to the extreme complexity of such systems, **solutions based on deep learning** are deployed in order to achieve as many interconnected transport systems as possible, which can be managed as a single unit. The use of **multi-level neural networks** for system control is the basis, various subsystems can be optimized using proprietary methods, such as artificial neural networks for light signalling control. Good results are also achieved by using learning systems with feedback (reinforcement learning).

Extensive research is underway in the area of the **use of neural networks** also for planning road infrastructure, public transport, incident detection and traffic situation prediction and a wide variety of supervised and unsupervised learning methods are use:

supervised learning methods including methods of support vectors (SVM - Support Vector Machine), probabilistic neural networks (PNN - Probabilistic Neural Networks), k-Nearest Neighbours (KNN - K-Nearest Neighbours) and also decision trees (Decision Trees);

the **use of fuzzy logic** (FLM - Fuzzy Logic Model) is suitable for finding the shortest path and can be compared with the results obtained using logistic regression models[214] [215].

The **design and development of the infrastructure** is critical due to the number of limiting conditions, the assumption of further expansion and also the necessity of constant assessment of the impact of infrastructure on all aspects of the transport, living, social and economic environment. The research focused also on the use of parallel neural networks and the growing volume of data available in the planning process has led to the adaptation of machine learning methods for pattern recognition in data.

Incident detection is a separate category where AI algorithms are applied. It should be noted that, in addition to the actual detection of incidents, the deployment of AI in the area of so-called **near-miss incidents**, i.e., situations where the incident did not actually occur, but the indicated event may lead to it. Algorithms from the field of neural networks are used in the given area, for example classifying neural networks, algorithms for object detection in real time [216], but also procedures from the field of simulation and analysis of social media.

3. MACHINE LEARNING IN ITS

The goal of machine learning is to get computers to learn from the data you give them. Instead of writing code that tells the computer what to do, your code gives the computer an algorithm that changes based on examples of how it should act. The employment of AI and machine learning in ITS involves massive data processing, evaluating large-scale complex systems, maintaining models for traffic optimization, enhancing safety, and enhancing the flow of transport. The following list provides an overview of the AI techniques most frequently used in ITS (**Figure 2**):

- supervised learning methods: classification, regression
- unsupervised learning methods: clustering, dimensionality reduction, data visualization
- reinforcement learning: intelligent agents, navigation and autonomous drive

Machine Learning	**Supervised Learning**	Regression	trip generation, traffic modes estimation, forecasting
		Classification	image classification, fraud detection, diagnostics and maintenance
	Unsupervised Learning	Clustering	recommender systems, customer segmentation, targeted marketing
		Dimensionality Reduction	main feature identification, input factors compression, structure discovery
		Data Visualization	big data visualization, data interpretation and understanding, reporting and dashboards
	Reinforcement Learning	Intelligent Agents	skills acquisition, real-time decision
		Navigation and Autonomous Drive	robot navigation, learning tasks

Figure 2: Machine learning methods in ITS

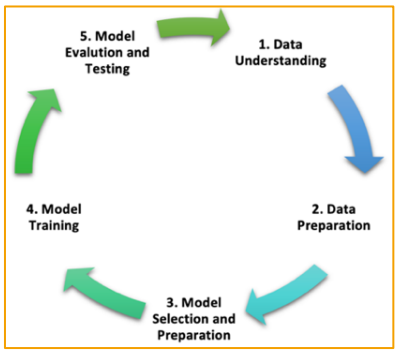


Figure 3: Machine learning workflow (lifecycle)

[214] R. Abduljabbar, H. Dia, S. Liyanage, and S. A. Bagloee, "Applications of artificial intelligence in transport: An overview," *Sustainability (Switzerland)*, vol. 11, no. 1. 2019. doi: 10.3390/su11010189.
[215] M. Machin, J. A. Sanguesa, P. Garrido, and F. J. Martinez, "On the use of artificial intelligence techniques in intelligent transportation systems," *2018 IEEE Wireless Communications and Networking*
[216] B. Bučko *et al.*, "Computer Vision Based Pothole Detection under Challenging Conditions," 2022, doi: 10.3390/s22228878.

A trained model is the program that is made up of the algorithm and the learned parameters that go with it (**Figure 3**):

Data understanding, an important prerequisite for the implementation of AI algorithms is the quality of the data entering the process of model preparation and learning. Data preparation involves the elimination of extraneous data, data consolidation, and data augmentation based on the anticipated result of data processing by AI algorithms;

Model development, the next step in getting the final model based on the AI is the learning process, which is often called "model training." This is part of the group of algorithms that belong to the field of machine learning. This is a very important step in preparing a model because it defines the desired output, the AI algorithm that goes with it, and the data representation in the form of a model. Model evaluation is a step that goes right along with it because the set of data used in the learning process can change the way the model turns out. The expected quality of the final model (model accuracy) is evaluated, and model performance criteria are set based on how the model will be used in the real world;

model integration and improvement, when there is a need to make changes to an existing model, the model improvement process is used and it may be necessary to change the learning algorithm or update the model.

4. AI MODELS

AI modelling is definition/creation, training, evaluation and deployment of machine learning algorithms to emulate logical decision making based on input data. The critical part of the process is the learning phase based on data. In principle, bad or incorrect data forms only bad or incorrect results and there is no other way to create good AI model than to feed it with good data. Specific modelling techniques are more suitable for one type of problems and less for other one:

linear regression (LR) is a **machine learning algorithm based on supervised learning**. Regression models are used for prediction by computing linear coefficients predictor function. LR is simple to use and very easy to interpret coefficients found by the model. Transportation problems that are suitable for LR application involve: trip generation, traffic modes determination, forecasting;

algorithms based on biological concepts based on evolutionary biology and evolution of biological systems. Some implementations are **inspired to living species ant their behaviour**, such as ant colony optimization (ACO), bee colony optimization (BCO), others are inspired by biological mechanisms such as artificial immune system (AIS) or genetic algorithms (GA). Transportation problems using biologically motivated algorithms are: scheduling, routing, optimization;

cellular automatons (CA) are evolving grid-based computational systems which model complexity growth. Basically, cellular automatons are **chaotic, one-way patterns that change over time**. The rules of evolution are very basic and easy to understand. However, evolution leads to structures and behaviors that are very complicated. CA have been used as models to show how physical chaotic systems get more complicated and how simple laws can lead to symmetry. The major disadvantages of CA include limited number of reversal rules and inability to produce long sequences of states. This can lead to less accurate results for high density traffic models. Applications of CA in transportation includes: road planning, traffic and pedestrian flow modelling, modeling of dynamical tendencies of traffic;

artificial Neural Networks (ANN) is made up of a **group of connected units, or nodes, called artificial neurons**. These artificial neurons are similar to the **neurons in a real brain**. Like the synapses in a real brain, each connection can send a message to other neurons. An artificial neuron takes in signals, processes them, and then sends out signals to other neurons that are connected to it. The "signal" at a connection is a real number, and each neuron's output is calculated by a function that is not linear in terms of the sum of its inputs[217]. The ANN concept is **very powerful and has significant place in transportation solutions**, but has some significant drawbacks. ANN are hardware dependent and require parallel processing units, mostly graphics processing units. They need significant amount of memory to estimate weights of complex network structure and a relevant overall training time necessary for the learning. ANN are referred as black box solution and without additional complex methods is difficult to explain, how the solution was obtained. Transportation applications benefit from ANNs in: planning (trip generation, O-D distribution), operation and control (traffic pattern recognition), construction and maintenance;

Generative adversarial networks (GANs) has a capability to produce augmented and synthetic data. Despite the existence of multiple data sources and storage systems, the availability of original non-aggregated data is problematic due to its time-limited existence, overall size, and the possibility of unambiguous interconnection with other generated data sources. Synthetic data for transport problems are created considering specific needs or a description of certain scenarios that may not be present in the original, actual data. The main problem with GANs comes with the training process. Data must be provided continuously to evaluate accuracy of the model and the overall model preparation is very complex. Applications of GANs for the transportation are in: data synthetization/generation, optimization.

5. SECURITY IN ITS AND AI

Taking into account the different nature of the systems deployed in different parts of the infrastructure, in the process of planning, management, communication and data archiving, **security requirements** can be perceived from two fundamental points of view. The first is the classic **view of an intelligent system**, specifically for the field of transport and infrastructure, which follows the division with respect to individual parts of the integrated system and specific elements. It is possible to perceive, for example, infrastructure as a part defined by building elements and a part consisting of monitoring and other systems working with data. The second view is more focused on the nature of the **changes perceived by the transport participant or the infrastructure operator,** where changes can be monitored from a time point of view and the interval in which the change occurs can be determined. An example is the fact that the change in physical road traffic takes place in the order of months and years, on the other hand, the change in traffic as such is a variable in the order of minutes and seconds.

The mentioned facts lead to the **need to establish security requirements for different types of systems** and also a different way of monitoring potential security problems. The field of security is specific in that it must actively prevent security incidents, establish a clear distribution and assessment of risks for individual parts of systems, and define proactive and reactive procedures

[217] "Artificial neural network - Wikipedia." https://en.wikipedia.org/wiki/Artificial_neural_network (accessed Feb. 27, 2023).

for each potentially identified security problem. Moreover, new security threats can arise that must be responded to.

Security problems with new technologies are appearing in the deployment and use of systems for **automated and semi-autonomous driving and systems** for monitoring traffic in the form of camera systems operating in real time. A challenge is also the direction towards highly optimized and **autonomous solutions working in real time**. Optimizing the infrastructure of electric cars, charging infrastructure, the use of automated and semi-autonomous driving systems brings new problems and challenges that cannot be solved without the integration of data sources and the appropriate level of data and communication security.

The complex multi-layered architecture makes **ITS particularly vulnerable to cyber-attacks**. Threats are potential causes of an incident that can lead to ITS damage that can not only disrupt the operation of the entire city and endanger passengers, but also leak confidential information about organizations and people.

The **connections between systems and the exchange of information** are particularly sensitive from a security point of view. Other **weaknesses that ITS are** wireless and mobile communication,

integration of physical and virtual layers, cooperation between old and new systems, automated systems.

The introduction of AI based technologies introducing new security risks. The critical part of AI model reparation depends on data. Since we are not able to control all the data collected from the infrastructure, we need to adopt new security culture facing the most common data security threats of AI [218] (see more details are in **Appendix 5**):

model poisoning, when an attacker is able to insert false data into the model's training program;

data privacy, if data preparation is in contrast to the regulation of personal data storing (in Europe GDPR);

data tampering, if there is intentional manipulation of training data;

inside threats, insiders often know where sensitive data resides;

deliberate attacks, to disrupt operation based on AI solutions;

AI driven attacks, the attack consists in designing and attacking phases.

Currently, **cyber security is often not considered a significant part of ITS** and various organizations including government agencies, public and private entities pay minimal attention to it. Security and protection are still handled separately in different systems due to lack of security awareness. Overall security and durability of new technologies need to be sufficiently verified in a real environment and by long-term operation.

[218] E. Nick, "Top 7 Artificial intelligence Data Security Threats to AI and ML," *https://www.datasciencecentral.com*, 2022. https://www.datasciencecentral.com/top-7-data-security-threats-to-ai-and-ml/ (accessed Feb. 28, 2023).

APPENDIX 5 - CYBER SECURITY AND ARTIFICIAL INTELLIGENCE RISKS FOR ROAD INFRASTRUCTURE

1. CYBER SECURITY

Cyber-security is aimed at guaranteeing the principles of confidentiality, integrity and availability of information (CIA factors). Given the complexity that the digital ecosystem has now reached, there are countless threats to CIA factors and therefore to data alteration and damage to the systems that manage them. To ensure the optimal maintenance of these factors in an organizational or corporate context, it is necessary to equip oneself with its own IT protection measures, possibly integrated with broader public protection measures.

Cyber-attacks aim to overcome protective software possibly without raising alarms, to enter information networks and databases with different objectives:

- **intrusion into networks and ITS systems, IoT devices and, more recently, AI systems** for interception and modification of data, acquisition of information, theft of sensitive data for ransom, spread of computer viruses or worms;
- **attack to critical infrastructures** through the IT systems that manage critical infrastructures (electricity, transport, gas and oil pipelines, telecommunications network, etc.) or, in the military field, specifically to weapons, command and control and communication systems;
- **vandalism by individual hackers** against servers and web pages;
- **cyber espionage**, as an evolution of traditional espionage;
- **propaganda** for the dissemination of political messages and fake news, especially through social media.

Cyber risk analysis consists in estimating the probability that an adverse event affects the digital system of a user or a company, evaluating both the probability of the occurrence of the harmful event and the consequences of this event on the overall activities of the damaged party. To understand these two elements that make up cyber risk, it is necessary to know the extent and value of the resources managed (data or information), as well as one's vulnerability to cyber-attacks.

The **risk assessment process** can be implemented according to the security risk management criteria of the IT security management system such as that of the ISO 27001 standard. This establishes a periodic review or in any case whenever there are significant technical, regulatory or organizational issues that impact information security risks. The data breach can arise both from human factors (cyber criminals or unprepared or even unfaithful staff) and from technological factors (damaged, obsolete or poorly managed equipment).

Some **examples of some current attack scenarios** are presented in the report of ENISA (2021)[219]:

- **sensor compromise, communication interception, sensor obfuscation and decommissioning:** an attacker can intentionally manipulate AI models by providing incorrect/manipulated data;

[219] ENISA - The European Union Agency for Cybersecurity, "Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving," 2021. https://www.enisa.europa.eu/news/enisa-news/cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving (accessed Feb. 28, 2023).

- **DoS and DDoS attacks:** attacks on the communication channel can cause "blindness" of devices (e.g., autonomous/automated vehicles);
- **manipulation of device and vehicle communication:** modification of sensor values and thereby change the behaviour of artificial intelligence models;
- **information leakage:** can lead to serious disruption of systems.

Considering the concept of cyber risk described previously, it is clear that the evolution of the network and services available online introduces a constantly growing level of complexity.

Different technologies based on various industry standards and proprietary protocols, make **ensuring cyber security in new technologies and in particular ITS systems** a quite complicate task. All telematics systems as well as smart technologies often use computerized control systems to monitor and manage technical assets and operations. All these limits the possibility of detecting cyber security incidents and conducting audits. Finally, the current life cycle of technologies, ITS systems and devices usually exceed the life cycle of standard IT components.

Cyber-attacks have therefore grown through **intelligent technologies interconnected via high-speed fixed and mobile networks**. The increasingly widespread adoption of the Internet of Things (IoT) and technologies useful for family and business life has amplified the application of these technologies. However, this was not followed by an increase in awareness of the need for IT security. An example is the **increasingly required integration of monitoring and control systems through IoT networks**. Devices and sensors for such networks are relatively inexpensive, but this, on the other hand, brings the problem of limited device resources to implement a sufficient level of security of such elements. The change is not simple since it requires either the use of more expensive devices or a complete change in the approach of device manufacturers to security (currently largely left to the solution implementer without direct support in the devices).

In the era of artificial intelligence (AI), **ITS in road infrastructure** is becoming increasingly important as it enables the seamless integration of vehicles, infrastructure, and data to create a more intelligent and connected transportation network. This includes the use of sensors, cameras, and other monitoring devices to collect real-time data on traffic conditions, as well as the implementation of smart traffic management systems that can analyze this data and adjust traffic signals and other infrastructure elements accordingly.

In **new intelligent infrastructure** some new requirements are identified:

- more complex results (answers) from analytical systems;
- very quick answers (near-real-time results);
- visual and contextual analysis;
- AI based solutions for data processing.

All of the identified new requirements are based on the **increasing amount of data we** are collecting, and these new requirements are largely linked to the process of obtaining new sophisticated results for decision-making.

2. CYBER SECURITY THREATS ASSOCIATED WITH DATA AND AI

Models aimed at interpreting the behaviour of systems are currently emerging with the consequent expansion of models using machine learning and deep learning methods. **Machine learning process** is based on model preparation usually trained on large amount of data. This

process is a crucial step in the development of predictive models and is highly affected by data itself. It involves a series of tasks and techniques aimed at getting the data ready for training the model effectively.

The most common security threats associated with data are:

- **model poisoning,** a poisoning attack (or dirty data attack) occurs when an **attacker is able to insert false data into the model's training program**, causing it to incorrectly learn something. The most frequent consequence of a poisoning attack is that the model's boundary shifts, which will cause the model to misclassify the data and make undesirable decisions. Model poisoning attack is typical for models with natural tendency to overtraining;
- **data privacy**, since AI needs significant amount of data for training, it requires **data preparation and storage for longer time period and not always the final result is predictable**. This also contrasts with the regulation of personal data storing (in Europe GDPR). One of the solutions proposed in this article is the use of synthetic data, but this kind of approach is not suitable for all the transportation problems mentioned;
- **data tampering**, it describes the **intentional manipulation of training data** to influence the decision of the algorithm. This kind of threat is almost impossible to detect and even the small amount of tampered data has a huge impact on decision accuracy;
- **inside threads**, insiders often know where **sensitive data resides within an organization** and typically have increased levels of access, regardless of whether they have malicious intent. Since this problem is common for all the systems, it must be considered seriously for AI solutions as well due to the high dependency on data;
- **deliberate attacks**, a deliberate attack on AI systems can disrupt operation based on AI solutions. This kind of attack is quite **straightforward in AI based solutions** since bad or corrupted data will cause overall AI based system malfunction. The main motivation factor is competitive advantage or sabotage and transportation systems, if they are not working properly, could cause chaos and catastrophes;
- **AI driven attacks**, they are a very sophisticated type of cybersecurity threat. Since the attack itself consists of design and attach phases, **AI can be used in design and attack phase to support attacker's needs.** AI based transportation solutions, as well as other industrial solutions, must be designed as safe for the current and future threats;

3. THE ADVERSARIAL AI ATTACK

One of the most common attacks on AI by using data is the **adversarial AI attack to AI systems** [220]. This is a type of cybersecurity threat that targets artificial intelligence systems eventually involving another AI. The target is to intentionally manipulating or deceiving other systems to produce incorrect or harmful outcomes. The goal of such attacks is to exploit vulnerabilities or weaknesses in the AI system's algorithms, data, or decision-making processes.

[220] The next example is based on the article of *Dave Gershgorn - Fooling the machine (The Byzantine science of deceiving artificial intelligence)* available online at https://www.popsci.com/byzantine-science-deceiving-artificial-intelligence/

Adversarial AI attacks can take various forms and can be executed through different means. One common approach is **to introduce specially crafted inputs or data into the AI system**. These inputs are designed to mislead the system and cause it to make incorrect predictions, classifications, or decisions. For example, an attacker might modify or manipulate images, text, or other types of data to deceive an AI system into misidentifying objects, misclassifying information, or making false judgments.

Another method of adversarial AI attack involves **perturbing or modifying existing data to subtly change its features or characteristics.** These modifications are often imperceptible to human observers but can significantly impact the AI system's performance. By introducing small changes to the input data, an attacker can manipulate the system's output and potentially exploit it for malicious purposes.

Adversarial AI attacks can have serious consequences in various domains. In the context of autonomous vehicles, for instance, an attacker could **manipulate traffic signs or road markings** in a way that confuses the AI system, causing it to misinterpret or ignore crucial information. This could lead to accidents or disruptions in traffic flow.

4. HOW TO FOOL AI?

The main aspect of problems with AI is clearly defined Dave Gershgorn – "An accelerating field of research suggests that most of the **artificial intelligence** we've created so far has learned enough to give a **correct answer**, but **without truly understanding the information**."

Let's have the following scenario to fool neural network with adversarial attack to modify the decision process of neural network to cause misclassification of traffic sign (**Figure 1)**.

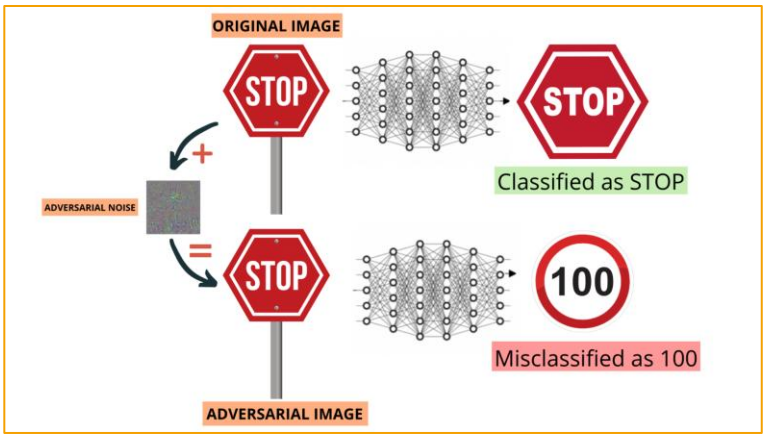


Figure 1: Adversarial attack on neural network scenario[221]

The mechanism of the attack is demonstrated by following **Figure 2**, where on sides we see the same image. The image itself can be represented by numbers defining colors (and intensity) for each displayed pixel.

[221] Dave Gershgorn - Fooling the machine (The Byzantine science of deceiving artificial intelligence) available online at https://www.popsci.com/byzantine-science-deceiving-artificial-intelligence/

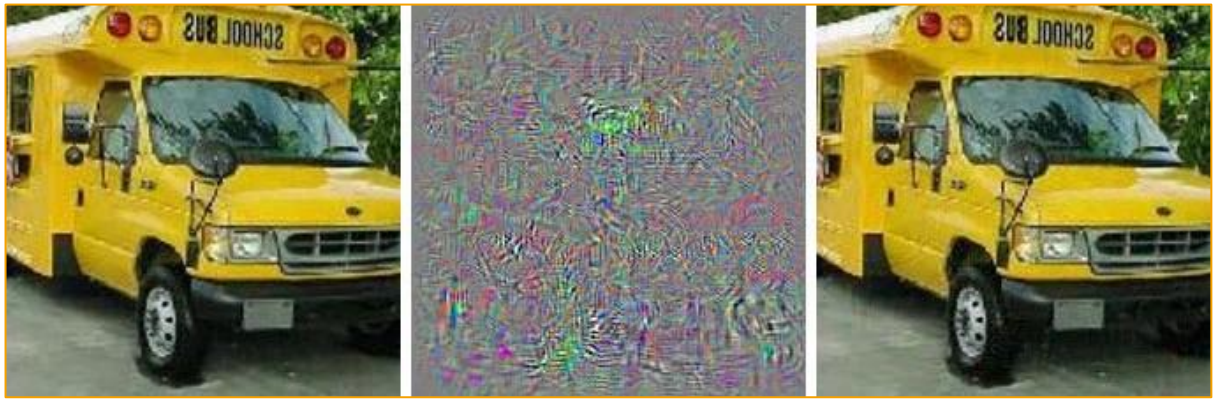


Figure 2 - The left image is unaltered and would be classified as a school bus, while the right would be classified as an ostrich. The middle image shows the distortions made to the adversarial example.

Since the resolution of the image allows to **"hide" some pixels** into the original image without noticing by human eye, some additional noise (middle image) can be added to the original left image.

The right image looks same as the left one. The result for the classification is **"bus" for the left, original image and "ostrich" for the right image** modified by the noise which looks same for human eyes.

The presented situation with the bus misclassification seems to be not very dangerous. The problem is when the same approach is applied to part of the traffic infrastructure – e. g. on traffic signs. The result of such misclassification is presented in **Figure 3** where traffic signs are misclassified to the different categories. Interesting is the fact that the misclassified signs are totally different in color, shape, and meaning!

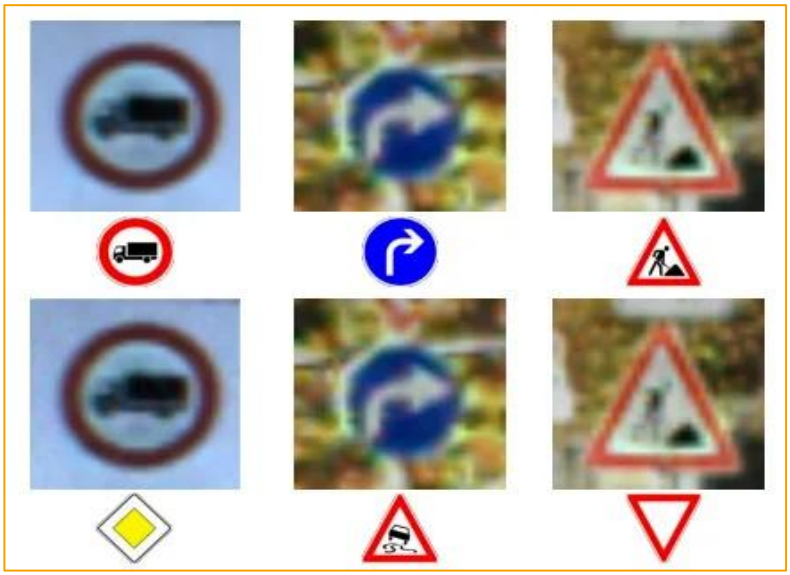


Figure 3 - Misclassified traffic signs – top row shows original signs, bottom signs classified by AI.

As seen the top row shows the original image with the corresponding classification. **The bottom row shows that the network was successfully tricked into thinking each sign was different from the original.** Here the consequences are far worse than for the previous example with the bus. [222]

The situation is very tricky with the AI model used for the mentioned misclassification example. We can summarize some of the observations as follows:

1. Instead of taking control of an infrastructural component, this method injects specific kinds of hallucination — **images that aren't really there**.
2. These attacks use **adversarial examples**: images, sounds, or potentially text that seems normal to human viewers, but are perceived as something else entirely by machines. Small changes made by attackers can force a deep neural network to draw incorrect conclusions about what is being shown.
3. "*Any system that uses machine learning for making security-critical decisions is potentially vulnerable to these kinds of attacks*," said Alex Kantchelian, a researcher at Berkeley University who studies adversarial machine learning attacks.
4. By altering the images fed into a deep neural network by just four percent, researchers were able to trick it into **misclassifying the image with a success rate of 97 percent** (black box attack on a deep learning system).

5. NIS 2 EU DIRECTIVE AND OTHER REGULATIONS

One of the most actual regulations in cyber security is the **NIS 2 EU directive**[223] to enhance the cybersecurity and resilience of critical infrastructures and digital services within the European Union, as the **update of the previous directive of 2016 which entered into force in 2018**. The directive establishes requirements and obligations for both public and private entities operating in the sectors of energy, transportation, finance, healthcare, and digital platforms.

NIS 2 EU directive aims to improve the cooperation and coordination among EU member states in responding to cybersecurity incidents and threats. It promotes the establishment of national cybersecurity strategies and the creation of Computer Security Incident Response Teams (CSIRTs) in each member state. The directive also emphasizes the importance of risk management and the implementation of appropriate security measures. It encourages the use of best practices, standards, and certifications to enhance the cybersecurity posture of organizations. It also requires organizations to report significant cybersecurity incidents to the competent national authorities.

The directive introduces new provisions to address emerging technologies and challenges in the digital landscape. It focuses on areas such as cloud computing, artificial intelligence, Internet of Things (IoT), and 5G networks. It aims to ensure that security considerations are integrated into

[222] An Israeli software house has made available to customers - government entities involved in national security - an app called TOKA which is capable of modifying video images in real time, both live and recorded, for example changing the faces of the people appear there, or by erasing the presence of subjects filmed by the cameras.
[223] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

the design and development of these technologies. Many countries have other specific regulations and directives related to cybersecurity and the transport sector[224]:

- **United States**: the US Department of Transportation (DOT) has implemented various directives and regulations to enhance cybersecurity in the transport sector. For example, the Federal Motor Carrier Safety Administration (FMCSA) has guidelines for securing commercial motor vehicles and their electronic systems. Additionally, the National Highway Traffic Safety Administration (NHTSA) has regulations concerning cybersecurity in the automotive industry;
- **European Union**: apart from the **NIS 2 EU directive**, the European Union has other regulations and directives that focus on cybersecurity in the transport sector. For instance, the General Data Protection Regulation (GDPR) sets standards for protecting personal data, including data collected by transport systems. The European Union Agency for Railways (ERA) also has regulations related to cybersecurity in the rail transport industry.

  Recently, on **December 9, 2023**, **the European Union approved an agreement on the Artificial Intelligence Regulation** which adds the world's first rules for AI to fully reap the benefits of innovative new products and avoid abuse and uncontrolled use of artificial intelligence. The approved draft regulation deals with harmonized rules on artificial intelligence that aim to ensure that AI systems placed on the European market and used in the EU are safe and respect fundamental rights and EU values;
- **Australia**: the Australian Cyber Security Centre (ACSC) provides guidelines and recommendations for enhancing cybersecurity in the transport sector. These guidelines cover various aspects such as securing networks, protecting critical infrastructure, and ensuring secure communications in the transport industry.
- **Japan**: the "Act on the Protection of Personal Information" (APPI) applies to safeguard personal data, and also to the transport sector. The Ministry of Land, Infrastructure, Transport and Tourism (MLIT) has implemented regulations for securing transportation systems and ensuring the privacy and security of user data.

6. FINAL CYBERSECURITY RECOMMENDATIONS

Some recommendations as in the following **Table 1** can help **enhance the cybersecurity of road infrastructure** and mitigate the risks of cyber threats and attacks in particular to road infrastructure and transportation services.

By using products, systems and services that use artificial intelligence (AI), the **security risks associated with it must be managed**. On the other hand, a road administration (RA) will be able to **benefit from increasingly integrating activities and functions related to artificial intelligence** into its security risk management processes. To assist RAs in this regard, the basic reference is **ISO 31000:2018** integrated by **ISO 22989:2022** ***Information technology — Artificial intelligence — Artificial intelligence concepts and terminology***. Recently, the **ISO 23894:2023** ***Information***

[224] See also UK Parliament, House of Lords Library, "Artificial intelligence: Development, risk and regulation", Published 18 July, 2023. https://lordslibrary.parliament.uk/artificial-intelligence-development-risks-and-regulation/

technology — Artificial intelligence — Guidance on risk management provides assistance in risk management processes with the use of AI, by providing broad-spectrum specialist support in policies, procedures and practices, communication and consultancy activities, in the definition of the context and in the evaluation, treatment, monitoring, review, recording and reporting of risk. It also identifies sources of risk relating to AI.

Recommendation	Description
Implement robust access controls and authentication measures	Utilize strong passwords, multi-factor authentication, and role-based access controls to ensure that only authorized individuals have access to critical systems and data. Regularly review and update access privileges to prevent unauthorized access.
Regularly update and patch software systems	Keep all software and firmware up to date with the latest security patches and updates. Vulnerabilities in outdated software can be exploited by cybercriminals to gain unauthorized access or launch attacks. Establish a patch management process to ensure timely updates.
Conduct regular security assessments and audits	Regularly assess the cybersecurity posture of road infrastructure systems through penetration testing, vulnerability scanning, and security audits. Identify and address any vulnerabilities or weaknesses in the system promptly.
Establish incident response plans	Develop and implement incident response plans that outline the steps to be taken in the event of a cybersecurity incident. This includes procedures for detecting, containing, and mitigating the impact of a breach or attack. Regularly test and update these plans to ensure their effectiveness.
Provide ongoing training and awareness	Educate employees and stakeholders about cybersecurity best practices, such as identifying and reporting suspicious activities, practicing good password hygiene, and being cautious of phishing attempts. Regularly conduct training sessions and awareness campaigns to reinforce cybersecurity practices.
Implement encryption and data protection measures	Encrypt sensitive data in transit and at rest to protect it from unauthorized access. Utilize encryption protocols and secure communication channels to ensure the confidentiality and integrity of data exchanged within the road infrastructure.
Monitor and log system activity	Implement robust monitoring and logging mechanisms to detect and respond to suspicious activities or unauthorized access attempts. Regularly review logs and monitor traffic patterns to identify any potential security breaches or anomalies.
Maintain backups and disaster recovery plans	Regularly backup critical data and establish robust disaster recovery plans to ensure business continuity in the event of a cyber incident. Test backup systems and recovery procedures to verify their effectiveness.
Collaborate with cybersecurity experts and organizations	Engage with cybersecurity professionals, industry associations, and government agencies to stay updated on the latest threats, trends, and best practices. Collaborate with relevant stakeholders to share information and enhance the collective cybersecurity posture of road infrastructure. Implement guidance as in the standards ISO 31000:2018 *Risk management*, ISO 22989:2022 *Information technology – Artificial intelligence* and ISO 23894:22023 *Information technology – Artificial intelligence – Guidance on risk management.*

Table 1: Cybersecurity Recommendations for Road Infrastructure

7. BIBLIOGRAPHY IN THE FOOTNOTES

The following documents represent the bibliography reported in the footnotes of this Report.

They are indispensable for its reading. For the dated references, the edition cited applies. For the undated references, the latest edition of the referenced document (including any amendments) applies.

Note n.	Bibliography
1	PIARC, "PIARC TF 3.1 – Literature Review – Documents Relevant to Road Infrastructure and Transport Security", report 2022R07EN, ISBN 978-2-84060-682-6.
2	PIARC, "Security of Road Infrastructure", Final report of the Task Force C.1., report 2019R12EN, Paris, France. ISBN 978-2-84060-524-9. Available in English, French and Spanish. https://www.piarc.org/en/order-library/30826-en-Security%20of%20Road%20Infrastructure
3	PIARC "Covid-19: Initial Impacts and Responses to the Pandemic from Road and transport Agencies", PIARC Covid-19 Response Team, report 2020BN03EN, ISBN 978-2-84060-628-4.
5	Palchetti S., Mastrangelo R., Bianchi M., "Security and Pandemic: Application of the Concepts of Resilience for Business Continuity", PIARC XVI World Winter Service and Resilience Congress - Calgary 2022. See it in LR as Sheet n.3 in Appendix B.7.
7	PIARC – The World Road Association, "Strategic Plan 2020-2023", Update October 2020, http://www.piarc.org
9	ISO 28000:2007 - Specification for security management systems for the supply chain (revised in 2022)
10	Deming W. E., "Out of the Crisis", MIT Press, 1986.
11	"Protective Security Management Systems (PSeMS)", by the Centre for the Protection of National Infrastructure, CPNI (UK), 2018.
12	ISO Guide 73:2009 "Risk management – Vocabulary" (now ISO 31073:2022).
13	ISO 31000:2018 - Risk management - Guidelines
14	ISO 9001:2008 – Quality management systems - Requirements
16-17-18	ISO 31010:2019 - Risk management – Risk assessment techniques
22	Hubbard, D. W. "The Failure of Risk Management", Wiley, 2009, 2nd edition 2020.
23	UNI – Italian National Standards Body - 10459:2017 - Non-regulated professional activities - Security professional - Knowledge, skill and competence requirements.
27	Taleb, N. N. "The Black Swan: The Impact of the Highly Improbable", 2007.
29	Orwell G., "Nineteen eighty-four – A novel", Secker & Warburg, 1949.
29	Camus A., "La Peste" (The Plague), Gallimard, 1947.
30	Palchetti S. and Scala A., "The Difficulties of Risk Assessments for Complex Network Infrastructure: Applications to the Security and the Resilience of Road Infrastructure", Prague PIARC WRC, 2023.
33	Hegel W. F., "Doctoral Dissertatio : Contradictio est regula veri, non contradictio, falsi", 1801.

35	Garzia F., “An integrated multidisciplinary model for security management and related supporting integrated technological system”, Proc. of IEEE International Carnahan Conference on Security Technologies, Orlando (USA), pp. 107-114, 2016, DOI: 10.1109/CCST.2016.7815690.
37	Biasiotti A., “Gli impianti di videosorveglianza” (Video surveillance systems), EPC, Italy, 2019.
40	European Parliament, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
41	Kraus L. M., “The Physics of Climate Change”, 2022.
44	UN Convention to Combat Desertification, Sustainability, Stability, Security”, www.unccd.int/sustainability-stability-security.
45	Allianz Risk Barometer 2022, www.agcs.allianz.com.
51	Schweitzer, A. “Die Ehrfurcht vor dem Leben: Grundtexte aus fünf Jahrzehnten” (The reverence for life: basic texts from five decades), Beck, 2020.
52	Pope Francis, Ecyclical “*Laudato Si*’”, 2015.
53	PIARC, “International Climate Change Adaptation Framework for Road Infrastructure “, report 2015R03EN.
54	HB 167:2006 Security risk management standard, Australia and New Zealand
55	PIARC, “Adaptation Methodologies and Strategies to Increase the Resilience of Roads to Climate Change – Case Study Approach”, report 2019R25EN, 2019.
56	PIARC, “Terminology on Resilience and Coordination with Related PIARC Technical Committees”, TC 1.4 Climate Change and Resilience of Road Networks, report 2021BN1.4EN.
57	IPCC 2019, Refinement to the 2006 IPCC Guidelines for National Greenhouse Gas Inventories, https://www.ipcc.ch/report/2019.
57	UNDRR, 2017 Global platform for disaster risk reduction: Proceedings, undrr.org/publication.
59	Trombetta M.J., “Environmental security and climate change: analyzing the discourse”, Delft University of Technology, Cambridge Review of International Affairs, 2009.
68	IWA 42: 2022 "Net zero guidelines", ISO, 2022.
72	Leonida G., “Dizionario della Logistica” (Dictionary of logistics), 2023.
73	PIARC, “Truck-Traffic on Highways for Sustainable, Safer and Higher Energy Efficient Freight Transport”, report 2019R23EN.
74	PIARC, “National Policies for Multi-Modal Freight Transport and Logistics”, report 2019R24EN.
79	European Parliament, TRAN Committee, “The impact of emerging technologies on the transport system”, European Commission, Policy Department for Structural and Cohesion Policies Directorate-General for Internal Policies - November 2020.
79	ADR Code, “European agreement concerning the international carriage of dangerous goods by road”, 2005.
79	Paval F., Palchetti S., “Current road security problems in the Romanian territory due to the illegal transport of dangerous goods”, PIARC WRC, Prague, 2023.

90	A. Seth, “Being you. A New Science of Consciousness”, 2021
91	The Highway Code, www.highwaycodeuk.co.uk, updated 27/07/2022.
93	PIARC, Road Safety Manual, October 2019, online on: https://roadsafety.piarc.org/en.
96	PIARC, Implementation of National Safe System Policies, 2019, report 2019R39EN.
97	PIARC, Road Safety - Case Studies Catalogue, 2019, report 2019R47EN.
99	SAE, Society of Automotive Engineering, https://www.sae.org.
100	A. Cappellini, “Machina Delinquere Non Potest. Brief notes on artificial intelligence and criminal liability”, Criminalia, 2019.
101	EU, European Commission Directive n.40 2010/22/EU “A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility”, COM/2016/0766 final, 15/03/2010.
105	P. Chanard, “Fight Against Vandalism” and “Vandalism survey results”, PIARC 2021; “Good Practices and Tips to Limit Theft and Vandalism of Road Assets”, PIARC World Road Congress, Prague, Czech Republic, 2023.
106	PAS 1885, “The fundamental principle of automotive cyber security. Specification”, 2018.
106	ISO/SAE International Standard 21434, “Road Vehicles – Cybersecurity engineering”.
106	“A Code of Practice: Automated Vehicle Trialling – Guidance”, UK Department of Transport, January 2022.
106	“Cybersecurity Best Practices for the safety of Modern Vehicles”, 2022, National Highway Traffic Safety Administration NHTSA, U.S. Department Administration.
114	AASHTO, “Fundamental Capabilities of Effective All-Hazards Infrastructure Protection, Resilience, and Emergency Management for State Departments of Transportation”, American Association of State Highway and Transportation Officials, Washington, 2015.
116	J. Manterola, La obra de ingenierìa como obra de arte, Fundacion Arquitectura y Sociedad, Ed. Laetoli, Pamplona, 2010.
117	Highways England, “CD 350 The Design of Highway Structures”, Design Manual for Roads and bridges, Rev. 0, 2020.
118	Bridge Engineering Handbook, edited by Wai-Fah Chen and Lian Duan, Boca Raton: CRC Press, 2000.
118	AASHTO, “Standard Specifications for Highway Bridges”, Washington, D.C., 18th Ed. 2014.
120	Highways England, “CD 351 The Design and Appearance of Highway Structures”, Design Manual for Roads and bridges, Rev. 0, 2020.
121	Garlock, M., Paya-Zaforteza, I., Kodur, V., and Gu, L., “Fire hazard in bridges and repair strategies, Engineering structures”, 35, pp. 89-98, 2012
121	Hu, J., Carvel, R. and Usmani, A., “Bridge fires in the 21st century: A literature review”, Fire safety journal, 126, 2012.
121	Lee, G.C, Mohan, S., Huang, C. and Fard, B.N., “A study of US bridges failures (1980 – 2012), 2013, Buffalo, NY.

127	European Council Directive 2008/114/EC, “Procedures for the identification and designation of European Critical Infrastructure”, 2008.
133	Franchini A., “Sicurezza antincendio di ponti: perché conta e come ottenerla” (Fire safety of bridges: why it matters and how to get it), Antincendio, EPC Editore, Roma, Italy, 5, 2023.
136	PIARC, “Improving Road tunnel resilience, considering safety and availability. A PIARC briefing note including a collection of case studies”, report 2022R04EN, 2022.
137	PIARC, “Road tunnels: complex underground road networks”, report 2016R19EN.
137	PIARC, “Design fire characteristics for road tunnels”, report 2007R01EN.
137	PIARC, “Experience with significant incidents in road tunnels”, report 2017R35EN.
137	PIARC, “Large Underground Interconnected Infrastructure”, report 2019R42EN.
137	PIARC, “Prevention and mitigation of tunnel-related collisions”, report 2019R03EN.
137	PIARC, “Introduction to the RAMS concept for road tunnel operations”, report 2019R05EN.
137	PIARC, “Road tunnel operation: first steps towards a sustainable approach”, report 2017R02EN.
137	PIARC, “Best practice for life cycle analysis for tunnel equipment”, report 2016R01EN.
137	PIARC, “Recommendations on management of maintenance and technical inspection of road tunnels”, 2report 2012R12EN.
137	PIARC, “Good Practice for the Operation and Maintenance of road Tunnels”, report 2004/05.13.EN.
138	PIARC, "Life cycle aspects of electrical road tunnel equipment”, report 2012R14EN.
138	PIARC, "Best practice for life cycle analysis for tunnel equipment", report 2016R01EN.
139	PIARC, “Road Tunnels: Complex Underground Road Networks”, report 2016R19EN.
140	European Union, Directive 2004/54/EC “Minimum safety requirements relating to the infrastructure and operation of road tunnels of the trans-European network longer than 500 meters”, 2004.
143	PIARC, “Risk analysis for road tunnels”, report PIARC 2008R02.
144	PIARC, “Current practice for risk evaluation for road tunnels”, report PIARC 2012R23EN.
146	ENISA - European Union Agency for Cybersecurity - “Guideline on security measures under the EECC”, July 2021.
150	ISO 22300:2018, “Security and Resilience – Vocabulary”, 2018.
152	Park, Jeryang, et al.,"Integrating risk and resilience approaches to catastrophe management in engineering systems." Risk analysis 33.3, 2013.
154	Flammini F., Setola R., and Lollini F., "Resilience Engineering and Risk Management," in Resilience Assessment and Evaluation of Computing Systems, Springer, 2012.
155	Yu, David J., et al., "Toward general principles for resilience engineering.", Risk Analysis 40.8, 2020.
164	The National Institute of Justice (USA), Mass Attacks Defence Toolkit 2, https://www.rand.org/pubs/tools/TLA1613-1.html.

168	A. Gandolfi, Formicai, imperi, cervelli - Introduzione alla scienza della complessità (Anthills, empires, brains - Introduction to the science of complexity), Bollati Boringhieri, 1999.
169	G. Parisi, “In un volo di storni. Le meraviglie dei sistemi complessi” (In a flight of starlings. The wonders of complex systems), Rizzoli, 2021.
170	L. von Bertalanffy, General System theory: Foundations, Development, Applications, ILI, 1968.
172	S. Pahwa, C. Scoglio, A. Scala, Abruptness of cascade failures in power grids, Scientific reports, 2014.
173	G. Caldarelli, Without equal. Understanding with networks a world that has no precedent, Egea, 2022.
177	G. D'Agostino, A.Scala, Networks of networks: the last frontier of complexity, Vol. 340. Berlin: Springer, 2014.
179	Complexity and Management – Interview with prof. Alberto Felice De Toni di Enrico Laurenti, July, 2021.
185	C. K. Chang and R. C. Chang, "An Overview of Vulnerability Analysis in the Field of Cybersecurity," Journal of Information Security, vol. 10, no. 5, pp. 279-291, Sep. 2019.
191	H.Mintzberg, The structuring of organizations, Prentice-Hall, 1979.
192	Various authors, 2Chaos and complexity, Interdisciplinary laboratory of scientific imagination” CUEN, 1996.
193	Borghetti, G. Marchionni, L. Studer, The concept of resilience of transport infrastructures. Framework of research and quantitative methods of analysis, Mobility and Transport Laboratory, Polytechnic of Milan and Department of Design, 2019, Milano.
196	Ch.Willmann and all; Breakdowns, accidents and fire in road tunnels – statistics; CETU information document – February 2022.
210	Road freight transport of dangerous goods 2017-2021, EUROSTAT (online data codes : road_go_ta_dg; road_go_ta_tott).
211	State inspector for road transport control Romania – I.S.C.T.R., “Directive1995/50/EC, Report Regarding Offenses and Sanctions - Control of road transportation of dangerous goods, 2021.
213	M. Niestadt, A. Debyser, D. Scordamaglia, and M. Pape, “Artificial intelligence in transport: Current and future developments, opportunities and challenges,” 2019.
214	R. Abduljabbar, H. Dia, S. Liyanage, and S. A. Bagloee, “Applications of artificial intelligence in transport: An overview,” Sustainability (Switzerland), vol. 11, no. 1. 2019. doi: 10.3390/su11010189.
215	M. Machin, J. A. Sanguesa, P. Garrido, and F. J. Martinez, “On the use of artificial intelligence techniques in intelligent transportation systems,” 2018 IEEE Wireless Communications and Networking.
216	B. Bučko et al., “Computer Vision Based Pothole Detection under Challenging Conditions,” 2022, doi: 10.3390/s22228878.
217	“Artificial neural network - Wikipedia.” https://en.wikipedia.org/wiki/Artificial_neural_network (accessed Feb. 27, 2023).
218	E. Nick, “Top 7 Artificial intelligence Data Security Threats to AI and ML,” https://www.datasciencecentral.com, 2022. https://www.datasciencecentral.com/top-7-data-security-threats-to-ai-and-ml/ (accessed Feb. 28, 2023).

221	D. Gershgorn - Fooling the machine (The Byzantine science of deceiving artificial intelligence) available online at https://www.popsci.com/byzantine-science-deceiving-artificial-intelligence/
223	https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
224	UK Parliament, House of Lords Library, "Artificial intelligence: Development, risk and regulation", Published 18 July, 2023. https://lordslibrary.parliament.uk/artificial-intelligence-development-risks-and-regulation/

World Road Association (PIARC)

La Grande Arche, Paroi Sud, 5e étage, F-92055 La Défense cedex