RESPONDING TO RISK OF SAFETY CRITICAL INFRASTRUCTURES THROUGH A SYSTEMS THINKING APPROACH: THE CASE STUDY OF ROAD TUNNELS

by

KONSTANTINOS N. KAZARAS

Master in Business Administration, Athens University of Economics and Business, 2011
Diploma in Mechanical Engineering, National Technical University of Athens, 2009

Submitted to the Sector of Industrial Management and Operational Research,
School of Mechanical Engineering, in fulfillment of the requirements for the degree of

DOCTOR OF ENGINEERING
at the
NATIONAL TECHNICAL UNIVERSITY OF ATHENS
June 2013

Supervisory Committee:

Assistant Professor Konstantinos Kirytopoulos (supervisor)
Professor Ilias Tatsiopoulos
Associate Professor Vrassidas Leopoulos

[Page intentionally left blank]

ABSTRACT

Over the last two decades there has been a great increase in the number of road tunnels worldwide. However, the increasing number of these infrastructures is a double-edged sword also raising upfront an endogenous problem, which is the severity of accidents that may occur. To cope with this problem, the European Commission launched the Directive 2004/54/EC that sets minimum safety requirements and suggests the implementation of a risk assessment in several cases. However, the EU Directive does not indicate either the method for performing the risk assessment or the criteria for risk acceptance. Therefore, a wide range of methods have been proposed most of them based on Quantitative Risk Assessment (QRA).

Although QRA contribution to manage safety has been important in many fields, it has been argued that QRA results should not form the sole basis for safety-related decision making since QRAs have limitations to consider: (1) the treatment of human performance, including not only human error per se but also management and organizational factors, (2) the kinds of failure modes that may be introduced by software, and (3) the adaptation of the system over time. Taking into account that road tunnels are not merely technical, engineering systems but also have intrinsic organizational, social and managerial dimensions that impact or contribute to their safety, the objective of this thesis is to propose an innovative method that has the ability to provide decision-makers with scenarios that even if they have not been considered by traditional road tunnel QRAs they have the potential to lead to safety issues. In order to achieve the objective, a change in the accident modelling paradigm seems to be essential. The hypothesis made in this thesis is that systems theory provides the foundation to create a road tunnel safety assessment method that has the ability to capture the “residual” risk which is left unnoticed by current road tunnel QRAs and provide guidance for responding to it.

The systems-theoretic method introduced in this thesis is primary based on the STAMP accident model. However, in order to give the opportunity to the safety analysts to search deeper for organizational pathologies and vulnerabilities, an extension of STAMP has been made with concepts from an organizational model, i.e. the Viable System Model (VSM). The joint STAMP-VSM framework is incorporated into the systems-theoretic road tunnel safety assessment method and is evaluated through an illustrative case study. The results revealed that the proposed method succeeded in copying with the several aspects that are not adequately handled by current road tunnel QRAs.

ACKNOWLEDGEMENTS (in Greek)

Η παρούσα διδακτορική διατριβή είναι γραμμένη στην αγγλική γλώσσα. Θεώρησα ότι η επιλογή αυτή θα βοήθαγε να αποτυπώσω, όσο καλύτερα γίνεται, τις σκέψεις μου αλλά και να εμπλουτίσω ιδέες που απαντώνται στη διεθνή βιβλιογραφία. Σε αυτό το εγχείρημα εξαίρεση αποτελούν αυτές εδώ οι γραμμές, στις οποίες δεν αποτυπώνονται επιστημονικοί συλλογισμοί αλλά συναισθήματα... Η εκπόνηση μιας διδακτορικής διατριβής είναι αναμφίβολα ένας δρόμος μοναχικός, δίχως αυτό να σημαίνει ότι είναι μια πορεία που μπορεί να ολοκληρωθεί χωρίς τις κατάλληλες συναντήσεις και συμπορεύσεις. Θα ήθελα λοιπόν να ευχαριστήσω θερμά τον Κωνσταντίνο Κηρυττόπουλο, επίκουρο καθηγητή του Εθνικού Μετσόβιου Πολυτεχνείου, για την πρόσκληση να ξεκινήσουμε μαζί αυτή τη διαδρομή και για την ασφαλή καθοδήγηση που μου προσέφερε σε όλη της την πορεία. Θα ήθελα ακόμα να ευχαριστήσω θερμά τα μέλη της επταμελούς μου επιτροπής, αλλά και όλα τα μέλη του Τομέα Βιομηχανικής Διοίκησης και Επιχειρησιακής Έρευνας, για την καθοδήγηση που μου προσέφεραν αλλά και για το γεγονός ότι συνέβαλλαν στο να βρίσκομαι σε ένα πολύ καλό και εποικοδομητικό ερευνητικό περιβάλλον. Ένα μεγάλο ευχαριστώ αξίζει και στην Nancy Leveson, η δουλειά της οποίας αποτέλεσε πηγή έμπνευσης για εμένα καθορίζοντας σε μεγάλο βαθμό όχι μόνο την εξέλιξη της παρούσας διατριβής, αλλά και ολόκληρη την επιστημονική μου θεώρηση.

Ξεκινώντας την εκπόνηση της διδακτορικής διατριβής, στόχος μου ήταν να φτάσω στην κορυφή της ακαδημαικής μου πορείας. Είχα όμως την ανέλπιστη τύχη να κερδίσω κάτι ακόμα περισσότερο, δυο πολύ καλούς φίλους. Ένα μεγάλο ευχαριστώ στον Θανάση Ρεντιζέλα και στον Στάθη Μαλάκη. Ελπίζω όταν έρθει ο καιρός που οι γραμμές αυτές θα έχουν ξεθωριάσει, να συζητάμε για όλες τις όμορφες εμπειρίες που ζήσαμε παρέα αυτό το διάστημα. Δίχως άλλο, το μεγαλύτερο ευχαριστώ το αξίζουν οι άνθρωποι εκείνοι οι οποίοι συμπορεύονται μαζί μου σε όλες μου τις προσπάθειες. Στην οικογένεια μου λοιπόν, ιδιαίτερα στον πατέρα μου και στην μητέρα μου, Νίκο και Πέγκυ Καζάρα, θα ήθελα να πω ένα μεγάλο ευχαριστώ που μου έδωσαν τη δυνατότητα να είμαι αυτός που είμαι -και να είμαι τόσο υπερήφανος για αυτό. Το αντικείμενο που πραγματεύεται η παρούσα διατριβή είναι η διαχείριση κινδύνων και η αντιμετώπιση επικίνδυνων καταστάσεων και εγώ έχω την ευλογία να έχω μια οικογένεια που δεν με αφήνει ποτέ μόνο, ιδιαίτερα τις στιγμές εκείνες όπου οι κίνδυνοι της ζωής απειλούν να με καταβάλλουν. Τέλος, θα ήθελα να εκφράσω ένα μεγάλο ευχαριστώ στη σύντροφο της ζωής μου, Γωγώ Θεοφανοπούλου, γιατί τα τελευταία έντεκα χρόνια αποτελεί έναν από εκείνους τους «κινδύνους» που δεν μπόρεσα, ή καλύτερα που δεν θέλησα, ποτέ να διαχειριστώ...

DECLARATION

- I Konstantinos Kazaras, hereby declare that to the best of my knowledge and belief, this PhD thesis is my own work and all sources or work of other people have been properly acknowledged. The dissertation contains neither plagiarism nor material that has already been used to any substantial extent for a comparable purpose.

- This research has been funded by the National Technical University of Athens Research Committee.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 Introduction

1.1 Problem description and challenges to be addressed

Over the last two decades there has been a great increase in the number of road tunnels worldwide and all the indications are that this number will continue to increase in the coming years since the improvement of tunnel construction technology has rendered tunnels as a cost-effective solution to connect steep mountainous regions and traverse urban areas (Zhuang et al. 2009). However, the increasing number of these infrastructures is a double-edged sword also raising upfront an endogenous problem, which is the severity of accidents that may occur. To cope with this problem, the European Commission launched the Directive 2004/54/EC that sets minimum safety requirements and suggests, apart from the measures imposed based on tunnel characteristics, the implementation of a risk assessment in several cases. The aim of the risk assessment, as indicated by the Directive, is to form a basis for decision-making and document a sufficient safety level to authorities (EU 2004). However, even if the objectives are clearly defined, the EU Directive does not indicate either the method for performing the risk assessment or the criteria for risk acceptance. Therefore, a wide range of methods have been proposed, most of them based on Quantitative Risk Assessment (QRA; PIARC 2008a).

Although QRA contribution to manage safety has been important in many fields, such as the nuclear power industry and the chemical processing industry, it has been argued that QRA results should not form the sole basis for safety-related decision making since there are several items that might not be handled well by the QRA modelling (Apostolakis 2004). Briefly, the main challenges to the acceptance of QRAs concern: (1) the treatment of human performance, including not only human error per se but also management and organizational factors, (2) understanding the kinds of failure modes that may be introduced when using software to control safety critical systems, and (3) capturing the adaptation of the system over time (i.e. the slow, incremental migration of the system to the boundaries of its safety envelope). It seems that with the arrival of the socio-technical approach and the recognition of multiple non-technical aspects in accidents' occurrence, the challenges to the acceptance of QRAs have been significantly stressed, particularly when trying to capture the overall risk picture of complex socio-technical systems (Leveson 2012).

Furthermore, QRAs based on chain-of-event accident models (i.e. event and fault trees) are sustained by the classical Newtonian/Cartesian view of the world which is founded on the idea that a system's behaviour can be understood from the behaviour of its constitutive elements and their causal links (i.e. reductionism; Zio 2009). Such decomposition assumes that the separation of the system is feasible and implies the absence of feedback loops and other non-linear interactions. It is notable that the challenges of QRAs, as they have been pinpointed in the literature, have not been adequately addressed in the road tunnel field. Therefore, although QRA methods are essential to assess the physical harm that may occur, they neglect an important part of non-technical factors that may contribute to tunnel accidents and they have several limitations to consider how the whole tunnel system interacts together.

1.2 Research Objective, Hypothesis and Approach

Taking into account that road tunnels are not merely technical, engineering systems but also have intrinsic organizational, social and managerial dimensions that impact or contribute to their safety (PIARC 2007a), the objective of this thesis is to propose an innovative safety assessment method that has the ability to provide decision-makers with scenarios (i.e. causal factors) that even if they have not been considered by the traditional road tunnel QRAs they have the potential to lead to safety issues. In order to achieve the objective, a change in the accident modelling paradigm seems to be essential. The hypothesis made in this thesis is that systems theory provides the foundation to create a road tunnel safety assessment method that has the ability to capture the “residual” risk which is left unnoticed by current road tunnel QRAs. The hypothesis is demonstrated by answering the following **research question: “can systems theory provide the foundation for creating a road tunnel safety assessment method that has the ability to identify causal factors that even if they have been left unnoticed by current road tunnel QRAs they have the potential to lead to safety issues?”**

This thesis has been developed in four steps (figure 1). The first, involved a thorough literature review on current road tunnel safety assessment methods with the aim to identify their limitations and their challenges in describing explicitly the overall tunnel safety. The conclusion of this literature review was that current road tunnel QRAs have limitations to consider: (1) how accidents may occur from the working of the whole tunnel system, (2) several organizational and human aspects, (3) the SCADA system’s software behaviour, and (4) the adaptation of the tunnel system over time. Considering that the aforementioned limitations have been mainly ascribed to the chain-of-event accident model underlying QRAs, the second step focused on searching in the literature for an accident model which meets the following requirements:

1. Considers the entire socio-technical system by taking into account all facets relating the organizational to the technical aspects.
2. Considers the relationships between the parts of the tunnel system, how they interact and fit together.
3. Considers how the SCADA system software behaviour may contribute to an accident.
4. Examines the entire process of an accident and not just the proximate events, i.e. the real causes of accidents must be identified and not only the symptoms.
5. Copes with the fact that the tunnel system is continually changing.

During this step, it has been concluded that the Systems Theoretic Accident Model and Processes (STAMP) which has been proposed by Leveson (2004) fulfills the aforementioned requirements, thus, STAMP was selected as the backbone of the proposed systems-theoretic road tunnel safety assessment method. However, to enhance the method with tools that give the opportunity to the safety analysts to search deeper for organizational pathologies and vulnerabilities, an extension of the STAMP model was regarded essential. Therefore, the third step was devoted to the extension of STAMP with concepts from an organizational model, i.e. the Viable System Model (VSM) so as to propose a framework which has the ability to identify distant causal factors into the breakdown of organizational processes. Finally, in the fourth step, the systems-theoretic road tunnel safety assessment method which has been developed on the basis of STAMP and the joint STAMP-VSM framework was introduced and evaluated through an illustrative case study. The results revealed that the method succeeded in identifying critical aspects that encompass both the technical system and the organizational structure. In addition, the method has considered several potential flaws of the SCADA system software and has coped with the dynamic nature of the road tunnel system and its adaptation over time. In a nutshell, the objectives have been fulfilled.

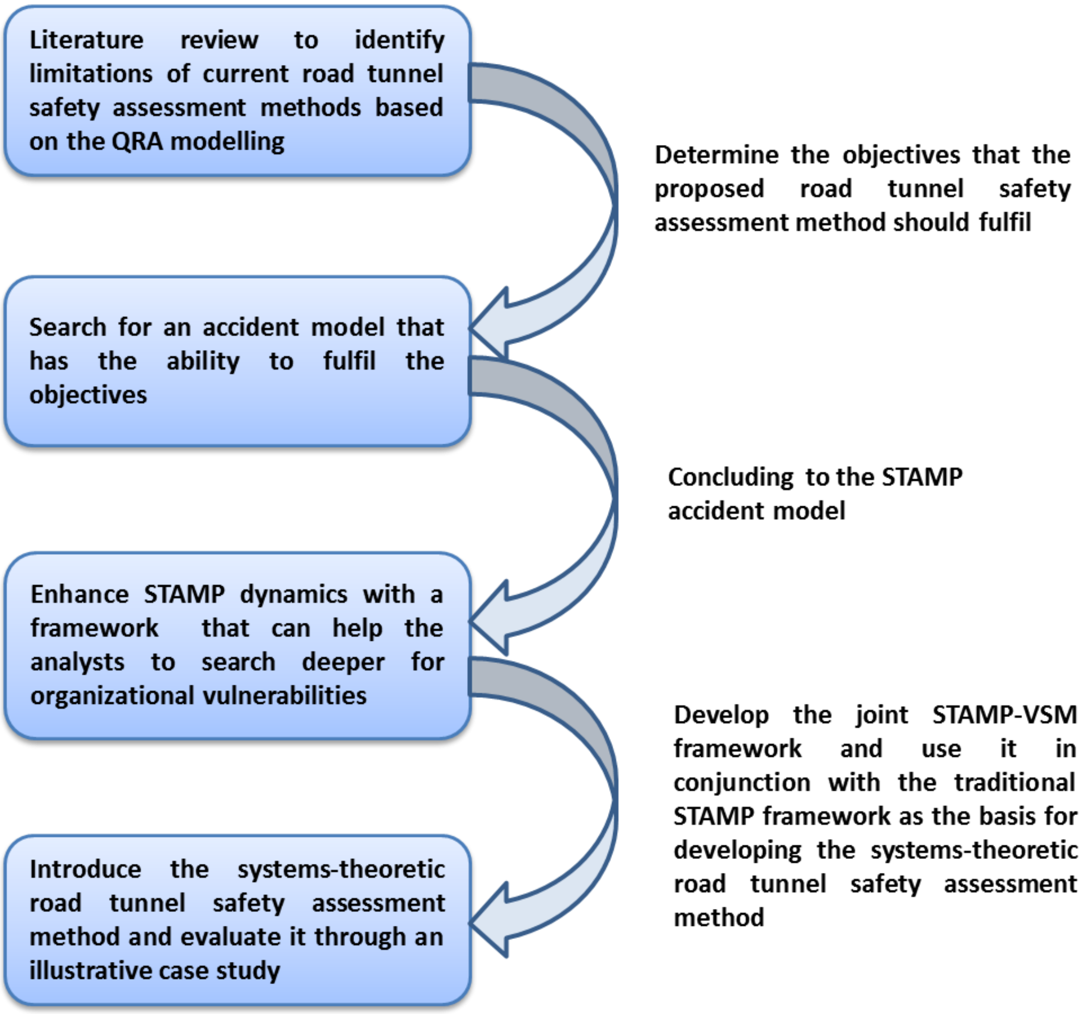

Literature review to identify limitations of current road tunnel safety assessment methods based on the QRA modelling
Determine the objectives that the proposed road tunnel safety assessment method should fulfil
Search for an accident model that has the ability to fulfil the objectives
Concluding to the STAMP accident model
Enhance STAMP dynamics with a framework that can help the analysts to search deeper for organizational vulnerabilities
Develop the joint STAMP-VSM framework and use it in conjunction with the traditional STAMP framework as the basis for developing the systems-theoretic road tunnel safety assessment method
Introduce the systems-theoretic road tunnel safety assessment method and evaluate it through an illustrative case study

Figure 1: The steps for developing the thesis

1.3 Thesis Outline

Chapter 1 introduces this thesis. The second chapter sets the scene of the road tunnel safety field. Chapter 3 presents a literature review of current road tunnel safety assessment methods and the challenges (i.e. their limitations) that need to be addressed. Chapter 4 highlights the need to make a swift in the accident modelling paradigm and proposes a systems-theoretic perspective in order to cope with the residual risk. In chapter 5, the STAMP model is enhanced on the basis of an organizational model (i.e. the Viable System Model) in order to provide a framework that may help safety analysts to search deeper for system vulnerabilities at the organizational level. In chapter 6, the systems-theoretic road tunnel safety assessment method is introduced and finally chapter 7 concludes this thesis.

1.4 Terminology and Abbreviations

1.4.1 Terminology

Accident: An unexpected event that results in a loss, including loss of human life, property damage and environmental pollution.

Emergency: A sudden, unexpected event requiring immediate action due to potential threats to safety.

Safety critical infrastructures: Organizations and facilities of key importance to public interest whose failure or impairment could result in detrimental consequences.

Hazard: A state or set of conditions of a system that together with other conditions in the environment of the system will lead to an accident.

Safety: The freedom from accidents.

Reliability: The probability that a piece of equipment or component will perform its intended function satisfactory for a prescribed time and under stipulated environmental conditions.

Road tunnel: An enclosed road structure intended for use by authorized traffic.

Safety Assessment: Aims on answering the fundamental question whether the desired safety level has been reached.

1.4.2 Abbreviations

CCTC: Closed-circuit Television

CFD: Computational Fluid Dynamics

DGs: Dangerous Goods

HGV: Heavy Goods Vehicles

HRR: Heat Release Rate

ICA: Inadequate Control Action

LCS: Lane Control Signs

QRA: Quantitative Risk Assessment

SCADA: Supervisory Control And Data Acquisition

STAMP: Systems-theoretic Accident Model and Processes

TDCS: Traffic Data Collection System

VMS: Variable Message Signs

VSLS: Variable Speed Limits Signs

VSM: Viable System Model

2 Setting the scene

2.1 Accidents statistics and major road tunnel accidents

According to French, German, Swiss, Norwegian and Italian statistics, accidents occur less frequently in road tunnels than on the open road section (Carvel and Marlair 2005). For example, an analysis of tunnel accidents on the Switzerland's national road network reveals that the accident rate in tunnels is 0.35 per million vehicle-km, compared to 0.47 which is on the open road. Similarly, Norwegian studies demonstrate that the frequency of tunnel accidents is comparable to that of high-speed roads in sparsely populated areas and half of the average road accident frequency (Amundsen 1994). Although the reliability of such statistics is questionable -mainly due to the lack of precision when reporting and recording road tunnel accidents (Beard and Cope 2008)- some general conclusions which can been drawn by analyzing the available data (e.g. Amundsen and Rane 2000; Beard and Cope 2008; Zhuang et al. 2009) are the following:

- Accident rates appear to be lower in tunnels than for the rest road network.
- Bi-directional tunnels have higher accident rates than unidirectional ones.
- The approach zones are more prone to accidents than the central location.
- Higher accident rates are observed in sections that affect the traffic flow (e.g. speed changes, variations in alignment).
- A significant number of tunnel accidents are caused by rear-end collisions and failure to maintain a safe distance from vehicles in front.

The fact that accidents rates appear to be lower in tunnels might be explained by the fact these infrastructures usually differ from the rest road network in several aspects. For instance, road tunnels are not affected by weather conditions such as fog, snow, ice, heavy rain, strong winds, sun-blurring, etc. Moreover, speed limits are usually lower in tunnels and, additionally, drivers have a higher awareness of danger. Finally, tunnels are usually equipped with several safety systems and are operated with specific procedures.

Nevertheless, if an accident occurs in a road tunnel it may have much greater impact. Past experience has shown that the consequences can be extremely destructive and dangerous, especially in the event of fire, since the limited environment hinders the dissipation of heat and smoke and puts great limitations in ensuring safe evacuation and effective rescue operations (Carvel and Marlair 2005). Indeed, tunnel fires are very complex phenomena because of the mutual interactions between physical and chemical processes.

Ingason (2005) states that tunnel fires differ from open fires in two important aspects. First, the heat to the burning vehicles in a tunnel is more intense than in an open fire because of the radiation mechanisms. Particularly, the Heat Release Rate (HRR) in a tunnel fire can be increased by a factor of 4 compared to that of the same material burning in the open road. Second, the interaction of a tunnel fire with the ventilation airflow generates aerodynamic disturbances. Fire may easily spread downstream, creating thus hazardous conditions for fire-fighters and those who are trapped inside the infrastructure. Following this line of thought, it can be deduced that although it is essential to address common traffic accidents, the main threat in road tunnel safety is undoubtedly related to fire events (ITA-PIARC 2004). This assumption is also enhanced by the fact that all of major tunnel accidents since 1995 have involved fire.

In fact, it was the spate of tunnel fires in Europe over the past decade resulting in many human and financial losses that highlighted tunnel safety as a matter of utmost importance. Accidents in Mont Blanc (1999), Tauren (1999) and St.Gottard (2001) resulted in 58 fatalities over a period of just two years. Particularly, the Mont Blanc Tunnel disaster occurred on the 24th of March 1999, when a refrigerator lorry, carrying margarine and flour, caught fire and stopped at the 6700m station of the tunnel. A fully-fledged fire was rapidly developed and spread to involve 23 Heavy Good Vehicles (HGVs) and 10 cars. Due to the prevailing wind direction from the south and the different ventilation regimes (i.e. ventilation ducts at the Italian side were set to supply fresh air, whereas at the French side some ducts were set to exhaust air) a strong longitudinal air velocity de-stratified smoke and created untenable conditions. The fire took 53hours to extinguish, resulting to the death of 39 persons. Apart from human losses and injuries, the fire also resulted in considerable financial losses and prejudicial consequences to the tunnel managers. Concerning the causes of the accident, investigators pinpointed the inadequacy of the ventilation system to control smoke and the lack of coordination between the tunnel organization and the emergency services (Lacroix 2001). A photograph of the aftermath of the accident is presented in figure 2.

During the same year and less than 3 months after the Mont Blanc Tunnel disaster, the Tauern Tunnel accident came to take place. According to Leitner (2001), construction works kept one lane of the 6400m long tunnel closed at the time of the accident, thus the other operated in both directions when a truck travelling from south crashed with full speed into the waiting queue. Only from the crash 8 people died and, moreover, the collision resulted to a fire that quickly spread to a lorry carrying a variety of goods. Altogether, 14 HGVs and 26 cars were destroyed, 12 people died and 49 were injured. It is notable that the tunnel was operated at the time of the accident bi-directionally with an average daily frequency of 15160 vehicles for both directions. The accident also entailed significant financial costs for remedial works and loss of toll feeds. Finally, in 2001 the Gotthard tunnel fire took place to raise the death toll. The accident occurred when a truck driver lost control of his vehicle, probably because of severe alcohol abuse, and crashed into an oncoming HGV. Both vehicles caught fire directly which spread to seven other HGVs causing tremendous masses of smoke and highly energetic fire loads. The accident finally resulted to the death of 11 persons (Carvel and Marlair 2005).

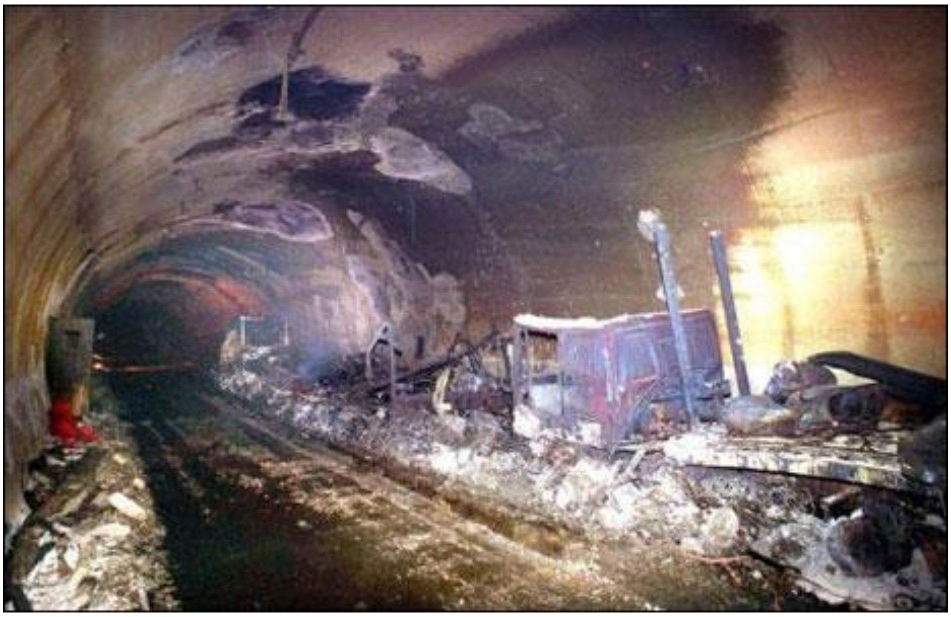


Figure 2: Consequences of the Mont Blanc tunnel fire (Lacroix 2001)

The common characteristic of the aforementioned accidents is that all occurred in long (> 6km) single bore tunnels. Moreover, apart from the direct impact, they also led to added traffic congestion in alternative routes and in turn, to a further rise in accident risks for many months or even years after the disasters (Haack 2002). A detailed description of the Mont Blanc, Tauern and St. Gottard accident can be also found in ITA-PIARC (2004). A much more extensive list of tunnel accidents is given by Carvel and Marlair (2005) and in the website of SIRAGGES Edu (http://shragges.edu.gr). Herein, it is mentioned that before the aforementioned disasters have taken place, road tunnel safety was regarded mainly as a matter of the structural safety of the infrastructure. Nonetheless, these major accidents dramatically revealed that there are many other important factors (e.g. degree of training of the tunnel operators, co-ordination of rescue operations and awareness of tunnel users) which significantly affect the overall tunnel safety. Additionally, the aforementioned disasters unveiled aspects of fire dynamics which were neither known nor expected before. One of these aspects has been the extremely fast development of the fire combined with an increase of temperature up to 1000^{0}C. Another crucial aspect which has been uncovered was the phenomenon of fire propagation from one vehicle to another, even over sections of more than 200m (ITA-PIARC 2004). All in all, **in the aftermath of these disasters an extensive review on the road tunnel safety issue has been as urgent as never before**.

2.2 Efforts to improve safety in the aftermath of tunnel disasters

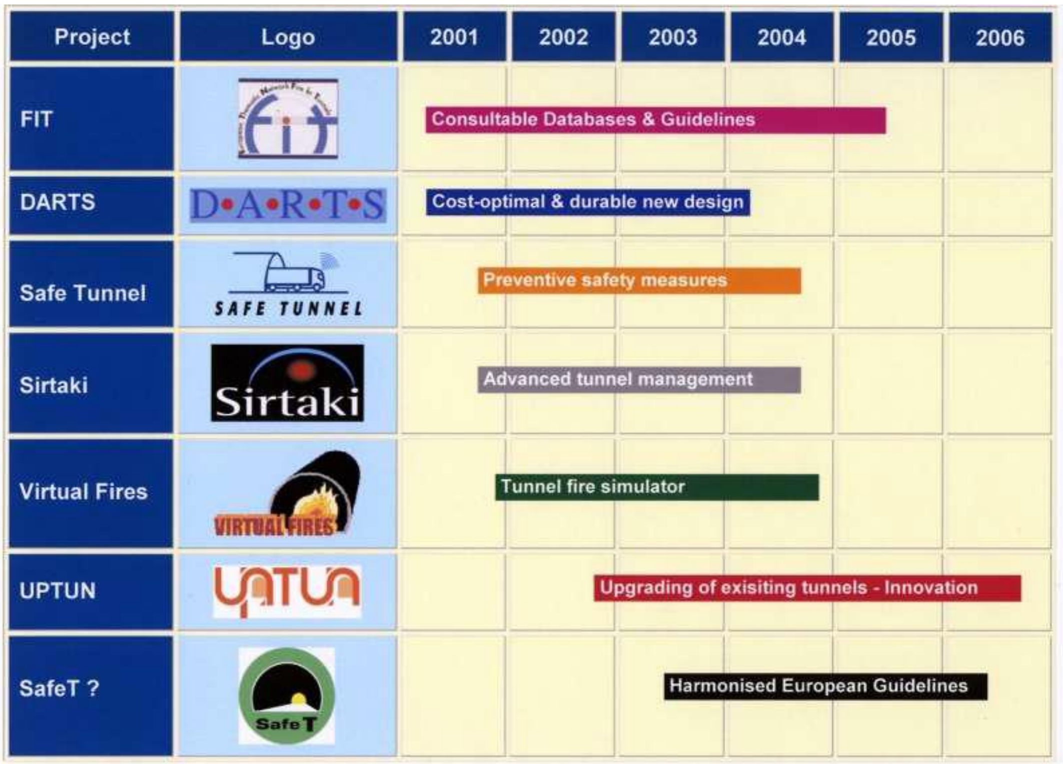
In the road tunnel field, two major associations have focused their activities on the road tunnel safety issue. The first is the World Road Association (PIARC), which in 1957 created a technical committee on "Road Tunnel Operation", and the second is the International Tunneling Association (ITA), which from 1974 has been involved in various aspects of the construction of any kind of underground structure. Although several recommendations on tunnel safety issues have been published by both organizations even before 1999, it goes without saying that the research has been intensified after the major disasters. Particularly, immediately after the Mont Blanc accident, a working group composed of representatives of the Alpine countries was created (supported by the United Nations Organization, PIARC and ITA) with the aim to harmonize the national initiatives. The final report which has been created by the working group was published in December 2001 and included 41 recommendations on all aspects of road tunnel safety, namely: users, operation, infrastructure and vehicles (UNECE 2001). Following these recommendations, the European Commission published the Directive 2004/54/EC which sets out particular safety requirements for tunnels in the trans-European road network longer than 500m (EU 2004). The Directive sets two main objectives for optimal level of safety: (1) the prevention of critical events that endanger human life and the tunnel infrastructure's integrity, and (2) the mitigation and reduction of possible consequences of safety critical events by enabling tunnel users to rescue themselves and ensuring an efficient intervention by emergency services. The EU Directive, consisted of 20 articles, describes all technical, operational and organizational requirements which are mandatory.

In detail, **technical requirements** regard specific features which should correspond to five tunnel categories (depending on traffic volume and tunnel length), such as: number of tubes and lanes, unidirectional or bi-directional traffic, tunnel geometry, emergency exits, escape routes, drainage systems, fire resistance of structures, lightning systems, ventilation systems, road signs, monitoring and communication systems, and equipment for closing the tunnel. **Operational requirements** are related to rules concerning works in tunnels, management of incidents, activities of the tunnel control center, information to users of alternative itineraries in case of tunnel closures and implementation of information campaigns. Finally, **organizational requirements** are based on defining the authorities that have to make legal decisions such as: (1) administrative authorities who hold responsibility for ensuring that all aspects of safety are assured, (2) inspection entities for inspecting safety, (3) tunnel managers who are responsible for tunnel functionality and daily operation, and (4) safety officers who are responsible for implementing safety measures.

It is notable that apart from the aforementioned requirements, the Directive requests the implementation of a risk assessment in several cases (EU 2004). In particular, Article 13 of the Directive mentions that "*Risk assessments, where necessary, shall be carried out by a body which is functionally independent from the Tunnel Manager […] (and shall consider) all design factors and traffic conditions that affect safety, notably traffic characteristics and type, tunnel length and tunnel geometry, as well as the forecast number of heavy goods vehicles per day*". Nevertheless, even if the objectives are clearly defined, the Directive does not advocate either a specific method for performing the assessment or the criteria for risk acceptance. Moreover, it is noteworthy to mention that although the Directive has been characterized as a welcome initiative for improving road tunnel safety, several reservations have been expressed by the European Federation for Transport and Environment (ETSC 2003). The main issues which have been raised are: (1) the emphasis of the Directive on the technical requirements whereas operational and organizational requirements are playing a lesser role, (2) the fact that the Directive applies only to tunnels on the trans-European road network, and (3) the lack of safety performance indicators.

In order to find out whether tunnel managers have implemented the requirements of the Directive, European automobile clubs issued a checklist approach named "European Tunnel Assessment Programme" with the aim to estimate the safety level of 26 European road tunnels (Khury 2003). The criteria for the evaluation were based on: tunnel conditions (e.g. speed limits), traffic surveillance systems, communication systems (e.g. loudspeakers), ventilation systems, escape and rescue routes, fire protection systems and incident management (e.g. regular fire drills). The rankings were evaluated from a checklist of 8 categories with points allocated in each category and weighted in importance varying from "very low risk" to "very high risk". In this way, a so-called risk potential was calculated. A key issue highlighted by EuroTAP was the absence of emergency response plans for many European road tunnels. However, the approach followed has been criticized on the basis that it does not take into consideration potential interaction among the various safety systems (Khury 2003).

In parallel, the European Commission launched several research projects for research and development (figure 3). These projects included: a research project on Fires in Tunnels (FIT), a thematic network on durable and reliable tunnel structures (DARTS), a research project on innovative systems and frameworks for enhancing traffic safety (Safe Tunnel), a research project for improving tunnel safety by using advanced information technologies and knowledge-intensive decision support models (SIRTAKI), a thematic network on upgrading methods for fire safety in existing tunnels (UPTUN) and a thematic network for harmonizing European guidelines (Khury 2003). Actions to improve road tunnels safety has been also taken worldwide. In the USA, the national standard for fire safety in road tunnels (NFPA 502) has undergone a periodic update, taking account of the recent developments. In addition, PIARC embarked upon a major review on the issue of road tunnel safety by issuing several reports. Each of these initiatives enhanced the understanding of significant aspects of the road tunnel system, such as the importance of effective fire-fighting and smoke control (PIARC 2007b), the risks involved in the transportation of Dangerous Goods (DGs) through the tunnels (OECD 2001) and the study of human behaviour (PIARC 2008b).



Project	Logo	2001	2002	2003	2004	2005	2006
FIT	FIT	Consultable Databases & Guidelines					
DARTS	D•A•R•T•S	Cost-optimal & durable new design					
Safe Tunnel	SAFE TUNNEL	Preventive safety measures					
Sirtaki	Sirtaki	Advanced tunnel management					
Virtual Fires	VIRTUAL FIRES	Tunnel fire simulator					
UPTUN	UPTUN		Upgrading of exisiting tunnels - Innovation				
SafeT ?	SafeT			Harmonised European Guidelines			

Figure 3: Research projects on road tunnel safety (Khury 2003)

Even more importantly, after the examination of all these deliverables and reports, a new perspective has been emerged. Particularly, **road tunnel safety experts concluded that there is a need for a new approach which should be based on considering the tunnel system in a holistic and systemic way** (PIARC 2007a). The infrastructure's stability is essential; however, the procedures of operation and intervention in case of an emergency, the training of personnel, the emergency services' performance and the communication with the tunnel users are parameters that should not be neglected. In a nutshell, **road tunnels are complex systems in which safety is an emergent property not a property of any single part**. At this point a question that might be raised is: "what actually constitutes a typical road tunnel system?" An informative answer is given in the next section.

2.3 The road tunnel system

Many elements constitute a road tunnel system. However, these elements can be collated into three main groups: (1) technical factors, (2) human agents, and (3) organizational aspects. These factors are briefly presented below.

2.3.1 Main Technical Aspects

In this section, the main technical aspects of a road tunnel system (e.g. figure 4) are briefly presented.

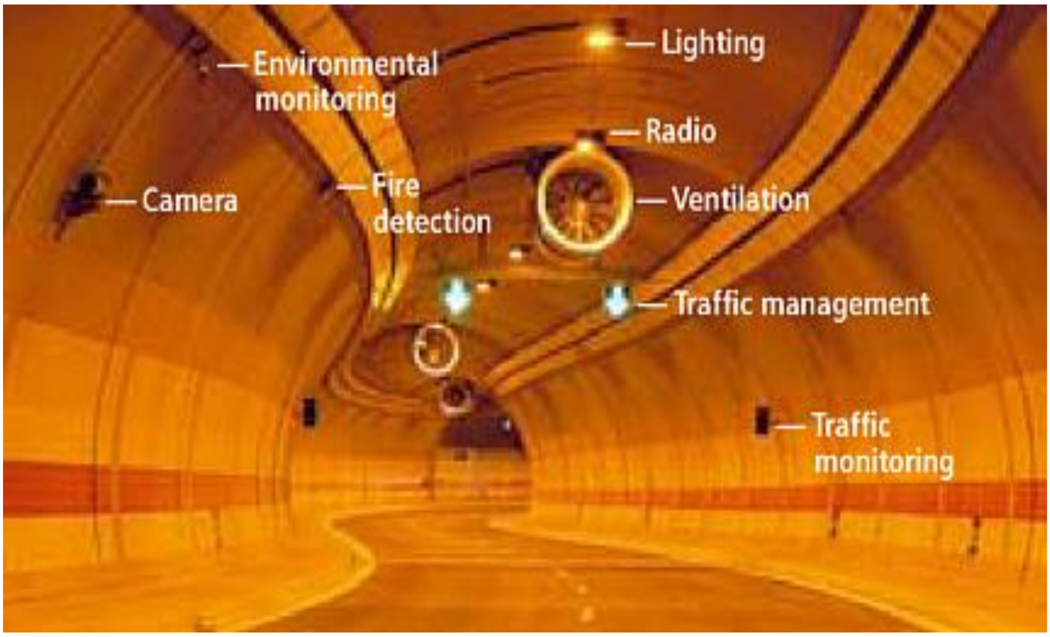


Figure 4: Technical aspects of a road tunnel system

2.3.1.1 Tunnel Layout and Tunnel Structure

In general, there are three main cross sectional shapes of road tunnels, namely: rectangular, circular and horseshoe, depending mostly on the ground conditions and the method used to construct the tunnel. For example, rectangular tunnels are mainly constructed by the cut and cover method[1], circular tunnels are often constructed by using tunnel boring machine[2], whereas horseshoe configuration tunnels are generally constructed by using drill and blast in rock. Typical cross section elements of a road tunnel include (U.S. Department of Transportation Federal Highway Administration 2009):

- Carriageway (i.e. traffic lanes).
- Off-carriage way (e.g. shoulders, sidewalks, emergency lanes, lay-bys, etc.).
- Tunnel drainage system.
- Tunnel ventilation system.
- Tunnel lighting system.
- Tunnel utilities and power supply system.
- Water supply pipes for firefighting.
- Cabinets for hose reels and fire extinguishers.
- Signals and signs above roadway lanes.
- Close Circuit Television (CCTV) and surveillance systems.
- Emergency telephones.
- Communication systems.
- Monitoring equipment of emissions and visibility.
- Emergency exits.

The dimensions of the tunnel cross section vary accordingly to traffic volumes, design speeds, the space for the tunnel equipment and the cost of the facility. More information related to cross sections and their capacity can be found in PIARC (2004). Concerning road tunnels' general alignment, it is mentioned that sharp curves are generally avoided and a minimal curvature of 550-600m is usually observed. Horizontal alignments are most of the times linear or radially large enough to ensure the safe visual perception. The headroom above the carriageway is usually, at least, equal to the maximum height of HGVs that are allowed to pass through the tunnel (for countries in the European Union this is more than

[1] Cut-and-cover tunnels are built by excavating a trench, constructing the concrete structure in the trench and covering it with soil.

[2] Such tunnels are excavated through the rock by drilled and blasting.

4.50m). Additionally to the basic cross-section and alignment geometry, road tunnels have several structural facilities, such as: emergency exits, cross-connections, lay-bys, turning bays, drainage systems and road signs.

Emergency exits (figure 5) are provided in road tunnels in order to allow users to evacuate in case of an emergency. They may be provided in different ways such as: cross-connection between tubes, safety galleries constructed alongside the traffic tube or escape passages leading directly to a safe place. The distance among emergency exits depends on the types of vehicles permitted to use the tunnel, the traffic volume, the ventilation system and the incident detection systems provided in the tunnel. Further information related to emergency exits design can be found in PIARC (2007b).

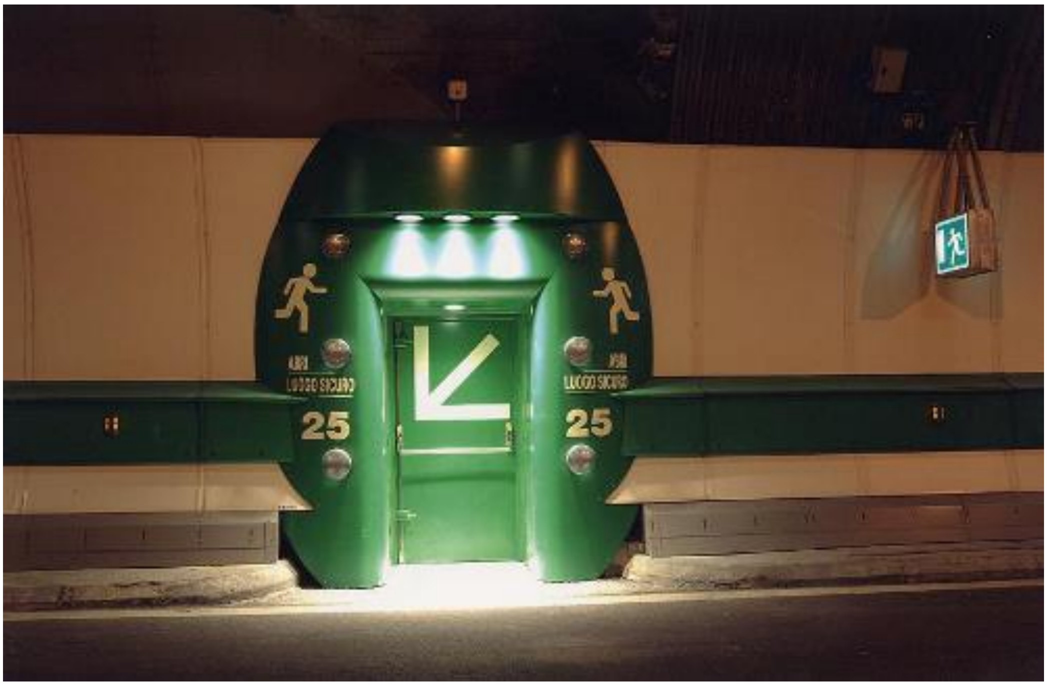


Figure 5: Emergency exits (PIARC 2007b)

Lay-bys and turning bays are usually provided in tunnels which are not equipped with emergency lanes to allow vehicles to stop without blocking the carriageway. In long bi-directional tunnels, turning bays may also be provided in order to allow vehicles to turn around or cross into an adjacent tube. Tunnel drainage systems are another important facility, particularly when the transport of DGs is permitted via the infrastructure. In such cases, the drainage system aims to minimize the size of spillage pools of flammable liquids which may have a major effect on a potential fire. Finally, road signs are vertical or horizontal signs that inform tunnel users about several aspects that need to know in normal conditions and emergency situations (e.g. location of emergency telephones).

2.3.1.2 Ventilation Systems

In general, tunnel ventilation systems fall into two main categories: longitudinal and transverse. In the **longitudinal type**, the air flows longitudinally though the tunnel moving along pollutants and smoke. Therefore, the air velocity is uniform throughout the length of the infrastructure and the level of pollutants increases from low at the entering portal to highest concentration at the exiting portal. Two different types of longitudinal systems are: (1) those that employ an injection of air from centrally located fans of the tunnel, (2) those that use jet fans mounted within the tunnel cross-section (Bendelius 2005). In general, the longitudinal strategy aims to provide clear air upstream the fire (figure 6) so as to create tenable conditions and a smoke free escape routes which allow users to evacuate and emergency services to intervene.

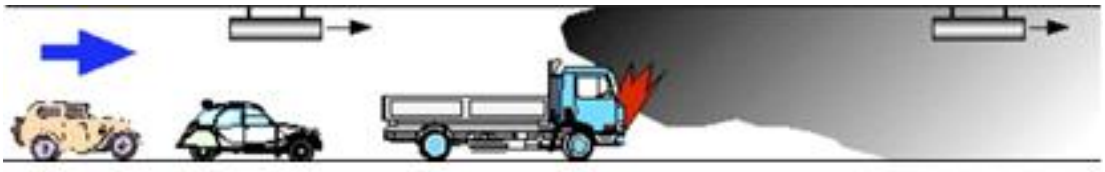


Figure 6: Longitudinal ventilation system

In a **transverse ventilation system** a uniform distribution of fresh air and collection of pollutants/smoke is created through the tunnel. Such types of systems have been used extensively in long road tunnels since the transverse strategy takes advantage of the buoyancy of fire smoke. PIARC (2011) recommendations for this type of ventilation system are to set extraction rate to the maximum near the fire zone and simultaneously stop air supply around the fire source in order to avoid smoke de-stratification. The design objectives for ventilation systems are usually based on two operating conditions, “normal” and “emergency”. Under normal conditions the aim of the ventilation system is to ensure sufficient air quality, generally for diluting pollutants, whereas in an emergency situation the primary objective is to make the environment as safe as possible for the tunnel users to evacuate and rescue services to intervene. It is mentioned that in emergency situations the progress of controlling smoke and fire can be impeded in case smoke moves against the direction of air flaw in the tunnel, a phenomenon which is known as *back-layering*. Therefore, the design of ventilation systems is usually based on the provision of a minimum longitudinal air velocity which enables to counteract back-layering, the so-called *critical velocity.* For more information on the topic the reader is referred to PIARC (2011).

*2.3.1.3 **Incident detection systems and fire detection systems***

PIARC (2007b) defines incident detection systems as "*devices located in the tunnel which continually monitor traffic conditions, automatically detect abnormal traffic and environmental conditions including stalled vehicles, traffic accidents, tunnel air quality or visibility and alert operators."* Incident detection systems aim to provide early detection of abnormal conditions which have the potential to lead to loss of human life and costly damage to the infrastructure. Such systems may include (PIARC 2007b):

- Close Circuit Television (CCTV): By monitoring the tunnel with automatic incident detection cameras (which may include image-processing algorithms), abnormal traffic conditions (e.g. stopped vehicles, traffic congestion, vehicles moving in the wrong direction, debris in tunnel) can be easily identified. Camera's distances often vary from 30m to 150m according to the horizontal and vertical curvature of the tunnel.
- Loop Detection System: This type of equipment is installed in slot cuts in the roadway at periodic intervals with the aim to monitor vehicles' speed, to measure inter-vehicle distances and to count the number of vehicles which have passed through the tunnel. The location of the loop detection system has a recommended maximum spacing of 100m.
- Overhight Vehicle Detection System**:** Such systems have the ability to provide warnings for over height vehicles (e.g. HGVs, buses) approaching the tunnel and are usually placed before the tunnel's entrance.

As far as fire detection systems are concerned, PIARC (2007b) defines such systems as *"devices installed in the tunnel to automatically detect fires along the roadway".* The automatic fire detection devices usually fall into one of the following two categories: (1) line-type heat detection systems and (2) smoke-opacity type detectors. **Line-type heat detection systems** consist of temperature-sensitive detectors which raise an alarm when the temperature is monitored over a pre-programmed rate of rise or a maximum temperature value. **Smoke-opacity type detection systems** are used for monitoring the opacity level of the tunnel. When this level is lower than a predefined threshold (probably because of smoke existence) then an alarm is activated. The latest development in fire detection systems is CCTV supported by special algorithms for fire and heat detection. However, CCTV image processing systems are regarded (for the time being) as a complementary to line-type heat or smoke opacity type detectors since they have limitations to detect hidden fires not visible directly by cameras. Finally, fire detection can be also triggered by manual alarm push buttons (installed in tunnels' emergency stations) and calls from the emergency telephones.

*2.3.1.4 **Communication systems and incident response systems***

Communication may take place from the tunnel operator to the tunnel users and vice versa, in normal and emergency situations. Systems that facilitate communication are:

- Emergency telephones: Such devices enable tunnel users to contact the control center of the tunnel. There are usually installed at fixed intervals in emergency stations specified by regulations.
- Radio communication systems**:** Considering that road tunnels are a closed and confined places, radio-transmission equipment is necessary in order to retransmit public radio broadcasts and cell phones network.
- Loudspeakers: Loudspeakers, sirens and sound beacons are usually installed at specific location in tunnels (e.g. near emergency exits) with the aim to give information and instructions in emergency situations.
- Variable Message Signs (VMS): Messages with warning information can be displayed to tunnel users by automatic or manual control.
- Lane Control Signals (LCS): Signals are used for permitting or prohibiting the use of specific lanes. These signals may consist of green or yellow down arrows and red "X".
- Variable speed limits signs (VSLS): These devices are used to inform users about the speed limits in the tunnel.
- Barriers: These devices aim to prevent users from entering the tunnel. Barriers may be used in conjunction with LCS.

*2.3.1.5 **Fire-fighting systems***

Fire-fighting systems provide the means to control a fire in a tunnel. PIARC (2007b) has extensively addressed the equipment necessary for the fire-fighting in road tunnels. The most common equipment is:

- Water Supply system: In order to provide water for fire-fighting, a water distribution system including water mains and standpipes is required within the tunnel.

- Fire hydrants: A hydrant system is required to provide a point of connection for fire-fighters for gaining access to the water supply. The spacing between hydrants varies according to regulations but usually does not exceed 250m.
- Hose reels: Hose reels are used for first aid fire-fighting and enable users to intervene at the early stage of the fire.
- Extinguishers**:** Similarly to hose reels, portable fire extinguishers are regarded essential for fight a modest size fire before the arrival of the fire services

Concerning fixed fire-fighting systems (e.g. sprinklers, water mist systems and systems with added foam) it is noteworthy to mention that their usage remains the exception rather than the rule.

2.3.1.6 ***Lighting systems***

Lighting systems are installed in order to allow satisfactory conditions of visibility to the users not only in normal conditions but also in emergency situations (e.g. a fire in the tunnel or in the case of power outage). Lighting systems design takes into account design speed, type of traffic and tunnel structure and include fundamental lighting, entrance lighting, exit lighting and connecting roads lighting. In tunnels, the level of luminance at the entrance is higher than that of the fundamental lighting because of the resolution of visibility problems, especially when driving from a very luminous outside environment to a much darker tunnel one. However, the significant light contrast between daylight and tunnel entrance zone (a phenomenon known as the "black hole effect") is difficult to be totally avoided.

2.3.1.7 ***Supervisory Control And Data Acquisition (SCADA) systems***

The term SCADA stands for Supervisory Control And Data Acquisition systems. The SCADA system is not a full control system since it also focuses on the supervisory level. By a combination of telemetry and data acquisition, the SCADA system collects information, executes the necessary analysis and control and then displays the information on a number of operator screens. Taking into account that in road tunnels there are several systems and equipment which are crucial for the overall tunnel safety, it is important for the tunnel operator to continuously monitor their status (i.e. working or faulty) and their operating mode (i.e. automatic, manual or stopped), Indeed, the SCADA system may monitor and control the power supply system, the ventilation system, tunnel lighting system, fire-fighting system, fire detection system, the incident management system, the tunnel communication system and power supply.

2.3.2 The human agents

Humans constitute an essential element of the tunnel system. Indeed, humans intervene in all phases of an accident, from its onset (being often responsible for the initiating events), to the operators and the emergency services who attempt to control the incident. Hence, in the road tunnel field, by the term “human” we consider the tunnel user, the tunnel operator and the emergency/rescue team.

*2.3.2.1 **The Tunnel User***

Taking into account that pedestrians and cyclists are usually forbidden to pass via road tunnels, with the term “tunnel user” one refers to drivers travelling through the infrastructure. Tunnel users’ behaviour determines, to a large extent, not only the probability of accidents but also the impact of their consequences. According to a report published by the Organization for Economic Cooperation and Development, incorrect behaviour of road users, in general, is the main cause of 95% of all road accidents. For this reason, the United Nations European Commission for Energy and Transport has published general recommendations about the correct behaviour that should be applied when driving through a tunnel. These recommendations are (UNCECE 2001):

- Recommended behaviour while driving via a tunnel
  - ✓ Listen to the radio station frequency indicated by signs.
  - ✓ Switch on headlights.
  - ✓ Take off sunglasses.
  - ✓ Obey traffic lights and signs.
  - ✓ Keep a safe distance from the vehicle in front.
  - ✓ Do not overtake if there is only one lane in each direction.
  - ✓ Do not turn or reverse.
  - ✓ Do not stop, except in an emergency.

- Recommended behaviour in the event of traffic congestion
  - ✓ Switch on warning lights.
  - ✓ Keep your distance, even if moving slowly or stopped.
  - ✓ Switch off engine, if the traffic has come to a halt.
  - ✓ Listen to possible messages on the radio.
  - ✓ Follow instructions given by tunnel officials or variable message signs.

In case of an emergency, it is of utmost importance for tunnel users to understand what is happening and to react as quickly as possible. In such situations, the recommendations are the following:

- ➢ Recommended behaviour in the event of a breakdown
    - ✓ Switch on warning lights.
    - ✓ Try to move the vehicle to an emergency lane or lay-by.
    - ✓ Switch off the engine.
    - ✓ Leave the vehicle.
    - ✓ If necessary and possible, give first aid to injured people.
    - ✓ Call for help from an emergency station.
- ➢ Recommended behaviour in the event of a fire
    - ✓ If possible drive the vehicle out of the tunnel.
    - ✓ If that is not possible, pull over to the side, switch off the engine and if extinction of the fire is not possible leave the vehicle immediately.
    - ✓ Call for help from an emergency telephone.
    - ✓ If possible, give first aid to injured people.
    - ✓ Go, as soon as possible, to an emergency exit.

2.3.2.2 ***The Tunnel Operator***

Tunnel operators have an important role in the safe operation of road tunnels with their role including among (Papaioannou and Georgiou 2003):

- Monitor the traffic by using cameras, sensors and other detecting systems.
- Identify disturbances which may escalate into accidents.
- Activate particular safety equipment and start pre-programmed response plans.
- Advise maintenance personnel in case of failures or malfunction of the technical equipment which may have an impact on the tunnel safety.
- Provide tunnel users and emergency services with information, in case of an emergency.
- Record and evaluate incidents, in order to analyze incidents and learn from events.

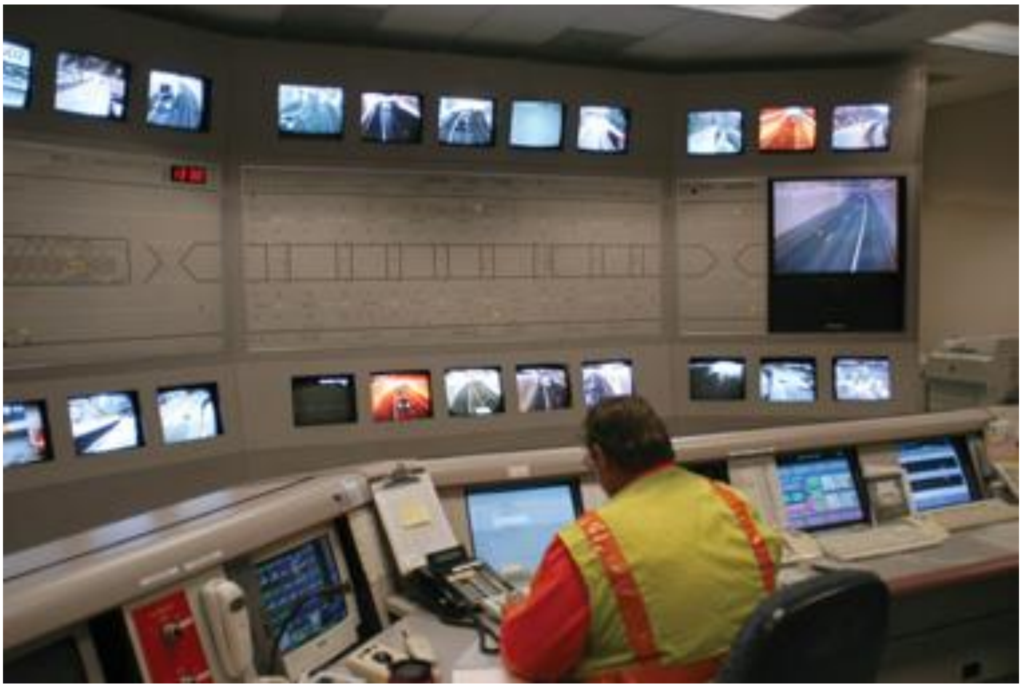


Figure 7: A road tunnel operator (PIARC 2008b)

2.3.2.3 Emergency services/response team

Emergency response may be regarded in terms of traffic management, policing, fire-fighting and medical assistance. It is argued that emergency response should be the last step in ensuring safety, coming after prevention and self-rescue. The key agencies constituting the emergency services and/or the response team may vary from country to country (or even from tunnel to tunnel), but in general the key actors are: the tunnel organization (i.e. road patrollers), the fire brigade, the police and the emergency medical services. Notwithstanding, it is crucial that every actor has a specific role in order to avoid overlaps in responsibility.

2.3.3 Organizational aspects

The overall tunnel safety depends not only on technical and human aspects but also on organizational ones. Organizational responsibilities vary from country to country; however, common organizational aspects that greatly affect tunnel safety include (PIARC, 2007a):

- Maintenance and inspection of the tunnel. Maintenance includes all necessary actions allowing maintaining or restoring the tunnel in the designed level of safety. The maintenance operations can be divided into two categories: (1) preventive interventions which are carried out at predefined intervals with the aim to preserve the tunnel’s equipment in a high operational condition and (2) corrective interventions which are carried out when a part of the tunnel’s equipment is malfunctioning. A safety inspection of the tunnel is usually conducted before starting the operation of the infrastructure. Furthermore, safety inspections should be conducted in particular time intervals to evaluate whether the safety level continues to remain at a satisfactory level.

- Recruitment of the tunnel personnel and its training procedures**.** The personnel responsible for the operation of the tunnel should be well-selected through a well-designed recruitment process, well-trained before taking up their duties and continuing to be trained throughout their career.
- Preparation of emergency plans and planning of emergency exercises. A tunnel organization should have emergency response plans for quickly intervening and preparing access for the emergency services. In order to check the effectiveness of the emergency response plans it is necessary to organize exercises with the participation of the tunnel personnel, the police, the medical services and the fire services.
- Analysis of exercises, past incidents and accidents. Debriefing of past exercises and data related to past incidents should be evaluated in order to learn from the past experience and continuously improve the overall safety level.

3 Literature review

3.1 Road Tunnel Safety Assessment methods

3.1.1 Prescriptive and Risk-based approaches

Safety assessment (i.e. safety analysis and evaluation) aims on answering the fundamental question whether the desired safety level has been reached (PIARC 2007a). In the past, road tunnel safety has been evaluated by prescriptive standards or guidelines (Beard and Cope 2008) which are mainly based on experience, tradition and engineering judgment. Specifically, such standards and guidelines that depend to a great extent on large scale tests performed in the 1960s and 1970s (Ignason and Wickstrom 2006), focused on assessing the structural safety of the infrastructures. In a prescriptive-based approach, a road tunnel is safe as long as it is in line with prescriptive requirements which are often linked to a tunnel classification system based on particular tunnel characteristics (e.g. length, number of tubes, and traffic volume). An example of a prescriptive legislative document of this type is the European Directive in which it is clearly mentioned that "*in any case, where for tunnels at the design stage a 15-year forecast shows that the traffic volume will exceed 1000 vehicles per day, per lane, a twin-tube tunnel with unidirectional traffic shall be in place at the time when this value will be exceeded*" (EU 2004).

A comparison and review of prescriptive requirements and guidelines for road tunnels can be found in ITA (2011). Noteworthy conclusions which can be drawn are the following: (1) most prescriptive requirements are linked to the tunnel length, (2) the minimum length above which prescriptive requirements should be applied varies from country to country, and (3) the capacity and spacing of fire-fighting systems significant differs among countries. The main advantage of using a prescriptive-based approach is the simplicity of its use, since in this approach the safety level can be easily demonstrated through an assessment of compliance with the specific requirements. For example, a tunnel may be regarded safe if it is equipped with: emergency exits every 150m, the ventilation system is capable to control a fire of at least 20 MW and the tunnel structure is able to withstand temperatures according to a time-temperature curve, as the ones described in ISO 834, EN 1363-1, EN 1362-2 (Ignason and Wickstrom 2006). However, such a safety evaluation is somehow crisply: "*design in accordance with the requirements is absolutely acceptable; otherwise it is absolutely unacceptable*" (Hoj and Kröger 2002). Moreover, the design values which should be met are also questionable. Ignason (2008) has introduced the term "magic numbers" to describe the uncertainties related to such design values. He notes: "*There is nothing magical about the numbers, but it is magical how they are derived. A magic number is defined as a technical design value obtained from a round table discussion of experts without any physical validation. They may be based on long experience and some limited experimental data but these numbers are usually a consensus in a group of experts sitting in technical meetings.[…]. Examples of such design values are choice of heat release rate in MW, the distance in meters between escape routes and the choice of time-temperature curves.* "

Another serious drawback of prescriptive approaches is related to engineers who might adhere blindly to the standards, forgetting thus to really think about safety. In road tunnel safety assessments, it is fundamental to consider all aspects constituting the tunnel system and the environment in which the infrastructure is located. This is hardly possible by using only prescriptive requirements since they have serious limitations to consider how various tunnel's subsystems interact when they are used together (PIARC 2008a). All in all, prescriptive requirements can ensure a minimum level of safety, but they are not able to handle unusual situations and innovative designs (Bjelland and Aven 2013). Hence, even if a tunnel fulfills all prescriptive requirements there is still a risk which is not obvious and not specifically addressed.

Beard and Cope (2008) further mention that another problem with prescriptive requirements is their lack of flexibility. The tunnel system continually changes and prescriptive requirements appropriate for one time may not be appropriate for a later time (e.g. new materials have been introduced which pose new hazards). The point is that road tunnels are becoming longer and more sophisticated while the safety assessment methods are based on traditions that were developed for much simpler applications. Taking into consideration the aforementioned drawbacks, there is a tendency nowadays to incorporate risk-based approaches not only in the design phase of a road tunnel but also during its operation. In contrast to prescriptive requirements, a risk-based approach allows a structured assessment of risks by considering the local environment and relevant influencing factors. Following a risk-based approach, a road tunnel is safe only as long as it meets the predefined risk criteria (PIARC 2008a).

Although the safety assessment of a tunnel is rarely based only on a risk-based approach, road tunnel risk assessments are currently introduced for a number of purposes, such as: (Hoj and Kröger 2002):

1. To demonstrate and document a sufficient safety level to authorities.
2. To provide a basis for risk communication.

3. To serve as a basis for decision making by choosing between alternative safety measures.

According to PIARC (2008a), the risk assessment process includes: risk analysis, risk evaluation and risk reduction (figure 8). Risk analysis aims to answer the question: “what might go wrong and what are the consequences?” Risk evaluation aims to provide the answer to the question: “is the estimated risk acceptable?” and risk reduction aims to answer the question: “which measures should be taken to assure a safe tunnel system?” All these processes, in conjunction with feedback concerning the safety performance of the system, can be included under the umbrella of risk management which is generally defined as all measures and activities carried out to manage risk (Aven 2003). Risk assessment is also requested by the EU Directive 2004/54 in order to: (1) demonstrate safety in case of deviation from prescriptions, (2) choose between alternative safety measures, (3) check general consistency of the safety level, and (4) decide on the transportation of DGs through the tunnel.

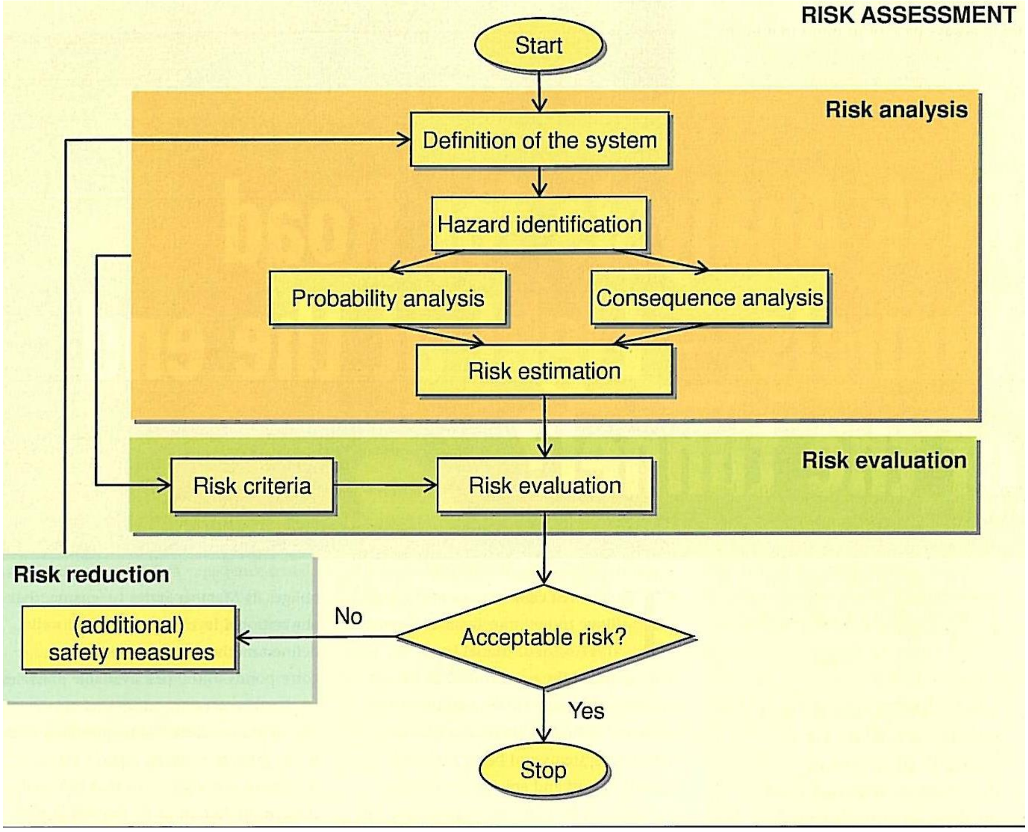


Figure 8: Flowchart of the risk assessment process (PIARC 2008a)

Road tunnel risk assessment methods can be divided into two major groups: qualitative and quantitative. Qualitative methods (e.g. what if method, Delphi method, expert judgment, etc.) are based upon arbitrary definable evaluation standards. They are simple, flexible and can be used for many kinds of problems. However, their main pitfall is their subjective character and the fact that they do not consider the interaction among different elements of the tunnel system. For this reason, they are not widely used. On the other hand, quantitative methods attempt to estimate the risk in a logical and integrated way by considering several aspects that may influence the road tunnel safety (PIARC 2008a). Quantitative Risk Assessment (QRA) utilizes several tools with the purpose to calculate the probability of occurrence of system-level events (e.g. an accident) based on the probabilities of occurrence of basic events (i.e. usually individual components failures and human errors). However, before probing into the road tunnel QRAs, a discussion on the general concept of this type of analysis seems to be essential. This issue is thoroughly presented in the following section.

3.1.2 The concept of QRA in general

3.1.2.1 ***What is QRA?***

QRAs have become a common method to assess and manage safety and risk in complex technological systems (Apostolakis 2004). This trend has been also followed in the road tunnel field, where risk-based approaches form a significant part of the safety-related decision making. When discussing about risk-based approaches, a question that might be raised is "what does the term risk actually means"? At this point it seems that there is not a consensus and the word "risk" is used in literature in many different senses (e.g. business risk, social risk, economic risk, safety risk, investment risk, military risk and political risk; Kaplan and Garrick 1981). Kaplan (1997) highlights the challenge of defining the term risk by noting: "*When Society for Risk Analysis was brand new, one of the first things it was to establish a committee to define the word risk. This committee labored for 4 years and then gave up, saying in its final report, that maybe it is better not to define risk. Let each author define it in his own way, only please each should explain clearly what way that is.*"

Even today, organizations like the Society for Risk Analysis have not been able to establish consensus on key concepts of risk. For example, ISO has issued a standard on risk management terminology (refer to Aven 2011a) but instead of bringing clarity to the field the standard may have introduced new confusion, as it is pinpointed by several experts on the field of risk management (Aven 2011a; Leitch 2010; Purdy 2010). A brief review of some prevailing perspectives and definitions can be found in Aven and Kristensen (2005), Aven (2010; 2012), Christensen et al. (2003) and Reenn (1998). Nevertheless, in safety engineering it is widely accepted that the common understanding of risk includes the following three components (Ale 2002; Kaplan and Garrick 1981):

- what can go wrong? (i.e. the accident scenarios)
- the consequences of these scenarios, if they occur
- the probability of the accident scenarios and their consequences

By following this definition, a QRA aims to address the following three questions (Kaplan and Garrick 1981): (1) what can go wrong with the examined system? (2) how likely is it?, and (3) what are the consequences? Essentially, QRAs have evolved over time to estimate the likelihood of accident scenarios in complex systems (such as nuclear and chemical plants), in situations where accident statistics are too small to give meaningful answers about their safety level. The approach taken in QRAs is "*to decompose the system as a whole into subsystems and components, stopping the decomposition at a point where substantial amount of data are available"* (Bier 1999). Apostolakis (2004) states: "*In QRA a set of undesirable end states (adverse consequences) is defined e.g. in terms of risk to the public, loss of the system, […] and for each end state, a set of disturbances to normal operation is developed that, if uncontained or unmitigated, can lead to the end state. These are called the initiating events (IEs). Event and fault trees or other logic diagrams are employed to identify the sequences of events that start with an IE and end at an end state. Thus, accident scenarios are generated. These scenarios include hardware failure, human errors, […]. The dependencies among failures of systems and redundant components (common-cause failures) receive particular attention. The probabilities of these scenarios are evaluated using all available evidence primarily past experience and expert judgment. Then the accident scenarios are ranked according to their expected likelihood of occurrence*".

To put it simple, in order to describe the accident scenarios two methods are commonly used. The first is to conclude to the initiating events and then utilize an event tree analysis for describing the sequence of events that may lead the system to undesirable end states. The second is to determine the undesirable end states and then draw the fault tree that leads to their initiating events. As far as the "likelihood" term is concerned, the format which is used to capture and quantify the intuitive idea of "likelihood" is usually the concept of probability (Kaplan 1997). Consequences of the accident scenarios may be related to human losses (i.e. fatalities), injuries, chronic diseases, pollution on environment and material damage. Then by multiplying the likelihood of accident scenarios with their potential consequences the final result of QRA might be given in risk indices such as (Aven 2008):

- individual risk (IR -the probability that a specific individual being present at a certain position is killed during 1 year).
- the expected number of fatalities during 1 year (EV).
- *F-N* curves showing the frequencies of accidents with at least N fatalities.

Such risk indices form the risk picture of a system and constitute the basis for risk evaluation. Risk acceptance criteria are usually defined so as to give a reference by which the risk is assessed to be acceptable or not (Aven 2008)[3]. The ALARP (As Low As Reasonably Practicably) principle is often established in order to express the need to reduce risk at a level at which more risk reduction requests costs that are grossly disproportionate to the gains obtain. In this sense, the ALARP principle can be incorporated in a cost-benefit analysis (Aven 2003). It is notable that the aforementioned way of estimating and evaluating risk is consistent with (and influenced by) the common definition of risk as "the combination of probability and consequences". Indeed, the notion of risk and the foundations of risk management are heavily entwined with the concept of probability (Kaplan 1997). But what is actually the meaning of "probability" in a risk and safety setting and how can it be interpreted?

3.1.2.2 ***How to define a probability in a risk and safety setting***

Kaplan and Garrick (1981) mention that people have been arguing about the meaning of probability for at least 200 years, since the time of Laplace and Bayes. The major polarization of the argument is between the "frequentist" school who views probability as the result of repetitive experiments and the "subjectivists" who view probability as an expression of an internal state -a state of knowledge or state of confidence. The argument is still relevant and even today there is substantial discussion within the scientific community about the meaning and interpretation of probabilities (refer for example to Aven and Reniers (2013) and the references therein). At this point, the controversy may seem to be a rather academic and philosophical discussion but it should not be underestimated since it also has essential implications on how to communicate and manage risk (as it will be further discussed in section 3.2.5). Kaplan (1997) highlights: "*50% of the problems in the world result from people using the same words with different meanings whereas the other 50% comes from people using different words with the same meaning*."

[3] This is basically an ethical decision not a technical one.

For the needs of this thesis, the author adopts Aven and Reniers' perspective (2013) noting that there are two different interpretations that could be used concerning the probability of an event A. The first is the frequentist probability, which has a statistician's meaning. This refers to the outcome of a repetitive experiment of some kind (e.g. flipping coins) and it includes the idea of population variability. Such a number is called an "objective" probability because it exists in the real world and is in principle measurable by actually doing the experiment. Hence, the frequentist probability of an event A expresses the fraction of times the event A occurs when considering an infinite population of similar situations or scenarios to the one analyzed. For example, in the case of a die, the probability of a specific outcome, say 3, is equal to the long run fractions of times that this number occurs (i.e. 1/6). The problem with this perspective is that it is not obvious how to make a proper definition of the population.

Singpurwalla (2006) notes that the concept of frequentist probabilities "*is applicable to only those situations for which we can conceive of a repeatable experiment.*" This statement excludes many situations of the real world. Aven and Reniers (2013) give an illustrative example by wondering "*what may be the frequentist probability of an accident occurring the next year, having more than 100 fatalities, on an offshore platform*?" They conclude that it is quite difficult to define the infinite population of similar situations (e.g. platforms with the same type of constructions, equipment and operational procedures but with some type of variation), thus they stress that the concept of a frequentist probability is difficult to be extended in real-life situations, particularly in the safety field. Indeed, even proponents of the "frequentist" interpretation have mentioned that there is a significant difference between situations with a well determined repeatable experiment (e.g. coin-tossing) and less well-determined situations, such as assigning probabilities to whether a major accident will happen in a particular system (Moller and Hanson 2008).

The second interpretation of probability in a risk and safety setting is the subjective (or knowledge-based) probability which expresses the assessor's uncertainty (degree of belief) of the occurrence of event A, based on the background knowledge (i.e. a Bayesian approach). This kind of probability does not exist in the real world and that is why it is often called subjective (Kaplan 1997). Following this interpretation, the assessor compares his uncertainty about the occurrence of the event A with the standard event of drawing at random a favorable ball from an urn that contains P(A)·100% favorable balls. For example, if the assessor assigns a probability P(A)=0.1 to the event A, then he compares his uncertainty about the occurrence of the event A and his degree of belief of event A occurring, with the standard of drawing at random a specific ball from an urn that contains 10 balls. Likewise, if the assessor assigns a probability P(A)=0.3 to the event A, then he compares his uncertainty about the occurrence of the event A with the standard of drawing at random a specific ball (e.g. a red ball) out of an urn containing 10 balls, where 3 are specifics (e.g. red balls; Lindley 2006)[4].

Apostolakis (1990) mentions that since safety assessments of technological systems require the investigation of the occurrence and consequences of rare events, the subjective theory of probability is the only appropriate framework for the quantification process[5]. In this framework, judgment experts' opinion is combined with observations and frequencies to express the belief of the occurrence of the examined rare events. If the risk analyst later faces new information, he may change his probability assessment in accordance with Bayes' theorem. As it has been highlighted from the beginning of this paragraph, the issue of interpreting probability in the risk and safety field is still controversial and different opinions exist within the scientific community. However, it is crucial to highlight that whatever interpretation of probability is adopted, the reason for utilizing probabilities in QRAs is to express to what extent an event A and/or the consequences of the event A are likely to occur. All in all, probability is just a tool to measure uncertainties in risk assessments. How useful is this tool is thoroughly discussed in the next section.

[4] A subjective probability can also be given other interpretations. For example, among economists and decision analysts a subjective probability is linked to betting. In this case, the probability of the event A is the maximum amount of money that the assessor would be willing to pay if he would receive a unit of payment in the case that event A were to occur, and nothing otherwise. However, this interpretation is not preferred in the safety field since it is regarded misleading to associate risk with attitude to winning or losing money in gambling situations (Aven and Reniers 2013).

[5] It must be mentioned that the classical interpretation of probability which goes back to Laplace (1812), is also not applicable in most real-life situations. According to the classical interpretation, the probability of A is equal to the ratio between the number of outcomes resulting in A and the total number of outcomes, i.e. P(A)= (Number of outcomes resulting in A)/(Total number of outcomes). As an example, consider the tossing of a die. Here P(the die shows two) = 1/6 since there are six possible outcomes which are equally likely to appear and only one that gives the outcome two. The requirement of each outcome to be equally likely is critical for the understanding of the classical interpretation and for this reason it is not applicable in the safety field in which it is impossible to have a finite number of outcomes which are equally likely to occur (Aven and Reniers 2013).

3.1.2.3 ***Uncertainties in QRAs***

In order to discuss the issue of uncertainties[6] in QRAs, the reader is referred to the example presented by Rosa (2010). Hence, consider the boulder depicted in figure 9. Whether the boulder will dislodge from the ledge is subject to uncertainty and there are also uncertainties about the consequences if the boulder dislodges. The bolder represents a threat to John who walks underneath the bolder; thus, a question arisen is what the risk is in this particular example? The boulder may dislodge from the ledge or not, and if the boulder dislodges the result could be that John is killed, or seriously injured. All of these events are possible, but the occurrence of these events is not known, i.e. they are subject to uncertainties. Uncertainty simple means that it is not known whether the event will occur or not, when it may occur, and what the consequences will be (how severe the outcome will be) if it does occur.

If the uncertainty is conceptualized by assigning a frequentist probability, one has to construct a population of similar situations. Then, the frequentist probability represents the fraction of times for which the boulder dislodges when John walks underneath the boulder. However, the conditions may greatly vary according to weather and climate variations, so it is very difficult to conceive a “repeatable experiment” and assign a frequentist probability in this particular example. Indeed, it seems to be awkward to use relative frequencies (i.e. a frequentist probability) in this example, since we may not have similar situations to compare and conclude to the frequency of that event (i.e. the expected number of boulder dislodging per unit of time).

[6] In the context of QRA, uncertainty is distinguished into two different types: randomness due to inherent variability in the system (i.e. stochastic process of behaviour) and imprecision due to the lack of knowledge and information of the examined system. The former type of uncertainty is often referred to as aleatory or stochastic uncertainty whereas the latter is often referred to as epistemic. It is notable that whereas epistemic uncertainty can be reduced by acquiring knowledge and information on the system, the stochastic uncertainty cannot be reduced, therefore, it is often called irreducible uncertainty (Aven and Zio 2011).

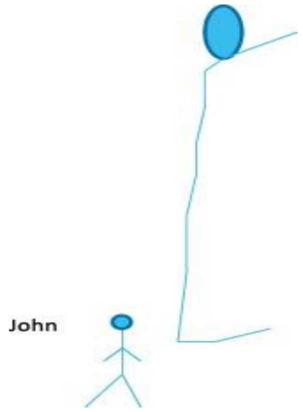


Figure 9: Boulder example (Rosa 2010)

If on the other hand one adopts the subjective probability perspective and assign, for example, a subjective probability P=0.001 for the event that the boulder dislodges, he compares his uncertainty (and his degree of belief) of boulder dislodging with the standard event of drawing a specific ball from an urn having 1000 balls. The uncertainty (degree of belief) of boulder dislodging and the standard event are the same. The crucial thing in this perspective is whether the risk analyst is well trained in the process of transforming uncertainty into probabilities, particularly for events on the lower part of the probability scale. For example, is it possible to distinguish probability numbers such as 10^{-6} and 10^{-7}? Moreover, even more crucial is the fact the assigned probabilities are conditioned on a number of assumptions and suppositions which are based on the analyst's background knowledge. Aven (2009) gives again an illustrative example: "*Consider offshore diving activities, and the risk seen through the eyes of a risk analyst in the 1970s, related to future health problems for divers working on offshore petroleum projects. An assignment is to be made for the (subjective) probability that a diver would experience particular health problems during the coming 30 years due to diving activities. Let assume that an assignment of 0.01 is made. This number is based on the available knowledge at that time. There are not strong indications that the divers will experience health problems. However, we know today that these (subjective) probabilities led to poor predictions. Many drivers have experienced severe health problems*".

The point made for both perspectives (i.e. frequentist and subjective probabilities) is that **by restricting the concept of risk to the probability assignments alone, many aspects of uncertainty and risk are actually hidden from the assessment**. "*Restricting attention to the assigned probabilities could camouflage factors that could produce surprising outcomes*" (Aven 2010). Based on the results of risk assessments, companies often spend enormous amounts of money; hence the adequacy and clarity of risk numbers which are based on arbitrary probabilities might be seriously questioned. Following this line of thought, some researchers have attempted to enhance the traditional QRAs with qualitative tools that see beyond probabilities (Aven 2008) while others have adopted alternative approaches based on probability bound analysis, random sets, fuzzy probability, possibility theory and evidence theory (Dubois 2010).

Although this thesis does not delve into such alternative approaches, it is essential to highlight that the key point in QRAs is to guarantee that uncertainties are taken into account in a way that the knowledge and information related to the examined system are represented in the most accurate manner. Otherwise, if the uncertainties that underlie the analysis are concealed, QRAs might seem to be irrational, unscientific and potentially misleading (Aven and Zio 2011). Even though the representation of uncertainty is a major challenge on the usage of QRA, it is not the only one that this type of modelling must overcome. Indeed, there are several other challenges for the acceptance of QRAs which are briefly presented below.

3.1.2.4 ***Challenges to the acceptance of QRAs***

As it has been pinpointed, QRAs are progressively becoming the selected method to manage safety and risk, not only in road tunnels but also in many other complex technological systems. Whether this may or may not be a desirable development depends upon how this method is carried out, since like any other method and technique the QRA modelling is subjected to several limitations. Therefore, before implementing a QRA and adopting a safety assessment approach based on this type of modelling one has to be aware of the several items that are not adequately handled by this approach. Briefly, in the literature it is pinpointed that challenges and limitations of QRAs are mainly related to human factors, organizational aspects and software behaviour (Apostolakis 2004; Bier 1999; Leveson 2012; Zio 2009).

With respect to modelling organizational aspects, the key questions in this line of research can be summarized as follows (Mohaghegh and Mosleh, 2009): (1) what are the organizational factors that affect the overall risk? (2) how do these factors influence risk?, and (3) what is the extent of their contribution to risk? Among the methods and techniques that attempt to quantify the impact of organizational aspects on risk the most cited ones are WPAM (Davoudian et al. 1994), SAM (Pate Cornell and Murhy 1996), I-Risk (Papazoglou et al. 2003) and a combination of a System Dynamics method (Mohaghegh et al. 2009). Although the aforementioned methods make a step forward on modelling organizational aspects, there is a significant number of major challenges in their application, as it is extensively discussed by Mohaghegh and Mosleh (2009). Shortly, any attempt to capture organizational aspects face the difficulties related to the scarce information at disposal and its subjective interpretation. Hard data based on statistics is usually not available for interactions between the social and technological system (Zio 2009). For example, is it possible to have a comprehensive database for calculating the probability that management does not implement effective organizational procedures?

As far as modelling human factors is concerned, the spectrums of methods that have been introduced in order to link human behaviour with accident causation are classified under the general heading of Human Reliability Analysis (HRA). Often, in HRA humans are regarded to fail just like mechanical, electrical and structural components do. Therefore, it makes sense to assign a probability of human failures in performing a particular task. The majority of work in HRA has come from the nuclear power industry through the development of techniques such as Human Error Assessment and Reduction Technique (HEART) and the Technique for Human Error Rate Prediction (THERP; refer to Reason 1997). An extended literature review and critique of HRA is presented by French et al. (2011). Briefly, the main limitation of HRA is that such methods face severe difficulties to describe the context in which human tasks are performed. Studies in Cognitive Engineering have revealed that humans do not “fail” randomly (just like mechanical components do), but it is the “error prompting” context that forces them to perform inadequately their tasks. In this sense, human error is a symptom rather than the cause (Woods et al. 2010). The major challenge of QRAs is to focus on the mechanisms and factors that shape human behaviour, i.e. the performance shaping mechanisms and the context in which human actions take place. Even more intense is the challenge to link such factors with probabilities.

Another controversial area concerning the implementation of QRAs is software behaviour (Apostolakis 2004; Leveson 2004). A QRA is typically performed by using fault and event tree analysis with the purpose to calculate the probability of occurrence of system-level events (e.g. an accident) based on the probabilities of occurrence of basic events (usually components failures and human errors). Therefore, it comes as no surprise that when considering the application of QRAs related to software attention turns to the question of software failure probabilities (Garret and Apostolakis 1999). Leveson’s conclusion on the issue (2012) seems coherent: “*Software failures can be traced back to design errors and incomplete requirements. If we knew enough to measure these types of design flaws, it would be better to fix them than trying to measure them*”. Garret and Apostolakis (1999) have also highlighted that software’s behaviour is almost always deterministic, meaning that there are not “random” changes that can be described in probabilistic terms. Concluding this long interval in the general concept of QRA, it is mentioned that the issues presented herein will be further discussed in the road tunnel field which is the topic of interest of this thesis.

3.1.3 Current QRA methods in the road tunnel field

PIARC (2008a) classifies road tunnel QRAs into two broad categories:

1. Scenario-based approaches which analyze a defined set of relevant accident scenarios, in terms of likelihood and consequences, and assess the risk level separately for each defined scenario.
2. System-based approaches which consider all relevant accident scenarios in an integrated process, thus, assess the risk for the whole tunnel system.

3.1.3.1 ***Scenario-based approaches***

In a scenario-based approach a set of relevant accident scenarios is defined with the aim to analyze their consequence. The consideration of probabilities is often neglected from the analysis and qualitative methods might be employed in order to indicate the likelihood of these scenarios. For example, risk matrices may be utilized in order to provide an index of criticality which links the likelihood and the severity of the examined scenarios. Then, scenarios which have been assigned a high likelihood of occurrence and high potential consequences are regarded as the most critical ones and are prioritized for the analysis. Typically, the accident scenarios are based on initiating events (also called “trigger events” or “critical events”) which may be generally available or specifically identified. For example, Hazard and Operability (HAZOP) study and Failure Mode Effects and Criticality Analysis (FMECA) can be used in order to conclude to the initiating events. Nevertheless, the assessment is usually limited on a restricted number of initiating events provided by specific checklists[7]. Once the initiating events have been selected, the analyst associates them with a specific context (i.e. tunnel location, time period and other aggravating factors) and continues with an event tree analysis which describes the sequence of events that may lead the tunnel system to undesirable end states. At this stage, the least favorable context should not always be chosen since it might hide the advantages of particular safety measures. For example, a scenario involving a fire occurring near an emergency exit might not be representative since it renders the exit inaccessible (PIARC 2008a).

[7] As a general rule, a scenario-based approach usually focuses on the examination of three to five initiating events (CETU 2005).

Having determined the evolution of the accident scenarios, the next step concentrates on investigating their potential consequences which are related to: (1) smoke and heat propagation, (2) tunnel users' behaviour, and (3) implementation of safety measures. In particular, smoke propagation is modeled by 1D models or 3D models. By modelling smoke propagation, it is possible to calculate the carbon monoxide (CO) and carbon dioxide (CO_2) concentrations, the temperature of the smoke and the visibility level at different times along the tunnel. Such information is often provided in space-time graphs (figure 10) that demonstrate the tunnel areas with untenable conditions. Having determined the areas of the tunnel with untenable level of conditions (e.g. due to toxic gases and high temperature), the assessment focuses on determining the number of people who might be exposed in these areas. To simulate the evacuation process several models can be used, varying from simple empirical relationships to complex simulation models. However, it is notable that the process of evacuation is a complex phenomenon, thus its simulation should consider not only the physical characteristics of the tunnel but also the human's behaviour variability. The next step of the assessment is based on ASET/RSET timeline analysis, meaning that if the Required Safe Egress Time (RSET) is more than the Available Safe Egress Time (ASET) then some people are considered unable to evacuate the area before the onset of untenable conditions. Hence, fatalities and injuries occur at this "risk interval" (Guanquan and Jinhui 2012; figure 11).

The evaluation of the results attained by a scenario-based approach is often made by a comparison of the resulting consequences for two similar scenarios with the one considering the influence of more safety measures. Particularly, since the results of the assessment are related to the expected number of fatalities, for each examined scenario it is revealed whether particular safety measures have the potential to reduce the impact of the consequences (i.e. the number of expected fatalities). In this perspective, the assessment highlights the contribution of particular safety measures in the accident scenario trajectory (PIARC 2013). Another way to evaluate the risk is to compare the results from the consequence analysis against tolerability criteria, such as temperature levels and toxic gases concentrations (Bjellan and Aven 2013). Finally, risk evaluation can be also made by comparing alternative designs against similar prescriptive designs. In this way, it is checked whether the alternative design has an equivalent, lower, or higher level of safety than that of the prescriptive reference design. It is noteworthy to mention that in a scenario-based approach risk cannot be conceptualized as "the combination of probability and consequences", since probabilities are not utilized in the assessment. In such type of assessment risk is rather understood as “the expected value of loss (i.e. fatalities) or simple “the potential/possibility of loss” (refer to Aven 2011b).

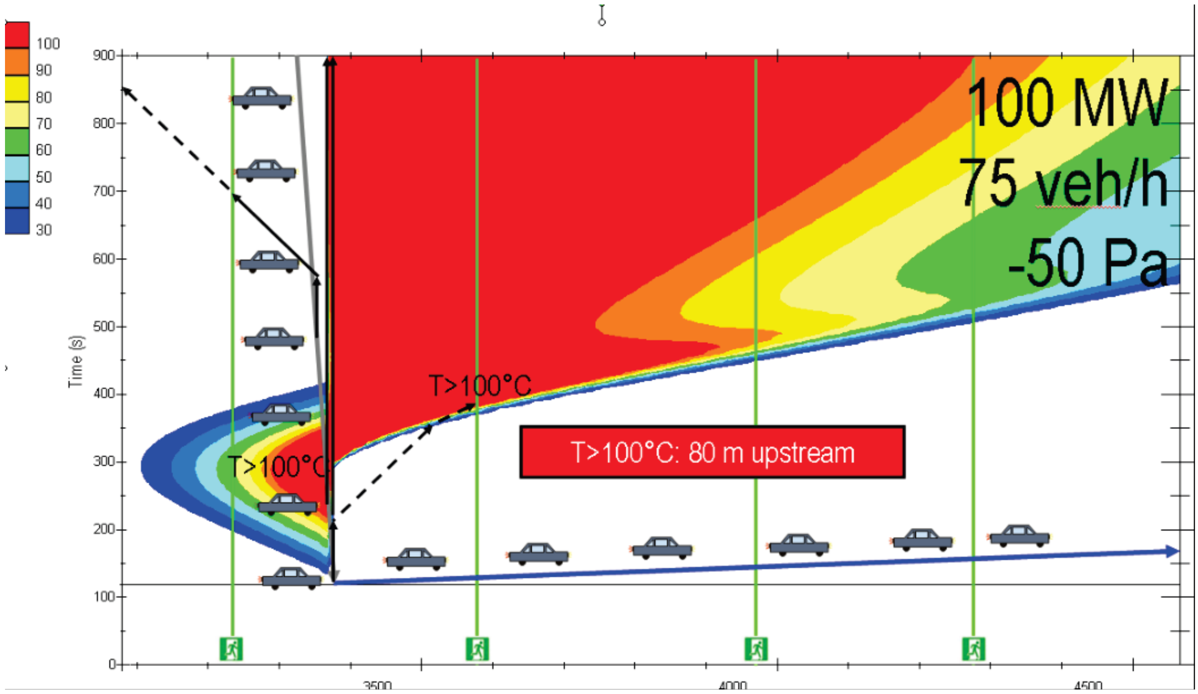


Figure 10: Representation of temperature effects (CETU 2005)

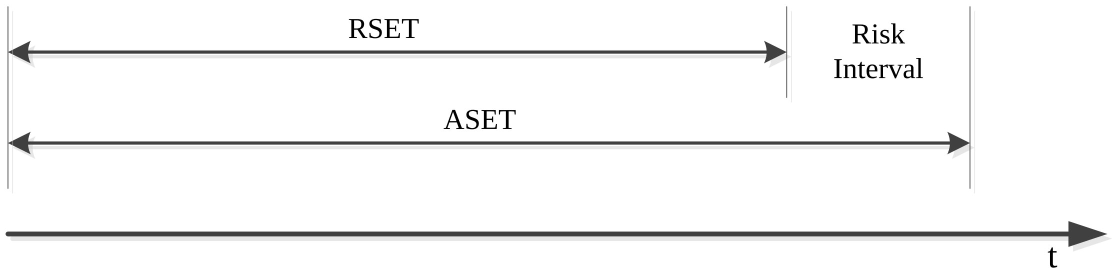


Figure 11: The ASET/RSET risk interval

Scenario-based approaches which have been proposed in the road tunnel field are: the Czech CAPITA method, the Dutch scenario analysis and the French specific hazard investigation (PIARC 2013). However, although the aforementioned approaches can unveil weak points in the tunnel system, it is essential to keep in mind that these approaches focus on the escalation of a limited number of accident scenarios. For this reason they cannot provide the overall risk picture of the whole tunnel system, as system-based approaches manage to do.

3.1.3.2 ***System-based approaches***

In order to determine the overall risk level of a road tunnel, a system-based approach is usually adopted (PIARC 2008a). The so-called system-based QRAs (which are indeed the typical probabilistic risk assessments performed in other industries) are based on an extensive inventory of possible accident scenarios. Following this line of thought, a system-based QRA seems to be an extension of several scenario-based approaches, for which probabilities have been assigned to express the likelihood of occurrence of the various scenarios analyzed (Arends et al. 2005). The general concept of a system-based QRA consists of the following modelling steps (figure 12):

1. Identification of hazards (e.g. fire, explosions, leaks, flood, etc.) and the selection of relevant initiating events.
2. Fault tree and event tree analysis for describing the chain of events that may lead the tunnel system from an initiating event to an undesirable end state (i.e. the evolution of the accident scenarios).
3. Consequence estimation models to calculate the expected number of fatalities for the identified accident scenarios, mainly by adopting the ASET/RSET criterion. Smoke dispersion calculations (varying from simple empirical relationships to complex CFD models) are used for fire scenarios in order to estimate the extent of the areas where the consequences may cause fatalities to the exposed population. Then, evacuation calculations are employed in order to predict the exposed population (i.e. the expected number of people in those areas), varying also from empirical relationships to complex simulation models.
4. After obtaining probability and fatality for each accident scenario, the societal risk and the expected value of fatalities is estimated and evaluated.

Brainstorming, root cause analysis, HAZOP, What-If approach, FMECA and checklists can be used in order to identify hazards (i.e. sources of potential harm) and the initiating events. Fault trees and event trees are usually constructed in order to describe the combination of the system states that may lead to the undesirable end states (see an example of an event tree in figure 13). Concerning the consequences of the examined accident scenarios, a large number of models may be employed. Similar to the scenario-based approaches, these may include fluid dynamics for modelling smoke propagation, and several models for describing the evacuation process.

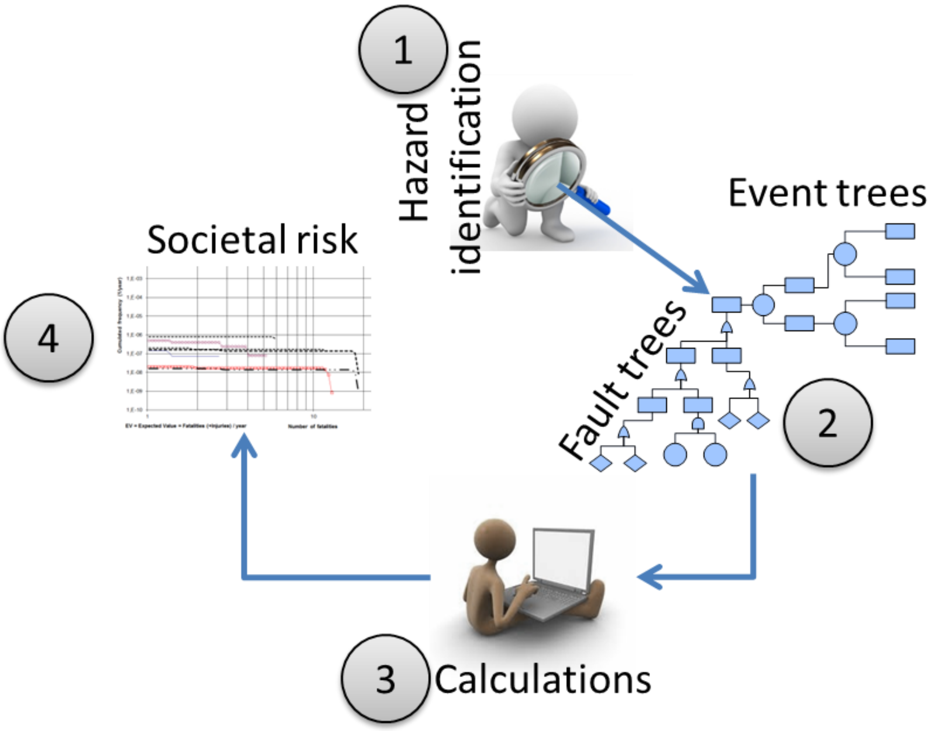


Figure 12: The general steps of a road tunnel QRA

The evaluation of system-based approaches is made mainly on the basis of the societal risk, presented by FN curves and the Expected Value (EV) formulation (PIARC 2013). In particular, FN curves (figure 14) are frequency-consequences graphs plotted on a double logarithm scale which presents the cumulative frequencies (F) of accidents involving N or more fatalities. Typically, the units of frequency correspond to a period of one year. When F/N curves are employed the risk evaluation is made either on a comparative basis (comparison to alternative routes or to a reference situation) or according to the positioning of the F/N curves in relation to acceptable limits. For practical applications such acceptable limits might be underlain by the ALARP principle, in which risks should be reduced As Low As Reasonably Practicable (Kirytopoulos et al. 2010b). The EV is another way to present the societal risk. The EV is the long-term average number of statistically expected fatalities per year and it is equal to the probability of the accident occurring multiplied by the number of fatalities expected to be caused. Hence, the risk is expressed as a single number and risk evaluation is based on the comparison of the resulting EV with a defined maximum threshold which defines the acceptable level of risk. If the estimated risk is lower than the threshold then the risk is regarded acceptable, otherwise it is regarded inacceptable (PIARC 2013).

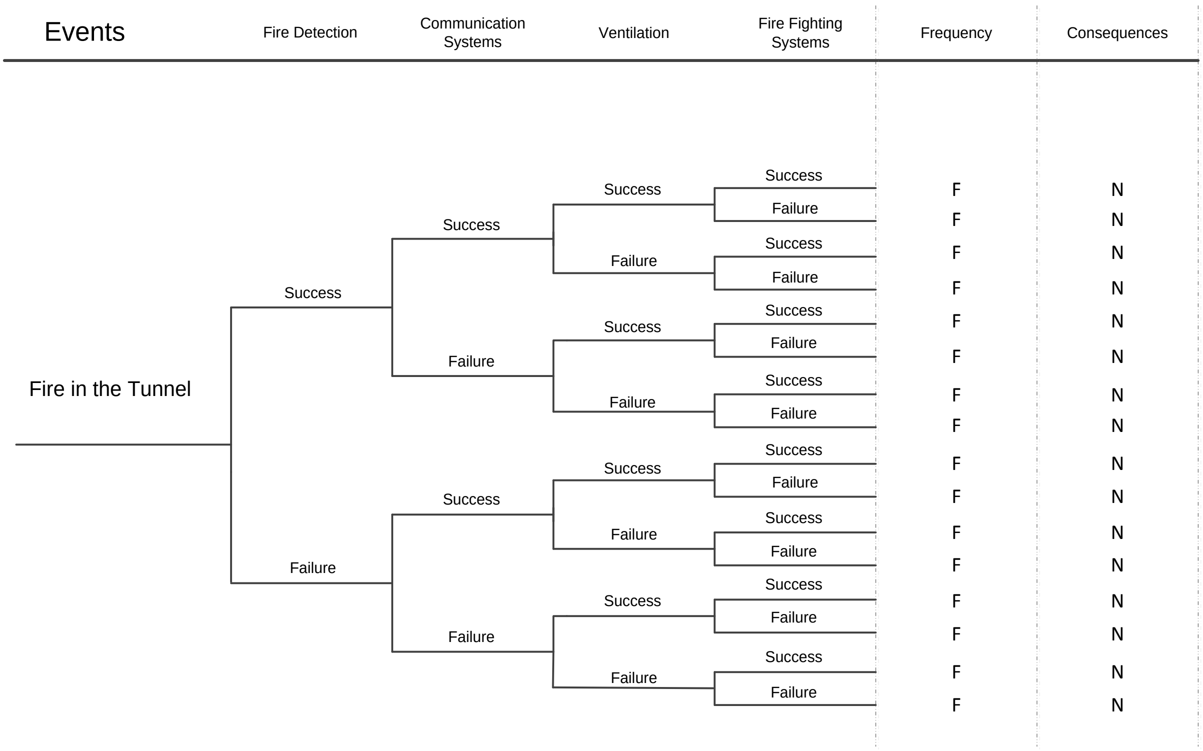


Figure 13: An event tree example of a road tunnel QRA

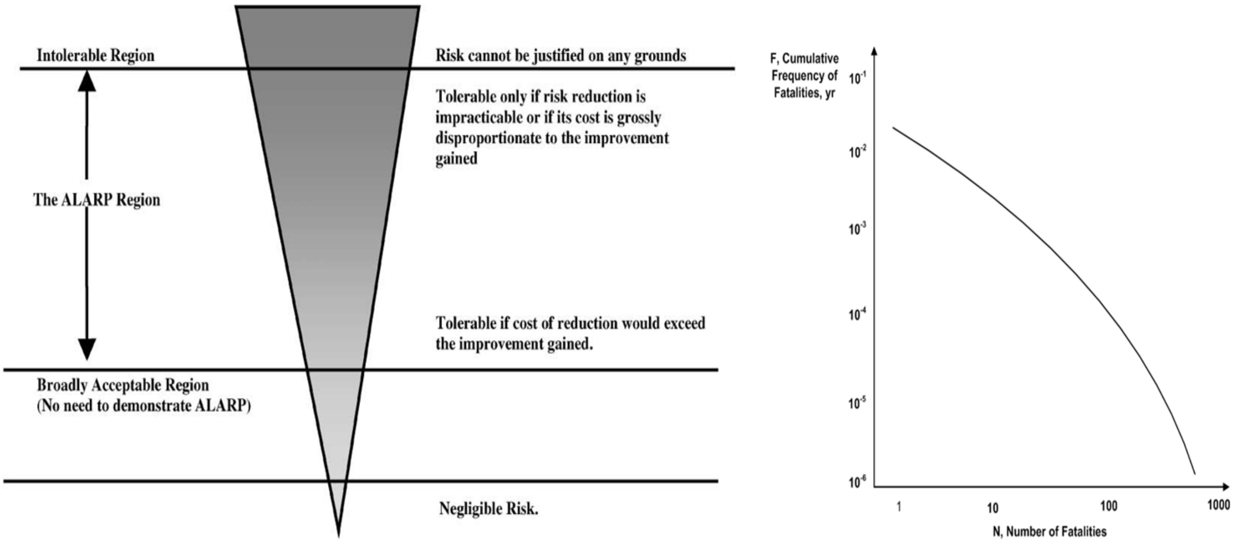

Intolerable Region
Risk cannot be justified on any grounds
Tolerable only if risk reduction is impracticable or if its cost is grossly disproportionate to the improvement gained
The ALARP Region
Tolerable if cost of reduction would exceed the improvement gained.
Broadly Acceptable Region (No need to demonstrate ALARP)
Negligible Risk.
F, Cumulative Frequency of Fatalities, yr
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
10^{-6}
1
10
100
1000
N, Number of Fatalities

Figure 14: An FN curve and the ALARP criterion

Having determined the risk level, the main purpose of a system-based QRA is to choose the risk-reducing safety measures that serve at least one of the following aspects: (1) may reduce the probability of the accident occurring, (2) reduce the consequences of accidents in case they occur (PIARC 2008a). Preventive measures may include: reduced speed limits, speed controls, prohibited lane change, prohibition of transport of DGs through the tunnel, portal inspections, etc. On the other hand, mitigation measures are related to: ventilation system, fire-fighting equipment, communication systems, evacuation supporting systems, facilities to close the tunnel, drainage system, illumination system and emergency procedures. Following the general framework presented above, several system-based QRAs exist in the road tunnel field, with the most cited ones in the literature being: the Austrian tunnel risk model TuRisMo, the Dutch TUNPRIM RWS-QRA model, the OECD/PIARC DG-QRAM model and the QRAFT model.

TuRisMo (refer to PIARC 2008a for a thorough presentation of the method) focuses on equipment related incidents and fires in which small and medium sized fires are involved. The main influencing factors that are taken into consideration by the model are related to: (1) the traffic conditions (e.g. traffic volume, portion of HGVs, speed, frequency of traffic jams), (2) the infrastructure's characteristics (e.g. type of tunnel, distance of emergency exits, cross section geometry), (3) the ventilation system (type of ventilation, response time to activate ventilation, etc.), and (4) the evacuation process (e.g. signaling, alarm and information systems supporting self-evacuation). The model incorporates an event tree analysis for describing the sequence of events that start with an initiating event (i.e. fire accidents and collisions) and end to an undesired end state. Tunnel accident rates (i.e. a statistical approach) are used in order to define the probabilities of both initial events and undesired end states. To estimate the consequences of accident scenarios, TuRisMo combines a smoke propagation model with an evacuation model. The smoke propagation is based on a ventilation simulation model which considers different design fires (e.g. 5MW and 30MW) and different ventilation regimes. The evacuation simulation is also supported by a software package which considers the effects of the smoke according to the Fractional Effective Dose (FED). For accident scenarios relating to traffic incidents, the consequences are estimated only on a statistical approach. For this purpose, a relevant database supports the estimation process. The evaluation of risk is based on the EV formulation and respective shares of risk are presented separately for equipment related incidents and fires. The EV produced by the model is compared either by a reference tunnel (a tunnel with the same characteristics complying with the EU Directive) or by absolute risk criteria. TuRisMo can be used for a wide range of applications (e.g. safety assessment of new or existing tunnels) and covers all types of road tunnels with longitudinal or transverse ventilation. However, the model does not consider accident scenarios in which DGs are particularly involved. In addition, the results of the model do not include information about the distribution of fatalities related to accidents probability (i.e. FN curves), thus the model is not suited to investigate accidents with very low probability and very high consequences (PIARC 2013).

The TunPrim RWS-QRA model (Weger et al. 2001) is a spreadsheet model which focuses on estimating the risk level of unidirectional road tunnels. The model is built on initiating events which are related to collisions, fires, explosions, and release of toxic gases. The assigned probabilities for the initiating events are based on accident rates, and an event tree analysis is employed to estimate the probabilities for the undesired end states. Specifically, the first branches of the event tree describe the traffic situation (e.g. period of the day, traffic jam) and the following branches determine the location of the accident and the type of the vehicles involved. To assess the consequences of the accident scenarios three categories of fatalities are considered. The first category incorporates victims due to traffic accidents. The second includes victims that are severely injured due to traffic entrapment in a vehicle under fire and the last category comprises victims from fires, explosion and releases of toxic gases. The number of injured users due to traffic accidents is derived from statistics, whereas the number of fatalities due to traffic entrapment in a vehicle under fire and the number of fatalities related to fires and explosions is estimated on the basis of a combination of statistics and conditional probabilities The results of the analysis performed by the model are presented in the EV formulation and the relevant FN curves. The model can be used to compare alternative routes, to calculate the influence of specific risk reduction measures and to support decision making related to the transportation of DGs through the tunnel. However, a limitation of the model is the lack of rigorous modelling techniques for smoke propagation and tunnel users' evacuation.

The OECD/PIARC Dangerous Goods QRA Model (DG-QRAM; INERIS 2005) has been developed by INERIS, WS-Atkins and the Institute for Risk Research. The aim of the DG-QRAM is to quantify the risks due to transport of DGs on given routes of the road system. A complete assessment of the risks involved in transporting DGs would require consideration of all kinds of dangerous materials and other general variables such as meteorological conditions. As the coverage of all circumstances is very difficult in practice, simplifications are made and the DG-QRAM considers 13 specific accident scenarios. These accident scenarios are representative of the groupings of DGs as described in ADR and have been chosen to examine different severe effects such as overpressure, thermal effect and toxicity. The quantitative probability analysis of the model is based on accident rates and conditional probabilities. The consequences analysis is supported by a specific spreadsheet tool which is called ‘pre-conditioner’ that determines the area in the tunnel affected by each scenario and the related consequences. The outcome of model is presented in the EV formulation, as well as the relevant F/N curves, and the risk evaluation is made either on a comparative basis (comparison to alternative routes) or according to the ALAPR principle (Kirytopoulos et al. 2010a).

The QRAFT model (Meng et al. 2011) has been developed by the National University and the Land Transport Authority of Singapore. The model focuses on estimating the risk in nonhomogeneous road tunnels i.e. road tunnels in which tunnel characteristics such as traffic volume and geometry vary from one section of the tunnel to another. The model firstly divides the nonhomogeneous road tunnel into a number of homogeneous sections and for each section analysis is performed to estimate the risk. Then risk integration principles based on particular criteria are applied to estimate the overall risk of the tunnel. The QRAFT model consists of seven initiating events (i.e. fire, flood, toxic gases, tunnel collapse, collision, explosion and spillage due to DGs) and an event tree analysis is used in order to describe the accident scenarios triggered by these initiating events. The probability of each particular accident scenario is estimated by multiplying the probability of the initiating event and the probabilities of sequential events associated with the particular scenario. Various models are employed in order to estimate the consequences of the accident scenarios and the performance of 19 electromechanical safety systems is taken into account when estimating the estimated number of fatalities. The overall risk is presented by the relevant FN curves.

Other similar system-based approaches (based on event/fault tree analysis combined with consequences estimation models) which have been proposed are: the Italian risk analysis model (IRAM; PIARC 2008a), the German BASt model (PIARC 2013), a probabilistic risk assessment method proposed by Nyvlt et al. (2011), a Quantitative Risk Analysis Procedure proposed by Persson (2002) and Tusi model (PIARC 2008a). In addition, Sacammano and Haastrup (2002) have proposed a method to evaluate the influence of safety measures when transporting DGs through tunnels (a method which basically enhances the DG-QRAM by considering additional safety measures) and Babbico et al. (2009) have introduced a simplified method for analyzing DGs transportation. On the other hand, alternative methods based on Bayesian Probabilistic Networks rather than event/fault tree analysis have been proposed by the TRANSIT model (Schubert et al. 2012) and Holicky (2009). PIARC report (2008a) presents a brief review of some QRAs which are currently used. It is notable that although papers and reports abound in the literature on the issue of road tunnel QRAs, few of them (refer for example to Kirytopoulos and Kazaras 2011; Kazaras et al. 2012) focus on the limitations and the challenges that should be meet for further improvements. This issue is exhaustively discussed in the next section.

3.2 Challenges for the acceptance of current road tunnel QRAs

Risk assessment is explicitly requested by the EU Directive 2004/54 with the main purpose to reveal, avoid or modify the causes that may lead to accidents. In this section, the main challenges for the acceptance of current road tunnel QRAs are thoroughly discussed.

3.2.1 Human factors

The term "human factors" and "human error" are often used interchangeably and without a clear understanding of their meaning. Although the traditional definition of human factors is "*the scientific study of the interaction between man and machine"* (Khan 2008), in this section we concentrate on human factors in the risk management process, meaning that the emphasis is on capturing potential human's contribution to the accidents' causation. In this sense, challenges on the acceptance of current road tunnel QRAs are mainly related to modelling: (1) the tunnel users' evacuation process, and (2) the tunnel operator's performance.

3.2.1.1 Modelling the evacuation process

A common step for all current road tunnel QRAs is related to modelling tunnel users' evacuation process. Concerning this area of research, several models have been proposed (e.g. cellular automata models, agent based models and flow based models; Ronchi et al. 2013). However, the subject still remains elusive (Nilsson et al. 2009; Zarboutis and Marmaras 2007) since there are many intrinsic uncertainties in capturing:

- the pre-evacuation time (e.g. reluctance of people to abandon vehicles)
- the social influence (e.g. herbing behaviour)
- the local interaction between the evacuees and their environment (e.g. the influence of signaling and other safety measures)
- the fire influence on walking speed

In particular, pre-evacuation time can be divided in: (1) detection time, i.e. awareness that something is happening, and (2) reaction time, which represents the time spent until people decide to evacuate. Both times are greatly influenced by technical systems, such as: alarms, sirens, loudspeakers, broadcasted radio messages and variable message signs. Social influence also impacts the pre-evacuation time since humans are greatly affected by the behaviour of others, meaning that if one starts to evacuate others may follow. As far as the evacuation time is concerned, it is noted that the walking speed of the evacuees may vary from 0.3 m/s up to 1.25m/s accordingly to the radiation, temperature and smoke level in the infrastructure (Ronchi et al. 2013). Therefore, a question arisen is whether all the aforementioned aspects which greatly influence tunnel users' evacuation are taken into account by current road tunnel QRAs.

At this point, it must be mentioned that current evacuation models are based on different methodological steps. Therefore, the obtained Required Safe Egress Time (RSET) may considerably differ according to the model being used. In particular, Ronchi et al. (2013) compared the results obtained from four state of the art evacuation models (FDS+Evac, STEPS, Simulex, Pathfinder) and observed significant differences in their estimated RSET. The authors note that these differences are related to the limitations of current evacuation models to precisely reproduce the fire conditions affecting the evacuation process and to capture the variability of human behaviour. All in all, research concerning human behaviour during tunnel evacuation is still at an early stage and further evacuation experiments should be carried out to improve the accuracy of the evacuation models. Therefore, it is of utmost importance for the analyst performing a QRA to be fully aware of the modelling assumptions and limitations which may result in great underestimation (or overestimation) of the true risk.

3.2.1.2 ***Modelling tunnel operator's performance***

Road tunnel operators have a fundamental role in the safe operation of road tunnels with their role including among others: (1) the continuous monitoring of the traffic, (2) the detection of critical events, (3) the assistance of rescue operations and evacuation. However, their great contribution to the overall tunnel safety is underestimated by current QRAs, which only reflect tunnel operator's performance variability in modelling input parameters such as: time to close the tunnel in case of an emergency and time to activate emergency ventilation. It is notable that such inputs parameters are determined by the analyst either on the basis of the relevant literature or they are just arbitrary estimations. In this sense, the "error-prompting context" and the performance shaping mechanisms are totally neglected from the analysis. It is important for road tunnel QRAs to take into account aspects such as:

- Task support, control room and interface design: The systems available for informing the tunnel operator about the operating status in the tunnel (e.g. cameras, CO sensors, smoke sensors, communication systems, alarms, etc.) and the systems in place for controlling events (e.g. ventilation, barriers, variable message signs) should be thoroughly considered by QRAs, since it is the availability, reliability and effectiveness of such systems that determines the performance of the tunnel operator and not randomness.
- Recruitment policy, training and organizational procedures: A road tunnel QRA should search for organizational deficiencies that may affect the operator's performance. For example, such deficiencies may include a poor recruitment policy that does not ascertain that the operator is able to handle stress and communicate effectively in emergency situations.

Following this line of thought, Kazaras et al. (2013) have proposed a fuzzy system based on the CREAM methodology in order to provide more sophisticated estimations for the tunnel operator's performance in safety critical situations. Their proposed system takes into account various performance shaping mechanisms, such as: the adequacy of man-machine interface, the availability of procedures and the adequacy of training and experience. Nevertheless, further enhancements should also be proposed, given that they meet the following requirements: (1) have a causal model of human response with roots in cognitive and behavioural sciences, and (2) be detailed enough to support data collection and experimental validation.

3.2.2 Organizational aspects

Management shortcomings, organizational aspects and the safety culture have been recognized as major factors in the occurrence of accidents in complex systems (Leveson 2004; Rasmussen 1997; Reason 1997). As a result, the effect of organizational factors on QRAs has attracted great research effort and still poses a challenging research agenda at the interface of engineering and social science. Despite this effort, in current road tunnel QRAs a solid framework to describe organizational factors has not been proposed yet. Organizational responsibilities in the tunnel field may vary from country to country; however, common organizational aspects that greatly affect safety include: (1) traffic management, (2) maintenance and inspection of the tunnel, (3) recruitment of the tunnel personnel and its training procedures, (4) preparation of emergency plans, (5) planning of emergency exercises and co-operation with the emergency services, and (6) analysis of past incidents and learning from events. All the aforementioned responsibilities are undeniably safety critical and the fact that they are not included in the analysis may hinder an accurate safety assessment process. Questions such as "what are the organizational factors that affect risk", "how do these factors influence risk?" and "how much do they contribute to risk?" should be taken into account.

3.2.3 SCADA system's software behaviour

SCADA systems are widely used in modern road tunnels to monitor and control equipment. The SCADA allows efficient maintenance and proper reaction of the tunnel operator in case of an emergency and, usually, it monitors and controls the following equipment:

- Power supply system
- Tunnel ventilation system
- Fire-fighting system
- Fire detection system
- Tunnel communication system
- Traffic management system

In order to ensure its safe operation, the SCADA software is usually required to be written in accordance with the latest issue of an internationally recognized standard. Such a requirement ensures reliability but not necessary safety. Garret and Apostolakis (1999) state: "*Software reliability assessment and software risk assessment are entirely unrelated. Reliability assessment is considered with the probability that the execution of the code will deviate from its specifications, whereas risk assessment is concerned with the likelihood that a software action will lead to the occurrence of a hazardous condition*".

Therefore, QRAs in the road tunnel field should investigate which actions of SCADA might lead to the occurrence or to the escalation of an accident. The question is whether the QRA modelling can capture accidents arising from the SCADA's software operation. Leveson (2012) presents an interesting concept stating that "*the "software failure" box found in many fault trees of QRAs might be a sign that this method has reached its efficacy limits in the analysis of software accidents. Trying to calculate the probability that the software will "fail" and reflect it in fault/event trees by containing boxes that indicate "Software Fails" does not make sense without first understanding in what ways the software may lead to the occurrence or to the escalation of an accident*". The behaviour of the SCADA software is not random and in this sense software is not a source of uncertainty that should be treated in probabilistic terms. Indeed, the SCADA system will act as it has been designed to act, thus the source of uncertainty is really in the context which may force the software to produce the hazardous result. The crucial point is that this context has several limitations to be actually assessed by QRA methods, mainly because software does not follow physical laws of degradation or failure like mechanical components do (Zio 2009).

3.2.4 Systems complexity and dynamic nature of risk

As the design of tunnel equipment systems has become more reliable, the causes of accidents are more likely to be attributed to the interactions among the tunnel's systems rather than due to individual system's failures. Examples of unpredicted and hazardous interactions that may occur in a road tunnel are the following:

- Unsafe interaction between fire-fighting and ventilation system, i.e. water droplets may be affected by the air flow provided by the tunnel ventilation system (Carvel 2009).
- The tunnel communication systems may be disturbed due to high noise resulting from the operation of the ventilation system.
- High ventilation velocity in the tunnel may affect the ability of fire detection systems to quickly detect smoke (Arralt and Nilsen 2009).

In the aforementioned examples none of the components fails to fulfill its requirements. Instead, it is the interaction among perfectly functioning components that creates hazardous system states. For example, the great majority of the ventilation systems fulfill their operating requirements (i.e. to control smoke) by producing high air velocities. However, most fire-detection systems have been demonstrated to work more reliably at low ventilation velocities. The point made is that treating such events as independent (like current road tunnel QRAs do) may lead to unrealistic tunnel risk assessment and to an underestimation of the true risk.

Another challenge of current road tunnel QRAs is related to the adaptation of the system over time. When looking at current road tunnel QRAs it seems that there is no link between the design stage conditions and the actual conditions of the tunnel. In this static view, it is implied that the tunnel equipment and the safety measures do not degrade over time. This seems to be a narrow perspective since adaptation or change is an inherent part of any system, particularly those that include human and organizational components (Rasmussen 1997). The critical factor is that such adaptation is not a random process thus should be predictable and controllable, meaning that the factors that may lead to the degradation of the overall safety should at least be identified.

3.2.5 Lack of data and uncertainties

As has been presented in figure 12, the process of a road tunnel QRA can be divided in four modelling steps. For each of these steps, several sources of uncertainty can be identified. Concerning the first two steps, the sources of uncertainty are related to the possible incomplete identification of hazards and accident scenarios. In the road tunnel field, the selection of the accident scenarios is often made on a basis of a check-list approach and -as it has been extensively discussed in this section- there is considerable shortage in exploring human and organizational aspects, software behaviour, dysfunctional interactions among system's components and the adaptation of the system over time. Therefore, several important factors related to the overall tunnel safety and major potential causes of accidents are totally omitted from the assessment.

As far as modelling the consequences of the accident scenarios is concerned (i.e. step 3), the uncertainty that is related to the evacuation models and to the tunnel operators' performance has been extensively discussed. On top of that, another major source of uncertainty is related to modelling smoke and heat propagation, which is a fundamental step of current road tunnel QRAs. As Haack (2002) notes, it is very difficult to estimate the consequences of tunnel fires since it is hard to predict precisely how a fire may develop due to the numerous specific conditions that may influence the situation (e.g. number and type of burning vehicles, location of fire, number and behaviour of tunnel users, time to activate appropriate actions etc.). "*Tunnels do not burn but vehicles do*" (Haack 2002) and this fact is actually posing great variability in the fire phenomenon. The limitations of models to calculate smoke and heat propagation are extensively discussed by Beard (2005). Apart from the fire phenomenon itself, uncertainties in this step of the analysis are also associated with:

- Traffic data (e.g. uncertainties related to: traffic volume, portion of DGs in the traffic, number of people in vehicles and speed of vehicles).
- The performance of safety systems (e.g. uncertainties related to their reliability).
- Variability of the environmental conditions.
- The choice of lethality thresholds for humans (e.g. the Fractional Effective Dose is also questionable).

Related to step 4 (i.e. estimating the risk level) there are significant uncertainties related to the probabilities estimates. Probability in a risk assessment context can be interpreted in the statistical sense (i.e. frequentist probability) or as a measure of uncertainty of future events (i.e. subjective probability). To the best of the author knowledge, the great majority of current road tunnel QRAs adopts the frequentist approach. In this perspective the probability of a fire accident is interpreted as the fraction of time a fire accident is present in the examined road tunnel when considering an infinitive number of operative years of the examined (or similar) road tunnel(s) (Bjellend and Aven 2013). However, frequentist probabilities can be justified only for these situations for which a repeatable experiment can be conceived (refer to section 3.1.2.2). It is hard to introduce a "repeatable experiment" in this case, unless the definition of "an infinitive number" of years and "similar tunnels" is interpreted quite loosely (Bjellend and Aven 2013). Indeed, statistics and accident rates that have been estimated in one particular road tunnel might not be applicable to another, since there might be several differences in the elements constituting the road tunnel system.

Moreover, road tunnels are dynamic systems continually changing (e.g. different safety systems, procedures, operators, traffic volumes, vehicles, etc.), and frequentist probabilities might not be justified even for a single tunnel. In addition, from the practical point of view, it is also notable that few tunnel organizations keep a uniform, comprehensive and obligatory reporting system of accidents and incidents (Beard and Cope 2008). Considering this lack of accurate statistical data, it is open to question whether a reliable probability model which can be used to predict future occurrence of accidents can be utilized.

Finally, the evaluation of the estimated risk is affected by all the types of uncertainty introduced in the previous steps of the analysis. Risk evaluation is made on a comparative basis (e.g. by comparing the estimated risk to the risk of a reference tunnel which is usually one in line with prescriptive requirements) or on the basis of risk acceptance criteria. In the first case, the uncertainties are related to the reference tunnel and to the underlying assumption that the prescriptive reference design constitutes, undeniably, a safe tunnel. Nevertheless, this may not be true (take into account that the prescriptive reference design is based on "magic numbers" and on large scale tests which have been performed 40 years ago). In the latter case, the uncertainties are associated with defining the proper risk acceptance criteria and concluding to an acceptable risk level (acceptable for whom?) that meets the necessary safety requirements. The ALARP principle is often utilized to highlight that risk should be reduced as low as reasonable practicable. However, there is a number of areas of concern and controversy about the validity of this approach, as it is extensively discussed by Melchers (2001).

4 Responding to the “residual” risk

4.1 Potential areas for improving road tunnel QRAs

In the previous section, it has been thoroughly presented that current road tunnel QRAs have several limitations to consider some of the most important factors that influence road tunnel safety, such as: organizational aspects, system accidents (i.e. accidents occurring from the interaction of the tunnel system’s components), software behaviour, human factors and the adaptation of the tunnel system over time. As far as potential areas for improvements are concerned, attempts should be made to incorporate human and organizational aspects in the risk assessment process -as it has been already attempted in other industries (the interest reader is referred to Mohaghegh et al. (2009)). In this line of research some efforts have been made by Kazaras et al. (2013) but there is still significant progress to be made. To cope with the dysfunctional interactions among system components (in particular with some common cause failures), road tunnel QRAs should be enhanced with common-cause-failure analysis and it is also possible to utilize Bayesian Belief Networks in order to describe the relationships among the various elements constituting the tunnel system. Concerning software behaviour and the dynamic nature of risk, it seems that little progress can be made. Indeed, it seems awkward to model the software behaviour in probabilistic terms since software’s behaviour is almost always deterministic.

The area that seems to have the most potential for improvement is related to the uncertainty representation. Based on the results of QRAs tunnel companies may plan to spend large amounts of money. Hence, the uncertainties underlying the estimated risk numbers should be clearly represented. Some considerations on the treatment of road tunnel QRAs’ uncertainties can be found in Meng and Qu (2012) where the authors propose a Monte Carlo-based method to propagate parameter uncertainty. However, many of the uncertainties which have been discussed in section 3.2.5 are still not adequately handled. The great majority of current road tunnel QRAs omits to highlight several uncertainties in phenomena, processes and manageability factors. They often present the overall risk in a single value (i.e. the EV formulation) and although they provide predictions of the future (i.e. the expected number of fatalities) they do not highlight the fact that some risks are more manageable than others, meaning that the potential for reducing the risk is larger for some accident scenarios compared to others. At this point, sensitivity analysis may be a useful tool to represent how changes in particular input parameters affect the outcome results.

Furthermore, it is important to introduce different representations formats for uncertainty due to observed variability (i.e. stochastic uncertainty; for example: traffic volume and failure rates of safety systems) and uncertainty due to incomplete information (i.e. epistemic uncertainty; for example: the reaction time of the tunnel operator to activate safety critical systems). In cases of stochastic uncertainty, action should be taken to circumvent the potential dangerous effects of such variability whereas in case of epistemic uncertainty more information should be collected (Dubois 2010).

Additionally, the knowledge (i.e. evidence part) and the analyst's judgment are seldom reflected in current approaches. Aspects such as: the expected number of fires in tunnels (i.e. accident rates), the propagation of smoke and heat, the modelling of the evacuation process, the performance of the safety systems and the performance of emergency services are based on several assumptions. Therefore, an important part of road tunnel QRAs should be to describe these assumptions and the background knowledge that forms the basis of the assessment. Bjelland and Aven (2013) suggest several aspects that should be considered in such an uncertainty representation. Moreover, it should be crystal clear what do the probabilities that are incorporated in the analysis reflect. Are they just frequencies or are they knowledge-based (subjective) probabilities? All this background knowledge should be represented and qualitative tools should be utilized if the underlying uncertainties cannot be transformed in mathematical formula.

Concluding, it is mentioned that the basic idea of QRAs is to use information available at the component level to assess the accident risk at the system level. It goes without saying that the safety assessment should consider all aspects that affect the overall safety of the tunnel system, since the purpose of the assessment is to identify weak points, propose for additional safety measures and design emergency plans. However, it should be kept in mind that road tunnel risk assessments are requested for every European tunnel longer than 500m. Hence, the appropriate balance between simplicity and accuracy should be made. All in all, current road tunnel QRAs represent a narrow framework and for this reason they should not be the single criterion for the safety assessment process. This point of view is extensively discussed in the following section.

4.2 Making a swift in the accident modelling paradigm

4.2.1 The underlying chain-of-event accident model in road tunnel QRAs

Many of the aforementioned challenges and limitations of current road tunnel QRAs (some of which are indeed general challenges of QRAs), can be ascribed to the chain-of-event accident model which underlies the QRA modelling. Accident models (often called accident causality models or accident causation models) are concentrating on describing the causes of accidents, i.e. the accident "mechanisms" (Hollnagel 2004; Nivolianitou et al. 2004). The purpose of accident models is twofold: they are used to understand past accidents and to prevent future ones. Particularly, in accident analysis they influence the data collected and the factors identified as causative, whereas they underlie all efforts to prevent accidents, such as hazard analysis, risk assessment and safety assessment (Leveson 2004). Like any other model, an accident model is just an abstraction of reality which is utilized to neglect what is assumed to be irrelevant and superfluous, whereas to highlight the aspects which are regarded to be the most relevant for the analysis. Several classifications of accident models have been proposed in the literature, however, for the needs of this thesis the classification proposed by Leveson (2012) dividing accident causation models in chain-of-event models (linear) and systemic (non-linear), is adopted.

Chain-of-event accident models conceptualize accidents as a chain of events which almost always involve some type of technical failure, human error or energy related event (e.g. fire, explosion, etc.). Such chains do not need to be single strands but they may include multiple parallel chains synchronized on time by logical conditions, such as "AND" and "OR" Boolean gates, which are often employed to define the relations between the events. For example, forward chain methods (e.g. FMECA and event trees) start form an initiating event and proceed forward by considering how this event may develop to an undesirable end state, whereas backward chain methods (e.g. fault trees) may determine the undesirable end state and work backwards to identify the relevant initiating events and all the possible conditions that could lead to it (Leveson 2004).

In the road tunnel field, the chain-of-event accident model is directly demonstrated by the several fault trees and event trees which form the basis of the quantitative part of the QRAs. Furthermore, the chain-of-events accident model is also reflected in the Bow-Tie diagram which actually underpins all safety efforts in these infrastructures (PIARC 2007a). In particular, the influence of safety measures on the evolution of the accidents scenarios can be conceptualized in a Bow-Tie diagram in which several barriers (i.e. safety measures) are employed to stop the sequence of events leading to the undesired end state (figure 15). Following this line of though, the analyst performing a road tunnel safety assessment aims to conclude whether the safety measures (i.e. defense lines) which are currently available within a tunnel are sufficient enough to accomplish the overall safety, or they are not, so recommendations should be proposed and improvements should be made.

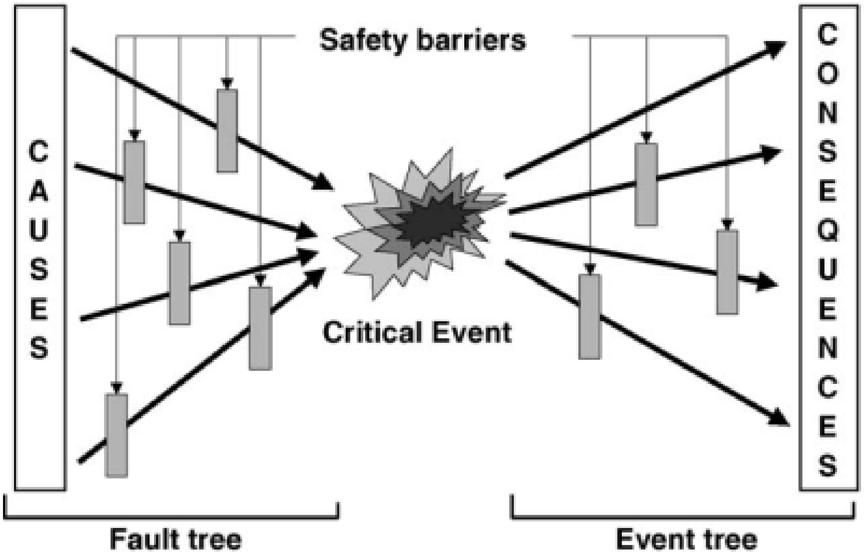


Figure 15: The Bow-Tie Diagram (Dianous and Fiévez 2006)

The main advantages of chain-of-event accident models are related to their simplicity. Fault trees, event trees and other logical trees (e.g. Petri nets) are easy to be used. Moreover, they can represent graphically the assessment, facilitating thus the communication of results. However, such models encourage limited notions of accident causality –linear causality relationships are mostly emphasized- and have several limitations to incorporate non-linear relationships including feedback (Leveson 2004, Woods et al. 2010). Leveson (2004) points out: “*the focus of chain-of-events accident models on failure events does not account for (1) social and organizational factors in accidents, (2) system accidents and software errors, (3) human error and (4) adaptation over time.*”

Considering road tunnels accidents as some unfortunate coincidence of “chain of events” seems to be a narrow perspective. A road tunnel system is not static, therefore, rather than accidents being a chance of occurrence of multiple independent events, they tend to involve a migration to a state of increasing risk over time, a so-called “drift into failure”, i.e. a slow, incremental movement of the tunnel system’s operation towards the edge of its safety envelope (Dekker 2011). This concept is reflected in the common observation that a disaster was “an accident waiting to happen”. Furthermore, when performing a road tunnel QRA, the initiating events are usually assumed to be independent. For example, as presented in figure 13, failure events such as “failure of the fire detection system”, “failure of the ventilation system” and “failure of the fire-fighting system”, are mutually exclusive: each of these failures has its own probability of occurring. However, although this assumption may facilitate the mathematics of the assessment it neglects the fact that in real accidents such independent failures usually have a common systemic cause (which is often neither a failure nor an event). Assigning probabilities to all these unrelated events and assuming independence may lead to unrealistic safety assessments (Leveson 2012).

Let’s consider the Mont Blanc accident for example, which is the most fatal tunnel fire accident until now. In this particular accident, the fire detection systems (from the Italian side of the tunnel), the ventilation system, the lighting equipment and the fire-fighting systems, they all failed to avoid the catastrophe. Such failure events might have been considered independent and such a “coincidence” - in which all safety systems fail - might have been ascribed with a low probability of occurring in a safety assessment performed before the accident. Notwithstanding, such an unexpected “coincidence” appears to be much more likely to occur if one considers the disagreement between the two operating companies of the tunnel on capital investments, which has actually led to the degradation of the overall tunnel equipment (Ministry of the Interior 1999). In addition, taking into consideration the inadequate number of safety exercises and drills which have been performed before the accident, it seems that the lack of co-ordination among road patrollers, emergency services and operators -which has been observed- was not really a random phenomenon but rather an inevitable result of the various organizational and managerial deficiencies (Ministry of the Interior 1999).

As far as the tunnel operators’ performance is concerned, it goes without saying that they did not deliberately aim to result to the escalation of the accident. It was their inadequate mental model of what was happening inside the tunnel (e.g. anemometers were out of order and longitudinal air flows were not recorded) which has significant contributed to their poor performance (Ministry of the Interior 1999). It is also notable, that it was the dysfunctional interaction of the ventilation system’s regimes that led to the escalation of the accident rather than the ventilation’s failure to operate. Particularly, from the Italian side, the ventilation system was configured to supply fresh air whereas, from the French side, the ventilation was utilized to exhaust air. This ventilation imbalance (fresh air supply was not balanced by the exhaust systems) created high longitudinal air flow which resulted in the spreading of fire and smoke within the entire cross section of the tunnel. All in all, the fire in the truck (i.e. the initiating event) may have triggered the loss, but the catastrophe occurred due to systemic causes not just because of an unfortunate coincidence of failure events (Lacroix 2001).

In short, aspects such as: organizational and human factors, dysfunctional interactions among system's components and several other non-linear factors should not be omitted from safety assessments since they can (and actually they have) lead to major tunnel disasters. One may claim that some of aforementioned aspects are currently controlled by organizational processes, such as quality management systems and safety inspection audits. Although such organizational processes are undeniably a step forward in road tunnel safety, it must be mentioned that the interactions among the various elements of the tunnel system may still come unnoticed. For example, a quality management system may ascertain that training is provided to the tunnel operators. However, to consider how the whole tunnel system interacts together, the quality of such training should be evaluated in relation to the specific vulnerabilities which have been identified in a particular tunnel system.

The point made is that although current risk-based safety assessments are often called systemic, they are far from what actually is considered systems thinking. Their systemic part is that they aim to evaluate the overall tunnel safety by examining a respectable number of accident scenarios considering many parts of the tunnel system. But their basis is sustained by the classical Newtonian/Cartesian view of the world, which is founded on the idea that system behaviour can be understood from the behaviour of its constitutive elements (i.e. reductionism) and their causal links (Zio 2009). Such decomposition assumes that the separation of the tunnel system is feasible and implies that the tunnel's subsystems are not subject to feedback loops and other non-linear interactions. However, such an assumption is wrong since road tunnels are complex systems with several interactions among their constituting components.

4.2.2 Road tunnels as complex socio-technical systems

Vicente (1999) notes that a system comprised of technical, managerial and social elements is a socio-technical one. Road tunnels are constituted of human, managerial and technical elements hence they can be understood as sociotechnical systems. But are they complex systems[8]? First, complex systems are open systems, meaning that they are open to

[8] In this thesis something is complex if it involves many parts and if the relations among the parts are not linear (Hollnagel 2012).

influences from the environment in which they operate and they also influence their environment in return (Dekker 2011). Road tunnels are open to transport and influence the area in which they are located by the transportation of people and goods. Moreover, if a major tunnel accident occurs, this may significantly affect the nearby region. So they can be regarded as complex systems in this sense. Second, in complex systems each of the components constituting the system is ignorant of the system as a whole and does not understand the effects of its actions on the behaviour of the overall system (Dekker 2011). In road tunnels, the average tunnel user is ignorant of what the entire road tunnel system actually comprises and, moreover, is ignorant of the effects of his behaviour on the overall tunnel safety. Likewise, the tunnel operator and the emergency services may be incapable of describing how tunnel users behave in case of an emergency.

Third, in complex systems the system itself is much more complex than its constituting elements (Dekker 2011). As far as road tunnels are concerned, it is the complexity of the non-linear interactions that characterize the overall system's behaviour (e.g. safety) and not the behaviour of its constituting elements -as it has been discussed in section 2.2. Fourth, complex systems need inputs in order to keep the system functioning (Dekker 2011). As such, if road tunnel users were stable the system would grind to a halt. Finally, complex systems have a history of path dependence (Dekker, 2011), meaning that their past is co-responsible for their present behaviour. This is significant the case in road tunnels where design decisions affect to a great extent the operation of the system. In a nutshell, **road tunnels can be regarded as complex socio-technical systems and in such systems a framework which is based on reductionism may not fully apt to assess the overall safety which emerges as a whole** (Leveson 2012). Beard and Cope (2008) make their point clear: "*Fatality, injury and harm results from the working of the whole tunnel system. (Safety) risk assessment, therefore, needs to be as systemic as possible. The question is how we do that? […]. Furthermore, the tunnel system is continually changing. How can we create a (safety) risk assessment which is capable of coping with this?*

4.2.3 Shifting from reductionism and chain-of-events to systems theory

Any attempt to manage and evaluate safety requires an underlying model of how accidents may happen. Rephrasing Lundberg's (2009) words, "what you look for in safety assessments is what you actually evaluate and fix". Awareness of risk is a major component of safety-related decision making and in the previous paragraphs it has been thoroughly discussed that QRAs (based on the chain-of-event modelling) have several limitations to consider some of the most important factors that influence road tunnel safety, namely: organizational aspects, system accidents, software behaviour, human factors and adaptation of the tunnel system over time.

A key point made in this thesis is that although QRA methods are essential to predict the physical harm that may occur, they have several limitations to consider an important part of non-technical factors that significantly affect the overall tunnel safety (Kazaras et al. 2012). This does not mean that current QRAs are unnecessary, or that they do not provide important estimations of the expected physical harm. However, it does mean that **it is of utmost importance to be complemented with innovative and sophisticated methods that have the ability to capture the factors that are not adequately handled by current road tunnel QRAs, i.e. to cope with the "residual" risk and provide guidance for responding to it**. Each safety assessment method is based on a model of accident causation, a paradigm that provides a conceptualization of how an accident may occur. Considering the challenges to be addressed in the road tunnel safety field, the accident model which should be utilized to enhance the safety assessment process should meet the following requirements:

1. Considers the entire socio-technical system by taking into account all facets relating the social to the technical aspects.
2. Considers the relationships between the parts of the system, how they interact and fit together.
3. Considers how the SCADA system may contribute to an accident.
4. The entire process of an accident needs to be examined and not just the proximate events. The real causes of accidents must be identified and not only the symptoms.
5. The model must cope with the fact that the tunnel system leading to accidents is continually changing.

To capture the process that leads to accidents and the adaptation of the system over time, what is needed is not another structural, chain-of-event model which simply decomposes the tunnel system into its constitutive elements and focuses on symptoms. What is needed, instead, is a model that is sensitive to the creation of deficiencies, a model which makes the socio-technical road tunnel system to come alive, a model of processes which depicts how the system works together and evolves over time. To achieve the aforementioned goals, a new theoretical pillar is needed for road tunnel safety. **The hypothesis made in this thesis is that systems theory provides the foundation to create a road tunnel safety**

assessment method that has the ability to capture the "residual" risk which is left unnoticed by current QRA approaches.

Systems theory, partly introduced by Ludwig von Bertalanffy, is the response to the limitations of the classic analysis techniques in describing systems that display organized complexity (Checkland 1981). Such systems (e.g. complex engineered systems, biological systems, social systems) are too complex for analytic reductionism[9] and too organized for statistics (i.e. they cannot be treated as aggregates since they have specific patterns). On the other hand, systems theory focuses on systems taken as a whole, not on the parts taken separately. The cornerstone of systems theory is the notion that "*the whole is more than the sum of its parts"*, and its foundation rests on two pair of ideas (Checkland 1981): (1) emergence and hierarchy, (2) communication and control.

In systems theory, complex systems are modeled as a *hierarchy* of levels. A system may be part of a larger system while at the same time it may be built up of subsystems which may themselves be composed of sub-systems (Checkland 1981). In this hierarchy, each level is more complex than the one below since it is characterized by emergent properties. *Emergence* results from the interaction of independent parts when they stop being independent and start influence each other (Skytter 2005). It is also notable that emergent properties which are associated with a set of components at one level in a hierarchy are related to constraints upon the degree of freedom of those components. Hence, constraints are always associated with control actions. As Checkland (1981) notes: "*a control is always associated to the imposition of constraints, and [...] any description of a control process entails an upper level imposing constraints upon the lower*." It is also notable that control in open systems (i.e. systems that exchange input and outputs from their environment) is directly related to *communication*.

Safety can be viewed as an emergent property since it can only be determined in the context of the whole. Hence, safety is controlled or enforced by a set of constraints on the behaviour of the components in the system, including constraints on their potential interactions. In this perspective, safety is a control problem and "*accidents occur when components failures, external disturbances and/or dysfunctional interactions among systems components are not adequately handled"* (Leveson 2012). Whereas, chain-of-event accident models focus on unsafe acts (i.e. events), systems-theoretic accident models look at what may go wrong with the system's operation and organization to allow the accident to take place. The focus of systemic models is not on erroneous actions or failures, but on the

[9] The system will lose its synergetic properties if analytic reductionism is used to examine it.

mechanisms that help generate such behaviours at a higher level of functional abstractions (Woods et al. 2010).

4.2.4 Systems theoretic accident models and techniques

By adopting a systems-theoretic perspective, several systemic accident methods and models have been proposed (refer for example to Goh et al. 2010; Hollnagel 2004; Larson et al. 2009; Moizes et al. 2011). However, two systems-theoretic accident models currently dominate the literature: Rasmussen's (1997) risk management framework and Leveson's (2004) Systems Theoretic Accident Model and Processes (STAMP).

4.2.4.1 ***Rasmussen's risk management framework and Accimap***

Rasmussen (1997) regards risk management as a control problem in socio-technical systems and safety as an emergent property arising from the interactions between the actors involved in the various system levels (e.g. government, regulators, company, company management, personnel and work; figure 16). Each level is involved in risk management via the control of hazardous process through laws, rules and instructions. For example, the top level describes the activities of government who control safety through legislation (e.g. the European Directive 2004/54). The second level depicts the activities of regulators and associations that are responsible for implementing the legislation in their sector (e.g. administrative tunnel authorities). The third level describes the activities of a particular company (e.g. a highway company) and the fourth level involves the activities of the management in the company (e.g. tunnel manager) that lead, manage and control the work of their personnel. The fifth level depicts the activities of the individual personnel (e.g. tunnel operator, maintainers, emergency response team) that are interacting directly with the processes being control (e.g. tunnel operation). Finally, the sixth level describes the application of engineering principles which are involved in the design of the equipment and procedures to control the system.

Although, each level of the framework is studied separately, Rasmussen highlights the need that the organizational and management decisions made at higher levels should transmit down the hierarchy, whereas information regarding the processes at lower levels should propagate up the hierarchy. Without this so called "vertical integration", systems can lose control of the processes that they are designed to control. Therefore, accidents can be caused by decisions and actions at all levels of the socio-technical system and not just agents at the "sharp-end". In particular, Rasmussen and Svedung (2000) outlined the Accimap method to graphically represent the system failures, decisions and actions involved in accidents, by considering control flaws across the six organizational levels mentioned above.

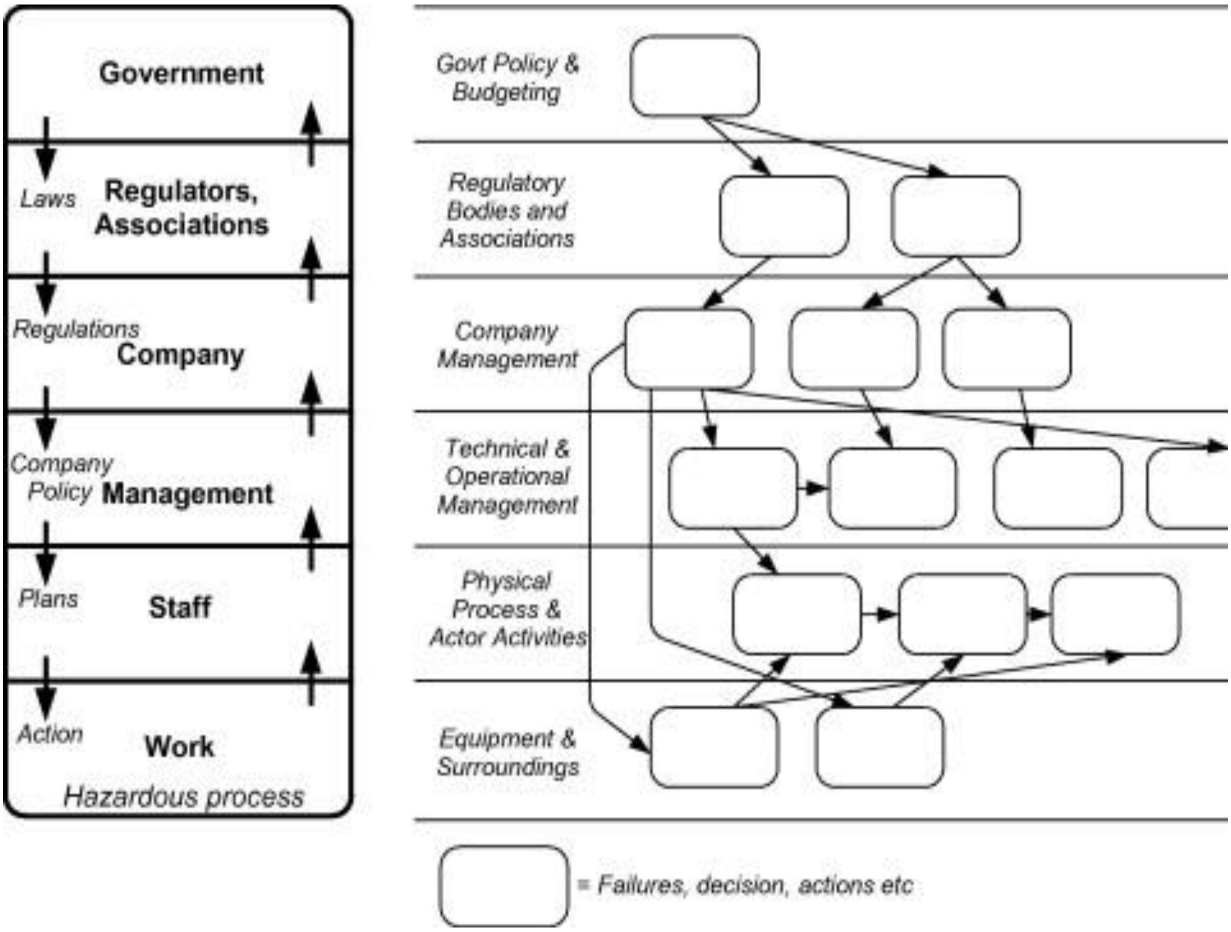


Figure 16: Rasmussen's risk management framework and Accimap method (Salmon et al. 2012)

*4.2.4.2 **Leveson's STAMP accident model***

STAMP has been recently proposed by Leveson (2004) and is based on two fundamental concepts from systems theory: (1) emergence and hierarchy, (2) communication and control. In this systems-theoretic approach, safety is an emergent property that is achieved through the enforcement of constraints. Hence, it is the inadequate control or enforcement of safety constraints on the design, development and operation of the system that mainly causes accidents not just a series of random events. STAMP includes traditional failure-based models as a subset but goes beyond physical failures to include causal factors involving interaction among non-failing components, software and design errors, errors in human decision-making and various organizational and managerial factors (Leveson 2004).

The three basic elements of STAMP are:

1. Safety constraints that specify what relationships among system components are important to achieve non-hazardous system states. Leveson (2004) emphasizes safety constraints, rather than failure events, as the most basic concept in safety. Instead of viewing accidents as the result of events, accidents are considered to be the result of the interaction among components that lead to the violation of safety constraints. The controlled processes (organizational and technical) that enforce these constraints must limit system's behaviour to the safe changes and adaptations. Therefore, a socio-technical control structure should be established that controls these processes and enforces the necessary constraints on the development and operation of the system.

2. Hierarchical control structures that enforce safety constraints. A hierarchical model of stakeholders is posited in STAMP (figure 17) that expands on the model of Rasmussen. Every level of the hierarchy can impose its own safety constraints on lower levels which in turn contribute to system safety. As Leveson (2004) states: "*While (failure) events reflect the effects of inadequate enforcement of safety constraints, the inadequate control itself is only indirectly reflected by the events, (meaning that) the events are the result of the inadequate control. Hence, the control structure itself must be examined to determine why it was inadequate to maintain the constraints on safe behaviour and why the events occur*".

3. Process models and control loops. Hierarchies in systems theory are characterized by control and communication processes operating at the interfaces between levels. Each hierarchical level of the safety structure represents a control process (i.e. a control loop) with a downward channel providing information or commands to the level below and an upward channel providing feedback about how effectively the constraints have been enforced. Finally, all controllers at all levels of the hierarchy must have a model of the process being controlled (i.e. a model of the system). Briefly, whether the model is embedded in an automated controller or maintained by a human controller "*it must contain the same type of information: the required relationship among the system variables (the control laws), the current state of the process and the ways the process can change state*" (Leveson 2004). Figure 18 presents a basic control loop in STAMP.

In this systems-theoretic approach STAMP allows safety problems to be transformed into control problems for which sophisticated tools can be employed. When used for safety assessments, STAMP produces a description of the safety control structure and identifies inadequate control actions that may lead to the violation of safety constraints and consequently to accidents. In STAMP terms there are four types of potentially inadequate control actions that may lead to accidents. These are:

1. A control action required for safety is not provided.
2. An unsafe control action is provided.
3. A potentially safe control action is provided too late, too early, or out of sequence.
4. A safe control action is stopped too soon or applied too long.

Moreover, to support the investigation of why an accident may occur, additional analysis should be performed so as to identify the control flaws that may lead to the inadequate/enforcement of the safety constraints (i.e. to the inadequate control actions). For this step, Leveson (2004) proposes the classification of control flaws depicted in figure 19. Nevertheless, it seems that the proposed classification is much easier interpreted at the lower level of control, e.g. at the sharp-end and particularly when automation is present at the system, rather than at the higher organizational level. This issue will be thoroughly discussed in chapter 5.

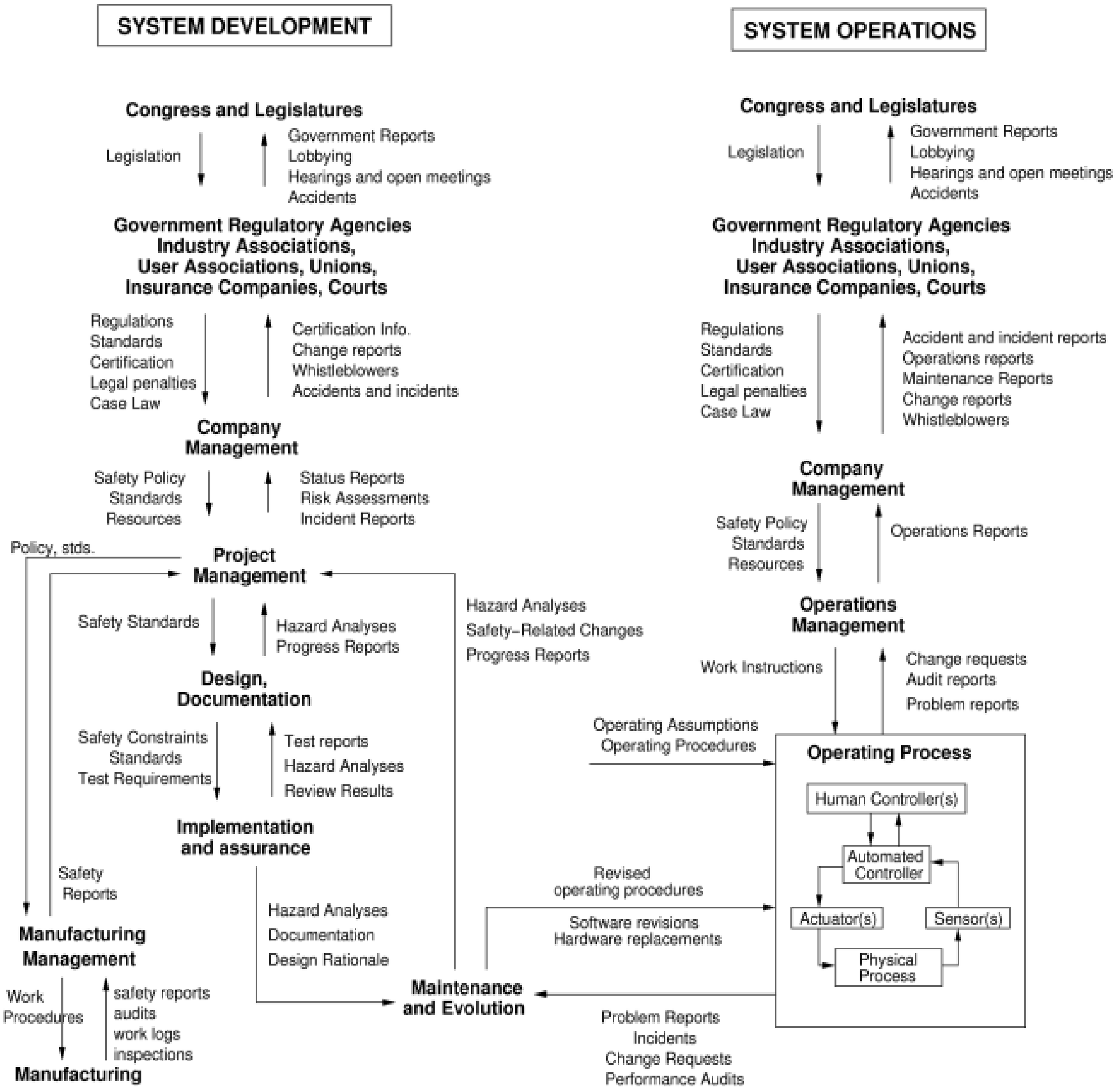


Figure 17: A hierarchical control structure diagram (Leveson 2004)

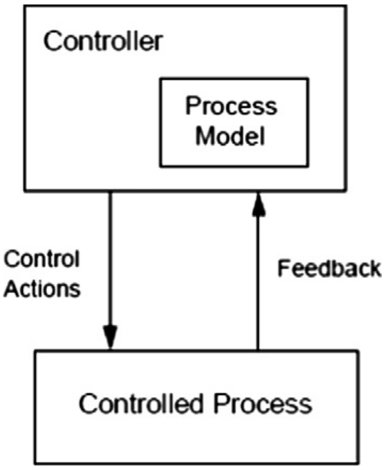
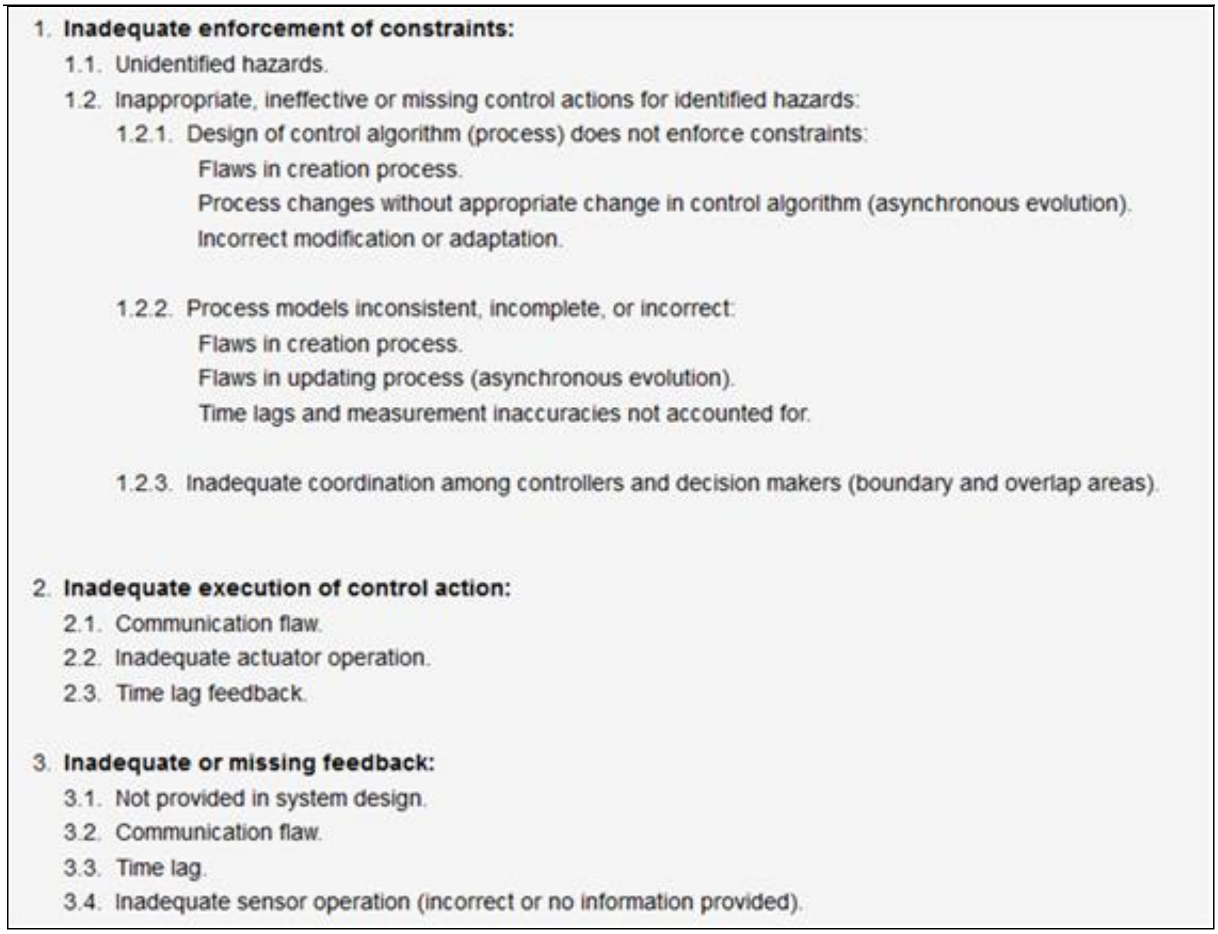


Figure 18: A basic control loop in STAMP



1. **Inadequate enforcement of constraints:**
   1.1. Unidentified hazards.
   1.2. Inappropriate, ineffective or missing control actions for identified hazards:
      1.2.1. Design of control algorithm (process) does not enforce constraints:
         Flaws in creation process.
         Process changes without appropriate change in control algorithm (asynchronous evolution).
         Incorrect modification or adaptation.

      1.2.2. Process models inconsistent, incomplete, or incorrect:
         Flaws in creation process.
         Flaws in updating process (asynchronous evolution).
         Time lags and measurement inaccuracies not accounted for.

      1.2.3. Inadequate coordination among controllers and decision makers (boundary and overlap areas).

2. **Inadequate execution of control action:**
   2.1. Communication flaw.
   2.2. Inadequate actuator operation.
   2.3. Time lag feedback.

3. **Inadequate or missing feedback:**
   3.1. Not provided in system design.
   3.2. Communication flaw.
   3.3. Time lag.
   3.4. Inadequate sensor operation (incorrect or no information provided).

Figure 19: Classification of control flaws (Leveson 2004)

4.2.4.3 ***Other systemic techniques based on organizational models***

In the previous paragraph it has been discussed that modern accident models are shifting their focus from shortfalls in the “sharp-end” of the system to shortfalls in the capacities of the organizations to bring about a safe system. At the same time, other researchers have relied upon organizational models to reveal vulnerabilities and degradation phenomena generating flaws in the control processes of the enforcement of safety constraints. For example, Charles Perrow’s Normal Accident theory (Perrow 1984), explains some major accidents in terms of mismatch between the properties of the technology to be controlled (i.e. its complexity) and the structure of the organization responsible for controlling the technology. From a systems-theoretic perspective, this of organizational cybernetics, several researchers (Dijkstra 2007; Malakis and Kontogiannis 2011; Santos Reyes and Beard 2008) have adapted the functions of the Viable System Model to take into account the particular control needs for safe organizations. Cybernetics is concerned with properties of systems that are independent of their constituting components and its foundations are associated with the notions of communication and control. Another critical concept of cybernetics is that of variety. Asby (1956) defines variety as “*a measure for a number of possible system states that can be differentiated from each other*” and has introduced the law of requisite variety, stating that “*a controller has requisite variety when he has the capacity to maintain the outcomes of a process within targets, if and only if he has the capacity to produce responses to all those disturbances that influence the process*”.

The Viable System Model (VSM) is a well-known cybernetics model (Beer 1984) that is helpful in designing and diagnosing the communication and control of viable organizations. Viability refers to the survival or preservation of an organization’s identity in a changing environment, and Beer (1985) argued that any organization that maintains its existence is viable otherwise it would not exist. It must be mentioned that the VSM describes how a nested group of autonomous units should interact in order to balance the variety of the environment and the variety of the organization. Each autonomous unit can also be perceived as a viable sub-system in its own right (figure 20). Particularly, system 1 is the basic unit that comprises both a management and an operational element and interacts with the local environment. Systems 2–5 facilitate the work of the basic units (system 1) and ensure continuous adaptation of the organization as a whole. The five units of VSM can be related to the following safety-related functions as presented in table 1: formulation of the safety-policy, safety-development, safety-functional, safety-co-ordination, and safety-policy implementation.

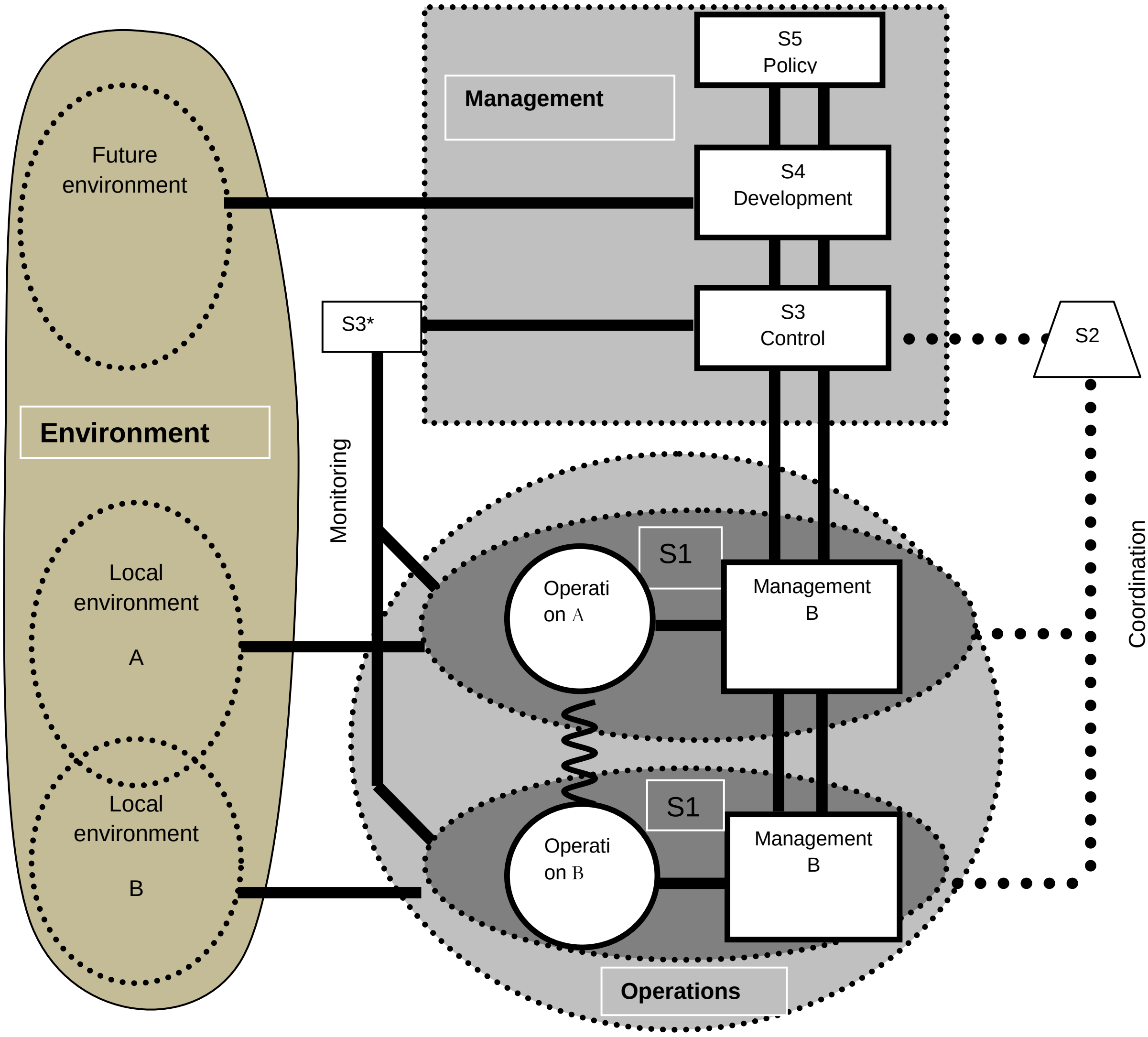


Figure 20: The VSM activities

System 1: Safety Policy Implementation	System 1 refers to the operational units of an organization and therefore, it is where the interactions with the environment and the risks are created. From a safety perspective, ***system 1 implements the safety policy and safety plans***. It consists of a management and an operational unit as well as its local environment. In a way, system 1 is a viable system on its own that exists within the other four VSM systems
System 2: Safety Co-ordination	The function of system 2 *is* ***to co-ordinate operations*** and implement, along with system 1, the safety plans received from system 3. Since there are many units within the total environment that may create conflicting situations, system 2 is responsible to control such interactions.
System 3: Safety Functional	System 3 is responsible for maintaining safety within an acceptable range and for ensuring that system 1 implements the organization's safety policy. For this reason, ***system 3 is employed to provide feedback by conducting audits sporadically into the operations of system 1***. System 3 receives strategic and normative safety plans and standards from system 4 and system 5 while it collects information about safety performance from system 1 and system 2 in order to close the feedback loop between planning and monitoring of safety. Then, ***system 3 forms more specific safety plans and allocates resources to system 1*** to accomplish these plans.
System 4: Safety Development and Adaptation	System 4 plays an intelligent function as it scans the environment for threats and opportunities while looking inside for internal strengths and weakness for the continual ***adaptation and anticipation*** of the whole system. Thus, ***system 4 provides a modelling of the organization's safety performance***. The model should contain the relationships among the system variables (i.e. relationships among those that can influence the safety performance), the current state of the system (i.e. the knowledge about the current level of the safety performance) and the ways the system can change (i.e. the adaptation of the organization).
System 5: Safety Policy	System 5 is responsible for formulating the ***safety policy*** and for making normative decisions (i.e. ***goal setting and assignment of control authority***). The safety policy must reflect the safety goals and beliefs of the whole organization, address the anticipation of accidents and promote the safety culture throughout the organization. System 5 should also achieve a balance between exploitation of existing safety rules and exploration of new safety concepts.

Table 1: The VSM's organizational functions

The VSM is proposed as a sufficient structure for an effective safety management system mainly because of the recursive structure of organizations (Kontogiannis and Malakis 2011). The concept of recursion is intended to clarify whether a safety management system refers to an entire organization, several parts of it, or just part of it. Recursion implies some sort of autonomy and "self-regulation" at each level of the system in the sense that the same five functions apply to each individual unit to ensure viability on its own. For example, system 1 can be seen as a group of sub-units that have relative autonomy in carrying out their tasks but at the same time all sub-units should comply with the requirements of the safety management system as a whole. Therefore, VSM brings into the fore the balance that must exist between ***decentralization*** (i.e. autonomy) and ***centralization.*** This is a delicate balance as sub-units must not become isolated but, equally important, must not drift away from the overall safety policy.

Another important issue highlighted by VSM regards the interactions between ***planning and monitoring***. Although VSM recognizes adequate resources and appropriate auditing mechanisms essential for effective planning and monitoring, it also highlights that monitoring and planning are coupled to form a closed control loop which if passes unnoticed may lead to several problems. Hoverstadt (2008) discusses the problem of “reverse polarity” where measures of performance are used not to monitor a process but instead to drive the planning of the process. Finally, a key concept advocated by the VSM is how organizations adapt to the complexity of both their environment and their own activities. Adaptation can be seen as the process of amplifying variety of the organization’s own capabilities or attenuating the variety or complexity of the environment. System 4 and system 5 play important functions so that new concepts of safety are explored whilst they also address the process of organizational learning. Thus, VSM emphasize the importance of maintaining a balance between ***exploration and exploitation***.

A detail description of VSM model in relation to designing and assessing safety management systems can be found in Reyes and Beard (2002; 2008). The authors adopt principles and concepts of VSM to construct a fire safety management system in the oil and gas industry. Furthermore, the application of VSM in accident analysis is extensively discussed in Kontogiannis and Malakis (2011) and Reyes and Beard (2009). It is noteworthy to mention that both STAMP and VSM have a systems-theoretic perspective, therefore, a cross-fertilization seems to be an interesting endeavor. Such an endeavor is thoroughly discussed in the next chapter.

5 Extending the STAMP model at the organizational level

In the previous chapter it has been discussed that a fundamental idea that emerges from system safety literature is that safety is a "control problem" that requires a "systems-theoretic" approach (Saleh et al. 2010). Following this line of though, systemic accident analysis models -such as STAMP- have been proposed to help analysts to probe into the complicated interactions among system components that may lead to accidents, whereas organizational models -such as the VSM- have been used with the aim to search deeper for organizational vulnerabilities and degradation phenomena that might lead to loss events. It must be mentioned that these two trends of application of systems thinking in safety have taken place in parallel and only recently a cross-fertilization has been attempted for post-accident investigations (Kontogiannis and Malakis 2011). In particular, Kontogiannis and Malakis (2011) attempted to elaborate the STAMP model on the basis of VSM and revealed many patterns of organizational breakdowns in a Helicopter Emergency Service. The results of that study concluded that the VSM provided a good basis for understanding the organizational patterns of breakdown behind the control flaws investigated with STAMP. The good match between STAMP and VSM in accident analysis has provided additional research impetus for using a similar joint framework for proactive safety assessments that may help the safety analysts to search deeper for system vulnerabilities at the organizational level (see figure 21 in relation to figure 17).

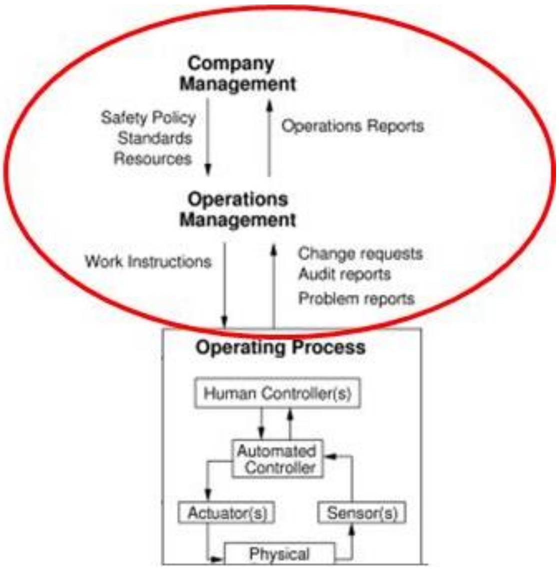


Figure 21: Extending the STAMP dynamics at the organizational level

5.1 The organizational “control requirements”

By using the STAMP model the main aim of safety assessment is to identify control flaws that may lead to violations of safety constraints (i.e. causal factors that may lead to the inadequate control/enforcement of safety constraints). In general, effective control of a system requires meeting the following conditions (Asby 1956):

1. The controller must have a goal (e.g. to maintain the set point).
2. The controller must be able to affect the state of the system.
3. The controller must contain a model of the system and be able to ascertain its state.

If these general requirements are not sufficiently fulfilled, then inadequate control or enforcement of constraints may occur. Therefore, the challenge in extending STAMP is to map these general requirements at the organizational level. Because VSM provides a good description of how organizations can control their operations to support their viability, an initial mapping between the STAMP’s general control requirements and the VSM is presented in figure 22.

This initial mapping is based on the concepts of the VSM that were discussed and presented in table 1 and in section 4.2.4.3. In short, organizations must have: (1) a policy and a prioritization scheme for the controlled processes, (2) the ability to affect the state of the processes, and (3) a good model of the processes under control. In particular, safety goals (system 5 of VSM - the goal condition for the requirements) are transformed into specific plans for action (i.e. system 3 - the ability to affect the system) and are assigned to suitable personnel (i.e. system 5 - the ability to affect the system). The design and implementation of safety plans (i.e. system 1 and system 3) are not the only prerequisite to affect the system since coordination (i.e. system 2) and resources (i.e. system 3) are also essential. To assess the adequacy of the safety goals and plans and to update them -when necessary- a feedback loop is established at the management level either by safety audits (system 3) or by other means provided by the intelligence function of the system (i.e. system 4).

For a more refined mapping, it may be assumed that resources and co-ordination are fundamental in designing and carrying out safety plans whereas audits and anticipation constitute the basis of modelling safety performance. Therefore, it is concluded that the organizational control “requirements” are related to the following:

- formulation of safety policy and goal setting
- assignment of control authority and responsibilities

- design and implementation of safety plans
- modelling of organization's safety performance
- adaptation to continually meet safety requirements

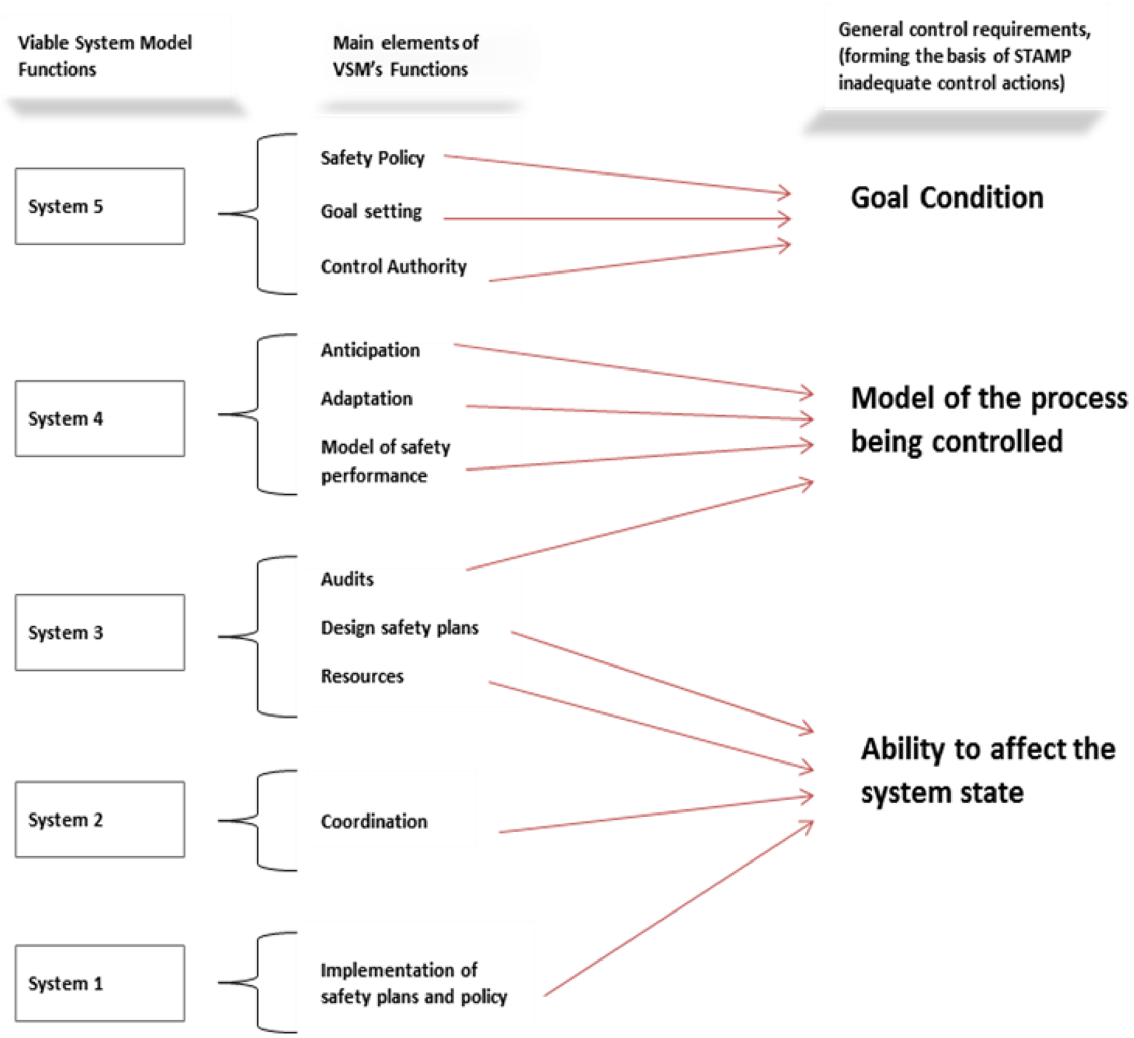

Viable System Model Functions
Main elements of VSM's Functions
General control requirements, (forming the basis of STAMP inadequate control actions)
System 5
Safety Policy
Goal setting
Control Authority
Goal Condition
System 4
Anticipation
Adaptation
Model of safety performance
Model of the process being controlled
System 3
Audits
Design safety plans
Resources
System 2
Coordination
Ability to affect the system state
System 1
Implementation of safety plans and policy

Figure 22: Mapping the VSM functions with STAMP's general control requirements

It must be emphasized that knowing the organizational safety control requirements is essential since it is their violation that might lead to the inadequate enforcement of constraints (i.e. inadequate safety policy, goals, assignment of control authority, design and implementation of safety plans, modelling of safety performance and adaptation to changes). However, a safety assessment should search deeper in order to understand *why* the inadequate enforcement of safety constraints may occur (i.e. to identify the control flaws).

5.2 Violation of the organizational requirements-organizational control flaws

According to STAMP, problems in safety arise mainly due to inadequate control actions that stem from control flaws. Leveson (2004) provides a classification of control flaws (refer to figure 19), in order to identify why the inadequate control may occur and she further mentions that "*this classification applies at each level of the socio-technical control structure even if their interpretation at each level may differ"*. However, the classification of control flaws proposed by Leveson, based on its control theory and system dynamics origin, is more easily understood at the lower level of control (e.g. at the sharp-end and specifically where automation is present at the system), rather than at the higher organizational level, rendering thus STAMP more suitable for identifying technical control flaws as opposed to organizational ones (Kontogiannis and Malakis; Salmon et al. 2012).

For this reason, it is believed that an extension of the control flaws of STAMP at the organizational level is essential to guide a rigorous and sophisticated safety assessment process. In order to achieve this goal and refine the general classification of control flaws proposed by Leveson with their organizational analogs, concepts from the VSM are mainly adopted. Furthermore, literature of safety science has been also used to enhance the proposed framework. For instance, a pillar for the proposed framework is how organizations manage uncertainty and variability. At this point, two paradigms can be distinguished (Grote 2008; 2012):

1. Uncertainty may be minimized by central planning, automation of work processes and high levels of specialization with few degrees of freedom for human controllers.
2. Uncertainty may be managed by empowering all actors in the organization to cope with uncertainty locally, by having options for actions rather than fixed plans and standards.

Grote (2012) notes that: "*In general terms these two paradigms aim to either maximize stability or flexibility. As the levels of uncertainty that companies are confronted with can change over time and also internal demands for different parts of companies may vary, recent research has addressed the need to balance stability and flexibility rather than opt for one or another*". Taking into account that many accidents have occurred due to this imbalance (Kontogiannis 2010), the issue of managing uncertainty and variability underlies many of the identified organizational control flaws which are presented below. It is noteworthy to mention that throughout the next section the term "safety plans and procedures" is referred to any plan or procedure that impact safety, directly or indirectly. Some plans and procedures are almost exclusively directed at safety (e.g. emergency response plans) while others have other primary objectives related to quality, sustainability, as well as safety (e.g. maintenance plans).

5.2.1 Inadequate formulation of safety policy and goals

*5.2.1.1 **Ambiguous safety policy or lack of safety policy***

Organizations should provide a written statement of their safety policy. This policy must be more than sloganeering and should explicitly define the relationships of safety to other organizational goals so as to provide the scope for discretion and judgment in case safety conflicts with productivity. Leveson (2012) mentions that many companies often justify the lack of safety policy explaining that "*everyone knows that safety is important in our business*". However, while safety may seem essential for a particular business, the "silence" of management on policy may give the impression that tradeoffs are acceptable when safety conflicts with other goals. Undeniably, an ambiguous or lack of safety policy can lead to an inadequate formulation of safety policy and goal setting.

*5.2.1.2 **Imbalance between exploitation and exploration***

One of the main principles of viable organizations is their ability to balance exploitation with exploration (Beer 1985). Exploitation is based on existing rules and practices whereas exploration has to do with "exploring" new rules and policies (i.e. an important function of system 5). Indisputably, an important element of safety policy and goal setting concerns the external oversight and regulation. Companies, especially those operating in high risk domains, are subject to external regulation that influences their safety policy. However, if policies are based solely on regulative standards (i.e. exploitation) organizations might find themselves a step behind their actual safety-related needs. Regulatory processes typically require 6-10 years to develop adequate prescriptions and during this time the existing practices and safety goals might have been rendered inadequate (Rasmussen 1997).

*5.2.1.3 **Trapped in the often unnoticed loop between formulating goals and monitoring***

The VSM highlights that goal setting and monitoring are coupled to form a closed control loop. This organizational feedback loop should always include information about safety performance. This information is vital since it is then fed back to alter planning and inform decisions (i.e. whether to do something more or less different). A common problem that might occur in this feedback loop is that of “reverse polarity” (Hoverstads 2008) that happens when the feedback is run in reverse so that the performance measures are used not to inform about a process but instead to do the opposite, to drive the process. In this sense, monitoring can end up driving the safety policy and the goal setting. Taking into account that “quick fixes” are more easily monitored than “systemic safety programs” (Kontogiannis 2012; Marais et al. 2006), the organization’s goals may focus on “fire-fighting”, while fundamental solutions are needed. Unfortunately, systemic safety programs often do not show immediate results to monitor (due to lagging effects), hence, under the adage “what get measured gets managed” the unnoticed loop between goals and monitoring may result in inadequate formulation of safety goals.

*5.2.1.4 **Eroding safety goals***

Safety goals may erode over time, particularly ahead of accidents. This movement of organizations towards higher risk areas was first identified by Rasmussen (1997) who advocated this “drift into failure”. Often, safety goals erode over time due to complacency, thus one possible way to avoid drift is to continuously monitoring risk (Marais et al. 2006). In general, it can be said that effective modelling of safety performance is essential to avoid subversion of safety goals. Vaughan (1996) proposes the term “normalization of deviance” to refer to situations where organizations repeatedly accept a lower standard of performance until the lower standard becomes the norm. Such “normalization” should be identified by the organizational feedback loops, however, this issue is extensively discussed later.

5.2.2 Inadequate assignment of control authority and responsibilities

*5.2.2.1 **Imbalance between autonomy versus centralized control***

One of the main principles of organizational viability refers to the balance that an organization must achieve between centralized and decentralized control. This principle is also reflected in other major concepts of VSM such as recursion and autonomy. Centralization is the degree to which formal decision-making is concentrated in high-level individuals, allowing lower level employees only minimal discretion in making decisions. In contrast, decentralized organizations allow lower level employees to make some decisions that affect the entire organization directly. From a safety viewpoint, the dilemma between centralization and decentralization is contentious, as indicated in the discussion on High Reliability Organizations (Roberts 1990). In general, Perrow (1984) argued that if organizations have to live with high interactive complexity they should build a decentralized structure whereas if they have to cope with tight coupling they should be centralized. As a rule of thumb, it can be suggested that decentralized control is appropriate when flexibility is required (i.e. for handling high levels of uncertainty caused by frequent changes of variances and disturbances) whereas centralization should be selected when stability is the purpose (i.e. due to tightly coupled processes, need for traceability of decisions, low fault tolerance or low qualification of personnel (Grote 2012)). As it has been mentioned, different parts of an organization may be to a greater or lesser extent representative of the aforementioned characteristics, thus the decision for centralization or decentralization must be examined throughout an organization, as it is implied in the recursion concept. All in all, an imbalance between autonomy and centralized control (i.e. choosing autonomy when stability is the purpose or choosing centralized control when flexibility is needed) may lead to inadequate assignment of control authority.

5.2.2.2 ***Gaps and overlaps in responsibilities***

As far as the assignment of responsibilities is concerned, there are two opposite tendencies. The first is to make everyone responsible for safety; the other is to assign safety to a separate group that is isolated from critical decision making. These two trends can be summarized as: (1) overlaps of responsibility, and (2) gaps in responsibility. Overlaps of responsibility exist when multiple controllers are responsible for the same process. Leplat (1987) suggests that accidents are most likely to occur in such overlapping areas of responsibility. It is notable that in many organizations overlap of safety-related responsibilities has been done with the intention of creating operational redundancy. However, the assumption that a human controller can step in and adequately control a process in the event that the primary controller fails is often an illusion. Usually, the reasons that rendered the primary controller to fail will also lead to the failure of the redundant one (Leveson 2012). On the other hand, gaps in responsibility occur when no controller is responsible for the enforcement of a particular safety constraint. Gaps usually occur when there is a confusion surrounding who is responsible for the enforcement task. Therefore, inadequate assignment of responsibilities may stem from such gaps and overlaps in the control boundaries.

5.2.2.3 ***Responsibility assigned is not suited to personnel***

Again, the organization’s approach to managing uncertainty should be thoroughly considered when responsibilities are assigned to personnel. Minimizing uncertainty (i.e. opting for stability) requires less qualified level of personnel whereas coping with uncertainty (i.e. opting for flexibility) requires more qualified people (Grote 2012). In addition, the requirements for each responsibility should be well-defined otherwise it is very difficult to ensure that the appropriate personnel undertake the necessary responsibilities. Finally, humans are from their nature inappropriate to engage specific tasks. For example, Bainbridge (1987) stated that in highly automated systems humans are usually assigned with the responsibility of checking the automation. However, this is an erroneous assignment since it is well known that even the best motivated people may have trouble maintaining vigilance for long periods of time. These aspects should be examined when assessing the assignment of responsibilities in an organization.

5.2.3 Inadequate design and ineffective implementation of safety plans

5.2.3.1 ***Mismatch between the safety plans and the strategy of managing uncertainty***

In order to design safety plans in ways that support the strategy of managing uncertainty, the nature of plans needs to be examined (Grote 2012). For this purpose, it is useful to repeat the distinction suggested by Hale and Swuste (1998).

- P*erformance goals* define only what has to be achieved and not how it must be done.
- *Process rules* define the process by which the organization should achieve certain goals but still leaves considerable freedom about the choice of the actions.
- A*ction rules* prescribe detailed courses of action, possible without even mentioning the goal to be achieved.

Grote (2012) points out that, roughly, action rules should be used when stability is required, whereas performance and process rules should be used when flexibility is the goal. Procedures may always be essential, because tasks may be too complex for people to remember the steps. However, when flexibility is required procedures are regarded as supports rather than as controls to limit freedom. This difference may be symbolized by re-labeling them “guidelines” instead of strict procedures. It is also notable that action rules cannot provide flexibility since the range of non-nominal conditions that can occur is so great that even thick volumes of procedures may be ineffective to cover them (Hale and Borys 2012a). Therefore, it becomes essential for people at the “sharp end” to use their competence and tacit knowledge to cope with unexpected and unforeseen situations (Hollnagel et al. 2006). All in all, a mismatch between safety plans and the strategy of managing uncertainty may lead to inadequate design and implementation of safety plans.

5.2.3.2 ***Lack of co-ordination***

The VSM regards co-ordination inside an organization essential in order to avoid unexpected side effects and conflicting actions. The importance of co-ordination, when designing safety plans and procedures, is also highlighted if one considers the constructivist view of how plans emerge and adapt throughout an organization's operation (Nathanael and Marmaras 2008). Furthermore, well-designed safety plans can still be ineffectively executed if poor communication channels exist. Communication channels can be created through several avenues, such as procedures that establish the documentation of safety plans, meetings, emails, etc. If such channels fail, then the implementation of safety plans is at stake. In addition, the timeliness of messages transmitted can also lead to inadequate execution of plans.

5.2.3.3 ***Inconsistency between plans and routines in practice***

It is usual for safety plans to be covered in formal procedures in order to specify the behavioural patterns that are required in predefined conditions. On the other hand, the actual patterns emerging and repeated with a high degree of regularity are often called "routines". Becker (2005) regards routines as emerging from experience and repetition in a social context in a way that is essentially informal and not written down. This difference in the written form of plans from the acted routines has much in common with how Argyris and Schon (1978) distinguish "espoused theory" from "theory in use". Several problems may arise when the artifact containing the written formal description of a behavioural pattern is not aligned with routines (Grote 2012). Such inconsistency may conceal outdated plans, conflicting goals (especially in relation to productivity), workload, non-compliance, poor supervision and normalization of deviance (see eroding safety goals above). Notwithstanding, all the above aspects may lead to the inadequate implementation of safety plans.

5.2.3.4 ***Plans not following changes in the system, stagnant plans***

When plans and procedures do not follow changes in the system under control (e.g. technological changes, operational changes, management changes, etc.) then safety may be compromised. Leplat (1987) notes that accidents are often caused due to an *asynchronous evolution* where changes in one part of the system (e.g. technical or organizational) are not followed by necessary changes in other related parts. In the process industries, a common problem with operating procedures is that these are not updated properly when equipment is modified. The causes of such inadequate adaptation are discussed below, in “the inadequate modelling of safety performance” control flaw.

*5.2.3.5 **Lack of resources***

The VSM pays close attention to the adequate allocation of resources necessary for the viability of organizations. When resources are insufficient (i.e. personnel, time, equipment, money), people involved in safety plans (either at the design or the implementation stage) will use their allotted resources to the best of their ability, but safety will be compromised and the risk of an accident will increase (Leveson 2012).

*5.2.3.6 **Inefficient training procedures***

Training is essential to build up the skills needed for effective implementation of safety plans, especially in emergency situations (Grote 2012). If the people involved in the implementation of safety plans are not given sufficient training then the implementation of safety plans might prove ineffective. Moreover, training should be elaborated accordingly to departments of organization or job position. For example, when safety plans are based on action rules, training should focus on drills which ensure the correct execution of predefined actions. On the other hand, when safety plans are based on performance goals and process rules then the training should aim at supporting decision making and problem solving (Grote 2012). Finally, in all cases a follow up of training should always be provided in parallel with an evaluation of the efficacy of training previously given.

5.2.4 Inadequate modelling of safety performance

The VSM highlights that management is a dynamic process of adaptation of policy, goals and plans to the changing realities of a system’s activity and environment. Therefore, in order to formulate policy, goals and plans either for the first time or when updating existing ones, the organization must have a model of the process, i.e. a modelling of the state of the safety performance. If the system is under development, risk analysis may be utilized to define safety constraints that must be enforced and to design the relevant plans for the enforcement of constraints. On the other hand, if the system is under operation, there is a need to continually monitor the gap between policy, goals and plans with reality and adapt when it is necessary. Inadequate modelling of the state of the safety performance may occur due to:

5.2.4.1 Inadequate feedback control

Monitoring is regarded as a key concept in VSM and feedback loops exist among all subsystems (i.e. system 1 to system 5) to ensure rational decision making. Leveson (2012) also argues that feedback is essential in order to provide a model of the current state of a system. Hence, an organization must have a model of its safety performance, a model that will provide the necessary information concerning whether its safety plans have been effective in achieving the safety goals. This organizational feedback is mainly based on: audits, reporting systems, and incident analysis. Therefore, the majority of possible organizational flaws might occur in the following feedback channels.

- **Inadequate safety audits**: The VSM regards safety audits (system 3) as a crucial procedure for the viability of organizations. The main goal of safety audits should be to determine whether the safety measures and safeguards of an organization are enforced and whether the assumptions underlying the initial design of both technical and social elements are still true. Therefore, safety audits should rely on information provided by risk analysis and hazard logs. There is also a need for an organizational memory to preserve information about the reasons why safety plans are formulated as they do. If such information is not available, the safety audit might not effectively depict the current state of an organization’s safety performance or may not identify hazardous adaptations. Since audits are performed with the aim to evaluate the safety performance and update the “process model” of organizations, it is crucial that all levels in an organization are audited, not only the sharp-end practitioners. Finally, an important requirement for audits is a follow-up to ensure that recommendations provided have been implemented or that the implementation was effective (Leveson 2012).
- **Inadequate learning from events**: Many companies have an incident investigation process that identifies only proximal failures that led to an event, not the more systemic ones. This common pitfall to look and fix only the proximal causes may lead to an inadequate understanding of the safety performance. Moreover, the people who perform a “learning from events process” should be appropriately educated and provided with the necessary tools (e.g. a structured incident analysis technique).
- **Improperly designed reporting schemes:** The VSM acknowledges that reporting schemes are crucial for the viability of organizations. Hence, a key for achieving an adequate model of current safety performance is to have an easy-to-use reporting system. A usual flaw that can affect the usage of reporting schemes is the managerial decision to reward the personnel when the number of incidents is

reducing. Such a strategy might lead to withholding information about incidents and near misses, creating the illusion that the organization is becoming safer when in reality it has merely been “muted” (Turner and Pidgeon 1997). Moreover, personnel may be reluctant to report if the information that they provided in the past appeared to go in the black hole, without anybody responding to it (Leveson 2012). Reports of mistakes or incidents should not be seen as failures but as an opportunity to focus attention and to learn (Dekker 2011).

5.2.4.2 ***Inadequate feed-forward control***

From a classic engineering control perspective, a system can be controlled either by using feedback or feed-forward information. In the previous paragraph, the feedback mechanisms that might affect an organization’s ability to model its safety performance were discussed. However, Hollnagel et al. (2006) argue that more emphasis should be put into controlling a system by responding to anticipated disturbances (i.e. feed-forward) instead of relying on actual outcomes (i.e. feedback). Beer’s Viable System Model also emphasizes the anticipation of changes (i.e. system 4). Organizational control flaws that might result in inadequate feed-forward control are:

- **A management of change procedures and risk analysis is not provided in the organization:** Organizations require safeguards for planned and unplanned changes. Before strategic organizational changes are made, the impact of such type of changes on safety must be evaluated. Many industries do have such safeguards, usually called “management of change procedures” based on risk analysis. If procedures to anticipate and evaluate changes do not exist, an organization might have serious difficulties in adapting to the inevitable changes that will occur in its structure and environment.
- **Lack of leading safety performance indicators and other early warnings:** Various safety indicators can play a key role in providing information for use in anticipating and developing organizational performance. Moreover, they should monitor the safety boundaries and recognize how close an organization is to the edge of its safety envelope. These indicators are called leading indicators (Hopkins 2009). If such indicators do not exist, then organizations will only have metrics about what has happened in the past, or even what is happening in the present, but they would not have a model about what may happen in the future.

5.2.5 Inadequate adaptation to changes

As it has been discussed, it is essential that organizations are provided with a model about their safety performance. In this model, feedback and feed-forward mechanisms are key parts in providing the necessary information of what has happened, what is happening and what may happen so as to adapt their policy, goals and plans accordingly. Several changes in the controlled system may occur (e.g. physical changes, human changes, organizational changes) and according to VSM it is useless to monitor such changes (i.e. with feedback or with feed-forward control) if the organization does not adapt to this information. Problems in adaptation may occur due to:

5.2.5.1 ***Open loops***

A common flaw that might lead to inadequate adaptation is the failure to close feedback and feed-forward loops. For example, information is collected but there is no way to use this information to affect the process. It is very common to collect "feedback" (i.e. from audits, reports, safety drills and risk analysis), but there is no actually feedback unless there is a mechanism that allows adaptation to this information (Hoverstand 2008). As Kontogiannis (2012) states a common problem in modern organizations is that a large amount of data is generated often overwhelming practitioners and supervisors.

5.2.5.2 ***Lack of double loop learning***

Turner and Pidgeon (1997) emphasize the need for the so called double loop learning (Argyris 1978). This concept stresses that in order to have an adequate model of safety performance it is not enough that organizations have feedback and feed-forward mechanisms. There is also a need to improve the procedures for gathering and assessing the signals provided by feedback (i.e. an updating process for the feedback itself). Lack of double loop learning may lead sooner or later to inadequate adaptation.

5.3 Summary of the organizational control flaws

In this chapter, concepts from VSM have been used in conjunction with principles from control theory and other notions found in the organizational safety literature in order to conclude to the safety requirements of organizations (i.e. what an organization needs in order to effectively control its safety). Then, a classification of organizational control flaws (that may lead to inadequate control/ enforcement of safety constraints) has been proposed. The classification of the organizational control flaws developed in this section is summarized in table 2. It must be mentioned that the classification provided does not aspire to be absolute. It is rather an attempt to provide a scheme that it can be further improved and enhanced. Moreover, it is mentioned that violation of the presented control flaws will not deterministically lead to loss events. If organizations deviate from this proposal then a problem may occur or not, however the potential for accidents should be examined. It is also notable that the issue of safety culture has not been discussed herein. Although many aspects of managing a safety culture are reflected in the proposed classification the reader interested in the issue of diagnosing a safety culture in safety management audits is referred to Grote (2008).

1) Inadequate formulation of safety policy and goals
a) Ambiguous safety policy or lack of safety policy b) Imbalance between exploitation and exploration c) Trapped in the often unnoticed loop between formulating goals and monitoring d) Eroding safety goals
2) Inadequate assignment of control authority and responsibilities
a) Imbalance between autonomy versus centralized control b) Gaps and overlaps of responsibilities c) Responsibility assigned is not suited to personnel
3) Inadequate design and ineffective implementation of safety plans
a) Mismatch between the safety plans and the strategy of managing uncertainty b) Lack of coordination c) Inconsistency between plans and routines in practice d) Plans not following changes in the system, stagnant plans e) Lack of resources f) Ineffective training procedures
4) Inadequate modelling of the state of the safety performance
a) Inadequate feedback control Inadequate safety audits Inadequate learning from events process Improperly designed reporting schemes b) Inadequate feed-forward control Lack of management of changes, inadequate risk analysis Lack of leading safety indicators
5) Inadequate adaptation to changes
a) Open loops b) Lack of double loop learning

Table 2: Organizational control flaws

6 Introducing a systems-theoretic method for road tunnel safety assessment

6.1 The outline of the method

The systems-theoretic road tunnel safety assessment method which is introduced in this chapter follows the typical steps of a STAMP-based safety assessment (figure 23; for more details the reader is referred to Leveson 2012). However, the method introduced herein is enhanced by the joint STAMP-VSM framework which has been developed in chapter 5. The ultimate goal of the method is to provide a set of causal factors that even if they have not been identified by current risk-based approaches, they have the potential to affect the overall safety. More specifically, the method considers: organizational and human aspects, software behaviour, the relationships between the parts of the system and its adaptation over time. In short, the goal is to identify causal factors that encompass the entire accident process, not just failures of electro-mechanical components of the infrastructure.

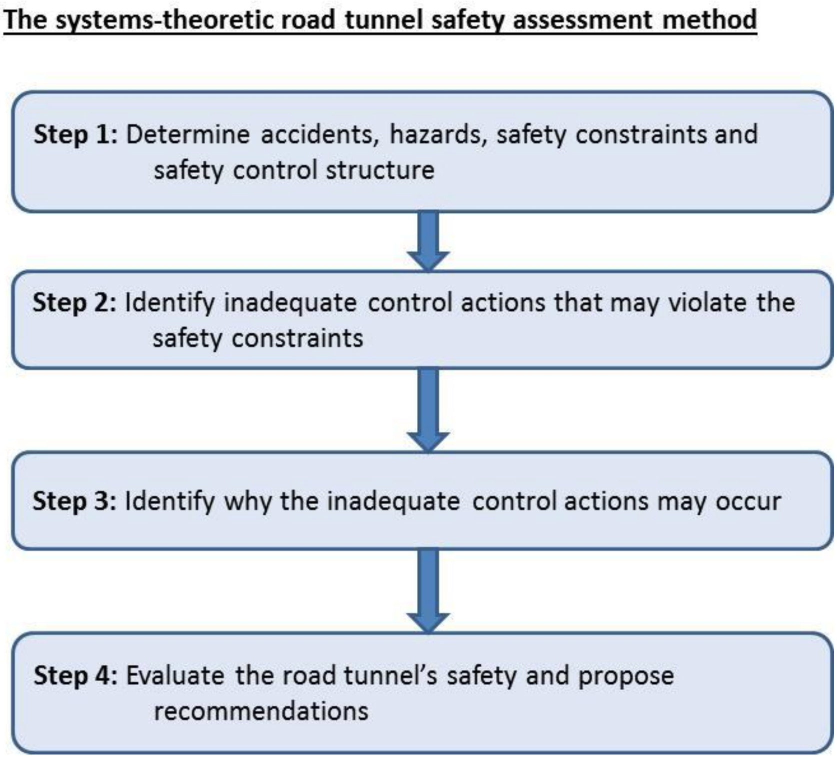

The systems-theoretic road tunnel safety assessment method
Step 1: Determine accidents, hazards, safety constraints and safety control structure
Step 2: Identify inadequate control actions that may violate the safety constraints
Step 3: Identify why the inadequate control actions may occur
Step 4: Evaluate the road tunnel's safety and propose recommendations

Figure 23: The steps of the systems-theoretic road tunnel safety assessment method

The first step of the method involves agreeing on the types of accident and hazards to be considered. Since definitions of such terms differ among industries, the term *accident* is defined herein as: *an unexpected event*[10] *that results in a loss, including loss of human life, property damage and environmental pollution* (Leveson 2012). In this sense, an accident occurs if there is an unexpected event *and* an unwanted outcome, i.e. both conditions must exist at the same time (Hollnagel 2004). In this thesis, the accident that will be considered **is the unexpected event of a *fire in a tunnel*** resulting **in loss of human lives and/or serious injuries**. However, other events (e.g. explosions, collisions, release of toxic gases, floods) and other unwanted outcomes (e.g. serious damage to the infrastructure, environmental pollution) may also be considered when applying the method in practice.

The first step of the method proceeds with identifying the hazards that are associated with the examined accident. Again, it is noted that the term hazard has been used in different ways among industries, nevertheless, herein it is defined as: "*a system state or a set of conditions that together with a set of worst-case environmental conditions, will lead to an accident"* (Leveson 2012). The definition is significant broad, and for practical reasons it precludes states of the system needed to accomplish the tunnel's system goal, which is to transport humans and goods. As such, the transportation of DGs via the tunnel is not considered to be a hazard. It is also notable that "*there is no right or wrong set of hazards, only a set that the system stakeholders agree that they should avoid*" (Leveson 2012). Following this line of though, the hazards ($H_{i,}$) that are associated with the examined accident are the following:

- H_1: Inadequacy of the tunnel's systems and organizational procedures to control traffic disruption during a fire incident.
- H_2: Inadequacy of the tunnel's safety systems and organizational procedures to control smoke and fire.
- H_3: Inability of road tunnel users to evacuate before the onset of untenable conditions.

After the hazards have been defined, it is important to conclude to the system-level safety constraints (i.e. the safe behaviours) that should be enforced in order to avoid the accident. Taking into account that hazards are indeed states and conditions which have the potential to lead to the accident, the system-level safety constraints (SC_j) can be determined by

[10] Event is defined as an isolated incident or a number of interrelated circumstances resulting in release of energy (Cristensen et al. 2003).

flipping them. Hence, the system-level safety constraints that should be enforced in order to avoid the examined accident are:

- SC_1: A safe and steady flow of traffic in the tunnel by responding to the traffic disruption in case of a fire incident.
- SC_2: The tunnel's safety systems and organizational procedures should control fire and smoke effectively.
- SC_3: Tunnel users should evacuate the tunnel before the onset of untenable conditions.

If the accident occurs, it is because one of the system-level safety constraints -or even all- has been violated. Rather than focusing on specific events that may reflect the effects of inadequate enforcement of the safety constraints (e.g. "ventilation system's failure", "delayed evacuation", etc.), the aim of the proposed systems-theoretic method is to identify *how* and *why* the aforementioned constraints may be inadequately enforced. In this perspective, the road tunnel safety is viewed as a control problem and is managed by a control structure which has the responsibility to enforce the safety constraints on the tunnel system's operation. In order to determine the actors that should be included in the safety control structure Leveson (2012) has proposed specific criteria. In a road tunnel complying with the EU Directive 2004/54, the main actors/entities responsible for enforcing the system-level safety constraints (SC_1-SC_3) are those depicted in figure 22. Namely:

- The *Tunnel Manager* who is responsible for the management of the tunnel (i.e. determining the safety goals and assigning responsibilities).
- The *Safety Officer* who: (1) ensures coordination with emergency services and takes part in the preparation of safety plans, (2) verifies that personnel and emergency services are well trained, (3) verifies that the tunnel structure and equipment are well maintained, and (4) takes part in the evaluation of all incidents.
- The *Designers* that affect safety by their design options.
- The *Maintenance personnel* intervening on the technical facilities of the tunnel in a preventive or corrective way so as to guarantee safety.
- The Emergency services/tunnel response team (e.g. police, fire brigade, rescue teams and road patrollers) who intervene in case of an accident.
- The *Tunnel Operator* and the *SCADA* system that control the operation of the tunnel.
- The Road *Tunnel Users* who drive through the infrastructure.

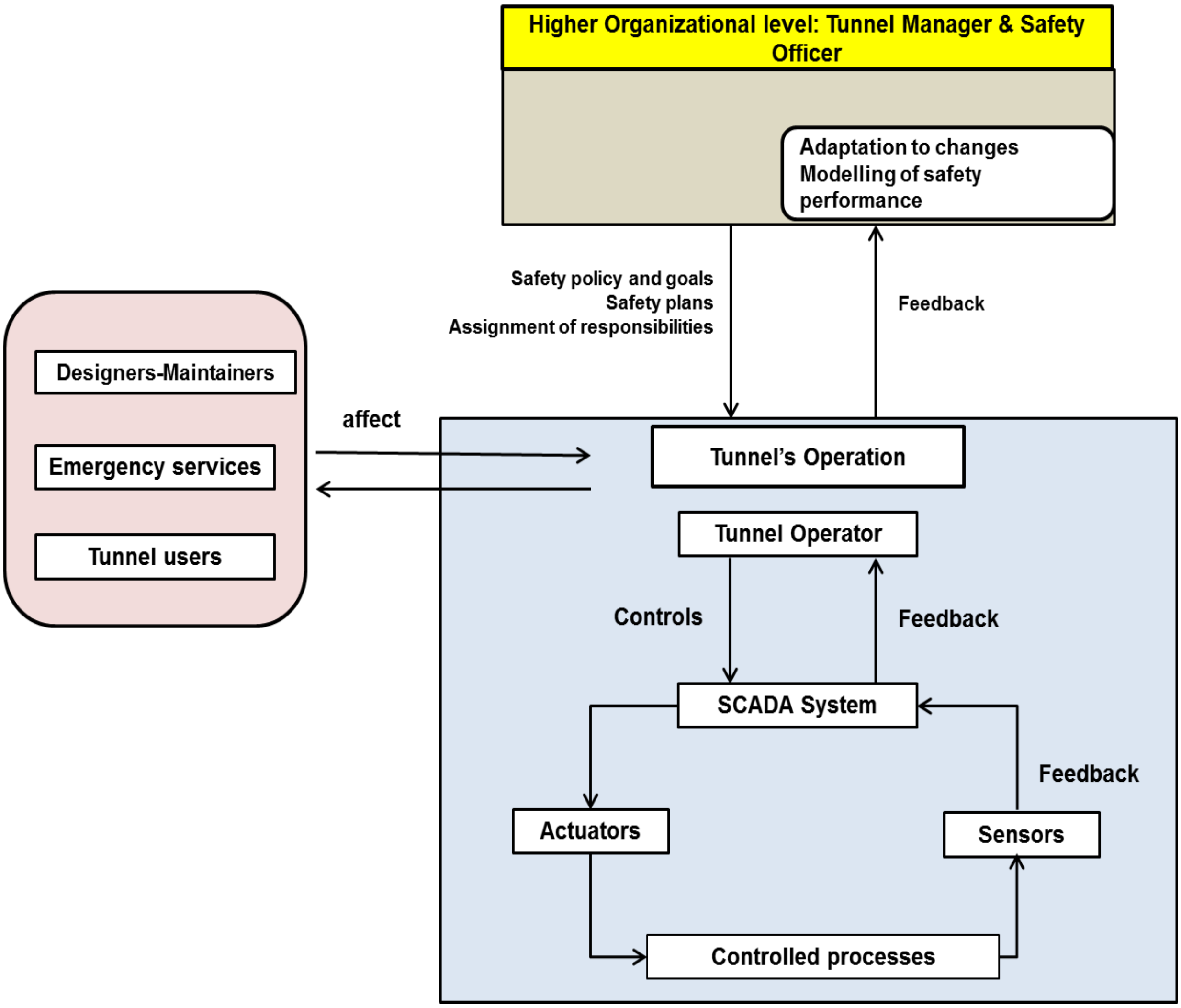


Figure 24: A road tunnel's safety control structure

Taking into account that the aforementioned actors/entities have the responsibility for enforcing the system-level safety constraints it is only natural to consider that they also have the potential to violate them (i.e. to inadequately enforce them). Therefore, the aim of **the second step of the assessment** is to identify *how* the safety control structure may inadequately enforce the system-level safety constraints, i.e. what type of inadequate control actions may occur. At this step, two types of inadequate control actions should be examined: (1) the ones identified by the traditional STAMP approach, and (2) those identified by the joint STAMP-VSM framework presented in chapter 5. Particularly, in STAMP terms there are four types of inadequate control actions that may occur **from a human or an automated controller**:

1. A control action required for safety is not provided or is inadequately provided (e.g. fire ventilation is not provided or is inadequately provided).
2. An unsafe control action is provided that leads to a hazard (e.g. fire ventilation contributes to the inability of road users to evacuate the tunnel before the onset of untenable conditions).
3. A potentially safe control action is provided too late or too early (e.g. fire ventilation is provided too late).
4. A safe control action is stopped too soon or is applied too long (e.g. fire ventilation stops before the fire incident has been declared close).

In STAMP-VSM extension, inadequate control actions that may occur **at the organizational level** (mainly due to an inadequate modelling of safety performance and inadequate adaptations to changes) are:

1. Inadequate safety policy and goal setting.
2. Ineffective assignment of control authority and responsibility.
3. Inadequate design and implementation of safety plans.

Having identified what type of inadequate control actions may occur (i.e. *how* safety constraints may be inadequately enforced), **the third step of the assessment** aims to determine *why* these inadequate control actions may occur (i.e. *why* the system-level safety constraints may be inadequately enforced). The aim is to identify potential causal factors that may lead to the safety constraints' violation and consequently to the accident's occurrence. At this step, the classification of control flaws proposed by Leveson (figure 19) and the classification of the organizational control flaws presented in table 2 are used as a guide to identify the causal factors (i.e. the path) that may lead to the accident. Furthermore, in order to enhance the method with tools that may help the analysts to identify causal factors related to the tunnel operators' behaviour, concepts of the cognitive load model (Neerincx 2003) and the CREAM method (Hollnagel 1998) are also incorporated in the assessment. Finally, once the potential causal factors have been identified, **the fourth step of the assessment** aims to evaluate the overall safety. This is done by exploring how the identified causal factors have been handled in an examined road tunnel organization. If safety measures and procedures are inadequate, recommendations for improvements should be made. **The proposed systems-theoretic road tunnel safety assessment method can be used for tunnels supervised and controlled by a tunnel operator and a SCADA system**. To demonstrate the method as thorough as possible, an illustrative assessment is presented.

6.2 Case study description

To facilitate the reader to follow the illustrative assessment some fundamental aspects are presented below. These are:

➢ **Tunnel length and traffic volume:**

The tunnel's length is 1500m and its traffic volume (vehicles per lane) is 2500 vehicles per day.

➢ **Incident detection systems**

The case study road tunnel is equipped with the following incident detection systems:

- A CCTV system that monitors the tunnel. The CCTV system includes 21 cameras with the camera's distance to be almost 150m long.

➢ **Incident response systems**

The road tunnel is equipped with:

- Radio-transmission equipment.
- Loudspeakers.
- Variable Message Signs (VMS).
- Lane Control Signals (LCS).
- Variable speed limits signs (VSLS).

➢ **Ventilation system**

The tunnel is equipped with a longitudinal ventilation system, supervised by a SCADA system and a manned control center. The required longitudinal airflow is provided through 22 jet fans located in the infrastructure. The examined ventilation system is controlled by the SCADA system as follows: In the normal operating mode, the system works without the intervention of the tunnel operator. The control in this ventilation mode is associated with measured pollution and opacity levels (CO, dust and NO_x thresholds). When measurements are monitored over a predefined threshold, the SCADA system activates a particular number of jet fans in order to reduce the concentration of pollutants. For cost effectiveness, the SCADA may avoid starting a jet fan that has reached a maximum number of starts per hour.

On the other hand, the fire ventilation mode is not really an automated mode, but a pre-programmed sequence of actions in a manual mode. A validation of fire detection by the tunnel operator is equivalent to a launch of commands to start and execute the right operation procedure, which is a function of the fire position. The ventilation process for the fire ventilation mode has two phases. In phase 1, the pre-ventilation phase is initiated: A fire has been detected and the ventilation system is prepared to operate quickly if the tunnel operator confirms the fire event. If there is a false alarm, the tunnel operator adjusts the ventilation to the normal mode. If fire is confirmed, then phase 2 -the smoke management phase- is activated. Thus, phase 2 is based on a waiting loop (30 seconds) expecting the tunnel operator's validation. The predefined number of jet fans to run for each fire scenario is an initial value of the control algorithm, specific for the tunnel.

➢ **Emergency telephones and emergency exits**

The tunnel is equipped with emergency phones every 150m and there are emergency exits every 300 m.

➢ **Tunnel operator and road patrollers**

The tunnel is continuously supervised by 2 tunnel operators. In addition, the tunnel organization employs road patrollers in order to:

- Patrol on daily defined schedules along the road network with specially equipped vehicles in order to point out any unusual condition like: object on road, traffic congestions, failure of equipment, bad road operation and accidents.
- In case of incidents, they intervene according to the safety plans, mainly to re-establish traffic.

It must be mentioned that in order to perform the assessment, several documents should be studied (i.e. the operation manuals, emergency plans, and technical reports). Moreover, on-site visits to the tunnel control center and interviews with the tunnel operators have to take place.

6.3 Step 1: Determine accidents, hazards, safety constraints and control structure

The accident to be considered is **a fire in a tunnel** resulting **in loss of human lives and/or serious injuries**. The hazards that should be eliminated or controlled are:

- H_1: Inadequacy of the tunnel's systems and organizational procedures to control traffic disruption during the fire incident.
- H_2: Inadequacy of the tunnel's safety systems and organizational procedures to control smoke and fire.
- H_3: Inability of road tunnel users to evacuate the tunnel before the onset of untenable conditions.

Consequently, the safety constraints that should be enforced are:

- SC_1: A safe and steady flow of traffic by responding to the traffic disruption in case of the fire incident.
- SC_2: The tunnel's safety systems and organizational procedures should control fire and smoke effectively.
- SC_3: Tunnel users should evacuate the tunnel before the onset of untenable conditions.

Finally, it is mentioned that the safety control structure of the tunnel system is very similar to the one presented in figure 24.

6.4 Step 2: Identify inadequate control actions

Having conceptualize the socio-technical road tunnel system in a control structure diagram (step 1 of the method), the second step continues the attempt to understand how the whole tunnel system may contribute to the accident. As presented in figure 25, the examined road tunnel system is included in the broader transportation system of Greece (i.e. the environment of the tunnel system) and has its own sub-systems (i.e. see level 1 and level 2). Taking into account that the assessment concentrates on the enforcement of the **system-level safety constraints**, the focus is on the identifying *how* and *why* the system-level safety constraints (SC_1-SC_3) may be inadequately enforced at level 0. At this point, it is crucial to mention that the system-level safety constraints may be inadequately enforced at level 0 due to inadequate control actions (aiming to enforce the constraints) at level 1 and level 2. Remember that in systems theory control actions are always related to the imposition of constraints. Therefore, in order to identify *how* the system-level safety constraints may be inadequately enforced, **the second step of the assessment concentrates on identifying inadequate control actions that may occur at level 1 and level 2**. It is noteworthy to mention that for each of the system-level safety constraints there is a relationship with a physical process at level 2. For example, the SC_1 is associated with *the traffic in the tunnel*, the SC_2 is associated with *the fire in the tunnel* and the SC_3 is associated with *the evacuation process*. The connection between the defined system-level safety constraints to the relevant physical controlled processes is an essential part for this step of the assessment.

Based on the joint STAMP-VSM framework, it has been deduced that, at level 1, the safety constraints may be inadequately enforced due to: (1) inadequate safety policy and goal setting, (2) inadequate assignment of control authority and responsibility, and (3) inadequate safety plans, that may result from inadequate feedback (i.e. inadequate modelling of safety performance and inadequate adaptation to changes). Concerning the inadequate control actions that may occur at level 2, these fall in the four general types of inadequate control actions proposed by STAMP, namely: (1) a control action required for safety is not provided or is inadequately provided, (2) an unsafe control action is provided, (3) a potentially safe control action is provided too late or too early, and (4) a safe control action is stopped too soon or is applied too long. For convenience, a table (like table 3 and table 4 presented below) can be used to record the results of this part of the assessment.

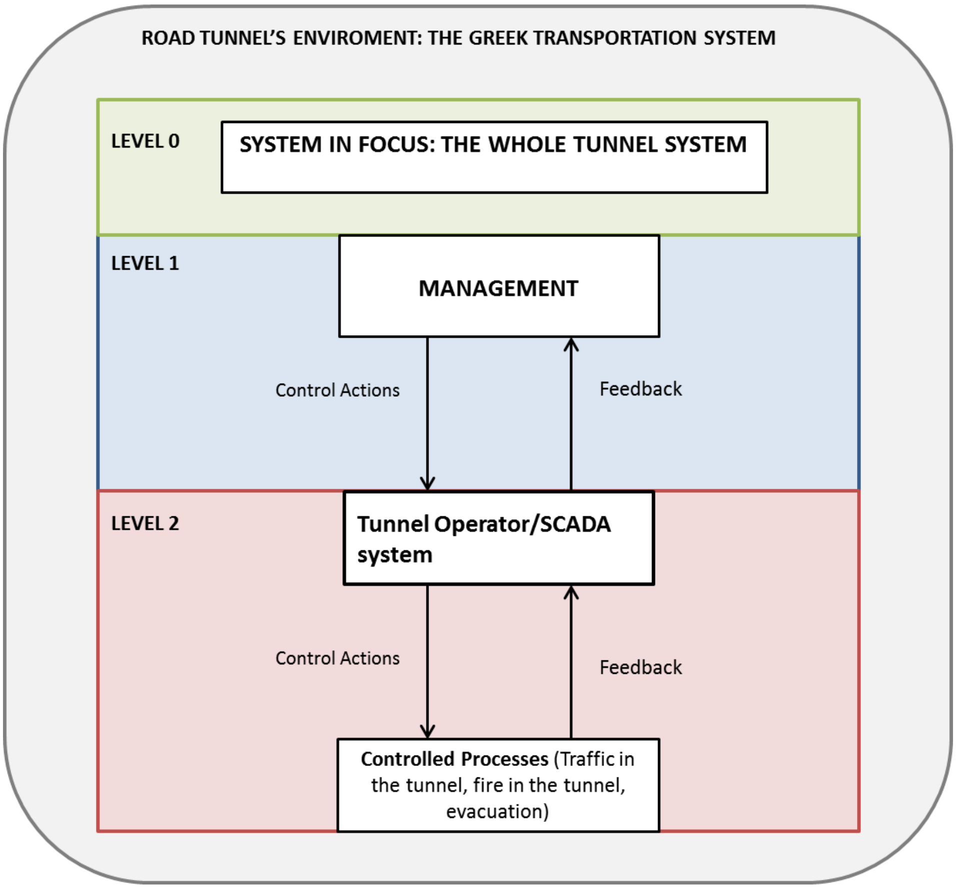

ROAD TUNNEL'S ENVIROMENT: THE GREEK TRANSPORTATION SYSTEM
LEVEL 0
SYSTEM IN FOCUS: THE WHOLE TUNNEL SYSTEM
LEVEL 1
MANAGEMENT
Control Actions
Feedback
LEVEL 2
Tunnel Operator/SCADA system
Control Actions
Feedback
Controlled Processes (Traffic in the tunnel, fire in the tunnel, evacuation)

Figure 25: Examine how safety constraints may be inadequately enforced

Potentially Inadequate Control Action at level 1
Inadequate Safety Policy and Goal Setting
Inadequate Assignment of Control Authority and Responsibility
Inadequate Safety Plans

Table 3: Inadequate control actions that may occur at level 1

		Potentially Inadequate Control Actions at level 2			
Controlled Process	**Control Action**	**Not Provided/ Inadequately Provided**	**Unsafe Control Action is Provided**	**Provided Too Late**	**Stopped Too Soon**
Traffic in the tunnel	Traffic Management	Traffic Management is not provided	-	Traffic Management is provided too late	-
Fire in the tunnel	Fire Ventilation Operation	Fire Ventilation Operation is not provided/ is inadequately provided	Unsafe Fire Ventilation Operation is provided	Fire Ventilation Operation is provided too late	Fire Ventilation Operation is stopped too soon
Evacuation process	Command Evacuation	Command for Evacuation is not provided	-	Command for Evacuation is provided too late	-

Table 4: Inadequate Control Actions that may occur at level 2

6.5 Step 3: Identify why inadequate control actions may occur

The third step of the method examines the safety control structure to identify causal factors (i.e. control flaws in STAMP terms) that may lead to the inadequate control actions and respectively to the inadequate enforcement of the safety constraints. In essence, step 3 identifies the paths that may lead to the accident. This step contains the main bulk of the assessment and it is the one that creates the content of a fault tree analysis for example. However, the difference with the proposed systems-theoretic method is that provides much more guidance for identifying the potential causal factors.

Particularly, in order to identify organizational vulnerabilities and pathologies that may lead to safety problems, the joint STAMP-VSM framework (refer to table 2) is used as a guide. To identify control flaws that may occur from the SCADA system, the classification of Leveson (figure 19) is utilized. Furthermore, in order to enhance the method with tools that may help the analysts to identify causal factors related to the tunnel operators' behavior, concepts of the cognitive load model (Neerincx 2003) and the CREAM method (Hollnagel 1998) have been also included in the assessment. Figure 26 briefly presents the causal factors that may lead to the inadequate enforcement of the system-level safety constraints. In sections 6.5.1-6.5.4 these factors are discussed in much more detail.

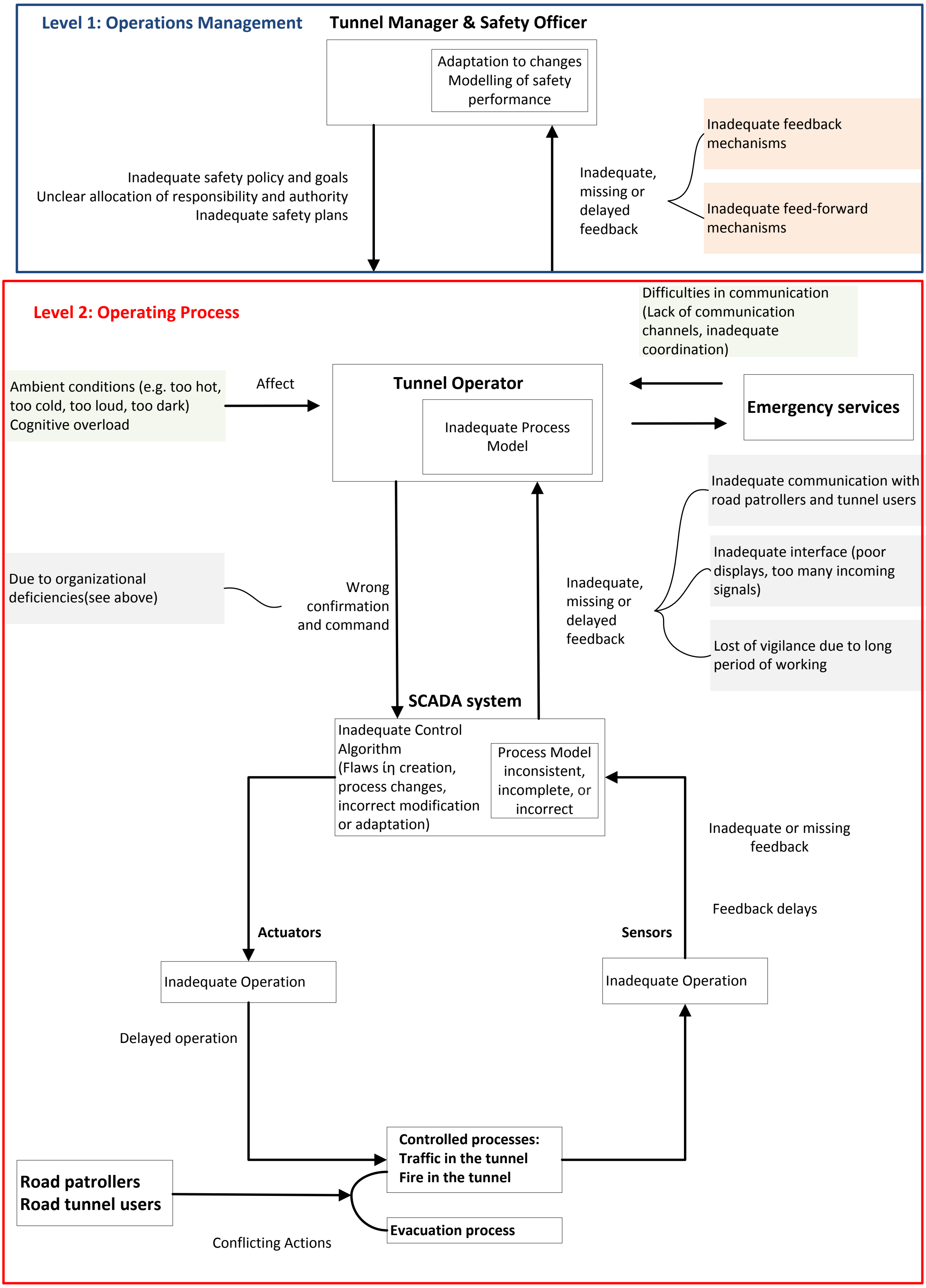

Level 1: Operations Management
Tunnel Manager & Safety Officer
Adaptation to changes
Modelling of safety performance
Inadequate safety policy and goals
Unclear allocation of responsibility and authority
Inadequate safety plans
Inadequate, missing or delayed feedback
Inadequate feedback mechanisms
Inadequate feed-forward mechanisms
Level 2: Operating Process
Difficulties in communication (Lack of communication channels, inadequate coordination)
Ambient conditions (e.g. too hot, too cold, too loud, too dark)
Cognitive overload
Affect
Tunnel Operator
Inadequate Process Model
Emergency services
Inadequate communication with road patrollers and tunnel users
Inadequate interface (poor displays, too many incoming signals)
Lost of vigilance due to long period of working
Due to organizational deficiencies(see above)
Wrong confirmation and command
Inadequate, missing or delayed feedback
SCADA system
Inadequate Control Algorithm (Flaws ίη creation, process changes, incorrect modification or adaptation)
Process Model inconsistent, incomplete, or incorrect
Inadequate or missing feedback
Feedback delays
Actuators
Sensors
Inadequate Operation
Inadequate Operation
Delayed operation
Controlled processes:
Traffic in the tunnel
Fire in the tunnel
Road patrollers
Road tunnel users
Evacuation process
Conflicting Actions

Figure 26: Causal factors that may lead to inadequate enforcement of safety constraints

6.5.1 Potential causal factors related to the SCADA system

By working around the loop related to the SCADA system (figure 26), potential causal factors that may lead to inadequate control actions for traffic management and fire ventilation operation are the following:

➢ **Process model inconsistent, incomplete or incorrect**

Related to inadequate control actions for traffic management

The process model of the SCADA system analyzes traffic data in order to understand how the traffic proceeds inside the tunnel and propose pre-programmed response plans to the tunnel operator. Potential causal factors belonging to this category are the following:

- Incomplete Traffic Data Collection System (TDCS). For example, the TDCS may not monitor for traffic congestions and stopped vehicles. This may lead to Inadequate Control Action (ICA): traffic management is not provided or is provided too late.

Related to inadequate control actions for fire ventilation

The process model is the way the SCADA system gets informed about the fire progress. When the SCADA system has a different "perception" of the process than the real state, erroneous control commands may be issued. Potential causal factors belonging to this category are the following:

- The fire ventilation strategy may be based on the assumption that vehicles downstream the fire are able to exit the tunnel unhindered, thus the ventilation system applies high velocities. However, this may not be the case and vehicles/people may be blocked downstream the fire. Hence, an incorrect process model may lead to ICA: unsafe fire ventilation operation is provided.
- The process model of the SCADA system may not reflect the actual state after a restart of the system. For example, due to technical reasons (e.g. failure of the power supply system or after a temporary public supply network shut down) the SCADA system may restart its operation. In this case, the sensors (e.g. temperature sensors and anemometers) may provide the values pertained before the start up although significant changes have occurred (i.e. process model inconsistent). This may lead to ICA: unsafe fire ventilation operation/inadequate fire ventilation operation.

- **Flaws in creation, incorrect modification, incorrect adaptation of control algorithm**

Related to inadequate control actions for traffic management

Potential causal factors belonging to this category are the following:

- The SCADA system may not provide a pre-programmed response (i.e. a response plan) for conceivable scenarios such as: vehicle breakdowns and traffic congestions. Such pre-programmed response should consider the total closure of the tunnel, the partial or lane closure and/or request for fluctuation in speed limits. This may lead to ICA: traffic management is not provided.

Related to the inadequate control actions for fire ventilation

Potential causal factors belonging to this category are the following:

- Flaws in the creation process of the control algorithm meaning that the design fire may have been underestimated. This may have occurred in the initial design stage, or it may have occurred due to incorrect adaptation over time (e.g. changes in the expected traffic volume, type of vehicles and combustible loads, etc.). This may lead to ICA: fire ventilation operation is inadequately provided.
- The tunnel is unidirectional; however for technical reasons (for example due to maintenance work at the other tube) the tunnel may be also used bi-directionally. For such situation the control algorithm may not provide adequate response plans (i.e. incorrect modification). This may lead to ICA: fire ventilation operation is inadequately provided.
- During normal ventilation, several operational constraints may be posed to the ventilation system. For example, particular jet fans may stop operating when they have reached a maximum number of starts per hour or because of vibration thresholds. Such operational constraints may not have been de-activated in case of an emergency, hence there is potential for incorrect modification of the ventilation system from normal to fire operation. This may lead to ICA: fire ventilation operation is stopped too soon.
- The fire ventilation mode should not stop until the tunnel operator declares the event close. Emission thresholds that are activated during normal ventilation mode (e.g. CO and CO_2) in order to stop the ventilation operation may not have been de-activated during the fire ventilation mode (i.e. incorrect adaptation). This may lead to ICA: fire ventilation operation is stopped too soon.

- **Inadequate operation of the actuators**

Related to inadequate control actions for traffic management

Potential causal factors belonging to this category are the following:

- The Variable Message Signs (VMS) may fail.
- The Variable Speed Limits Signs (VSLS) may fail.
- The Lane Control Signs (LCS) may fail.
- Traffic lights may fail.
- Management of the brightening of the VMS, VSLS, LCS may not have been provided (for example in case of dense smoke).
- Degradation of the VMS, VSLS, LCS and traffic lights, due to poor maintenance.

The aforementioned causal factors may lead to ICA: traffic management is not provided.

Related to inadequate control actions for fire ventilation

Potential causal factors belonging to this category are the following:

- Ventilation command transmission network may fail and redundant networks may not have been provided.
- Mechanical failure of jet fans due to high temperatures inside the infrastructure.
- Delayed operation of jet fans due to the starting procedures (i.e. a sequential procedure) which is used to avoid electrical overload (i.e. time lag).
- Degradation of the jet fans due to poor maintenance.

The aforementioned causal factors may lead to ICA: fire ventilation is inadequately provided.

- **Inadequate operation of sensors**

Related to inadequate control actions for traffic management

Potential causal factors belonging to this category are the following:

- The TDCS may totally fail. This may lead to ICA: traffic management is not provided.

Related to inadequate control actions for fire ventilation

Potential causal factors belonging to this category are the following:

- The anemometers and temperature sensors may fail. This may lead to ICA: fire ventilation is inadequately provided or unsafe fire ventilation is provided.

- **Feedback inadequate, missing or delayed**

Related to inadequate control actions for traffic management

Potential causal factors belonging to this category are the following:

- Feedback delays from TDCS.
- The SCADA system may not respond to the lack of an expected input over a given period of time (i.e. lack of reconstitution of missing data from TDCS).
- The SCADA system may not adequately respond to out-of-range or unexpected data (i.e. lack of reconstitution of invalid data from TDCS).
- Particular actuators (e.g. LCS, VMS, VSLS) cannot be activated (i.e. due to failures) but the SCADA system does not have feedback channels to verify that the commands issued are not executed.

The aforementioned causal factors may lead to ICA: traffic management is not provided.

Related to the inadequate control actions for fire ventilation

Potential causal factors belonging to this category are the following:

- The SCADA system may not respond to the lack of an expected input over a given period of time (i.e. lack of reconstitution of missing data from anemometers and temperature sensors).
- The SCADA system may not adequately respond to out-of-range or unexpected data (i.e. lack of reconstitution of invalid data from anemometers and temperature sensors).
- Particular jet fans cannot be activated (i.e. due to failures) but the SCADA system has not feedback channels to verify that the commands issued are not executed.
- Fire detectors usually activate an alarm upon a pre-programmed rate of rise of the temperature and/or a maximum temperature value in the tunnel. If this process model is incorrect then the fire detection is prone to fail or to delay.
- The air flow provided in the tunnel due to pressure differences at the tunnel portals or due to the normal ventilation operation may significantly affect the detectability of the sensors. When a fire occurs in a tunnel, it will probably cause an increase in the temperature and smoke level. Such an increase might not be enough to raise a fire alarm; however, it might be high enough to activate normal ventilation for diluting emissions. This airflow (typically in the area of 2-5m/s) may significantly increase the detection time of the fire.

The aforementioned causal factors may lead to ICA: fire ventilation is not provided or it is provided too late.

6.5.2 Potential causal factors related to the Tunnel Operator

Related to inadequate control actions for fire ventilation, traffic management and the evacuation process

➢ **Inadequate process model**

If the tunnel operator does not know what is happening inside the tunnel it goes without saying that he cannot take the appropriate actions. Potential causal factors belonging to this category are the following:

- **Poor displays** about the status in the tunnel related to: the location of the fire incident, the possibility of traffic congestions, the presence of DGs and the approximate number of people inside the infrastructure (particularly downstream the fire). Examples of causal factors that may lead to this category are:
    - Surveillance cameras may not cover all lanes of the tunnel, images may be unclear, and the distance between the cameras may be too long.
    - Difficulties in setting up the nearest camera to the incident location.
    - The tunnel layout may not be presented in an informative way by displays..
    - Lack of redundant feedback channels. For example, when specific cameras are not usable (e.g. in case of dense smoke) there is no other way to get informed about the situation in the tunnel.
    - The SCADA system may not produce alarms for important failure events (e.g. failures in anemometers, fire detectors, jet fans).
    - The SCADA system produces only visual alarms although audio alarms are also needed.
    - Feedback delays from the SCADA system.

➢ **Inadequate communication with road patrollers and emergency services**

If the communication between the tunnel operator and the emergency services is not well organized this may lead to an extra pressure on the tunnel operator and consequently to deterioration of his performance.

- **Poor working conditions**

The CREAM method (Hollnagel 1998) highlights that particular ambient conditions (e.g. much noise and/or too dark in the control center) may lead to deterioration of operators' performance. Therefore, the potential for such ambient conditions to exist in the control center should be examined.

- **Cognitive overload**

According to Neerincx's cognitive load model (2003) there are three factors that may have a substantial effect on the mental effort of the tunnel operator.

- The first is the **percentage time occupied**. According to the cognitive load model, in a control center two tunnel operators should be on duty, switching roles every few hours (Papaioannou and Georgiou 2003).
- The second factor is the **level of information processing**. To address the cognitive tasks demands, the cognitive load model incorporates the Skill-Rule-Knowledge framework of Rasmussen. At the skill-based level, information is processed almost automatically; hence, the cognitive effort is very little. At the rule-based level the input information results in routine solutions (i.e. safety plans with rules of the type: if <event> then do <action>) and the cognitive effort is manageable. Finally, at the knowledge-based level the input information should be analyzed and innovative solutions should be designed at hoc. This type of information processing is very demanding in cognitive effort. In addition, during the fire incident too many incoming in coming signals, not all of which are relevant to the emergency, may lead to a high level of information processing.
- The third factor is the **task-set switching** and results in cognitive overload in cases the tunnel operator has to perform too many different tasks at the same time.

The combination of the aforementioned three factors determines the cognitive task load of the tunnel operator. Therefore, the aforementioned aspects should be considered when performing the systems-theoretic road tunnel safety assessment.

6.5.3 Potential causal factors related to the Tunnel Users

Related to traffic management

Although particular traffic instructions may be given by the tunnel operator and the SCADA system through the VMS, VSLS and LCS, several studies (e.g. Noizet et al. 2003; PIARC

2008b) have revealed that during a fire incident the tunnel users may not adhere to such instructions. Particularly, tunnel users may choose to drive their vehicle outside the infrastructure in a reverse mode or by making a U-turn. Such driving behaviour may lead to hazardous situations (i.e. collisions). However, the only possible way to avoid such behaviours might be through information campaigns which inform users about the behaviour they should adhere in case of an emergency. For this reason, the safety assessment should examine whether such information campaigns have been organized by the road tunnel organization.

Related to fire ventilation

The first thing that tunnel users should do in case of a fire is to raise an alarm by using the available emergency telephones. Whether tunnel users activate an alarm, or not, is mainly related to the design of the emergency telephones (i.e. ergonomic issues) and the information they may have received in the past through information campaigns on this issue. Hence, the safety assessment should investigate the design of the emergency telephones and should examine whether information campaigns have been organized.

Related to evacuation

In case of a fire, tunnel users should go immediately to the nearest emergency exit. Aspects that greatly affect the evacuation process are the following (Noizet et al. 2003; PIARC 2008b):

- The safety assessment should examine whether there is a way to clearly inform the users that an emergency situation exists in the road tunnel. This may be achieved by alarm sirens, loudspeakers or broadcasting radio messages.
- The safety assessment should examine if there is a permanent lighting at the emergency exits and if doors are painted in green -in order to help tunnel users to identify them easier.
- The safety assessment should examine whether flashing lights and sound beacons (informing “exit here”) have been installed in the tunnel in order to help the users locate the exit even in the midst of smoke.
- The safety assessment should examine whether there are means to inform tunnel users how to proceed after passing the emergency exit.
- If audio devices (e.g. sirens, loudspeakers and sound beacons) exist in the tunnel the safety assessment should examine whether such devices remain audible in spite of the fire ventilation operation.

All the aforementioned causal factors can be classified in the following three categories: (1) lack of knowledge on how to behave during an emergency, (2) poor design of the emergency telephones, and (3) poor means to facilitate the evacuation process.

6.5.4 Potential causal factors related to Management

Moving up to level 1 of the safety control structure (figure 26) the safety assessment shifts to identifying potential causal factors at the organizational level. The classification presented in table 2 is used as a guide.

❖ **Inadequate formulation of safety policy and goal setting**

➢ **Ambiguous safety policy or lack of safety policy**

Potential causal factors belonging to this category are the following:

- The tunnel organization may not provide a written statement of its safety policy (mentioning that the ultimate goal is to save human lives even without considering potential damage to the structure). The policy should also provide the scope for discretion and judgment in case safety conflicts with productivity (i.e. the operation of the tunnel).

➢ **Trapped in the often unnoticed loop between formulating goals and monitoring**

Potential causal factors belonging to this category are the following:

- The tunnel organization may only monitor equipment's reliability, neglecting other important aspects of co-ordination with emergency services and training. This may lead to "reverse polarity" where the tunnel organization's goals are limited only to what has been monitoring.

➢ **Eroding safety goals**

Potential causal factors belonging to this category are the following:

- Normalization of deviance exists, where false alarms, degradation of equipment, poor maintenance, lack of safety audits, lack of risk analysis, inadequate adaptation of safety plans, inconsistency between safety plans and routines in practice may have been accepted.

❖ Ineffective assignment of control authority and responsibilities

➢ Imbalance between autonomy versus centralized control

Potential causal factors belonging to this category are the following:

- The tunnel organization may have chosen a decentralization mode of authority for its personnel although some traceability of actions is needed.
- The tunnel organization may have chosen a centralization mode although flexibility is needed.

➢ Gaps and overlaps in responsibilities

Potential causal factors belonging to this category are the following:

- Gaps and overlaps of responsibilities related to the constant monitoring of the availability and functionality of technical installations. For example, it may not be clear which technical installations are monitored by the SCADA and which are monitored by the tunnel operator, the maintenance personnel and road patrollers.
- Gaps and overlaps of responsibilities among road patrollers and emergency services in relation to traffic management, fire control and rescue operations. For example, it may not be clear whether road patrollers have the authority to intervene in order to ensure an initial control of the fire incident or whether they should just prepare and facilitate the access for the emergency services.
- In case that the tunnel is simultaneously supervised by two or more tunnel operators, gaps and overlaps of responsibilities may occur. In such cases, it is essential to have precisely define the tasks and determine the “senior” operator, if conflicts in decision making occur.

➢ Responsibility assigned is not suited to personnel

Potential causal factors belonging to this category are the following:

- The tasks, roles and required skills for the maintenance personnel, the road patrollers and the tunnel operators may not have been precisely defined. Without well-defined requirements for each role it is very difficult to ensure that the appropriate personnel adequately undertake the necessary responsibilities.
- The organization’s approach to managing uncertainty may have not been considered when responsibilities are assigned to personnel. For example, opting for flexibility requires more qualified personnel.

- The tunnel operator may have been assigned with the responsibility of checking automation and this may create trouble in maintaining vigilance for a long period of time.

❖ **<u>Inadequate design and ineffective implementation of safety plans</u>**

➢ **Mismatch between the safety plans and the strategy of managing uncertainty**

Potential causal factors belonging to this category are the following:

- Action rules may not have been determined for the personnel although stability is the purpose.
- Process rules may not have been determined for the personnel although flexibility is the purpose.

➢ **Lack of co-ordination**

Potential causal factors belonging to this category are the following:

- Lack of coordination between the tunnel operator and the emergency services during the design/implementation of safety plans. Training visits for the emergency services may not be regular enough. In addition, the timeliness of the messages transmitted may have not been considered.

➢ **Inconsistency between plans and routines in practice**

Potential causal factors belonging to this category are the following:

- Inconsistency between written safety plans and routines in practice.

➢ **Plans not following changes in the system, stagnant plans**

Potential causal factors belonging to this category are the following:

- Safety plans may not have been updated although significant changes have occurred, e.g. changes in the traffic volume, in the equipment, related to human resources and emergency services, etc.

➢ **Lack of resources**

Potential causal factors belonging to this category are the following:

- Lack of human resources (i.e. tunnel operators, road patrollers, maintenance personnel) for the implementation of safety plans.

- Lack of availability of spare parts of equipment needed for maintenance, i.e. there is lack of a mechanism to ensure that spare parts of equipment needed for preventive maintenance are available.

➢ **Inefficient training procedures**

Potential causal factors belonging to this category are the following:

- Inadequate training for the tunnel operator and the maintenance personnel (e.g. infrequent training, lack of problems solving, lack of evaluation of training), before starting their tasks and throughout their career.

❖ **<u>Inadequate modelling of safety performance</u>**

➢ **Inadequate feedback channels**

Potential causal factors belonging to this category are the following:

- Periodic technical inspections in order to confirm the correct functionality of safety equipment may not have been undertaken.
- A detailed maintenance record may not be available in terms of defects and repairs.
- Exercises and safety drills aiming to test the integration of the system may not have been performed, or may have been inadequately de-briefed.
- Reporting schemes which can be used by the tunnel personnel in order to communicate problems may not have been provided or may have been inadequately provided.
- The tunnel personnel may be unwilling to report on “near misses” because of fear for repercussions.
- An incident analysis methodology may not have been provided.
- The tunnel organization may have not distinguished between the minimum dataset needed for statistical reasons and the detailed dataset needed in order to perform specialized incident analysis.
- Lack of feedback about the actual conditions (i.e. traffic volume, portion of DGs transported via the tunnel, ageing of equipment and frequency of traffic congestions).
- Lack of feedback concerning changes in the tunnel personnel or in relation to the emergency services.
- An initial safety inspection that allows setting a reference point to be tested by periodic inspections may not have been provided.

- Lack of feedback about the knowledge of the road tunnel users on road tunnels safety issues (i.e. what can be expected from them in case of an emergency).

- **Inadequate feed-forward control mechanisms**

Potential causal factors belonging to this category are the following:

- Risk analysis results may have not been used in order to develop safety plans hence there are several scenarios for which response plans have not been designed.
- The minimum operating conditions, under which the tunnel should be closed to traffic, may not have been defined.

- ***Inadequate adaptation to changes***

- **Open loops**

Potential causal factors belonging to this category are the following:

- A procedure that ensures the incorporation of feedback (e.g. from incidents, accidents, safety exercises, information campaigns and technical inspections) in safety plans may not have been provided.
- A procedure that ensures that reviews and updates of risk analysis, whenever significant changes have occurred, may not have been provided.

- **Lack of double loop learning**

Potential causal factors belonging to this category are the following:

- A procedure that ensures the adjustment of incident analysis methodology and reporting schemes, based on practical experience, may not have been provided.

6.6 Step 4: Evaluating safety

The evaluation of the overall tunnel safety is made by examining how the identified potential causal factors have been handled. If safety measures and procedures are inadequate, recommendations for improvements should be made.

6.6.1 The results of the assessment

6.6.1.1 *Potential causal factors related to the SCADA system*

Related to Traffic Management

The results of the assessment are summarized in table 5.

Potential Causal Factor	How the potential causal factor has been handled
Process model incomplete or incorrect	The SCADA system does not monitor for traffic congestion and stopped vehicles. It only monitors the vehicles' speed. Hence, the process model of what is happening inside the infrastructure seems to be incomplete.
Flaws in creation, incorrect modification, incorrect adaptation of control algorithm	The SCADA system provides a pre-programmed response for scenarios related to vehicle breakdowns and traffic congestions (once they have been identified by the tunnel operator). For example, in the case of a fire in the tunnel, the VMS displays the message: "fire in the tunnel, do not enter the tunnel" and traffic lights at the entrance are turned to red color.
Inadequate operation of the actuators	The tunnel organization does not have a coherent maintenance strategy (mainly due to lack of resources and financial problems), hence inadequate operation of VMS, VSLS, LCS and traffic lights is possible. In addition, a management of the brightening of the aforementioned equipment has not been considered.
Inadequate operation of the sensors	The TDCS is directly supervised by the SCADA system. Hence a failure of TDCS will immediately raise an alarm to the tunnel operator.
Inadequate, missing or delayed feedback	Although the time for transmission of the signals from the TDCS (mainly speed records) to the SCADA system has been considered, the technical report on the SCADA system's design does not provide the necessary information to conclude whether the system adequately responds to invalid data from TDCS.

Table 5: The results related to the SCADA system's traffic management

Related to Fire Ventilation Operation

The results of the assessment are summarized in table 6.

Potential Causal Factor	How the potential causal factor has been handled
Process model incomplete or incorrect	The fire ventilation strategy is based on the assumption that vehicles downstream the fire are able to exit the tunnel unhindered, thus the ventilation system applies high air velocities. The SCADA ventilation operation is not automated linked to TDCS, hence if traffic congestion occurs downstream the fire the only way to identify it is by the tunnel operator who observes the CCTV. As far as the incorrect restart of the system is concerned, the technical report on the SCADA system's design does not provide the necessary information to conclude whether this particular causal factor has been handled.
Flaws in creation, incorrect modification, incorrect adaptation of control algorithm	- The SCADA system provides pre-programmed response plans for controlling fires up to 100MW. Fires with HRR more than 100MW cannot be adequately controlled. - The SCADA system does not provide a control algorithm in case the tunnel is used with bi-directional traffic. - All operational constraints which are activated during normal operation are de-activated in the fire ventilation mode.
Inadequate operation of the actuators	- A redundant ventilation command transmission network has been provided. - The jet fans can operate in temperatures near 250^{0}C so they are not expected to fail due to high temperatures, except from near incidents. - Degradation of the jet fans due to poor maintenance should be expected. - The jet fan starting procedure is based on a star delta start system, meaning that the SCADA is managing the time between each start of the installation in order to limit an electrical overload with a default value at 10 seconds. This time interval is too short and it is not considered to result to a delayed operation of the jet fans.
Inadequate operation of the sensors	The anemometers and the temperature sensors are directly supervised by the SCADA system.
Inadequate, missing or delayed feedback	- The SCADA system has a reconstitution process for missing or invalid data from anemometers and temperature sensors. - If particular jet fans fail to be activated, the SCADA system is informed by specific feedback channels. - The pre-programmed rate of rise of the temperature that activates the fire detection has been settled 3^{0}C over a period of 3 minutes, which is an acceptable detection criterion. - The airflow at the normal operation of the ventilation system does not exceed the value of 2m/s, hence it is not considered to affect the detectability of the sensors.

Table 6: The results related to the SCADA system's ventilation operation

6.6.1.2 *Potential causal factors related to the Tunnel Operator*

The results of the assessment are summarized in table 7.

Potential Causal Factor	How the potential causal factor has been handled
Inadequate process model	Part of the fire detection system has been de-activated due to technical failures. Hence, the road tunnel operators rely only on the CCTV in order to detect fire incidents. Additionally, considering that the SCADA system does not monitor for traffic congestions and stopped vehicles, such events should also be detected by the tunnel operators who are requested to constantly observe the CCTV. However, two problems have been identified: 1. The distance among the surveillance cameras is too long (especially if one considers that CCTV is the only way to observe what is happening inside the tunnel). As a result, images are unclear at the end of the area supervised by each camera. 2. The tunnel operators supervise more than one tunnel. Consequently, the images displayed to the video matrix (which the tunnel operators observe) are more than the matrix's capacity can handle. For this reason, images captured by the surveillance cameras are presented to the video matrix circularly with a time interval of 30 seconds. During this time particular locations of the tunnels are not depicted to the video matrix. As it has been already mentioned, the only way to observe what is happening inside the tunnel is via the CCTV. Other channels have not been provided. However, in case of a fire incident, CCTV will be rendered useless because of dense smoke (figure 27). Hence, other feedback channels should have been provided. Furthermore, it should be mentioned that the SCADA system does not produce alarms for many critical events.
Inadequate communication	The radio frequency dedicated to the communication between the tunnel operators and the emergency services has change over time (i.e. emergency services broadcast in a different radio frequency than the one re-broadcasted in the tunnel). Hence, it may take considerable time for the tunnel operators to communicate with the road patrollers who are the only link between the operators and the emergency services.
Poor working conditions	The tunnel operators declared that the ambient conditions in the control center are satisfactory.
Cognitive overload	The control center has continuously two operators on duty. However, the operators supervise more than one tunnel. This means that the level of information processing is high. On the contrary, the SCADA system provides pre-programmed responses for many scenarios, therefore it can be deduced that the cognitive effort is manageable in this sense. Factors that have been identified to have a substantial effect on the mental effort of the operators are the following: 1. Tunnel operators have to perform too many different tasks at the same time in case of an emergency (i.e. call emergency services,

	communicate with tunnel users, activate pre-programmed response plans and monitoring what is happening). Therefore, the task-set switching is considered to be high. 2. The information presented to the tunnel operators are restricted to several indicators which are distributed in a simplified sketch of the tunnel in their displays. It is remarkable, that both functional and not functional systems are represented in red color. In this way, it seems very difficult to identify failures that may have been presented by the SCADA system.

Table 7: The results related to the Tunnel Operator

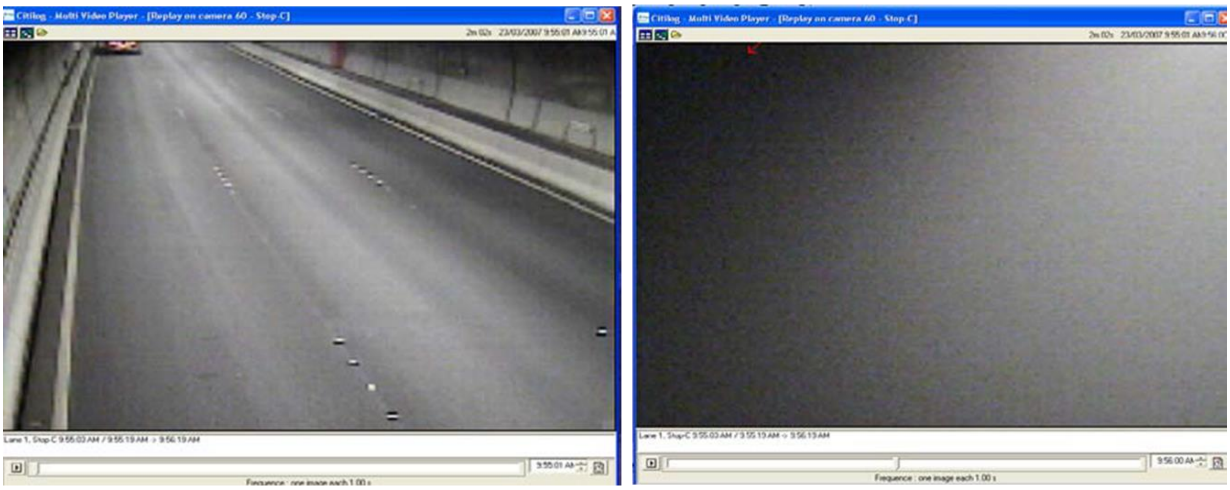

Citilog - Multi Video Player - [Replay on camera 60 - Stop-C]
2m 02s 23/03/2007 9:55:01 AM 9:55:01 A
Lane 1, Stop-C 9:55:03 AM / 9:55:19 AM -> 9:56:19 AM
9:55:01 AM
Frequence : one image each 1.00 s
Citilog - Multi Video Player - [Replay on camera 60 - Stop-C]
2m 02s 23/03/2007 9:55:01 AM 9:56:0
Lane 1, Stop-C 9:55:03 AM / 9:55:19 AM -> 9:56:19 AM
9:56:00 AM
Frequence : one image each 1.00 s

Figure 27: How smoke may render the CCTV useless in only 60 seconds (Dix 2011)

6.6.1.3 Potential causal factors related to the Tunnel Users

The results of the assessment are summarized in table 8.

Potential Causal Factor	How the potential causal factor has been handled
Lack of knowledge on how to behave during an emergency	Information campaigns on road tunnel safety have not been performed by the motorway company in which the examined road tunnel is located. Furthermore, it is notable that information campaigns have not been performed, in general, in Greece. A recent questionnaire survey on road tunnel users' behaviour (Kirytopoulos et al.) revealed that the Greek road tunnel users are prone to make U-turns and to drive in reverse gear in case of an emergency. In addition, a large share of people declared that does not comply with the traffic instructions given through the VMS, VSLS and LCS and, moreover, may shelter in vehicles rather than evacuate the tunnel. All in all, it seems that Greek road tunnel users do not have the appropriate level of knowledge on the issue of road tunnels safety; hence many inadequate actions should be expected from them.
Poor design of emergency telephones	The road tunnel is equipped with emergency telephones every 150 m. However, taking into account that the emergency telephones are installed in emergency boxes, and not in emergency stations, it is open to question whether the road tunnel users are indeed able to communicate with the tunnel operators in an environment where the noise may exceed the 90dB. In addition, it is remarkable that emergency boxes (like the ones in which the emergency telephones are installed) are located every 50m in the tunnel to provide fire-fighting equipment. Therefore, although the design of the emergency boxes is exactly the same, only the one third of them is equipped with emergency telephones. This means that the tunnel users in their attempt to communicate with the tunnel operators may open an emergency box which is only equipped with fire- fighting equipment. It is questionable whether users will comprehend that they should search for an emergency telephone in the following emergency box or they will just abandon their effort to communicate with the tunnel operators. Finally, it should be mentioned that the emergency boxes are not easy visible. Especially, in case of a fire, the dense smoke will make it very difficult for the tunnel users to identify them.
Poor means to facilitate the evacuation process	Loudspeakers have been installed in the tunnel; however pre-recorded messages are not transmitted in case of an emergency. This means that emotion or stress in the voice of the operator may cause stress or even panic to users. Additionally, the tunnel organization has never checked whether the loudspeakers remain audible in case the fire ventilation operation is fully activated. The doors of the emergency exits are painted in green but they are not equipped with flashing lighting. Finally, there are no signs to inform tunnel users how to proceed after passing the emergency exits.

Table 8: The results related to the Tunnel Users

6.6.1.4 Potential causal factors related to Management

The results of the assessment are summarized in table 9.

Potential Causal Factor	How the potential causal factor has been handled
Inadequate safety policy and goals	
Ambiguous safety policy or lack of safety policy	The tunnel organization has not provided a safety policy.
Trapped in the often unnoticed loop between formulating goals and monitoring	The tunnel organization monitors only the equipment's reliability. There are not well-defined and measurable goals for aspects such as co-ordination with emergency services and training.
Eroding safety goals	Normalization of deviance exists. Degradation of equipment, lack of preventive maintenance, lack of safety audits, inconsistency between safety plans and routines in practice have become the norm.
Ineffective assignment of control authority and responsibilities	
Imbalance between autonomy versus centralized control	The tunnel organization has not decided whether to opt for stability or flexibility. For example, some action rules have been given to the tunnel operators. However, in practice, the tunnel operators are allowed to make their own decisions.
Gaps and overlaps of responsibilities	Although the tunnel is supervised by two operators, the specific tasks that each operator should perform in case of an emergency have not been defined. In this overlapping area many conflicts or gaps may occur.
Responsibility assigned is not suited to personnel	The tasks, roles and required skills for the personnel have not been defined; hence it is very difficult to ensure that personnel are indeed the appropriate. It is also notable, that the tunnel operators have been assigned with the responsibility of monitoring what is happening inside the tunnel. Since more than one tunnels are supervised by the particular tunnel control center, it is possible for the operators to have difficulties in maintaining vigilance for a long period of time. Finally, it must be highlighted that although the tunnel operators have been given (informally) the authority to take initiative during an emergency, specific qualifications for their recruitment have not been defined.
Inadequate design and ineffective implementation of safety plans	
Mismatch between the safety plans and the strategy of managing uncertainty	The tunnel organization has not decided on the strategy to managing uncertainty. Action rules have been given to the tunnel operators but in practice the organization operates in a decentralized mode. In this sense, there is a significant mismatch between the plans and the operating mode.

Lack of co-ordination	Some coordinated exercises have been made with the participation of representatives from the fire brigade, however considering the communication problems that exist (i.e. the emergency services broadcast in a different radio frequency than the one re-broadcasted in the tunnel) it can be deduced that problems in co-ordination should be expected.
Inconsistency between plans and routines in practice	Road patrollers have been assigned with the responsibility to prepare and facilitate the access for the emergency services, in case of an emergency. Nevertheless, in practice they are usually intervening in order to attempt an initial control of the fire incident. Similarly, some action rules have been given to the tunnel operators in case of an emergency but in practice they have the freedom to make their own decisions.
Plans do not follow changes in the system, stagnant plans	Half of the fire detection system has failed, notwithstanding, safety plans have not been updated even if the reliability of the fire detection system was a crucial assumption when the safety plans have been formulated. Similarly, safety plans have been based on the assumption that DGs are not transported via the tunnel but this is not always the case (i.e. several violations on this restriction occur and DGs are frequently transported through the infrastructure).
Lack of resources	There is significant pressure on resources (i.e. availability of spare parts of equipment needed for preventive maintenance) due to financial problems. This systemic causal factor affects the availability and reliability of all safety systems. Moreover, many safety inspections and audits which should have been performed have been postponed.
Inefficient training procedures	Although some basic training is given to the tunnel operators before they undertake their responsibilities, there is a lack of a structured training curriculum.
Inadequate modelling of safety performance	

Inadequate feedback channels	- Periodic technical inspections in order to confirm the correct functionality of safety equipment have been undertaken. - A detailed maintenance record is available; however the problem is that due to lack of resources the maintenance strategy is most of the times corrective rather than preventive. - As it has been mentioned some coordinated exercises have been made with the participation of representatives from the fire brigade. Nevertheless, these exercises have not been de-briefed. - Tunnel operators are requested to complete a report at the end of their shift. However, these reports are not reviewed either by the tunnel manager or by the safety officer. - An incident analysis method has not been provided, moreover, the tunnel organization has not distinguished between the minimum dataset needed for statistical reasons and the detailed dataset needed in order to perform specialized analyses. - There is lack of feedback concerning changes in key positions in the emergency services. - An initial safety inspection that allows setting a reference point that should be tested by periodic safety inspections has not been provided. - There is significant lack of feedback about the knowledge of the road tunnel users on road tunnels safety issues (i.e. what can be expected from them in case of an emergency).
Inadequate feed-forward control mechanisms	The minimum operating conditions, under which the tunnel should be closed to traffic, and/or leading safety performance indicators, have not been provided.
Inadequate adaptation to changes	
Open loops	A mechanism (i.e. a procedure) that ensures the incorporation of feedback and the update of safety plans whenever necessary has not been provided.
Lack of double loop learning	A procedure that ensures the adjustment of feedback based on practical experience has not been provided.

Table 9: The results of the assessment related to Management

6.6.2 Recommendations for improvements

This step of the assessment includes **improvements that should be made in order to eliminate the possibility for inadequate control actions to occur** (i.e. to eliminate the potential for inadequate enforcement of the system-level safety constraints). Concerning the illustrative case study assessment, most of the causal factors related to the technical system (i.e. the SCADA system) have been handled by the road tunnel organization. Nevertheless, it is crucial for the SCADA system to be enhanced with a process model that monitors for traffic congestion and stopped vehicles. This will also affect the performance of the tunnel operators since the surveillance of such events will be made automatically and not by constantly observing the video matrix. As far as the fire ventilation operation is concerned, response plans (i.e. operational schemes) should be designed for fires exceeding 100MW which cannot be adequately controlled by the current technical system. It is also of utmost importance to update the ventilation strategy with scenarios where tunnel users are not able to evacuate downstream the fire. Concerning the causal factors related to the tunnel operator, the recommendations proposed can be summarized as follows:

- The interface design should be improved. The functional equipment is recommended to be presented in green color and only alarms should be depicted in a red state. Additionally, a combination of visual and audio alarms should be adopted since it may lead to a more reliable detection of disturbances.
- The detectability of critical events should be supported by the SCADA system. The CCTV should not be the only mean for presenting what is happening inside the tunnel.
- All irrelevant alarms should be disabled during an emergency. Incoming signals should be limited to only those which are important for handling the incident.
- The number of different tasks that the tunnel operators are requested to perform should be reduced. Groups of actions should be trigged by only one button.
- The level of information processing should be reduced by providing rule-based level of tasks rather than knowledge-based.
- The tunnel organization should ensure that all hardware and software is located in such a way that can be reached by the tunnel operators.

- The radio communication system should be fixed in order to broadcast in the same frequency with the emergency services. Moreover, the tunnel operators should communicate on a regular basis with the emergency services with the aim to facilitate the implementation of the response plans.
- The tunnel organization should define the senior operator, in case of conflicts in decision making occur.

Concerning the causal factors related to the tunnel users, the recommendations proposed can be summarized as follows:

- Information campaigns should be performed, covering the correct behaviour of road tunnel users not only in normal conditions (i.e. when approaching and driving through tunnels) but also in emergency situations (i.e. vehicles breakdowns and fires). It is also important before designing the campaign to evaluate the users' awareness and state of knowledge in order to identify knowledge gaps that should be managed.
- In case of an emergency, it is important to send a strong message so that the tunnel users become conscious of the necessity to evacuate the tunnel. For this reason, it is recommended to multiply the communication modes by combining visual (i.e. flashing lights) and sound messages. It is also important to use pre-recorded messages in order to avoid emotion or stress at the voice of the operator. Finally, it is highly recommended to check that these messages retain audible even when the fire ventilation mode is activated.
- When the tunnel users have reached the emergency exit, clear instructions must be given on what they should do. This may result to avoid returning to the tunnel to see what is happening.
- A permanent lighting above the emergency exits should be installed since it is believed that it enhances the evacuation process.
- The signaling of the emergency telephones should be improved.

Concerning the causal factors related to management, the recommendations proposed can be summarized as follows:

- The tunnel organization should design well-defined and measurable goals related to the availability and maintainability of the equipment (e.g. response times for repairing or replacing defective equipment), the time needed for patrollers to reach the tunnel in case of an emergency, the training of the tunnel personnel and the co-ordination with the emergency services.

- It is very important for the tunnel organization to conclude on the strategy for managing uncertainty, especially in relation to the tunnel operators. If the organization concludes that the tunnel operators should not be allowed to make their own decisions during an emergency, specific action rules should be proposed for all possible events. On the other hand, if the tunnel organization leaves considerable freedom to the operators, performance goals and process rules should be suggested.
- The recruitment of the appropriate personnel can be considered only if the tasks and roles in relation to the position are defined as precisely as possible.
- A detailed safety inspection should be performed that allows setting a reference point for upcoming period inspections.
- The responsibilities of the road patrollers in relation to the emergency services should be clearly defined.
- The road tunnel organization should provide a mechanism in order to incorporate findings from incidents, exercises and audits.
- A specific training program for the tunnel personnel should be provided.
- The minimum operating conditions under which the tunnel should be closed to traffic should be provided.

At this section some indicative recommendations have been given for the illustrative case study assessment. However, in a real life safety assessment recommendations should be made for **all the identified potential causal factors with the aim to ensure the correct enforcement of the safety constraints as much as possible**.

7 Conclusions

7.1 Comparing the proposed systems-theoretic method to current road tunnel QRAs

This thesis has attempted to answer the research question whether systems theory provides the foundation for creating a safety assessment that has the ability to identify causal factors that they have been left unnoticed by current road tunnel QRAs. In this section, a comparison of the proposed method to the current road tunnel QRAs is made.

7.1.1 Assessing safety or reliability?

Current road tunnel safety assessments methods (mainly based on the QRA modelling) assume that tunnel accidents are primary caused by component failures (e.g. fire detection system's failure, ventilation system's failure and human errors) which are usually assumed to be random events. In this perspective, the whole tunnel system is decoupled and reliability analysis techniques -such as fault tree and event tree analysis- are utilized in order to depict how an accident may occur. However, in road tunnels, accidents may also occur from components that satisfy their requirements, i.e. that they have not failed. In section 6.5.1 several causal factors have been identified in relation to the SCADA system many of which do not actually involve component failure events. Indeed, if the SCADA system has an inadequate control algorithm or an inadequate process model, **an accident may occur due to design inconsistencies not only due to random failure events**.

The point is that when historical reliability data are used in road tunnel QRAs, non-failure events (such as the identified control flaws) are not taken into consideration (figure 28). It must be kept in mind that safety and reliability are not the same properties since safety tends to have a broader scope of interest (Leveson 2012). Hence, the safety assessment should concentrate not only on failure events but also on unsafe scenarios in which none of the components has failed. The systems-theoretic method introduced in this thesis fulfills this requirement.

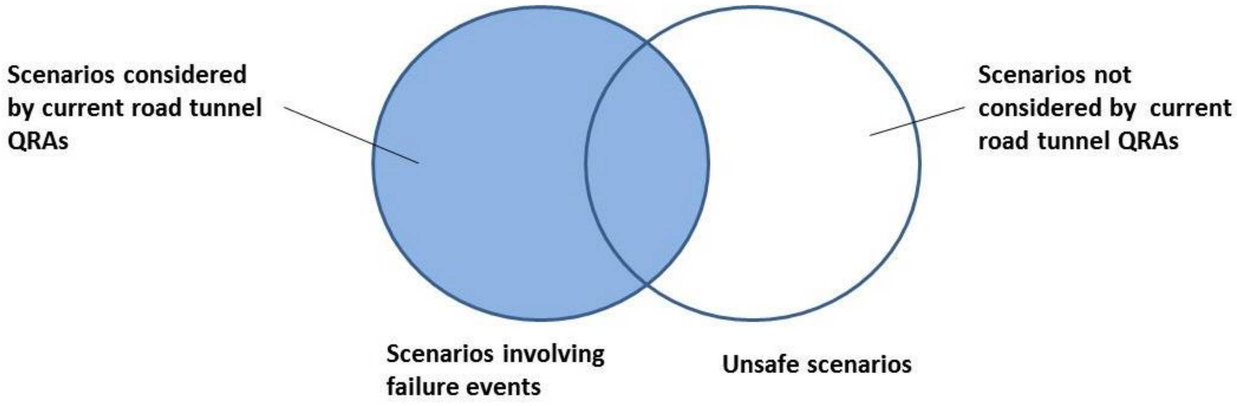

Scenarios considered by current road tunnel QRAs
Scenarios not considered by current road tunnel QRAs
Scenarios involving failure events
Unsafe scenarios

Figure 28: Scenarios that may lead to a tunnel accident

7.1.2 The role of the tunnel operator

The tunnel operator has a significant contribution to the overall tunnel safety. However, his role is underestimated by current QRAs which only reflect tunnel operators' performance variability in modelling input parameters such as: time to close the tunnel in case of an emergency and time to activate emergency ventilation. Because it is quite difficult to find a (proximal) event preceding the operator's behaviour, it is very usual in QRAs to use the label "operator's error" as a common explanatory factor. In this perspective, the underlying assumption is that tunnel operators "fail" just like mechanical components do. On the contrary, the systems-theoretic method builds on the ascertainment that the tunnel operator's performance is influenced by the environment -both physical and social- in which the actions take place. In particular, the method highlights the fact that operators use feedback mechanisms to update their mental model about what is happening inside the tunnel, therefore the method search for deficiencies in the human-machine interface. The method considers the ambient conditions of the working place, potential communication flaws, and moreover, the possible cognitive overload that may occur. All in all, rather than focusing on the results of the tunnel operators' behaviour (e.g. time to activate particular systems) the method attempts to capture the factors that may shape and determine potential unsafe actions.

7.1.3 The role of organizational aspects

As it has been discussed in paragraph 3.2.2, organizational aspects such as: (1) maintenance and inspection of the tunnel, (2) recruitment of the tunnel personnel and training procedures, (3) preparation of safety plans, (4) co-operation with the emergency services, and (5) analysis of past incidents and learning from events, are aspects that are recognized as major contributors in the occurrence of accidents. Nevertheless, current roads tunnels QRAs do not have a solid framework to consider such organizational factors. As a result, they concentrate mainly on the proximate events that may immediately precede a loss, neglecting the conditions that may have contributed to these proximate events. On the other hand, the proposed systems-theoretic method investigates several management deficiencies that may contribute to the accident's occurrence. In particular, the method search for organizational causal factors related to:

- Inadequate safety policy and goal setting.
- Inadequate assignment of control authority and responsibility.
- Inadequate design and implementation of safety plans.
- Inadequate modelling of safety performance.
- Inadequate adaptation to changes.

The aforementioned organizational causal factors are only indirectly related to the events that may lead to an accident. Nevertheless, they are critical in order to understand why/how an accident may occur.

7.1.4 The role of software behaviour

In current road tunnel QRAs the role of the software -embedded in the SCADA system- is totally omitted from the assessment. Indeed, the SCADA system's potential contribution to an accident is reflected into the potential failures of the equipment controlled by the SCADA system (i.e. ventilation, fire detection, etc.). In contrast, the systems-theoretic method is based on the assumption that the SCADA system's software may be unsafe when:

- Correctly implements the control algorithm but the specified behaviour may be unsafe from a system perspective (e.g. the SCADA system issues a forced ventilation strategy downstream the fire although users have not evacuated the tunnel).

- Does not specify some particular behaviour required for tunnel safety (e.g. does not provide a pre-programmed traffic management response for conceivable scenarios such as vehicle breakdowns and traffic congestions).

In paragraph 6.5.1 several causal factors (i.e. control flaws) have been identified with the aim to investigate why the SCADA system may contribute to an accident.

7.1.5 System's complexity and the dynamic nature of the tunnel system

Current road tunnel QRAs suffer from the limitation of considering only the proximate events that may lead to an accident and not the entire accident process. In addition, they examine the road tunnel system in a static view, implying that the tunnel equipment and the safety measures do not degrade over time. On the other hand, the proposed systems-theoretic method considers the processes involved in an accident. The method makes the whole tunnel system to become “alive” through the socio-technical safety control structure and takes into account all facets relating the organizational to the technical aspects. In this way the method attempts to consider the relationships between the parts of the tunnel system, how they interact and fit together. Furthermore, the method gives emphasis on the organizational feedback mechanisms (e.g. reporting schemes, safety audits, etc.) that should be enforced in order to identify the migration of the tunnel system to a state of increasing risk over time. In this manner, the degradation of the tunnel system over time can be detected.

7.1.6 Data and resources for the assessment

In order to perform a road tunnel QRA specific data is needed as input, since such an approach is usually based on calculating historical data-based probabilities. However, in the road tunnel field such kind of data (i.e. accident frequencies and reaction time of tunnel users and tunnel operators) is often either incomplete or subjected to a high degree of uncertainty. Apart from the lack of statistical data and the difficulty to calculate the probability of a tunnel accident to occurring, it is also very difficult to estimate the consequences of such accidents. It is hard to predict exactly how a fire may develop due to the numerous specific conditions that influence the situation (number and type of burning vehicles, location of fire, behaviour of tunnel users, time to activate appropriate actions, etc.). On the other hand, the systems-theoretic method concentrates mainly on the processes that may lead to an accident; therefore it is not affected by the lack (or the uncertainty) of data concerning the physical harm.

Nevertheless, the resources required to perform the systems-theoretic method are much more than those required by current road tunnel QRAs. Several aspects concerning the road tunnel infrastructure (e.g. the design of emergency telephones, emergency exits, etc.), the road tunnel organization (e.g. safety plans, recruitment, training and audits), the SCADA system's software design (e.g. control algorithm) and the displays of the tunnel operators should be thoroughly examined. For this reason, it is regarded that a safety assessment with the proposed systems-theoretic method will take much more time to be implemented.

7.1.7 The safety evaluation process

The results of any safety assessment method are inextricably linked to the overall philosophy and viewpoint of the method and its underlying accident model. Current road tunnel QRAs try to predict accident causation based on a nominal road tunnel operation and the potential deviations that may occur. Such deviations are represented mainly as failure events that may happen independently from each other. However, past experience has revealed that tunnel accidents seldom occur when the tunnel system is behaving normally. Indeed, they occur due to a confluence of events and causes that are often tightly related. For this reason, the systems-theoretic method assumes a worst-case scenario (i.e. a potential accident) and identifies the potential causal factors that could lead to that worst case. In this way -by trying to show how and why an accident *can* happen- the safety assessment considers a much more complete set of causal factors than those identified by current QRAs. However, it is crucial to highlight that when adopting the systems-theoretic perspective there is no way to quantify the probabilities of these causal factors. Therefore, the systems-theoretic method fails to provide an accurate estimation of the probability of the accident or a quantitative estimation of the risk level. In contrast to the safety evaluation process adopted by current road tunnel QRAs (e.g. comparing the estimated risk to an acceptable level), the safety evaluation process in this systems-theoretic perspective is based on concerning how the causal factors which have been identified during the assessment have been eliminated or controlled. Table 10 summarizes the comparison of current road tunnel QRAs to the systems-theoretic road tunnel safety assessment method.

	Current road tunnel QRAs	The systems-theoretic method
Assessing safety or reliability	Emphasize on failure events and reliability aspects.	Emphasize on unsafe scenarios, considering not only failure events but also design errors and unsafe interactions in the socio-technical system.
The role of the tunnel operator	Considers the results of the tunnel operator's performance (e.g. time to activate ventilations, etc.)	Considers why the tunnel operator may contribute to an accident.
The role of the organizational aspects	Does not consider organizational aspects.	Considers why organizational aspects may contribute to an accident.
The role of software behaviour	Does not consider the SCADA software behaviour.	Considers several control flaws that may occur.
System's complexity and its dynamic nature	Assumes that the tunnel system is static. Does not consider unsafe interactions among the tunnel system's components.	Assumes that the tunnel systems adapts over time. Considers the interactions that may occur in the sociotechnical system.
Data and resources	Is affected by the uncertainty in the data required for the assessment.	Is not affected by the uncertainty in the data since it does not focus on the physical process of the accident. However, it requests much more time and more data.
The safety evaluation process	Concentrates on the estimated risk number (i.e. expected number of fatalities).	Concentrates on how the potential causal factors have been handled.

Table 10: Comparison of the systems-theoretic method to current road tunnel QRAs

7.1.8 Defining risk in the proposed systems-theoretic perspective

As it has been discussed in section 3.1.2., there is no agreed definition for the concept of risk. Indeed, if one studies the literature he may find a number of different ways of understanding the risk concept. As far as the term "safety" is concerned, it is noted that although much research has been devoted to studies of safety, the concept of safety is in itself under-theorized. As a result, in most technical contexts safety is defined as the antonym of risk: the lower the risk, the higher the safety (Aven 2009). Taking into account that the systems-theoretic method does not focus on the combination of events, their consequences and their probabilities, it seems that a traditional safety (risk) assessment, based on probabilities and consequences estimates cannot be performed. A question that may arise therefore is how risk can be defined in this systems-theoretic perspective? To answer this question some of the prevailing definitions of the term risk are repeated. These are (Aven 2011b):

1. Risk=expected value of loss. For example, in current road tunnel QRAs risk is usually conceptualized by the expected number of fatalities.
2. Risk=the probability (frequentist or subjective) of an undesirable event. For example, the risk of a road tunnel under operation equals the probability of a fire.
3. Risk=the triplet (s_i, p_i, c_i), where s_i is the ith scenario, p_i is the probability of the ith scenario and c_i is the consequence of the ith scenario, i=1,2,…,N. Following this definition, the risk of a tunnel under operation equals the probability of a fire occurring (i.e. the examined scenario) and the expected consequences of this scenario (e.g. in terms of human losses or structural damage).
4. Risk=the combination of the two-dimensional combination of: (i) events A and the consequences of these events C, and (ii) the associated uncertainties U (will A occur and what value will C take?). In this perspective, the risk of a tunnel under operation is related to a fire in the tunnel (i.e. the event) that may lead to fatalities (i.e. the consequences of the event) and the associated uncertainties (i.e. what is the likelihood of the fire's occurrence) and what are the uncertainties associated with the number of fatalities.
5. Risk=Potential/Possibility of an accident to occur. In these terms, the risk of a tunnel under operation is related to the potential/possibility of a fire in a tunnel resulting in loss of human lives.

As mentioned before, the systems-theoretic method does not focus on the combination of events, their consequences and their probabilities; hence risk cannot be understood as described in definitions 1-4 above. On the contrary, risk in this systems-theoretic perspective is linked to the challenge of conceptualizing that an activity (i.e. a road tunnel under operation) could lead to outcomes that are not desired (i.e. fatalities and injuries). This concept has much in common with the definition 5 presented above. Taking into account that it is the effectiveness of the overall system to enforce the system level safety constraints that determines the potential/possibility of an accident to occur, it is deduced that **safety and risk are understood as functions of the effectiveness of the overall system to enforce the system level safety constraints.**

7.2 Thesis contribution

By adopting the systems-theoretic road tunnel safety assessment method, the goal is to "investigate" an accident before it occurs. Therefore, **the aim is to determine whether particular causal factors can emerge from the functioning of the whole tunnel system**. The method presented in this thesis succeeded in copying with several aspects that are not adequately handled by current road tunnel QRAs, briefly to:

1. Consider the entire socio-technical system and treat it as a whole by taking into account all facets relating the social to the technical aspects.
2. Consider the relationships between the parts of the system, how they interact and fit together.
3. Consider how the SCADA system's software behaviour may contribute to an accident in road tunnels.
4. The entire process of an accident has been examined and not just the proximate events.
5. The method has coped with the fact that the tunnel system is continually changing.

Therefore, it is believed that the systems-theoretic road tunnel safety assessment can be used as an "added value" complementary support tool for the safety assessment. In particular, analysts who perform road tunnel safety assessments can use the systems-theoretic method in order to investigate several aspects that may have been left unnoticed by current road tunnel QRAs. In this way, it is possible to supplement the quantitative part of their analysis with sophisticated qualitative tools. Furthermore, the EU Directive 2004/54 requests the opinion of an expert on road tunnel safety (e.g. a safety inspection entity) when a tunnel is under operation (EU 2004). For this purpose, the systems-theoretic method can be used to investigate the overall tunnel safety and determine improvements which should be made. Finally, the method can be used as a proactive safety audit for the safety officer in charge of the overall tunnel safety. By using the proposed method, the safety officer may identify several technical and organizational deficiencies that have the potential to lead to accidents.

In addition, this thesis has attempted to bridge the gap between two parallel trends in systemic safety approaches. In particular, the STAMP model which looks into control flaws processes and into problems in enforcing safety constraints has been enhanced with concepts adopted from a cybernetic model of organizational viability (i.e. VSM) in order to specify organizational aspects that might affect safety. The proposed joint STAMP-VSM framework relies on an extension of the control flaws of STAMP while maintaining the main underlying ideas of the model. Indeed, the proposed framework aspires to provide an insight on how safety management practices and organizational aspects may lead to inadequate enforcement of safety constraints despite best efforts and intentions of the operators involved. The framework can be used as a supplement to classic STAMP assessments or even as a standalone method that analyzes organizational influences. Although the joint framework has been used herein in the road tunnel safety field, it is believed that it can be tested in other safety domains.

7.3 Limitations

A critical question that may arise is whether the application of the systems-theoretic road tunnel safety assessment method can replace a road tunnel QRA. Road tunnel QRAs focus on the events that may precede an accident and on the physical harm that may occur. In this way, QRAs aim to evaluate the design and the technical facilities of a tunnel, i.e. whether they are adequate to control the potential physical harm. On the contrary, the systems-theoretic method concentrates on “internal aspects” of the safety management system, i.e. how the whole tunnel organization may inadequately enforce the system-level safety constraints. Design options such as the required capacity of the ventilation system and the distance between the emergency exits are not evaluated by this approach. Therefore, **it can be deduced that the systems-theoretic method can complement current road tunnel QRAs rather than replace them**.

Moreover, if risk should be quantified in accurate estimates (for example in order to represent the cost effectiveness of the safety measures) the systems-theoretic method will certainly fail to provide the required results. Risk in this systems-theoretic perspective is a qualitative property related to the effectiveness of the overall system to enforce the system-level safety constraints rather than quantitative estimates of events, their consequences and their probabilities.

7.4 Future Work

Examining other type of accidents

The systems-theoretic method has focused on the accident of a fire in the tunnel resulting in loss of human lives and/or serious injuries. However, future work should concentrate on analyzing other type of accidental events such as explosions, floods and collisions. Some of the safety-level constraints may differ, nonetheless, the safety control structure of the system and the steps for identifying the causal factors that may lead to the accident are exactly the same.

Extending the STAMP model at the human level

Likewise to organizational aspects (refer to chapter 5), the STAMP taxonomy of control flaws is somehow limited to understand the underlying mechanisms that may lead to the tunnel operator's "errors". Significantly, the systems-theoretic method (using concepts of the cognitive load model and the CREAM method) can capture much more contributory factors than current road tunnel QRAs. However, future work should aim to extend the STAMP control flaws in relation to other concepts from human factors analysis. For example, concepts found in the Human Factors Analysis and Classification System (HFCAS, Reason 1997) can be used in a joint framework with STAMP so as to enhance the explanatory power of how and why a tunnel accident may occur from causal factors at the human level.

Proposing criteria for the safety evaluation process

The safety evaluation process in the systems-theoretic method is based on examining how the identified causal factors have been handled in an examined road tunnel organization. If safety measures and procedures are inadequate to control the identified causal factors, recommendations for improvements should be made. However, this way of safety evaluation is somehow crispy. Therefore, research work should focus in this area in order to propose particular criteria when evaluating the overall tunnel safety performance.

Using the method for safety-guided design

The systems-theoretic method focuses on road tunnels under operation. Future work should concentrate on refining the method in order to provide a safety-guided tunnel design. Indeed, it is regarded better (and much more cost effective) to build safety into design rather than to simply add on safety equipment afterwards. The steps of a safety-guided design will be much similar to the steps of the systems-theoretic method presented in this thesis, for example:

1. Determine the system-level safety constraints that should be enforced.
2. Create a safety control structure and assign responsibilities for enforcing safety constraints.
3. Identify potentially inadequate control actions and determined what factors may lead to the inadequate enforcement of the safety constraints.

4. Evaluate the overall safety and refine the design (technical and organizational aspects) until the causal factors have been eliminated or controlled.

Creating safety indicators

As with every field of science, what needs to be measured has to be pertinent with what we want to know. Safety, however, is phenomenon that it is hard to describe and measure. Following this line of though, much work has been made in trying to establish proactive safety indicators of safety performance (Hale 2009; Woods 2009). Harms-Ringdal (2009) describes safety indicators as "*observable measures that provide insight into a concept - safety- that it is difficult to measure directly*". The challenge is that safety indicators are heavily dependent on the accident model that defines what can be expected to happen. If the underlying causes and contributing factors to accidents have been well defined, then it is possible to establish safety indicators that have the ability to: 1) monitor the level of safety and (2) indicate where and how to take action.

Taking into account that the proposed systems-theoretic method identifies causal factors that have the potential to lead to accidents, safety indicators can be introduced in order to detect the potential inadequate control well before the risk level increases and accidents occur. As presented in figure 29, inadequate control actions contributing to accidents indicate the existence of causal factors which can be used as a pool of perceived data for creating safety indicators. Considering the several causal factors which have been identified in section 6.5, future work should focus on creating leading safety indicators that can be used for the monitoring of the overall tunnel safety.

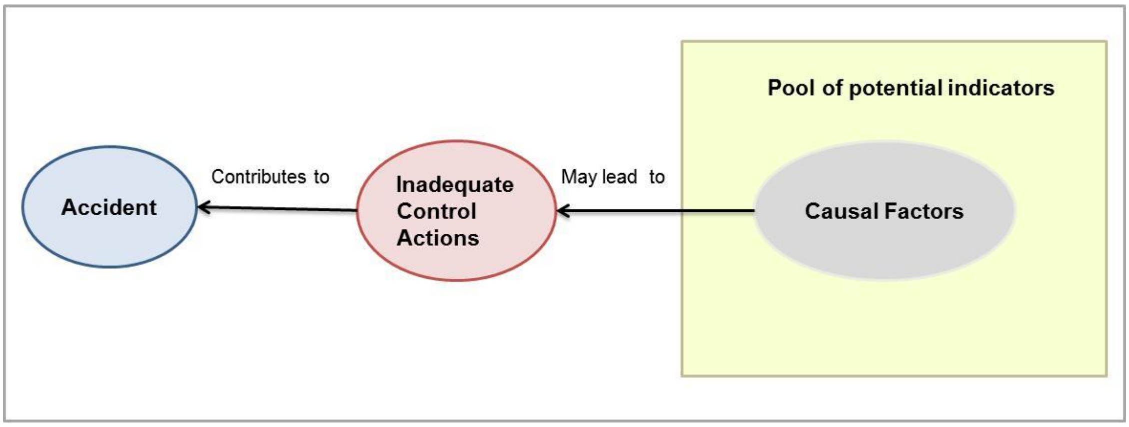


Figure 29: Creating safety indicators

Creating a road tunnel accident analysis method

The STAMP model has been widely used for accident analysis in order to determine the causal factors that have led to past accidents (refer for example to the analysis performed by Quyang et al. (2010)). In the road tunnels field, a framework to analyze accidents has not been proposed yet. Therefore, the STAMP and the joint STAMP-VSM framework can be used for this purpose. A systems-theoretic accident analysis method will have many common steps with the safety assessment method introduced in this thesis. In particular, these are:

1. Identify the hazards and the system-level safety constraints involved in the accident.
2. Document the safety control structure with entities which had the responsibility to enforce the safety constraints.
3. Determine the proximate events that led to the accident.
4. Analyze the accident at the operating level, i.e. identify with the STAMP the causal factors related to the tunnel operator and the SCADA system.
5. Moving up to the organizational level, identify with the joint STAMP-VSM framework how the management contributed to the accident.
6. Generate recommendations for avoiding a similar accident in the future.

References

Amundsen, F.H. 1994, 'Studies on traffic accidents in Norwegian road tunnels', *Tunnelling and Underground Space Technology,* vol. 9, pp. 9-15

Amundsen, F.H. & Ranes, G. 2000, 'Studies of driver behaviour in Norwegian road tunnels', *Tunnelling and Underground Space Technology,* vol. 15, pp. 3-11.

Apostolakis, G. 1990, 'The concept of probability in safety assessments of technological systems', *Science*, vol. 250, pp. 1359-1364.

Apostolakis, G. 2004, 'How useful is Quantitative Risk Assessment?', *Risk Analysis*, vol. 24, pp. 515-520.

Arends, B.J., Jonkman, S.N., Vrijling, J.K., Van Gelder, PHAJM. 2005, 'Evaluation of tunnel safety: Towards an economic safety optimum', *Reliability Engineering and System Safety,* vol. 90, pp. 217-228.

Argyris, C. & Schön, D.A. 1978, *Organizational Learning,* Addison-Wesley, Massachusetts.

Arralt, T.T. & Nilsen A.R. 2009, 'Automatic fire detection in road traffic tunnels', *Tunnelling and Underground Space Technology,* vol. 24, pp. 75-83.

Ashby, W.R. 1956, *An introduction to cybernetics*, Methuen, London.

Ale, B.J.M. 2002, 'Risk assessment practices in the Netherlands' *Safety Science*, vol.40, pp. 105-126.

Aven, T. 2003, *Foundations of risk analysis: a knowledge and decision oriented perspective*, Wiley, New York.

Aven, T. & Kristensen, V. 2005, 'Perspectives on risk: review and discussion of the basis for establishing a unified and holistic approach', *Reliability Engineering and System Safety,* vol. 90, pp. 1-14.

Aven, T. 2008, 'A semi-qualitative approach to risk analysis, as an alternative to QRAs', *Reliability Engineering and System Safety,* vol. 93, pp. 768-775.

Aven, T. 2009, 'Safety is the antonym of risk for some perspectives of risk', S*afety Science,* vol. 47, pp. 925-930.

Aven, T. 2010, 'On how to define, understand and describe risk', *Reliability Engineering and System Safety,* vol. 95, pp. 623-631.

Aven, T. 2011a, 'On the new ISO guide on risk management terminology', *Reliability Engineering and System Safety,* vol. 96, pp. 719-726.

Aven, T. 2011b, 'A risk concept applicable for both probabilistic and non-probabilistic perspectives', S*afety Science,* vol. 49, pp. 1080-1086.

Aven, T & Zio, E. 2011, 'Some considerations on the treatment of uncertainties in risk assessment for practical decision making', *Reliability Engineering and System Safety,* vol. 96, pp. 64-74.

Aven, T. 2012, 'The risk concept-historical and recent development trends', *Reliability Engineering and System Safety,* vol. 99, pp. 33-44.

Aven, T. & Reniers, G. 2013, 'How to define and interpret a probability in a risk and safety setting', *Safety Science*, vol. 51, pp. 223-231.

Bainbridge, L. 1987, 'Ironies of automation', in *New Technology and Human Error, eds* Rasmussen, J., Duncan, K. & Leplat, J., Wiley, pp. 271-283.

Becker, M. 2005, 'The concept of routines: some clarifications', *Cambridge Journal of Economics,* vol. 29, pp. 249-262.

Beard, A.N. 2005, 'Problems with using models for fire safety', in *The Handbook of Tunnel Fire Safety*, eds Beard, A. & Carvel, R., Thomas Telford, London, pp. 299-317.

Beard, A.N. & Cope, D. 2008, 'Assessment of the Safety of Tunnels'. Commissioned by the European Parliament; Report IP/A/STOA/FWC/2005-28/SC22/29. Published in February 2008 on the European Parliament web-site under the rubric 'Science and Technology Options Assessment' (STOA).

Beer, S. 1985, *Diagnosing the System for Organizations* Wiley, Chichester.

Bendelius, A. 2005, 'Tunnel ventilation-state of the art', in *The Handbook of Tunnel Fire Safety*, eds Beard, A. & Carvel, R., Thomas Telford, London, pp. 127-143.

Bier, V. 1999, 'Challenges to the acceptance of probabilistic risk analysis', *Risk Analysis,* vol. 19, pp. 703-710.

Bjelland, H. & Aven, T. 2013, 'Treatment of uncertainty in risk assessments in the Rogfast road tunnel project', *Safety Science,* vol. 55, pp. 34-44.

Brussard, LA., Kruskamp, MM.& Essink, M.P. 2001, 'The Dutch model for the quantitative risk analysis of road tunnels', *Proceedings of European Safety and Reliability Conference 2010 (ESREL 2001)*, Italy.

Bubbico, R., Cave S., Mazzarotta, B. & Silvetti, B. 2009, 'Preliminary study on the transport of hazardous materials through tunnels', *Accident Analysis and Prevention*, vol. 41, pp. 1199-1205.

Carvel, R. & Marlair, G. 2005, 'A history of fire incidents in tunnels', in *The Handbook of Tunnel Fire Safety*, eds Beard, A. & Carvel, R., Thomas Telford, London, pp. 4-41.

Carvel, R. 2009, 'Ventilation and suppression systems in road tunnels: some issues regarding their appropriate use in a fire emergency', *Proceedings of the second International Tunnel Safety Forum for road and rail*, Tunnel Management International, pp.375-382.

Centre d'Etudes des Tunnels (CETU), 2005, *Guide to road tunnel safety documentation, Booklet 4, Specific Hazard Investigation*, France.

Checkland, P. 1981, *Systems Thinking, Systems Practice,* John Wiley & Sons, New York.

Christensen, F.M., Andersen, O., Duijm N.J. & Harremoes, P. 2003, 'Risk terminology-a platform for common understanding and better communication', *Journal of Hazardous Materials*, vol. 103, pp.181-203.

Davoudian, K., Wu, J & Apolostolakis, G. 1994, 'The Work Process Analysis Model (WPAM)', *Reliability Engineering and System Safety*, vol. 45, pp. 107-125.

Dekker, S.W.A. 2011, Drift into failure: from hunting broken components to understanding complex systems, Ashgate Publishing, UK.

Dianous, V. & Fiévez, C., 2006, 'ARAMIS project: A more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barriers performance', *Journal of Hazardous Materials*, vol. 130, pp. 220-233.

Dijkstra, A. 2007, 'Cybernetics and Resilience Engineering: Can Cybernetics and the Viable System Model Advance Resilience Engineering?' *Proceedings of the Resilience Engineering Workshop*, Sweden.

Dix, A. 2011. *Expert report for the Victorian Cooner,* Available from: http://www.arnolddix.com/library [2 May 2013].

Dubois, D. 2010, 'Representation, propagation and decision issues in risk analysis under incomplete probabilistic information', *Risk Analysis*, vol. 30, pp. 361-368.

Duijm, N. & Goosens, L. 2006, 'Quantifying the influence of safety management on the reliability of safety barriers', *Journal of Hazardous Materials*, vol. 130, pp. 284-292.

EU Directive 2004/54/EC. 2004. Directive 2004/54/EC of the European Parliament and of the Council on minimum safety requirements for tunnels in the Trans-European Road Network. European Commission, Directorate-General for Energy and Transport, Brussels.

European Federation for Transport & Environment (T&E)/European Transport Safety Council (ETSC). 2003, *Position paper on tunnel safety requirements*, Available from: http://www.etsc.eu/oldsite/pre_20june03.pdf [2 May 2013].

Fabiano B., Curro, F., Reverberi, A.P. & Rastorino B. 2005, 'Dangerous goods transportation by road: from risk analysis to emergency planning', *Journal of Loss Prevention in the Process Industries,* vol. 18, pp. 403-413.

French, S., Bedford, T., Pollard, J.T. & Soane E. 2011, 'Human reliability analysis: A critique and review for managers', *Safety Science*, vol. 49, pp. 753-763.

Garret, C. & Apostolakis, G. 1999, ‘Context in the risk assessment of digital system’, *Risk Analysis*, vol. 19, pp. 23-32.

Goh, Y.M., Brown, H. & Spickett, J. 2010, ‘Applying systems thinking concepts in the analysis of major incidents and safety culture’, *Safety Science*, vol. 48, pp. 302-309.

Grote, G. 2008, ‘Diagnosis of safety culture: A replication and extension towards assessing “safe” organizational change processes’, *Safety Science*, vol. 46, pp. 450-460.

Grote, G. 2009, *Management of Uncertainty – Theory and Application in the Design of Systems and Organizations*, Springer, London.

Grote, G. 2012, ‘Safety management in different high-risk domains- All the same?’, *Safety Science*, vol. 50, pp. 1983-1992.

Guanquan, C. & Jinhui W. 2012, ‘Study on probability distribution of fire scenarios in risk assessment to emergency evacuation’, *Reliability Engineering and System Safety*, vol. 99, pp. 24-32.

Haack, A. 2002, ‘Current safety issues in traffic tunnels’, *Tunnelling and Underground Space Technology*, vol. 17, pp. 117-127.

Hale, A.R. & Swuste, P. 1998, ‘Safety rules: procedural freedom or action constraint?, *Safety Science*, vol. *29*, pp. 163–177.

Hale, A. 2009, ‘Why safety performance indicators?’, Safety Science, vol. 47, pp. 479-480.

Hale A. & Borys D. 2012a, ‘Working to rule or working safely? Part 1: A state of the art review’, *Safety Science*, vol. 55, pp. 207-221.

Hale A. & Borys D. 2012b, ‘Working to rule or working safely? Part 2:The management of safety rules’, *Safety Science*, vol. 55, pp. 222-231.

Harms-Ringdal, L. 2009, ‘Dimensions in safety indicators’, *Safety Science*, vol. 47, pp. 481-482.

Holicky, M. 2009, ‘Probabilistic risk optimization of road tunnels’, *Structural Safety*, vol. 21, pp. 260-266*.*

Hollnagel E. 1998, *Cognitive reliability and error analysis method (CREAM)*, Elsevier Science Ltd, Amsterdam.

Hollnagel E. 2004, *Barriers and accident prevention*. Ashgate Publishing Limited, England.

Hollnagel, E. Woods, D. & Leveson, N. 2006, *Resilience engineering: Concepts and precepts.*, Ashgate, UK.

Hollnagel, E. 2012, ‘Coping with complexity: Past, present and future’, *Cognition, Technology and Work*, vol. 14, pp. 199-205.

Hoj, N.P. & Kröger, W. 2002, ‘Risk Analyses of transportation on road and railway from a European Perspective’, *Safety Science*, vol. 40, pp. 337-357.

Hopkins, A. 2009, ‘Thinking about process safety indicators’, *Safety Science*, vol. 47, pp. 460–465.

Hoverstadt, P. 2008, *The Fractal Organization: Creating Sustainable Organizations with the Viable System Model*, John Wiley, Chichester.

Ignason, H. 2005, ‘Fire dynamics in tunnels’, in *The Handbook of Tunnel Fire Safety*, eds Beard, A. & Carvel, R., Thomas Telford, London, pp. 231-263.

Ignason, H. & Wickstrom U. 2006, ‘The international FORUM of fire research directors: A position paper on future actions for improving road tunnel fire safety’, *Fire Safety Journal*, vol. 41, pp. 111-114.

Ignason, H. 2008, ‘Magic numbers in tunnel fire safety’, *Proceedings of the third International Symposium on Tunnel Safety and Security*, Sweden.

INERIS. 2005, *Transport of Dangerous goods through road tunnels Quantitative Risk Assessment Model (v. 3.60 and v. 3.61) Reference Manual*, Verneuil-en-Halatte, France.

ITA. 2011, *Updated survey of existing regulations and recognised recommendations (operation and safety of road tunnels),* Available from: http://www.ita-aites.org/fileadmin/filemounts/general/pdf/ItaAssociation/ProductAndPublication/Commitees/ITA_COSUF/Updated_Survey_Road_Tunnel_Regulations_August_2011.pdf [2 May 2013].

ITA-PIARC. 2004, *Fire safety in tunnels,* Available from: http://www.piarc.org/en/log-in.htm?path=/ressources/publications/3/5445,RR324-007.pdf [2 May 2013].

Kazaras, K., Konstandinidou M., Nivolianitou, Z. & Kirytopoulos, K. 2013, ‘Enhancing road tunnel risk assessment with a fuzzy system based on the CREAM methodology’, *Chemical Engineering Transactions,* vol. 31.

Kazaras, K., Kirytopoulos, K. & Rentizelas, A. 2012, ‘Introducing the STAMP method in road tunnel safety assessment’, *Safety Science,* vol. 50, pp. 1806-1817.

Kaplan, S. & Garrick, B. 1981, ‘On the quantitative definition of risk’, *Risk Analysis*, vol. 1, pp. 11–28.

Kaplan, S. 1997, ‘The words of risk analysis’, *Risk Analysis*, vol. 17, pp. 407-417.

Khan, F. 2008, ‘Preface: Human factors special issue’, *Journal of Loss Prevention in the Process Industries*, vol. 21, pp. 225-226.

Khury, G.A. 2003, ‘EU tunnel fire safety action’, *Tunnels and Tunnelling International,* pp. 20-23.

Kirytopoulos, K., Rentizelas, A., Kazaras, K. & Tatsiopoulos, I. 2010, ‘Quantitative operational risk analysis for dangerous goods transportation through cut and over road tunnels', *Proceedings of European Safety and Reliability Conference 2010 (ESREL 2010)*, eds. Ale, B. Papazoglu, I. & Zio, E., Taylor & Francis, Greece.

Kirytopoulos, K., Rentizelas A., Tatsiopoulos, I. & Papadopoulos, G. 2010, 'Quantitative risk analysis for road tunnels complying with EU regulations', *Journal of Risk Research*, vol. 13, pp. 1027-1041.

Kirytopoulos, K. & Kazaras, K. 2011. 'The need for a new approach in road tunnels risk analysis', *Proceedings of European Safety and Reliability Conference 2011 (ESREL 2011*), eds. Berenguer, C.,Grall, A. & Soares, CRP Press, France.

Kontogiannis, T. 2010, 'A contemporary view of organizational safety: variability and interactions of organizational processes', *Cognition and Technology*, vol. 12, pp. 231-249.

Kontogiannis, T. & Malakis, S. 2011, 'A systemic Analysis of Patterns of Organizational Breakdowns in Accidents: A Case from Helicopter Emergency Medical Services Operations', *Reliability Engineering and System Safety,* vol. 99, pp. 193-208.

Kontogiannis, T. 2012, 'Modelling patterns of breakdown (or archetypes) of human and organizational processes in accidents using system dynamics', *Safety Science* vol. 50, pp. 931-944.

Lacroix, D. 2001, 'The Mont Blanc Tunnel fire: what has happened and what has been learned', *Proceedings of the fourth International Conference on Safety in Road and Rail Tunnels*, Madrid, pp. 3-16. .

Larsson, P., Dekker, W.A. & Tingvall C. 2009, 'The need for a systems theory approach to road safety', *Safety Science*, vol. 48, pp. 1167-1174.

Leitch, M. 2010, 'ISO 31000:2009-The new international standard on risk management', *Risk Analysis*, vol. 30, pp. 887-892.

Leitner, A. 2001, 'The fire catastrophe in the Tauern tunnel: Experience and conclusions for the Austrian guidelines', *Tunnelling and Underground Space Technology,* vol. 16, pp. 217-223.

Leplat J.1987, 'Occupational accident research and systems approach', in *New Technology and Human Error*, eds. Rasmussen J., Duncan K. & Leplat, J. John Wiley, New York.

Leveson, N.G. 2004, 'A new accident model for engineering safer systems', *Safety Science*, vol. 42, pp. 237–270.

Leveson, N.G., 2011, 'Applying systems thinking to analyze and learn from events', *Safety Science*, vol. 49, pp. 55-64.

Leveson, N.G., 2012, *Engineering a safer world: Systems Thinking Applied to Safety,* MIT Press, Cambridge, MA.

Lindley, DV. 2006, 'The philosophy of statistics', *The Statistician*, vol. 49, pp. 293-337.

Lundberg, J., Rollenhagen C. & Hollnagel, E. 2009, 'What you look for is what you find-The consequences of underlying accident models in eight accident investigation manuals', *Safety Science*, vol. 47, pp. 1297-1311.

Marais, K., Saleh J. & Leveson N.G. 2006, 'Archetypes for organizational safety', *Safety Science*, vol. 44, pp. 565-582.

Melchers, R.E. 2001, 'On the ALARP approach to risk management', *Reliability Engineering and System Safety,* vol. 71, pp. 201-208.

Meng, Q., Qu, X., Wang, X., Yuantita, V. & Wong, S. 2011, 'Quantitative Risk Assessment for Nonhomogeneous Urban Road Tunnels', *Risk Analysis*, vol. 31, pp. 382-403.

Meng, Q. & Qu., X. 2012, 'Uncertainty propagation in quantitative risk assessment modelling for fire in road tunnels', *IEEE Transactions on Systems, Man and Cybernetics Part C: Application and Reviews,* vol. 42, pp. 1454-1464.

Ministry of the Interior. 1999, *Report of the Mont Blanc tunnel fire*, Available from: http://www.firetactics.com/MONTBLANCFIRE1999.htm [2 May 2013].

Mohaghegh, Z. & Mosleh. A. 2009, 'Incorporating organizational factors into probabilistic risk assessment of complex socio-technical systems: Principles and theoretical foundations', *Safety Science*, vol. 47, pp. 1139–1158.

Mohaghegh, Z., Kazemi R. & Mosleh. A. 2009, 'Incorporating organizational factors into probabilistic risk assessment of complex socio-technical systems: A hydric technique formalization', *Reliability Engineering and System Safety*, vol. 94, pp. 1000–1018.

Moizés, M., Marcello, J., Mario S., Cesar, R., Vidal P. & Paulo Victor R. 2011, 'Overcoming the blame game to learn from major accidents: A systemic analysis of an Anhydrous Ammonia leakage accident', *Journal of Loss Prevention in the Process Industries,* vol. 25, pp. 33-39.

Moller, N. & Hansson, S.O. 2008, 'Principles of engineering safety: Risk and uncertainty reduction', *Reliability Engineering and System Safety,* vol. 93, pp. 776-783.

Nathanael, D. & Marmaras, N. 2008, 'On the development of work practices: a constructivist model', *Theoretical Issues in Ergonomic Science*, vol. 9, pp. 359-382.

Neerincx, M. 2003, 'Cognitive task load design: model, methods and examples', in *Handbook of Cognitive Task Design,* eds. Hollnagel E., Mahwah, NJ: Lawrence Erlbaum Associates, pp. 283-305.

Nilsson, D., Johansson, M. & Frantzich H. 2009, 'Evacuation experiment in a road tunnel: A study of human behaviour and technical installations'. *Fire Safety Journal*, vol. 44, pp. 458-468.

Nivolianitou, Z.S., Leopoulos, V.N. & Konstantinidou M. 2004, ‘Comparison of techniques for accident scenario analysis in hazardous systems’, *Journal of Loss Prevention in the Process Industries,* vol. 17, pp. 467-475.

Noizet, A.S., Dedale, A., Richard, F. 2003, ‘ACTEURS: Improving understanding of road tunnel users with view to enhancing safety’, *Proceeding of the fifth International Conference Safety in Road and Rail Tunnels*, France.

Nývlt, O., Prívara, S. & Ferkl, L. 2011, ‘Probabilistic risk assessment of highway tunnels’, *Tunnelling and Underground Space Technology*, vol. 26, pp. 71-82.

OECD. 2001. *Safety in tunnels – Transport of dangerous goods through road tunnels*, Organization for Economic Co-operation and Development - OECD Publications, Paris.

Papaioannou, P. & Georgiou, G., 2003, ‘Human behaviour in tunnel accidents and incidents: end users, operators and response teams’, Report of European Project UPTUN, No. GRD1-2001-40739.

Papazoglou, I., Bellamy, L., Hale, A., Aneziris, O., Ale, B., Post, J. & Oh, J., 2003, ‘I-Risk: development of an integrated technical and management risk methodology for chemical installations’, *Journal of Loss Prevention in the Process Industries*, vol. 16, pp. 575-591.

Pate-Cornell, E. & Murphy*,* D. 1996, ‘Human and management factors in probabilistic risk analysis: the SAM approach and observations from recent applications’, *Reliability Engineering and System Safety*, vol. 53, pp. 115-126.

Perrow, C. 1984, *Normal Accidents: Living with High-Risk Technology.* Basic Books, New York.

Persson M. 2002, *Quantitative Risk Analysis Procedure for the Fire Evacuation of a road tunnel-An Illustrative Example*, Report 5096, Lund University, Sweeden.

PIARC. 2004, *Cross Section Geometry in Unidirectional Tunnels* (PIARC), France.

PIARC. 2007a, *Integrated Approach to Road Tunnel Safety*, World Road Association (PIARC), France.

PIARC. 2007b, *Systems and equipment for fire and smoke control in road tunnels*, World Road Association (PIARC), France.

PIARC. 2008a, *Risk analysis for road tunnels,* World Road Association (PIARC), France.

PIARC. 2008b, *Human factors and road tunnel safety regarding users,* World Road Association (PIARC), France.

PIARC. 2011, *Road tunnels: operational strategies for emergency ventilation*, World Road Association (PIARC), France.

PIARC. 2013, *Risk evaluation, current practice for risk evaluation for road tunnels*, World Road Association (PIARC), France.

Purdy, G. 2010, 'ISO 31000:2009-setting a new standard for risk management', *Risk Analysis*, vol. 30, pp. 881-886.

Quyang, M., Hong, L., Yu, M. & Fei, Q., 2010, 'STAMP-based analysis on the railway accident and accident spreading: Taking the China-Jiaoji railway accident for example', *Safety Science*, vol. 48, pp. 544-555.

Rasmussen, J.,1997, 'Risk Management in a dynamic society: A modelling problem', *Safety Science*, vol. 27, pp. 183-213.

Reason, J., 1997, *Managing the risks of organizational accidents*, Ashgate Publishing Ltd , Aldershot Hants.

Renn, O. 1998, 'Three decades of risk research: accomplishments and new challenges', *Journal of risk research,* vol. 1, pp. 49-71.

Roberts K.H.1990, 'Some characteristics of one type of high reliability organization', *Organization Science*, vol. 1, pp. 160–76.

Ronchi, E., Colanna, P. & Berloco. N. 2013, 'Reviewing Italian Fire Safety Codes for the analysis of road tunnel evacuation: Advantages and limitations of using evacuation models', *Safety Science,* vol. 52, pp. 28-36.

Rosa, EA. 2010, 'The logical status of risk- to burnish or to dull', *Journal of Risk Research,* vol. 13, pp. 239-253.

Saccomanno, F. & Haastrup, P. 2002, 'Influence of safety measures on the risks of transporting dangerous goods through road tunnels', *Risk Analysis*, vol. 22, pp. 1059-1069.

Saleh, J.H. Marais, K.B. Bakolas E. & Cowlagi, R.V. 2010, 'Highlights from the literature on accident causation and system safety: Review of major ideas, resent contribution and challenge', *Reliability Engineering and System Safety*, vol. 95, pp. 1105-1116.

Salmon P., Cornelissen M. & Trotter M. 2012, 'Systems-based accident analysis methods: A comparison of Accimap, HFCS, and STAMP', *Safety Science*, vol. 2012, pp. 1158-1170.

Santos-Reyes, J. & Beard, A. 2002, 'Assessing safety management systems', *Journal of Loss Prevention in the Process Industries*, vol. 15, pp. 77–95.

Santos-Reyes, J. & Beard, A. 2008, 'A systemic approach to managing safety', *Journal of Loss Prevention in the Process Industries,* vol. 21, pp. 15–28.

Santos-Reyes, J. & Beard, A. 2009, 'A systemic analysis of the Edge Hill railway accident', *Accident Analysis and Prevention,* vol. 41, pp. 1133–1144.

Schubert M., Hoj, P., Ragnoy A. & Bulvik, H. 2012, ‘Risk Assessment of Road Tunnels using Bayesian Networks’, *Procedia-Social and Behavioural Sciences* vol. 48, pp. 2697-2706.

Singpurwala, N. 2006, *Reliability and Risk. A Bayesian Perspective*. Wiley, New York.

Skytter, L. 2005, *General systems theory problems-perspective-practice*, World Scientific Publishing Co, Singapore.

Svedung, I. & Rasmussen J. 2002, ‘Graphic representation of accident scenarios: mapping system structure and the causation of accidents’, *Safety Science,* vol. 40, pp. 397–417.

Turner, B. A. & Pidgeon, N. F. 1997, *Man-made disasters, 2ndEdition*, Butterworth-Heineman, London.

UNECE. 2001, *Recommendations of the group of experts on safety in road tunnels,* Available from: http://www.unece.org/fileadmin/DAM/trans/doc/2002/ac7/TRANS-AC7-09e.pdf [2 May 2013].

U.S. Department of Transportation Federal Highway Administration. 2009, *Technical Manual for Design and Construction of Road Tunnels-Civil Elements,* National Highway Institute, US.

Vaughan D. 1996, *The Challenger launch decision: Risky technology, culture and deviance at NASA,* University of Chicago Press, Chicago.

Vicente, K.J. 1999, *Cognitive work analysis: Toward safe, productive, and healthy computer-based work*, Lawrence Erlbaum Associates, New York.

Weger, D., Kruiskamp, M & Hoeksma, J., 2001, ‘Road tunnel risk assessment in the Netherlands-TUNprim: a spreadsheet model for the calculation of the risks in road tunnels’. *Proceedings of International Conference in Safety and Reliability*, ed. Piccinni, Torino.

Woods D.D. 2009, ‘Escaping failures of foresight’, *Safety Science*, vol. 47, pp. 498-501.

Woods, D., Dekker, S., Cook, R., Johannesen, L. & Sarter, N. 2010, *Behind Human Error*, second edition. Asghate Publishing Limited, England.

Zarboutis, N. & Marmaras N. 2007, ‘Designing of formative evacuation plans using agent-based simulation’, *Safety Science*, vol. 45, pp. 920-930.

Zhuang, M., Chun-fu, S. & Sheng-rui, Z. 2009, ‘Characteristics of traffic accidents in Chinese freeway tunnels’, *Tunnelling and Underground Space Technology*, vol. 24, pp. 350-355.

Zio, E. 2009, ‘Reliability engineering: Old problems and new challenges’, *Reliability Engineering and System Safety,* vol. 94, pp. 125-141.