Title page information

Title: STAMP-based technique as an alternative method for road tunnel safety risk assessment.

Authors: Konstantinos Kazaras[a], Konstantinos Kirytopoulos[a], Athanasios Rentizelas[a]

[a]National Technical University of Athens, Mechanical Engineering School, Sector of Industrial Management and Operational Research, Zografou Campus, Iroon Polytexneiou 9, 15780, Zografou, Greece.

Email addresses: kkaz@central.ntua.gr (K.Kazaras), kkir@mail.ntua.gr (K.Kirytopoulos), arent@central.ntua.gr (A.Rentizelas)

Corresponding Author-Contact Details: Konstantinos Kazaras, kkazaras@gmail.com, Zografou Campus, Iroon Polytexneiou 9, 15780, Zografou, Greece Tel. 0030 210 7723575.

STAMP-based technique as an alternative method for road tunnel safety risk assessment.

Abstract

After the tremendous accidents in European road tunnels over the past decade, many safety assessment methods have been proposed worldwide, most of them based on Quantitative Risk Assessment (QRA). However, QRAs based on causal chains and event modeling (i.e. fault and event trees), have been subject to strong criticism for their limitations to capture the overall risk picture of complex socio-technical systems. In such systems, human and organizational factors, software errors, design flaws and the safety culture of the system are not efficiently handled by the current QRA methods and systemic accident models have been proposed as an alternative approach to better understand and manage safety. The aim of this work is to overview the limitations of current QRAs in the road tunnels field, and to introduce a STAMP-based technique as an alternative method for establishing a proactive safety strategy and evaluating the overall safety of these critical infrastructures, with the objective to overcome the QRAs limitations. The STAMP method is applied to a case study analysis in the safety critical process of tunnel ventilation during an emergency.

Keywords: Road Tunnel; Safety; Risk Assessment; STAMP; Quantitative Risk Assessment

1 Introduction

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. Even if accident rates appear to be slightly lower in tunnels than on open road, an accident in a tunnel may have much greater impact (Beard and Cope, 2008). The consequences can be extremely destructive and dangerous, especially in the event of fire, since the enclosed space hinders the dissipation of smoke and poses difficulty in ensuring safe escape route of the tunnel users. Furthermore, except for human losses and injuries, accidents in road tunnels can also result in considerable financial losses and prejudicial consequences for the tunnel manager. As a result, tunnel safety is now considered as being one of the key elements in tunnel design, development and operation.

Indeed, it was the spate of tunnel fires in Europe over the past decade, resulting in many human and financial losses that highlighted safety in road tunnels 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, and forced the European Commission to embark upon a major review of road tunnel safety (Beard and Cope, 2008). In this context, the European Commission launched the Directive 2004/54/EC that sets minimum safety requirements and suggests, apart from the measures imposed based on parameters such as the tunnel length and the traffic volume, the implementation of a safety risk assessment in several cases. This is a remarkable aspect about this Directive because it combines both a "guideline-oriented" and a "risk-oriented" approach. However, the EU Directive (2004) does not indicate neither the method for performing the safety risk assessment nor the criteria for risk acceptance**.** Consequently, a wide range of methods have been proposed and applied, most of them based on Quantitative Risk Assessment (QRA; Piarc, 2008a).

Although QRA contribution to manage safety has been indisputably great in many fields, such as the nuclear power industry (where it is called Probabilistic Risk Assessment-PRA), QRAs based on causal chains and event modeling (i.e. fault and event trees), have been subject to strong criticism for their limitations to capture the overall risk picture of complex socio-technical systems (Rasmussen, 1997; Hollnagel, 2004; Leveson, 2004). In such systems, even proponents of QRAs argue that human and organizational factors, software errors, design flaws and the safety culture of the system are not efficiently handled by the currently existing QRA methods (Apostolakis, 2004; Bier, 1999). 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, 2007), it is open to question whether QRA, with the aforementioned limitations, is the appropriate tool to investigate potential risks and evaluate the overall safety level of these infrastructures. Khoury (2005) makes his point clear: "Current road tunnel safety is seriously limited by the traditional approach to risk assessment". Furthermore, Beard (2010) stresses the need for a more "systemic" safety risk assessment method in the road tunnels field and particularly writes: "Fatality, injury and harm result from the working of the whole tunnel system. Safety risk assessment, therefore, needs to be as 'systemic' as possible. The question is how do we do this?".

In other hazardous socio-technical systems in society, systems-theoretical assumptions are considered a promising way to better understand and manage safety (Larsson et al., 2009). In aerospace, aviation, process industry and maritime, systemic accident models that view accidents as emergent phenomena arising due to the complex interactions among components of the whole socio-technical system are currently used for the safety assessment process (Hollnagel, 2004). In this perspective, safety is viewed as a control problem (i.e. inadequacy to enforce safety constraints) and accidents are regarded to occur when component failures, external disturbances and dysfunctional interactions among system components are not adequately handled by the safety control system (Leveson, 2004). Two notable systemic accident models that have been proposed are Rasmussen's (1997) hierarchical socio-technical

framework and Leveson's (2004) Systems-Theoretic Accident Model and Processes (STAMP).

This article's objective is twofold. The first objective is to examine whether the QRA modeling is indeed the best suited method to perform safety assessment of road tunnels. Nevertheless, to manage risk it is necessary to understand how accidents happen and in order to do this the use of an appropriate model of accident causation is critical. Having reviewed the inadequacy of the sequential accident models of QRAs, the second objective is to propose an alternative approach based on a different foundation. Thus, in this paper we introduce and present the utilization of the STAMP accident model as an alternative approach for the safety assessment process of these infrastructures. The use of the STAMP model for safety risk assessment in road tunnels is an innovative concept of this work. The STAMP-based road tunnel safety risk assessment method characteristics and advantages are thoroughly presented through a case study.

The remainder of this work is organized as follows. In Section 2 the concept of QRA is briefly presented and the limitations of this method in the road tunnels field are reviewed. In section 3 the need for a new approach based on systems theory is pinpointed. Section 4 introduces the STAMP model in the road tunnels field as an alternative approach. To demonstrate the STAMP-based road tunnel safety risk assessment method, an illustrative example of a STAMP analysis in the safety critical process of tunnel ventilation during an emergency is provided. In Section 5 the proposed method is discussed and its limitations are analyzed. Finally, Section 6 presents the concluding remarks of this work.

2. Reviewing limitations of QRA in road tunnels

2.1. The concept of QRA in the road tunnel field

QRA methods have been adapted to the road tunnels field in order to cope with the limitations of prescriptive standards and regulations that traditionally and globally have controlled the safety issue (Beard and Cope, 2008; Dix, 2004; Piarc, 2008a). Such regulations and standards, even if they manage to ensure a minimum level of safety, they are implemented more or less without taking into account the individual characteristics of a tunnel, or the interactions among different parts of the tunnel system such as the infrastructure, technical systems and operational procedures (Piarc, 2008a). As a result, a risk-based safety assessment approach is also needed so as to provide a structured and transparent assessment of risks for each particular tunnel. In this perspective, the concept of tunnel's QRA methods is to calculate and evaluate the risk level of a road tunnel and then determine whether the desired safety level has been accomplished.

The risk is defined by two aspects: the occurrence probability of an event and the consequences of that particular event. The Quantitative Risk Assessment is based on an inventory of all possible accident scenarios. Event and fault trees are employed to identify sequences of events that start with a set of disturbances to the normal operation (i.e. initiating events) and end at a set of undesirable end states (Piarc, 2008a). The fault or event trees that are used to represent the accident causation may vary among the different existing methods, but the underlying event-based accident model is always the same. The overall risk level of a tunnel is estimated and presented in the dimension of the consequences (e.g. the number of fatalities or/and injuries) when both the probability and the consequences are assigned to every branch of the event or fault tree, as the sum of all probabilities times their consequences.

In order to evaluate the risk level two criteria are mainly used. The first criterion is the personal level of risk which is expressed by the individual risk indicator (fatality rate per tunnel kilometer). However, even if the individual risk is acceptable, the aggregated level of risk on a local or national scale could still be considered unacceptable, therefore a societal risk criterion is needed. The societal risk is the risk to society 'as a whole'. A common way to describe societal risk is the expected value (number of fatalities per year) and the F/N curves that illustrate the relationship between accident frequency and accident severity. Both indices are based on the As Low As Reasonably Practicably (ALARP) principle. If the risk index generated by the QRA is below a predefined safety target, the road tunnel is regarded as safe. Otherwise, risk reduction measures such as traffic volume control, need to be implemented (Beard and Cope, 2008).

An extended literature review of the QRA methods applied in the road tunnels field can be found in Piarc (2008a). The models that are presented in this report are the Austrian tunnel risk model TuRisMo, the Dutch TUNPRIM model, the French specific hazard investigation, the Italian risk analysis model for road tunnels and the OECD/PIARC DG-QRA model which is the most widely used decision aiding tool for the transportation of hazardous materials through a road tunnel. A detailed risk assessment with the OECD/PIARC DG-QRA method can also be found in Kirytopoulos et al. (2010a; 2010bq). Other QRA methods for road tunnels have also been proposed (Holicky, 2009; Nývlt et al, 2011; Weger et al, 2001; Xiaobo et al., 2011). All the aforementioned QRA methods not only consider different accident scenarios, but are also developed for different types of routes and tunnels (i.e. unidirectional or bidirectional tunnels, longitudinally or transverse ventilated tunnels, etc.). The considerable number of parameters used in the QRA model also differs. However, the key input parameters required in general by QRA models may commonly include traffic parameters, tunnel user characteristics, tunnel geometrical/geophysical characteristics and tunnel electrical/mechanical systems. Traffic parameters may include traffic volume, accident frequencies and traffic vehicle composition. Tunnel user characteristics usually refer to the reaction time of tunnel users, movement speeds, etc. Tunnel characteristics relate to distance between

emergency exits, number of lanes, tunnel height and various safety measures. These parameters are always fraught with a certain degree of uncertainty (Piarc, 2008a).

However, even if there are many differences in current road tunnel QRA methods, most of them consist of the same following modeling steps (Xiaobo et al., 2011):

1. Identification of all possible hazards such as fire, explosions, leaks and flood as top events.
2. Fault trees and event tree analysis for each top event. Event tree consists of a number of particular scenarios triggered by the top event and fault tree analysis is used to estimate the probability of a top event that could occur. Then, consequence estimation models can be applied to calculate the expected number of fatalities for various scenarios involved in the event tree.
3. After obtaining probability and fatality of each scenario, the societal risk and expected value is estimated. Smoke dispersion calculations are particularly used for fire scenarios in order to estimate the extent of the areas affected, where the consequences may cause fatalities to the exposed population. The smoke movement modeling varies from simple empirical relationships to complex CFD models. Moreover, evacuation calculations are employed in order to predict the expected number of people in those areas, varying also from empirical relationships to complex simulation models.
4. Having estimated the risk level of the tunnel, the last step is to evaluate the results and determine if additional risk reduction measures are needed.

Therefore, what seems to be clearly common in current QRAs applied in road tunnels is their event-based accident model (i.e. fault and event trees) combined with simulation tools so as to estimate the expected number of fatalities. If the estimated number is out of the predefined acceptable limits, then the tunnel is regarded unsafe and additional safety measures (mostly technical equipment) are proposed. The process is iterative and stops when the estimated risk is accepted. However, adding only technical equipment (a defense in depth strategy) is neither a cost-effective nor the most appropriate way to improve safety. The interested reader can refer to Høj.and Kröger (2002) for more information about the underlying concept of current QRAs in road tunnels.

Nevertheless, the causal chains and event modeling (i.e. fault and event trees) of QRAs have been subject to strong criticism for their limitations to capture the overall risk picture of complex socio-technical systems (Rasmussen, 1997; Hollnagel, 2004; Leveson, 2004). Indeed, the chain-of-event conception of accidents typically used in QRAs cannot account for the indirect, non-linear, and feedback relationships that characterize many accidents in complex systems and such a type of analysis has limitations to handle safety critical factors such as human behavior, organizational aspects, software errors, design flaws, and risk migration over time (Apostolakis 2004; Leveson 2004). Since road tunnels have organizational, social and managerial

dimensions that impact their safety, it is considered of outmost importance to examine whether the general limitations of QRAs, as have been highlighted in the literature, also exist in the road tunnels field. Due to its significance for the purposes of this work, this issue is analyzed in detail in paragraphs 2.2 – 2.7.

2.2 Lack of data and uncertainties

In order to perform a QRA, specific data is needed as input, since such an approach is based on calculating historical data-based probabilities (Steen and Aven, 2011). However, in the road tunnel field such kind of data (i.e. accident frequencies, reaction time of tunnel users, reliability of the tunnel equipment, etc.) is often either incomplete or not available at all (Nývlt et al, 2011). QRA is based on combining the probabilities of simple events to obtain the probabilities of system failures and this is the reason why it is quite difficult for QRA to deal with the absence of data concerning the reliability of all the components. Furthermore, the probability of a fire starting in a tunnel or the probability of an accident occurring cannot be calculated reliably since there is not a uniform, comprehensive and obligatory reporting of accidents and incidents in road tunnels (Beard and Cope, 2008). Apart from the lack of statistical data and the difficulty to calculate the probability of a tunnel accident, it is also very difficult to estimate the consequences of such accidents (Haack, 2002). It is hard to predict exactly how a fire may develop in a tunnel due to the numerous specific conditions that influence the situation (number and type of burning vehicles, location of fire, number and behavior of tunnel users, time to activate appropriate actions etc.). In this context, it is obvious that it is very difficult for a QRA to establish a reliable overall risk picture. One might claim that all the aforementioned uncertainties exist independently of whether we perform a QRA or not and by attempting to quantify the uncertainties, QRA will contribute to the understanding of road tunnels safety issues (Apostolakis, 2004). Even if this is true, quantifying risk by using the expected number of fatalities gives the impression that the risk can be expressed in a very precise way (Aven, 2003). This is definitely not the case in road tunnels, where risk indices include a too strong element of arbitrariness since the probability of accidents cannot be easily measured and the consequences cannot be precisely estimated.

2.3 Human errors and behavior during accident conditions

The driver error has been regarded as the causal factor in many road accidents (Larsson et al., 2009) so it is only natural to wonder whether the potential of such errors could be incorporated into QRA. Human errors in general are divided in errors of omission (neglecting to perform a well defined procedure) and errors of commission (deliberately undertaking an action not specified in procedures; Reason, 1990). Errors of commission have been considered impossible to analyze and the simple engineering-style models used in QRA does not capture some of the important influences on error probabilities, sometimes referred as “the error-prompting context”

(Apostolakis, 2004). This is in line with Leveson (2011a) and Rasmussen (1997) who also state that the way we design the environment or context in which humans operate is fundamental as far as safety is concerned, and this context cannot be adequately depicted in fault and event trees analysis. Moreover, by simply identifying and assessing human "failures" (e.g. the tunnel operator did not effectively use the ventilation system) in fault trees, it is not possible to make progress in designing and operating safer tunnels. The risk assessment must identify how specific hazardous human behavior might occur, so as to evaluate the current design and propose mitigation measures, in order to avoid such hazardous behaviors.

As far as modeling the motorists' evacuation in case of an emergency in a road tunnel is concerned (a crucial step in current QRA models), researches have shown that this subject remains elusive (Nilsson et al, 2009). Zarboutis (2007) has proposed an agent-based modeling as an approach to capture a number of psychological crowd effects on individual psychomotor behavior, which in turn influence crowd behavior in tunnels. However, this method is aiming at designing plans for emergency rescue rather than predicting the evolution of the evacuation process. Experimental results (Nilsson et al, 2009) have shown that social influence is particularly important during evacuation in road tunnels, (i.e. people are influenced by the behavior of others). Other aspects such as evacuation messages, the magnetism of emergency exits (e.g. flashing lights) and the kind of information provided to the motorists during the evacuation, also affect the evacuation process (Piarc, 2008b). Notwithstanding, all the aforementioned aspects are omitted from tunnel QRAs. Concluding, queuing and network models that simulate the evacuation during an emergency in a road tunnel and are explicitly used in current QRA tunnel models may be useful tools to design appropriate safety barriers and escape routes, but they cannot be used afterwards in order to evaluate the design they have themselves proposed. For the safety evaluation of the tunnel design another approach is needed.

2.4 Organizational factors and safety culture

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 1990; 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 the notable attempts of some researchers to quantify organizational aspects (Pate-Cornell and Murphy, 1996; Mohaghegh and Mosleh, 2009), it is generally agreed that QRAs have limitations to capture the influence of management (Apostolakis, 2004). The authors of this work do not share the opinion of many safety experts that "QRAs do not include organizational factors. Case closed!" since there is little research to prove the validity of this statement. The field of QRAs is under constant development and in some industries QRAs have been applied taking into consideration organizational aspects (Skogdalen and Vinnem, 2011).

However, in the road tunnels field, a framework to describe human and organizational factors (HOFs) has not been proposed yet, hence the current methods omit organizational factors from their analysis. Organizational responsibilities in the tunnels field may vary from country to country; however, common organizational aspects that greatly affect safety include (Piarc, 2007):

- Traffic management and decisions concerning speed limits and allowing the transportation of hazardous materials through a tunnel.
- Maintenance and inspection of the tunnel.
- Recruitment of the tunnel staff and its training procedures.
- Preparation of emergency plans and procedures, planning of emergency exercises and co-operation with the emergency services.
- Analysis of past incidents and the learning from events.

All the aforementioned activities are undeniably safety critical aspects. Accidents frequency, emergency preparedness, emergency response and mitigation of the consequences of an accident are all aspects highly dependent on the organizational and inter-organizational structure. The fact that organizational factors are not included in the safety assessment is thus a striking weakness of current QRAs methods.

2.5 Software errors

Supervisory Control and Data Acquisition (SCADA) systems are widely used in modern road tunnels to monitor and control tunnel equipment. The SCADA allows efficient maintenance and proper reaction of the tunnel operator in case of an emergency. Usually, SCADA monitors and controls the following equipment systems:

- power supply system
- tunnel ventilation system
- tunnel lighting system
- fire fighting system
- fire detection system
- tunnel communication system
- traffic management system

In case of an emergency, pre-programmed equipment configuration actions are activated by the SCADA or are proposed for validation to the tunnel operator. Hence, the SCADA system is a safety critical component of the tunnel 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. Nevertheless, such a requirement ensures reliability and not safety. As 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".

Safety risk assessment in road tunnels should investigate which actions of SCADA might lead to the occurrence or to the escalation of an accident. The question is whether QRAs can capture accidents arising from SCADA's operation. 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 (Leveson, 1995). Trying to calculate the probability that the software will fail and reflect it in fault trees by containing boxes that indicate "SCADA Fails" does not make sense without first understanding in what ways the SCADA may fail. Nevertheless, the behavior of the SCADA software is not random; software is not a source of uncertainty (Garret and Apostolakis, 1999). 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. This context is not actually assessed by QRA methods (Leveson 1995).

2.6 System accidents

As the design of tunnel equipment systems has become safer and more reliable, the causes of accidents are more likely to be attributed to the interactions among the tunnel's equipment systems, rather than due to individual systems failure. 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).
- 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 a hazardous system state. Treating such events as independent may lead to unrealistic tunnel risk assessment and to a large underestimation of the true risk. Perrow (1984) coined the term *system accidents* to describe such accidents that arise in the interaction among components and Leveson (2004) claims that QRAs have limitations to assess such common-cause accidents. Tunnel equipment should not be considered and evaluated as separate entities but as part of an integrated safety system and the existing road tunnels QRAs have limitations to do that.

2.7 Adaptation of the tunnel system over time

The traditional view of QRA is that it is an activity carried out at the beginning of a system's lifecycle, providing a "snapshot" of the risk associated with the system design. However, many road tunnels that are initially designed and built with adequate safety margins have migrated to a state of increasing risk over time. This is mainly due to the lack of management commitment (e.g. poor maintenance) or because the system changes over time (different traffic volume, different portion of dangerous goods vehicles in the traffic, etc.). In both cases the dynamic feedback processes that may cause risk to increase over time must be defined and QRA is unable to do that (Dulac and Leveson, 2005). When looking at QRAs in road tunnels it seems that there is no link between the design stage conditions and the actual conditions of a tunnel**.** In this static view of the tunnel system it is implied that the tunnel equipment and the safety measures do not degrade through time. This seems to be a narrow perspective since systems tend to involve a migration to a state of increasing risk over time (Rasmussen, 1997). Adaptation or change is an inherent part of any system, particularly those that include human and organizational components (Leveson, 2004). Rasmussen (1997) has argued that major accidents are often caused by the migration of the system to hazardous states. The critical factor is that such adaptation is not a random process thus should be predictable and controllable. The risk assessment in road tunnels should reveal how the system may degrade over time and the QRA modeling lacks in feedback mechanisms to provide such kind of information.

3. The need for a new approach to road tunnel safety assessment

In a nutshell, QRA treats tunnel accidents as random phenomena although the system design errors and the insufficiency in predicting the interactions among tunnel components (electromechanical, digital, human and social such as emergency services and tunnel operator actions) giving rise to accidents are not really random events. QRA is performed mainly by using event-based accident models (i.e. fault trees and event trees analysis) which explain accidents in terms of multiple events sequenced as a chain over time. The events considered almost always involve some type of component failure (e.g. ventilation failure) or human error (e.g. driver/operator/emergency service error). These sequential accident or event-based accident models according to Hollnagel (2004) are limited in their capability to explain accident causation in more complex socio-technical systems. As Leveson (2011a) refers "In event-based models, the causal factors identified depend on the events that are considered and the selection of the conditions related to those events. However the choice of events to include is subjective and the selection of conditions to explain the events is even more so". Events chains developed to explain an accident concentrates on the proximate events. Nevertheless, the foundation of an accident may lay years before in the engineering and management decisions.

Component failures as initiating events are also inadequate explanations for major accidents in road tunnels. Investigations have shown that the causes of tunnel accidents are much more complex, involving factors at all levels of the system, from component failures to organizational and social factors. In the Mont-Blanc accident, for instance, it was concluded that fatal consequences could have been greatly reduced by a more efficient operation of emergency services, more skilled personnel, more powerful safety systems and higher awareness among users (Lacroix, 2001). Furthermore, the tunnel system (both the organizational and technical) had been degraded before the accident (Lacroix, 2001). The fire in the truck triggered the loss, but the catastrophe occurred due to systemic causes, not just because of an unfortunate coincidence of factors.

However, any attempt to manage risk and evaluate safety requires an underlying model of how accidents happen. This underlying model also influences the strategies that an organization uses. If the model focuses on human error and component failures, the most risk reduction will tend to reduce the effects of human errors and component failures neglecting other important factors. As Lundberg (2009) states what you look for in an accident analysis is what you actually find and fix. Thus, if the aim of a road tunnel risk assessment is to give the impression that risk can be expressed in a very precise way so as to satisfy the tunnel managers and insurances companies, QRAs may certainly achieve that purpose. On the contrary, if the aim of safety risk assessment is to establish a risk picture and identify factors, conditions, activities and systems that are important with respect to safety, then arbitrary risk indices such as the expected value formulation used in road tunnels safety assessment is not an enough safety effort.

Awareness of risk is a major component of safety-related decision making and in this section we have presented that QRAs do not take into account some of the most important factors that influence road tunnels safety such as organizational aspects, system accidents, software errors, human errors and adaptation of the tunnel system over time. On the one hand improvements can be made in current road tunnel QRAs in order to cope with some of the aforementioned limitations. Following this line of thought road tunnel QRAs can be enhanced with human reliability analysis (HRA) and common-cause-failure analysis (CCF). HRA deals with methods for modeling human error while CCF deals with methods for evaluating the effect of inter-system and intra-system dependencies which tend to cause simultaneous failures and thus significant increases in overall risk (Skogdalen and Vinnem 2011). Moreover, Bayesian Belief Networks (BBN) can be used in order to cope with uncertainty. However, we believe that there is a need for a resolution in the road tunnel safety assessment, a need to see beyond probabilities when trying to assess the safety level of those critical infrastructures. Even if the events triggering an accident may be regarded as random events, the ‘uncertainty’ of the tunnel system to control the trigger event and avoid the accident is not really a random phenomenon. This type of risk (that may indeed determine the extent of the accident) is potentially knowable

and not some amorphous property denoted by probability and fatality estimates. Aven (2010) makes his point clear: “the risk cannot be adequately described and evaluated simply by reference to summarizing probabilities and expected values.” . Steen and Aven (2011) also stress that in order to analyze systemic accidents there is a need for concepts and tools that see beyond the probabilistic world. There is a need for a new paradigm.

Systemic accident models have been particularly useful in helping analysts probe into the complicated interactions among system components that may lead to unfortunate events hence; it might worth trying to describe tunnel’s uncertainties and risks with such a model. Following this line of thought, in this article we introduce a systemic accident causation model in the road tunnel safety topic and propose a STAMP-based method as an alternative or even complementary approach to road tunnel safety assessment.

4 Introducing STAMP in road tunnel safety assessment

4.1. The STAMP approach

The STAMP (Systems-Theoretic Accident Model and Processes) is a systemic accident model that has been recently proposed by Leveson (2004). The model is based on the two major pairs of ideas underlying systems theory and systems thinking (Checkland, 1981):

1. Emergence and hierarchy
2. Communication and control

The term ‘systemic’ is significantly broad, but is adopted to indicate that STAMP covers both the technical and the organizational dimension. Based on a systems approach, STAMP focuses on systems considered as a whole, not on parts considered separately. This systems theoretic approach treats safety as an emergent property that arises when the system components interact with the environment. Emergent properties, like safety, are controlled or enforced by a set of constraints related to the behavior of the system components. Hence, it is the inadequate or inappropriate control of safety-related 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 concepts of the STAMP model are:

- Safety constraints: Safety-related constraints are relationships among system variables, safety barriers and processes that prevent the system from reaching hazardous states. Leveson (2004) emphasizes safety constraints, rather than failure

events, as the most basic concept in accident analysis. Instead of viewing accidents as the result of events, accidents are considered as the result of interaction among systems' components that result in a violation of safety-related constraints. The controlled processes (organizational and technical) that enforce these constraints must limit system behavior to the safe changes and adaptations (Checkland, 1981). Therefore, a socio-technical control structure that controls the aforementioned processes and enforces the necessary constraints on systems development and operation must be designed.

- Hierarchical safety control structures: The hierarchical safety control structure represents the components of the socio-technical system that enforce the aforementioned safety constraints (i.e. the controllers). A hierarchical multilevel model of stakeholders is posited in STAMP, similar to the model of Rasmussen (1997), but more expanded. Every level in this hierarchical model can impose safety constraints that in turn contribute to accident prevention and safety. On the contrary, accidents result due to improper imposition or control of constraints. An example of a hierarchical safety control structure is given by Leveson (2004, pp.257).
- Process models and control loops: Hierarchies in systems theory are characterized by control and communication processes operating at the interfaces between levels. Control loops operate between the hierarchical levels of each control structure that have a downward (i.e. reference) channel providing the information or commands necessary to impose the constraints in the level below and a measuring channel to provide feedback measurements about how effectively the constraints were enforced. Finally, each controller at all levels of the hierarchical control structure (and not just at the lower physical levels) must have a process model of the process being controlled (i.e. a model of the system). Briefly, whether the model is embedded in an automated controller or in the mental model 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 1 presents a basic control loop in STAMP.

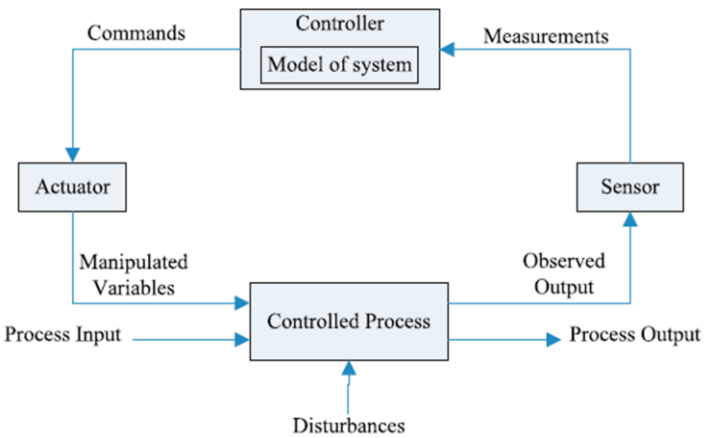

Figure 1. A basic process control loop in STAMP (Quyang et al., 2010).

In STAMP terms, accidents result from inadequate control, i.e., the control loop creates or does not handle dysfunctional interactions in the process. Dysfunctional interactions can be caused either by component failures or/and by design flaws. Thus, the process that leads to accidents can be understood in terms of flaws in the components of the system development and operation. STAMP provides a useful classification of control flaws leading to hazards. This classification is presented in figure 2. In each control loop at each level of the socio-technical control structure, potential inadequate control actions may include: (1) the controller may issue inadequate control actions, (2) control actions may be inadequately executed and (3) there may be missing or inadequate feedback. These general factors apply at each level of the socio-technical control structure, but the applications of the factors at each level may differ (Leveson, 2004).

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 2: A classification of control flaws (Leveson, 2004)

The STAMP accident model has been used to analyze many major accidents, such as a public water supply contamination accident that happened in a small town of Walkeron, a Friendly Fire Accident (Leveson, 2011b) and a railway accident in China (Quyang et al., 2010). Apart from accident analysis, the model has also been used for risk assessment and hazard analysis of several socio-technical systems (Dulac and Leveson, 2005; Leveson, 2011b; Hardy and Guarnieri 2010). A STAMP based risk assessment considers the technical (including hardware and software), human/organizational factors and the adaptation of the analyzed system over time. Thus, it worth trying to adopt the STAMP in the road tunnel field, where, as already

discussed in Section 3, organizational aspects, human errors, software design and the dynamic nature of the tunnel system influence to a great extent the overall safety.

4.2 STAMP implementation: Illustrative example in tunnel ventilation system

To illustrate the STAMP-based road tunnel safety risk assessment method introduced in this paper, the proposed framework is applied to the analysis of a tunnel ventilation system. The choice to analyze only a particular system component and not a whole tunnel system might hide the major ability of the proposed method to describe the interactions among tunnel subsystems (i.e. tunnel ventilation system, fire fighting system, fire detection system, tunnel communication system and traffic management system). Moreover, crucial elements of tunnel safety and particularly the co-operation between the tunnel operator and emergency services are also omitted from our analysis. However, the authors prefer to demonstrate the framework in a particular tunnel subsystem in order to present the method as thoroughly as possible, even if some advantages of the technique are not highlighted, due to space limitations. Recommendations of how to apply the method for the whole tunnel system are made, so as to explain how the proposed framework can be used for the assessment of the overall tunnel safety.

4.2.1 Case description

In the road tunnels safety field, much attention is paid to the ventilation system and particularly to its ability to maintain a smoke-free evacuation route for the tunnel users in the early phase of a fire incident (self-rescuing phase). The time for arrival of emergency services, in case of fire in a tunnel, is very variable, depending mainly on the traffic condition. Therefore, the ventilation system is one of the most important safety measures in tunnels, since it affects smoke propagation, temperatures in the fire zone, concentration of contaminants, visibility, etc. (Carvel et al., 2001). The ventilation strategy to be adopted depends on the particular tunnel geometry, traffic density and whether the tunnel is bidirectional or unidirectional (Piarc, 2011). Since this paper focuses on the safety assessment technique, the information presented in this section is limited to what the authors regard crucial for the implementation of the STAMP-based road tunnel safety assessment. For more technical information about this topic the interested reader is referred to Carvel et al. (2001), Piarc (2011) and the references therein.

The examined case study is a typical long twin bore unidirectional tunnel, equipped with longitudinal ventilation system, supervised by a SCADA system and a manned control centre. The case described herein represents a typical design of tunnel ventilation met in many countries (Piarc, 2011). In a longitudinal ventilation system the air is introduced or removed from the tunnel at a limited number of points, such as portals. In the examined case the required longitudinal airflow is provided through a set of ceiling mounted jet fans.

If a fire occurs in a tunnel, hot smoke rises due to buoyancy forces. This separation between the hot upper layers and cooler layers is termed *stratification* and it is a temporary phenomenon that experience shows lasts for about 15 minutes. After that time, smoke completely fills the tunnel both downstream and upstream of the fire. Very often the longitudinal airflow is low and the smoke moves against the ventilation stream; a phenomenon called *back-layering* (Piarc, 2011).

Ventilation systems such as the one examined are usually designed on the provision of minimum longitudinal air velocity to avoid back-layering, the so-called *critical velocity*. During emergency, the goal of the examined ventilation system is to maintain tenable conditions mainly upstream the fire, supposing that the tunnel is not congested and the vehicles downstream the fire will have the opportunity to exit the tunnel unhindered (Piarc, 2011), as shown in figure 3.

Figure 3. Fire-induced smoke longitudinal control

The examined ventilation system is controlled by the SCADA system as follows: In the normal operating mode of the tunnel, the system works in an automated mode, without any intervention of the tunnel operator. The control in this ventilation mode is associated with measured pollution and opacity levels (e.g CO, dust and NO thresholds). When measurements are monitored over the predefined threshold, the SCADA activates a particular number of jet fans in order to reduce the concentration of CO and other pollutants. For cost effective ventilation operation in the normal mode, the SCADA avoids starting a jet fan that has reached a maximum number of starts per hour. Moreover, a jet fan's vibration information is monitored and if it is measured over a threshold the SCADA also does not activate the particular jet fan.

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 a fire is confirmed, then the phase 2, the smoke management phase, is activated. Thus, the phase 2 is based on a waiting loop expecting the tunnel operator's validation. The aim of phase 2 is the internal airflow to reach the target critical velocity, as defined by the designers of the ventilation system. The predefined number of jet fans to run for each fire

scenario is an initial value of the algorithm, specific for each tunnel. The non-incident (escape) tube ventilation (as has been mentioned, the tunnel is twin bore) is also set up aiming at avoiding smoke recycling at the portal by limiting the pressure differences between the two tubes. Finally, 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, to limit an electrical overload. As a result, the start up of the required jet fans is sequential at each electrical substation of the tunnel even in phase 2 (fire ventilation mode). The starting is depending on a timer setting in the SCADA, with usual default values at 5 seconds.

The examined case described above is a typical design of tunnel ventilation system used in twin bore unidirectional road tunnels. Accident scenarios, deterministic or probabilistic risk assessment and simulation models mainly drive the design of ventilation systems. Even if another type of ventilation or SCADA is installed in a road tunnel, the basic principles underlying the safety assessment presented in this article would not be affected. In the next paragraph, the STAMP-based road tunnel safety risk assessment is introduced to identify how the particular ventilation system might prove inadequate to control the fire, even if a QRA has been performed and claimed that the tunnel is safe. Moreover, the aspects that must be examined in order to decide whether the tunnel system is safe or not (as far as the smoke control is concerned) are presented. The STAMP analysis consists of four main steps (fig. 4), which are analyzed in detail.

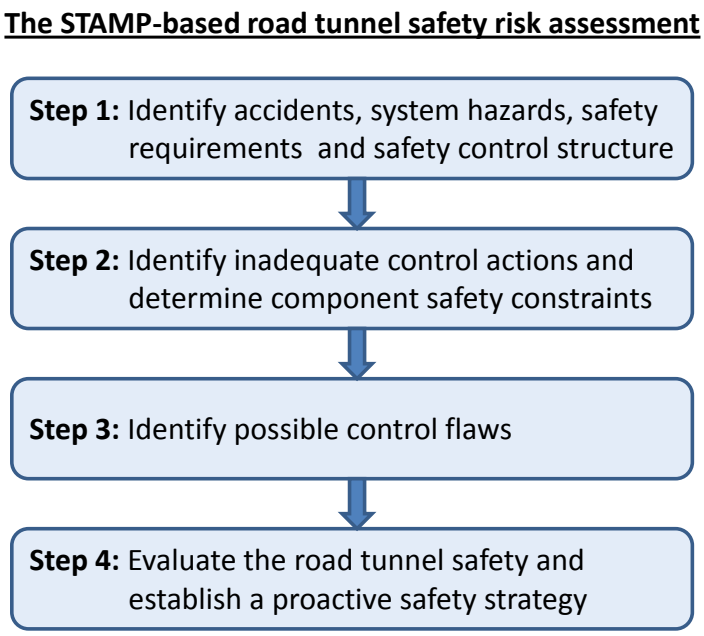

Figure 4. Methodology steps of the STAMP-based analysis

4.2.2 Step 1: Identify accidents, high level hazards, safety constraints and the safety control structure

The first thing to be done in any safety effort involves agreeing on the types of accidents or losses to be considered. Then, the high level hazards that might lead to

the particular accident must be defined. A hazard is a system state or set of conditions that, together with a particular set of environmental conditions may lead to an accident (Leveson, 2004).

In the road tunnel field, the main undesired events that may result in losses (i.e. accidents) are (Piarc, 2008a):

1. Fire in a tunnel
2. Explosion in a tunnel
3. Release of toxic gas in a tunnel
4. Traffic accidents (e.g. vehicle collisions)
5. Flooding

In this paper the proposed safety assessment method focuses on the following accident: **Human losses/injuries and tunnel damage due to a fire in a tunnel** (i.e. the first one mentioned in the above list). The high-level hazards that may lead to the accident are:

- Dangerous driving in the tunnel
- Inadequacy of the tunnel ventilation system to control smoke and fire in the initial (self-rescuing) phase of a fire
- Inability of the road users to rescue themselves
- Inability of the tunnel operator to effectively intervene and provide the appropriate actions
- Inability of the emergency services to control the incident

It must be mentioned that for a complete risk assessment of the whole tunnel, all the aforementioned accidents and hazards must be identified. However, in order to demonstrate the method we focus only on the particular hazard: **"Inadequacy of the tunnel ventilation system to control smoke and fire in the initial (self-rescuing) phase of a fire".**

Having identified the system hazard, the next step in the safety risk assessment is to determine the high-level safety requirements and constraints that must be enforced in order to control the particular hazard. It is mentioned that safety requirements represent the reason for the existence of the system (in terms of safety) while constraints represent acceptable ways that the system can achieve those goals. High-level safety requirements and constraints are identified by analyzing the way the hazard could occur, by past experience on similar hazards and by safety guidelines. The high level safety requirement and the high level constraints for this particular hazard are:

High level requirement of tunnel ventilation system: to provide the tunnel users escape routes with tenable levels of temperature, toxicity and visibility from both downstream and upstream the fire.

High level safety constraints that must be enforced in order to address the safety requirement are:

1. In case of fire, the ventilation operation needs to be changed from normal mode to smoke management mode as quickly as possible.
2. The longitudinal air flow velocity must be reliably controlled to avoid de-stratification and back-layering of the smoke.
3. The operator must be well trained so as to react within the time available and under high stress conditions. Moreover he must adjust the ventilation strategy according to the information available.
4. The ventilation system must be well maintained and tested so as to provide the necessary air flow capacity.

The next step is to identify the controllers who enforce the above high-level safety constraints in the safety control structure. Leveson (2011b) has proposed specific criteria about who should be included in a safety control structure. However, in our simple examined case (i.e. without complex organizational structures) we include every component of the tunnel system (human, organizational, automation) that plays a role in the enforcement of the high level safety requirement and constraints identified so far. The safety control structure of a typical road tunnel (at least a tunnel that is conformed to European Directive 2004/54) is presented in figure 5 and the roles and responsibilities for each component in the structure are also discussed.

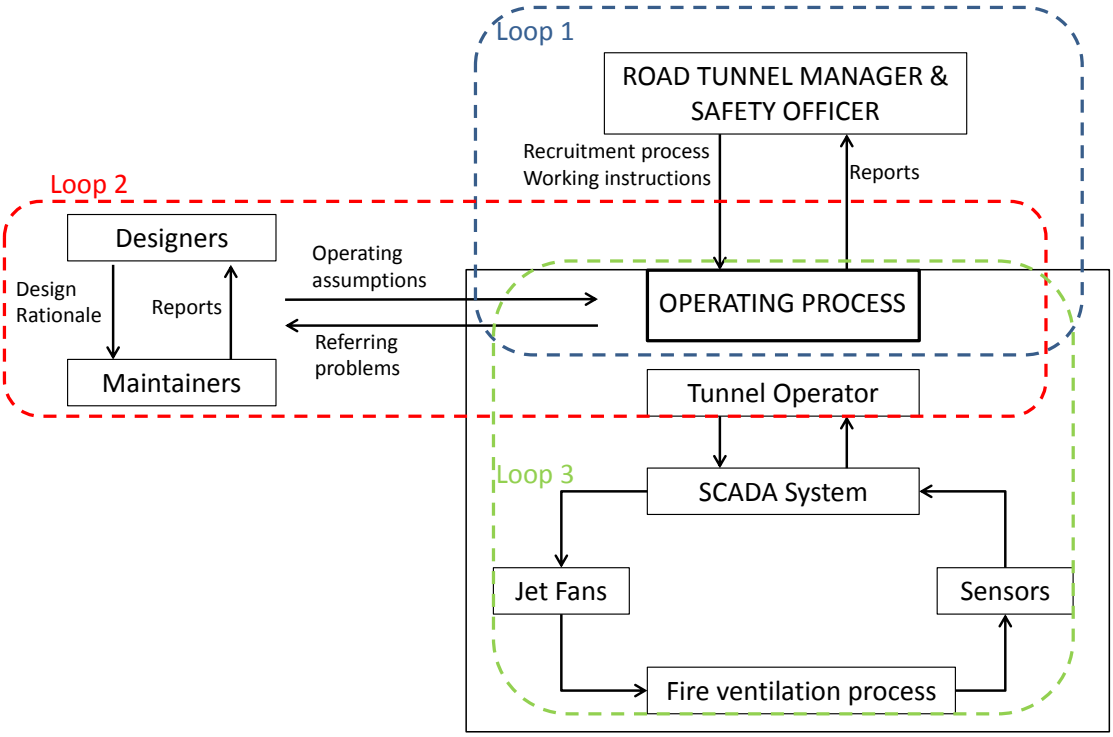

Figure 5: The tunnel hierarchical safety control structure

The *Tunnel Manager* is responsible for the day to day operation and safety of the tunnel. He forms working instructions, draws up the maintenance strategy and is responsible for the recruitment and training of the tunnel staff.

The *Safety Officer* takes part in the implementation and evaluation of emergency operations, verifies that the operational staff is trained and must also take part in the organization of exercises. Lastly, he examines whether the tunnel structure and equipment is maintained and repaired.

The *maintenance* personnel's role is to intervene on the technical facilities of the tunnels in a preventive and corrective way as it has been planned by the tunnel manager.

Designers and contractors affect tunnel safety to a great extent. It must be crystal-clear that tunnels safety during operation greatly depends on the original design and development of the tunnel system.

In the operating process the two main controllers are the *tunnel operator* (often named traffic operator if the tunnel is included in a controlled high way section) and the *SCADA system*. The role of the SCADA system is to propose a pre-programmed fire control scenario to the tunnel operator to validate. If the scenario is considered the appropriate, the mitigation action is activated by the tunnel operator.

All the aforementioned controllers can be mapped in the safety control structure presented in figure 5 by control loops.

4.2.3 Step 2: Identify inadequate control actions and determine component safety constraints

The second step identifies how the safety requirements and constraints identified in step 1 could be violated. In STAMP terms, safety constraints are violated when the process model used by the controller who enforces them does not match the real process and as a result, the following four *general* types of inadequate control actions may occur:

1. A required control action is not provided
2. An incorrect or unsafe control action is provided
3. A potentially correct control action is provided at the wrong time (e.g. too late)
4. A potentially correct control action is stopped too early

Inadequate control actions can arise at all levels of the safety control structure, thus all the components in the structure must be examined. It must be mentioned that some of the possible inadequate control actions may not be applicable for a controller. For, example, working instructions are provided or not. They cannot be provided too late, neither can be stopped too soon. The hazardous states that could occur due to the four general inadequate control actions are:

In control loop 1 (i.e. from the Tunnel Manager and the Safety Officer):

1. Working instructions are not provided by the tunnel management (Tunnel Manager and tunnel Safety Officer) to the tunnel operator or wrong/misleading working instructions are provided (i.e. they have not been updated).
2. Specific recruitment and training requirements are not applied for the recruitment/training of the tunnel staff (tunnel operator and maintenance personnel), or the requirements do not match the required skills that must be accomplished.

In control loop 2 (i.e. from designers/maintainers):

1. The operating assumptions and the operational limitations for the ventilation system have not passed from the designers of the system to the tunnel operators. Similarly, safety critical components of the tunnel ventilation system are not given by the designers to the maintenance process for prioritization of effort. Even if this seems very difficult to happen we should keep in mind that road tunnels have a very long operating life and very few of those involved with the original planning and construction works will be available to share their knowledge with those coming after them to operate and maintain the tunnel. Consequently, if the assumptions of the design have not been recorded it is probable that operational quality will not be maintained.

In control loop 3 (i.e. from tunnel operator and SCADA system):

1. The tunnel operator and/or the SCADA system do not activate the tunnel ventilation system for the emergency.
2. The ventilation system creates high longitudinal velocities downstream of the fire, the tunnel users have not evacuated that area, and therefore they are affected by the fire. Moreover, high longitudinal velocities feed the fire with oxygen creating enhancement of heat release rate.
3. The tunnel operator waits too long to validate the alarm or the SCADA system is inadequate to activate the ventilation system quickly enough.
4. The emergency ventilation mode is stopped before the fire event has been declared closed.

The information provided in this step of the analysis is used to identify the more refined safety constraints on systems component behavior to prevent the identified system hazards. All the aforementioned inadequate control actions are turned into components' safety constraints though a simple process. In order to develop the more refined safety constraints it would be also helpful to take into consideration guidelines and best practices used in the tunnel safety field. Concluding, the safety constraints that must be enforced are presented in Table 1:

Table 1

Safety constraints to be enforced

Constraint	Description of the safety constraint
C1	Specific recruitment requirements that reflect the necessary required technical skills of tunnel personnel (maintenance agents, tunnel operator) must be well defined in parallel with a feedback mechanism that ensures that the tunnel personnel satisfies these requirements.
C2	The working instructions provided to the tunnel operator must enable a quick response in case of an emergency.
C3	Rigorous and ongoing training must be provided to the tunnel personnel in conjunction with a feedback mechanism which tests the effectiveness of the training procedures.
C4	The operating assumptions and the operational limitations for the ventilation system must be recorded and passed from the designers of the system to the tunnel operators and maintainers.
C5	Fire ventilation mode must be always activated if a fire exists in the tunnel.
C6	The airflow provided by the ventilation system must prevent back-layering and smoke de-stratification for at least the first 10-15 minutes from the onset of the fire.
C7	If people are situated downstream the fire they must not get fired.
C8	The application of forced ventilation could assist the fire since it feeds the fire with oxygen. Thus, the tunnel operator must be able to identify the fire type, the exact situation and adjust the ventilation strategy accordingly.
C9	The full operation of the smoke control must be achieved within 2-3 minutes from the onset of the fire.
C10	The fire ventilation mode must not stop until the smoke is under control.

For those involved in tunnel safety there may be an endogenous conflict in C6 to prevent both back-layering and smoke de-stratification. However, a safe system is not necessarily free of such conflicts. What really is of utmost importance for safety engineers is to be aware of these conflicts.

In this step more refined components safety constraints are provided and a first assessment of the safety controls of a particular tunnel can be made, at least for safety control measures that enforce or do not enforce constraints C1-C4. The tunnel's procedures must be thoroughly examined in this stage of the analysis. For example does a quality plan or specific organizational procedures that enforce constraints C1-C4 exist or have been designed (if the tunnel is under construction)? Does a Routine Maintenance Management System exist for the effective management of the maintenance of the tunnel? However, for constraints 5-10 the assessment is more complex and even if the appropriate safety constraints have been provided to the system through safety controls (i.e. smoke detectors are provided so as to activate the ventilation system, etc.) the safety constraints might still fail to be enforced and prevent the accident. In the next step the crux of the causal analysis is presented and the aspects that must be examined in the risk assessment are highlighted.

4.2.4 Step 3: Determine how unsafe actions could occur and identify possible control flaws

Step 3 of our analysis is the one that identifies the scenarios or paths leading to a hazard as found in a classic risk analysis. However, the guidance provided by Leveson (2004) with the control flaws terminology greatly helps the analysis process and more than just failures are taken into consideration. Identification of control flaws starts by examining each of the basic components of the loop 3 and determines how their improper operation may contribute to the general types of inadequate control as presented in 4.2.3 and consequently to the violation of constraints C5-C10 presented in Table 1.

The general control flaws (figure 2) are mapped into the examined loop 3 as presented in figure 6.

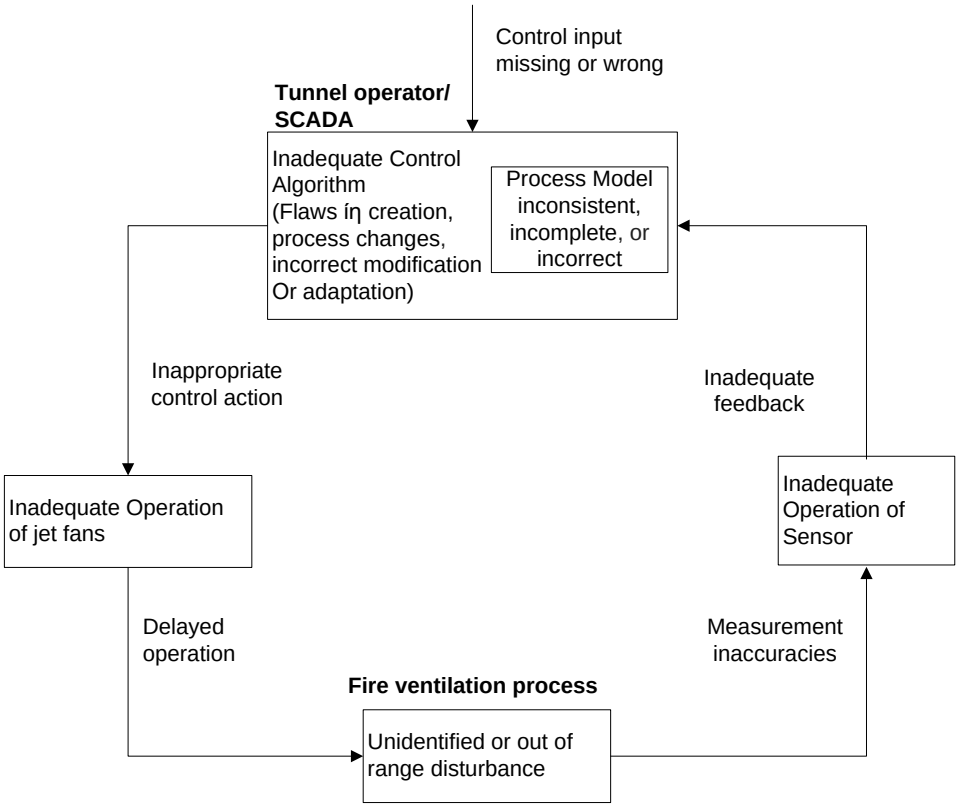

Figure 6: The examined control loop of the fire ventilation process

Thus, by working around the loop presented in figure 6 and examining the control flaws leading to accidents, the identified causal factors are:

- **Control inputs or external information wrong or missing**

The tunnel operator and the SCADA system co-operate with other components in the tunnel system. As a result, actions and outputs from other system components are

needed in order to control the fire ventilation process. The safety constraints might be inadequately enforced or violated due to the following scenarios:

a. The power supply has failed; the ventilation system has not the necessary input to start the fire ventilation process. Violation of C5-component failure.
b. Fire detection has failed. Consequently, the tunnel operator and the SCADA system are not aware of the fact that a fire exists in the tunnel and the fire ventilation mode is not activated. Violation of C5-component failure.
c. When a fire occurs, it will cause an increase in dust and CO levels. Before the levels are high enough to define a fire, the ventilation (normal operating mode) will have increased the ventilation rate. This rise in airflow will affect the time to detect the fire and turn the ventilation in a fire mode. Violation of C9-systemic factors.
d. Inadequate/wrong working procedures have been given to the tunnel operator by the tunnel management concerning how to safely operate the ventilation system Violation of constraint C2-organizational factor.
e. Frequently false alarms (wrong inputs) have created complacency during the tunnel operation. As a result, fire alarms do not immediately activate emergency procedures. The tunnel operator has slipped into a state of inertia. Violation of C9-human factor.

It must be mentioned that the previous control flaws are resulting from the inadequate control of other controlled processes and from their safety constraints violation. Thus, in a detailed risk assessment the fire detection process and the power supply of the tunnel must also be carefully analyzed as they affect the fire ventilation mode to a great extent and can cause system accidents.

- **Inadequate control algorithm of SCADA system and tunnel operator (flaws in creation, incorrect modification or adaptation)**

Algorithms are the procedures designed by engineers for the SCADA system and the procedures that the tunnel operator follows for the emergency ventilation process. Scenarios that may violate the safety constraints belonging to this classification are:

a. The predefined number of jet fans to run in order to avoid back-layering fails to achieve the necessary critical velocity. Violation of C6-design error.
b. The fire ventilation mode cannot override the normal operation mode. Consequently, the SCADA avoids starting particular safety critical jet fans because they have reached the maximum number of starts per hour or because of the vibration threshold. Violation of C6-software error.
c. The fire ventilation mode stops because of the CO, NO2 thresholds. Violation of C10-software error.

d. The non-incident ventilation tube is inappropriately set up leading to smoke recycling due to the pressure differences between the two tubes. Violation of C6-design error.
e. The traffic volume has changed considerably during time. Although the ventilation system was initially effective, it is presently insufficient to control the fire and nobody has noticed the migration of the system to a hazardous state. Violation of C6- lack of feedback/organizational factor.
f. The tunnel operator has inadequate understanding of his controlled authority. For example, he does not know that he can reverse electrically the flow of the jet fans although such an action is needed. Violation of C6-human error.
g. The pre-programmed scenario proposed by SCADA is the appropriate but the tunnel operator cannot validate the scenario. This may be due to his absence of the control room without someone to stand in for him or due to his panic (cognition characteristics). Violation of C5-organizational factor.

- **Process model of SCADA system and tunnel operator inconsistent or incomplete**

The process model is the way both SCADA and the tunnel operator get informed about the fire ventilation process progress. When both the SCADA and the operator have a different perception of the tunnel environment than the real state, erroneous control commands may be provided. Scenarios which may lead to inadequate enforcement/violation of the safety constraints are the following:

a. Anemometers coherency test performed by SCADA system has failed to detect that anemometers are out of order. As a result the SCADA system has an incorrect process model of the tunnel longitudinal ventilation velocity and inadequate air flow is provided. Violation of C6-component failure.
b. Anemometers have not been calibrated due to poor maintenance policy. Violation of C6-organizational factor.
c. The buoyant fire plume that is moving within the tunnel environment affects the anemometers operation; wrong airflow values are provided to the SCADA. Violation of C6-design error.
d. The tunnel operator does not have sufficient feedback of the tunnel environment and the controlled process. The fire incident tunnel team, the sensors and communication with tunnels users does not provide the necessary information in order to update his mental model of the controlled process. The displays and the human machine interface of the SCADA might be not ergonomic enough. In a nutshell, the feedback information bandwidth is incorrectly designed. As a result, the pre-programmed scenario proposed by the SCADA system is validated by the tunnel operator although it is not the appropriate. For example, the scenario is based on the assumption that people downstream the fire have evacuated and applies forced ventilation. However, this is not the case; the tunnel operator

incorrectly validates the scenario leading to tunnel users being exposed to fire. Violation of C7, C8-human error.

- **Inadequate operation of the actuators**

The scenarios discussed so far involved inadequate/hazardous control. What follows involves scenarios where adequate/safe control commands are produced but cannot be executed.

a. Ventilation command transmission network fails; ventilation fans are not activated. Violation of C5, C6-component failures.
b. Fans and dampers have not been constructed to withstand high temperatures and pressures, therefore during the fire some of them do not operate. Violation of C10-design error.
c. The jet fan starting procedure (as has already been mentioned is based on star-delta start system) brings about the delayed operation of safety critical jet fans. Violation of C9-design error.
d. A reversed flow mode of jets fans has not been designed. Violation of C6-design error.
e. Lack of operation, wrong working instructions and poor maintenance has resulted to the degradation of the ventilation equipment. Violation of C6-migration of the tunnel system to hazardous state.

- **Flaws due to the controlled process**

The final category concerns flaws due to the fire ventilation process itself. This category may also help us to identify component interaction accidents (system accidents).

a. Atmospheric back pressure and external wind direction and velocity are out of the range the ventilation system has been designed to control. This is not regarded as a control algorithm flaw but an out of range external disturbance.
b. Process outputs that may contribute to the system hazard are:
    - High longitudinal ventilation velocity feeds the fire with oxygen and increase the heat release rate of the fire. Violation of C8-systemic factors.
    - Untenable conditions downstream the fire due to high ventilation airflow in this direction. Violation of constraint C7-systemic factors.
    - The fire ventilation mode may result in high level noise, thus disturbing communications inside the tunnel. Violation of high-level safety requirement-systemic factors.

4.2.4 Step 4: Evaluating the road tunnel safety and establishing a proactive safety strategy

After the end of step 3 of the analysis, the causal pathway leading to the accident has been described. Once the potential causes and hazards have been identified, the information of the STAMP-based road tunnel safety assessment must be provided to the Tunnel Manager and Safety Officer in order evaluate the current tunnel design, if the tunnel has been constructed, or in order to establish and enforce a proactive safety strategy, if the tunnel is under development. In this case, safety measures should be proposed that address the identified hazards.

Safety control measures that must be evaluated (or enforced) may for example include:

- Organizational procedures that enforce constraints C1-C4 as presented in Table 1. For example a quality plan or specific organizational procedures that define specific recruitment requirements, working instructions and the operator's training should exist or should be designed. Additionally, a Routine Maintenance Management System for the effective management of the maintenance of the tunnel should exist or enforced.
- Whether the ventilation-control routines (SCADA algorithm) ensure adequate response for all conceivable scenarios in the analysis as presented in 4.2.3. (i.e. people downstream the fire, need for reversed flow mode of jet fans, scenarios where some equipment is not available or where the measured data are lacking etc.).
- Commissioning and periodic tests of the ventilation system that proves its capability to achieve its requirements.
- Automated or scheduled maintenance procedures so as to examine the plausibility of anemometers and sensors.
- Organizational procedures and incident analysis processes so as to determine if the tunnel organization detects the occurrence of the above hazardous scenarios and has the ability to "learn from events".

It must be mentioned, as far as the evaluation of tunnel safety is concerned, that risk indices which imply expected number of fatalities or probabilities of events deviates from the purpose of such type of analysis which is moreover insufficient to provide this kind of information. However, if the causal factors identified by the risk assessment must be categorized somehow accordingly to their risk level, a risk matrix can be used for the evaluation process.

Risk matrices based on likelihood-consequence grids are commonly used to document the perception of the most critical risk in a system or in order to summarize the results of the risk assessment. However, since the proposed STAMP-based approach is not based on probabilities of events, a likelihood-consequence matrix cannot be provided. Therefore, an alternative approach to rank risks must be proposed. Aven (2010) gives

an alternative definition that can be used somehow in the STAMP analysis. He states that risk can be understood as the two dimensional combination of:

i. events A and consequences C of the events
ii. the associated uncertainties U (will A occur and what value C will take)

In STAMP terms, as events one may consider the inadequate control actions and control flaws identified in step 2 and 3 of the STAMP-based road tunnel safety risk assessment. The consequences of these events are the violation of the component level safety constraints. As far as their consequences are concerned, the ranking of the risks depends on which constraint is violated. In a qualitative risk matrix, a low, medium or high consequence value can be given to categorize the consequences of control flaws. For example, if we regard the constraint C7 "If people are situated downstream the fire they must not get fired" more important (i.e. its consequences are regarded more severe) than constraint C9 "The full operation of the smoke control must be achieved within 2-3 minutes from the onset of the fire", then events (i.e. causal flaws and inadequate control actions) that violate constraint C7 might take the value 'high' while those which violate constraint C9 might take the value 'medium'.

Having classified the inadequate control actions and control flaws in terms of consequences, the next step is ranking them in terms of uncertainty. How uncertain is such an 'event' to occur depends mainly on the uncertainty of the safety control measure responsible to control the particular causal event. In order to assess the uncertainty of the safety controls to be violated we propose as a metric the observability parameter, a fundamental concept of Control Theory (Brogan, 1991). For example, a CCTV (Close Circuit TV) might be used as a safety control measure for the control flaw: "The tunnel operator does not have sufficient feedback of the tunnel environment and the controlled process". The observability parameter of this safety control is high since the tunnel operator can easily observe if the control measure (i.e. the CCTV) is in operation or not. On the contrary, a safety control measure embedded in ventilation control routines and SCADA algorithm can be easily modified by the maintenance operator without anybody observing this modification. Hence, it has a low observability. As far as organizational procedures is concerned (as safety control measures), the ease with which procedures can be monitored and compliance detected, depends on various factors. For example, more complicated procedures are in general more difficult to monitor than simple procedures because there are more ways for them to be violated either intentionally or unintentionally. Furthermore, procedures that require specialized skills cannot be effectively monitored by personnel who do not have the same specialized skills. Consequently, such procedures have lower observability than procedures that require less specialized skills. Again a qualitative scale can be used to evaluate the observability parameter in a risk matrix.

In this perspective, risks are classified according to their observability and consequence. Low observability, high consequences risks are deemed to be the most

critical while high observability, low consequences risk are deemed to be less important. A risk matrix which can be used as a way of summarizing the STAMP-based safety risk assessment is shown in figure 7. However, it must be mentioned that the whole risk assessment must be provided to those taking decisions about the safety of the tunnel, since matrices are always based on a rough classification and high subjectivity from the analyst.

Observability	Consequences		
	Low	Medium	High
High	Accepted	Accepted	to be examined
Medium	Accepted	to be examined	not accepted
Low	to be examined	not accepted	not accepted

Figure 7: Risk Matrix

A final step in the STAMP-based assessment is to consider how the safety controls could degrade over time and to build protection against it in order to cope with the migration of the tunnel system in hazardous states. Protection might include, for example, planned technical audits based on the STAMP-based road tunnel safety risk assessment. The assumptions and results of the STAMP-assessment could be the preconditions for such operational audits.

5 Discussion

The analysis in the previous section showed how a ventilation system that has been designed to control fire and smoke can be proven insufficient to provide the tunnel users escape routes with tenable levels of temperature, toxicity and visibility. Moreover, the aspects that should be evaluated in order to determine its safety level have been highlighted. Notwithstanding the ability of STAMP to identify hazardous scenarios, it should be mentioned that the fire ventilation process is somehow more complex than the proposed assessment might imply. Ingason (2005) states that there is always significant uncertainty on how the tunnel ventilation affects certain fire characteristics (smoke evolution, flame length, HRR, etc.), hence there is no accident model that could reveal all hazardous scenarios when fire is the examined case. Accident models are simply a representation of reality and they must always be used in this perspective. However, it is crucial to understand that the accident model selected to perform the safety assessment is indeed the most crucial aspect and leverage in the safety evaluation process of a tunnel. The analysis of how an accident may happen provides the reality that the safety assessment must cope with. Accident models do not always focus on the same features or facets of this reality since they have been developed for different circumstances. The critical aspect is therefore to choose the one or a combination of some methods that can provide a comprehensive

and thorough analysis. The limitations of current QRAs based on fault and event tree analysis have been exhaustively discussed in Section 2 and the need for a different approach was also highlighted in Section 3.

On the other hand, the proposed method presented in this article, based on a systemic accident model, is regarded as an appropriate approach to model accidents in road tunnels, evaluate their safety and propose appropriate safety measures. The control theory and systems thinking framework of the method is regarded as an appealing construct for assessing tunnel safety because the factors (technical and organizational) that contribute to tunnel accidents are numerous, complex and interrelated. Moreover, as presented in paragraph 4.2, the STAMP-based risk assessment method succeeds in taking into consideration organizational aspects, design and software errors, systemic factors and the adaptation of the tunnel system, all aspects that current road tunnel QRAs have limitations to cope with. Following this line of thought, it is believed that the STAMP model can be helpful in the road tunnels field, particularly for the Safety Officers and the Tunnel Managers of the tunnel so as to better conceptualize the safety picture of these infrastructures. The authors believe that the application of an accident model to evaluate the overall tunnel safety as a complementary tool to traditional approaches is necessary. The analyst or/and the Safety Officer may be able to assess causal factors closely related in time and space by applying individual knowledge and expertise, but it is extremely difficult to effectively see the broad picture of the whole tunnel system and evaluate the overall safety without a systematic model.

It must be mentioned that in the present analysis the regulations and standards for road tunnels have not been analyzed. This decision has been made as the technique presented in this article refers to the Safety Officers and to the Tunnel Managers, who cannot influence or deviate from the regulations and standards. However, an analysis of the whole socio-technical system, including regulators, could be performed in the future, to evaluate the efficiency of the current standards and legislation.

Like any other model or technique, STAMP has also limitations. It cannot drive the design of specific tunnel subsystems, so simulation models must always be used when decisions concerning the number of emergency exits or the capacity of ventilation system are made. Moreover, if risk must be quantified in accurate estimates (i.e. expected number of fatalities) a STAMP-based approach will certainly be unable to provide the required results. Risk in STAMP terms is not a function of probabilities and consequences of events as described in the classical approach of risk assessment (Kaplan, 1981) but a function of the effectiveness of controls to enforce safe system. In STAMP, risk is directly related to communication and feedback. The more and better the information we have about the potential causes of accidents in our system and the state of controls implemented to prevent them, the more accurate will be our perception of risk. Thus, in such type of safety risk assessment the information provided by the STAMP analysis must be presented to the Tunnel Manager and Safety Officer (decision-makers) as a basis for risk-informed decisions or as a tool to

evaluate current road tunnels design. In this sense, decisions to be made will be based on a well described risk picture and not on some subjective risk numbers produced by probability estimates.

Finally, some may claim that the presented method seems to have similarities with Failure Mode, Effects and Criticality Analysis (FMECA) that is widely used for tunnel hazard analysis. However, FMECA is a bottom-up reliability engineering analysis technique whereas STAMP analysis is a top down safety analysis framework. Thus, the framework of the analysis significantly differs.

6. Conclusion

The evolution of accident causation models over time shows a shift from the sequence of events to the representation of the whole system (Katsakiori et al., 2009). Event-based accident models that underlie QRAs have been subject to strong criticism for their limitations to capture the overall risk picture of complex socio-technical systems and a systemic approach is adopted as an alternative approach. In the road tunnels field the need for a systemic safety assessment has also been mentioned (Santos-Reyes and Beard, 2005).This paper reviews the limitations of current QRAs in the road tunnels field and proposes a STAMP-based method as an alternative technique (or even complementary support tool) for road tunnel safety risk assessment.

The concept of STAMP-based safety risk assessment in road tunnels has been introduced and illustrated through an analysis of a tunnel ventilation system. Nevertheless, the overall safety of a tunnel can be evaluated only if the STAMP-based safety risk assessment is performed for the whole tunnel system and for all the identified accidents and their associated hazards as mentioned in 4.2.2. Particularly, dangerous driving in the tunnel, the inability of the road users to rescue themselves, the inability of the tunnel operator to effectively intervene and provide the appropriate actions and finally, the inability of the emergency services to control the incident should be analyzed with the steps of the STAMP analysis. In the whole tunnel system, the STAMP model will have the capability to examine interrelationships among tunnel systems (i.e. tunnel ventilation system, fire fighting system, fire detection system, tunnel communication system and traffic management system). Moreover, crucial elements of tunnel safety and particularly the co-operation of the tunnel operator and emergency services will be also examined in an overall tunnel safety assessment. The proposed method can be used either to evaluate a current tunnel design or to drive the design of a new road tunnel and in this work the STAMP has been complemented with a Risk Matrix in order to evaluate risk. However, future work should concentrate in developing methods and tools that have the ability to categorize the identified causal factors more thoroughly. The authors believe that in general, the STAMP technique must be supported with tools that improve the way the information provided by the STAMP analysis is presented to decision makers.

Notions of systems theory in safety may be characterized as ‘organizing common sense’ therefore a more mathematical-based risk assessment method (such as QRAs)

might be regarded with more esteem. However, it is important to understand that some properties cannot be described mathematically and this fact must not hinder the safety assessment. Indeed, the organizational and human influences on the safety level of a road tunnel are complicated enough in their causal relations and are therefore difficult to be represented quantitatively in numerical units. As a result, such factors are frequently left out of the analysis entirely, because it is argued that they cannot be estimated successfully. This means that the causal factors considered are not a comprehensive overview of aspects that have the potential to affect the overall tunnel safety, but a set of factors that can be quantitatively modeled. We conclude this article by reminding that the main benefit of assessing risk (quantitatively or qualitatively) lies in the achievement of a detailed understanding of the engineering system and this was the major concept that has driven the present work.

References

Apostolakis, G., 2004. How useful is Quantitative Risk Assessement?. Risk Analysis 24, 515-520.

Arralt, T.T, Nilsen A.R., 2009. Automatic fire detection in road traffic tunnels. Tunnelling and Underground Space Technology 24, 75-83.

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

Aven, T., 2010. On how to define, understand and describe risk. Reliability Engineering and System Safety 95, 623-631.

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).

Beard, A.N, 2010. Tunnel safety, risk assessment and decision-making. Tunnelling and Underground Space Technology 25, 91-94.

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

Brogan LW., 1991. Modern Control Theory. Prentice Hall, New Jersey.

Carvel, R.O., Beard, A.N., Jowitt, P.W., 2001. The influence of longitudinal ventilation systems on fires in tunnels. Tunnelling and Underground Space Technology 16, 3-21.

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

Dulac, N, Leveson, N.G., 2005. An approach to incorporating safety in early concept formation and system architecture evaluations. In: Lacoste H. (Ed.). Proceedings of the first IAASS conference on space safety, a new beginning, 221–226

Dix, A., 2004. Risk management takes on a key role. Tunnel Management International 7, 29–32.

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.

Garret, C., Apostolakis, G., 1999. Context in the risk assessment of digital system. Risk Analysis 19, 23-32.

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

Hardy, K., Guarnieri, F., 2010. Modelling and Hazard Analysis for Contaminated Sediments Using Stamp Model. Chemical Engineering Transactions 25, 737-742.

Holicky, M., 2009. Probabilistic risk optimization of road tunnels. Structural Safety 21, 260-266.

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

Høj, N.P., Kröger, W., 2002. Risk Analyses of transportation on road and railway from a European Perspective. Safety Science 40, 337-357.

Inganson, H., 2005. Fire dynamics in tunnels. In: Carvel, R.O., Beard A.N. (Eds.), The Handbook of Tunnel Fire Safety, 231-266. Thomas Telford, London.

Katsakiori, P., Sakellaropoulos, G., Mantakis, E., 2009. Towards an evaluation of accident investigation methods in terms of their alignment with accident causation models. Safety Science 47, 1007-1017.

Kaplan, S., Garrick, B., 1981. On the quantitative definition of risk. Risk Analysis 1, 11–28.

Khoury, G.A., Molag, M., 2005. Actual time tunnel safety-A new approach. Tunnels and Tunelling International 37, 46-48.

Kirytopoulos, K. Rentizelas, A. Kazaras, K , Tatsiopoulos, I. 2010a. Quantitative operational risk analysis for dangerous goods transportation through cut and over road tunnels. In Ale, B. Papazoglu, I. & Zio, E. (eds.), Back to the future. Proceedings of European Safety and Reliability Conference 2010 (ESREL 2010), Rhodes, Greece, 5-9 September 2010, 167-172.

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

Lacroix, D. 2001. The Mont Blanc Tunnel fire: what has happened and what has been learned. Proceedings of the 4th International Conference on Safety in Road and Rail Tunnels, Madrid, 2-6 April 2001, 3-16.

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

Leveson NG. 1995. Safeware: system safety and computers. Addison-Wesley.

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

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

Leveson, N.G., 2011b. Engineering a safer world: Systems Thinking Applied to Safety (Engineering Systems), MIT Press, Cambridge, MA.

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 47, 1297-1311.

Mohaghegh, Z., Mosleh. A., 2009. Incorporating organizational factors into probabilistic risk assessment of complex socio-technical systems: Principles and theoretical foundations, Safety Science 47, 139–1158.

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

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

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 53, 115-126.

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

PIARC, 2007. Integrated Approach to Road Tunnel Safety, 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.

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 48, 544-555.

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

Reason, J., 1990. Human Error. University Press, Cambridge, UK.

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

Santos-Reyes, J., Beard, A.N., 2005. A systemic approach to tunnel fire safety management. In: Alan Beard and Richard Carvel, (Eds.) The Handbook of Tunnel Fire Safety, 389-406. Thomas Telford, London.

Skogdalen, J., Vinnem, J. 2011. Quantitative risk analysis offshore-Human and organizational factors. Reliability Engineering and System Safety 95, 468-479.

Steen, R., Aven, T., 2011. A risk perspective suitable for resilience engineering. Safety Science 49, 292-297.

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. In Piccinni (ed.), ESREL;Proc. International Conference in Safety and Reliability, Torino, 16-20 September 2001.

Xiaobo, Q., Quiang M., Vivi Y., Yoke., H.W., 2011. Design and implementation of a quantitative risk assessment software tool for Singapore road tunnels. Expert Systems with Applications 38, 13827-13834.

Zarboutis, N., Marmaras N., 2007. Designing of formative evacuation plans using agent-based simulation. Safety Science 45, 920-930.

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

Figure Captions