Engineering Safety

With applications to fire safety design of buildings and road tunnels

by

Henrik Bjelland

Thesis submitted in fulfillment of
the requirements for the degree of
PHILOSOPHIAE DOCTOR
(PhD)

Faculty of Science and Technology
Department of Industrial Economics, Risk Management and Planning
University of Stavanger
Norway
2013

University of Stavanger.
N-4036 Stavanger
NORWAY
www.uis.no

ISBN:	978-82-7644-549-7
ISSN:	1890-1387
Thesis no.:	207

PREFACE

The motivation for this work emerged during the work with my Master's thesis in 2009. Moreover, after five years as a professional fire safety engineering consultant, it was liberating to be able to dig into the problems that so often had made professional life frustrating. Engineering in real life turned out to be something more than what is taught at the universities. The dimensions the problems take on are often different and more multi-faceted, and, in reality, a professional cannot spend years searching for a perfect answer. The needs are urgent: the new school is needed before next semester; the shopping center must be renovated in time for Christmas shopping; the arena must be prepared for a large concert in two months, and the tickets are (of course) sold. Decisions need to be taken based on the available knowledge. Hence, my aim was to get a better understanding of these engineering problems and contexts and, maybe, to contribute to some development in the field. This thesis is submitted with that goal and in fulfillment of the requirements for the degree of Philosophiae Doctor (PhD) at the University of Stavanger.

My main interest is safety design, which involves applying concepts from different branches of research in order to design and build useful and safe artifacts. The chaos of different perspectives and viewpoints has made it an interesting, and sometimes frustrating, journey. Research into a new concept seldom leads to instant clarity but usually reveals its multiple perspectives and interpretations from different philosophical and professional fields. To dig deeper often leads to realizing that one should be an expert in so many fields, only to find out that time is limited.

This also illustrates the complexity of professional design. Everyone is involved, on some level, in designing for themselves, in their own lives. In this individual sense, however, this type of design often involves small projects and non-critical decisions. Moreover, the concepts, goals and values are usually clearly defined: they are your own. However, designing in the professional sense is about synthesizing conceptions, goals and values from all relevant stakeholders, which are often conflicting. Different stakeholders hold different perspectives on important concepts. Some are even unaware of what perspectives (in a theoretical sense) they have, but all of them have some goals and values. In some cases, however, these goals may only be tacitly known. The stakeholders are unaware of what they actually want before their tacit goals and values are triggered by the design process. This is why design processes often are non-linear.

A rule of thumb in the professional design process is that the more people involved, the more complexity is added to the design situation. The challenge is, in a way, to both *compromise* and *not compromise* at the same time. That is, you should include all stakeholders' values and goals and create a design that all of them judge as the best solution possible. What you want to avoid is a design that all stakeholders judge as mediocre, or one that a few important stakeholders judge a total failure, for instance, the "safety stakeholder". It basically seems like an impossible task. This is also what makes it so interesting.

The thesis is written for an audience of safety engineering professionals and safety regulators in general and those operating within the field of fire safety engineering in particular. I hope that it manages to challenge the current way of thinking about safety engineering, especially in the way we think about knowledge for design.

ACKNOWLEDGEMENTS

Professor Ove Njå has been my supervisor during the project. I greatly appreciate the work you have put into this and the way you have shown me how to think creatively and critically as a researcher. Your positive enthusiasm and devotion to knowledge is inspiring. Dr. Atle William Heskestad has been my cosupervisor. Thank you, Atle, for interesting discussions and your contributions to papers and the dissertation.

The University fund in Rogaland has been the main sponsor of this work. Their contribution and willingness to invest in safety research is gratefully acknowledged. Multiconsult, my employer for nearly nine years, has also been an important sponsor of this work. I especially want to thank my former managers, Ari Soilammi and Kjell Bjarte Kvinge, for getting the wheels going, and my current managers, John Erling Strand and Kristin O. Augestad, for patiently seeing the work come to a finish. I am grateful for being part of a company that finds this kind of work worthwhile and for my inspiring colleagues at the section for Fire and Risk Consultancy.

At the University of Stavanger, I have to thank all the staff members at the library and the Ph.D. coordinator at the Faculty for Science and Technology, Elisabeth Stornes Fiskå. The service you are providing is exemplary and has made my work much easier. Professor Terje Aven is also greatly acknowledged for his contribution to one of the papers and for inspiring thoughts about risk and scientific work. As a visiting Ph.D. student, I also appreciate the efforts of Hans Jacob Fevang, Head of Institute, for getting me comfortably seated in an office at the university whenever I visited.

The Ph.D. work has provided me with the opportunity to participate in both national and European standardization work. The introduction to the complicated world of standards has been very interesting and insightful, especially the discussions on the status and future of fire safety engineering in Europe. Hence, I want to thank the former and current heads of the committees SN/K 227 (Standards Norway), Wiran R. Bjørkmann and Lisbeth Landfald, and of CEN TC 127/TG1 (Comité Européen de Normalisation), Dr. Jöel Kruppa and Dr. Daniel Joyeux, for letting me participate and contribute. Moreover, I would like to thank Michael Strömgren (SP Technical Research

Institute of Sweden), Caroline Cronsioe (Swedish National Board of Housing) and David Tonegran (Tyréns), for letting me in on the collaboration for a paper written to the Society for Fire Protection Engineers-conference in Hong Kong 2012.

I would also like to thank my former colleague and "Ph.D. colloquium member," Anders Arnhus, fellow Ph.D. students at the Institute for Industrial Economics, Risk Management and Planning, and especially Audun Borg. Thank you very much, Audun, for your contribution to papers and the dissertation and for pleasant lunch and dinner conversations at the university.

The property owners who contributed with documentation from construction projects and the project management in the Rogfast project are gratefully acknowledged for their contribution to the data.

Finally, I thank my family and friends for continuous support and patience. Without the love and support from my fiancée, Ulla, I could not have finished this thesis. Thank you very much for your prolonged patience, for keeping me going and reminding me that there are also other important things to life than safety research. I look forward to spend more time with you and the coming baby.

Røyse, July 5, 2013

Henrik Bjelland

SUMMARY

A continuously changing and increasingly complex society leads to new challenges in safety design. Modern buildings and road tunnels are being packed with new technology that creates new failure modes, multiple sub-system interactions and tight couplings between different socio-technical systems. Meanwhile, safety is largely designed into these systems using prescriptive design rules that have evolved through reactions to accidents in systems with limited resemblance to modern systems.

The traditional prescriptive approach to safety design was developed to avoid the re-occurrence of previously experienced accidents. New types of systems and accidents need a different design philosophy. The focus should be on the future instead of the past. Hence, the following question was outlined as the major issue of this thesis: *what promotes and inhibits performance-based safety management of design processes?*

Performance-based design principles and regulations are nothing new. In Norway, performance-based fire safety legislations were introduced in the onshore building industry in 1997, and the international fire safety science community had a great focus on promoting these issues during the 1990s. However, experience with the performance-based legislation regime shows that the majority of fire safety designing activity is still based on prescriptive design rules, even in the most novel and complex cases. This is an unfortunate practice, considering that the prescriptive design rules have a boundary of validity associated with historically appropriate designs. Another matter is the restricted empirical foundation for the prescriptive design rules. Accidents are relatively rare events in socio-technical systems. Hence, the 'test of time' is a rather weak test in terms of determining the appropriateness of the prescriptive design rules. Strengthening the performance-based alternative to safety management of design process is thus of major importance.

Four research questions were developed to support the major issue. The research questions were associated with: (1) understanding current fire safety engineering practice, (2) investigating the scientific foundation of the concepts of fire safety level and safety margin, (3) investigating methodological challenges associated with current practice, and (4)

transforming the understanding associated with current challenges into proposals for improvement. The research was limited to issues associated with engineering practice, safety science and safety regulation, explored through six case studies:

A. A study of fire safety engineering practice in Norway in the period from 1997 to 2012.
B. A study of fire safety science's treatment of major concepts associated with the measurement of safety levels and safety margins.
C. A study of 40 different technical fire safety strategies (combinations of safety measures) for multi-story residential apartment buildings.
D. A study of the application of an engineering methodology to a specific design example: a concert hall.
E. A study of the risk analyses and uncertainty management process in the Rogfast road tunnel project.
F. A study of the application of a Bayesian Network model for risk analysis in road tunnels generally and in the Rogfast tunnel specifically.

The data the case studies dealt with has mainly been written documents, either collected from the different projects or through literature surveys associated with the topic. Documents have been analyzed using qualitative text analyses, except for case studies C, D and F, which also include quantitative risk and fire modeling approaches.

The major finding of the project is that there is a mismatch between current fire safety engineering practices and fire safety science. Fire safety engineering practice builds largely on the application of prescriptive design rules. Deviations from these design rules are often made, and the consequences of these deviations are often documented qualitatively using engineering judgment and argumentation. Fire safety science, on the other hand, builds on a rather narrow scientific framework, greatly inspired by the natural sciences. Fire safety is preferably measured by the application of quantitative relationships and models. The type of qualitative knowledge reflected by the fire safety engineering practice is poorly reflected in fire safety science, and the type of quantitative rigor reflected in fire safety

science is poorly reflected in fire safety engineering practice. Obviously there is a need to increase the common understanding.

I argue that the scientific framework for fire safety science is too narrow to capture the essence of the concept of fire safety. The traditional framework builds on scientific reductionism, which leads to great simplifications in the treatment of systems and environmental complexity and excludes critical issues that are difficult to quantify dependably. Examples of the latter are human and organizational behavior. Similar conclusions are drawn with regards to the risk concept from the Rogfast cases. Overemphasis on model concepts, such as relative frequencies or universal causal structures, excludes the individual knowledge safety experts may bring to the table in novel designs.

An alternative scientific framework is suggested, which builds on a constructivist systems thinking perspective. A fundamental assumption is that complex socio-technical systems, such as certain modern buildings and road tunnels, are modeled as social hierarchies. The macro-level includes social institutions, such as national safety authorities and fire departments, while the micro-levels include the building's components, sub-systems, and nuts and bolts. Fire safety, then, is a property of the system as a whole and cannot be associated with any lower layer in the hierarchy, for instance by only considering the technical infrastructure or the reliability of an automatic sprinkler system. Moreover, complex socio-technical systems are constantly adapting to changes within themselves and in the environment. Hence, safety design is a matter of creating a control structure that enables the system to change in a safe manner.

Application of the proposed framework would lead to a more holistic approach to safety design, regardless if one applies a risk-based methodology or a systems safety methodology. For instance, it would broaden the view on what knowledge is relevant in design processes and what measures could be used to achieve safety. Knowledge associated with the individual engineer's experience would become more important. This knowledge may be tacitly known, and works, for instance, in terms of how the engineer creatively frames and reframes design problems to the stakeholders' needs. A holistic perspective on safety measures includes, in principle, all thinkable measures, and not only those measures associated with quantitative knowledge. A consequence of this would be that mathematical rigor would have to give way to more qualitative and discursive decision processes. Alternative processes and supplementing methods to traditional quantitative modeling and analysis for determining quality and coherence of the documentation would have to be developed.

Table of content

PART I

1 INTRODUCTION

A valuable thesis about safety engineering, with special focus on fire safety design of buildings and road tunnels, is, to me, a thesis about how to deal with the increased complexity of socio-technical systems. Is current safety engineering practice appropriate for the tasks at hand?

Fire safety engineering is often contrasted with fire safety designing by prescriptive design rules, by making a reference to scientific and engineering principles. For instance, Hurley (2009) defines fire safety engineering as the *"application of science and engineering principles to protect people and their environment from destructive fire."* In this context *science* and *engineering principles* generally mean *natural science* and *quantitative engineering principles*, such as models, empirical relationships and simulation tools (Bjelland, Njå, Braut, & Heskestad, Submitted). But science is more than the natural sciences, and engineering principles may be more than quantitative models. Hence, a fundamental question is whether we have the appropriate scientific foundation for our fire safety engineering practice, or could there be valuable contributions from other fields as well?

A major contribution to knowledge from this thesis is increased understanding of the capabilities and limitations of modern fire safety engineering practice. Broadly speaking, a large part of the capabilities may be attributed to the breadth of engineering knowledge and skills, while a large part of the limitation is associated with how this knowledge is utilized in a normative scientific and regulative framework. This insight emerged from exploring and contrasting current safety engineering practice with the needs and nature of design projects. Hence, a contribution to knowledge is also the innovative application of existing knowledge in the fields of design science and systems thinking to the field of fire safety design and engineering.

1.1 Complexity of socio-technical systems

During the 20th century, we saw enormous changes in the way we live our lives, in the way we work, in the technology that surrounds us, in the ability to create impressive structures, and in the sciences, to name a few (Funtowicz &

Ravetz, 1992; Leveson, 2011b). A consequence of modernity is increased complexity in buildings and infrastructures. During the late 19th century, the first modern city building codes were established in Norway, due to urbanization and risk associated with large city fires (Stenstad, 1983). More buildings in smaller areas led to tighter couplings, using Charles Perrow's (1999) term. The major aim of the fire codes was to prevent fire spreading between buildings; the means was the enforcement of fire resistant materials, such as brick and masonry walls.

The buildings as such were not that complex at that time. The amount of available construction technology limited their size, and controls within the structures were largely manual or mechanical, for instance the opening/closing of windows and doors and locks. Today, modern buildings are packed with technology. What used to be controlled by humans directly or by mechanical means are now often connected to electromechanical controls dependent on computers and software. While previous systems, sub-systems and components were largely segregated and loosely connected, modern systems are integrated – causing interactions and dependencies that are both unanticipated and unwanted (Leveson, 2004, 2011b; Perrow, 1999, 2011). Moreover, developments in construction technology mean that our imagination is the most effective boundary of increasingly taller buildings serving multiple societal needs. For instance, an urban building may be a subway station below the ground level, a shopping mall on the ground and first floor, and contain offices, hotels or apartments on the remaining floors.

The work of this thesis has been directed at the fields of fire safety design, using buildings and road tunnels as objects for the study. What we find in these fields is that a set of *accepted safety solutions* (prescriptive codes) has a great impact on the way thinking about safety is conducted in design. These solutions are based on experiences with previous buildings and road tunnels that over time has made them references of what is to be acceptable safety. We can say the solutions, or design rules, has not yet been falsified, using Popper's terms (Blockley, 1980). However, are we sure that these experiences are still relevant in the world we live in today and for the future? Moreover, are we sure that previous experiences are a good source of knowledge for safety design? Serious accidents are rare. The absence of a serious accident during some time period is not necessarily good evidence for not having a serious accident in the future. To paraphrase Law & Beever (1995:79): *The fact that no babies have been killed due to a fire in a parking building is poor evidence of the success of the prescriptive fire safety codes*. When technology is moving as fast as it does today, there is no possibility of gaining widespread experience with design rules before they are implemented (Leveson, 2011b). Thus, there is an urgent need for scientific and engineering principles to support design decisions.

1.2 Science and scientific

The underlying scientific framework is crucial to understanding the worldview of any professional discipline. In the early 20th century, the scientific landscape was influenced by the logical positivists (see section 2.1). For them, the only meaningful propositions worth considering were either analytical, such as logic and mathematics, or empirical, which express knowledge of the world (Giere & Richardson, 1996; Godfrey-Smith, 2003; Schön, 1991; Stadler, 2003). According to Schön (1991:33-34):

> *Practical knowledge was to be construed as knowledge of the relationship of means to ends. (…) The question, "How ought I to act?" could become a scientific one, and the best means could be selected by the use of science-based technique."*

According to the logical positivists, then, there is no fundamental difference between science, engineering and decision making. Engineers should apply science to measure the level of risk or safety and make a scientifically sound decision. In this framework, science and engineering principles are not supporting decisions but practically making the decisions.

For instance, research in the social sciences has shown that science is not objective and universally true, as the positivists liked to believe. Data from experiments are based on our underlying models and conceptions and are, thus, value-laden (Checkland, 1999). Moreover, complex socio-technical systems are not suitable to study by repeating experiments (Blockley, 1980; Blockley & Godfrey, 2000). The question of what is the correct action in a high-risk technology project cannot be decided by science alone.

In systems thinking, the concept of a system *"embodies the idea of a set of elements connected together which form a whole, this showing properties which are properties of the whole, rather than properties of its constituent parts"* (Checkland, 1999:3). Properties such as safety or accidents may be seen as such holistic properties of the system (Blockley & Godfrey, 2000; LeCoze, 2005; Leveson, 2004, 2011a, 2011b; Leveson, Daouk, Dulac, & Marais, 2004; Wallace & Ross, 2006). A holistic system property can only be found or described at a macro level of the system. A common example is the "wetness of water," which cannot be found by looking at the individual hydrogen and oxygen atoms. The traditional way of dealing with complexity in the natural sciences is by decomposing the system into its constituent parts, to atoms and electrons, and then try to explain how the system functions as the sum of these constituent parts. This is called scientific reductionism. Complex socio-technical systems do not submit well to scientific reductionism without losing important understandings of holistic system characteristics. The systems studied by the natural sciences are stable. The system is what it is no matter what a scientist might believe about it. However, changes occur continuously in complex socio-technical systems, and the scientists' predictions about system behavior also have the potential to change future behavior (which should be a relief to managers of such systems) (Checkland, 1999).

An engineering approach influenced by social science and systems thinking may lead to a more constructivist worldview (LeCoze, 2012; Wallace & Ross, 2006). In such a framework, science and engineering principles are seen as tools for producing decision support (Aven, 2012a; Nilsen & Aven, 2003). The results presented by engineers and risk analysts, for instance, are not objective values representing the truth but are, rather, descriptions of uncertainty or knowledge that are dependent on the analyst's or engineer's background experience and knowledge.

1.3 The power of truth: decision making

Authors such as Shrader-Frechette (1991), Beck (1992) and Perrow (1999) make a connection between the technical rationality regime and power structures in the society. A major concern is that people or organizations with power may, with the help of scientists, engineers and professional risk analysts, impose risks on people who are uninformed or ignorant about the risks. If science tells us that the risk of a certain technology is low, then it must be so, and it would irrational to believe otherwise. Beck and Perrow are strong critics of risk analysts. They argue that risk analysts are claiming that they know the truth about risk. Risk analysts see the public as ignorant regarding risks and that, if properly informed, the public will adjust their perception of high risks to the scientifically correct view. This builds on an assumption of risk analysts sharing the positivists' values.

However, engineers are seldom acting solely in their own interest. They are usually working as consultants for resourceful actors in the society, e.g., property developers, industrial entrepreneurs or governmental agencies. It will surely be in the engineer's own economic interest to provide the answers their clients want, which may cause a conflict between attending to the well-being of the client or the ethics of the profession (Funtowicz & Ravetz, 1992:257). However, they are not necessarily "committed to the cause" or benefitting from the activities the same way their clients are. One day an engineering company may work with the nuclear industry, while the next they are concerned with solar energy or providing consulting services to environmental organizations. Those most interested in using the "weapon of truth" are not the engineers but, rather, their clients, who need support for their case or project. If it could be argued that the engineers or risk analysts are presenting the truth and nothing but the truth (as they say in the courts), they would be considered far more credible than if they started questioning their theories, models and methods.

Hence, it is open to question whether or not the focus on technical rationality and the accompanying focus on truth and objectivity comes from within the engineering discipline or from their clients, whoever they are. Moreover, it is open to question to what degree risk analysts or engineers really care about issues related to the truth content of the theories they apply. Nevertheless, a fundamental assumption for this thesis is that engineers *should care* about the implications of their theories and the scientific foundation of their profession. Otherwise, engineers may become "useful puppets" for any social actor with resources and a cause.

It has been pointed out that engineers contribute little to the public debate about politics and societal development (see, e.g., Anon, 2003; Gram, 2012; Haugstad, 2010, 2012; Lamvik, 2001). It is suggested that this lack of interest in the public debate is due to engineers' being *"very cautious giving public statements about something they do not have definitive answers to"* (Haugstad, 2012). Other views are that *"engineers would rather solve problems than talk about them"* and that the role of a public debater *"is not desirable to engineers, as it may be seen as a way of creating problems rather than solving them"* (Drevon, 2013). This suggests a picture of engineers as cautious and conservative professionals with a tight connection to their clients. Obviously, there is a desire to avoid conflicts with previous, current and future clients. The picture of engineers as problem solvers is probably a good one. However, it could be questioned whether or not engineers are solving the right problems. This is associated with how scientific principles and theories are perceived, the engineers' role in the design processes and the nature of design processes.

1.4 The design task and dynamic societal values

Designing and engineering is about balancing different stakeholders' requirements and needs while having in mind general societal values and professional rigor and ethics. The major challenge is that, while designing, we are unable to be certain about how the artifact will perform. The quality of the design, meaning its real performance relative to some performance criteria, will reveal itself only after the artifact is put into use or operation. At the time of design, we must rely on predictions about how it will perform. This introduces challenges about knowledge. What knowledge is relevant or appropriate when we are to make predictions about the future performance of an artifact? To what extent can we rely on knowledge from the past, from comparable designs and their performance? How much reliance can we place on our engineering models and methods derived from the natural sciences and empirical evidence? Who has the reliable and appropriate knowledge to analyze and make decisions about the future performance of artifacts?

By creating a new artifact, we are changing the world to some extent. For instance, one could say that the introduction of skyscrapers has changed the world in many ways, and one of them is by creating a new target for terror. At the time the first skyscrapers were designed, the shortage of land in big cities was the main concern, and one can imagine that the predicted performance of the buildings was largely associated with how the land-shortage concern was tackled by the new design. However, safety was also a concern. It is claimed that the specific event of a plane crash was considered by the designers of the New York City Twin Towers, although the criteria and execution of the impact assessment is not documented (Shyam-Sunder, 2005:55). Evidently, the towers did withstand the collision impact, and it is suggested that the progressive collapse was initiated by the fire that followed. There are, however, different theories of how the fire caused the initial collapse, two of which are presented in Quintiere et al. (2002) and Usmani et al. (2003).

The symbolic value of the Twin Towers in 2001 was not a direct result of the design characteristics of the buildings. Such values are created when the artifact and its content and users interact with the society, and these values are constantly changing. One can say that the events on 9/11 changed the world, or, since the world is constantly changing, maybe it is more precise to say that the events *showed* that the world had changed. The events made it clear that high-rise buildings should be evaluated against performance criteria related to terror attacks. This might not have been precisely acknowledged during design, and the events were a milestone in the world development regarding design loads. Furthermore, this illustrates that the values we (the society) place on artifacts today are not necessarily the same in the future. The artifacts, including their content and activities, and large events, such as terror attacks and fires, are changing the world, the way we look at it and the things we value. This has consequences for design and engineering. The artifacts we considered good yesterday might be considered dangerous today. This makes evaluation of the quality of design a relative question.

Consider the Norwegian *Grue church fire* in 1822, when as many as 113 people were killed. In hindsight, it was found that the church's doors had two major design flaws. First, the opening direction was *into* the church; second, when placed in the *open position* they also blocked the passage from the upstairs galleries. Reports from the fire say that a stampede occurred when people rushed towards the doors, causing increased pressure on the doors from the inside, rendering them unable to open. Consequently, people were trapped inside the church, especially those seated on the gallery (Østberg, 1897). It is said that it is as a consequence of this fire that the present Norwegian fire safety regulation (KRD & MD, 2010) specify that all doors in means of egress should have an outward direction. It is also interesting to note that the galleries were reserved for unmarried women and that only seven grown men were among the fatalities, which points to some social characteristics of the time (Østberg, 1897). Nevertheless, the Grue church fire created awareness about fire risk that was not present before the event. The church was probably considered safe up until the day the fire occurred. The hazard associated with the doors was not recognized before the fire.

As a final example of how the changing world affects our values and performance criteria, consider the social development in Norway during the last century. Along with the member countries of the *Organisation for Economic Co-operation and Development* (OECD), Norway experienced economic growth during the 1960s and 1970s. Moreover, optimistic predictions for continuous economic growth were made. Then, oil was found in the North Sea in the early 1960s. In 1973 the *Organization of the Petroleum Exporting Countries* (OPEC) proclaimed an oil embargo to punish countries that supported Israel in the Yom Kippur war. The embargo led to greatly increased oil prizes, which, of course, was very positive for Norway's economic growth (Bjerkholt, Offerdal, & Strøm, 1985). Hence, the oil and gas activities are a major reason for Norway's economic position today. During the depression years before the Second World War and during the reconstruction of the nation after the war, the basic needs of the population were prioritized. However, economic growth and "well-being" leads to new opportunities and priorities.

The *Norwegian Opera house* was opened in Oslo in 2008. The building is designed by the well-known Norwegian architect company *Snøhetta,* which also was responsible for the design of the recognized *Bibliotheca Alexandrina* in Egypt. Compared with the largest skyscrapers in the world, the Norwegian Opera house is modest in its dimensions. However, the building is a good example of an artifact that is something more than just a building to cover basic needs. The building is, rather, the result of a design idea that integrates the necessary functionality, internal and external beauty, landscaping details and the creation of a landmark. We could also say that the building is a result of the Norwegian wealth and ability to see the world with new eyes, that is, to develop what we consider as important values in a building.

As previously mentioned, designing is about balancing the concerns from different stakeholders. Some of the examples may seem a little far-fetched, but the point is that changes in the world we live in lead to different priorities and values. These are dynamic, not static, values that are affected by a complex and globalized world. The continuously changing world will lead to new needs in the society. Developments in technology will drive new and novel designs forward, and our needs and worldview will affect the values we use when balancing different concerns. The way we deal with different concerns in design and engineering thus needs to be flexible. However, this is not the same as saying that our values are completely relative, and that, for some good reason, for example, we can forsake safety at the benefit of, for instance, beauty, functionality or cost. Rather, we should be aware of what we mean when we talk about safety, for instance, fire safety in a building or a road tunnel. Safety with regards to a design is not an end, or goal, in itself. If safety comes at a too high cost of other important concerns, the design will probably not be realized. Again, finding the right balance is the key.

1.5 Major issue and research questions

The work associated with this thesis is best regarded as an exploratory journey. The starting point was defined in terms of research into the issues of risk management and technical safety in the Norwegian fire safety engineering field. Otherwise, the road was fairly open. The following major issue was developed to give directional guidance during the research:

> ***What promotes and inhibits performance-based safety management of design processes?***

The major issue is broad in terms of asking *what promotes and inhibits*. For reasons discussed in the opening of section 1, it was decided to focus on engineering *practice*; safety *science*, and; safety *regulations* (cf., Figure 1). If performance-based safety design is to have any impact on the novel designs of the future, there is a need to have a clear understanding of the limitations and possibilities of the way we work, think and state societal demands.

The concepts that are applied in engineering practice are closely connected to their scientific foundation. This is often forgotten, or taken as given, by the practitioners. During periods characterized by change, for instance after implementation of, and adapting to, a new regulation regime, the fundamental understanding of important concepts become vitally important. It is no longer possible to rely on the agreed-upon practice and common understanding. Normal science and practice develops, in Thomas Kuhn's (1996) terms, towards a paradigm change. There is the possibility of "sticking with the old" as far as possible or developing something entirely new. In any case, current practice needs to be understood: both the practice on the "scientific side" and the "professional side" involving consultants/engineers. Figure 1 depicts the two major targets of research, the domains of "practice and knowledge" and "safety management," and a link between them. The assumption is that all that is included in practice and knowledge affects how safety management is conducted. Moreover, current safety management models affect practice, for instance with regards to where we search for knowledge. In both domains, we need to ask: What are the consequences of sticking with the old? What are the limitations, and what are the opportunities? Is there a need for a change of practice, both in science and practice? Are the old knowledge and practice compatible with future needs? What are the future needs, and whose needs are they? How do these issues affect safety management?

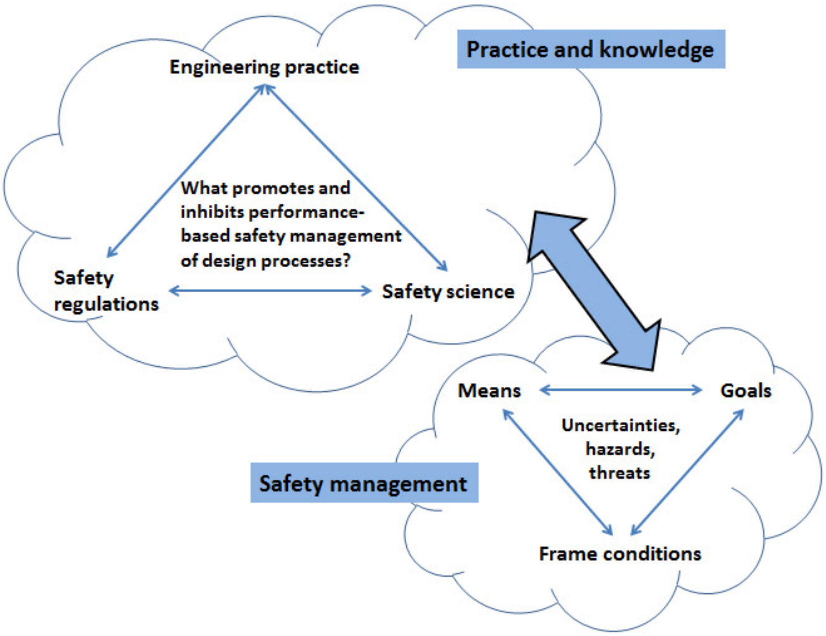

Figure 1: Major issues and research focus connected to a model for safety management (Aven, Boyesen, Njå, Olsen, & Sandve, 2004:68).

Based on this starting point, it was considered important to gain an understanding of the current fire safety engineering practice and science. The introduction of goal-oriented safety regulations in several sectors during the last decades has promoted the use of risk management and scientific engineering principles. This led to the development of the first research question:

- *Research question 1:* What characterizes current fire safety engineering practice after the introduction of performance-based regulations and promotion of scientific engineering principles? (papers 1, 2 and 3)

A major reason for implementing a performance-based fire safety legislation regime was to allow alternative solutions that provided the same level of safety at a lower cost, or a higher level of safety at equal costs. Another reason was that the prescriptive legislation simply did not fit for novel and complex designs. New measurements for safety, such as risk and fire modeling, were thus promoted by the authorities in cases where one deviated from the prescribed design rules. In the work associated with research question 1, I set out to increase understanding of how this new legislation regime was adopted by the fire safety engineers. How did they relate to the new freedom of choosing alternative solutions? How did they build documentation that showed that the designs had an appropriate level of fire safety? How did they relate to the new[1] concept of risk, which was suggested as an appropriate measure of fire safety?

As a consequence of the findings from the initial studies, it was decided to look into the understanding of some major concepts within fire safety engineering. The concepts of “safety” and “safety level” were chosen, with an aim to identify not only how the fire safety science community thinks about these concepts but also whether or not there is a need for broadening understanding. Hence, the following research question was developed:

- *Research question 2:* How are the concepts of “safety” and “safety level” reflected in the fire safety engineering research community? (papers 4 and 3)

Another finding from the initial research into current engineering practice identified some characteristic methodological issues. When analytical tools are introduced to fire safety engineering processes, there is a great focus on “relative safety” through “comparative analyses.” That is, a design alternative is analyzed in comparison with a “prescribed” design alternative. Focus is on the differences, and everything else is assumed to be equal. Research question 3 was developed in order to investigate the consequences of such a methodology:

- *Research question 3:* Why are current fire safety engineering practice, fire safety science and fire safety regulations focusing on “relative safety” and the associated “equivalence approach” for evaluating fire safety levels? (papers 5, 6 and 7)

---

[1] The risk concept itself is not new (see, e.g., Bernstein, 1996; Covello & Mumpower, 1985), but it was new to the fire safety engineering industry.

While the three first research questions deal with current practice, the final research question is associated with the future. The research is founded on the findings from current practice from the perspective of how things might possibly be done differently:

- *Research question 4:* What can we learn from current engineering practice, safety science and regulations in order to promote performance-based safety management of design processes in the future? (papers 4, 7 and 8)

The major results are presented in Section 6 and in the papers in Part II.

1.6 Theoretical prerequisites

In order to answer the research questions presented in the previous section, a theoretical platform is needed. This platform is presented in section 2 and 3, but first I will give a brief explanation of the theoretical perspectives that are selected.

Searching for answers to the research questions solely within the engineering sciences, typically those associated with the technical rationality framework or positivism, seemed futile. For instance, there has been discussion about “acceptable risk” for decades (Aven, 2007; Fischhoff, Lichtenstein, Slovic, Derby, & Keeney, 1981; Kaplan, 1982; Kaplan & Garrick, 1981; Starr, 1969). However, no one has come any closer to a definitive answer in terms of finding “the acceptable level of risk.” A possibility is that there are no such universally acceptable levels of risk. Rather, risk and safety are properties that cannot be associated only with the activity in question but must also involve elements from who is analyzing risk and safety. If this is the case, there is a need to broaden the scientific perspective on what is relevant knowledge in safety engineering. Elements of practitioners’ tacit knowledge, creativity and experience may play an important role in achieving functional and safe designs. Designing for safety is not just about solving problems but also about finding the right problems to solve – which makes the activity more than an exercise in logic and mathematics.

From this background it was decided to include a discussion of philosophical issues associated with the technical rationality paradigm and an alternative, and more appropriate, holistic perspective. Also, it was decided to include elements from design science, for two reasons: First, findings from the design science literature are an empirical foundation to my own case studies, for instance with regards to how designers may think and act and how design processes evolve. Secondly, this project *is* design science, i.e. research associated with the activity of fire safety design, which, in my opinion, calls for an introduction to the field.

1.7 The structure of this thesis

This thesis comprises two parts: Part I provides a general background and a description of the major research questions. Furthermore, it provides a theoretical foundation for design science, risk management and associated concepts, along with methodological issues.

Part II contains the research papers that have been written in association with this Ph.D.-project. Eight papers have been included in the thesis:

1. Bjelland, H., & Njå, O. (2012a). *Fourteen years of experience with performance-based fire safety engineering in Norway – lessons learned*. Paper presented at the 9th International Conference on Performance-Based Code and Fire Safety Design Methods.
2. Bjelland, H., & Njå, O. (2012b). *Interpretation of safety margin in ASET/RSET assessments in the Norwegian building industry*. Paper presented at the 11th International Probabilistic Safety Assessment and Management Conference (PSAM11) and The Annual European Safety and Reliability Conference (ESREL2012).
3. Bjelland, H., & Njå, O. (2012d). *Safety factors in fire safety engineering*. Paper presented at the Advances in safety, reliability and risk management: proceedings of the European Safety and Reliability Conference, ESREL 2011, Troyes, France, 18-22 September 2011.
4. Bjelland, H., Njå, O., Braut, G. S., & Heskestad, A. W. (Submitted). A Discussion of the Concepts of Safety Level and Safety Margin: Applications in Fire Safety Design for Occupants in Buildings.

5. Bjelland, H., & Njå, O. (2012c). *Performance-based fire safety: risk associated with different designs*. Paper presented at the Advances in safety, reliability and risk management: proceedings of the European Safety and Reliability Conference, ESREL 2011, Troyes, France, 18-22 September 2011.
6. Bjelland, H., & Borg, A. (2013). On the use of scenario analysis in combination with prescriptive fire safety design requirements. *Environment, Systems & Decisions, 33(1):33-42*.
7. Bjelland, H., & Aven, T. (2013). Treatment of Uncertainty in Risk Assessments in the Rogfast Road Tunnel Project. *Safety Science, 55:34-44*.
8. Borg, A., Bjelland, H., & Njå, O. (Submitted). Reflections on Bayesian Network models for road tunnel safety design: A case study from Norway.

2 SCIENTIFIC PLATFORM

The underlying scientific framework of an engineering discipline will affect, for instance, what is regarded as meaningful questions to pursue and what knowledge is relevant to answer the questions. In that respect it may be useful to pinpoint some major contrasts in how science is perceived by different philosophies of science and how this has affected safety science. The general scientific foundation for safety and risk assessment in the engineering disciplines are what may be called *Technical Rationality* (TR) (Blockley & Godfrey, 2000; Schön, 1991; Wallace & Ross, 2006). Section 2.1 aims to clarify what is meant by TR in this context. The complexity dealt with by the social sciences and in systems engineering requires a broad scientific framework. In this context it has been suggested that the TR framework is unsuitably narrow (Checkland, 1999; Wallace & Ross, 2006). To contrast the paradigm of TR, we take a look at some features of alternative theories in section 2.2, which I have come to favor over the traditional TR perspective in engineering. In section 2.3 I discuss some implications of these contrasts and historical developments into the interpretation of major concepts of safety science and how this discussion can be related to fire safety science and engineering.

2.1 Technical rationality

A fundamental contrast within epistemology is that between *rationalism* and *empiricism*. Rationalism is the idea that things are known *a priori*, i.e., independent of experience. Pure reasoning is the route to knowledge, as the knowledge is within our intuition and part of our nature (Markie, 2013). Empiricism, on the other hand, is the idea that the only source of knowledge about the world is sense experience (Godfrey-Smith, 2003; Markie, 2013). Our knowledge is dependent on our sense experiences; thus, we can only know things *a posteriori*.

Positivism may be seen as a branch of empiricism and is an important contributor to what we shall call technical rationality. Positivism was coined by the French philosopher Auguste Comte (1798-1857). Inspired by the successes in physics, Comte aimed at developing a scientific sociology. The new science was to be based on the *observable*, *countable*, *measurable* and *certain* aspects of social life. The structure of society was to be discovered by the same means that physics discovered the structure of nature, a perspective where religion and metaphysics had no place. Hence, the aim was to discover the relationships among positively given (observable) entities without searching for possible underlying (unobservable and, hence, metaphysical) structures behind these relationships (Wormnæs, 1987:25).

Positivism, under the flag of "logical positivism," gained reinforced interest with the Vienna Circle during the 1920s, associated with names such as Moritz Schlick, Otto Neurath and Rudolf Carnap. Similar to Comte's, the new positivism was strongly focused on science, inspired by successes within the natural sciences and, especially, the achievements of Einstein. Moreover, the positivists' view was in opposition to the traditional philosophy of science at the time, especially all forms of mysticism and idealism (which is often connected to forms of nationalism). This may be related to the political climate in Europe in the 1930s (Godfrey-Smith, 2003). As with the early positivism, metaphysical claims were rejected as meaningless to science (Wormnæs, 1987). Instead, they focused all their attention on experiencing the world: *"what every scientist seeks, and seeks alone, are… the rules which govern the connection of experiences, and by which alone they can be predicted"* (Moritz Schlick, quoted in Godfrey-Smith, 2003:29). Experience was considered to be the only source of meaning and knowledge (Godfrey-Smith, 2003). As mentioned in the introduction, the positivists only considered propositions that are *analytic* (logic and mathematics) or *empirical* as meaningful for scientific and philosophical study.

Positivism had a strong position within science in the period between the World Wars and after World War II. This led to a great focus on "the scientific method" (Godfrey-Smith, 2003; Nola & Sankey, 2007). In safety science this is reflected by, for example, Heinrich's book *Industrial accident prevention: a scientific approach* (Heinrich, 1931). However, during the 1950s and 1960s positivism disappeared due to irreconcilable difficulties with, for instance, the problem of induction and their focus on verification of scientific theories. Thomas Kuhn (1996) is often mentioned as influential on the fall of positivism by his pointing out that science did not progress by the application of a single scientific method. Kuhn found that science was better represented by paradigms of shared ideas, problems and methods through which scientists progressed in a modest, puzzle-solving matter. At times, controversies built up within the existing paradigm of "normal science" and practice progressed towards a state of "revolutionary science." At this point, the agreed upon fundamentals, problems and methods of the existing paradigm is lost and open to challenge. The revolutionary science continues until an alternative paradigm emerges, and once again practice settles into a stage of normal science. An interesting issue in this regard is that the settlement of a new paradigm may be the result of social power-structures during the time (Feenberg, 1999).

Another source of influence on what we call technical rationality is *scientific realism*. However, a fundamental difference between positivism and scientific realism is that realism does not reject a metaphysical or ontological stance about the *external world,* which cannot be tested empirically and thus has to accepted at "face value" (Chakravartty, 2011a, 2011b; Lincoln & Guba, 1985; Sankey, 2008). The aim of science for a scientific realist is to *discover and explain the truth* about the external world. Scientific progress is about *accumulating knowledge* about the world in order to *advance towards* the discovery of the true structure of the external world (Chakravartty, 2011a). Knowledge gained from scientific inquiry into both observable and unobservable entities is genuine, objective and independent of the inquirer (Sankey, 2008; Sardar, 2001). That is, the truth of a statement is not dependent on whether or not you believe it is true but is *"entirely determined by how things stand in the world, independent of us"* (Sankey, 2008:18).

An observed phenomenon, e.g., the motion of a car, is explained through underlying unobservable causal processes, which are responsible for the observed phenomenon. This claim has both ontological and semantic dimensions. First, the ontological dimension is associated with the existence of such underlying, unobservable causal processes. That is, they do actually, or literally, exist in the world and not merely as human constructions and are useful for explaining certain phenomena (Chakravartty, 2011b). Second, the semantic dimension is associated with the requirement to interpret theories literally (Chakravartty, 2011b; Suárez, 2011). That is, their relations of reference are, rather, directed towards the unobservable entities, e.g., to genes and quarks and whether or not they exist, not to a specific theory (Sankey, 2008). Consequently, *"one can successfully refer to an entity despite significant or even radical changes in theoretical descriptions of its properties; this allows for stability of epistemic commitment when theories change over time"* (Chakravartty, 2011a).

The empiricist ideal is described by the *correspondence theory*, which asserts that for a statement to be true, it has to correspond to the observable facts. This has implications for the predictive nature of realist statements or laws. For instance, for a law or statement to be considered as true, the predictions it provides need to correspond with the actual outcomes of an experiment or reality (Sankey, 2008).

To summarize, what is called technical rationalism in this thesis has the following attributes:

- The natural sciences are generally considered as a major inspiration. Some claim that all sciences could eventually be reduced to physics (Checkland, 1999).
- Science applies scientific methods associated with empiricism. Scientific propositions should be tested in carefully designed experiments that generate empirical data.
- Science aims to discover universally objective or true laws that explain the true structure of the society or the external world. Attitudes towards metaphysical claims may vary (c.f., positivism versus scientific realism), but this is of minor concern here.
- Inspired by successes in the natural sciences, complex systems are decomposed into their constituent parts where scientific knowledge is available. The behavior of the system is perceived as the sum of its constituent parts (Checkland, 1999; LeCoze, 2005; Leveson, 2004, 2011b).
- Quantitative methods and data are preferred over qualitative data (e.g., Wallace & Ross, 2006).
- There is a search in safety science for root causes and causal relationships between components, events and barriers (e.g., Heinrich, 1931).

2.2 An alternative holistic perspective

> *"To a living science nature will not be dead, but alive; and it will be like a friend about whom one can learn in sweet intimacy how to penetrate the soul and spirit, to know the tastes and inclinations, and to understand the character, impulses and abandonments"* (de Finetti, 1989:170).

The growing complexity of our society during the 20th century led to an increased focus on systems theory in safety engineering (Leveson, 2011b; McIntyre, 2000; Wallace & Ross, 2006). Instead of decomposing complex systems into their constituent parts, it is acknowledged that complex systems have properties that are properties of the whole. Such properties, e.g., safety, risk or accidents, are only meaningful to speak of at an elevated system level. This involves looking at complex systems as socio-technical hierarchies, which blurs the distinction between a system and its environment. This makes it problematic to apply the thinking associated with technical rationality. For instance; it becomes impossible to conduct scientific experiments of complex socio-technical systems as a whole; there will be important issues where quantitative data and models are non-existent, and there will be stakeholders with contrasting values. It seems obvious that there is a need for a broader scientific framework. In what follows, I will discuss elements of a more holistic scientific framework, which I have come to prefer.

The work of Kuhn (1996/1962) is considered important with respect to broadening the perspective on what could be regarded as science and scientific methods. Others have tried to broaden the perspective even more, Paul Feyerabend, for instance, who argues for epistemological anarchism in his book *Against Method* (Feyerabend, 2010/1975). Whether or not he was successful is another matter, but what is interesting with Feyerabend, at least for the sake of this thesis, is his view of theory-laden observations in experiments and perceiving scientific methods as straightjackets and constraining creativity. For instance, Kuhn's notion and "acceptance" of the "puzzles" of normal science was regarded by Feyerabend as professionalization and narrow-mindedness that excluded unorthodox ideas (Godfrey-Smith, 2003:112). Feyerabend proposed the principle of *tenacity* and *proliferation* as guides for science. Tenacity is concerned with holding onto attractive theories despite initial problems, while proliferation is concerned with the parallel production of new theories and ideas (Godfrey-Smith, 2003:115). Most scientists will argue that the scientific method is important and that the application of a scientific method is what distinguishes science from pseudo-science. Although Kuhn's work undermines Popper's (2002/1963) scientific method of conjectures and refutations (falsificationism) on a historical account, the principles of Popper are still important to science. What Kuhn showed was that Popper's principles are not exclusive to what is traditionally called science.

In the social sciences, the concept of social constructivism is important and may be a candidate for a foundation for systems thinking (Wallace & Ross, 2006). Having a social constructivist perspective on science implies that one believes that scientific facts, theories or concepts are social constructions (epistemological dimension). An even stronger position holds that reality, i.e., the entities reflected by our scientific theories, is constructed (metaphysical dimension). Hence, reality is not an external, objective and independent world that we are to discover through scientific inquiry but something that is created by and dependent on its observers and players (Kukla, 2000; LeCoze, 2012; Yeganeh & Su, 2005).

Scientific realism is often separated into the three dimensions: *metaphysical; epistemological*, and *semantic;* the same dimensions may also be attributed to social constructivism. Kukla (2000) argues that there exist "degrees" of realist and constructivist perspectives. You do not necessarily have to accept all the dimensions of either realism or constructivism if you define yourself as either a realist or a constructivist. For instance, you may take a position of metaphysical constructivism while still favoring a position of epistemological realism. In that context, this may include perspectives that claim that the *concepts* of safety and risk are socially constructed, but our ideas about these concepts may be true or false in an absolute sense.

The knowledge gained from scientific inquiry in a constructivist perspective is context-specific, not universal and objective. This may seem to undermine the knowledge gained from such inquires in comparison with the view of knowledge in scientific realism. However, the key issue is that the phenomena under consideration are *not amenable* to universal descriptions (Weinberg, 1972). Rather, they are unique, one-off events that require exploration and understanding instead of explanation through observation and generalization (Wallace & Ross, 2006). For instance, in fire safety science great efforts have been put into the discovery of the true statistical relationships governing human reaction time in case of a fire (see, e.g., Gwynne, Galea, Parke, & Hickson, 2003; MacLennan, Regan, & Ware, 1999; Nilsson & Johansson, 2009; Nilsson, Johansson, & Frantzich, 2009; Olsson & Regan, 2001; Purser & Bensilum, 2001; Shi et al., 2009; Xudong et al., 2009). Data is usually obtained through unannounced evacuation drills resembling controlled scientific experiments. However, the results of such inquiries may be seen, rather, as constructed, e.g., in terms of what categories the data are grouped into (detection time, warning time, reaction time, travel time), and highly context-dependent in terms of experiment/reality differences (e.g., lack of stress, aggression and fear associated with a real fire situation) (Wallace & Ross, 2006).

Since different people tend to have different views on reality, constructivists make use of hermeneutical, rather than positivistic, approaches. The aim is to understand the phenomena (the meaning of action), not to produce explanations through generalization (Yeganeh & Su, 2005). This leads to results that are both subjective and context-specific (low external validity). However, the knowledge gained from inquiries enables rich descriptions and understanding (high internal validity) of the situation. When the context of a certain situation is adequately known, this knowledge may be used for accurate predictions. In contrast, generalizations obtained from positivist inquiries may have a high external validity, i.e., are universal, but lack relevance to most practical cases due to a low internal validity (Wallace & Ross, 2006). A parallel can be drawn to Schön's (1991) *dilemma of rigor or relevance*, to De Bono's *intelligence trap* (Blockley & Godfrey, 2000:119; de Bono, 1978, 2007) and to the concept of "lamp-posting" (Ravetz, 1997:21-22).

In fire safety science, for example, it does not seem problematic that a TR paradigm functions side-by-side with more constructivist ideas. In fact, this is a mixture that seems necessary in order to strengthen the field. The fire phenomenon is effectively studied in the laboratory, where it is possible to develop generalizations in terms of models and relationships that may be useful to fire safety engineers. However, fire safety engineering is a lot more than describing or predicting a fire. The human factor and the interactions between humans, buildings, the environment and fire are not amenable to laboratory studies. In sum, we end up with a design or engineering situation that is highly situation-specific, wherein models and methodologies become tools for the design/building to achieve some future purpose while being maintained in a safe state (Bjelland, et al., Submitted). The narrow-minded focus on objectivity and truth may become more of a straightjacket, in Feyerabend's terms, than a constructive mindset contributing to social development. I will discuss some implications of this broad(er) philosophy of science for safety science in the following section.

2.3 Implications for safety science

In this section I discuss some important concepts within safety science and how they traditionally have been viewed within a technical rationality framework and then contrast that with an alternative holistic view. I will also connect some important findings from the fire safety science literature to the discussion. The aim is to present a broader understanding than that provided by the common technical rationality perspective and to point at how fire safety science relates to this understanding.

2.3.1 Risk

The risk concept has different interpretations and meanings in different fields of science and professional disciplines (for a broad overview see Adams, 1995; Althaus, 2005; Apostolakis, 2004; Aven, 2010a, 2010b, 2012a, 2012b; Aven, Renn, & Rosa, 2011; U. Beck, 1992; Bernstein, 1996; Covello & Mumpower, 1985; Damodaran, 2008; Douglas & Wildavsky, 1982; Holton, 2004; Kaplan & Garrick, 1981; Mairal, 2008; Paté-Cornell, 2012; Renn, 2008; Rosa, 2010; Shrader-Frechette, 1991; Solberg & Njå, 2012; Wilde, 2001). In a safety engineering context, risk is associated with possible future losses and the associated uncertainties (Aven, 2012a), that is, the consequences of initiating an activity, e.g., operating a road tunnel or having a large arrangement at a concert arena. Accidents could occur, and people and structures may be affected.

In a traditional TR framework, risk is seen as an objective property of the activity. The risk analyst aims at estimating this true risk using models and underlying causal relationships. Risk is usually understood as the combination of future consequences and the associated probabilities (see, e.g., Kaplan & Garrick, 1981). The analyst makes an estimate, r*, of the true risk, r, associated with an activity. Uncertainty, then, is associated with the error of estimate relative to the true value. This type of uncertainty is usually measured by a $(1-\alpha)100\%$ confidence interval. A confidence interval is a stochastic interval that either contains the true value of r or does not. If the situation under consideration is repeated an infinite number of times, and a confidence interval is calculated each time, one would find that the true value of r is contained within the interval in $(1-\alpha)100\%$ of the trials (Aven, 2012a:12). Hence, the interval is a reflection of the variation in a population (aleatory uncertainty), from which we assume repeated sampling of data. This thinking makes sense in a classical statistics setting, when operating with large populations. However, when we are interested in analyzing the risk of a specific unit, say a one-of-a-kind building, we run into problems of defining a population of similar units.

An alternative view is to claim that risk is a construction of the analyst, rather than an objective property of the activity, building, road tunnel, etc. The aim of the analyst is, thus, not to discover the true risk but to express his/her uncertainty about the possible future consequences of the activity (Aven, 2012a). In a TR framework, such a view of risk is perceived as subjective and relativistic. However, the underlying phenomena of safety science and the interactions between phenomena, structures, humans, organizations and society is not amenable to universal and objective descriptions by laws. Hence, a subjective framework may be the only way forward. In fact, the application of the TR framework is no less subjective than a constructivist approach, although the subjectivity is usually introduced "through the back door" and is, thus, improperly handled (Wallace & Ross, 2006). For instance, the definition of a "population of similar units" involves, in most practical cases, a great deal of subjective judgments, which are not reflected by the aleatory uncertainty reflected by a confidence interval. A subjective framework, often called a Bayesian or knowledge-based framework, does not suppress the subjectivity in the analysis but makes the subjectivity specific and visible to the decision-makers (Apostolakis, 1990; Aven, 2012a; Njå, 1998; Singpurwalla, 2006). Instead of making reference to thought-constructed populations of similar units, from which confidence intervals are established in the TR framework, the uncertainty associated with the future performance/outcome of a specific unit may be reflected by a credibility interval (Aven, 2012a:18). For instance, Y may represent the number of deaths due to building fires in Norway next year. A 90% credibility interval for Y is, say, [40, 90], meaning that our subjective probability is 90% that the true number of deaths next year will be between 40 and 90 people.

The quality of a subjective risk assessment is determined by the background knowledge on which it is based (Aven, 2011, 2012a; Bjelland & Aven, 2013). Background knowledge includes everything that the assessment is conditioned on, for example, physical models; causal models; data; simulations; the analysts' competency; stakeholder involvement, and expert knowledge introduced to the analysis. That is, the uncertainty description includes all of our lack of knowledge (epistemic uncertainty), including the aleatory uncertainty associated with variations in data. The risk assessment is a foundation for decision making, and it will be useful as such if there is a relationship based on trust between the analysts, stakeholders and the decision-makers.

Decision making about safety on the basis of risk analyses should be influenced by the underlying assumptions about the ontological status of risk. Either the risk analysis represents estimations of the truth, or they are subjective constructions of the analysts. This discussion is not intrusive in the major fire safety science journals and literature. Compared with research on, for instance, the fire phenomenon, smoke spread and materials' or constructions' reactions to fire, the risk concept is not discussed to any large extent in fire safety science. There are some examples, though. The traditional TR understanding of the risk concept is most commonly found (see, e.g., V. R. Beck & Yung, 1990; Frantzich, 1998; Hall Jr & Sekizawa, 1991; Lundin & Johansson, 2003; Ramachandran, 1988). The fundamental TR understanding of risk seems to be an axiomatic assumption and is not discussed. Some authors do, however, provide a critical debate about different interpretations of risk (see, e.g., Meacham, 2001, 2004a, 2004b; Noonan & Fitzgerald, 1991; Wade & Whiting, 1996; Watts Jr, 1991), but these examples are not representative for the community as a whole. A diverse debate about the foundations of major concepts in the discipline is inevitable in order to reach a higher scientific maturity.

2.3.2 Uncertainty and probability

Designing is about proposing or devising actions that will solve some problems in the future. That is, we generally propose statements in the form of "*this design will work in the specified circumstances*." For instance, in fire safety engineering, we propose the introduction of a sprinkler system in a building while at the same time proposing a statement of its performance: *"the sprinkler system will save lives in case of a future fire*." Uncertainty is a state of not knowing whether these statements are true (Holton, 2004; Lindley, 2006). In most cases, the best we can do is gather evidence to support them (Blockley, 1980; Blockley & Godfrey, 2000).

But can we not just act *as if* we were certain? For instance, when we design in accordance with prescribed fire safety solutions, we do not incorporate uncertainty specifically. We simply act as if fire safety is achieved through the application of the prescribed solutions. According to Puchovsky (1996), this practice seems to have served us well during the last century. The great reliance on prescriptive regulations in the US and in large parts of Europe (e.g., France and Germany), suggests that many actors perceive them as successful.

Maybe we can act as if we are certain in many cases. However, an obvious motivation for taking uncertainty seriously in safety design is that certainty does not exist, especially when faced with novelty and complexity. Why would we then want to describe the world as black and white when we know this is not the case? In fact, omitting a description of uncertainty may be seen as a value judgment made by the analyst. As different people tend to have different values, omitting uncertainties may be the same as misleading people, by not presenting the complete information (Paté-Cornell, 1994:153). In decision-making about risk in design projects, two different decisions could be made, simply based on whether uncertainty is presented or not (Aven, 2010b; Bjelland & Aven, 2013).

Probabilities are measures of uncertainty, which makes probability a useful concept in risk and safety assessments. However, there are several interpretations or types of probabilities that may be attributed to one's scientific foundation, that is, a TR or a constructivist foundation. The major difference between a TR and a constructivist perspective is whether the probability is an objective property of a population (the frequentist perspective) or a subjective degree of belief, dependent on the background knowledge of the analyst (the Bayesian perspective). For a thorough discussion of these differences, see de Finetti (1989), Lindley (2006), Bedford & Cooke (2001), Aven (2012a), Franklin (2009), Singpurwalla (2006), Apostolakis (1990), Wallace & Ross (2006), Holton (2004).

In fire safety science, as with the risk concept, there is little discussion about the philosophical foundation of probabilities, even though probabilities are important to many authors. When risk and probabilities are discussed, the frequentist perspective is often encountered (see, e.g., Frantzich, 1998; Hall Jr & Sekizawa, 1991; Ramachandran, 1988), while the supporters of the Bayesian, or subjective, perspective are more rare (Fitzgerald, 1991; Noonan & Fitzgerald, 1991). The frequentist perspective has severe limitations in the context of fire safety engineering, and a more diverse debate is inevitable, both for the sake of scientific maturity and for the sake of more appropriate decision making. Paper 7 (Bjelland & Aven, 2013) discusses safety engineering based on risk in more detail, while Paper 4 (Bjelland, et al., Submitted) discusses a framework for fire safety engineering that omits the use of risk and probability. The latter paper builds on the recognition that the great complexity of socio-technical systems and human intentionality is not easily quantified in terms of probabilities. That is, in a Bayesian perspective, probabilities may always be assigned, as they represent the subjective degree of belief of the analysts. However, it could be questioned whether such an assignment is dependable; for instance, in cases where the probabilistic data material is scarce, knowledge is represented in non-probabilistic terms and "the language of probability" is poorly understood by the actors involved in the processes.

2.3.3 Models

Generally, one can say that the *"purpose of models in science and technology is to make complex phenomena mentally manageable"* (Östberg, 2003:257). This should be valid whether one takes the position of a technical rationality framework or a constructivist framework.

However, the position of models, laws and causal relationships in the technical rationality tradition is more prominent than in the constructivist position. According to Wallace & Ross (2006:2) technical rationality *"presupposes that science is the disinterested discovery of objective laws of nature that are not context specific (i.e., are universal) and should be mathematically expressed if possible."*

Hence, the discovery of models that describe reality, i.e., truth, is a fundamental aim for science within a technical rationality framework. In a constructivist framework, however, acquiring a rich understanding of the situations of scientific interest is the goal. Models are not passively discovered but, rather, are generated actively during the scientific inquiry or engineering process in order to make sense of the perceived complexity of reality. *"Models are active designs, related to the purpose of the modeler"* (LeCoze, 2005:621).

A model may be judged on the basis of whether or not it is a good representation of reality. This would be the technical rationality view, and in fire safety science it may be represented by, for instance, Beck & Yung (1990) or Hadjisophocleous & Fu (2007). Other possibilities are whether the model is useful for its purpose, a constructivist or instrumentalist view (LeCoze, 2005; Wallace & Ross, 2006), or empirically adequate, a constructive empiricist view, when the aim is to discover facts about the observable world (Monton & Mohler, 2012). In any case a model needs to capture the relevant (observable) structure of reality in order to be useful (March & Smith, 1995). Borg & Njå (2013) provide a broad discussion of the concept of validation of fire models in a fire safety engineering context and aim to release the concept of validation from its traditional TR interpretation in fire safety science. Meacham (1997) is also expressing similar concerns about the narrow TR perspective of validation of fire models, and proposes that "validation" is substituted by the term "confidence".

2.3.4 Data

In a TR framework, certain data will be given more credit than other data (Wallace & Ross, 2006). According to Singpurwalla (2003), data is that which is directly observable and, therefore, measurable, i.e., an empiricist view. In this case, data may simply be called facts or factual (Lindley, 2006; Singpurwalla, 2003). In the TR framework, quantitative data will also generally be favored before qualitative data. This may be statistics in terms of, for example, historical failure or accident frequencies that may be applied into the quantitative models of the technical rationality framework.

Designing is a creative task of imagining and conceptualizing/representing future improved realities. Safety engineering is also a multidisciplinary task. Even though there is a safety engineer associated with a project, information and designing of safety-related issues come from many engineering disciplines. The conceptualizations of optional designs have a potential of being a catalyst for realizing tacit knowledge from the involved stakeholders. A broad perspective on safety engineering epistemology hence acknowledges a broad perspective on data relevant for design. Much of this data may not be realized before it is "activated" through possible design solutions, which fundamentally results from creative innovation.

A strict empiricist, or TR, perspective may be too narrow to capture all relevant data/evidence in a design project. Take the difference of *novices* and *experts* (Cross & Cross, 1998; Dorst, 2008; Dreyfus & Dreyfus, 1986; Lawson & Dorst, 2009; Rust, 2004; Wood, Rust, & Horne, 2009). Novice designers and engineers within their respective disciplines will have different qualifications and mental capabilities. The difference in their competency may not be associated with their formal training and qualifications but with their potential for activating tacit knowledge, a knowledge of which they may be unaware until presented with a problem that requires it. The technical rationality framework would generally reject the possibility of tacit knowledge, as experience is seen as the only source of knowledge. Moreover, quantitative data would be preferred over qualitative data. However, according to Wallace & Ross there should not be a prima-facie acceptance or priority of data in a specific form: "*[t]he source of the data does not really matter because the key point is that data gathered from whatever source and in whatever form (e.g., textual or numeric) have to be treated similarly: as information to be classified and analyzed*" (Wallace & Ross, 2006:31).

Fire safety science builds on a strong empiricist tradition, and there is a great emphasis on obtaining fire and casualty statistics (see, e.g., Banks & Montgomery, 1983; Brennan, 1999; DSB, 2013; FEMA, 2013; Hasofer & Thomas, 2006; Holborn, Nolan, & Golt, 2003; Kose, 1999; Lizhong, Xiaodong, Zhihua, Weicheng, & Qing'an, 2002; Rahikainen & Keski-Rahkonen, 1998; Ramsay, 1979; Richardson, 2001; Rosenberg, 1999; Spinna Jr, Spinna, & Dunn, 1984; Steen-Hansen, 1995) with, among others, the aim of using the data in design. However, the statistics are often coarse or relevant on a national level, while design projects are very specific and context dependent. This may be illustrated by the recent governmental work on fire safety for vulnerable groups (MJPS, 2012). Although fire safety for vulnerable groups is of major concern to the society, it is not possible to "rationalize" this concern using available statistics in benefit-cost analyses. The question, then, is whether the statistics represent the truth or whether there should be other sources of data also implemented in the analysis. Although fire statistics and other empirical data, e.g., fire tests or experiments, are important, the task of fire safety design may benefit from a broader perspective.

2.3.5 Systems

Systems are important "objects" within safety engineering and play a major role in both a technical rationality and a constructivist approach. However, the approach towards describing a system is fundamentally different.

In a technical rationality framework, systems are described through decomposition into subsystems, components and individual parts. This is a reductionist framework. A fundamental assumption is of the existence of a linear "cause/effect-relationship" between components governed by underlying deterministic or probabilistic relationships. The system boundaries are effectively determined through the specification of components and interactions, and, thus, there is a clear distinction between the system and its outer environment. According to Wallace & Ross (2006), this leads to a false simplicity. A narrow focus on individual components and reliability misses important "component interaction" failures. That is, there are cases when the systems components work reliably and "as intended," but the system still fails, a problem positively correlated with increasing system complexity (Berk, 2009; Leveson, 2004, 2011b; McIntyre, 2000; Perrow, 1999; Sagan, 1993; Wallace & Ross, 2006).

According to Checkland (1999), the scientific method of reductionism, carefully executed experiments, and refutations of conjectures encounters problems in the face of *increased system complexity*; *the social sciences*, and *real-life management and decision making*. The keyword is complexity, and the systems are characterized as "open to the environment." In contrast with the structured systems of natural sciences, it is difficult to draw a clear line between a social system and its environment. There *"may be exchange of materials, energy, and information"* (Checkland, 1999:82-83) between the system and its environment. Hence, the system as you knew it yesterday may not be the same system today. The predictions you make about the system may actually change the future behavior of the system. The search for fundamental and universal laws is exchanged with understanding *"the logic of situations"* (Checkland, 1999:71). At best one may be able to make predictions about a system's behavior, given some clear assumptions about the situation. The difficulties of the scientific method to bring clarity to such complex situations led to the development of systems theory.

Systems theory builds, according to Checkland (1999), on two pairs of fundamental ideas: *emergence*[2] *and hierarchy* and *communication and control*. All complex systems can be modeled in terms of hierarchical levels of organizational control (Checkland, 1999; Leveson, 2004, 2011b; Jens Rasmussen, 1997; J Rasmussen & Svedung, 2000; Simonovic, 2010; Sydenham, 2003). System properties are *emergent* at a specific *hierarchical level* of the system and make sense only at this level. The systems behavior or

---

[2] The concept of emergence does not have a precise philosophical definition. For a background, see, for example, O'Connor (1994); O'Connor & Wong (2012); Johnson (2006); Pepper (1926); Meehl & Sellars (1956); Bedau (2003; 1997); Bedau & Humphreys (2008).

performance is *controlled* by the higher levels of system hierarchy imposing constraints on the lower levels. In order for this control to be effective, there is a need for *communication*, feed-back and feed-forward, about the state of the system (Leveson, 2011b). A holistic scientific framework needs to reject the reductionist thinking and would better off building on systems thinking.

Systems thinking is not commonly adopted in the fire safety science literature, although some examples exist: e.g., Beard (1982) and Santos-Reyes & Beard (2001). The traditional view, more in line with the reliability engineering school (e.g., McIntyre, 2000), is associated with scientific reductionism with a focus on failure events and causal modeling (V. R. Beck, 1987; V. R. Beck & Yung, 1990; Frantzich, 1998; Hasofer & Beck, 1997; He, 2010; He, Horasan, Taylor, & Ramsay, 2002; Magnusson, Frantzich, Karlsson, & Särdqvist, 1994).

2.3.6 System performance

The traditional TR perspective may be summarized by saying that a system's performance is described as the sum of its parts (Checkland, 1999). Safety performance is measured in terms of a low risk. As we mentioned earlier, risk is an objective property of the system in a TR framework, thus performance may also be seen as an objective property of the system. The focus is on estimating this true performance (e.g., risk) using underlying causal relationships between system components.

In systems theory the performance of a system cannot be described by decomposition into its constituent components. According to Wallace & Ross (2006), the performance of systems are best understood as a self-regulating process towards a point of natural homeostasis, which is context-dependent and may change over time (rheostasis). The key issue is to acknowledge the need for flow of open and precise/reliable information from top to bottom and from bottom to top in the system hierarchy to empower necessary adaptations at all levels (Checkland, 1999; Leveson, 2011b; Wallace & Ross, 2006). Such self-regulating system processes are also described by Gerald Wilde (2001) and John Adams (1995) as risk homeostasis. Safety management then becomes associated with the task of imposing controls and creating an environment that enables the system to be kept within a safe state (Bjelland, et al., Submitted).

In the interface between fire safety science and regulation, there is focus on verification of fire safety performance (Bukowski & Babrauskas, 1994; Bukowski & Tanaka, 1991; Lundin & Johansson, 2003; Magnusson, Frantzich, & Harada, 1996; NKB, 1994; Wolski, Dembsey, & Meacham, 2000). The verification process, associated with fire safety for occupants, involves checking, for instance, whether the available safe egress time (ASET) is larger than the required safe egress time (RSET), either deterministically or probabilistically. This kind of verification makes sense in a technical rationality perspective. However, in an alternative holistic perspective, where system performance is constantly changing or adapting to the environment, the concept of verification of safety is more difficult to understand. Paper 4 deals with this issue, and a holistic framework for fire safety engineering is proposed (Bjelland, et al., Submitted).

3 DESIGN SCIENCE

Selected topics from a design science perspective are presented in this section. The purpose of discussing design science is twofold, as mentioned in section 1.6. First, design science involves, among other things, research into how designers work, how design processes evolve, and design methods. Hence, findings from the field of design science are an empirical foundation (data source) into the case studies conducted in this thesis (see section 5). Second, the work conducted in this project is design science, although the connection between fire safety engineering and design science is, to my knowledge, not often encountered. Hence, it was considered interesting to investigate design science with two questions in mind:

- Why are *designing* and *safety engineering* perceived as different activities, demanding different knowledge and approaches?
- What can safety engineering learn from the field of design science, with respect to increased understanding of what promotes and inhibits performance-based safety management of safety design?

3.1 Simon's positivism

The field of design science emerged during the 1950s and is continuously evolving (Cross, 2007; Dorst, 2008; Galle, 2008). The early phase, which coincided with the positivistic tradition within the philosophy of science, is greatly influenced by Herbert A. Simon's book *The Sciences of the Artificial* (Simon, 1996). Simon argues that design is about the activities we perform in making existing situations into preferred ones. Although Simon's work and definition of designing has been quite influential (Cross, 2007; Dorst, 1997; Galle, 2011; Krippendorff, 2006; Lawson & Dorst, 2009; Schön, 1991), it is quite broad and unspecific. According to the definition, nearly everything can be called designing.

Simon argues that an artifact *"can be thought of as a meeting point – an "interface" in today's terms – between an "inner" environment, the substance and organization of the artifact itself, and an "outer" environment, the environment in which it operates"* (Simon, 1996:6). This distinction illustrates that the attainment of an artifact's functions and goals are not entirely dependent on the artifact itself but must be seen in relation to the context in which it operates, that is, the outer environment and how this environment affects the artifact. Given that the outer environment is known, the behavior of the inner environment can be explained, much like the rationality of the "economic man" in economic theory (Simon, 1996). Examples of operationalization of such mechanist decision-making approaches are found in, for instance, Hazelrigg (1998) and Wassenaar & Chen (2001).

Simon was influenced by the positivistic technical rationality tradition and aimed to develop a science of design capable of solving design problems within a technical rationality paradigm. As a basic assumption for this paradigm, he argues that there is no clear distinction between well-structured and ill-structured problems, and as such, the same principles to problem-solving could be usable for both kinds (Simon, 1973). According to Simon, *"no one in his right mind will satisfice if he can equally well optimize; no one will settle for good or better if he can have the best"* (Simon, 1996:119). However, to accommodate the practical problems of the real world, he acknowledged that sometimes one would have to choose a *satisficing* solution instead of the *optimal* solution, since the number of possible designs is infinite. This is associated with the concept of *bounded rationality* (Simon, Egidi, Marris, & Viale, 1992), which is closely associated with Herbert Simon as well.

Following Simon's principles, safety engineering becomes an activity of structuring goals and performance criteria into a mathematical language (Cross, 2011; Dorst, 1997). Modeling, calculations and simulations are then devised to identify design alternatives that best fulfill the goals and performance criteria. This is an important part of safety engineering, which is emphasized in engineering practice, engineering education, safety regulations and safety standards development. However, technical rationality is not a solution to all design problems. For instance, it is not straightforward for developing goals and performance criteria for novel designs. Different stakeholders will have different opinions. Furthermore, there are great uncertainties associated with phenomena involved in safety engineering, e.g., how fires occur and develop and how people react in accident situations. A great deal of knowledge about accidents, causal factors, human behavior etc., may only be present in qualitative form and sometimes only be tacitly understood. This makes the knowledge difficult to formalize in mathematical language and to transfer focus to individual engineer's and expert's skills.

3.2 Schön's reflective practice

Donald Schön claims that *design is a reflective conversation with the situation* (Schön, 1991:79). The focus of his work is on the skills and experience a designer brings to situations of uncertainty, instability, uniqueness, and value conflict (Galle, 2011:84-85), and he is a strong critic of Simon's technical rationality paradigm. His thoughts have influenced a great deal of recent work within design research (Blockley & Godfrey, 2000; Cross, 1999, 2001, 2011; Cross & Cross, 1998; Galle, 2011; Lawson & Dorst, 2009).

Schön argues that technical rationality within design is only useful when the problems are well-structured, which important design problem are not. He uses a landscape analogy to illustrate this point, where it is argued that the major problems of professional design practice are revealed in the "swampy lowland," whereas the well-structured part of design problems is the "high, hard ground" (Schön, 1991:42). While the technical rationalist tradition could produce tools to tackle those high, hard ground problems, such questions are relatively unimportant. It is the problems associated with the landscape of swampy lowlands that are of greatest human concern.

Schön describes this as a dilemma of *rigor or relevance* in the development of instrumental design science theory. On the one hand, one could apply sophisticated technical methods to relatively unimportant problems; on the other hand, one could face the "messy but crucially important" problems that are outside the scope of technically sophisticated methods. In such cases one must rely on *"experience, trial and error, intuition and muddling through"* (Schön, 1991:43). Schön refers to messiness as situations involving complexity, uncertainty, instability, uniqueness, and value-conflict. To resolve these issues, he seeks an epistemology of practice implicit in the artistic, intuitive processes that some practitioners seem to bring to such situations

(Cross, 1999, 2011; Galle, 2011; Lawson & Dorst, 2009; Rittel & Webber, 1984; Schön, 1991).

In my view, Schön contributes to safety engineering by expanding the notion of relevant knowledge for engineering problems into a more holistic perspective. Designing is not just about technical rationality but about what skillful practitioners brings to the table in design projects (Dreyfus & Dreyfus, 1986). An important skill of the designer is the ability to frame the design problems in different ways (Cross & Cross, 1998; Dorst, 2011; Schön, 1991). In fire safety engineering, a practitioner may, for instance, frame fire safety within a historical context. For him, design solutions that were acceptable yesterday must be acceptable today (Bjelland & Njå, 2012a). Another practitioner may frame the issue of fire safety as an emergent property of a system (Leveson, 2011b). The way these two practitioners go about solving a design problem, their epistemological framework, and how they evaluate the quality of the finished design will be considerably different.

Another important skill is associated with the designer's ability to structure the "solution space" and mode of thinking in a certain design context by building on a repertoire of previous experience (Schön, 1991:315-317). An example from fire safety engineering is the study of common sets of design problems in different occupancy classes. If one deals with a hospital, one knows that there will be people unable to rescue themselves in a fire, and the knowledge of how this was solved in similar cases will guide the design – even if the design situation is new to the designer.

A major challenge with recognizing reflection-in-action as a source of knowledge in engineering is that practitioners are unaware of what they knows and why they know it. Consequently, it is a challenge to justify the quality and rigor of an approach based on this knowledge. Schön argues that this is an important reason for studying reflection-in-action with the goal to develop an epistemology of practice. In this epistemology, technical problem solving is placed within a broader context of reflective inquiry, i.e., it is a part of, but not the sole content of, the epistemology. Furthermore, it would show how reflection-in-action is rigorous in its own right and be relevant to the messiness of the spiral and co-evolving process of problem *framing* and problem *solving* that goes on in real-life projects (Blockley & Godfrey, 2000;

Dorst, 2011; Schön, 1991). The goal of the design process becomes one of developing a matching pair of design problems and design solutions (Cross, 2011; Lawson & Dorst, 2009; Rittel & Webber, 1984): *"What you need to know about the problem only becomes apparent as you're trying to solve it"* (Cross, 2011:14). Creativity then becomes an important part of the designer's repertoire of thinking skills and knowledge (Blockley & Godfrey, 2000; de Bono, 1990; Dorst & Cross, 2001). The need for a broadening of the knowledge base, from technical rationality to more social and human skills, is also increasingly emphasized within the engineering community (e.g., ASCE, 2008).

3.3 Krippendorff's second-order knowledge

Klaus Krippendorff argues that design is the activity of proposing realizable artifacts to others (Krippendorff, 2006:25). The artifact does not exist at the time of designing. What we want is to create an artifact that will have a set of properties that will fulfill its stakeholders' needs. Since it does not exist at the time of designing, it cannot have any properties, so the only way to succeed is to predict the properties of the artifact when it is put into use. According to Dorst (2003:6), a design project is a *"problem-solving process for the outside world."* This process needs to be *controlled and justified* to the stakeholders. Consequently, the designer anticipates and justifies what the design will mean to others, a second-order knowledge (Galle, 2011:87; Krippendorff, 2006). Based on this we see that while Schön focuses on the reflective designer's knowledge, Krippendorff focuses on the design/artifact's stakeholders: What will be the technological, social and cultural consequences of the artifact for the different stakeholders?

A science for design needs to build on a distinct type of epistemology that has the potential to reflect the revolutionary and innovative characteristics of design. What worked previously is a poor standard for new designs, as is common with the conventions and rules set forth by authorities. Conversely, what Krippendorff argues for is a search for variability – to create spaces of possibility. Furthermore, since designers are concerned with making artifacts that will produce new, desirable futures (anticipated by the designer), there is a need to inquire into sources of resistance to change and how to circumvent them. The designer must rely on others, the stakeholders, to realize a design. As such, the designers' visions of desirable futures must be shared by the stakeholders' visions.

This is an invitation to conduct a broad search for possible stakeholder needs and values. When dealing with issues of risk and safety, costs and benefits are often distributed among different stakeholders. A narrow perspective may lead to poor designs when seen from the society's perspective, in which risks are unfairly distributed across different groups. In the context of human-centered design, Krippendorff argues for a broad methodology that can capture the user's understanding and learning processes about how interfaces between the design and its users evolve, how stakeholders will talk about the design, and which communities are likely or unlikely to embrace the design (Krippendorff, 2006:211).

3.4 Evaluating quality in design decisions

The search for quality in design is not a search for truth. Even Simon (1996), who argues from a positivistic tradition, admits that one often will have to *satisfice* rather than *optimize*. The real world is not a cold, rational and logical world. Designing is, thus, "*rather about getting agreement about what is best in the context – it is a social process*" (Blockley & Godfrey, 2000:66). Moreover, it is *"fortunate that strict truth and precision are not necessary for practice – for if it were, nothing would ever get done!"* (Blockley & Godfrey, 2000:113).

While search for *truth* is the goal in natural science, *safety* is the goal of safety engineering. Consequently, the truth may not be necessary as long as the evidence (for safety) is *dependable*. Truth is (of course) sufficient but unnecessary for dependability. Testing the evidence through scientific experiments is one way to achieve dependability, but this is not always possible, especially when dealing with "soft systems" (Blockley & Godfrey, 2000:95). The amount of "verification" of the evidence depends on the context and what problem to solve. If the specific problem is critical for the design, more efforts should be put into obtaining supporting evidence in order to achieve dependability. According to Krippendorff's (2006), designers must substantiate what are essentially semantic claims without bypassing the stakeholders involved.

Quality is multi-faceted and not just a straightforwardly measurable property of the design. According to Weinberg (1972) and Funtowicz & Ravetz (1992), there are limits to what can be answered by "normal science," which is also relevant for design issues. Some parts of the design may be evaluated using the technical rationality of quantitative models and formulas. Other qualities need to be evaluated qualitatively, subjectively and even creatively, as the design may be a solution to problems with which we have no previous experience. The idea that a regime of technical rationality will solve all the problems seems to miss what design is all about. Knowledge in design is about understanding what stakeholders want, whether they are a building's owner or users, its regulators, or a new building's neighbors. According to (1972:218), *"he whose shoe pinches can tell something to the shoemaker."* Some values will be quantitative, others will not. The design process must resolve conflicts and attend to the different demands using the appropriate skills and knowledge. A designer has a responsibility to act on the basis of a theory or model and a professional *duty of care* to fulfill a role as a designer (Blockley & Godfrey, 2000). This includes developing professional respect in the community, a respect that is enhanced by outstanding performances and demolished by manifested incompetence and unethical behaviors (Krippendorff, 2006).

3.5 Creativity in design

> *"Imagination is more important than knowledge. For knowledge is limited to all we now know and understand, while imagination embraces the entire world, and all there ever will be to know and understand."* – Albert Einstein

Edward De Bono argues that there is a fundamental difference between intelligence, the ability to analyze, and the ability to be able to operate in the real world: *"Intelligence is concerned with the truth, while design is concerned with possibility and value: you can have truth about the past but you can only have possible value about the future"* (de Bono, 2007:47).

Humans tend to develop categories and links between categories. In this way, standard situations and links are created that constitute patterns for their thinking. Due to our developed linking patterns between them, it is easy to connect issues belonging to already known categories to other categories. Consider the link between a certain symptom of a disease and the common treatment for this disease. The treatment becomes obvious once the symptoms are categorized. Similarly, we tend to prescribe solutions for buildings and road tunnels based on predetermined categories and linking rules, i.e., prescribed design rules (Blockley, 1980). The advantages of creative thinking are brought forward when one is able to see patterns which, at first, seem illogical. When the pattern is identified, logic is often found by hindsight (de Bono, 2007).

Sometimes our pre-determined categories are narrow and single-minded. It may be hard to see that an issue should belong to one of our already developed categories of thinking. As such, we might miss the connection between this issue and some other important category. The result of such thinking is an emphasis on *"what is"* by the use of tools like analysis, judgment and argument. Although this is useful in many situations, it limits our perspective on thinking about *"what could be,"* which is more about constructive and creative thinking and *"designing a way forward"* (de Bono, 1999:2).

The engineering disciplines are sometimes associated with vertical thinking (ASCE, 2008). The American Society of Civil Engineers (ASCE) illustrates the concept of vertical thinking by a silo of relevant knowledge for the specific field of engineering. Skilled engineers are those who have managed to develop a very deep silo of knowledge that they apply to the problems encountered. The cost of such thinking may be the lack of attention to knowledge outside the silo, which may lead into an intelligence trap. The intelligence trap is, among other things, characterized by defending a bad solution by the application of flawless logic. Lateral thinking, e.g., multidisciplinary thinking; multi-layer thinking; horizontal thinking etc., is a preventive measure in this respect. Lateral thinking involves expanding the repertoire of patterns in which we think about the world (ASCE, 2008:52; Blockley & Godfrey, 2000:119; de Bono, 1978, 1990). Designing in the constantly changing and complex world is about resolving issues in multidisciplinary teams towards a specified purpose. The design problem does not present itself for standard problem-solving but needs to be developed and reframed as possible solutions emerge, taking into account the evolving design situation and the designers' knowledge and skills (Blockley & Godfrey, 2000; Cross, 2011; Dorst, 2011; Dreyfus & Dreyfus, 1986; Schön, 1991).

4 SETTING THE SCENE

In this section I introduce the targets of design, i.e., buildings and road tunnels, and the targets of my research, i.e., fire safety engineering and design processes. Fire safety design of buildings and road tunnels is dealt with by fire safety engineering using either prescriptive design rules or performance-based principles. Hence, a short introduction to these concepts is provided, followed by a short presentation of the common design process.

4.1 Buildings and road tunnels

A common trait with the artifacts we are concerned with in this thesis is that they are socio-technical systems. The artifacts are designed to serve one or more purposes, and these purposes are fulfilled by combining the properties of the physical construction and the human intervention within a situational context (Blockley & Godfrey, 2000; Checkland, 1999; Kobes, Helsloot, de Vries, & Post, 2010; Leveson, 2011b; Njå, 1998). The output, that is, the performance of the socio-technical system, leads to some smaller or larger change in the world that will feed back to the operation of the socio-technical system. See Figure 2.

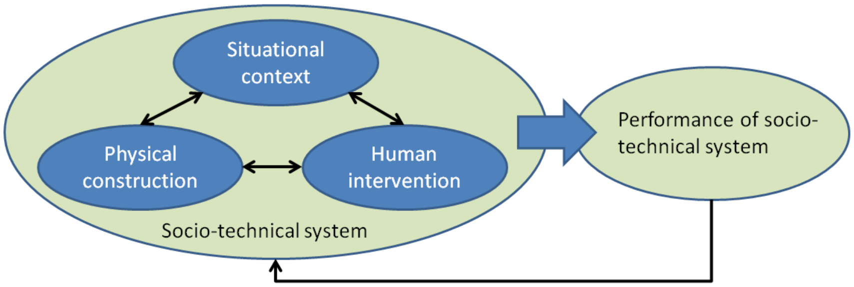

Figure 2: Goal-achievement of socio-technical systems.

The physical construction is the “hard” part of the system. In a road tunnel, for instance, it is the tunnel walls, the traffic signs, the emergency exit doors, the smoke ventilation fans and the signaling system. In a building, it may be the structural load bearing system, the separating walls, the windows and doors, the alarm systems and so on. Practically all modern technical systems include some computerized control, which includes software. In this context, the computerized control and software are understood as part of the physical construction.

Human intervention is needed for the system to perform and produce outputs. Hard systems are embedded in soft systems (Blockley & Godfrey, 2000). For instance, a residential building is not a home before someone starts living there, and concert arenas are not fulfilling their purpose before people are present. A situational context for the concert arena may be the occurrence of a fire caused by pyrotechnics on the stage. In order to produce favorable outputs in this situation, the physical construction need to be properly designed and maintained. The involved humans have to be prepared through procedures and training (crew and internal staff) and need to respond to the current situation (both crew and audience).

In association with work on this thesis, we have had the pleasure of being involved in the Rogfast subsea road tunnel project. The Rogfast project aims to provide a ferry-free connection across the Bokn Fjord in Rogaland, Norway. Since the early visions of a project in the beginning of the 1980s, the number of alternatives has been effectively narrowed down to a single route. The proposed tunnel will be approximately 25.5 kilometers long due to the breadth and depth of the fjord, with an additional four kilometer tube to the island of Kvitsøy. It will be approximately 390 meters below the sea surface at its deepest point. The Rogfast will, if realized, be the longest and deepest road tunnel in the world. For more information about the Rogfast project, see Alsaker (1997), NPRA (2007), Dahle et al. (2006), Jenssen et al. (2006), Hokstad et al. (2012).

Lately, there has been concern about whether steep and long descents and ascents may cause problems for heavy goods vehicles (see, e.g., NPRA, 2012; Nævestad & Meyer, 2012; Skogvang, Rokstad, Værnes, Øglænd, & Jenssen, 2011). An important issue is whether or not the existing knowledge, regulations, and design process procedures are appropriate for this project. Using the existing framework involves extrapolating our knowledge into spheres of uncertainty. This has proven fatal before, for instance, when looking at the history of bridge building (Petroski, 2006). In paper 7 (Bjelland & Aven, 2013), included in part II of this thesis, we look at the treatment of uncertainty in the Rogfast's risk analyses and propose a framework for how to deal with uncertainty in a risk analysis context. In paper 8 (Borg, et al., Submitted), we scrutinize a new Bayesian network risk assessment model applied to the Rogfast case.

4.2 Fire safety engineering

Fire safety engineering (FSE) is often used interchangeably with fire protection engineering (Wilkinson, Glockling, Bouchlaghem, & Ruikar, 2011). A common definition is that FSE is the *"application of science and engineering principles to protect people and their environment from destructive fire"* (Hurley, 2009). This involves activities associated with the identification and analysis of fire hazards: developing proposals for mitigating fire damage by design; constructing, arranging and using buildings and transportation systems; assessing the consequences of using different materials and structures; determining the feasibility and designing of fire detection and fire suppression system, and contributing to fire investigations and post-accident analyses.

Although FSE often is associated with the application of "scientific" and "engineering principles," fire safety design by the application of prescriptive solutions is often included in FSE. The reason may be that most fire safety designing activity is based on the application of prescriptive solutions (Bjelland & Njå, 2012a). Nevertheless, the mixture causes some confusion, as fire safety design based on prescriptive solutions can hardly be recognized as using scientific and engineering principles in the traditional sense of understanding these concepts.

If we want to be clear about understanding FSE as the application of scientific and engineering principles to the design activity, we have to add the term "performance-based," i.e., performance-based FSE. Performance-based FSE is commonly known within the FSE community as the design of a building by determining (1) performance goals and objectives, (2) analyzing fire scenarios, and (3) quantitatively assessing design alternatives against the fire safety goals and objectives using engineering tools, methodologies and performance criteria (SFPE, 2000).

FSE is a multi-disciplinary field of engineering. A complete fire safety design for a building often includes a sprinkler system, a fire alarm system, fire separating walls and fire-protected, load-bearing constructions. This involves interfaces with mechanical, plumbing, electrical and structural engineering, as well as architecture.

In Norway, the responsibility for design of systems, subsystems and buildings is separated into two levels: “concept” and “detailed” design (NBRI, 2003a, 2003b, 2003c). The fire safety engineering discipline is only responsible for concept design, while the other engineering disciplines and the architect are responsible for detailed design. For instance, in the case of a fire alarm system, the fire safety engineer specifies whether a system shall be present, what areas it shall cover and relevant dimensioning standards. The detailed design, i.e., the selections of detectors, spacing of detectors, programming design, etc., are conducted by the electrical engineer (and sometimes by a sub-contracted fire alarm system supplier). Consequently, the Norwegian fire safety engineer has a limited effect on the detail design of the systems he/she proposes. The fire safety engineer supplies the other disciplines with necessary premises for detailed design.

4.3 Design principles

4.3.1 Safety by prescription

The prescriptive codes may be viewed as a collection of design solutions or performance requirements which: (1) have been introduced to prevent the reoccurrence of a specific accident, and (2) are not yet proven to be inadequate in that respect. The prescriptive design rules are not falsified yet (Blockley, 1980). Prescriptive regulations may be seen as “IF-THEN”-rules (cf., Figure 3) (Blakstad, 2006). Necessary actions, measures, and activities are given in advance. For instance, IF you are designing a concert arena, THEN the maximum distance to an emergency exit should be 30 m.

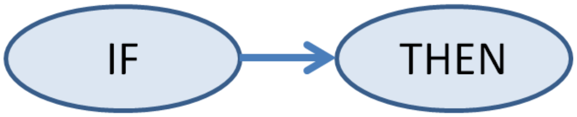

Figure 3: Prescriptive regulations as IF-THEN-relationships.

While the premodern designs and artifacts were quite simple and operated in a transparent environment, our contemporary designs are not. Introduction of modern technology, which, for instance, relies on computers and software and operates in a globalized environment of systems with tight couplings, has made it difficult to identify clear and isolated causes of accidents (U. Beck, 1992; Leveson, 2011b; Perrow, 1999; Jens Rasmussen, 1997). The major challenge with a reactive safety approach and prescriptive regulations is illustrated by Figure 4. Our collective experience, which is documented through the prescriptive regulations, only covers a part of the possible universes of IFs and THENs that might be appropriate in a certain situation. This may be a problem when both the IFs and the THENs need to be determined in advance of a specific project or problem (Hale & Swuste, 1998). Consider again the maximum distance to emergency exits in a concert arena. First, there are many ways of designing a concert arena, so the IF-side is not easy to determine. Second, there may be multiple means available in terms of satisfying the ultimate purpose: safe egress during fire. Hence, the THEN-side is not easily determinable either.

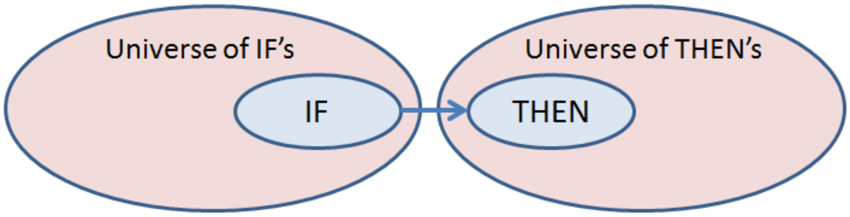

Figure 4: Prescriptive regulations as IF-THEN-relationships.

4.3.2 Safety by clarifying objectives

A focus on system performance is a focus on the “ends” (results/outcomes) rather than the “means” (measures or activities) during the design phase. This focus allows the implementation of any measure or activity that will fulfill performance objectives (Blakstad, 2006; Bukowski & Babrauskas, 1994; Bukowski & Tanaka, 1991; Hadjisophocleous, Benichou, & Tamim, 1998; Kirwan, Hale, & Hopkins, 2002; Meacham & Custer, 1995; Watkins, 2007). Fewer constraints are thus imposed on the designs, which possibly make it unnecessary to compromise some other important trait of the design for fire safety requirements.

Performance objectives need to be developed to assess performance. The performance objectives state what the system is desired to accomplish on all levels of the socio-technical system (Maguire, 2008; Watkins, 2007). Developing performance objectives involves identifying the project’s stakeholders and their individual objectives. For a new building, this may be its future users, neighbors, owners, maintenance personnel, fire and rescue service and the society as a whole (represented by legislators). Paper 4 (Bjelland, et al., Submitted) proposes as framework for fire safety engineering that builds from fire safety performance objectives that define the desired state of safety.

4.4 Design processes

Construction projects, whether buildings, road tunnels or offshore platforms, often follow the Capital Value Process (CVP) depicted in Figure 5 (Kjellén, 2007). The CVP outlines the phases a project goes through from a business development plan to operation. At the end of each phase, there are decision processes, illustrated by decision gates (DG) in Figure 5, where one evaluates the foundation for decision-making developed in the preceding phase. The project may not proceed to the next project stage before the requirement given in the DG is fulfilled.

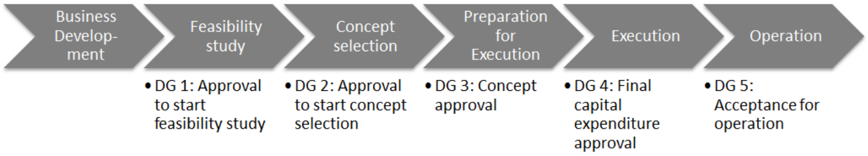

Figure 5: The Capital Value Process (CVP) from business development to operations (Kjellén, 2007).

The CVP is linear. The process is initiated with a design problem, for instance one developed from the societal need to cross a fjord. As the CVP progresses, the level of detail associated with the design increases. In the feasibility study, one could consider several alternatives: a subsea road tunnel, a ferry-connection, a floating bridge, a suspension bridge, doing nothing, etc. The level of detail is coarse, but the assessments need to point to the important factors that separate the different options. When one comes to the preparation for the execution phase, the concept has been selected and many decision variables have been locked. At this stage, the assessments need to point to consequences of selecting different products, equipment or measures, such as what fire alarm system is required, where the detectors should be placed, and what sensitivity the detectors need.

4.5 Putting it together

In summation, then, we have future buildings and road tunnels that are to serve some purpose and cover human needs. In most cases, safety is an important function. For instance, residential buildings are designed to give people shelter from the elements, and road tunnels may be designed to replace accident-prone stretches of the open road. However, all our activities lead to some future consequences, some of which may be considered as losses or negatives. At the time of design, the future consequences are uncertain. We do not know whether they will occur or what their magnitude will be if they should occur. This is the risk that is involved, for someone, with carrying out an activity. The major challenge is to balance different concerns and fundamentally to attain designs that are fit for their purpose (Blockley & Godfrey, 2000).

A large system is involved in reaching decisions about design and safety. For instance, we have professionals, such as safety scientists and fire safety engineers, whose aim is to develop new knowledge and systematize existing information and knowledge. The work they are doing is based on fundamental worldviews, scientific methods and conventions, models, techniques and principles. Moreover, we have safety legislation, either prescriptive or performance-based, and we have design processes that create interactions between those having a need, designers and other stakeholders. Safety legislation is dependent on the status of science and engineering knowledge. For instance, should the height of a timber-frame constructed building be limited by political consensus, or are we in a position to trust science and engineering to reach appropriate decisions? Furthermore, safety legislation affects the way design processes are organized. For instance, the actors who are involved in a design project and at what time they are involved depend upon national requirements for competency and building application processes.

The aim of this thesis is to explore elements of this complex system for attaining designs that are fit for their purpose. Especially, the focus is on the perspectives of *risk-informed thinking* (e.g., Aven, 2012a) and *systems thinking* (e.g., Leveson, 2011b) for safety engineering. A fundamental question is associated with the appropriateness of the scientific foundation, connected to the nature of engineering knowledge and thinking, and the nature of complex socio-technical systems and design processes.

5 RESEARCH APPROACH

5.1 Background for the research

The major issue on which it was hoped that this work could shed some additional light is: *what promotes and inhibits performance-based safety management of design processes?* Factors associated with this question may be considered the dependent variables. From the definition of fire safety engineering (FSE), performance-based safety management is the application of scientific and engineering principles and judgments to accommodate specified performance objectives. As depicted in Figure 1, the research was focused around these units: (A) fire safety engineering practice, (B) safety science in general, and fire safety science in particular, and (C) safety regulation. The question could thus be rewritten: what, *in (A), (B) and (C),* promotes and inhibits performance-based safety management of design processes?

Lincoln & Guba (1985:251) emphasize the value of lengthy experience with the field of study in terms of increasing the effectiveness and the efficiency of the formal work. Hence, it should be mentioned that an important background for this work is the author's professional experience with the fire safety engineering business in one of Norway's largest consulting companies since 2004, being involved in some 20-30 projects each year. This involves both fire safety design projects and peer reviews of other consultant companies' designs. A crucial issue, which should be kept in mind here, is the experience that the current performance-based safety management regime is not working properly. Generally, the application of prescriptive design rules is the norm of practice, while scientific principles and discussions of performance objectives, are rather rare exceptions. This background has affected the research approach in terms of narrowing down the research questions and the selections of units for analysis.

During the project the author had the opportunity to be involved in national and European standardization committees. The national work involves participating in Standards Norway Committee SN/K 227, which in 2012 was responsible for the revision of the Norwegian standard *NS 3901 Requirements* *for risk assessment of fire in construction works* (SN, 2012). The European work concerns participation and responsibility for developing a work item concerning risk assessment and evaluation criteria in *Task Group (TG) 1 Fire Safety Engineering*, which is organized under *CEN Technical Committee (TC) 127 Fire Safety in Buildings*. Participation in these committees was helpful in identifying how major concepts in fire safety engineering are interpreted by different actors. The CEN-work also triggered collaboration with Swedish colleagues and a contribution to a paper (Cronsioe, Strömgren, Tonegran, & Bjelland, 2012) that discusses the revised Swedish building regulations as a possible model for performance-based fire safety legislations in Europe. The participation in the standardization committees showed that the identified "a-priori challenges" with maintaining a functional performance-based fire safety management regime was also a major European concern. Generally, the major issue is debates about how to verify that a certain design has an acceptable safety level. Discussions are especially connected to the deterministic fire modeling approach. For instance: What design fire scenarios are appropriate? What occupant loading scenarios are appropriate? What tolerability criteria are appropriate (temperature, toxic concentration, visibility etc)? The risk analysis (probabilistic) approach is also discussed. However, it seems to be a common view that universal risk acceptance criteria are lacking; hence, developments of this approach may be postponed until such criteria exist. This focus on universally true or appropriate values (for scenarios, tolerability criteria and risk acceptance) makes sense in a technical rationality regime for safety science, but is rather meaningless in a holistic, constructivist perspective. This kindled the idea of investigating the scientific framework as one of the independent variables in this study.

5.2 General research strategy

An underlying topic through the preceding sections has been the contrast between technical rationality and an alternative, holistic approach to safety science. This contrast also influences the research approach, i.e., the fundamental paradigm in which the research is conducted (Lincoln & Guba, 1985:250). The technical rationality regime favors research methods associated with the natural sciences. For instance, the hypothetico-deductive method (Popper, 2002) is the foundation of a framework where propositions are deduced from hypotheses, which are tested using controlled and clearly defined experiments. The experiments will either falsify or corroborate the propositions. Generalizing research findings is a major objective of science, and focus is directed at a few clearly defined variables, holding the situational context at an arm's length. The researcher is detached from the situation, collecting "hard" quantitative data that are analyzed in formal language.

The "scientific method" associated with the technical rationality regime has produced a great amount of important knowledge in the natural sciences. However, this does not necessarily mean that it will be appropriate in other fields of research and phenomena, especially phenomena associated with the social sciences and the increasing complexity of socio-technical systems (Checkland, 1999; Wallace & Ross, 2006). An alternative perspective to the technical rationality approach includes taking a naturalist approach to research (Hammersley, 1990; Lincoln & Guba, 1985; Ritchie, 2008). In a naturalistic enquiry, there is less connection between the scientific paradigm and research methods. According to Hammersley (1990:153) a naturalistic research approach *"respects the nature of the social world."* The goal is to understand the world as it is, preferably without seeing it through the spectacles of a predetermined theory or a rigid scientific method.

This thesis builds on a holistic systems perspective on safety science. Buildings, infrastructures and the activities associated with them are complex socio-technical systems. They involve interactions among components that are non-linear, and they involve people with intentions. The system you may want to test in a scientific experiment one day may be a completely different system the next day. In accordance with a holistic perspective on science and the phenomenon involved in this research, it was decided to adopt a research strategy based on case studies (see, e.g., Andersen, 1997; Blaikie, 2000; Gagnon, 2010; Host, Rainer, & Runeson, 2012; Wellington & Szczerbinski, 2007; Woodside, 2010; Yin, 1981, 1994). According to Yin (1994:13) a case study is "*an empirical inquiry that investigates a contemporary phenomenon within its real life context, especially when the boundaries between phenomenon and context are not clearly evident."*

A case study focuses on an individual or single object, rather than a representative sample from a large population (Andersen, 1997; Flyvbjerg, 2006). The key issue is not representativeness, in the statistical sense, but the knowledge that can be attained through studying the specific object. The object refers here to a social unit, such as an individual, a group, a profession or an activity. The formulation of the research questions defines what “the case” is (Yin, 1994). In this study a major focus has been directed at professional, scientific and regulative practice as units for investigation in order to identify possible variables that affect performance-based safety management.

Designing is a social activity that involves actors with different knowledge, ambitions and goals. Moreover, there are external frame conditions, such as political decisions and national economy, which may affect a certain design project. Hence, the object of study is approached holistically, i.e., the case study acknowledges the importance of context in the research situation. The major objective is to achieve a deep understanding of the cases that are being researched. Researchers are encouraged to adopt several methods for data collection and also to obtain data/evidence from different sources. All evidence is of some use, and nothing is automatically disregarded as irrelevant. There is a continuous weighing of the importance/relevance of evidence, checking and corroborating. The aim is to develop a *chain of evidence* (Yin, 1981, 1994). In this thesis the major issue has been investigated from different angles, through different case studies and using multiple types of data/evidence.

5.3 Case studies

In order to shed light on the major issue of this project, research has been conducted as a series of case studies. Six case studies have been conducted in total, each of which aims to cover its specific part in the overall goal to shed light on the dependent variables associated with the question: *what promotes and inhibits performance-based safety management of design processes?* Table 1 provides an overview and description of the different case studies.

Table 1: Overview of case studies.

#	Description of case study	Unit of study	Variables
A	Fire safety engineering practice in Norway in the period from 1997-2012. Important contexts are the performance-based fire safety regulation regime that was introduced in 1997 and the contributions/interactions with fire safety science and general safety science.	A professional practice	Methodology, building characteristics, deviations from prescriptive design rules, regulative framework
B	Fire safety science's treatment of major concepts associated with the measurement of safety levels and safety margins. Important contexts are philosophy of science, general safety science and engineering epistemology.	A scientific practice	Scientific foundation, methodological issues, approaches for decision making
C	40 different fire safety configurations (fire safety strategies) of multi-story residential apartment buildings. Important contexts are the fire safety engineering practice and the fire safety regulations.	An engineering methodological practice	Building characteristics, fire safety measures, value of model parameters
D	Application of an engineering approach/ methodology to a specific design example: a concert hall. Important contexts are the regulative and scientifically methodological assumptions about decision making in FSE.	An engineering methodological practice	Building characteristics, methodological issues, scientific foundation, regulative framework
E	Risk analyses and uncertainty management in the Rogfast road tunnel project. Important contexts are the Norwegian safety regulations for road tunnels and risk analysis research.	An engineering process	Uncertainty treatment, risk concept understanding, regulative framework
F	Application of the TRANSIT Bayesian Network model for risk analysis in road tunnels generally, and the Rogfast tunnel specifically. Important contexts are the engineering practice and epistemology and risk analysis research.	An engineering process	Risk analysis practice, decision-makers' needs, road tunnel characteristics, use of models

Table 2 shows the connection between the research questions (RQs), the case studies and the papers included in Part II. The RQs presented in section 1.5 are repeated here:

- *RQ 1:* What characterizes current fire safety engineering practice after the introduction of performance-based regulations and promotion of scientific engineering principles?
- *RQ 2:* How are the concepts of "safety" and "safety level" reflected in the fire safety engineering research community?
- *RQ 3:* Why are current fire safety engineering practice, fire safety science and fire safety regulations focusing on "relative safety" and the associated "equivalence approach" for evaluating fire safety levels?
- *RQ 4:* What can we learn from current engineering practice, safety science and regulations in order to promote performance-based safety management of design processes in the future?

Table 2: Connection between RQs and the case studies A-F.

RQ #	**Case studies** [1]						**Papers** [2]
	A	**B**	**C**	**D**	**E**	**F**	
1	M	S	S	S	-	-	1,2,3,(4)
2	S	M	S	S	-	-	(3),4
3	-	-	M	M	-	-	5,6
4	S	M	S	S	M	M	4,7,8

[1] M = Main contribution, S = Secondary contribution

[2] A paper's secondary contribution illustrated by parentheses

5.4 Sources of data/evidence

The different sources of data/evidence for the thesis are described in Table 3. I have tried to illustrate how the different sources of data/evidence connect with the research questions and case studies. For instance, literature surveys were relevant as data to all four research questions and all six case studies. Another example is that fire and smoke simulations were conducted using the Fire Dynamics Simulator (McGrattan, McDermott, Hostikka, & Floyd, 2010) as input to answer research question 3 in case studies C and D.

Table 3: The sources of data/evidence and connection with research questions (RQ) and case studies.

	What promotes and inhibits performance-based safety management of design processes?				**Input to case studies:**
Sources of data/evidence	**RQ 1**	**RQ 2**	**RQ 3**	**RQ 4**	
Literature surveys: fire safety science, safety science and design science	X	X	X	X	A,B,C,D,E,F
Fire safety regulations in the building industry	X		X	X	A,B,C,D
Safety regulations in the road tunneling industry				X	E,F
Documentation from FSE projects	X		X		A,D
Fire and smoke simulations: available versus required safe egress time (ASET versus RSET)			X		C,D
Risk analyses			X		C
Papers	1,2,3,(4)	(3),4	5,6	4,7,8	

5.4.1 Literature surveys

Literature searches were performed on several topics to develop an understanding of current research developments. The following databases were mainly used: Scopus, Science Direct, IEEE Xplore, SpringerLink, Bibsys (Norwegian public library search engine), Google Scholar and Google, and ISI Web of Knowledge. In addition, searches were conducted on public databases associated with recognized institutions within their fields of research (e.g., Lund University, Sintef Norway, SP Sweden, National Institute of Standards and Technology and the National Research Council Canada). Literature surveys have been conducted on the subjects: fire safety science; general safety science; risk research and design science.

5.4.2 Documentation from fire safety engineering projects

Data were collected from current Norwegian fire safety engineering projects in order to answer research question 1, which is related to understanding current practice. It was decided to collect documentation from construction projects since 1997, when a performance-based regulation regime was introduced. There is no public archive for design documentation in Norway. The documentation was thus requested by sending an initiating letter to approximately 50 private and public property developers/owners. To follow up, we emailed the initial letter to the original recipients of the letters and called them. We received documentation on 75 different projects from 21 different property developers/owners (Bjelland & Njå, 2012a, 2012b). Another approach could have been to collect data directly from fire safety engineering consultant companies. Given that the companies had been willing to participate, it would probably have been easier to collect the data. Nevertheless, the main reason for not asking consultant companies was the risk of receiving only “favorable projects,” i.e., projects where the consultant company were especially satisfied with their work.

The data covering current fire safety engineering practice were analyzed by investigating central concepts and methodologies. Selection of the analysis’ focus was based on personal experience with the business and major emerging trends from the documentation. For instance, a major issue was related to how fire safety engineers used the risk concept and evaluated a safety level. This issue has been heavily discussed in the business, both nationally and internationally, since the introduction of a performance-based fire safety regulation regime in the 1990s. A qualitative methodology was applied, with an aim of understanding the meaning of central concepts and the characteristics of design processes.

5.4.3 Fire and smoke simulations and risk analyses

Risk assessments and simulations were conducted to pinpoint the methodological challenges, the task associated with research question 3. The analyses and simulations may be regarded as case studies, based on the foundation of collected documentation from construction projects and work carried out in the author's master thesis (Bjelland, 2009). The risk assessments were conducted by the application of a standard methodology (identified through current practice) of 40 variants of possible fire safety designs for residential apartment buildings (Bjelland, 2009; Bjelland & Njå, 2012c). The analyses included event trees, Monte Carlo simulations and fire development simulations using the computational fluid dynamics (CFD) code Fire Dynamics Simulator (FDS). The FDS, as well as egress calculations, was also applied to analyze and compare a prescribed reference design against an alternative design in order to demonstrate challenges with "the equivalence approach" in Bjelland & Borg (2013).

5.4.4 Participating in the Rogfast planning process

A colleague Ph.D. student and I also had the opportunity to participate in the Rogfast subsea road tunnel project in Rogaland, Norway. The project was considered especially interesting for this thesis, as it will be the longest and deepest road tunnel in the world, challenging the limitations of prescriptive regulations. The Rogfast may be a good example of the type of "novel design" in which we are most interested here. Participation in the project involved meetings with the project management team and project meetings with the rescue services and members from the affected municipalities. Resulting data include notes and minutes from the meetings that express the different parties' concerns about risk, safety and uncertainties in the project and design specifications and documentation, which comprised the fundamental data material for paper 7 (Bjelland & Aven, 2013).

5.5 Developing methodology

The case studies initiated in this project initially had a descriptive, or interpretative, purpose (Andersen, 1997). The goal was to achieve better understanding of fire safety engineering practice, fire safety science and its relation to fire safety regulations (cf., Figure 1). Nevertheless, with increased understanding it becomes possible to pinpoint insufficiencies, and possible solutions to such insufficiencies may emerge. A fundamental assumption of case study research is to keep an open mind: *"In naturalistic case study research, theorizing emerges. That is because you cannot usefully theorize in* *the absence of evidence, or on very little. The evidence you look at is initially dictated by your broad aims. But increasingly it is directed by your successively revised theories or explanations. And it is negative or complicating evidence that precipitates these revisions"* (Gillham, 2010:35).

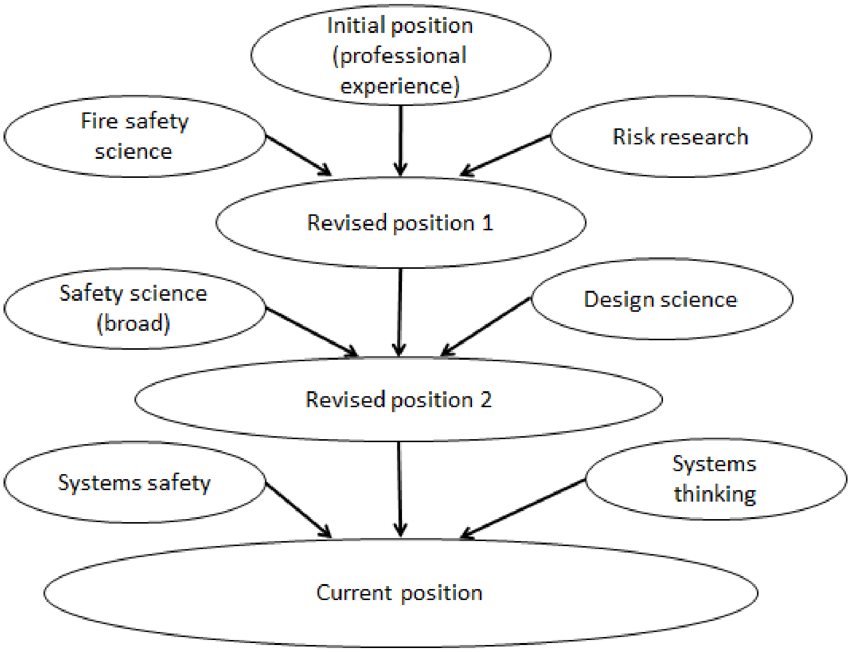

Figure 6: Deepening understanding in case study research.

Figure 6 depicts the evolution of my process from my initial position and worldview to my current position and worldview. The initial aim was to research the application of risk analysis methodology in fire safety engineering. This aim was based on personal interest and my current experience with the Norwegian fire safety engineering business. It seemed as if there was a gap in knowledge and methods with regard to implementing risk analyses effectively in the Norwegian building sector. Research was initiated with a case study on Norwegian fire safety engineering projects (Case Study A), which revealed the need to read up on fire safety science and risk research. This led to a revised and broader position of the reality (revised position 1).

A fundamental realization at this point was that risk analyses and the risk concept played a minor role in Norwegian fire safety engineering practice. In order to understand why, a literature survey was made into design science and safety science in a broader sense. At this point, an alternative could have been, for instance, to interview fire safety engineers or conduct protocol analyses of engineering-in-action. However, design science deals with, among other things, how practitioners, i.e., designers, think and work, and how design processes evolve. As such, it was anticipated that knowledge gained from design science research could deepen understanding of fire safety engineering practice as well, and parallel with developing a broader view on safety science, a new worldview emerged (revised position 2).

The final development towards my current position involves tackling problems related to dealing with socio-technical system complexity. This led to research into systems thinking and systems safety. The current position is described in section 5 in paper 4 (Bjelland, et al., Submitted). A proposed framework that builds on a constructivist systems thinking approach to fire safety engineering emerged from the data (in a broad sense). The next step would be testing the theory empirically, although that is outside the scope of this thesis.

5.6 Discussion of research approach

The major issue of the thesis was to identify what promotes and inhibits performance-based safety management of design processes. Generally, the performance-based approach is most fruitful in cases where there are no prescriptive design rules. This often involves novel cases, often those with large complexity. The case study research strategy was selected due to its ability to include complexity and context. The focus is on what is particular and special to the case, not necessarily on what is generalizable. Moreover, the case study approach allows inclusion of several methods for obtaining data or evidence. Finally, a case study of a particular and special case will always lead to the creation of new knowledge. The question is whether this new knowledge has any significance or relevance. In what follows, I will discuss some issues that may be subjected to criticism when using the case study research approach and its use in this project.

5.6.1 Sources of data/evidence

Within the technical rationality regime, quantitative data and analyses are preferred to qualitative (Wallace & Ross, 2006). The idea is that quantitative data and analyses lead to more precise results and are easier to reproduce. However, quantitative data and analysis do not guarantee an appropriate result on their own. There is, for instance, a need to determine beforehand what variables to measure and how to categorize them. Thus, the discussion about the "inherent appropriateness" of certain types of data and analysis is considered meaningless. The real issue is whether the data and analyses have managed to capture the essence of the phenomena studied and whether the data are represented accurately enough for others to replicate the study. Generally, no source and type of data or analysis methods have been favored or disfavored. The most appropriate method, considering the available data, has been selected. For instance, if more data material had been obtained in case study A, a quantitative analysis may have been conducted. In order to obtain good results from case study research, the application of multiple methods and data sources is encouraged. The idea is that if data from different sources converge towards the same result, confidence in the results may be increased. This is also known as triangulation (e.g., Blaikie, 2000; Yin, 1994).

The case studies investigate the subject from different angles in order to gain a broad perspective, or a deep understanding, of the major issue. Case study A involves a qualitative empirical analysis of project documentation from the Norwegian fire safety engineering industry.

Case study B is a discussion of theory developed in fire safety science on the concepts of safety level and safety margin. The discussion points to weaknesses in the current framework from a holistic perspective, which leads to methodology development in order to improve such weaknesses.

Case study C, associated with 40 different fire safety concepts for residential apartment buildings, and case study D, the application of a fire safety engineering approach to a specific building, are quantitative studies that aim to test the current practice. Both these case studies may be seen as examples of attempts to falsify current fire safety engineering and regulative practice.

Case studies have been developed in which the current practice should have been efficient, and it is shown that the current practice is not efficient.

Case studies E and F both involve the Rogfast road tunnel project, but the unit of study is different. In case E the unit of study is an engineering process, i.e., the risk analysis and uncertainty management process. In case study F, the unit of study is an engineering process using a new Bayesian Network model for risk analysis. Both case studies involve theoretical discussions with respect to what is good engineering practice in uncertainty management and risk analysis. Based on the theoretical discussions and comparisons with empirical findings, inconsistencies are identified. The resulting suggestions for improving current practice may be seen as examples of developing methodology on the basis of evidence/data.

In sum it is argued that the case studies cover the major issue from a broad scientific and empirical foundation. The work may be seen as an evolution towards the current position (cf., Figure 6). At this point, challenges with the existing engineering, scientific and regulative practices have been pointed out and suggestions for improvements have been developed. The next stage would be to test the developed methodology with new data (cf., section 9.2).

5.6.2 Generalizability

Case studies are criticized for their inability to produce generalizations, but this is a misunderstanding (Andersen, 1997; Blaikie, 2000; Flyvbjerg, 2006; Wellington & Szczerbinski, 2007). In order to accommodate such a critique, the researcher may initiate a search for "typical cases." The idea, then, is to create generalizability through inductive statistical inference. However, this is not the kind of inference that is relevant to case studies. Rather, the aim is to enable generalization from the individual case to new instances through logical inference. Logical inference *"is the process by which the analyst draws conclusions about the essential linkage between two or more characteristics in terms of some systematic explanatory schema – some set of theoretical propositions"* (Mitchell quoted in Blaikie, 2000:223). Hence, instead of being concerned with "representativeness" of the individual case in a narrow sense, it is more appropriate to be concerned with the appropriateness of the case. For instance, the degree to which findings from the Rogfast case study will be generalizable to new instances depends on the Rogfast case's appropriateness in pinpointing critical issues also relevant to the new instances. The point is that, although the studied case is unique in some sense, it also has similarities with other cases, and this is where the knowledge may be generalized. Yin (1994), on the other hand, is more concerned with multiple case studies that may cumulatively produce generalizations. In this sense, the total set of case studies conducted in this project with the aim of supporting a common major issue may be seen as a way of working towards a generalization.

5.6.3 The case studies' coverage of the major issue

The major issue of this thesis is quite broad in asking what promotes and inhibits performance-based safety management of design processes. It was decided early on to look only at engineering practice, safety science and regulations. Still, this is quite a broad task for a Ph.D.-project. Six case studies have been conducted to provide a foundation to shed light on the major issue.

An obvious critique to this approach is that the case studies only cover a fraction of what may be important to answer the major issue. For instance, what about the role of national/European standardization or the management of individual projects? It is certain that the case studies conducted in this project do not cover all relevant issues for the major issue. This must be considered a major risk to the theories developed. However, I believe that the traditional framework for fire safety engineering has been broadened. Moreover, the proposed frameworks to future safety engineering (see Bjelland & Aven, 2013; Bjelland, et al., Submitted; Borg, et al., Submitted) are open to include new knowledge. In Bjelland et al. (Submitted) we argue that the key issue is that *"systems need to be designed for change."* This may also be said about models and frameworks for the design activity (LeCoze, 2005).

6 MAJOR FINDINGS

The major findings from the papers are presented in this section. The research associated with the thesis started by exploring the field of fire safety engineering (research question 1) in a search for factors that promoted and/or inhibited performance-based safety management of design processes. The findings from the initial research led to the development of new research questions and focus areas.

For instance, it was found that the practitioners had few reflections around concepts such as “safety level” and “safety margin.” The concepts seem to be closely connected to design solutions from prescriptive fire safety codes. Similar findings were obtained from the road tunneling sector. In both sectors, risk assessments has been introduced and promoted as a tool to show that alternative solutions (than specified in the prescriptive code) have an equivalent safety level. Hence, it should be possible to evaluate fire safety design rather independently of the prescriptive code/guide. This has not happened, which led to development of research questions 2 and 3, dealing with fundamental understanding of the concepts of safety level and safety margin and the methodological challenges in current fire safety engineering practice.

The research associated with research question 1, 2 and 3 is mainly concerned with current practice, safety research and regulations. Based on findings from these efforts, it should be possible to make some claims about the future direction of safety engineering towards what promotes and inhibits performance-based safety management in design processes. This is what we are mainly concerned with in part 4 and what leads to the following structure of this section:

- Part 1: Understanding current fire safety engineering practice
- Part 2: Broadening understanding of major concepts: safety level and safety margin.
- Part 3: Understanding current methodological challenges
- Part 4: Relevant learning for the future

Table 4: Structure of findings, research question and associated papers.

Part no.	**Research question**	**Paper no.**
1	What characterizes current fire safety engineering practice after the introduction of performance-based regulations and promotion of scientific engineering principles?	1, 2, 3
2	How are the concepts of "safety" and "safety level" reflected in fire safety engineering research?	4, (3)
3	Why is current fire safety engineering practice, fire safety science and fire safety regulations focusing on "relative safety" and the associated "equivalence approach" for evaluating fire safety levels?	5, 6, 7
4	What can we learn from current engineering practice, safety science and regulations in order to promote performance-based safety management of design processes in the future?	7, 8

6.1 Current fire safety engineering practice

Although performance-based regulations exist within the Norwegian building industry, fire safety engineering based on prescriptive design rules is, by far, the most common approach. Fire safety requirements for buildings are determined by classifying them into predetermined categories dependent on characteristics such as their expected usage, height, floor area, and so on (Bjelland & Njå, 2012a, 2012b, 2012d). This is also common within the Norwegian road tunneling industry (Bjelland & Aven, 2013). The performance-based aspect of the legislation seems to be relevant to handle deviations from the prescriptive design rules. When deviations from common design rules are introduced, there is a focus on verifying that the alternative solution is at least equally safe as the prescribed solution ("the equivalence approach") (Bjelland & Aven, 2013; Bjelland & Borg, 2013).

In the building industry, fire safety engineers usually adopt a deterministic analytical approach, for instance the calculation of available safe egress time (ASET) versus the required safe egress time (RSET). The concept of risk and probabilistic analyses are uncommon. Uncertainties are seldom addressed specifically in the analyses. Rather there is a focus on identifying and applying “conservative assumptions” (Bjelland & Njå, 2012b).

The current practice in fire safety engineering leads to a narrow view on what is relevant design knowledge. The focus on prescriptive design rules fails to emphasize special characteristics of the projects. Instead of discussing safety, it is often a discussion of whether it is “better or worse” than a prescriptive solution. This may include great emphasis on finding an appropriate prescriptive reference building, rather than focusing efforts on safety engineering (Bjelland & Borg, 2013; Bjelland & Njå, 2012b). Similar remarks apply also for the road tunneling industry (Bjelland & Aven, 2013).

6.2 The concepts of safety level and safety margin

Research into current practice in fire safety engineering showed that reflections about major concepts such as safety level, safety margin and risk were given little attention (Bjelland & Njå, 2012b, 2012d; Bjelland, et al., Submitted). It was hypothesized that the knowledge from fire safety science is reflected in fire safety engineering practice. Hence, it became important to also investigate how major concepts are reflected upon in fire safety science. It was decided to focus on safety level and safety margin.

Our main findings are that fire safety science builds on the ideals of the natural sciences. The original phenomena research in fire science aims to discover the underlying relationships that govern, for instance, fire growth and human behavior in fire situations. This view is denoted “technical rationality,” where knowledge is mainly gathered from scientific experiments, i.e., using “the scientific method.” When fire safety engineering became more common in engineering practice, fire safety science increasingly started focusing on decision making. Many methods and associated decision rules were suggested. A common trait for these methods is that the focus is on decision making rather than on discovering the truth. This may be seen as more of a pragmatic instrumentalist approach to science. Major efforts have been made in previous decades to mechanize decision making to obtain consistency in fire safety engineering. This largely involves research into methodologies such as fire and egress modeling, risk ranking methods and risk analyses. Lots of knowledge has been produced, but the goal of mechanizing decision making has still not been reached. Safety is usually considered relative to a prescribed reference-design or as the inverse of risk, and in both cases there is a fundamental focus on the equivalence approach for evaluating safety (Bjelland, et al., Submitted).

Our analysis suggests that the concept of safety is linguistically flexible. There is no need to restrict it to other concepts, such as risk or safety measures. Originally safety referred to an ideal situation or state. This is also our interpretation in paper 4, where we suggest a framework for fire safety engineering that circumvents the use of the concept of risk (Bjelland, et al., Submitted). It is suggested that buildings may be perceived as continuously changing systems, where safety must be managed in order for the system to be kept within a safe state. The system is kept within a safe state by imposing safety constraints on the system's behavior or freedom, inspired by system theoretical perspectives adopted from, for example, Perrow (1999), Leveson (2004, 2011b), Blockley and Godfrey (2000), Checkland (1999) and Rasmussen (1997). Based on a constructivist view of safety measurements, the ideal of a mechanistic decision process is rejected. Instead, it is argued for a clear separation between analysts and decision makers. The role of the engineers is to explore system performance against safety objectives and possible loading scenarios, where the aim is to develop a control structure for safety management. It is suggested that the strength of the engineers' documentation may be built and judged on the basis of general coherence principles (Bjelland, et al., Submitted).

6.3 Methodological challenges

As stated earlier, the application of analytical approaches to engineering is usually introduced only when there are deviations from prescriptive design rules. In order to verify that the fire safety goals are fulfilled, we find that the fire safety designers often use subjective and qualitative arguments. Quantitative analyses involve deterministic modeling using empirical equations from the fire safety science literature and simulation models for fire and smoke spread and egress. There is seldom any reference to guidance documents that have been published in order to standardize the design processes on a national level. Moreover, there were generally lacking references to international guidance documents published, for instance, by the International Organization for Standardization (ISO), the European Committee for Standardization (CEN), the British Standards Institution (BS), the National Fire Protection Association (NFPA) and the Society for Fire Protection Engineers (SFPE) (Bjelland & Njå, 2012a, 2012b).

In cases where analytical approaches are applied, safety is usually considered relative to a prescribed design solution, i.e., using the equivalence approach. This causes several challenges, for instance:

- *Lack of consistency:* Bjelland & Njå (2012c) present the findings from a comparative analysis involving a total of 40 different variants of fire safety design solutions for residential apartment buildings. An important finding from the analysis is related to the lack of consistency of prescribed solutions using the common conceptions and methods of thinking about fire safety. It is nearly always possible to find a prescribed design variant that has a higher risk than that of an alternative design.
- *Wrong analytical focus:* The application of the equivalence approach directs attention towards finding an appropriate reference design and assessing the differences. This leads to less focus on assessing the safety of the proposed design (Bjelland & Borg, 2013).
- *Cannot handle novel designs:* Prescriptive design rules are based on prolonged experience. Consequently, for novel designs there cannot, in principle, be any applicable prescribed design rules. Hence, the equivalence approach fails to guide decisions in such situations (Bjelland & Aven, 2013).

Borg et al. (Submitted) discuss the proposed application of a risk analysis methodology based on Bayesian Networks (BN) in the road tunneling industry (TRANSIT). A major challenge is associated with the transition of the full range of engineering knowledge into probabilistic knowledge. For instance, engineering knowledge may be tacitly understood. Hence, the engineers do not always know why or how they know something (Polanyi, 1962; Rust, 2004; Schön, 1991; Wood, et al., 2009). When this knowledge is to be transformed into conditional probabilities or distributions, there is a chance that something “gets lost in the translation.” The resulting perspective on relevant knowledge for design becomes narrow. We find this unfortunate from a design research perspective (Borg, et al., Submitted).

6.4 Contributions to the future of safety engineering

6.4.1 Learning – a challenge for the engineer

Design problems are seldom clearly stated but co-evolve along with possible problem solutions in a spiral process. In order to reach good design solutions, the designer constantly must reframe the problems and situations (Dorst, 2011; Schön, 1991). This is an inherently creative process, where thinking outside the common conceptions, categories and linking patterns is a vital ingredient (de Bono, 1990).

Standardized safety assessment processes and mechanized decision processes tends to lead to the opposite. The major purpose of the analytical safety assessments becomes quality assurance or verification with reference to the legislation. Instead of promoting a lateral thinking process, it will lead to vertical, or “silo,” thinking. The focus will be on gaining greater knowledge about the predefined categories and linking patterns. The depth of the silo determines the status of the knowledge. For instance, in the TRANSIT case (Borg, et al., Submitted), this may result in gaining knowledge about the defined variables and conditional dependencies among them. The more knowledge we gain on these variables, the deeper the silo gets. This focus may block the ability to see that there may be other important variables or other linking patterns that are not included in our common way of thinking. That is, we need to see beyond the silo and search for connections that may not be obvious within our conventional categories.

6.4.2 Dealing with risk and uncertainties

There are different views on how to understand risk in the academic environment and among practitioners, as well as different views on how important uncertainties are with respect to decision-making processes. Our perspective on risk is broad by defining risk as the two-dimensional combination of consequences and associated uncertainties (Bjelland & Aven, 2013). The risk assessments should focus on prediction of observable events and consequences and on description of uncertainties. The uncertainties are related to our lack of knowledge about whether these events and consequences will occur, not to the deviation between estimates and true values of thought-constructed parameters of probability distributions, which is the dominant view.

Through our proposed framework, we argue that greater emphasis will be placed on the background knowledge on which the risk assessments are conditioned. This will hopefully lead to discussions and assessment about the quality of the background knowledge, as decision-makers would be made explicitly aware of what assumptions are needed to support a conclusion or recommendation. Consequently, the decision-makers must not only consider the conclusions of the assessment but also the background knowledge on which is it based (Bjelland & Aven, 2013).

6.4.3 Focusing on safety performance

In Bjelland et al. (Submitted), we explore the possibility of examining safety performance of systems without using the risk concept. Current fire safety engineering practice shows that the risk concept is not commonly adopted. Still, fire safety science perceives the risk concept as fundamental to solving future fire safety engineering problems. The previous couple of decades show a vast number of articles that focus on developing methods for calculating risk and making decisions from risk results. However, the search for objective risk and decision criteria seems futile (Bjelland, et al., Submitted).

Fire safety in buildings, it is argued, is a system property. It involves technical systems, people and interactions with the environment. Systems are continuously changing, as are our perceptions of what is an acceptable level of safety. It all boils down to perceiving decisions about safety as subjective. It could be argued that a framework based on the risk concept and the methods of quantitative risk assessment leads to mathematical rigor and precision. In a positivistic worldview, such a framework makes a lot of sense, and the positivists influence on risk assessments has been dominant (e.g., Aven, 2012a; Renn, 1992; Shrader-Frechette, 1991). However, if we acknowledge that decisions about safety are subjective, there might not be the same need for mathematical rigor and precision. Recently, we have seen that the field of risk research and risk assessment is rejecting the positivist worldview and adopting more of a constructivist approach. For instance, it is acknowledged that uncertainty is more than probabilities (Aven, 2012a). In practice, this calls for a clear distinction between the analysts and decision makers, acknowledging that the application of mechanistic risk acceptance criteria is excessively simplistic.

It could be questioned, then, what advantage safety assessments based on the risk concept have on safety assessments based on other concepts, such as the concept of safety itself. It could be argued that approaches to safety based on the risk concept is one language, while approaches to safety based on the safety concept is another language. Both may be applicable in certain situations. However, in paper 4 we argue that engineers may be more comfortable speaking the language of safety rather than risk. Discussing safety performance of systems and the behavior of important phenomena is simply closer to the engineering epistemology than probabilities and uncertainty.

Inspired by authors such as Perrow (1999), Rasmussen (1997), Blockley and Godfrey (2000) and Leveson (2004, 2011b), we set out to develop a framework for fire safety engineering based on the concepts of safety and safety margins. The framework is founded on the principle of safety constraints, based on coherence theory, resilience engineering and systems theory, combined with fire modeling approaches (Bjelland, et al., Submitted).

6.4.4 Safety regulations

Papers 4 (Bjelland, et al., Submitted) and 7 (Bjelland & Aven, 2013) may be seen as two different approaches to safety engineering. In paper 7 we address the risk concept and associated engineering approaches, while in paper 4 we address safety engineering simply by applying the concept of safety itself. As argued in the previous section, the two approaches may be seen as two different languages of safety engineering.

A common foundation for both approaches is the need for a performance-based legislation regime. Paper 4 is concerned with fire safety engineering in the building industry, while paper 7 is concerned with the road tunneling industry.

A major disadvantage with the current road tunneling legislation is the lack of operational safety goals and performance-requirements. Safety is generally defined through the set of prescribed solutions based on tunnel classes within the handbooks (NPRA, 2010). There is no difference between the *concept of safety* and the *means to achieve safety*. This promotes comparative analyses or the equivalence approach, with the weaknesses described in section 6.3 (see also Bjelland & Borg, 2013; Bjelland & Njå, 2012b). This may lead to design processes going into the *intelligence trap*, which may be described as providing logically sound answers to the wrong problems. Consequently, one may end up selecting poor designs even though the analyses conclude the opposite.

Although a performance-based legislation regime is present in the building industry, we find that it is more common to apply the option of using prescriptive solutions there as well. There may be many reasons for this. However, in order to meet the challenges represented by novel design proposals, the performance-based option should be strengthened.

To increase the impact of information gained from safety engineering and to promote good risk or safety assessment processes, we argue for a transition from prescriptive to performance-based regulations within the road tunneling sector (Bjelland & Aven, 2013) and for a strengthened focus on safety objectives in the building industry (Bjelland, et al., Submitted). In both cases, it involves making clear what we want to achieve by our designs and structures.

7 DISCUSSION

The following sections will discuss the traditional safety engineering framework with regard to *engineering practice*; *scientific practice*, and *regulative practice* in light of the research findings and theoretical framework of this thesis. The discussion is based on the following set of assumptions from the technical rationality regime, which may be questioned:

- There exists an objective threshold that describes an acceptable level of safety.
- The objective threshold for acceptable safety is given (although implicitly) by the prescribed solutions.
- Only the variables manipulated by prescriptive solutions are relevant for safety design.
- Analyses have the main purpose of verification, i.e., to reveal the relative differences between a design proposal and a reference design.

7.1 Engineering practice

Aven, et al., (2004) provide a general model for safety management, in which safety is managed through the identification of safety goals and associated means to achieve these goals (cf., Figure 7). In addition there is a need to take into account the frame conditions by which goals and means are derived. The model is sensitive to what level of the system hierarchy it is being used. For instance, regulations are an important part of the frame conditions for engineers and designers in a construction project. However, for the national authorities the regulations are the means by which safety is managed.

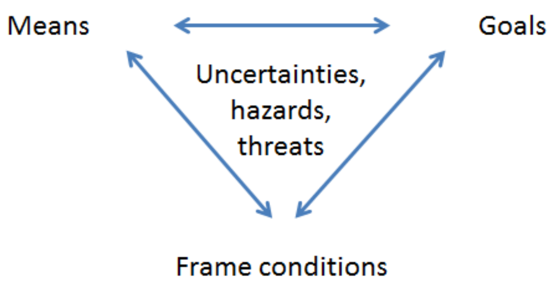

Figure 7: A model for safety management (adopted from Aven, et al., 2004:68).

The traditional approach to safety engineering builds on a technical rationality framework (Bjelland & Aven, 2013; Bjelland, et al., Submitted). Such a framework will affect how the safety management model is perceived. For instance, safety will be regarded as an objective property of the designs. This may affect how goals are stated, emphasizing clear distinctions between acceptable and unacceptable safety. Moreover, in order to evaluate whether safety is acceptable or unacceptable, the traditional approach includes decomposition of systems into their constituent parts, where quantitative models are available. Hence, focus is naturally directed towards the technical (hard) part of the system. This system view is part of the frame conditions, which affect both how goals are stated and what means are considered appropriate to achieve the goals. For instance, focus on the hard part of the system tends to increase focus on the reliability of technical components and strategies like redundancy or defense-in-depth (Leveson, 2011b; Perrow, 1999).

The traditional approach to safety engineering is challenged through work within a constructivist scientific framework to safety and risk (e.g., LeCoze, 2005, 2012; Nilsen & Aven, 2003; Wallace & Ross, 2006) and systems thinking (e.g., Blockley & Godfrey, 2000; Checkland, 1999; Leveson, 2011b). The alternative approach to safety engineering will greatly affect the boundary conditions in terms of how a system is perceived. While the traditional approach makes a clear distinction between a closed system and its environment, the systems approach views complex socio-technical systems as open to the environment. This affects the boundaries of engineering analyses in terms of broadening the scope of what to include in the system and who is to be included among the system's stakeholders. This will affect the way goals are stated and what means are relevant for safety management.

The major issue here is that the fundamental view of science, engineering and safety affects all important parts of the safety management process. For instance, it affects what type of knowledge is perceived as good or bad; whose opinions are worth taking into account; how systems are defined; and how safety is achieved. A too narrow framework on the fundamental issues (science, engineering and safety) could lead to great restrictions on the safety management process. This may be of minor importance in normal design processes that deal with standard buildings and infrastructures. The potential for improving safety may be minimal, and tradition has led to an evolutionary development of designs that function appropriately. However, when faced with novel needs, problems and design proposals, tradition may be a deceitful companion. The traditional approach to safety engineering may be more of a straightjacket that inhibits creativity and innovation than a fruitful framework for safety management. A broader framework may be needed. Although Newton's theories still are appropriate for the majority of practical cases, Einstein's theories have a greater explanatory power in certain special cases and, thus, may be regarded as more fruitful for future scientific endeavors (Checkland, 1999). With no comparison of the theoretical significance, the point is that, although the traditional framework seems to function appropriately in the majority of cases, it may still be contested – and more appropriate theories may be adopted.

7.1.1 Knowledge in safety engineering

In general, the traditional approach has an impersonal focus of knowledge. The idea is that knowledge may be formalized into structural models, standard data, quantitative laws, and predetermined decision criteria. Consequently, it should not matter who is designing a building as long as the designer is in possession of the standard, relevant knowledge within the engineering discipline.

This view of relevant designer knowledge stands in sharp contrast with how great designers think and work in practice (Bjelland & Njå, 2012a, 2012b;

Cross, 2011; Lawson & Dorst, 2009; Schön, 1991). Although quantitative models may lead to rigorous results, they are only useful to some extent and do not tackle the most important and fundamental problems of design. Technical rationality cannot bring clarity in cases of ill-structured and multi-faceted problems the way skilled, experienced practitioners (reflective practitioners) can.

A fundamental challenge associated with the traditional engineering regime is the simplifications that are necessary in order to impose the tools of technical rationality. For instance, it is necessary to assume that the actual problem to be solved is clearly defined. This is seldom the case in design projects. Although the project owner has some idea about what he/she wants, the underlying goals and values may not be clearly defined before several design proposals have been tested. Moreover, there are many stakeholders who similarly may be unaware of their concrete values and goals. Design processes are, thus, more circular than linear processes, going back and forth while testing different aspects associated with the design. Designing is an act of balancing different values and goals. Hence, to assume that goals can be predetermined in an objective way, at least in a precise, quantitative way, is another simplification. According to Krippendorff (2006), designers need to understand how others (the stakeholders) understand the design. Hence, designing is not mainly about calculations and evaluations against objective criteria but also about making sense of the designs to the stakeholders in a language they can understand.

Designing is also inherently a creative task. It is about finding innovative solutions to new needs and problems. As a design tool, risk management is, thus, also dependent on creativity, especially in the hazard identification processes. In order to make predictions about the future, which is the goal of risk assessments, one must develop an understanding about what might happen if the system is operated. This includes looking at the system in different contexts and under different environmental situations. The ability to introduce new frameworks, categories and links may be fruitful, especially with respect to identifying accidents that have never happened before.

A key characteristic of the objects involved in design processes is that they do not yet exist. They may come to exist in the future if their performance is predicted to be a good solution to the problems at hand. Michael Polanyi (1962) describes the *“logical gap between existing knowledge and any significant discovery or innovation.”* In terms of designing, our current situation and understanding, combined with our needs and desires, makes us able to perceive an improved world, but we may be inhibited from seeing how to get there.

A designer imagines possible future scenarios, including possible artifacts and environments. Consequently, the designer conceptualizes an improved world and how this world could function. The conceptualized world is imaginary, and there is freedom to adjust all the factors that seem relevant for the design without the boundaries of our current reality. Such imaginary worlds are optional realities on which we may employ known scientific and engineering principles. Furthermore, such imaginary worlds create an environment for catalyzing the application of tacit knowledge: knowledge of which we ourselves are unaware and that science cannot formalize (Rust, 2004; Schön, 1991; Wood, et al., 2009).

Consider the activity of designing a new building. The building owner may have a rather clear specification of what he/she wants before the project is initiated. However, as the designers bring the ideas to life through models and drawings in accordance with the specification, new needs may emerge from the new contexts, leading to the original specification being adjusted or clarified. Similar processes may be present within the design team. Although a design proposal solves the client’s original specified needs, there may be tacitly understood qualities that are not acknowledged or appreciated before the design is brought to life at some level of abstraction. For instance, when the floor plan is drawn, it is possible to picture the activities to be carried out in the building and assess how it will function in specific operational scenarios. Schön (1991:79-102) provides an example of what he calls a reflective conversation with the situation, which involves an architectural design student who, with the help of a skilled design professor, is working to make a building fit into the landscape. The process he is describing is circular, involving framing and reframing the problem based on the challenges posed by new design proposals.

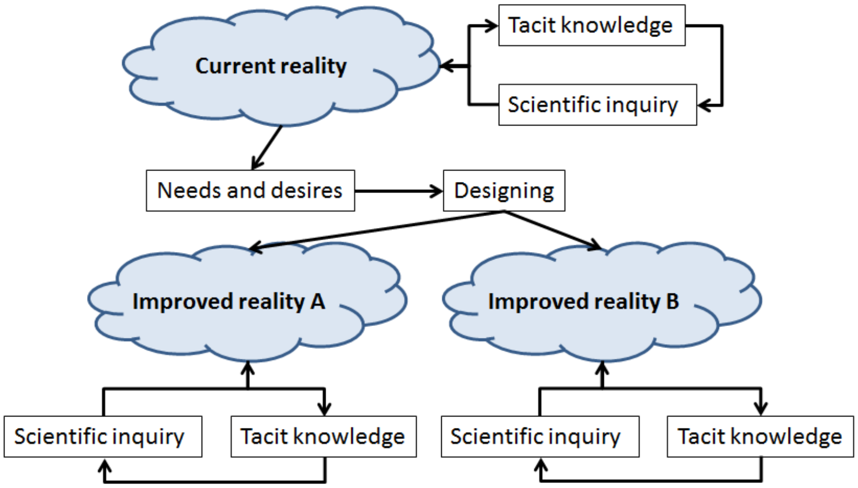

Figure 8: Bridging the gap between current reality and improved realities by designing.

According to Simon (1996:6), artifacts *"have no dispensation to ignore or violate natural laws."* Consequently, designing future improved realities may be supported by our understanding of the natural phenomena that affect artifacts. Our current reality gives rise to scientific inquiry and the accumulation of tacit knowledge through the activities we undertake to understand why certain artifacts work and others do not. When faced with possible and suggested improvements, we activate this knowledge in the design process through scientific inquiry and tacit knowledge (cf., Figure 8).

Our research into design science suggests that there is more to safety engineering than the application of knowledge obtained from the natural sciences. Fundamentally, we are interested less in finding the truth about safety than in the usefulness of the knowledge, models, methods and processes that are being used to propose improved artifacts. While the fundamental concepts of safety and risk may have a sound ontological status, their measurements may be more of an epistemological issue.

7.1.2 From verification of safety to identification of safety constraints

Designing is about proposing artifacts that serve a purpose for some stakeholders. The artifact cannot be realized without its purpose being clarified (Blockley & Godfrey, 2000). However, a clear purpose of the artifact may not exist when the design project is initiated. As the previous section mentioned, the initiation of design projects with the conceptualization of possible improved futures may act as a catalyst, for instance, for the development of stakeholders' goals, values and purposes. Hence, design processes are not linear. Working out a design proposal on an initiating set of goals and values may lead to the identification of a new set of goals and values (Cross, 2011; Dorst, 2011).

Current design processes in the building sector assume linearity in terms of goals and values. The ideal design project progression is the selection of a design alternative early in the design process; this is increasingly detailed by engineers and architects as the project continues towards execution. Fire safety design is similarly crudely sketched during the preliminary design, assuming the solutions may be verified in a later project phase.

A different approach would be to recognize that designing is not just about developing technical solutions but is also about developing the goals and values by which these technical solutions are to be judged. This implies a new way of thinking about the goal of fire safety design. Instead of assuming that there exists a universal and objective acceptable safety level against which the design should be evaluated, the goal could be to identify critical safety constraints associated with the selected design (Leveson, 2011b).

It needs to be recognized that the design of an artifact proceeds in stages, e.g., following the capital value process (CVP) model (cf., Figure 5) (Kjellén, 2007). The process owner does not want to spend a great deal of resources on verifying the safety level of a number of initial design alternatives. Such efforts would be wasted, as many early design alternatives are scrapped long before they are ever realized. In the early project phases, there is a need for a crude set of decision criteria that take into account a broad set of goals and values. For instance, how are the traffic flow across the Bokn fjord and the environment affected by the different alternatives of a subsea road tunnel, a floating bridge, or gas-powered ferries?

In this early phase, fire safety design must be implemented in terms of crude analyses, engineering judgments and rules of thumb. Detailed analyses at this stage are surely a waste of time and money, considering the nature of developing goals and values in design processes. In most cases changes will be made to early design proposals, rendering detailed analyses practically useless. Hence, flexibility is a keyword in the early stages of a design project. This applies not only to the safety engineers but also to the whole project team. In fact, it also applies to the definition of the system. The system is open to its environment (Checkland, 1999; Wallace & Ross, 2006), and, hence, to the development of goals and values, and the following design proposals also affect what are considered parts of the system and what are considered parts of the environment. For instance, the increasing weight placed on the value "autonomy" may lead to the exclusion of external stakeholders in the system. In a road tunnel project, increased weight on autonomy could, for instance, lead to focus on a "self-rescue" and internal preparedness approach, rather than reliance on the municipality fire and rescue service. As a consequence, the distance between emergency exits may be reduced; the alarm system may be carefully "human-centered designed" to different scenarios, and an automatic sprinkler system may be adopted.

Finally, when the artifact is complete, safe operation must be assured. This is the first time the design is actually tested in reality, and the first time we are able to determine whether the design performs as intended. Our efforts during the design phase are directed into making the final artifact fit to its purpose in reality and the loads to which it is subjected. It makes no sense to state that the design is safe or unsafe on a general basis. The quality of the design is context dependent. Our available knowledge during design (e.g., models, methods, actors and data) makes us able, at best, to predict that the system will be safe during a set of situational circumstances (Bjelland, et al., Submitted; Checkland, 1999; Leveson, 2011b; Wallace & Ross, 2006). At an appropriate time in the design project, it is, thus, important to identify critical safety constraints for the system operation. Critical safety constraints may be, for instance, control actions that have to be imposed on any level of the system hierarchy, e.g., the "safety boundaries" within which one has to operate. Examples of safety boundaries may include the maximum number of people in an assembly building, the maximum amount of fire load in a building, the maximum number of vehicles in a road tunnel, and so on.

Every design effort during the project will lead to safety constraints. This is part of the knowledge created during the design process. Each design alternative is associated with a set of safety constraints that are communicated back to the decision makers, who, at each decision gate (see the CVP model in Figure 5), determine whether such safety constraints are acceptable. If the constraints are acceptable, the design alternative may be continued for further designing – if not, it is modified or rejected. A critical task in the early design stages is, thus, to identify possible safety constraints associated with alternative designs. Uncertainty may be present, and decisions need to be made about whether more knowledge is needed to reduce this uncertainty. In such cases, it may be decided to conduct risk assessments to look into specific issues of the design fairly early in the design process. Such risk assessments may clarify knowledge associated with the decisions by identifying, for instance, appropriate safety measures or boundaries. The point is that analyses may be needed during the whole design process, but their level of detail needs to reflect the decision that is to be made and the available information at that time. Too detailed analyses in the early stage of the project may be useless due to changes in later design stages, or they may impose unwanted constraints on creativity and innovation in the design process (Blockley & Godfrey, 2000:160).

The end goal of safety engineering of a complex socio-technical system may be perceived as the development of an appropriate structure of safety constraints. Safety constraints are identified continuously during the process, but as more design variables are locked in, the more modeling and analytical detail may be introduced. Examples of safety constraints in a building may be a specified maximum number of people on each floor, maintaining a functional sprinkler system, maximum fire load and configuration on each floor, the specification of interaction between technical systems, such as the fire alarm system and electrical locks and light system, or the staff's involvement in emergency situations. In a road tunnel, possible safety constraints may be the minimum required volume flow and distance between jet fans in the ceiling, the maximum gradient, the maximum distance between emergency exits, the specification of interaction between technical systems, the maximum speed limit in specified situations, etc. Bjelland et al. (Submitted) describe a framework for identifying safety constraints from functional requirements to safety in a design project.

The design process should end by completing the list of safety constraints and examining the specified level of detail. In some cases the final identification of safety constraints for operation may be the collection of constraints identified in earlier project phases. In this case the work may consist in finishing a "safety case" document. In other cases, early crude analyses and decisions made by rules of thumb may be associated with great uncertainty. For instance, the maximum number of people in a concert arena may be estimated to be in the range of 3,000 – 4,000 people under different situational circumstances. This may be an acceptable safety constraint for the project owner, and the process is terminated. However, more detailed analyses, using updated variables of the design and the most detailed models available, may show that 5,000 people may be appropriate under certain situational circumstances.

Finally, the following points are introduced to summarize this section in order to clarify why the focus on verification should be shifted towards identification of safety constraints:

- Safety is not an objective property of a design that may be measured in terms of universal laws and values. Measures of safety cannot be separated from who is measuring the safety level. Thus, the focus on verification of safety levels is unfortunate and impossible in the universal sense. Safety is constantly challenged through a strong focus on optimization. A constructivist approach acknowledges that safety descriptions are social constructions. There is an inherent subjectivity in the descriptions, which need to be judged on the basis of the analysts' background knowledge. In this approach, focus is shifted from discovering the truth to identifying the appropriate solution that considers all relevant stakeholders' goals and values.
- The focus on verification of safety levels indicates that a building is either safe or unsafe independent of context. This is not true and may lead the users to be "passive believers," assuming that the building

may be appropriate for "everything." Safety is context dependent, which may be illustrated with car safety: A Volvo has a good reputation for being a safe car, but if the car is driven by an inexperienced, drunken driver on a narrow, icy road during the night, safety will be compromised. Consequently, safety is an emergent property of the *car-driver-environment system* (Wallace & Ross, 2006). A focus on identifying safety constraints implies efforts spent on understanding the conditions under which one would expect safe operation, which, to a greater extent, activates different stakeholders on the various levels of the system's hierarchy (Checkland, 1999; Leveson, 2011b; Wallace & Ross, 2006).

- Verification may be, and often is, used about compliance with safety objectives in the regulation. Thus, rather than verifying a safety level, per se, one verifies whether the objectives of the regulations are fulfilled. This may be possible if the safety regulations are prescriptive, when there is universal agreement about categorization of both the IF and the THEN side (cf., Figure 3). However, for novel designs there are no prescriptive regulations, and even, if there were, there will be disagreement about interpretations. Nevertheless, at best one would be able to verify that the design complied with the regulation at a specific point in time of the design phase. During later design phases, the construction and operation phases, it is likely that something is changed, rendering the verification work useless. If verification was substituted for identification of safety constraints, focus would be on the future performance of the system under different situational circumstances, or, more precisely, the focus would be on how the system can change while being maintained in a safe state (Bjelland, et al., Submitted). This is also relevant in the cases where prescribed solutions are adopted. Technical safety measures are a necessary, but insufficient, ingredient for achieving safety. The fact that some set of technical safety measures was designed and assumed present at some point in time is a poor indicator of whether or not safety will be maintained over time. In any case, it will be crucial to understand what recognizes the boundaries of safe operation of the artifact, whether or not the design is based on performance codes or prescriptive codes.

7.1.3 Developing goals and values

Traditional safety design based on prescription makes a clear distinction between acceptable and unacceptable safety. Either there is compliance, or there is not. In the former case the design is safe, and in the latter it is unsafe. However, this is based on an assumption that everything else, besides technical safety measures, is equal. For instance, an office building is just an office building no matter where it is located; who works there; what maintenance procedures are implemented, and so on.

In a constructivist' system thinking framework, there is no such clear distinction between acceptable and unacceptable. The constructivists argue that safety is socially constructed; hence, one would possibly find some parts of a society that find any solution acceptable. Systemic thinking regards safety as an emergent property of the system as a whole. Hence, in a systems perspective all technical designs could, in principle, be considered acceptable given the right system conditions. For instance, a low technical fire safety standard might be accepted by introducing severe safety constraints on the operation of the building. Consider handguns: they are acceptable, but only in the hands of people who live by moral standards shared by the society.

This begs the question of how to separate good designs from bad designs. It may seem like everything is relative and that speculative project owners focusing only on profit could get away with everything they want. This must, of course, not become the case. The fundamental difference is how one thinks about safety, by rejecting the major simplifications associated with perceiving safety as an objective property in a reductionist framework.

The quality of a system design may be determined and measured by its fitness for the intended purposes (Blockley & Godfrey, 2000:159). Hence, quality comes down to values about what purposes are relevant and how these values are prioritized, e.g., based on the importance of the stakeholder.

In general we can say that some stakeholders' values are universal when stated in a broad and general form. For instance, the following objective, representing society's values, may be considered a universal fire safety value: *"The building shall be designed and constructed so that there are appropriate* *provisions for the early warning of fire, and appropriate means of escape in case of fire from the building to a place of safety outside the building capable of being safely and effectively used at all material times"* (UK-Gov, 2000:13). However, if the objective is more detailed, for instance by specifying the measures to accommodate early warnings and the maximum distance to an exit to accommodate appropriate means of escape, it is difficult to perceive them as universal. There may be cases where a certain alarm measure or a specific maximum egress distance will create unwanted restrictions. To determine if 30 m or 60 m is an appropriate distance to an emergency exit depends on the situation and can hardly be a subject of universal agreement.

Hence, in a design project it is necessary to develop a structure of the goals and values. Blockley & Godfrey (2000:157) distinguish between goals that are *necessary (must achieve)*, *highly desirable (should achieve)*, *desirable (could achieve)*, and those which may be seen as *a bonus (want to achieve)*. The development of this structure of goals and values is an important task of engineering practice in design projects in order to evaluate quality as fitness for purpose. Bjelland et al (Submitted) propose a new framework for fire safety engineering in which the identification of safety goals is a fundamental component.

7.2 Safety science practice

The fire safety science literature contains a rich catalogue of normative studies. For instance, there are a number of papers concerned with how to state appropriate fire safety objectives (e.g., Bukowski & Babrauskas, 1994; Bukowski & Tanaka, 1991; Hadjisophocleous, et al., 1998; NKB, 1994) and examples of tools that may be used to evaluate if these objectives are met (e.g., V. R. Beck & Yung, 1990; ISO, 2009; Lundin, 2005; Olenick & Carpenter, 2003; SFPE, 2000). During the 1990s there was a great focus on promoting performance-based fire safety codes, but it is difficult to find scientific contributions that describe why the introduction of performance-based fire safety codes was a good idea. Some common arguments were the unnecessary barriers that prescriptive codes imposed on global trade and that performance codes would lead to a higher safety level at a lower cost. From the fire science community's perspective, the introduction of performance-based codes would lead to a need for scientific engineering principles and tools. Hence, it could be argued that fire science, itself, had a strong motive for the introduction of such codes.

In Norway, performance-based fire safety codes were introduced in 1997. Investigations into the fire safety engineering practice (Bjelland & Njå, 2012a) show that the old principles based on a prescriptive practice still dominate the field. Similar findings are common internationally and are reflected, for instance, through papers and keynote speeches presented at the Society of Fire Protection Engineers' (SFPE's) International Conference of Performance-Based Codes and Safety Design Methods (SFPE, 2010, 2012).

The problems encountered in engineering practice may not come from the introduction of performance-based fire safety codes. In a fast evolving world with constantly new problems and needs, a prescriptive code will just not be able to keep up with technological innovation. As such, the introduction of performance-based codes may be seen as more or less inevitable.

Fire safety engineering is a rather new engineering discipline that gained great interest through the introduction of performance-based codes. According to common community definitions, fire safety engineering is the application of science, engineering principles and expert judgment/experience to protect people, property and environment from the effects of fire. A question of great interest in regards to the work of this thesis is what goes into the definition of *science* and *engineering principles*. Based on our literature review (see Bjelland, et al., Submitted), it could be argued that these concepts are strongly associated with the natural science approach, leading to a preferred application of ideas such as scientific realism, reductionism, and favoring of quantitative laws over qualitative discourse. For instance, the leading journal in the field of fire safety science, Elsevier's *Fire Safety Journal,* includes the following statement in its scope: *"Original contributions (…) are invited, particularly if they incorporate a quantitative approach to the subject in question"* (Elsevier, 2013).

A major issue associated with the work of this thesis has been directed at developing a better understanding of the current fire safety engineering practice, mainly in Norway. There is a sharp contrast between the focus on natural sciences and quantitative laws of fire safety science and on common fire safety engineering practice. The models of natural science are being used, to some extent, but they are simply not covering the full range of engineering problems. In order to solve practical problems, qualitative discourse and engineering judgment seem to have a greater importance. This places emphasis on the designer's individual skills (Dreyfus & Dreyfus, 1986; Schön, 1991), rather than generalized methods and principles. This finding led to a theoretical investigation into design science (section 3), systems thinking (section 2.2) and some major concepts seen in the light of different philosophies of science (Section 2.3) and (Bjelland, et al., Submitted). Based on these investigations, it could be argued that fire safety science could benefit strongly from gaining a better understanding of the problems of design practice and how this would affect the scientific framework adapted to support this practice.

7.3 Regulative practice

7.3.1 Limitations of prescriptive regulations

The use of prescriptive regulations can sometimes be viewed as "thinking inside the box," or to lend credibility to "what is" and "what has been appropriate before." As we have argued in section 3.5, humans tend to categorize situations and use a common, or standard, pattern of links between the categories that are known to us. Prescriptive design is a good example of categorization and common pattern. It states that a design proposal with certain characteristics should be placed into category X or Y. Once the category is selected, the solution becomes obvious (cf., Figure 3): We just apply the common pattern of linking between categories X or Y to the prescribed solutions. This is obviously a useful way of thinking in many cases. Figure 9 depicts a situation where such thinking is useful. Design proposal A is categorized to fall within the "domain of prescriptive performance levels." In this case we use the prescribed performance levels that apply for the category into which design proposal A falls. The approach provides consistency about practical solutions in cases of great similarity, and it reduces the efforts spent on design, that is, it saves energy and money.

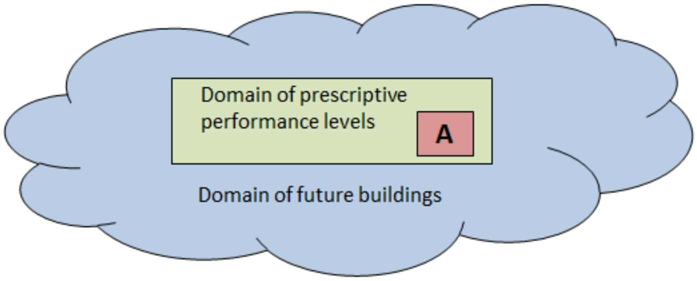

Figure 9: Design proposal A falling inside the domain of prescriptive performance levels.

The limitations of such thinking becomes apparent in cases when the design proposal seems to fall outside an apparent category, like design proposal B depicted in Figure 10. First, there are no predetermined categories where design proposal B can be placed. Second, since we have no known category for B, we have no link between the design proposal and possible practical solutions. This is the case with all novel designs: i.e., those designs that are pure innovations, that stretch the limits of our previous experience, e.g., buildings being increasingly higher or subsea road tunnels being increasingly longer and deeper below sea-surface, that are combinations never seen before, i.e., a fusion of previously known designs into a new mixture, like airports also being shopping malls and hotels and designs we have seen before but that contain new activities and hazards, and so on.

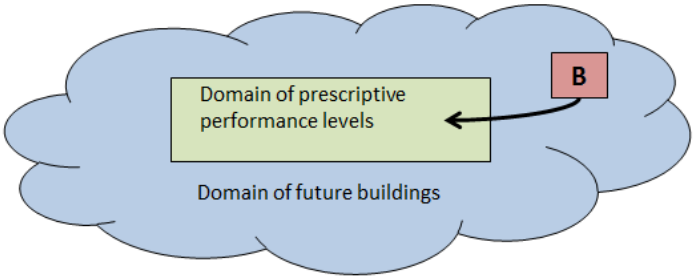

Figure 10: Design proposal B falling outside the domain of prescriptive performance levels.

From the research associated with this thesis, we have seen a trend in which engineers are molding designs of type B into known categories. Great efforts are spent discussing and defining the design proposal such that it will fit into our common categories, which again visualize a standard pattern of linking a "design problem" to a "design solution." This trend is depicted by the arrow from design proposal B inside the domain of prescriptive performance levels.

A major limitation with this approach is that many resources and much energy are put into the semantic molding of design proposal B. Different and inconsistent rules within the prescriptive regulations are often combined in order to either fit design proposal B into a known category, or to expand the scope of a known category so it will fit design proposal B. Nevertheless, all this molding may be conducted without considering the real hazards and traits of design proposal B.

A good example of this approach within the Norwegian fire safety engineering community is related to floor area limitations within the prescriptive regulations. The example is about combining two inconsistent rules within the guide to the regulation in order to expand a known category of prescribed solutions. The first rule states that when a building is provided with an automatic sprinkler system, the floor area per story not separated with a fire wall may be 10 000 m^2. The second rule states that a compartment may have an open connection across three floors. The combination of the two rules leads to an argument that it is allowed to include 30,000 m^2 into a compartment not separated by a fire wall. Consequently, a design proposal including a one-story building of 30,000 m^2 would now fit the prescribed category, although the initial limit was 10,000 m^2. All that was needed was some "linguistic molding." If we would like to draw this line of thinking even further, we may say that, according to the guide to the regulation, a building may be built with, say, 8 floors. Each floor may be 10,000 m^2 and have an open connection across three floors. So, for every third floor, we would have to include a fire separating barrier with 60 minutes fire resistance. The situation is depicted in Figure 11.

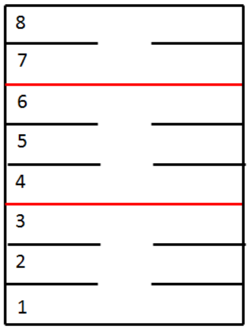

Figure 11: Section of an 8-story building having a floor area of 10,000 m^2 on each floor and separated by a fire resistant barrier every third floor (depicted by a red floor separator).

This design is based on the same logic as the first example. We are combining the different prescriptive design rules in order to stretch the scope of a prescribed category. The end result of this latter example is that one would be allowed to include 80,000 m^2 inside a fire section before having to erect a fire wall. However, for each 30,000 m^2 one would have to include a fire separating barrier of 60 minutes. Again, if we would like to erect a one-story building we would now, based on our logic, allow it to cover 80,000 m^2 before erecting a fire wall. Remember that the first limit was 10,000 m^2.

There are several lessons to learn from these examples. First is the issue of thinking inside the box. As discussed above, we tend to mold anything as much as possible in order to make it fit with our common conceptions and patterns. The consequence of this activity is that real issues associated with the proposed design are neglected and treated in a generic way. Information is only relevant as long as it is related to the categories we already have created. Since our categories are only concerned with whether a sprinkler system is present or not present, it is hard to see how one is able to affect the quality of the sprinkler system. There are many ways to construct a sprinkler system that finally will affect its performance during a future fire. A similar concern is related to organizational factors. Our categories do not include organizational fire safety factors. Even though our design proposals, implicitly or explicitly, includes assumptions about organizational factors, they are outside the scope of the building regulations. When the building is finished, a different regulation takes over in order to implement organizational fire safety. The question, then, is how should one ensure that the designed building will match the organization? At best, one can make and state assumptions about future usage and about organizational fire safety measures. However, to attain a holistic perspective on fire safety, one must think "outside" the box. Fire safety in buildings and safety in road tunnels is more than what is reflected by our common conceptions from prescriptive design rules.

Second, there is the concern that the fire safety engineering community sometimes falls into some sort of an intelligence trap (Blockley & Godfrey, 2000; de Bono, 1978). We are so focused on defending our proposed design that we become unable to look for alternatives. Our logic may be flawless, based on the premises of the argumentation. Still there should be concerns whether the final result, the design, will be appropriate. After all, all the thinking was done without even considering any properties of the design proposal. This issue is mainly related to what we consider relevant or credible knowledge in the safety community today, and it is closely related to the first point of thinking inside the box. The engineering community is traditionally concerned with the application of knowledge gained from science, and mainly natural science, to come to conclusions. In this tradition, logic and empirical evidence have a strong position. Thus, all arguments and knowledge that are derived from logic and empirical evidence will be favored before other types of knowledge. A major problem, however, is that one can question the premises of the logical arguments, as they often build on the assumption that the guidelines reflect the "truth" about safety. Novel designs falls outside the scope of prescriptive performance requirements, and there is no truth about safety. Nevertheless, there are good and bad designs. Judgments about quality need to be made by competent people in a rigorous engineering process where all relevant knowledge is brought to the table for decision making.

Third, the examples illustrate that floor area may be a poor indicator of fire safety. The floor area requirements are introduced to limit material damages and societal consequences of a fire. However, a square meter floor area is not of constant value. Two quite similar buildings, say two schools in two different municipalities, may be of different value to the local community. The first school is located within a municipality having many other schools. If the school is lost in a fire, there will be redundancy in the municipality to handle pupils that lost their original school. In the second municipality, there is just a single school. There will be no other alternative available if the school is lost to fire. No matter how many square meters are lost, this will have a huge consequence to the community. Thus, other indicators than floor area should be used to assess the consequences of a fire. More specifically, the societal goals and performance requirements should be clearly stated instead of specific indicators and safety measures. This would allow for a safety concept that is tailor made for the specific, proposed design and design situation/context. We need to remember that novel design proposals are outside the domain of prescriptive performance levels. They do not necessarily fit previously-accepted categories and linking patterns. There is no correct or true solution to the design problem. In fact, we may have to start designing and investigating the design proposal and the design context before we are able to develop the design problems that we are to solve. In such cases there is a need to think "outside the box," or use what De Bono (1990) calls lateral thinking. This is only possible within a framework that does not impose category thinking. A development of the goal-oriented framework is thus necessary.

8 CONCLUDING REMARKS

In a time where there were only so many ways of constructing a building and only so many materials and products to use in the process, designing for safety was largely a matter of doing the things that worked yesterday or the last century. The slow pace of technological development made it possible to test and develop designs, and gain knowledge specifically associated with the individual designs. This is how the prescriptive design rules developed and led to an effective regulation of the construction industry.

But that is not the same reality we are faced with today. Never have changes in the society occurred faster and complexity grown more rapidly as in the past few decades (e.g., U. Beck, 1992; Covello & Mumpower, 1985; Leveson, 2011b). New knowledge is created in every little corner of the world and instantly shared with the international scientific online community. Technology that was state of the art last year is obsolete today. New knowledge about climate change, for instance, leads to new priorities when constructing buildings. The materials we adopt for our constructions should have a small environmental footprint and the energy consumption of the buildings should be as low and as possible and, preferably, renewable.

This reminds us that the society's needs, desires and values are flexible, continuously adapting to the global situation and the present state of affairs. And with new needs, desires and values come appeals for new solutions. The "boundaries of validity" of the old prescriptive design rules are increasingly being challenged and sometimes crossed. In some cases we are not even sure where we are in comparison with the old prescriptive design rules, such as the Rogfast case (Bjelland & Aven, 2013). The proposed design is breaking so many conventions that it becomes impossible to keep track of the total consequences of deviations. This is where designers come in, and this is where "performance" comes in. Never before has performance-based safety engineering been more appropriate. Moreover, the demand for performance-based safety engineering will grow in line not only with evolving needs, desires and values but also with the increasing complexity that involves component interactions and tight couplings among socio-technical systems.

The aim of this dissertation has been to investigate what promotes and inhibits performance-based safety management of design processes. When considering the outlook for the future of safety engineering and the limitations of prescriptive design rules, this issue is generally justified. The focus has been on safety engineering practice, the scientific foundation and safety regulations.

From the study of Norwegian fire safety engineering practice, presented in papers 1, 2 and 3 (Bjelland & Njå, 2012a, 2012b, 2012d), it was found that performance-based engineering is only used to a limited extent, even though performance-based legislative policies were introduced in 1997. Deviations from prescriptive design rules exist in practically all the studied projects, but there was always a reference to the prescriptive design rules with regard to determining whether the level of safety was acceptable. This is a major challenge, since the purpose of performance-based safety engineering is to function as a framework when the validity boundaries of the prescriptive design rules are exceeded. The research points to the high status of prescriptive design rules as an inhibitor for effective performance-based engineering. This is associated with how the various legislative policies are stated with regards to clarifying functional safety objectives. Currently, there is too strong a connection in the legislation between safety goals and safety measures. For instance, instead of clearly stating a functional objective, property fire protection is directly linked with fire compartmentation (KRD & MD, 2010:§11-7).

Research into current fire safety engineering practice also showed that safety levels were usually measured in terms of qualitative arguments and judgments. The risk concept, which is found to be a preferred measure in the fire science literature, is not commonly adopted in practice. If quantitative analyses are conducted, they are usually scenario analyses using deterministic fire models, where the results are compared with tolerability criteria, e.g., for human exposure to heat from a smoke layer and toxic substances. This finding is also corroborated by research into international fire safety engineering practices. Paper 4 deals with the scientific foundation in fire safety science on the concepts of safety level and safety margin. It is found that the concepts are understood in two rather narrow, traditional, technical rationality perspectives: one whose underlying assumption was that measurements of safety or risk have an ontological status, i.e., a positivist view, and another that had a more pragmatic or instrumental focus (Bjelland, et al., Submitted). The major challenge of both perspectives is associated with scientific reductionism, which aims to explain system performance by decomposing it into its constituent parts. This approach has been successful in the natural sciences and may also have been appropriate for the simple, technical systems of the past. However, modern buildings are packed with technology and software controls that create interactions that are practically unforeseeable by the designers. Hence, the traditional technical rationality framework places too much emphasis on technical problem solving while excluding important aspects of a designer's knowledge, e.g., tacit knowledge. A need exists for a broader scientific framework for safety engineering in order to both accommodate this kind of complexity in designs and cover the way designers think and act and how design processes evolve. A possible solution points in the direction of a constructivist-oriented, systems thinking perspective. Such a perspective would provide a holistic treatment of fire safety in buildings and road tunnels. An important consequence would be the rejection of mechanistic decision processes. Rather, there needs to be a clear separation between engineers/analysts and formal decision makers who have the necessary oversight to make a balanced decision.

Some limitations with the current framework for fire safety engineering, including engineering practice, science and regulation, are pinpointed by papers 5 and 6 (Bjelland & Borg, 2013; Bjelland & Njå, 2012c). The focus of the papers is on methodological issues, especially those associated with "the equivalence approach." Although safety scientists have been searching for a universal quantified level of acceptable risk for decades, no such level has been found. While waiting for this discovery, a practice has developed in which calculated risk for alternative designs is evaluated against the risk implicitly acceptable in the prescriptive regulations. Papers 5 and 6 show that this practice leads to a disproportionate focus on identifying an appropriate reference design, rather than focusing on the safety of the specific design proposal. In practice, due to inconsistencies in the prescriptive regulations, it will nearly always be possible to find a prescriptive reference that comes out poorly in this comparison. The major point of the analysis, though, is that the methodology fails to capture the important issues associated with safety. The methodology is reductionist by excluding vital issues associated with the socio-technical system hierarchy; for instance, the management resources, the user organization, the municipality resources and the actual performance of safety systems. The comparison is made on a coarse level, focusing on differences between the alternative design and the reference design, using standardized data. Hence, it is not really an analysis of safety but rather of some kind of technical standard that may, or may not, contribute to a safe performance of the building during operation.

According to Leveson (2011b), safety must be designed into the system from the beginning of the design process. To assume that the system will be operated in accordance with how the designers intended it to be operated is a matter of sheer luck if expectations from the users are not communicated and taken into consideration in the design process. Of course, it is currently required for engineers to clarify the assumptions about operating limitations, but the point is that these issues are held as boundary conditions to the design process, rather than as resources or measures that can be actively manipulated during design (cf., Figure 7). Papers 4, 7 and 8 (Bjelland & Aven, 2013; Bjelland & Borg, 2013; Bjelland, et al., Submitted) aim to contribute to a broader framework for risk and safety analyses that enables application of all relevant knowledge to reassure the best possible preconditions for safe operation of complex, socio-technical systems during the full life cycle. Complex socio-technical systems are constantly adapting to changes within themselves and the environment. Designing for safety, then, is not about verification but, rather, about creating a management structure that enables the system to change safely. It may be that mathematical rigor has to give way to more qualitative and discursive processes, but this may not be such a bad thing. After all, what is really gained from rigorous solutions to problems that are simply not relevant?

9 FURTHER RESEARCH

9.1 Safety research and design research

In this thesis I have tried to combine safety research and design research. After all, safety research is fundamentally design research. While the technical rationality framework still has a strong position in the pure safety research, the design research community seems more open to a holistic perspective on science. This affects what scientists perceive as, for instance:

- What are important research questions?
- What is important knowledge for practitioners, i.e., safety engineers?
- What is the nature of design processes?
- How do we distinguish successful designs from bad designs?

Some work has been done in this thesis with regards to pointing to the link and visualizing some opportunities. However, the next step would be to explore how safety issues could be investigated in a broad design research framework. Along with aesthetics and functionality, for instance, safety is an emergent property of the system as a whole. Hence, it seems reasonable to suggest that safety should be an integrated part of the design task as a whole and not just an add-on characteristic. To achieve this, there is a need for interdisciplinary research to promote truly interdisciplinary design processes.

9.2 Empirical testing

The research associated with this thesis has resulted in the proposal of alternative safety engineering frameworks. These proposals may be seen as grounded theory, and, as such, explain the problems encountered in this project with the particular focus of this project in mind. However, there may be other solutions, as scientific theories may be underdetermined by the data (Stanford, 2009). The major issue, then, is whether the proposed framework is actually useful to safety engineering. At this point, I can say that I believe it will be, since it is built on the basis of identified weaknesses in the current framework, but I cannot be sure until it has been tested in practice and empirical evidence of its performance is gathered.

Critical issues to test and develop further are those associated with determining quality in the safety engineering process and with how to enable effective decision making based on the engineering efforts. For instance:

- How should stakeholders be involved in the design projects, and who are the relevant stakeholders to involve? A broad framework involves data and values stated in many different ways. There will not be a mechanistic way to optimize all concerns. Decision making needs to be a matter of striking a balance between relevant concerns, without compromising the important traits of the design and important values of society, such as safety.
- What are indicators of a good design with regards to safety?
- What kind of data or evidence is needed in the analyses? Obvious sources are data from accident investigations and learning from rescue services. Less obvious are data from good safety practice, i.e., from systems that have not experienced any failures. Also, how do we distinguish between the individual engineers? What distinguishes an expert from a novice in safety engineering (Dreyfus & Dreyfus, 1986), and how do we configure the design processes to take advantage of these differences?
- How do we determine the quality of the engineering documentation? The legal system, for instance, is making critical decisions under uncertainty every day, but probabilities are seldom incorporated specifically. According to Graver (2009), principles of judging the coherency of all the presented evidence are more useful in this respect. Similarly, coherence principles may be useful in decision making about safety, but there is need to test this in practice and to gather empirical evidence as to how effective it can be.

9.3 Project management

A design project is assumed to progress in clearly defined phases, from concept exploration to construction (cf., section 4.4 and Figure 5). However, in practice the boundaries between the different phases will be less clear. For instance, it is not uncommon that designing is conducted during construction or that fundamental conceptual questions are posed during detail design. It has been pointed out in this thesis that design processes are nonlinear. Design problems and solutions co-evolve as the project develops.

There are several ways for the project owner to involve the different actors in the project with regards to, for instance, *when* and with *what responsibility*. A major issue is related to when the contractor should be involved. Some form of turnkey contracts (e.g., Merna & Smith, 1990) are often used in Norway. A design project is conducted in accordance with the CVP under the management of the architect or a hired project manager, for example, up until the detailed design phase. Then the contractor is involved. The contractor becomes responsible for designing during the detailed design phase and the construction phase. A new design team may be hired by the contractor, and technical solutions may be redesigned, which enable the contractor to increase profit by making it easier and/or cheaper to build.

From a systems thinking perspective, and taking into account the circular nature of design processes, it seems reasonable that the knowledge of the contractor should be included from the beginning of the design project. To include the contractor in the detailed design phase, or even later, may lead to suboptimizations, made from the contractor's perspective. The final building may be cheaper for the project owner, but it is far from certain that it will be better.

In order to gain the best possible foundation for successful and safe buildings and infrastructures, the project management and contract issues should be included into the framework. Possible research questions are:

- What contract model is preferable in a systems engineering perspective? A possible model may be the *Designer-Builder contractor* (Chan & Yu, 2005), where the contractor is responsible for both the design and construction during the whole design project.
- What precautions are needed to assure system safety when applying different forms of construction contracts? For instance, what

precautions must be taken if one is to use a turnkey contract as discussed above?

REFERENCES

Adams, J. (1995). *Risk*. London: UCL Press.

Alsaker, B. M. (1997). "Rogfast" A Vision? *The road ahead...? When do we get a permanent connection across the Bokn Fjord? (in Norwegian).* Presentation manuscript by Bjørn Martin Alsaker, Norwegian Public Road Authorities Rogaland, at Rennfastkonferansen, 1997.

Althaus, C. E. (2005). A Disciplinary Perspective on the Epistemological Status of Risk. *Risk Analysis, 25*(3), 567-588.

Andersen, S. S. (1997). *Case studies and generalization: Research strategy and design (in Norwegian)*. Bergen: Fagbokforlaget.

Anon. (2003). The technologist's absence (in Norwegian). *Teknisk ukeblad* Retrieved April 5, 2013, from http://www.tu.no/nyheter/fagartikler/2003/10/06/teknologenes-fravar

Apostolakis, G. E. (1990). The Concept of Probability in Safety Assessments of Technological Systems. *Science, 250*(4986), 1359-1364.

Apostolakis, G. E. (2004). How Useful Is Quantitative Risk Assessment? *Risk Analysis, 24*(3), 515-520.

ASCE. (2008). *Civil Engineering Body of Knowledge for the 21st Century : Preparing the Civil Engineer for the Future (2nd Edition)*. Reston, VA, USA: American Society of Civil Engineers (ASCE).

Aven, T. (2007). On the ethical justification for the use of risk acceptance criteria. *Risk Analysis, 27*(2), 303-312.

Aven, T. (2010a). *Misconceptions of risk*. Chichester: Wiley.

Aven, T. (2010b). On how to define, understand and describe risk. *Reliability Engineering & System Safety, 95*(6), 623-631.

Aven, T. (2011). *Quantitative risk assessment: the scientific platform*. Cambridge: Cambridge University Press.

Aven, T. (2012a). *Foundations of Risk Analysis (2nd Edition)*. Hoboken, NJ, USA: Wiley.

Aven, T. (2012b). The risk concept—historical and recent development trends. *Reliability Engineering and System Safety, 99*(1), pp. 33-44.

Aven, T., Boyesen, M., Njå, O., Olsen, K. H., & Sandve, K. (2004). *Societal safety (in Norwegian)*. Oslo: Universitetsforlaget.

Aven, T., Renn, O., & Rosa, E. A. (2011). On the ontological status of the concept of risk. *Safety Science, 49*(8–9), 1074-1079.

Banks, J., & Montgomery, D. C. (1983). Aanalysis of three natural experiments relating to fire death rate. *Journal of Fire Sciences, 1*(1), 33-53.

Beard, A. N. (1982). A stochastic model for the number of deaths in a fire. *Fire Technology, 18*(3), 280-291.

Beck, U. (1992). *Risk society : towards a new modernity*. London: Sage.

Beck, V. R. (1987). A cost-effective, decision-making model for building fire safety and protection. *Fire Safety Journal, 12*(2), 121-138.

Beck, V. R., & Yung, D. (1990). A cost-effective risk-assessment model for evaluating fire safety and protection in Canadian apartment buildings. *Journal of Fire Protection Engineering, 2*(3), 65-74.

Bedau, M. (2003). Downward causation and the autonomy of weak emergence. *Principia, 6*, 5-50.

Bedau, M., & Humphreys, P. (2008). *Emergence : Contemporary Readings in Philosophy and Science*. Cambridge, MA, USA: MIT Press.

Bedau, M. A. (1997). Weak Emergence. *Noûs, 31*, 375-399.

Bedford, T., & Cooke, R. (2001). *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge: University Press.

Berk, J. (2009). *Systems Failure Analysis*. Materials Park, OH, USA: ASM International.

Bernstein, P. L. (1996). *Against the gods: the remarkable story of risk.* New York: Wiley.

Bjelland, H. (2009). Fire safety concepts for residential apartment buildings - Fire safety measures and risk (in Norwegian). Stavanger: M.Sc. thesis, University of Stavanger.

Bjelland, H., & Aven, T. (2013). Treatment of uncertainty in risk assessments in the Rogfast road tunnel project. *Safety Science, 55*, 34-44.

Bjelland, H., & Borg, A. (2013). On the use of scenario analysis in combination with prescriptive fire safety design requirements. *Environment Systems & Decisions, 33*(1), 33-42.

Bjelland, H., & Njå, O. (2012a). *Fourteen years of experience with performance-based fire safety engineering in Norway – lessons learned*. Paper presented at the 9th International Conference on Performance-Based Codes and Fire Safety Design Methods, The Excelsior Hong Kong, 20-22 June 2012.

Bjelland, H., & Njå, O. (2012b, 25-29 June 2012). *Interpretation of safety margin in ASET/RSET assessments in the Norwegian building industry.* Paper presented at the Proceedings to the 11th International Probabilistic Safety Assessment and Management Conference (PSAM11) and The Annual European Safety and Reliability Conference (ESREL2012), Scandic Marina Congress Center, Helsinki, Finland.

Bjelland, H., & Njå, O. (2012c). *Performance-based fire safety : risk associated with different designs.* Paper presented at the Advances in safety, reliability and risk management: proceedings of the European

Safety and Reliability Conference, ESREL 2011, Troyes, France, 18-22 September 2011.

Bjelland, H., & Njå, O. (2012d). *Safety factors in fire safety engineering.* Paper presented at the Advances in Safety, Reliability and Risk Management: Proceedings of the European Safety and Reliability Conference, ESREL 2011, Troyes, France.

Bjelland, H., Njå, O., Braut, G. S., & Heskestad, A. W. (Submitted). A discussion of the concepts of safety level and safety margin: applications in designing fire safety for occupants in buildings. *Submitted to Fire Technology*.

Bjerkholt, O., Offerdal, E., & Strøm, S. (1985). *Oil and gas in the Norwegian economy: a contribution to the understanding of the petroleum industry's importance to Norway in the years to come (in Norwegian).* Oslo: Universitetsforlaget.

Blaikie, N. (2000). *Designing social research : the logic of anticipation*. Cambridge: Polity Press.

Blakstad, H. C. (2006). *Revising rules and reviving knowledge : adapting hierarchical and risk-based approaches to safety rule modifications in the Norwegian railway system* (Vol. 2006:90). Trondheim: Norges teknisk-naturvitenskapelige universitet.

Blockley, D. I. (1980). *The nature of structural design and safety*. Chichester: Ellis Horwood.

Blockley, D. I., & Godfrey, P. (2000). *Doing it differently : systems for rethinking construction*. London: Thomas Telford.

Borg, A., Bjelland, H., & Njå, O. (Submitted). Reflections on Bayesian Network models for road tunnel safety design: A case study from Norway. *Submitted to Tunnelling and Underground Space Technology*.

Borg, A., & Njå, O. (2013). The concept of validation in performance-based fire safety engineering. *Safety Science, 52*(0), 57-64.

Brennan, P. (1999). Victims and survivors in fatal residential building fires. *Fire and Materials, 23*(6), 305-310.

Bukowski, R. W., & Babrauskas, V. (1994). Developing Rational, Performance-based Fire Safety Requirements in Model Building Codes. *Fire and Materials, 18*, 173-191.

Bukowski, R. W., & Tanaka, T. (1991). Toward the Goal of a Performance Fire Code. *Fire and Materials, 15*, 175-180.

Chakravartty, A. (2011a). Scientific Realism, March 21, 2013, from http://plato.stanford.edu/archives/sum2011/entries/scientific-realism/

Chakravartty, A. (2011b). Scientific Realism and Ontological Relativity. *The Monist, 94*, 157-180.

Chan, E. H. W., & Yu, A. T. W. (2005). Contract strategy for design management in the design and build system. *International Journal of Project Management, 23*(8), 630-639.

Checkland, P. (1999). *Systems thinking, systems practice*. Chichester UK: Wiley.

Covello, V. T., & Mumpower, J. (1985). Risk Analysis and Risk Management: An Historical Perspective. *Risk Analysis, 5*(2), 103-120.

Cronsioe, C., Strömgren, M., Tonegran, D., & Bjelland, H. (2012). *New Swedish building regulations and a framework for fire safety engineering*. Paper presented at the 9th International Conference on Performance-Based Codes and Fire Safety Design Methods, The Excelsior Hong Kong, 20-22 June 2012.

Cross, N. (1999). Design Research: A Disciplined Conversation. *Design Issues, 15*(2), 5-10.

Cross, N. (2001). Designerly Ways of Knowing: Design Discipline Versus Design Science. *Design Issues, 17*(3), pp. 49-55.

Cross, N. (2007). Forty years of design research (Editorial). *Design Studies, 28*(1), 1-4.

Cross, N. (2011). *Design thinking : understanding how designers think and work*. Oxford: Berg.

Cross, N., & Cross, A. C. (1998). Expertise in Engineering Design. *Research in Engineering Design, 10*, pp. 141-149.

Dahle, G. A., Andersen, J. H. S., & Børresen, B. A. (2006). Risk and Vulnerability Analysis of the Rogfast Tunnel (in Norwegian). Sandvika: Norconsult.

Damodaran, A. (2008). *Strategic risk taking : a framework for risk management*. Upper Saddle River, N.J.: Wharton School Pub.

de Bono, E. (1978). *Teaching thinking*. London: Temple Smith.

de Bono, E. (1990). *Lateral thinking: A textbook of creativity*. London: Penguin Books.

de Bono, E. (1999). *Six Thinking Hats*. London: Penguin Books.

de Bono, E. (2007). *Intelligence is not enough* Dublin: Blackhall Publishing.

de Finetti, B. (1989). Probabilism: A Critical Essay on the Theory of Probability and on the Value of Science (translation of the article "Probabilismo", published in Logos Vol. 14, 1931). *Erkenntnis, 31*(2/3), 169-223.

Dorst, K. (1997). *Describing design - A comparison of paradigms.* PhD-thesis, Delft University of Technology, Delft.

Dorst, K. (2003). *The Problem of Design Problems*. Paper presented at the 6th Design Thinking Research Symposium (DTRS6), Sydney, 17-19 November 2003.

Dorst, K. (2008). Design research: a revolution-waiting-to-happen. *Design Studies, 29*(1), pp. 4-11.

Dorst, K. (2011). The core of 'design thinking' and its application. *Design Studies, 32*(6), 521-532.

Dorst, K., & Cross, N. (2001). Creativity in the design process: co-evolution of problem–solution. *Design Studies, 22*(5), 425–437.

Douglas, M., & Wildavsky, A. (1982). *Risk and culture : an essay on the selection of technical and environmental dangers*. Berkeley, Calif.: University of California Press.

Drevon, F. (2013). Engineers think too narrowly (in Norwegian). *Teknisk ukeblad* Retrieved April 5, 2013, from http://www.tu.no/bygg/2013/04/05/-ingeniorer-tenker-for-snevert

Dreyfus, H. L., & Dreyfus, S. E. (1986). *Mind over machine: the power of human intuition and expertice in the age of the computer.* Oxford: Basil Blackwell.

DSB. (2013). Fire statistics (in Norwegian) Retrieved 25 April 2013, from http://www.dsb.no/no/Statistikk/Statistikk1/Branner/

Elsevier. (2013). Fire Safety Journal: An international journal devoted to research on Fire Safety Science and Engineering, March 4, 2013, from http://www.journals.elsevier.com/fire-safety-journal/

Feenberg, A. (1999). *Questioning Technology*. Florence, KY, USA: Routledge.

FEMA. (2013). National Fire Incident Reporting System (NFIRS), Federal Emergency Management Agency (FEMA) Retrieved 25 April 2013, from http://www.nfirs.fema.gov/

Feyerabend, P. K. (2010). *Against method: Outline of an anarchistic theory of knowledge (First published by New Left Books 1975)*. London/New York: Verso.

Fischhoff, B., Lichtenstein, S., Slovic, P., Derby, S. L., & Keeney, R. L. (1981). *Acceptable risk*. Cambridge: Cambridge University Press.

Fitzgerald, R. W. (1991). Integration of fire science into building requirements. *Fire Safety Journal, 17*(2), 159-163.

Flyvbjerg, B. (2006). Five Misunderstandings About Case-Study Research. *Qualitative Inquiry, 12*(2), 219-245.

Franklin, J. (2009). *What Science Knows : And How It Knows It*. New York, NY, USA: Encounter Books.

Frantzich, H. (1998). Risk analysis and fire safety engineering. *Fire Safety Journal, 31*(4), 313-329.

Funtowicz, S. O., & Ravetz, J. R. (1992). Three Types of Risk Assessment and the Emergence of Post-Normal Science. In S. Krimsky & D.

Golding (Eds.), *Social Theories of Risk* (pp. 251-273). Westport, CT: Praeger.

Gagnon, Y.-C. (2010). *The Case Study as Research Method: A Practical Handbook*. Quebec, QC, CAN: Les Presses de l'Université du Québec.

Galle, P. (2008). Candidate worldviews for design theory. *Design Studies, 29*(3), 267-303.

Galle, P. (2011). Foundational and Instrumental Design Theory. *Design Issues, 27*(4), pp. 81-94.

Giere, R. N., & Richardson, A. W. (1996). *Origins of Logical Empiricism*. Minneapolis, MN, USA: University of Minnesota Press.

Gillham, B. (2010). *Case Study Research Methods*. London, GBR: Continuum International Publishing.

Godfrey-Smith, P. (2003). *Science and Its Conceptual Foundations : Theory and Reality : An Introduction to the Philosophy of Science*. Chicago, IL, USA: University of Chicago Press.

Gram, T. (2012). Engineers lacks power (in Norwegian). *Teknisk ukeblad* Retrieved April 5, 2013, from http://www.tu.no/jobb/2010/02/19/ingeniorer-mangler-makt

Graver, H. P. (2009). Evidence evaluation - unscientific gut feeling or a rational holistic assessment? (in Norwegian). *Tidsskrift for Rettsvitenskap, 122*(2), 191-233.

Gwynne, S., Galea, E. R., Parke, J., & Hickson, J. (2003). The collection and analysis of pre-evacuation times derived from evacuation trials and their application to evacuation modelling. *Fire Technology, 39*(2), 173-195.

Hadjisophocleous, G. V., Benichou, N., & Tamim, A. S. (1998). Literature review of performance-based fire codes and design environment. *Journal of Fire Protection Engineering, 9*(1), 12-40.

Hadjisophocleous, G. V., & Fu, Z. (2007). Prediction of Fire Growth for Compartments of Office Buildings as Part of a Fire Risk/Cost Assessment Model. *Journal of Fire Protection Engineering, 17*, 185-209.

Hale, A. R., & Swuste, P. (1998). Safety rules: procedural freedom or action constraint? *Safety Science, 29*(3), 163-177.

Hall Jr, J. R., & Sekizawa, A. (1991). Fire Risk Analysis: General Conceptual Framework for Describing Models. *Fire Technology, 27*(1), 33-53.

Hammersley, M. (1990). *Dilemma of Qualitative Method : Herbert Blumer and the Chicago Tradition*. Florence, KY, USA: Routledge.

Hasofer, A. M., & Beck, V. R. (1997). A Stochastic model for compartment fires. *Fire Safety Journal, 28*(3), 207-225.

Hasofer, A. M., & Thomas, I. (2006). Analysis of fatalities and injuries in building fire statistics. *Fire Safety Journal, 41*(1), 2-14.

Haugstad, T. (2010). Seize the opportunities, engineers! (in Norwegian). *Teknisk ukeblad* Retrieved April 5, 2013, from http://www.tu.no/meninger/tumener/2010/02/19/grip-mulighetene-ingeniorer

Haugstad, T. (2012). Anonymous consultant's association (in Norwegian). *Teknisk ukeblad* Retrieved April 5, 2013, from http://www.tu.no/meninger/tumener/2011/05/13/anonyme-radgiveres-forening

Hazelrigg, G. A. (1998). A Framework for Decision-Based Engineering Design. *ASME Journal of Mechanical Design Issues, 120*(4), 653-658.

He, Y. (2010). Linking safety factor and failure of probability for fire safety engineering. *Journal of Fire Protection Engineering, 20*, 199-217.

He, Y., Horasan, M., Taylor, P., & Ramsay, C. (2002). *Stochastic Modelling for Risk Assessment*. Paper presented at the 7th international Symposium on Fire Safety Science, 15-19 June, 2002, Worcester, MA, USA.

Heinrich, H. W. (1931). *Industrial accident prevention : a scientific approach*. New York: McGraw-Hill.

Hokstad, P., Jenssen, G. D., Mostue, B. A., & Foss, T. (2012). E-39 Rogfast. Risk and Vulnerability Analysis, Tunnel (in Norwegian). Trondheim: Sintef/Cowi.

Holborn, P. G., Nolan, P. F., & Golt, J. (2003). An analysis of fatal unintentional dwelling fires investigated by London Fire Brigade between 1996 and 2000. *Fire Safety Journal, 38*(1), 1-42.

Holton, G. A. (2004). Defining Risk. *Financial Analysts Journal, 60*(6), 19-25.

Host, M., Rainer, A., & Runeson, P. (2012). *Case Study Research in Software Engineering : Guidelines and Examples*. Hoboken, NJ, USA: Wiley.

Hurley, M. (2009). Fire protection engineering Retrieved February 1, 2013, from http://www.wbdg.org/design/dd_fireprotecteng.php

ISO. (2009). ISO/TR 16738:2009 (E) Fire-Safety Engineering – Technical information on methods for evaluating behavior and movement of people. Switzerland: International Organization for Standardization.

Jenssen, G. D., Bjørkli, C., & Flø, M. (2006). Assessments for E39 Rogfast. Security, monotony, and safety in emergency situations and normal traffic (in Norwegian). Trondheim: SINTEF Teknologi og Samfunn, Transportsikkerhet og -informatikk.

Johnson, C. W. (2006). What are emergent properties and how do they affect the engineering of complex systems? *Reliability Engineering & System Safety, 91*(12), 1475-1481.

Kaplan, S. (1982). Safety goals and related questions. *Reliability engineering, 3*(4), 267-277.

Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis, 1*(1), pp. 11-27.

Kirwan, B., Hale, A. R., & Hopkins, A. (Eds.). (2002). *Changing regulation : controlling risks in society*. Amsterdam: Pergamon.

Kjellén, U. (2007). Safety in the design of offshore platforms: Integrated safety versus safety as an add-on characteristic. *Safety Science, 45*(1-2), 107-127.

Kobes, M., Helsloot, I., de Vries, B., & Post, J. G. (2010). Building safety and human behaviour in fire: A literature review. *Fire Safety Journal, 45*(1), 1-11.

Kose, S. (1999). Emergence of aged populace: Who is at higher risk in fires? *Fire and Materials, 23*(6), 337-340.

KRD, & MD. (2010). *Building regulations, BTEK2010 (in Norwegian)*. Oslo: Ministry of Local Government and Regional Development (KRD) and Ministry of the Environment (MD).

Krippendorff, K. (2006). *The semantic turn: a new foundation for design*. Boca Raton, Fla.: CRC/Taylor & Francis.

Kuhn, T. S. (1996). *The Structure of Scientific Revolutions (third edition) (first published in 1962)*. Chicago and London: The University of Chicago Press.

Kukla, A. (2000). *Social Constructivism and the Philosophy of Science*. London, GBR: Routledge.

Lamvik, H. (2001). Contributes little to the societal debate (in Norwegian). *Teknisk ukeblad* Retrieved April 5, 2013, from http://www.tu.no/nyheter/samfunn/2001/12/13/bidrar-lite-i-samfunnsdebatten

Law, M., & Beever, P. (1995). Magic Numbers and Golden Rules. *Fire Technology, 31*(1), 77-83.

Lawson, B., & Dorst, K. (2009). *Design Expertise*. New York: Taylor & Francis.

LeCoze, J.-C. (2005). Are organisations too complex to be integrated in technical risk assessment and current safety auditing? *Safety Science, 43*(8), 613-638.

LeCoze, J.-C. (2012). Towards a constructivist program in safety. *Safety Science, 50*(9), 1873-1887.

Leveson, N. (2004). A new accident model for engineering safer systems. *Safety Science, 42*, 237-270.

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

Leveson, N. (2011b). *Engineering a safer world: systems thinking applied to safety*. Cambridge, Mass.: The MIT Press.

Leveson, N., Daouk, M., Dulac, N., & Marais, K. (2004). A systems theoretic approach to safety engineering. Cambridge, MA: Aeronautics and Astronautics Dept., Massachusetts Institute of Technology.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Beverly Hills, Calif.: Sage.

Lindley, D. V. (2006). *Understanding uncertainty*. Hoboken, N.J.: Wiley.

Lizhong, Y., Xiaodong, Z., Zhihua, D., Weicheng, F., & Qing'an, W. (2002). Fire situation and fire characteristic analysis based on fire statistics of China. *Fire Safety Journal, 37*(8), 785-802.

Lundin, J. (2005). *Safety in Case of Fire – The Effect of Changing Regulations.* Doctoral thesis., Lund University (LTH), Lund.

Lundin, J., & Johansson, H. (2003). A Risk-Based Approach to Verification of Fire Safety Design Solutions. *Fire Science & Technology, 22*(1), 1-15.

MacLennan, H. A., Regan, M. A., & Ware, R. (1999). An engineering model for the estimation of occupant premovement and or response times and the probability of their occurrence. *Fire and Materials, 23*(6), 255-263.

Magnusson, S. E., Frantzich, H., & Harada, K. (1996). Fire safety design based on calculations: Uncertainty analysis and safety verification. *Fire Safety Journal, 27*(4), 305-334.

Magnusson, S. E., Frantzich, H., Karlsson, B., & Särdqvist, S. (1994). *Determination of Safety Factors in Design Based on Performance*. Paper presented at the Fourth International Symposium on Fire Safety Science, 13-17 July, 1994, Ottawa, Canada.

Maguire, R. (2008). *Safety Cases and Safety Reports : Meaning, Motivation and Management*. Abingdon, Oxon, GBR: Ashgate Publishing Group.

Mairal, G. (2008). Narratives of risk. *Journal of Risk Research, 11*(1/2), 41-54.

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems, 15*(4), 251-266.

Markie, P. (2013). Rationalism vs. Empiricism, from http://plato.stanford.edu/entries/rationalism-empiricism/

McGrattan, K., McDermott, R., Hostikka, S., & Floyd, J. (2010). Fire Dynamics Simulator (Version 5) User's Guide: National Institute of Standards and Technology (NIST).

McIntyre, G. R. (2000). *Patterns in safety thinking: a literature guide to air transportation safety*. Aldershot: Ashgate.

Meacham, B. J. (1997). *Concepts of a Performance-based Building Regulatory System for the United States*. Paper presented at the 5th international Symposium Proceedings 3-7 March, 1997, Melbourne, Australia.

Meacham, B. J. (2001). *Understanding risk*. Paper presented at the Australian Building Codes Board Conference: Building Tomorrow's Future – International and National Partners, 9-11 April 2001, Canberra, ACT, Australia.

Meacham, B. J. (2004a). Decision-Making for Fire Risk Problems: a Review of Challenges and Tools. *Journal of Fire Protection Engineering, 14*, 149-168.

Meacham, B. J. (2004b). Understanding Risk: Quantification, Perceptions, and Characterization. *Journal of Fire Protection Engineering, 14*(3), 199-227.

Meacham, B. J., & Custer, R. L. P. (1995). Performance-Based Fire Safety Engineering: an Introduction of Basic Concepts. *Journal of Fire Protection Engineering, 7*(2), 35-54.

Meehl, P. E., & Sellars, W. (Eds.). (1956). *The Concept of Emergence*: University of Minnesota Press.

Merna, A., & Smith, N. J. (1990). Project managers and the use of turnkey contracts. *International Journal of Project Management, 8*(3), 183-189.

MJPS. (2012). *Government White Paper 2012:4, Safe at home: fire safety for exposed groups (in Norwegian)*. Oslo: Ministry of Justice and Public Security (MJPS).

Monton, B., & Mohler, C. (2012). Constructive empiricism, from http://plato.stanford.edu/archives/win2012/entries/constructive-empiricism/

NBRI. (2003a). 321.025 Documentation and Control of Fire Safety (in Norwegian). Oslo: Norwegian Building Research Institute (NBRI).

NBRI. (2003b). 321.026 Fire Safety Strategy. Documentation and Control (in Norwegian). Oslo: Norwegian Building Research Institute (NBRI).

NBRI. (2003c). 321.027 Detailed Planning for Fire Safety. Documentation and Control (in Norwegian). Oslo: Norwegian Building Research Institute (NBRI).

Nilsen, T., & Aven, T. (2003). Models and model uncertainty in the context of risk analysis. *Reliability Engineering & System Safety, 79*(3), 309-317.

Nilsson, D., & Johansson, A. (2009). Social influence during the initial phase of a fire evacuation - Analysis of evacuation experiments in a cinema theatre. *Fire Safety Journal, 44*(1), 71-79.

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*(4), 458-468.

Njå, O. (1998). *Approach for Assessing the Performance of Emergency Response Arrangements.* Ph.D. dissertation, Stavanger University College, Stavanger.

NKB. (1994). Performance Requirements for Fire Safety and Technical Guide for Verification by Calculation: Nordic Committee on Building Regulations, NKB Fire Safety Committee.

Nola, R., & Sankey, H. (2007). *Theories of Scientific Method*. Durham, GBR: Acumen.

Noonan, F., & Fitzgerald, R. W. (1991). *On the Role of Subjective Probabilities in Fire Risk Management Studies*. Paper presented at the 3rd international Symposium on Fire Safety Science, 8-12 July, 1991, Edinburgh, UK.

NPRA. (2007). E39 Rogfast Impact Assessment: Traffic and Cost-Benefit Analysis (in Norwegian). Leikanger: Norwegian Public Road Administration (NPRA).

NPRA. (2010). Handbook 021 Road Tunnels (in Norwegian). Oslo: Norwegian Public Road Administration (NPRA).

NPRA. (2012). Agency Program on Contemporary Road Tunnels 2008-2011. Pioneering tunnels - long and deep, is there a limit? (in Norwegian). Oslo: Norwegian Public Road Administration (NPRA).

Nævestad, T.-O., & Meyer, S. F. (2012). Survey of vehicle fires in the Norwegian road tunnels 2008-2011. Oslo: Institute of Transport Economics.

O'Connor, T. (1994). Emergent Properties. *American Philosophical Quarterly, 31*, 91-104.

O'Connor, T., & Wong, H. Y. (2012). Emergent Properties, March 10, 2013, from http://plato.stanford.edu/cgi-bin/encyclopedia/archinfo.cgi?entry=properties-emergent

Olenick, S. M., & Carpenter, D. J. (2003). An Updated International Survey of Computer Models for Fire and Smoke. *Journal of Fire Protection Engineering, 13*(2), 87-110.

Olsson, P. A., & Regan, M. A. (2001). A comparison between actual and predicted evacuation times. *Safety Science, 38*(2), 139-145.

Paté-Cornell, E. (1994). Quantitative safety goals for risk management of industrial facilities. *Structural Safety, 13*, 145-157.

Paté-Cornell, E. (2012). On “Black Swans” and “Perfect Storms”: Risk Analysis and Management When Statistics Are Not Enough. *Risk Analysis, 32*(11), 1823-1833.

Pepper, S. (1926). Emergence. *Journal of Philosophy, 23*, 241-245.

Perrow, C. (1999). *Normal Accidents: Living with High-Risk Technologies (First published by Basic Books 1984)*. Princeton, New Jersey: Princeton University Press.

Perrow, C. (2011). Fukushima and the inevitability of accidents. *Bulletin of the Atomic Scientists, 67*(6), 44-52.

Petroski, H. (2006). *Success through failure : the paradox of design*. Princeton, N.J.: Princeton University Press.

Polanyi, M. (1962). *Personal Knowledge: Towards a Post-Critical Philosophy*. London: Routledge.

Popper, K. R. (2002). *Conjectures and refutations : the growth of scientific knowledge*. London: Routledge.

Puchovsky, M. (1996). NFPA's perspectives on performance-based codes and standards. *Fire Technology, 32*(4), 323-332.

Purser, D. A., & Bensilum, M. (2001). Quantification of behaviour for engineering design standards and escape time calculations. *Safety Science, 38*(2), 157-182.

Quintiere, J. G., di Marzo, M., & Becker, R. (2002). A suggested cause of the fire-induced collapse of the World Trade Towers. *Fire Safety Journal, 37*(7), 707-716.

Rahikainen, J., & Keski-Rahkonen, O. (1998). Determination of ignition frequency of fires in different premises in Finland. *Fire Engineers Journal, 58*(197), 33-37.

Ramachandran, G. (1988). Probabilistic Approach to Fire Risk Evaluation. *Fire Technology, 24*(3), 204-226.

Ramsay, G. C. (1979). Australian Fire Statistics. *Fire and Materials, 3*(4), 188-194.

Rasmussen, J. (1997). Risk management in a dynamic society: a modeling problem. *Safety Science, 27*, 183-213.

Rasmussen, J., & Svedung, I. (2000). *Proactive Risk Management in a Dynamic Society*. Karlstad: Swedish Rescue Services Agency.

Ravetz, J. R. (1997). Integrated Environmental Assessment Forum: developing guidelines for "good practice" *ULYSSES Working Paper-*

97-1: Urban LifestYles, SuStainability and Integrated Environmental ASsessment (ULYSSES).

Renn, O. (1992). Concepts of Risks: A Classification. In S. Krimsky & D. Golding (Eds.), *Social Theories of Risk* (pp. 53-79). Westport, CT: Praeger.

Renn, O. (2008). *Risk governance : coping with uncertainty in a complex world*. London: Earthscan.

Richardson, L. R. (2001). What fire statistics tell us about our fire and building codes for housing and small buildings and fire risk for occupants of those structures. *Fire and Materials, 25*(6), 255-271.

Ritchie, J. (2008). *Understanding Naturalism*. Durham, GBR: Acumen.

Rittel, H. W. J., & Webber, M. M. (1984). Planning problems are wicked problems. In N. Cross (Ed.), *Developments in design methodology* (pp. 135-144). Chichester: J Wiley & Sons.

Rosa, E. A. (2010). The logical status of risk - To burnish or to dull. *Journal of Risk Research, 13*(3), 239-253.

Rosenberg, T. (1999). Statistics for fire prevention in Sweden. *Fire Safety Journal, 33*(4), 283-294.

Rust, C. (2004). Design Enquiry: Tacit Knowledge and Invention in Science. *Design Issues, 20*(4), pp. 76-85.

Sagan, S. D. (1993). *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons*. Princeton, New Jersey: Princeton University Press.

Sankey, H. (2008). *Scientific Realism and the Rationality of Science*. Abingdon, Oxon, GBR: Ashgate Publishing Group.

Santos-Reyes, J., & Beard, A. N. (2001). A systemic approach to fire safety management. *Fire Safety Journal, 36*(4), 359-390.

Sardar, Z. (2001). *Thomas Kuhn and the Science Wars*. London, GBR: Icon Books.

Schön, D. A. (1991). *The reflective practitioner: how professionals think in action*: Ashgate Publishing Group.

SFPE. (2000). *SFPE engineering guide to performance-based fire protection analysis and design of buildings*. Quincy, Mass.: National Fire Protection Association (NFPA).

SFPE. (2010). *Proceedings to the 8th International Conference on Performance-Based Codes and Safety Design Methods, Lund, Sweden*. Bethesda, MD: Society of Fire Protection Engineers (SFPE).

SFPE. (2012). *Proceedings to the 9th International Conference on Performance-Based Codes and Safety Design Methods, Hong Kong, China (published electronically)*. Bethesda, MD: Society of Fire Protection Engineers (SFPE).

Shi, L., Xie, Q., Cheng, X., Chen, L., Zhou, Y., & Zhang, R. (2009). Developing a database for emergency evacuation model. *Building and Environment, 44*(8), 1724-1729.

Shrader-Frechette, K. S. (1991). *Risk and rationality: philosophical foundations for populist reforms*. Berkeley, Calif.: University of California Press.

Shyam-Sunder, S. (2005). Final report on the collapse of the World Trade Center towers *NIST NCSTAR 1 Federal Building and Fire Safety Investigation of the World Trade Center Disaster*. Washington: National Institute of Standards and Technology.

Simon, H. A. (1973). The Structure of Ill-structured Problems. *Artificial Intelligence, 4*, 181-201.

Simon, H. A. (1996). *The Sciences of the Artificial, Third Edition (first published by MIT Press in 1969)*. Cambridge, Massachusetts: The MIT Press.

Simon, H. A., Egidi, M., Marris, R., & Viale, R. (1992). *Economics, bounded rationality and the cognitive revolution*. Aldershot: Edward Elgar.

Simonovic, S. P. (2010). *Systems Approach to Management of Disasters : Methods and Applications*. Hoboken, NJ, USA: Wiley.

Singpurwalla, N. D. (2003). Knowledge management and information superiority (a taxonomy). *Journal of Statistical Planning and Inference, 115*, 361-364.

Singpurwalla, N. D. (2006). *Reliability and risk: a Bayesian perspective*. Chichester: Wiley.

Skogvang, Ø. S., Rokstad, E. M., Værnes, R., Øglænd, E., & Jenssen, G. D. (2011). Risk analysis of the Oslofjord tunnel and bypass roads (in Norwegian). Oslo: Safetec.

SN. (2012). Norwegian Standard (NS) 3901 Requirements for Risk Assessments of Fire in Buildings (in Norwegian). Lysaker: Standards Norway (SN).

Solberg, Ø., & Njå, O. (2012). Reflections on the ontological status of risk. *Journal of Risk Research, 15*(9), 1201-1215.

Spinna Jr, R. J., Spinna, R. J., & Dunn, V. (1984). *Study of the fire statistics of the Seventh Division, New York Fire Department (Northwest Bronx)*, Riverdale, MY, USA.

Stadler, F. (2003). *Vienna Circle and Logical Empirism : Re-Evaluation and Future Perspectives*. Secaucus, NJ, USA: Kluwer Academic Publishers.

Stanford, K. (2009). Underdetermination of Scientific Theory, March 21, 2013, from http://plato.stanford.edu/entries/scientific-underdetermination/

Starr, C. (1969). Social Benefit versus Technological Risk. *Science, 165*(3899), 1232-1238.

Steen-Hansen, A. (1995). Deaths due to fire in buildings. An analysis of fatal fires in the period 1978-1992 (in Norwegian). Trondheim: Sintef NBL.

Stenstad, V. (1983). *Older brick buildings and fire: a survey of brick buildings built in the period ca. 1870-1940, especially with regard to fire safety issues and fire safety.* Ph.D. thesis, Norwegian Institute of Technology (NTH), Trondheim (In Norwegian).

Suárez, M. (2011). Scientific Realism, the Galilean Strategy, and Representation. In W. J. Gonzalez (Ed.), *Scientific Realism and Democratic Society: The Philosophy of Philip Kitcher (Poznañ Studies in the Philosophy of the Sciences and the Humanities, vol. 101)*. Amsterdam/New York: Rodopi.

Sydenham, P. (2003). *Systems Approach to Engineering Design*. Norwood, MA, USA: Artech House.

UK-Gov. (2000). *Building and Buildings England and Wales: The Building Regulations 2000*. The Stationery Office Limited.

Usmani, A. S., Chung, Y. C., & Torero, J. L. (2003). How did the WTC towers collapse: a new theory. *Fire Safety Journal, 38*(6), 501-533.

Wade, C., & Whiting, P. (1996). Fire risk assessment using the building fire safety engineering method. *Journal of Fire Protection Engineering, 8*(4), 157-168.

Wallace, B., & Ross, A. (2006). *Beyond human error : taxonomies and safety science*. Boca Raton, Fla.: CRC/Taylor & Francis.

Wassenaar, H. J., & Chen, W. (2001). *An approach to decision-based design*. Paper presented at the ASME 2001 Design Engineering Technical Conferences and Computers and Information in Engineering Conference, Pittsburgh, Pennsylvania, September 9-12, 2001.

Watkins, R. (2007). *Performance By Design*. Amherst, MA, USA: HRD Press.

Watts Jr, J. M. (1991). Axioms of Fire Risk (Editorial). *Fire Technology, 27*(1), 1-2.

Weinberg, A. M. (1972). Science and Trans-Science. *Minerva, 10*(2), 209-222.

Wellington, J., & Szczerbinski, M. (2007). *Research Methods for the Social Sciences*. London, GBR: Continuum International Publishing.

Wilde, G. J. S. (2001). *Target risk 2 : a new psychology of safety and health : what works? what doesn't? and why*. Toronto, Ont.: PDE Publications.

Wilkinson, P., Glockling, J., Bouchlaghem, N., & Ruikar, K. (2011). A Historic Perspective of Fire Engineering in the UK. *Journal of Applied Fire Science, 21*(1), 37-51.

Wolski, A., Dembsey, N. A., & Meacham, B. J. (2000). Accommodating perceptions of risk in performance-based building fire safety code development. *Fire Safety Journal, 34*(3), 297-309.

Wood, N., Rust, C., & Horne, G. (2009). A tacit understanding: The designer's role in capturing and passing on the skilled knowledge of master craftsmen. *International Journal of Design, 3*(3), 65-78.

Woodside, A. (2010). *Case Study Research: Theory, Methods and Practice*. Bradford, GBR: Emerald Group Publishing Ltd.

Wormnæs, O. (1987). *Philosophy of science, 2nd edition (in Norwegian)*. Oslo: Gyldendal.

Xudong, C., Heping, Z., Qiyuan, X., Yong, Z., Hongjiang, Z., & Chenjie, Z. (2009). Study of announced evacuation drill from a retail store. *Building and Environment, 44*(5), 864-870.

Yeganeh, H., & Su, Z. (2005). Positivism and constructivism: two opposite but reconcilable paradigms in cross-cultural management research *Proceedings of 33rd ASAC Annual Conference (Administrative Sciences Association of Canada)*. Toronto, Ontario.

Yin, R. K. (1981). The Case Study Crisis: Some Answers. *Administrative Science Quarterly, 26*(1), 58-65.

Yin, R. K. (1994). *Case study research: design and methods*: Sage Publications.

Östberg, G. (2003). Some reflections on relationships between structure, properties, and performance of engineering materials. *Materials and Design, 24*, 255-262.

Østberg, K. (1897). *The church fire in Grue 1st Pentecost 1822 (in Norwegian)*. Christiania: Robert Østberg, Øvre Ullern.

PART II: PAPERS

The following papers are included in the thesis:

1. Bjelland, H., & Njå, O. (2012a). *Fourteen years of experience with performance-based fire safety engineering in Norway – lessons learned*. Paper presented at the 9th International Conference on Performance-Based Code and Fire Safety Design Methods.
2. Bjelland, H., & Njå, O. (2012b). *Interpretation of safety margin in ASET/RSET assessments in the Norwegian building industry*. Paper presented at the 11th International Probabilistic Safety Assessment and Management Conference (PSAM11) and The Annual European Safety and Reliability Conference (ESREL2012).
3. Bjelland, H., & Njå, O. (2012d). *Safety factors in fire safety engineering*. Paper presented at the Advances in safety, reliability and risk management: proceedings of the European Safety and Reliability Conference, ESREL 2011, Troyes, France, 18-22 September 2011.
4. Bjelland, H., Njå, O., Braut, G. S., & Heskestad, A. W. (Submitted). A Discussion of the Concepts of Safety Level and Safety Margin: Applications in Fire Safety Design for Occupants in Buildings.
5. Bjelland, H., & Njå, O. (2012c). *Performance-based fire safety: risk associated with different designs*. Paper presented at the Advances in safety, reliability and risk management: proceedings of the European Safety and Reliability Conference, ESREL 2011, Troyes, France, 18-22 September 2011.
6. Bjelland, H., & Borg, A. (2013). On the use of scenario analysis in combination with prescriptive fire safety design requirements. *Environment, Systems & Decisions, 33(1):33-42*.
7. Bjelland, H., & Aven, T. (2013). Treatment of Uncertainty in Risk Assessments in the Rogfast Road Tunnel Project. *Safety Science, 55:34-44*.
8. Borg, A., Bjelland, H., & Njå, O. (Submitted). Reflections on Bayesian Network models for road tunnel safety design: A case study from Norway.

On the Use of Scenario Analysis in Combination with Prescriptive Fire Safety Design Requirements

Henrik Bjelland*[1] and Audun Borg[1]

[1]*University of Stavanger, 4036 STAVANGER, NORWAY*

*(0047) 91 63 75 87

*(0047) 51 83 17 50

*henrik.bjelland@uis.no

Abstract: Experience with fire safety engineering under a performance-based fire safety regulation regime shows that the majority of the analyses performed are scenario-based. A comparison with purely pre-accepted performance requirement is made in order to assess the relative safety level of the alternative design compared to the pre-accepted design. We find this approach problematic because it undermines the value of performing analyses. The approach accepts oversimplification and justifies unrealistic assumptions on the basis that it will not affect the comparison. This distances the analyses from reality and reduces their value to answer a yes/no question on acceptability. The considerable time and resources spent on searching for and analyzing a pre-accepted design could be spent on analyzing the design at hand. If fire safety analyses are to have any real impact on design, it is necessary that regulators strengthen the position of analytical design. This must include a provision of a clear set of performance goals, which are possible to transform into quantitative evaluation criteria by the engineers, to avoid comparisons with pre-accepted performance requirements.

Keywords: *fire safety, analytical design, comparative analyses, performance-based regulations*

1. Introduction

Fire safety in Norwegian buildings is usually provided in two ways: 1) by specifying pre-accepted performance requirements from the guide to the regulations (DiBK 2010) alone, or 2) by a combination of pre-accepted performance requirements and deviations. Pre-accepted performance requirements are provided by the national authorities and constitute a set of performance levels that, through the test of time, are regarded as acceptable. However, the Norwegian fire safety regulations are performance-based. This implies that alternative fire safety designs deviating from the pre-accepted could be selected if deemed appropriate. In theory, any alternative design could be chosen as long as it is shown that the functional requirements in the regulations are fulfilled. In practice, pre-accepted performance requirements function as a base for the fire safety design in every project (Bjelland and Njå 2012a). This saves time for the fire safety engineer and provides predictability for the client. Predictability because this approach have become a discipline standard and is rarely questioned. Designing for fire safety in this way thus ensures a “smooth” design phase.

Since the pre-accepted performance requirements are generic, deviations are almost unavoidable in any project. When deviations are introduced the fire safety engineers become responsible for showing that the alternative design has an acceptable safety level. The common way of doing so is to show that the alternative design is *as good* as the pre-accepted design. In many cases this is done through comparative analysis, which means that scenarios are introduced to analyze the difference between the pre-accepted design and the alternative design (Bjelland and Njå 2012a, b).

Performing a comparative analysis of this kind simplifies responsibility issues, as there is no need to actually relate to the safety level of the design. The fire safety engineer simply assumes that the pre-accepted performance requirements are safe and the safety level provided by the alternative design is assessed relative to the pre-accepted design. Our hypothesis is that such an approach undermines the analysis process by creating a distance to reality. The introduction of comparable pre-accepted designs and assumptions is often a mere thought construct. As such, the analyses have the single purpose of covering the fire safety engineer's back in terms of responsibility. The actual results have no meaning outside the scope of the thought-constructed framework and are thus of very limited use to the client and society in general.

In Section 2 of this paper we will introduce some perspectives on the purpose of an analytical approach to safety design. In Section 3 we provide a simple example of a fire safety analysis in combination with pre-accepted fire safety design. Our purpose is to illustrate both a common practice and the limited value of this practice. In Section 4 we discuss the implications of our analysis for fire safety engineers and regulators, followed by some conclusions in Section 5.

2. Analytical Approach to Fire Safety Design

2.1 Expectations to Performance-based Engineering

During the late 1980s and early 1990s there was considerable momentum with respect to introducing fire safety science into the design of buildings, by moving from a prescriptive to a performance-based fire safety regulation regime in many countries. Emmons (1990) and Friedman (1990), amongst others, discuss the advances, challenges and future possibilities of fire safety science. Although progress has been made, the scientific field is still faced with large gaps in knowledge. Some parts of the fire phenomena are adequately understood and computer models have been developed, but there is still a long way to go before comprehensive models to investigate the wide variety of fire safety aspects are available. According to McGrattan et al. (2007) the ability to include model predictions of complicated fire phenomenon, such as fire growth and burning of complicated targets, lacks the empirical understanding of the phenomenon. Although the relevant physics is well understood, the actual process of combustion, radiation and solid phase heat transfer is more complicated than the mathematical representation currently available in the models. As a result the fire growth rate and maximum heat release rate is usually described by the analyst, and not predicted by the model. In fire safety design, however, there are also uncertainties related to future fire scenarios and what the consequences will be, i.e. future risk.

New engineering methodologies and models, discussed by Emmons (1990), Lucht (1989, 1992), Friedman (1990) and others, were introduced along with performance based codes. Some of the advantages associated with such codes were their ability to address unique aspects of the building and/or its use, address a client's specific needs, increase engineering rigor by introducing tools for evaluating fire safety, the possibility of addressing the overall fire safety of the building instead of treating each system in isolation, cost-effective solutions and an improved knowledge of the loss potential in the buildings (Meacham and Custer 1995).

The risk concept and risk assessment tools have been discussed in the fire safety science literature during the past few decades for possible introduction into fire safety engineering (see e.g. Hall and Sekizawa 1991; Watts Jr 1988; Frantzich 1998). However, our experience is that risk assessments are not a commonly used tool to measure fire safety levels in building designs (Bjelland and Njå 2012a, b). The most common tool, when analyses are being performed, is a scenario-based approach. Formal guidance for this approach has been provided, amongst others, by the International Organization for Standardization (ISO) and the Society for Fire Protection Engineers (SFPE). The basic principle in this approach is to develop a *trial design* which the engineers must verify to comply with the regulations. The trial design is based on the client's (or architect's) proposal, where fire safety measures are introduced in an intuitive way by the fire safety engineer such that the design is expected to meet performance requirements. Possible fire and situational scenarios must be identified and a set of design scenarios must be selected from these. The design scenarios are to be evaluated against performance criteria which define some critical limits of human tolerability, e.g. a temperature limit which leads to human incapacitation or a visibility limit which restrains motion. If the design scenarios lead to violation of the performance criteria, e.g. visibility is too low when people are still present in the building, a modified trial design must be developed and the process repeated until all performance criteria are met (SFPE 2000; ISO 2006).

2.2 Comparative analyses

Comparative analyses assess the performance of the alternative design relative to the code compliant design given a fire. The parameters of interest may be related to life safety, for example the available safe egress time (ASET) and the required safe egress time (RSET), or property protection, for example the thermal load on the structure or fire and smoke spread.

When considering the appropriateness of the comparative analysis it is important to address the reasons for choosing this approach in the first place. One argument for choosing a comparative analysis is that a performance based fire safety code rarely contains explicit acceptance criteria for fire safety. The desired function of the building, in terms of fire safety, is given by the fire safety code. However, the "translation" of the desired function into an explicit safety requirement is only reflected in the proposed pre-accepted performance requirements. This means that for example the transformation of the functional requirement; "... occupants should be provided with adequate means of escape," into explicit quantitative requirements, is only given by examples in the pre-accepted performance requirements.

Generally there are two situations where a comparative analysis is applied:

1) To assess the level of safety obtained in a building through inclusion of the pre-accepted performance requirements and compare the answer to the level of safety obtained in the alternative design.
2) To apply the pre-accepted performance requirements for fire safety as far as possible and assess the consequences of the deviations on a case by case basis.

In both cases the decision to accept an analytical design solution is reduced to a simple yes or no answer. In the following the two situations for comparative analysis are assessed.

Level of safety based on pre-accepted fire safety design:
In some design situations the engineer may be required to document an analytical design solution by assessing the overall level of safety in the building or construction. One of the main challenges for the engineer in this case is that the required level of safety is not stipulated in quantitative terms. A comparative analysis will hence be an attractive approach.

In order to conduct a comparative analysis in this case it is necessary to construct a reference building based on pre-accepted performance requirements. An issue with this approach is that the prescriptive code provides the engineer with several design options. However, the level of safety provided by these various choices is not consistent (Bjelland and Njå 2012c). This issue is illustrated in **Fig. 1** by the following example: Consider a 6-story office building with a footprint of 2000 m^2 where the engineer is faced with at least the following pre-accepted performance requirements:

- Structural fire safety: steel, or concrete.
- Active fire safety measures: sprinklers, or smoke ventilation.
- Egress: access to the stairs directly, or via a corridor / lobby.

In practice there are even more design options, but these alone would result in 8 different combinations, all of which would lead to an acceptable design in Norway and in accordance with DiBK (2010).

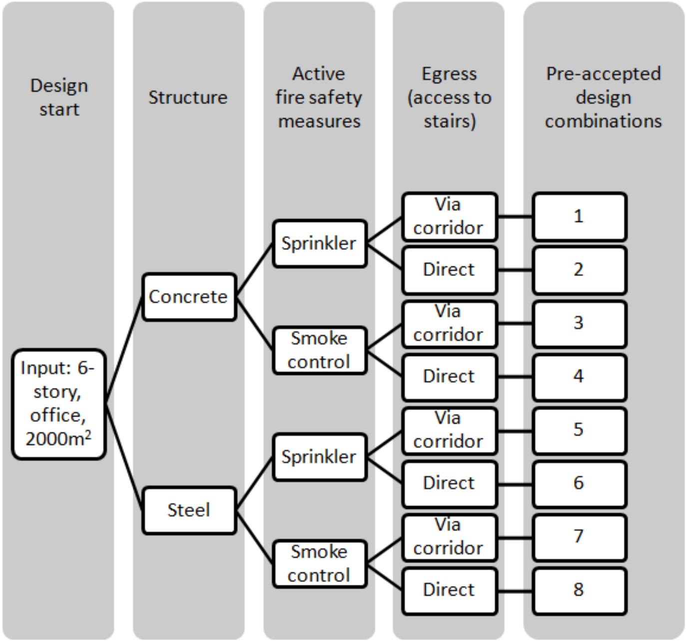

Fig. 1 Illustration of possible combinations leading to a set of different pre-accepted designs

Fig. 1 illustrates the issue of selecting a valid basis for comparison amongst several options with different safety levels. Let us suppose, for example, that the building under consideration was planned to include a sprinkler system: one may argue that choosing a pre-accepted design without a sprinkler system for comparison is not valid. On the other hand, one may argue that it is when the pre-accepted performance requirements are pushed to the limit that the actual minimum safety level provided by the code is revealed.

<u>Case by case analysis of the deviations:</u>

Another situation where a comparative analysis is used is in a case by case analysis of the deviations from the pre-accepted performance requirements. This means that the fire safety design follows the pre-accepted performance requirements as far as possible, and a comparative analysis is conducted for the deviation only. The study made by Bjelland and Njå (2012a) showed that a majority of analyses in fire safety engineering are conducted in this manner. The methodology is illustrated in **Fig. 2**, where the design follows a set of pre-accepted performance requirements to a certain point before a deviation is introduced.

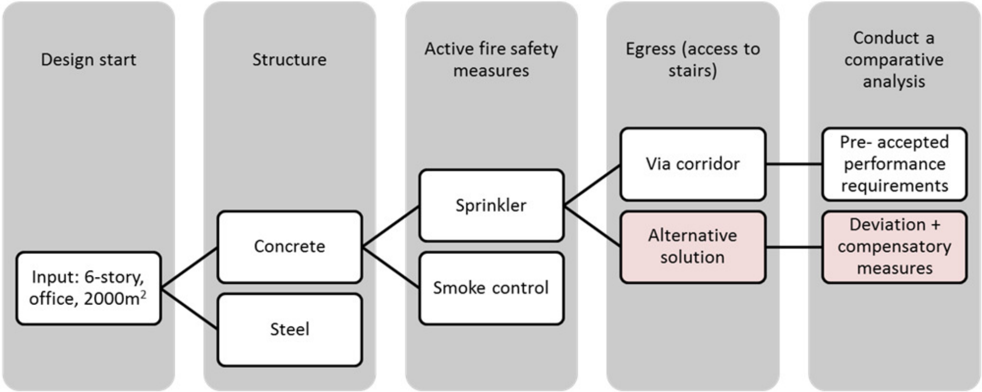

Fig. 2 Illustration of the implementation of a deviation leading to a pre-accepted reference building and an alternative/deviating design

In practice the analytical design in this case consists of a deviation from the pre-accepted performance requirements including a compensatory measure which is compared to a strict pre-accepted design. The acceptance criteria for the design are found by measuring a quantity in both cases, for example time to untenable conditions, and the design is acceptable if the quantity is equal to, or better than, the value provided by the pre-accepted design. An example of this approach is given in the next section. The positive aspects of this method are largely the same as in the method above. It is also effective, as areas that follow pre-accepted performance requirements do not require in-depth analysis. However, a major issue here is whether all risk-influencing factors are included in the analysis.

3. Life Safety in Case of Fire in a Concert Hall

In this section we introduce an example that will illustrate some of the problems of performing comparative scenario analyses. The example represents a common decision problem within fire safety design: will our alternative design perform as good as or better than a pre-accepted design with respect to life safety in case of fire? The example is inspired by our findings with respect to common practice (Bjelland and Njå 2012b). The common practice is to introduce the available safe egress time (*ASET*) versus required safe egress time (*RSET*) concept. If *ASET* is larger than *RSET*, with an acceptable safety margin, life safety is provided. The safety margin is the difference between *ASET* and *RSET*.

$$\textit{Safety margin} = ASET - RSET$$

In the example we are considering a single story building with characteristics in accordance with **Table 1**. Our design, referred to as the alternative design, deviates from pre-accepted performance requirements in terms of exit width. According to the guide to the regulation (DiBK 2010), the exit width should be 30 m, distributed over at least 10 exits. It is argued that a ceiling height of 6 m is far more than what could be expected in a pre-accepted design, where the minimum requirement is 2.7 m. In the example we have used 3 m ceiling height. Since we know that a tall ceiling will increase *ASET*, by delaying the hot smoke layer from reaching the persons underneath it, we find it acceptable to allow for a larger *RSET*, as long as the safety margin stays the same.

A tall ceiling means that the smoke detectors will be slower to respond than in the case of a low ceiling. To compensate for this we assume the installation of a more sensitive alarm system based on optical line detection. Other factors such as the time of day, occupant characteristics, building location, preparedness measures, structural fire resistance, materials on internal surfaces etc. are assumed to be equal and not relevant for the purpose of the analysis. As such, the assumptions made in this example are in accordance with common practice for this type of analysis.

Table 1 Building characteristics

	Alternative design	**Pre-accepted design**
Floor area	1 800 m^2 (30 m x 60 m)	1 800 m^2 (30 m x 60 m)
Number of people	3 000 people	3 000 people
Ceiling height	6 m	3.0 m
Maximum distance to exit	Less than 30 m	Less than 30 m
Number of exits	13 x 1.2 m	12 x 2.4 m + 1 x 1.2 m
Total exit width	15.6 m	30 m
Sprinkler system	No	No
Alarm system	Yes, optical line detection	Yes, common smoke detection

3.1 RSET Calculation

RSET is defined as the sum of time for *detection*, *warning*, *pre-travel* and *travel* (ISO 2009). In this case warning and pre-travel time are treated as constants for both designs, i.e. it is assumed that they are equal. Consequently, detection and travel time are the only relevant variables when calculating *RSET* in this case. Since there are large uncertainties associated with the time it takes before people start moving towards an exit in case of fire it would be hard to justify such an assumption outside a comparative framework. Travel time, t_{trav}, is calculated as the sum of the time it takes to reach an exit, t_{walk}, and the time taken to queue and pass through the door, t_{que} (NBRI 2006b):

$$t_{walk} = L/v$$
$$t_{que} = N/F$$
$$F = v \times \rho_p \times B$$

where;

L	is the maximum length to an exit [30 m].
v	is the walking speed [0.6 m/s].
N	is the number of persons [3000 persons].
B	is the effective width of the exit [m], which is 0.15 m less than the free width.
F	is the flow of people through an exit [person/s].
ρ_p	is the occupant density [1.67 person/m^2].

Time needed to walk to the exits, t_{walk}, is calculated to be 50 s for both the alternative and pre-accepted design. Time spent queuing and passing through doors is dependent on the flow capacity of the doors. The flow capacity is calculated to be 13.7 person/s and 28.1 person/s for the alternative and pre-accepted design respectively. Resulting travel time is presented in **Table 2**.

According to Norwegian guidance documents a line detection system can be assumed to have a response time of 20-40 % of a regular smoke detector (NBRI 2006a). Response time for common smoke detectors is given as a function of ceiling height and fire growth in BE (2000). For rooms with a ceiling height of 3 m and 6 m and a fire growth of t_g = 225 s it prescribes a detection time of 60 s and 90 s respectively. This leads to a detection time of 36 s (40 % of 90 s) for the alternative design and 60 s for the pre-accepted design.

Table 2 The components of *RSET* for the alternative and pre-accepted design

	Detection time	**Reaction time**	**Travel time**	***RSET***
Alternative design	36 s	180 s	270 s	486 s
Pre-accepted design	60 s	180 s	157 s	397 s

3.2 ASET Calculation with Fire Dynamics Simulator (FDS)

ASET is the available safe egress time, and is here assumed to be the time from when a fire occurs until the visibility measured at a height of 2 m above floor level reaches 10 m on average. A complete *ASET* assessment should include other factors, for instance heat exposure and toxicity, but our experience is that lack of visibility is often the first indication of the occurrence of *ASET*. Hence, for the sake of this example, lack of visibility is considered sufficient as an indicator of *ASET*. To evaluate *ASET* for the two situations described above, computational fluid dynamics (CFD) models have been made using the computer software FDS version 5.5.3. FDS is a model for fire-driven fluid flow developed by the National Institute of Standards and Technology (NIST), and it solves a version of the Navier-Stokes governing equations applicable for in-compressive low velocity flow, which makes it applicable for fire modeling (McGrattan et al. 2007).

Although the example is included for illustrative purposes, efforts have been made to follow best practice in constructing the model. No grid sensitivity study to determine the grid resolution has been conducted but the well-known criteria: $D^*/\delta x$ has been assessed, where δx is the grid resolution (in meters) and D^* is the characteristic fire diameter (McGrattan et al. 2010):

$$D^* = \left(\frac{\dot{Q}}{\rho_\infty c_p T_\infty \sqrt{g}} \right)^{\frac{2}{3}}$$

where;

$\dot{Q}$	is the heat release rate [kW]
ρ_∞	is the density of air [kgm^{-3}]

c_p is the thermal heat capacity of air [$\mathrm{kJkg^{-1}K^{-1}}$]

T_∞ is the ambient temperature [K]

g is the acceleration due to gravity [$\mathrm{ms^{-2}}$]

Guidelines for required grid resolution vary depending on the scope of the analysis, and values of $D^*/\delta x$ normally range from 4 to 16 (McGrattan et al. 2010). Similar guidelines for required resolution are provided elsewhere such as in Hadjisophocleous and McCartney (2005) and U.S.NRC (2007:6-5). In the example the value $D^*/\delta x = 12.5$ which is assumed to be an appropriate resolution for this model given the scope of the analysis, which is to compare two design alternatives, and calculating the heat and mass transfer from the fire to the hot smoke layer. The area of the fire is chosen as a function of the maximum heat release rate, such that the dimension-less quantity, Q^*, is in the order of 1, as recommended for accidental fires by NRC (NRC 2007:6-4). The quantity, Q^*, is a relationship between the heat release rate, $\dot{Q}$, and the diameter of the fire, D:

$$Q^* = \frac{\dot{Q}}{\rho_\infty c_p T_\infty \sqrt{gD}\, D^2}$$

Table 3 lists some of the properties of the FDS model.

Table 3 Properties of FDS model

Factor	**Input**	**Comment**
Heat release model	$\dot{Q} = \alpha t^2$	$\alpha = 0.01975$
Time to reach 1 MW, t_g	225 s	
Heat release rate per unit area, HRRPUA	2 291 $\mathrm{kWm^{-2}}$	Leads to $Q^* = 1.03$
Burning material	Dry wood	Original set-up
	Polyurethane/wood	Sensitivity study
Soot yield burning material, S_y	0.01	Dry wood
	0.07	Polyurethane with reduced soot yield to represent a mixture of plastics and wood.
Radiation fraction	0.35	Default value in FDS (McGrattan et al. 2010)
Grid size, [*dx, dy, dz*]	0.2 m, 0.2 m, 0.2 m	Leads to $D^*/\delta x = 12.5$
Simulation length	900 s	
Room temperature	20 °C	
Outside temperature	10 °C	

Fig. 3 depicts the reduction of visibility as a function of time for a measuring point 2 m above the floor in the example. The measuring point is the same in all graphs and shows both the pre-accepted design and the alternative design for a soot yield of both 0.01 and 0.07. The fire growth rate, t_g, is assumed to be 225 s in accordance with common practice in Norway for this kind of occupancy (BE 2000). The results are summarized in **Table 4**.

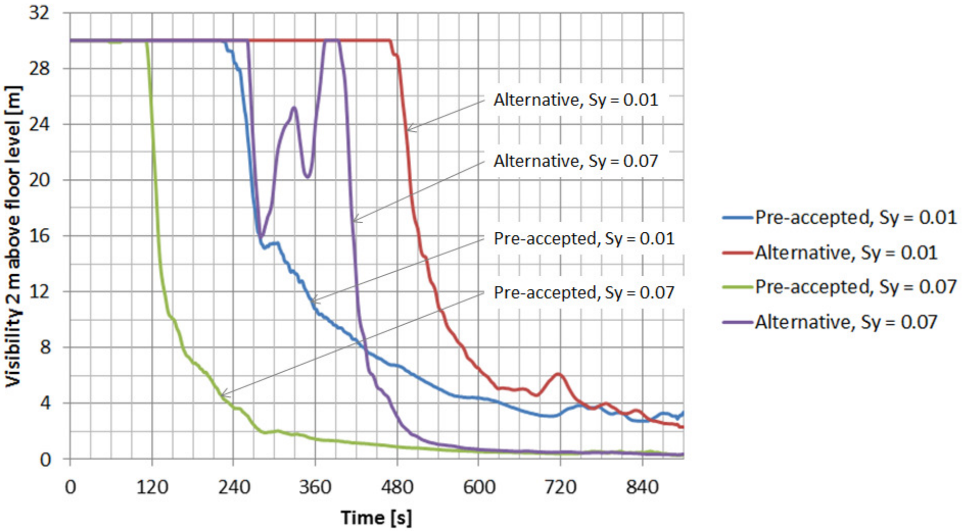

Fig. 3 Reduction of visibility as a function of time for a measuring point 2 m above the floor for two different designs and two different soot yields

Table 4 Comparison of safety margin for the alternative and pre-accepted design

	ASET	RSET	Safety margin
Alternative design, $S_y = 0.01$	546 s	486 s	60 s
Alternative design, $S_y = 0.07$	428 s	486 s	- 58 s
Pre-accepted design, $S_y = 0.01$	387 s	397 s	- 10 s
Pre-accepted design, $S_y = 0.07$	157 s	397 s	- 240 s

When assuming that the burning material is pure dry wood, with a soot yield, S_y, of 1 %, we find that the safety margin is positive for the alternative design and marginally negative for the pre-accepted design. When using a different soot yield, S_y, of 7 %, representing a combination of wood and plastics materials, we find that both designs have a negative safety margin.

4. Discussion

4.1 Interpretation of the results from calculation example

The main purpose of this paper is to elaborate on the use of scenario analysis in combination with prescriptive fire safety requirements, which very often implies a comparative analysis methodology. In a previous paper we have documented that more or less appropriate assumptions are justified by the fact that the analysis is comparative (Bjelland and Njå 2012b). This means that for example the soot yield is not considered specifically, since it is assumed that this yield is equal for both the alternative design and the pre-accepted reference building.

In the previous section we have provided an example of an analysis which we would expect to find in real life projects. From our main scenario analysis we find that the safety margin between *ASET* and *RSET* is positive only for the alternative design. Hence we can conclude that the alternative design is better than, or as good as, the pre-accepted design with respect to life safety. Based on the results presented, the alternative design would have been found acceptable, since it performs better than the pre-accepted design.

It could be argued that a safety margin of 60 s is too small in any case. This would of course be an appropriate concern, but then we would also have to question the safety level of the pre-accepted design, which has a negative safety margin for the same scenario. This illustrates our main message: as long as you can "hide" behind pre-accepted performance requirements, it is hard to question the results of the analysis. Consequently the overall application of comparative analyses and the information value from such analyses should be questioned. This is not least the case when the pre-accepted performance requirements are highly generic, as is the case in Norway, and when there is no guidance on how to select a valid reference design.

To illustrate what happens when we consider a different soot yield, representing a combination of wood and plastics, we have provided an additional *ASET* calculation. We find that the safety margin is negative for both the alternative and the pre-accepted design. Paradoxically, the conclusion remains the same as the alternative design is better than the pre-accepted design, since the safety margin is less negative for the alternative design. Consequently the alternative design could be selected on this basis. However, the soot yield could probably be reduced to a value which leads to a positive safety margin, so that the message of the analysis does not become excessively alarming for the client. After all, the attractive trait of the comparative analysis is that it does not matter what quantity is used, as long as they are treated equally in both designs.

In an earlier paper (Bjelland and Njå 2012c) we have shown that the pre-accepted performance requirements do not provide a single consistent safety level. Thus, knowing that an alternative design is better than a pre-accepted design would not provide much information about the safety level in the building. However, one important benefit of this knowledge is that the fire safety engineer need not take on responsibility for the fire safety level. It is simply implicitly assumed that the safety level is sufficient based on the pre-accepted design. This is an appreciated property of the approach for the fire safety engineer and one which implies a low liability risk.

Our experience is also that clients make very few demands with respect to fire safety design, and if they do there is usually a reference to the pre-accepted performance requirements as a maximum level of fire safety, although these are supposed to represent a minimum level (DiBK 2010). Consequently, fire safety design is closely related to pre-accepted performance requirements, both for the sake of simplicity and responsibility issues for the fire safety engineers and because it is a low priority for the client. A large number of deviation assessments are performed in most projects, but none of them has any information value in terms of describing a fire safety level (Bjelland and Njå 2012a).

4.2 Problems of Comparative Scenario Analyses

From an analytical point of view the use of comparative assessments is problematic. By an analytical point of view we mean an analysis of design issues made with the purest intentions and goals. Analyses are tools to aid the designer when there is uncertainty, i.e. lack of knowledge, related to the consequences of the design. With respect to fire safety, this could be uncertainty related to how the building will perform during a fire and how people in the building will be affected by the fire.

In our example in Section 3 we introduced many assumptions to simplify the problem, justified by the fact that we were only interested in the difference between an alternative and a pre-accepted design. First of all, we only considered one scenario for each design under the assumption that other scenarios would show the same tendency of difference in favor of the alternative design. It is difficult to determine that this is actually so without performing a systematic search for possible scenarios. However, our experience is that this is the common way of verifying fire safety design when deviations are introduced (Bjelland and Njå 2012b).

If we were to gain insight from the analysis with respect to safety, we would have to introduce the factors that actually affect safety level and question whether the models used were sufficiently accurate or appropriately tuned for our purpose. For the example provided in this paper this would include a thorough assessment of the possible fire scenarios in the actual building. This would include an analysis regarding the impact the ceiling height has on the actual fire, the fire load in the building and the occupants escaping. In addition this assessment would be necessary to determine required level of safety in the building on the basis of the use of the building and the characteristics.

The reasons for performing a performance based analysis in fire safety engineering are due to the fact that the building, or construction, in question falls outside the prescriptive regime. As such it is our view that the analysis should aim to accommodate the unique features of the building in both the fire scenarios and methodology adopted in the analysis. This is important in order to assess the features of the building that makes it inappropriate for prescriptive design in the first place. However, the current approach seems to acknowledge oversimplification in fire scenario selection and methodology. Questionable assumptions is justified on the basis that it will not affect the assessment as a comparative analysis is undertaken.

One of the main traits of performance based design regime is that the fire safety engineers should have the opportunity to explicitly assess the level of fire safety required in a building, or a construction. In a consequence analysis this implies that the fire scenarios selected for the analysis are appropriate, and include the characteristics of the building. This would typically be done through an assessment where specific parameters which influence the fire scenario, such as the fire load, occupancy, ventilation, materials and surfaces, are assessed. Our experience is that the fire scenario itself is seldom analyzed in such assessments, and only a few generic scenarios are chosen as the basis for a comparison (Bjelland and Njå 2012b).

4.3 Implications for Fire Safety Regulators

In a performance-based fire safety regime the ideal would be to have quantifiable performance requirements which the results of the analysis could be evaluated against. This is not an easy task since there are large gaps in current knowledge of the causal relationship between fire safety requirements and the resulting risk to the lives and health of occupants and fire and rescue personnel, and property protection. It seems unrealistic to expect fire safety designs to be based on pure performance requirements in the near future. A combination of best practice performance requirements and analytical approaches is inevitable, but as our knowledge of the phenomena and causal relationships grows, the analytical part can be expanded. The regulators need to take on responsibility for creating a framework for the development of important fire engineering knowledge. Today, feedback from real fires and firefighting actions are nearly non-existing, leading to analyses which makes use of very generic data.

However, what we consider a matter of urgency is the provision of a framework for analytical fire safety design that does not involve comparisons with pre-accepted designs. This must include a set of precise functional requirements and performance goals to be addressed by the analyses. Furthermore, a set of fire and situational scenarios seems necessary, including tolerability criteria to compare the scenarios against. The level of detail in the description of scenarios seems to be a matter of trust in the fire safety engineering community. Under the assumption that all complex fire safety designs must be subject to independent control, it is possible that the community will adhere to the best practice and that a limited level of detail is necessary. This will infer a drive towards more knowledge-based designs. Today it is routine-based, requiring little or no specific knowledge.

The main goal of encouraging more analytical designs should be the introduction of updated knowledge into design decision problems. A first step is to acknowledge that the pre-accepted performance requirements have great limitations with respect to covering the variety of complex buildings expected to be erected in the future. Other countries have taken steps to improve the current situation of analytical fire safety design. Examples are new guides on analytical fire safety design in Sweden (Boverket 2011) and New Zealand (DBH 2012). Both countries have made efforts to provide clearer performance goals and minimum requirements to the selection of design scenarios and tolerability criteria for evaluation. The work in these countries will hopefully lead to analyses having more impact on the decisions to be made.

4.4 Implications for Fire Safety Engineers

Although the authorities need to take steps to improve the situation, the organizations dealing with fire safety engineering represent both high competency and capacity with respect to developing the discipline further. It is necessary that fire safety engineers contribute to regulative development and that they build and sustain competency on analytical design.

In the current situation it could be questioned to what degree fire safety engineers contribute with any valuable knowledge by performing comparative analyses. They are to some degree managing the requirements from the authorities by considering if the alternative designs are just as good as, or better than, pre-accepted designs. The phrasing “to some degree” is used because the selection of reference buildings, or pre-accepted designs, for comparison is often a thought-construction and the validity of the selections could be questioned. However, it is towards the demands of the clients that the fire safety engineers fail to make any real influence. Even though most clients fail to state any explicit fire safety requirements, it does not mean that they do not have any. But clients need to address many functional requirements, and fire safety is just a small part of the whole design. If fire safety engineers are to have any impact on the client, the decision maker, they must show that their work benefits the overall design and project costs. An appropriate way forward would be to perform analyses which are as close to reality as possible, without introducing disturbing reference designs which really does not exist. Then it would be possible to assess the cost-effectiveness of fire safety measures and take part in an optimization process involving other disciplines.

5. Conclusions

To accommodate the principles of performance-based fire safety engineering, the industry has adopted a methodology largely based on scenario analyses in combination with pre-accepted performance requirements and deviations, through comparative assessments. This is unfortunate with respect to achieving important goals of performance-based engineering, for instance the ability to address unique buildings and build awareness about safety levels. Fire safety engineers find it appropriate to introduce assumptions and simplifications which distance the analysis from the actual situation. It is argued that important issues, most likely to affect fire safety in the building, are not relevant for the purpose of comparative analyses. The only goal is to show that the alternative design is just as good as, or better than, a pre-accepted design. Hence, the analyses do not provide any insight into issues which really affect the safety level, and are only useful within the framework of the comparative assessments. Since important factors are left out, e.g. the way different people will react to a fire, differences in their walking speed and variations in fire development and characteristics, only a limited amount of information is transferred from the engineer to the building operator.

Our view is that analyses should only be performed when there is uncertainty, i.e. lack of knowledge, which prevents one from making a decision on fire safety design. That is why the focus of the analyses should be on gaining knowledge which is important to the decision makers. When comparative analyses are performed, much time is spent on defining and analyzing a pre-accepted design, which is not relevant for the design at hand. We find this to be an inappropriate use of resources. Furthermore, since pre-accepted designs are loosely described, it is often possible to find a pre-accepted design with a lower safety level than the one you are designing.

Scenario analyses are, and will probably always be, important in fire safety engineering. The current engineering framework is designed in such a way that scenario thinking is encouraged. Furthermore, the models used in fire safety engineering are usually deterministic and are based on a certain fire, situational and behavioral scenario. The challenges involved in gaining probabilistic information on human behavior, i.e. a foundation for developing uncertainty distributions, will also favor deterministic scenario analyses in fire safety engineering.

If scenario analyses are to be successful in fire safety engineering, all factors affecting fire safety level should be incorporated. Regulators need to develop a clear set of performance requirements to fire safety, capable of being readily transformed into performance criteria by the designers. Regulators should also impose requirements on the engineering process and the competency of the designer. We find it appropriate to separate between two approaches:

1. Design by the use of pre-accepted performance requirements.
2. Analytical design.

Most buildings will fall into category one. Hence, less competence and assessment effort should be required by enterprises dealing with pre-accepted design. This is in accordance with the system in Norway today. A major change, however, should be that no deviations are allowed within approach one. A more extensive guide to the regulations, i.e. pre-accepted performance requirements, should be implemented. This guide should have a clear range of application and presumably be arranged specifically for building types, or service category. In this way, common deviations that we find today can be incorporated into the pre-accepted performance requirements, which would lead to both flexibility and predictability for the designer and building owner.

When approach two is selected, it is recognized that there are no pre-accepted performance requirements to compare with. The design must be based on analyses and the regulators should establish a procedure which includes the development of fire safety goals and performance criteria and stakeholder involvement. In addition, some minimum requirements should probably be imposed on the scenario selection and the use of models. Furthermore, specific data is needed for the analyses, which imply the need for a feedback loop from real fires and firefighting operations. Designers following the analytical approach should continuously be able to document a high competency in fire safety engineering. Under the present Norwegian system responsibility is assigned to the enterprise as a whole. As competence might differ amongst different engineers within the enterprise, project-specific quality requirements seem more appropriate. The documentation of competency should be a part of the project. An independent controller should have the task of considering whether competency is appropriate.

Acknowledgements

The authors are grateful to two anonymous reviewers for valuable comments to the original version of this paper. The authors declare that there are no conflicts of interests with respect to the content of this paper.

References

BE (2000) Guideline on Smoke Ventilation (in Norwegian). National Office of Building Technology and Administration (BE), Oslo.

Bjelland H, Njå O (2012a) Fourteen Years of Experience with Performance-Based Fire Safety Engineering in Norway – Lessons Learned. Paper presented at the 9th International Conference on Performance-Based Code and Fire Safety Design Methods, The Excelsior Hong Kong, 20-22 June 2012.

Bjelland H, Njå O (2012b) Interpretation of Safety Margin in ASET/RSET Assessments in the Norwegian Building Industry. Paper presented at the European Safety and Reliability Conference (ESREL 2012), Helsinki, Finland, 25-29 June 2012.

Bjelland H, Njå O (2012c) Performance-based Fire Safety: Risk Associated with Different Designs. Paper presented at the Advances in safety, reliability and risk management: proceedings of the European Safety and Reliability Conference, ESREL 2011, Troyes, France, 18-22 September 2011.

Boverket (2011) Boverkets allmänna råd 2011:xx. Vägledning i analytisk dimensionering av byggnaders brandskydd (in Swedish). Boverket, Oktober 2011.

DBH (2012) C/VM2 Verification Method: Framework for Fire Safety Design. For New Zealand Building Code Clauses C1-C6 Protection from Fire. New Zealand Government, Department of Building and Housing, Wellington.

DiBK (2010) Guide to the Building Regulations of 2010. The Directorate of Building Quality, Oslo.

Emmons HW (1990) Firesafety Science - The Promise of a Better Future. Fire Technology 26 (1):5-15.

Frantzich H (1998) Risk analysis and fire safety engineering. Fire Safety Journal 31 (4):313-329.

Friedman R (1990) Fire Protection Engineering - Science or Art? Journal of Fire Protection Engineering 2 (1):25-29.

Hadjisophocleous GV, McCartney CJ (2005) Guidelines for the use of CFD simulations for fire and smoke modeling.

Hall JR, Sekizawa A (1991) Fire risk analysis: General conceptual framework for describing models. Fire Technology 27 (1):33-53.

ISO (2006) ISO/TS 16733:2006 Fire safety engineering - Selection of design fire scenarios and design fires. International Organization for Standardization, French Standard Institute (AFNOR).

ISO (2009) ISO/TR 16738:2009 (E) Fire-Safety Engineering – Technical information on methods for evaluating behavior and movement of people. International Organization for Standardization, Geneva.

Lucht DA (1989) Coming of Age. Journal of Fire Protection Engineering 1 (2):35-48.

Lucht DA (1992) Changing the way we do business. Fire Technology 28 (3):271-276.

McGrattan K, Hostikka S, Floyd F, Baum H, Rehm R (2007) Fire Dynamics Simulator (Version 5) Technical Reference Guide. National Institute of Standards and Technology (NIST) Special Publication 1018-5, Washington.

McGrattan K, McDermott R, Hostikka S, Floyd J (2010) Fire Dynamics Simulator (Version 5) User's Guide. National Institute of Standards and Technology (NIST) Special Publication 1019-5, Washington.

Meacham BJ, Custer RLP (1995) Performance-Based Fire Safety Engineering: an Introduction of Basic Concepts. Journal of Fire Protection Engineering 7 (2):35-54.

NBRI (2006a) 520.380 Smoke Control in Buildings (in Norwegian). Norwegian Building Research Institute, Oslo.

NBRI (2006b) 520.385 Required Safe Egress Time in Fire Situations (in Norwegian). Norwegian Building Research Institute, Oslo.

NRC US (2007) Verification and Validation of Selected Fire Models for Nuclear Power Plant Applications, Volume 7: Fire Dynamics Simulator (FDS). U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research (RES), Rockville, MD and Electric Power Research Institute (EPRI), Palo Alto, CA.

SFPE (2000) SFPE engineering guide to performance-based fire protection analysis and design of buildings. NFPA, Quincy, Mass.

Watts Jr JM (1988) Fire Risk Analysis (editorial). Fire Technology:289-290.

Treatment of Uncertainty in Risk Assessments in the Rogfast Road Tunnel Project

Henrik Bjelland[a]* and Terje Aven[a]

[a] University of Stavanger, 4036 Stavanger, Norway

* Corresponding author, email: henrik.bjelland@uis.no, telephone: (+47) 916 37 587, fax: (+47) 51 83 17 50

Abstract

In this paper we review and discuss the use of risk assessments in the design of the world's longest and deepest subsea road tunnel, the Rogfast. We show that there is a discrepancy between the existence of uncertainties in both phenomena and assumptions on the one hand, and the way these uncertainties are assessed and handled in the risk assessment and risk management processes on the other: considerable uncertainties and risks are neglected. The main purpose of the paper is to point to this situation and present a more suitable framework for how to assess and manage this type of risk and uncertainties.

Keywords: *Sub-sea road tunnels, risk, risk assessments, uncertainty*

1. INTRODUCTION

The Rogfast subsea road tunnel project is based on a vision from the early 1980s of replacing the heavily trafficked ferry connection across the Bokn fjord in Rogaland county, Norway (Alsaker, 1997). It will be an important link in the transport corridor on Norway's west coast, and its existence holds the promise of a more reliable and effective transportation system. This could lead to new jobs and housing markets and a growth in the regional economy. The benefits of the project are considered numerous and the proponents outnumber the opponents. Societal cost benefit analyses also show, in contrast to many other Norwegian road projects, that the benefits outweigh its costs.

On the other hand, the Rogfast will be the world's longest and deepest road tunnel if realized, and this causes concerns about the safety of its users and rescue personnel in the case of accidents. Many drivers experience anxiety when driving in large road tunnels (Amundsen, 1994; Flø and Jenssen, 2007; Vashitz et al., 2008). This can lead to unwanted behavior and accidents. Monotony due to lack of visual stimulation is also considered a problem in the long tunnel (Jenssen et al., 2006), which can lead to people falling asleep while driving. Furthermore, the consequences of road accidents always have the extra potential of being catastrophic when they occur in tunnels. If a fire or explosion occurs, the tunnel geometry will affect fire and smoke spread (Carvel, 2004; Lönnermark and Ingason, 2006; Melvin and Gonzalez, 2009; Nilsen, 2011) and explosion pressure waves (van den Berg and Weerheijm, 2006), with the potential of exposing a large number of people to fatal danger. Furthermore, the longer the tunnel, the longer the distance to safe areas and response times for rescue services (Manca and Brambilla, 2011).

Safety in Norwegian road tunnels is generally handled within a prescriptive regulatory framework. Rogfast, on the other hand, falls outside the scope of the prescriptive regulations *Handbook 021 Road Tunnels* (HB 021) (NPRA, 2010) due to its length. The standard does not provide solutions for tunnels longer than 10 km, while the main tubes of Rogfast is planned to be approximately 25.5 km, plus a 4 km intersected tube to Kvitsøy (**Fig. 1**). Furthermore, the planned tunnel route results in a gradient of maximum 7 %, with the lowest point at 390 m below sea level. In such cases the safety design is to be based on risk assessments, and additional safety measures (with respect to the prescriptive regulations) should be introduced if necessary. Two risk and vulnerability assessments have been conducted in the Rogfast project on behalf of the project management: one in 2006 (Norconsult, 2006) and another in 2011/2012 (Sintef/Cowi, 2012). The second assessment builds upon the first and is intended to provide a more detailed analysis, with special emphasis on events with a large loss potential, i.e. fires and explosions.

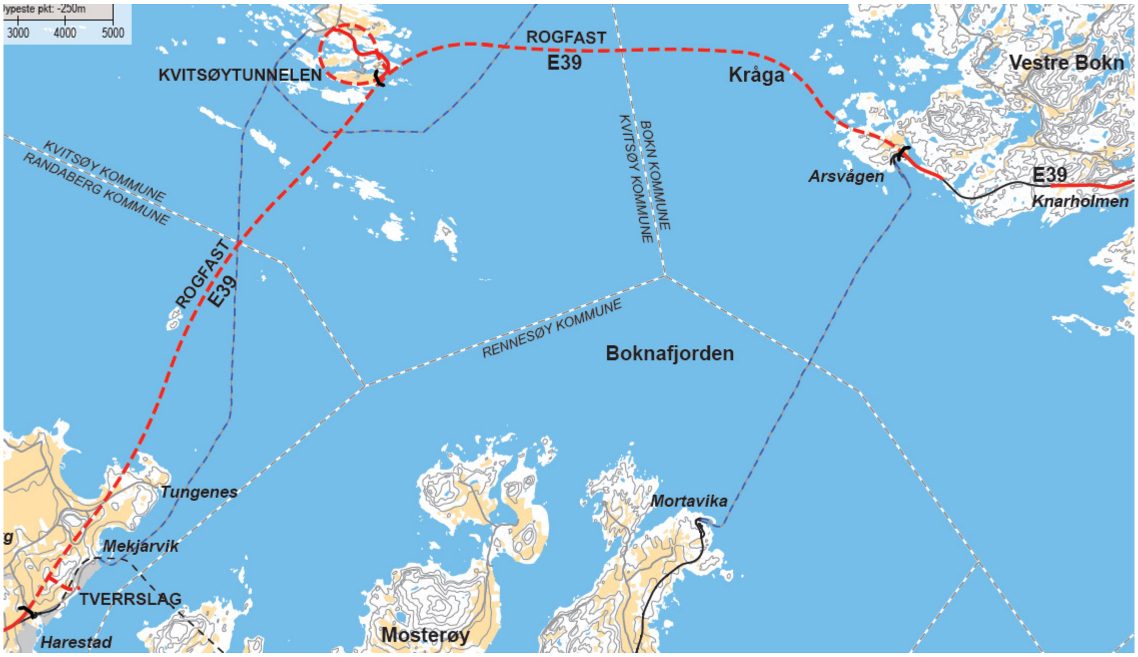

Fig. 1 The Rogfast route from Randaberg (Harestad) to Bokn (Arsvågen) with an arm to Kvitsøy

In this paper we review and discuss the findings from the risk assessments in the Rogfast project. Our starting point is that the regulatory framework/system has limited experience with handling projects of this size and complexity. We question whether the existing regulatory framework is appropriate, or whether there is a need for improvements. Our first part of the review focuses on the general risk assessment framework and methodology. Our hypothesis is that the regulative framework undermines the value of the risk assessments. Secondly, we are interested in the message contained in the risk assessment. When prescriptive regulations are insufficient as decision support with respect to safety and emergency response design, the risk assessment becomes an increasingly important document for both internal and external decision makers. However, it is easy to understand that a project of this size and complexity is associated with large uncertainties with respect to analyzing causes and consequences of accidents, regional development due to the tunnel, the impact of length, depth/gradient, intersection, smoke ventilation system and more. The second part of our review focuses on how the risk analysts manage to analyze and describe the broad picture of risk and uncertainties, and as such, manage to provide an informative tool for decision making. Our hypothesis is that, although uncertainties are recognized by the analysts, they are not adequately reflected in the risk assessments and descriptions. Hence they do not provide a proper basis for making decisions about tunnel safety design and emergency response.

The paper is structured as follows: in Section 2 we present our key findings from the review of the risk assessment process, and discuss the implications of our findings with respect to the risk assessment framework and methodology, and the informative message from the risk assessment. In Section 3 we provide a general discussion of our findings and suggest a solution for this and similar cases. Finally, in Section 4 we provide some conclusions.

2. REVIEW AND DISCUSSION OF THE ROGFAST SAFETY ASSESSMENT PROCESS

2.1 Regulatory Framework and Methodology

2.1.1 Regulating Safety in Norwegian Road Tunnels

Safety in Norwegian road tunnels has traditionally been governed by a prescriptive regulation regime, and it still is. Handbooks describe minimum safety requirements as a function of tunnel length and traffic load. In 2004 the European Parliament adopted the directive on minimum safety requirements for tunnels on the Trans-European Road Network (TERN) (EU, 2004). The aim of the directive was to improve and standardize tunnel safety on the TERN by specifying minimum safety requirements, measures and equipment. As a member of TERN, the directive was fully implemented in Norway. As such, the directive played an important part in the regulative changes that took place at the time of implementation. Now, however, the requirements from the directive are implemented in the national prescriptive regulations. This means that a deviation from the

Norwegian prescriptive regulations is a deviation from the European minimum requirements. Consequently, the European Commission is to be informed about cases where alternative risk reducing measures are introduced to justify deviations (EU, 2004).

The new minimum requirements were more stringent than earlier Norwegian requirements, and also different than Norwegian construction practice. For instance, emergency exits shall be provided where the traffic volume is higher than 2 000 vehicles per lane (EU, 2004:2.3.6), which has not previously been the practice in Norway. The Norwegian practice of using a longitudinal ventilation concept was also contested, and should now only be allowed on the basis of a risk assessment. But perhaps the largest discrepancy between the new directive and Norwegian road tunnel construction practice was with respect to longitudinal gradients. The directive states that a gradient above 5 % shall not be permitted in new tunnels. This is a requirement which makes Norwegian subsea fjord-crossing tunnels hard to realize without having to increase the length extensively. While there are examples of older subsea tunnels with a gradient of 12 %, Norwegian legislation now limit the gradient to 7 % (NPRA, 2012:3), which is also the maximum gradient in the Rogfast tunnel. Due to this discrepancy in construction practice, many of the tunnel projects since 2004 have required a risk assessment. In fact, it has been decided that a risk assessment shall be performed for all tunnels longer than 500 meters (NPRA, 2007b). The purpose of the risk assessments is twofold: 1) to found a basis for emergency preparedness plans, and 2) to "determine if it is necessary with additional safety measures and/or safety equipment to achieve the safety level required in handbook 021" (NPRA, 2010:48). It is interesting to notice that "the safety level of handbook 021" is the reference, the definition of safety, so to speak.

To be able to describe and discuss the risk regulating regime we have established a model of it, see **Fig 2**. It is showing a hierarchical safety regulation structure which depicts possible means of achieving compliance with safety regulations. The model is representing a regulation regime where the requirements in the regulation are stated in terms of safety goals and performance requirements. The model is separated into four levels: 1) the general tunnel safety regulations, which are common to all tunnels, 2) the design principles, 3) engineering analysis principles, and 4) evaluation principles.

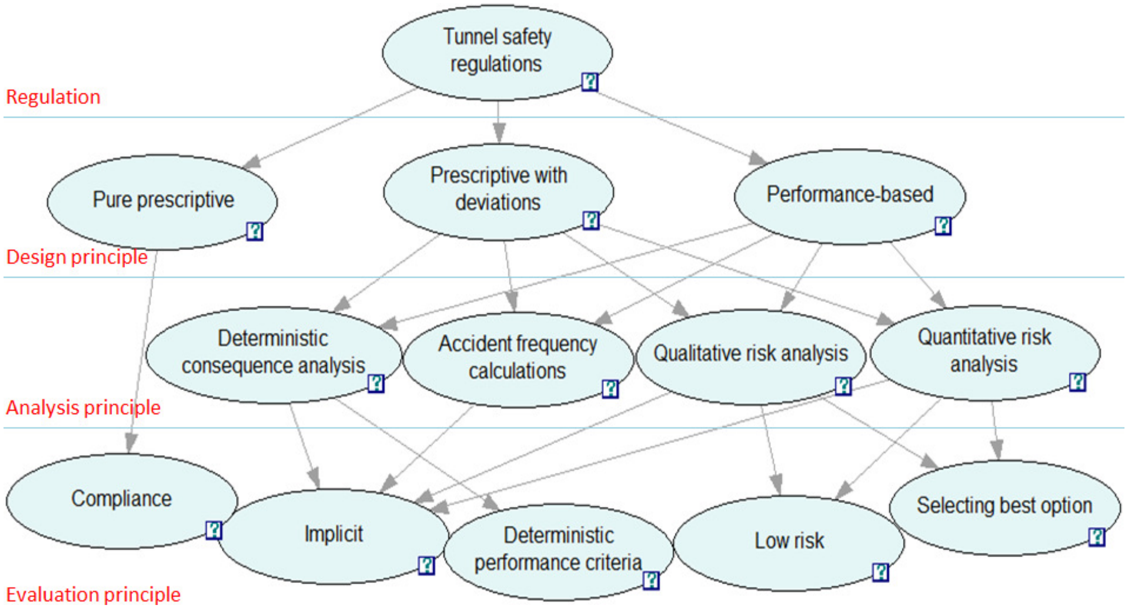

Fig. 2 Tunnel safety regulations and safety engineering principles to reach a decision on safety level

The *evaluation principle level* might need a more detailed description:

- The *compliance* principle includes checking the proposed design against prescriptive regulation requirements, which in the Norwegian tunneling industry implies handbooks, e.g. HB 021.
- The *implicit* principle includes comparing alternative designs against similar prescriptive designs. I.e. the safety measures might be different but the analysis methodology is similar. One is interested in checking whether the alternative design has an equivalent, or higher, level of safety than that of the prescriptive reference design. Thus, one uses the safety level which is implicitly stated by the prescriptive regulations as a reference for measuring the relative safety level of the alternative.

- The principle of using *deterministic performance criteria* includes comparing results from consequence analyses, e.g. fire and explosion simulations, against tolerability criteria such as temperature levels, toxic gas concentrations, explosion pressure levels, etc.
- The *low risk* principle includes the use of risk acceptance criteria (expressed by risk matrices, F-N curves or other metrics) to determine whether the presented risk level from the analysis is high or low. The ALARP principle, i.e. that risk should be *as low as reasonably practicable*, would also fall under this category.
- The *selecting the best option* principle is related to decision theory concepts, where the ideal is to select the decision alternative which is most useful and beneficial to the society. The decision alternative having the highest expected utility or benefit-cost ratio should be selected. Utilities, benefits and costs should be considered on a broad societal level.

What we find in the Norwegian road sector is that the tunnel safety regulations are prescriptive, and hence the top level of **Fig. 2** is non-existent. Neither is the "performance-based" design principle option. Consequently, there is generally no separation between the *concept of safety* and the *means to achieve safety* within the Norwegian road sector regulation regime. The regulations do, however, allow for alternative designs which deviates from the prescriptive regulations, as long as it can be demonstrated that the alternative design has an equivalent, or higher, safety level than a prescriptive design. Using the model in **Fig. 2** we could say that the safety issues in the Rogfast project has been treated using a design/regulation principle of prescriptive solutions with deviations. To analyze the consequences of the deviations accident frequency calculations, qualitative risk analyses and deterministic scenario analysis have been conducted. The results from the analyses are evaluated using the *implicit safety principle* and, to some extent, the *low risk principle*, by introducing risk matrices.

Handbooks and minimum requirements are important tools to achieve safety for the large mass of road tunnels and to enhance efficient and consistent planning and construction processes. However, when a project with the characteristics of Rogfast appears on the drawing board, it could be argued that such prescriptive handbooks have severe limitations. In fact, the main challenge of a prescriptive regulation regime is to handle innovative designs, which falls outside the scope of existing practice. Nonetheless, it could be argued that the safety issues of the Rogfast project are treated just like any other road tunnel project with respect to methodology within the regulatory framework. Two risk and vulnerability analyses (Norconsult, 2006; Sintef/Cowi, 2012) have been produced in accordance with the requirements in NPRA (2010) and the guideline for risk analysis in road tunnels (NPRA, 2007b). The risk and vulnerability analyses could be separated into the following main parts, which also constitutes the three obligatorily analysis parts in the regulation's guidelines:

- Calculation of accident and fire frequencies with the "TUSI" model. TUSI is a model which uses statistical data from existing roads and road tunnels to predict future accident and fire frequencies (NPRA, 2007b). Both works include TUSI calculations.
- Coarse qualitative risk analysis of a set of specified unwanted events. Both analyses include a qualitative analysis.
- Quantitative risk analysis of a set of fire scenarios. Only the latest analysis includes such an analysis.

In the following we will discuss the regulation-required analyses in relation to their applications and limitations in the Rogfast project. The discussion is here related to the rationale of the Norwegian regulative framework. We will come back to the content and information value, in terms of how risk is presented, of the analyses in section 2.2.

2.1.2 TUSI calculations: accident frequencies

The use of the TUSI model is required in every project which includes a road tunnel longer than 500 m. Accident and fire frequencies are calculated on the basis of accident statistics on existing roads and road tunnels. It is possible to take into account variables like speed limit, gradient, length, the number of tubes, etc. (NPRA, 2007b).

Describing uncertainty, often through probabilities, or expected values over a certain time period (frequencies), is an important part of a quantitative risk analysis. In some cases, probability models could be used to predict future occurrences of accidents, while in other cases a physical model, like an event tree or fault tree, could be employed. TUSI is an example of the latter: a physical model which describes causal relationship between certain characteristics of the tunnel, and quantifies them by the use of statistics. In any case, whether you choose a probability model or a physical model, the analyst must justify the application, i.e. show that the model is appropriate to describe what it is supposed to describe. We argue that the relevancy of this model in the Rogfast project and hence the purpose of its application can be challenged.

It could be questioned whether it is reasonable of the Norwegian Public Road Authorities (NPRA) to require a TUSI calculation in every road tunnel project on a general basis. However, to require such calculations in the Rogfast project seems meaningless, as the model is outside its scope of application. The statistics on which it is based do not include any tunnel which resembles the Rogfast. Nonetheless, the model has been required and applied, and the results are important premises for the risk assessments. Although the latest risk analysis (Sintef/Cowi, 2012) discusses the appropriateness of using the TUSI model, it places more emphasis on justifying its results, than on analyzing and describing the uncertainty associated with accidents that might occur in the future. This is not to say that TUSI calculations could not provide useful information to the analysts, also in the Rogfast project. The problem is related to the regulatory requirement of using this tool, which places too much weight on this specific tool and on the frequencies that it provides.

2.1.3 Coarse qualitative risk analysis

A thorough and systematic qualitative analysis is generally considered an important part of a risk assessment. Common practice in the Norwegian road sector is to carry out hazard identification (HAZID) processes, where possible threats to the system are identified along with their causes and consequences. The process is usually organized as seminars, where experts on different areas of the tunnel system, or emergency response system, are gathered to feed information into the analysis. The major trait of the methodology is associated with both the systematical process (often by the use of checklists) and the involvement of experts. Consequently, it should be possible to reveal specific safety problems to any new design. However, the quality of the results is mainly related to the knowledge of the group, and how the management of the process is able to reveal this knowledge.

What we find in the Rogfast project is that a standard set of unwanted events have been considered, and we find no documented attempt to identify any new threats. In fact, the threat of terror (intended events) has deliberately been omitted from the latest analysis, based on instructions from NPRA (Sintef/Cowi, 2012). In order to provide the broadest possible foundation for further analyses, creativity should be encouraged in the HAZID processes. The list of standard unwanted events in the guideline might limit creativity, but seems necessary to make sure that previous experiences are not overlooked in new analyses. Hence, it becomes the responsibility of the analysts to include the relevant competency in the HAZID processes and to document that a broad creative process has been conducted. We argue that this is lacking in the Rogfast project.

The Norconsult analysis mentions a team of reference, when discussing relevant unwanted events, but the competency of the team is not documented. The Sintef/Cowi analysis (2012) is based on an internal identification of unwanted events, and has therefore not included any knowledge from e.g. local emergency response services or tunnel operators. An information meeting with the emergency response services, where the results of the risk analysis were discussed, was organized in December 2011, shortly before the analysis was published.

The apparent lack of both a systematic procedure and involvement from external experts and stakeholders, when conducting the qualitative risk analysis, is an obvious weakness of the process. However, in this case it could be argued that the weakness is related to the implementation of the analyses, not the regulatory framework.

2.1.4 Quantitative risk analysis

In accordance with the guidelines for risk analysis of road tunnels, the level of detail of the analysis should increase as a function of tunnel complexity (NPRA, 2007b). For subsea tunnels and tunnels with ramps and intersections inside the tunnel, a detailed risk analysis should always be carried out. In less complex cases, a coarse risk assessment might be sufficient. The risk assessment carried out in 2012 (Sintef/Cowi, 2012) was supposed to increase the level of detail from the first analysis (Norconsult, 2006) and thus comply with the requirements from NPRA (2007b).

The guidelines on detailed risk analysis from the NPRA are not strictly defined but allow the analysts to plan and execute the analysis as it is found appropriate. In the Rogfast project it has been decided to conduct a detailed risk analysis of some specific fire events, on the basis that these events were considered to represent high risks in the coarse qualitative risk analysis. Hence, the quantitative risk analysis does not present an overall picture of risk in the Rogfast tunnel. However, our major concern at this stage is related to the combined methodology of risk analysis principle and evaluation principle (see **Fig. 2**).

To evaluate the risk, the NPRA has instructed the analysts to compare the Rogfast tunnel with a pre-accepted reference tunnel, designed in accordance with HB 021 (Sintef/Cowi, 2012). This is a common approach in the road sector, as one of the two purposes of a risk analysis is to consider whether the safety level of HB 021 is fulfilled. The approach is founded on the premise that there are no nationally quantified risk acceptance criteria, so the implicit safety levels of the pre-accepted designs are being used instead. In most cases it is possible to imagine a pre-accepted version of the road tunnel to be designed. There might be some small deviations regarding for instance the distance to an emergency exit, or the use of a slightly different geometrical tunnel profile. In these cases it is relatively straightforward to analyze the consequences of the deviations, and conclude what additional safety measures are needed to level out the differences. In these cases it might not be that important to provide a detailed description of risk, as long as the necessary factors for the comparison are considered. However, we see that the concept of safety in this approach is closely related to the validity of the prescribed reference design, and how the consequences of the differences between the designs are represented by the analysis methodologies.

In the Rogfast case it is not possible to imagine a design in accordance with HB 021, and this makes it problematic to introduce a reference tunnel. It could be argued that any tunnel designed in accordance with HB 021 has an acceptable risk level, and thus should be an appropriate reference tunnel. However, if this was so, the risk of the reference tunnel would have to be analyzed and described on a detailed level, incorporating every relevant causal factor for accidents and associated consequences. This could have formed the basis for adopting the *low risk evaluation principle* according to **Fig. 2.** Such detailed analyses have not been conducted for the reference tunnel in the Rogfast project. Simplifications in the analyses are justified by choosing an evaluation strategy based on the *implicit safety principle*. As argued above, this increase the importance of selecting a valid reference for the comparison, as one deliberately excludes knowledge from the analyses which one would have included using a different evaluation principle.

The reference tunnel, which is chosen for the comparison, is 10 km and has an average annual daily traffic (AADT) of 50 000 vehicles per day. Since both the frequency of accidents and fires, and the number of exposed persons, is largely dependent on AADT within the common models used to calculate risk, it comes as no surprise that the reference tunnel has a higher risk, measured as the expected number of fatalities. As such, much work is carried out to justify that the Rogfast has a lower risk than a thought-constructed reference tunnel, which we, based on the premises for the comparison, knew before we started.

Would it not be better if the risk analysis focused only on the Rogfast, and the specific threats of this tunnel? Should it be necessary to introduce highly discussable reference tunnels to make decisions about safety? In cases where we are faced with unique designs, like the Rogfast, we find it problematic to base decisions on risk on comparisons with pre-accepted designs. There is no support for the assumption that the new design will behave in an equivalent way to the reference design. The prescriptive regulatory framework may entail a too strong connection between the concept of safety and the solutions to provide safety, i.e. confusion about means and ends. This becomes especially evident when we look at novel designs and there are no overall safety goals or performance requirements to obtain from the regulations. This forces the analysts to choose a design process which is far from optimal if one wants to reap the benefits of a risk-informed approach to design.

2.2 The presented picture of risk

To form a proper basis for decision making about safety, a risk assessment should provide a broad and complete picture of the risks. Our concern here is whether the Rogfast risk assessments manage to do so. We have chosen to focus on:

1. uncertainties related to input variables;
2. uncertainties related to novel designs, and;
3. uncertainties reflected by the presentation of risk.

The three different aspects of uncertainty are discussed in the following sub-sections. The examples from the risk assessment are not exhaustive, and merely have the purpose of illustrating our point.

To illustrate uncertainties related to input variables we take a look at the purpose of the tunnel and the possible regional consequences of the project, which mainly affect two important factors in the risk assessment: AADT and fraction and characteristics of heavy goods vehicles (HGV). While we know that there are great uncertainties associated with these factors, they are treated as constants in the risk assessments. The numbers are inputs from NPRA, and are not critically reviewed in the risk assessment process. Uncertainties related to novel designs are illustrated by the emphasis which is put on the vertical gradient, or lack thereof. We aim to show that the selection of analysis method and evaluation strategy has consequences in terms of excluding possibly important knowledge from the assessment. Finally, uncertainties reflected by the presentation of risk are illustrated by the focus the analysts have placed on vulnerabilities, averages and expected values.

2.2.1 Uncertainties related to input variables

The Rogfast will serve as an important connection for the flow of goods from Kristiansand to Trondheim, and regionally. When it is finished it will shorten the travel time across the Bokn fjord significantly. More precisely, it will involve areas on the north side of the fjord having less than one hour travel distance to Stavanger, which is not the case today. Consequently, it could be expected that the Stavanger area, which still experiences large economic growth due to the oil and gas industry, will attract a growing number of workers from the north side of the fjord. This could lead to a large growth in traffic across the fjord, both in private cars and public transportation.

Recent experience with traffic forecasts in Norway shows that they underestimate future traffic volumes considerably (Hultgren and Bentzrød, 2012). Separate traffic forecasts have been conducted in the Rogfast project (NPRA, 2007a). We find that the traffic analysts describe the use of a "fresh model", having large uncertainties, and which is not yet fully calibrated against the traffic in the area. The analysis describes a maximum AADT-number of 10 400 vehicles in 2014, in the case without a toll charge (NPRA, 2007a). Since the AADT is important information for the risk assessments, it could be argued that the uncertainties from the traffic analyses should have been pursued further, as a part of the risk assessment. However, such uncertainty analysis has not been conducted. An AADT-number of 13 000 vehicles, 20 years after opening, have been used in the risk assessment, based on input from NPRA (Sintef/Cowi, 2012). We are not in a position to question the actual numbers in the assessments, but it seems reasonable to question whether the numbers used reflect all available knowledge about future traffic volumes. For instance, what future scenarios are reflected by the AADT numbers? What will happen if the Norwegian oil and gas industry continues its growth, or the opposite: takes a blow and is moved abroad?

Heavy goods and dangerous goods transportation is closely connected to the needs of the industry in the region. Therefore it should be possible to estimate what kind of dangerous goods, and in what quantities, are expected, in the Rogfast under different future scenarios. However, we find that heavy goods transport is treated as a fraction of the AADT, and dangerous goods are superficially treated in the qualitative risk assessment. To compensate for this, a sensitivity study has been conducted for both the variables *AADT* and *fraction of HGVs*. AADT has been raised from 13 000 to 17 000, and the fraction of HGVs has been set to 25 % instead of 15 %. This raises the fire frequency by 45 % (Sintef/Cowi, 2012:125), which the analysts consider to be substantially. However, the message from these calculations is unclear: We are presented with numbers that imply that AADT and fraction of HGVs greatly affect risk, but since risk is only assessed relative to a reference tunnel, it is hard to see how the sensitivity study can lead to any change of the conclusion that risk is acceptable. It could be argued that the uncertainties associated with these assumptions are recognized, but neglected. In summary, we find that AADT, the number of heavy goods vehicles and dangerous goods transportations, is treated generically, where it is hard to see the specifics of the Rogfast tunnel and the way this tunnel will affect the region. Furthermore, the AADT is an annual average daily traffic. Maybe focus should have been directed to a greater extent at the traffic volume in general at different time and/or operative conditions.

2.2.2 Uncertainties related to novel designs

Another issue is the uncertainty associated with the uniqueness of the Rogfast. As mentioned above, this uncertainty has led to discussions on the appropriateness of standards and common procedures. Risk assessments are a common tool to deal with the uncertainties of new and unique designs, and, when it is decided to conduct risk assessments, it could be expected that the consequences of the uniqueness of the tunnel will be considered.

Although the Rogfast tunnel looks like a standard two- tube road tunnel, only longer, the significance of its long descent and ascent could be questioned. After a serious fire in the Oslofjord tunnel (SHT, 2012), which has a gradient of 7 % over 3.5 km, in 2011, it was closed to heavy goods vehicles for nearly a year afterwards, due to recognition of the serious challenges such vehicles experience in long steep tunnels (NPRA, 2012). When driving towards north, the Rogfast will have a 7 km steep ascent, from the lowest point, at – 392 m, to the portal in Arsvågen. The gradient in the ascent will be 5 % the first 3.5 km, and then increase to 7 % the last 3.5 km, i.e. a considerably longer stretch than that of the Oslofjord tunnel. Furthermore, the risk assessment has questioned the efficiency of the ventilation system in this complex tunnel, especially in the event of a fire. Taking into account that Norway accepts heavier trailers than the rest of Europe, heavier than the standards against which brake systems are tested, and that malfunctioning brakes are common on heavy goods vehicles (NPRA, 2012), it should be expected that this issue would be extensively treated in the risk assessment. However, we find that the topic is only remotely treated when estimating the fire frequency using TUSI. Since the quantitative analysis has been conducted comparatively with a reference tunnel, the specifics of the Rogfast tunnel are toned down. One could say that the knowledge is excluded based on the assumption that it will behave as the reference tunnel, and that the reference tunnel do not have any problems with respect to vertical gradients. These might not be valid assumptions.

It is concluded that the fire frequency of the Rogfast is close to equal with that of the reference tunnel (Sintef/Cowi, 2012). The length of the Rogfast is compensated by a high AADT in the reference tunnel, while the maximum gradient is the same. However, the distance of the descent and ascent is not the same, and the impact of this deviation is at the core of the question the decision makers need to consider. Will the geometrical layout of the Rogfast cause problems in the operation of the tunnel, causing a large number of fires in brakes and engines of heavy goods vehicles, and accidents due to large speed differences in descents and ascents?

We find it hard to answer these questions on the basis of the risk assessments. However, a newly published document from the NPRA states that gradients of 7 % should not exceed a distance of maximum 1.5 km in new road tunnels (NPRA, 2012:19). We notice that there is a different conclusion in the Rogfast risk assessment, where the risk is considered acceptable.

2.2.3 Uncertainties reflected in the presentation of risk

Finally, the fire assessment is a substantial part of the 2012 risk assessment (Sintef/Cowi, 2012). The analysts have made two decisions that have a large effect on the information value of the fire assessment: 1) the assessment is a comparison with the reference tunnel, and 2) results are presented as the expected number of fatalities, given a fire scenario. Since we have discussed the use of comparative analyses in previous sections, and on a general basis in a separate paper (Bjelland and Borg, 2013), we will focus on the use of expected values in the presentation of risk.

The fire assessment builds on the use of a set of scenarios describing location in the tunnel, traffic load at the time of the fire and the heat release rate of the fire. The probability of an initiating fire in the tunnel is calculated by the TUSI model as an annual frequency. As such, the probability of fire is interpreted as the fraction of time a fire incident is present in the Rogfast tunnel in the long run, when considering an infinite number of operative years of the Rogfast, or similar tunnel systems. Since we do not have operative experience with the Rogfast tunnel, the reference must be similar tunnels. However, as mentioned earlier, when discussing the TUSI model, there are not any similar tunnels, unless the definition of similar is interpreted quite loosely. Our point is that the use of relative fire frequencies, in this case, is hard to justify without having to introduce thought-constructed populations of similar systems. We will point to a more suitable alternative in Section 3, since the interpretation of the presented probabilities is important when a decision maker reviews the results of the analysis (Aven, 2013). In the Rogfast case, however, the fire frequencies are just mentioned, but not used any further. It is concluded that the fire frequencies of Rogfast are in the same magnitude as for the reference tunnel, and the expected consequences, given a set of fire scenarios, are compared. Consequently, it would be wrong to say that the results are a presentation of risk, unless a very narrow perspective on risk is adopted; see discussion in Section 3. Rather, the expected value is to be considered a measure of vulnerability, given a fire. Subscribing to the view that risk would be an appropriate measure to describe the presence of safety, or lack thereof, in this case, we find it unfortunate that the analysis and presentation of results is restricted to vulnerability numbers.

Firstly, it is not possible to identify the likelihood of the consequences of a given fire scenario. For instance, it is calculated that in the case of a 300 MW fire near the Harestad portal with a normal traffic load, the expected number of fatalities will be 9.7 persons if a bus is present in the accident's influence area. If the same fire occurs at the lowest point of the tunnel, when the traffic load is high, the expected number of fatalities will increase to 34.3 persons. At most, an expected number of fatalities of 250.3 persons is calculated, assuming that the ventilation system fails during a 300 MW fire. Our question is then: how should a decision maker deal with the message that 250 people are expected to die in an accident in the tunnel, when the associated uncertainties are not presented? The decision maker is provided with the additional information that the reference tunnel, to which the Rogfast is compared, will have an expected number of fatalities of 483 persons for the same scenario, but does that really improve the situation? Intuitively it sounds like both tunnels have an unacceptable risk, and the society should be spared from the existence of them both. However, the risk of the Rogfast is judged acceptable by the analysts without any additional safety measures, besides standard requirements from NPRA's HB 021 (NPRA, 2010). Consequently, it would confuse the decision maker when an extensive list of costly additional safety measures are evaluated and recommended by the risk analysts, for instance: reducing the distance between emergency exits from 250 m to 125 m, creating four large cavities to reduce monotony while driving through the tunnel and introducing a number of drivable crosscuts between the tubes (Sintef/Cowi, 2012). It is difficult to see the link between the descriptions of risk and the recommendations provided by the analysts.

Secondly, it could be questioned whether the use of expected values provides the decision makers with a broad and complete picture of the risks. The risk assessment is an important tool in emergency preparedness planning, and in order to dimension the emergency response services in the region appropriately, a broad picture of risks is needed. The emergency services are especially needed when the accidents develop further than expected. Scenarios not captured by the use of expected values are very interesting and relevant in this respect. This also applies the other way around: emergency response services should be incorporated into the risk assessments in order to develop performance requirements and possible weaknesses of the present system. A possible scenario is the transportation of a large number of commuters across the fjord every day. Is it not possible that the buses in this case will be quite full, and that there are several buses traveling at the same time in rush hours? Hundreds of bus passengers might be exposed to a fire in such a case. Should not the risk assessment enlighten this situation, making the decision makers aware of the possibility and providing some guidance on how to manage this risk? In our opinion this is not properly reflected when the risk assessment is limited to expected values and averages. Some examples are: the average number of bus passengers is 20 persons, the average number of people in cars is 1.5, and the location of the bus, relative to emergency exits, is considered "average" (Sintef/Cowi, 2012).

3. DISCUSSION AND PROPOSAL FOR IMPROVEMENTS

In the following we will discuss the implications of our findings from the previous section with respect to the appropriateness of using risk assessments as decision support in large road tunnel projects. As indicated in the introduction and Section 2, we have separated our review and discussion into the two topics: *regulative framework/methodology* and *presentation of the risk*.

If risk assessments are going to be an important and influential tool in decision-making in safety issues, and function as decision support for novel designs, which is the goal of both EU (2004) and the NPRA (2007b, 2010), we argue that there is a need for a change in the regulatory framework. The change we are proposing is basically to separate between the *concept of safety* and the *means to obtain safety*. This is necessary to enhance risk-based thinking, which under the present regulation regime is restricted by a too narrow understanding of safety. Such a change implies a transition from a prescriptive to a performance-based regulation regime, where the concept of safety is defined by a set of safety goals and performance requirements, which pay due attention to the technical, organizational and human factors that interact in order to obtain safety (see e.g. Hopkins and Hale, 2002; Leveson, 2011; Reason, 1997).

The changes we are proposing in the regulatory regime seem necessary to prioritize in order to create a functional framework for risk-based thinking, which seems to be the goal of the European and national authorities. The changes we are proposing with respect to the assessments and presentations of risk are in line with the way we understand the concept of risk. We acknowledge that there are different views on how to understand risk in the academic environment and amongst practitioners, as well as different views on how important uncertainties are with respect to decision-making processes. However, we claim that our understanding of risk is based on a sound scientific foundation and provides meaningful interpretations of otherwise narrowly understood concepts (see also Aven, 2010a; Aven, 2011). The change we are proposing is related to focusing on prediction of observable events and consequences, and description of uncertainties. The uncertainties are related to our lack of knowledge about whether these events and consequences will occur, and not to the deviation between estimates and true values of thought-constructed parameters of probability distributions which is the dominating view (Aven, 2003). This should lead to increased focus on the background knowledge on which the risk assessments are conditional on, and on what constitute good knowledge in order to solve the decision-problems created by the safety goals and the alternative design solutions. The change is in order to obtain a broader foundation for decision-making and a meaningful interpretation of the concepts involved. We argue that this does not necessarily using more resources on risk assessment, but using the resources somewhat differently.

3.1 Regulative framework/methodology: the problem-solving strategy

In the introduction we claimed that the regulative framework undermines the value of the risk assessment in this case. We find that the risk assessment is conducted in accordance with standard guidelines from the NPRA, adopting common models (e.g. the TUSI model) and methodologies (e.g. the coarse qualitative risk analysis). Furthermore, a fire risk assessment has been conducted for the Rogfast tunnel and a pre-accepted reference tunnel. This latter assessment represents a mixture of both analysis and risk evaluation, where only the differences between the tunnels are considered. This builds on the assumption that the reference tunnel has an acceptably low risk, and if the Rogfast has lower, or equal, risk, it should be considered safe enough. This methodology is common in road tunnel risk assessment and in other sectors (Bjelland and Borg, 2013; Bjelland

and Njå, 2012). A major problem with this methodology is that it is difficult to apply when we face new risks, i.e. risks that are not managed by the safety measures provided by the standards. This is due to the fact that the concept of safety is closely related to the means of achieving safety. When one operates outside the scope of the prescriptive regulations, one does not have any objective safety goals or performance criteria to evaluate ones design against. Considering that the Rogfast will be the longest and deepest road tunnel in the world, it could be questioned whether it is appropriate to conduct a comparative analysis. Should it not be possible to analyze risk and make decisions based on the risk analyses without a reference to a pre-accepted tunnel?

Funtowicz and Ravetz have developed a model for classifying problem-solving strategies based on the two dimensions (i) decision stakes, and (ii) system uncertainties (Funtowicz and Ravetz, 1993). The model states that in the case of low decision stakes and low system uncertainties, the *applied science perspective* is appropriate to deal with problem-solving. This could be in the case of planning and construction of standard road tunnels, where both the consequence dimension (decision stakes) and the uncertainty dimension are well understood. On the other hand, when the decision stakes and the system uncertainties are high, the *postnormal science perspective* should apply for problem-solving. Climate change has been provided as an example where this perspective is appropriate (Aven, 2012; Funtowicz and Ravetz, 1993). Between these extremes we find the *professional consultancy perspective*, which applies when either decision stakes or system uncertainties are high, or both are on a “medium” level (Funtowicz and Ravetz, 1993).

Using this terminology, it could be argued that problem-solving with respect to risk assessments in the Rogfast project has been in accordance with the applied science perspective. However, the characteristics of the tunnel, and questions from external stakeholders with respect to problem-solving strategies, could be taken as arguments that a different, more comprehensive, problem-solving strategy should have been selected. Our view is that we should be careful of adopting the standard (applied science) problem-solving strategy, when we face unique design challenges. However, we subscribe to the view that risk assessments have the potential of being valuable decision support in such situations, provided that a broad description of risk is provided.

In order for risk assessments to be a valuable tool in decision making in the Rogfast project or similar projects, we argue that the regulative framework should separate between the concept of safety and the means to achieve safety. This would ideally imply the introduction of a performance-based regulation regime, where the society’s safety goals and performance requirements are stated in the regulations. Another approach would be to require that project-specific safety goals and performance requirements are developed in the case of novel designs. How to achieve these goals would be a matter of choice between prescriptive solutions, when available, and a performance-based approach (see **Fig. 2**). This would open all the possible ways of conducting risk analysis and risk evaluation illustrated in **Fig. 2**. The safety goals and related performance requirements should cover all the issues which are relevant for the design of the tunnels and could, for instance, include the following:

- Life safety goals for tunnel users, maintenance personnel and rescue personnel.
- Life safety goals for 3rd parties, e.g. persons which are located in the proximity of the tunnels.
- Material/economic safety goals, e.g. related to replacements of structural elements and/or safety equipment, the time necessary to resume operation after accidents etc.
- Environmental safety goals, e.g. related to spill of toxic substances, handling of contaminated ventilation air etc.

It is important to emphasize that decision making about final design, and thus acceptability of risk, is outside the mandate of the risk analysts. The analysts’ task would end after evaluating the level of risk against the criteria specified by the evaluation principle chosen. Decision making about acceptability is the task of the project management, who is in a position to see the results of the risk assessments in association with other project goals and also reflect the limitations of the tools used. Consequently, a new regulative framework should include requirements to the risk management process, including, for instance, which stakeholders who should be included, and when, to allow for making decisions about risk. The structure of a proposed decision-making structure is presented in **Fig. 3**.

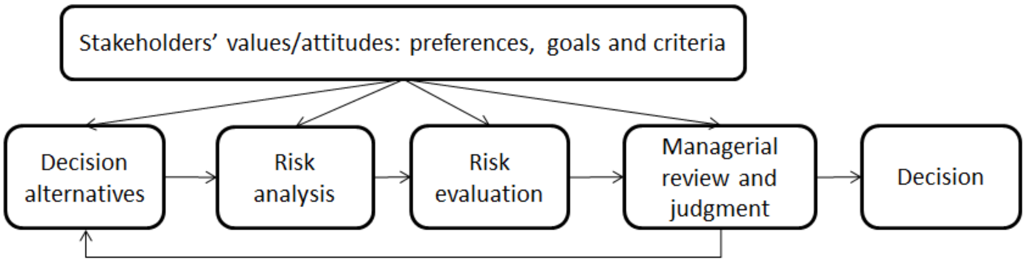

Fig. 3 Basic structure of the decision-making structure, adopted from Aven (2003:98)

3.2 Presentation of the risk

3.2.1 A framework for risk assessments focusing on describing uncertainty

The Rogfast risk assessments lack a proper risk framework, which we have attributed to both the regulative framework (standardized methodology) and the analysts' perspective of risk. The risk assessments do not provide a broad picture of the risks, as the presentation is fragmented by the use of semi-quantitative risk matrices and quantified expected losses, relative to a reference tunnel for some specific fire scenarios. We have argued that this risk description is not adequate if information about risk is to be a valuable contribution to decision making about safety in design and operation of the Rogfast and similar projects.

We recommend an approach based on a perspective where risk is described by specific events A', specific consequences C' of these events, knowledge-based probabilities P of A' and C', and K, the background knowledge that these probabilities are based on. Formally this description can be viewed as a risk description in a risk framework where risk is defined as the two dimensional combination of events/consequences, A/C, and associated uncertainties, U (Aven, 2010b). See **Table 1**.

Table 1 Illustration of the separation between risk concept and risk descriptions

Risk concept	Risk description
[A, C, U]	[A', C', P(A',C'|K), K]

The risk assessment process could be separated into the following steps (Aven, 2011):

1. Identify possible future events A' and associated consequences C'. A model G could be used to describe C'. In such cases the model G links a set of input quantities X to the quantities of interest C'. C' could for instance be the number of fatalities during a specific period of time, and $C' = G(X)$.
2. Describe uncertainty associated with A' and C' by the use of knowledge-based (subjective, judgmental) probabilities P(A',C'|K). If models are used, uncertainties are associated with the input quantities X, e.g. $P(X \leq x|K)$, which, by the use of the model G(X), leads to uncertainty descriptions of the quantity of interest, for instance $P(C' \leq z)$, the expected value EC', or the variance VarC'.
3. Assessment of uncertainty factors hidden in the background knowledge K, which extends beyond the knowledge-based probabilities. These could be related to quality of data or expert judgments and the significance of assumptions and suppositions.

Fig. 4 depicts a performance-based regulatory framework where safety goals and performance requirements are stated for the relevant safety objectives of the activity. Risk assessments are used to assess the safety performance of the activity, and this includes identifying, for instance, accident scenarios, contexts and situations in which certain scenarios can occur, human response and tolerability to accident loads and performance of rescue operations. Although safety goals are stated towards individual objectives, the risk assessment process has a holistic perspective. It is necessary to see beyond the separate areas. For example, environmental safety might have an impact on life safety as well. This is shown by the double arrows between the different topics treated in the risk assessment in **Fig. 4**. These factors and associated uncertainties are to be described using the risk assessment framework, to establish a foundation for decision-making about tunnel safety.

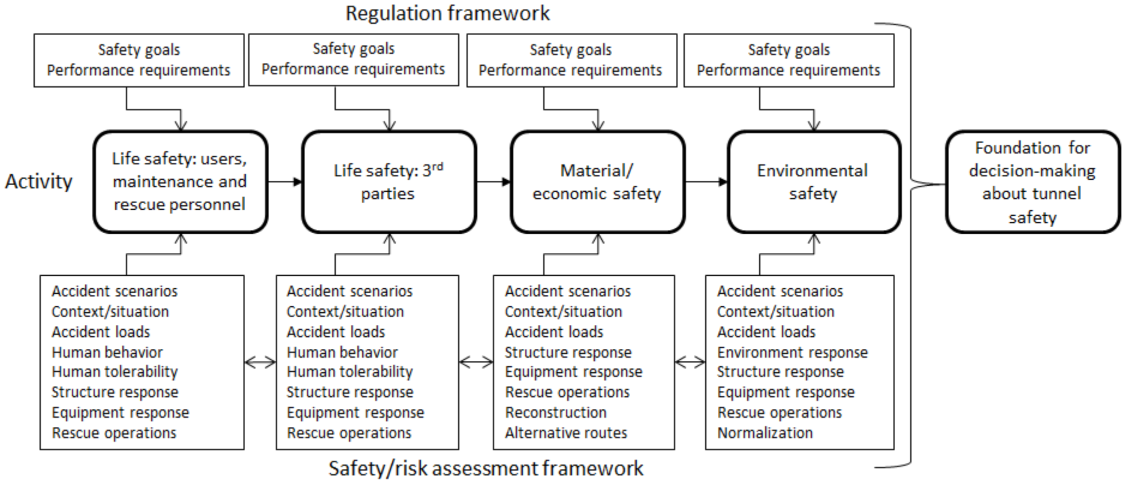

Fig. 4 Relationship between regulatory framework and safety/risk assessment framework

Following this approach, a risk assessment has the purpose of predicting future consequences and describing uncertainties. The uncertainty we are describing here is our lack of knowledge, i.e. epistemological uncertainties (Aven, 2011), about the unknown quantities, for instance the number of fires in HGVs, the number of injuries or fatalities in the case of accidents, or the performance of the ventilation system in the case of a fire. The challenge is to use the knowledge available today to predict the future consequences of the activity. This knowledge base includes all the information an analyst takes into account when measuring and describing uncertainty, for instance models (probability, physical, structural/causational), empirical data, expert judgments, and personal experiences/education. In the following we will discuss the importance of describing the background knowledge, the use of knowledge-based probabilities as a tool to describe uncertainties and uncertainties in assumptions.

3.2.2 The importance of describing the background knowledge

In our framework an uncertainty description cannot be separated from the background knowledge. An important part of the risk assessment is therefore to describe this background knowledge. As mentioned above, the uncertainties are due to our lack of knowledge. This implies that it is possible to improve predictions by increasing the background knowledge. This is important in a decision making context, because it implies that the risk assessment is not a definitive answer about risk. Other analysts, having different background knowledge, or weighing the importance of certain background knowledge differently, could come to different conclusions. Our review of the Rogfast risk assessment (Section 2) has led to the identification of a number of factors which are associated with great uncertainties. To illustrate the meaning of background knowledge, and how it could be treated within our framework, we consider the examples of AADT numbers and heavy/dangerous goods transport.

Estimation of AADT is not a part of the risk assessment, but has been conducted as an individual task in the impact assessment by the NPRA (2007a). The AADT number is very important in the risk assessment, as it is considered by the analysts as one of the main components in both the frequency of accidents and the number of exposed people in the case of an accident. According to NPRA (2007a) the estimations of AADT are associated with large uncertainties, as we pointed out in Section 2. Having acknowledged the importance of this factor, we use our risk assessment framework for an uncertainty analysis:

1. Identification of future scenarios, or events A', as a result of Rogfast. The scenarios would include factors which are important for the development of traffic volume. For instance, how will the housing market change and, whit it, the associated commuting pattern across the Bokn fjord? What future scenarios could we anticipate with respect to industry development or reduction? The oil and gas industry and the aluminum industry are important in Rogaland. How would changes in these industries affect traffic volume? Having such concrete scenarios in mind, it would be possible to estimate the associated number of people having to travel through the Rogfast on a daily basis.
2. Prioritize the set of future scenarios by ranking them in terms of likelihood. This could be conducted by the use of categories such as *low*, *medium* or *high*, or by the use of knowledge-based probabilities. The AADT number of 13 000, which is applied in the risk assessment, is surely a result of a thought-constructed

scenario. Other numbers are also possible, based on other scenarios, and we could obtain the traffic volume categories (say): (< 5 000, 5 000 – 10 000, 10 000 – 15 000, 15 000 – 20 000, > 20 000) with the associated probability distribution (0.10, 0.20, 0.40, 0.20, 0.10).

3. Assessment and description of the quality of the knowledge, i.e. informing the users of the risk assessment (the decision makers) about the foundation for the probability numbers or categories. A knowledge-based (subjective) probability distribution can be developed in any case. However, in some cases one could have a strong knowledge base, where appropriate models and data are available for prediction. In other cases, both models and data may be poor. Without the associated assessment of the knowledge base, the user of the risk assessment could be led to believe that the numbers are more precise than they really are.

Similar analyses could have been conducted for the number of heavy goods vehicles and the number of dangerous goods transportations. Identification of distributors and receivers of goods and dangerous substances could lead to a set of future scenarios, with an associated number, and type, of heavy and dangerous goods transportations. It could be argued that such an analysis should be a part of the risk assessment process associated with early design development, because it will affect what safety measures to include (especially pumps, drainage systems, buffer tanks, reservoirs, or the need for fire extinguishment equipment) and operative procedures.

3.2.3 The use of knowledge-based probabilities

When we try to measure risk we need a tool to describe uncertainty, and probability is the most obvious tool. In our approach the probabilities are knowledge-based (subjective, judgmental), and reflects the assessor's degree of uncertainty about A' and C', given K, P(A',C'|K). The background knowledge, discussed above, could be strong or poor.

In contrast with traditional frequency probabilities, there is no reference to a population of similar systems, where the probability of an event is considered as the relative fraction of time this event occurs in the long run when the activity is repeated. A frequency probability is considered a property of the system under consideration and the analysts provide estimates of this (true) probability in the risk assessments. The uncertainty descriptions in a frequentist framework are related to how close the estimate of the probability, P_f*(A',C') is to the real probability, P_f(A',C'). When a similar population of systems cannot be appropriately defined, it is hard to provide a meaningful interpretation of a frequentist probability (Aven, 2011).

Consider the uncertainty associated with fire in heavy goods vehicles (HGVs) in the Rogfast. An estimate of the fire frequency is provided, based on a TUSI-calculation. Uncertainty is related to how close this estimate is to the true frequency in a thought-constructed population of similar systems. The use of the TUSI model is discussed in the conducted study, and it is concluded that the model will yield appropriate estimates of the fire frequency (Sintef/Cowi, 2012). However, as we have pointed out in Section 2, the TUSI model cannot be justified in this case because it is built on statistical data from a population of systems with limited resemblance to the Rogfast. A major concern is related to this trust in an unjustified model, and to what degree it conceals real problems with the Rogfast design. For instance, there is no previous experience with a 5-7 % descent/ascent of length 7 km. This could lead to a great increase in the number of fires in HGVs, due to overheating in brakes and engines, compared with other Norwegian road tunnels. If knowledge-based probabilities had been introduced, the focus would also have been on the background knowledge K. Questions related to this K would be prompted: what do we know about fires in HGVs in long descents/ascents? How appropriate are the models (e.g. TUSI) we use today? Should we try to provide more knowledge before assigning a probability, or should we state that our knowledge base is poor?

When considering the reliability of the ventilation system, it seems like the analysts have assigned knowledge-based probabilities. There is no reference to a population of similar systems. Probability of failure for the ventilation system is assumed to be 0.02 (2 %) for the Rogfast system and 0.005 (0.5 %) for the reference tunnel (Sintef/Cowi, 2012:113). The probability assignment is based on a judgment that Rogfast is more complicated with respect to ventilation than the reference tunnel. However, we do not find a good assessment of the quality of K. We will argue that this probability alone does not provide a good basis for improving the system, or designing it according to relevant performance criteria. It is just assumed that the system is more complex at Rogfast, and thus should have a higher probability of failure. Causes and links are not investigated and described. It is stated that pessimistic values have been chosen because the ventilation system has not been analyzed (Sintef/Cowi, 2012:113). However, it sends a message that the subject should be treated comprehensively in a later stage of the project.

3.2.4 Uncertainties in assumptions

Probabilities are not a perfect tool to measure uncertainty. The probabilities are assigned on the basis of a set of assumptions, for instance about the behavior of people given a fire, the behavior of a heavy goods vehicle driver during the long descent in Rogfast, or the heating of the brakes or engines under certain loads. All risk analysts need to make assumptions. If an uncertainty analysis should be carried out for all possible variables, the risk assessments would be very time-consuming, and a large part of the work would probably not be relevant for the decision problem at hand. Consequently, there is a need to simplify, and assumptions are important in this regard.

The fire frequencies in the Rogfast case are estimated by the use of the TUSI-model. A knowledge-based probability could also be based on TUSI, as long as the model is justified. However, a probability assignment based purely on TUSI would imply several assumptions: the extraordinary length of the steep descent/ascent of Rogfast has no special impact on the likelihood of fire, the intersection does not affect the likelihood of fire, or the additional tunnel arm does not affect the likelihood of fire to any special degree. Under different assumptions, the TUSI-model might have been rejected, and other probability assignments would have been provided by the analysts.

Consider also the issue of predicting fatalities in the case of fire. The analysts assume a certain location of the fire, a certain fire growth, a certain maximum heat release rate, the effect of the ventilation system, the direction and speed of smoke spread, the number of vehicles near the fire, the location of the vehicles relative to the fire and emergency exits, the number of persons in a car or bus, the walking speed of the people in the tunnel, and the decision whether or not to use emergency exits. Due to the chosen comparative framework in the Rogfast case, it is implicitly argued by the analysts that the assumptions are not that important, as they would affect the reference tunnel equally. In our framework, these assumptions would greatly affect the assigned probabilities of specific consequences.

Assumptions which are critical to the results of the assessment and decision making should be subjected to uncertainty analysis. A sensitivity study would normally function as a basis for considering the criticality of the assumptions, by showing how different uncertain input values affect the results of the risk assessment. The sensitivity analysis of AADT and the fraction of HGVs in the Rogfast case (see Section 2) reveal that these variables have the potential to affect the result substantially. As a consequence, the uncertainty associated with these factors should have been investigated further, for instance in accordance with our proposed framework above.

4. CONCLUSION

In this paper we have reviewed and discussed the risk assessment of the Rogfast project. Our focus has been on the regulatory framework/methodology and the presentation of risk, and we argue that the risk assessment presents an unclear message to the decision makers and stakeholders. On the one side, they state that the Rogfast basis tunnel is considerably safer than the reference tunnel, and therefore should meet minimum requirements in the regulations. On the other side, they suggest extensive safety measures based on expert opinions, which do not seem to be supported by the risk analysis. This indicates that the risk assessment fails to reveal important aspects of uncertainty, which the analysts apparently are aware of.

Therefore, we argue that the type of risk assessment carried out does not provide a proper basis for making decisions about tunnel design and emergency preparedness. The presented risk picture is too narrow. Uncertainties in regional development, accident phenomena, accident consequences and effectiveness of safety measures are neglected. The type of risk assessment carried out needs to be replaced by broader assessments that pay due attention to such uncertainties, and a more suitable framework for how to assess and manage the risks and uncertainties of a large road tunnel project is discussed in Section 3. The framework is based on the broad definition that risk is the two-dimensional combination of consequences and associated uncertainties. When describing risk, focus should be on the background knowledge, which cannot be separated from the probability assignments. Furthermore, uncertainty in assumptions needs to be explored by conducting sensitivity studies, and if necessary by undertaking more thorough uncertainty analyses for the critical assumptions.

In order to realize the advantages of using risk assessments as decision support in novel design problems, when prescriptive requirements are not available, there is a need for a change in the regulatory framework. The major change is related to the need of separating the concept of safety and the means of obtaining safety. In other industries, this has been done by the introduction of performance-based regulations, which states safety goals and performance requirements instead of the required safety measures. This is necessary in order to reflect a holistic perspective on safety, which in addition to technical safety measures, also includes organizational and human factors.

Our review is made from an academic standpoint and in hindsight of the process thus far. We do not have to restrict ourselves to operating within the existing regulative framework and standards, nor do we need to only play the part of the analysts or comply with any mandate, customers' demands, tight time schedules and limited economic resources. The point we are making is that the reasons for the outcome of the risk assessment discussed in this paper, could be many. However, we are confident that the limited resources available in a construction project could be more efficiently used. This will require changes both with respect to the regulative framework and to the way risk is understood and assessed by the engineers/analysts.

Acknowledgements

During 2011 and 2012, the first author and a colleague had the opportunity to observe and participate in the Rogfast risk assessment process. Our gratitude goes to the Norwegian Public Road Authorities, and especially the project manager for making this possible, and the project's safety coordinator for support and valuable comments to the manuscript.

The insightful comments received from two anonymous reviewers to an earlier version of this paper are greatly appreciated. These comments led to an important process of clarifying our perspectives and arguments.

REFERENCES

Alsaker, B.M., 1997. "Rogfast" En Visjon?, Vegen vidare...? Når kjem fast forbindelse over Boknafjorden? (in Norwegian), Presentation manuscript by Bjørn Martin Alsaker, Norwegian Public Road Authorities Rogaland, at Rennfastkonferansen, 1997.
Amundsen, F.H., 1994. Studies of Driver Behaviour in Norwegian Road Tunnels. Tunnelling and Underground Space Technology 9, 9-15.
Aven, T., 2003. Foundations of risk analysis: a knowledge and decision-oriented perspective. Wiley, Chichester.
Aven, T., 2010a. Misconceptions of risk. Wiley, Chichester.
Aven, T., 2010b. On how to define, understand and describe risk. Reliability Engineering & System Safety 95, 623-631.
Aven, T., 2011. Quantitative risk assessment: the scientific platform. Cambridge University Press, Cambridge.
Aven, T., 2012. On Funtowicz and Ravetz's "Decision Stake—System Uncertainties" structure and recently developed risk perspectives. Article in press Risk Analysis.
Aven, T., 2013. How to define and interpret a probability in a risk and safety setting. Discussion paper Safety Science, with general introduction by Associate Editor, Genserik Reniers. Safety Science 51, 223-231.
Bjelland, H., Borg, A., 2013. On the use of scenario analysis in combination with prescriptive fire safety design requirements. Submitted for publication in Environment, Systems and Decisions.
Bjelland, H., Njå, O., 2012. Interpretation of Safety Margin in ASET/RSET Assessments in the Norwegian Building Industry, 11th International Probabilistic Safety Assessment and Management Conference (PSAM11) and The Annual European Safety and Reliability Conference (ESREL2012), Scandic Marina Congress Center, Helsinki, Finland.
Carvel, R.O., 2004. Fire Size in Tunnels, School of the Built Environment, Division of Civil Engineering. Heriot-Watt University, Edinburgh.
EU, 2004. Directive 2004/54/EC of the European Parliament and of the Council of 29 April 2004 on minimum safety requirements for tunnels in the Trans-European Road Network., The European Parliament and the Council of the European Union, Official Journal of the European Union.
Flø, M., Jenssen, G.D., 2007. Drivers' perception of long tunnels: Studies from the Quinling Shongnan Tunnel in China as well as the Lærdal tunnel and the world's longest sub sea tunnel (Rogfast) in Norway, 4th International Conference - Traffic and Safety in Road Tunnels, Hamburg.
Funtowicz, S.O., Ravetz, J.R., 1993. Science for the post-normal age. Futures 25, 739-755.
Hopkins, A., Hale, A., 2002. Issues in the Regulation of Safety: Setting the Scene, In: Kirwan, B., Hale, A., Hopkins, A. (Eds.), Changing Regulation - Controlling Risks in Society. Elsevier Science Ltd, Oxford, UK.
Hultgren, J., Bentzrød, S.B., 2012. Staten bommer grovt på veksten i trafikken (in Norwegian). Aftenposten.

Jenssen, G.D., Bjørkli, C., Flø, M., 2006. Vurderinger E39 Rogfast. Trygghet, monotoni, og sikkerhet i krisesituasjoner og ved normal ferdsel (in Norwegian). SINTEF Teknologi og Samfunn, Transportsikkerhet og -informatikk, Trondheim.

Leveson, N., 2011. Engineering a safer world : systems thinking applied to safety. The MIT Press, Cambridge, Mass.

Lönnermark, A., Ingason, H., 2006. Fire spread and flame length in large-scale tunnel fires. Fire Technology 42, 283-302.

Manca, D., Brambilla, S., 2011. A methodology based on the Analytic Hierarchy Process for the quantitative assessment of emergency preparedness and response in road tunnels. Transport Policy 18, 657-664.

Melvin, B., Gonzalez, J., 2009. Considering tunnel geometry when selecting a design fire heat release rate for road tunnel safety systems, 13th International Symposium on Aerodynamics and Ventilation of Vehicle Tunnels 1, New Brunswick, New Jersey, USA, pp. 225-236.

Nilsen, A.R., 2011. Contributions to fire safety design of tunnels. University of Stavanger, Stavanger.

Norconsult, 2006. Risiko- og Sårbarhetsanalyse (ROS) av Rogfast. Fase: Kommunedelplan (in Norwegian), Sandvika.

NPRA, 2007a. E39 Rogfast KU/kommunedelplaner: Trafikk- og nyttekostnadsanalyse (in Norwegian). Ressursavdelingen, Region Vest, Statens Vegvesen, Leikanger.

NPRA, 2007b. TS 2007:11 Veileder for risikoanalyser av vegtunneler (in Norwegian). Norwegian Public Road Authorities (NPRA), Oslo.

NPRA, 2010. Håndbok 021 Vegtunneler (in Norwegian). Norwegian Public Road Authorities (NPRA), Oslo.

NPRA, 2012. Etatsprogrammet Moderne vegtunneler 2008 - 2011. Grensesprengende tunneler - lange og dype, går det en grense? (in Norwegian). Trafikksikkerhet, miljø- og teknologiavdelingen, Statens Vegvesen Vegdirektoratet, Oslo.

Reason, J., 1997. Managing the Risks of Organizational Accidents. Ashgate.

SHT, 2012. Foreløpig rapport om brann i vogntog i Oslofjordtunnelen 23. juni 2011 (in Norwegian). Statens Havarikommisjon for Transport (SHT), Lillestrøm.

Sintef/Cowi, 2012. E-39 Rogfast. ROS Analyse, tunnel (in Norwegian), Trondheim.

van den Berg, A.C., Weerheijm, J., 2006. Blast phenomena in urban tunnel systems. Journal of Loss Prevention in the Process Industries 19, 598-603.

Vashitz, G., Shinar, D., Blum, Y., 2008. In-vehicle information systems to improve traffic safety in road tunnels. Transportation Research Part F: Traffic Psychology and Behaviour 11, 61-74.

Appendix B: Basis for AMF, indicators, zones and observable indicators

Table B1: Basis for AMF and indicators, from (Schubert et al., 2011).

Observable indicator	**Basis for priori distribution**	**Range of AMF values**	**Basis for assigning AMF value**
Time variation curve of the traffic*	Statistics for Switzerland and Germany mean value used for Norway.	Not included. Indicator provides an interface for further development of the model.	-
Number of lanes*	Switzerland: published data Norway: expert judgment	See traffic volume	See traffic volume
Traffic volume	Switzerland: traffic count 2007. Norway: published statistical data. NB: *Not used directly as traffic volume need to be known to perform analysis.*	1 – 2.60	Joint influence between number of lanes and traffic volume. Empirical correlation based on observation from Elbe tunnel in Hamburg.
Exit and entrance conditions	Not included	1 – 4.68 (41 states)	Expert judgment
Horizontal radius	Expert judgment	Joint influence with speed limit 1 – 5 Realistic range 1 - 3	Empirical correlation based on observations from selected tunnels.
Tunnel lighting	Expert judgment	0.59 – 1.60	Expert judgment
Lane width	Published data from tunnels in Switzerland.	0.85 -1.8 (9 states) Calculated empirically including speed limit	Expert judgment
Bi directional*	Statistical data	AMF unidirectional = 0.4 AMF bi-directional = 1.0	Expert judgment
Fraction of HGV	Based on data from Swiss Federal Statistical Office (FSO)	AMF = 0.427 * HGV (%) + 0.949 (21 states)	Empirical basis from observations (PIRAC and OECD)
Gradient	Published data from tunnels in Switzerland.	$\mathrm{AMF} = e^{0{,}081 * G-2}$ Fire frequency modification factor (implicitly included): $\mathrm{FMF} = 0.773 + 6.27 * 10^{-2} G^2$ ($G > 1\%$) $G \leq 1\% = 0.8358$	Expert judgment
Speed limit	Based on statistics from tunnels (including actual speed measurements).	Included in lane width and H- radius. Influence accident, injury and fatality rates	Increase in frequency based on models published by OECD

* It is possible to choose N/A, which means that no information regarding the indicator is available and a priori distribution is applied.

Table B2: Zones

Observable indicator for distribution of accident, injury and fatality rate*		
Number of zones	**Influence**	**Basis**
7	Zones influence the background rates in the tunnel	Statistics show variation along tunnel length. Method based on Amundsen and Ranes's (1997) 4-zone model, extended to 7 zones in TRANSIT.

*also influenced by speed limit.

Table B3: Observable indicators

Observable indicators for estimating number of fatalities and injuries due to fire*			
Indicator	**States**	**Influence and priori**	**Basis**
Monitoring system installed?	Yes – No, and N/A**	Influence consequence of tunnel fire and possibility for self-rescue. Priori assumption: installed in 50% of tunnel.	Based on assumptions. To be upgraded when models become available.
Ventilation system	9 types of ventilation systems included and N/A**	Influence the probability for successful escape through conditional probabilities. Priori distribution for type of ventilation system.	Based on expert judgment
Congestion	Congestion- no congestion, and N/A**	Influence the ventilation system and number of people affected. Priori: corresponds to 100 h/year Switzerland and 10 h/year Norway	Based on expert judgment
Emergency light	Yes - No	Influence probability of escape through conditional probabilities.	Based on expert judgment
Distance to the emergency exit	151 states based on distance to exit (0 to 1500m), and N/A**.	Influence the probability of escape.	Based on approach used in TUNprim (Vrouwenfelder et al., 2001) and (Weger et al., 2001).

*also influenced by time variation curve, traffic volume, bi directional traffic, fraction of HGV`s and gradient.

** N/A: Means that no information is available and a priori distribution for the states will be applied.

Appendix C: Transit input

Table C1: TRANSIT input

Seg. no.	Zone	Seg. start (m)	Length (m)	AADT (each direction)	Gradient (%)	Entrance/exit (state)	Emergency exits (m)
0	1	-50 (outside)	50	6500	-1.21	1	125
1	2	0	50	6500	-1.21	1	125
2	3	50	100	6500	-1.21	1	125
3	4	150	150	6500	-1.21	1	125
4	4	300	6200	6500	-5.15	1	125
5	4	6500	500	6500	0	1	125
6	4	7000	6500	6500	1	1	125
7	4	13500	300	6225	1	8	125
8	4	13800	300	6225	1	1	125
9	4	14100	300	6500	1	4	125
10	4	14400	2100	6500	-4.5	1	125
11	4	16500	2200	6500	-1.35	1	125
12	4	18700	3800	6500	5	1	125
13	4	22500	2800	6500	7	1	125
14	4	25300	50	6500	7	1	125
15	5	25350	100	6500	7	1	125
16	6	25450	50	6500	7	1	125
17	7	25500 (outside)	50	6500	2	1	125