NTNU

Norwegian University of
Science and Technology

Implementing IEC 61508 for Qualification of Safety-Instrumented Systems for Submergible Tube Bridges

Ole-Henrik Dag Olsen

Reliability, Availability, Maintainability and Safety (RAMS)
Submission date: June 2016
Supervisor: Mary Ann Lundteigen, IPK
Co-supervisor: Inger Lise Johansen, Statens Vegvesen
Anne Barros, IPK

Norwegian University of Science and Technology
Department of Production and Quality Engineering

Preface

This master's thesis is written during the spring semester of 2016 at the Norwegian University of Science and Technology (NTNU) within the field of Reliability, Availability, Maintainability, and Safety (RAMS) at the Department of Production and Quality Engineering. The thesis marks the final step of the five year master program in Mechanical Engineering. The thesis is written in cooperation with the Norwegian Public Road Administration (NPRA) regarding their project "Ferjefri E39".

The topic and objectives of this thesis was decided upon in cooperation with the NPRA. The thesis is mainly written for readers with basic knowledge of qualification of new technology and RAMS theory. However, the main topics are introduced in a manner that hopefully makes the thesis enjoyable for persons without any prior knowledge on these topics.

Trondheim, 2016-06-10

Ole-Henrik Dag Olsen

Acknowledgment

I would first of all thank my supervisors, Professor Mary Ann Lundteigen at Department of Production and Quality Engineering, and Inger Lise Johansen at the NPRA. I am extremely grateful for their intelligent and reflective inputs and feedback during this semester. When the work has been slow, or I have found myself in need of support, they have encouraged me and provided fresh insight to the problems.

I am also grateful for the opportunity given to me by the NPRA to partly write my thesis at their locations in Oslo. The oppurtinity made it possible to maintain a close connection to the NPRA during the writing of the report.

Finally I would like to thank my friends, family and SO for supporting me and making the master thesis period as enjoyable as possible.

O.H.D.O.

Summary and Conclusions

Qualification of new technology (or systems) has become an important discipline within application areas that have strict requirements to safety and/or reliability, and where new technology is not adequately covered by established rules, standards, and practices. With new solutions, which potentially affect a lot of people, it is important to reduce the uncertainty related to the development of the technology and document that the technology will have an acceptable performance during its lifecycle.

The Norwegian Public Road Administration (NPRA) has adopted technology qualification as an approach to ensure that the extreme fjord-crossing concepts evaluated for the "Ferry free E-39" project inherits the necessary attributes. Several uncertainties are related to the E-39 project. To empower decision making, and systematically address these uncertainties, the agency has begun the development of a technology qualification programme.

It is expected that the extreme fjord-crossing concepts will require installation of dedicated safety-related systems that employ electrical/electronic/programmable electronic technology (so called “safety-instrumented systems”) to ensure safe operation. Many of these systems may be considered unproven (in technology and/or application area), and will require a systematic and structured process of qualification before deemed safe to install.

IEC 61508 is considered the main standard for safety-instrumented systems, and elements from this standards may supplement and improve a potential framework for qualification of such systems. The standard can be classified as a RAMS (reliability, availability, maintainability and safety) standard. RAMS requirements are key attributes of system performance, and RAMS assessments are therefore key tools in any qualification process.

This thesis aims to contribute to the currently on-going work of implementing a technology qualification programme in the NPRA, by proposing a qualification framework for safety-instrumented systems related to the submerged floating tube bridge concept. The concept is being addressed as a solution for the crossing of Bjørnafjorden. The framework aims to draw on several different approaches, and implement principles from RAMS engineering and IEC 61508. Focus has been placed on the transferability of a framework for qualification of safety-instrumented systems, and a framework for qualification of entire bridge concepts.

To understand the basics of technology qualification, this thesis includes an in-depth review of the different approaches towards qualification of new technology. This includes the more established recommended practices, such as DNV-RP-A203 and API-RP-17N. With focus on safety-instrumented systems, IEC 61508 is presented and the potential contributions of the standard towards qualification of such systems are discussed. It was identified that the central safety lifecycle from the standard is similar to a qualification process with several elements that may supplement a qualification framework.

In order to adapt the framework to the NPRA's practices, central aspects and challenges of a qualification framework in the NPRA have been identified and discussed. The lack of a RAMS management framework in the agency was identified as a key challenge towards implementing a risk-based qualification framework. The scope and role of a qualification framework is another challenge that must be addressed prior to a potential implementation.

Based on the challenges in the NPRA, central aspects of RAMS engineering and IEC 61508, and the established approaches towards technology qualification, a framework for qualification of safety-instrumented systems is introduced. The framework contains some new methods and approaches towards the stating of requirements and assessing readiness of technology.

The framework is demonstrated on a water-mist fire suppression system for the submerged floating tube bridge concept over Bjørnafjorden. In order to understand the environmental and operational conditions for such a system, a description of the submerged floating tube bridge concept and its' risk picture are included.

Sammendrag og Konklusjon

Kvalifisering av ny teknologi (eller systemer) har blitt en viktig disiplin innen applikasjonsområder der det stilles strenge krav til sikkerhet og/eller pålitelighet, og hvor ny teknologi ikke er tilstrekkelig dekket i etablert regelverk, standarder og praksis. Med ny løsninger, som potensielt påvirker mange mennesker, er det viktig å redusere usikkerheten knyttet til utviklingen av teknologien og dokumentere at teknologien vil ha en akseptabel ytelse gjennom sin livssyklus.

Statens Vegvesen har adoptert teknologikvalifisering som en tilnærming for å forsikre at de ekstreme fjordkryssingskonseptene under vurdering for "Ferje-fritt E-39" prosjektet innehar de nødvendige egenskapene. Flere usikkerheter er knyttet til E-39 prosjektet. For å sikre gode beslutninger, og systematisk adressere disse usikkerhetene, har etaten begynt å utvikle et rammeverk for teknologikvalifisering.

Det er forventet at de ekstreme fjordkryssingskonseptene vil kreve installasjon av dedikerte sikkerhets-relaterte systemer som bruker elektrisk/elektronisk/programmerbar elektronisk teknologi (såkalte "instrumenterte sikkerhetssystemer") for å forsikre at sikkerheten blir opretthold under operasjon. Mange av disse systemene kan anses som uprøvd (innen teknologi og/eller applikasjonsområde), og vil behøve en systematisk og strukturert kvalifiseringsprosess før de anses trygge til å bli installert.

IEC 61508 anses som hovedstandarden for instrumenterte sikkerhetssystemer, og elementer fra denne standarden kan supplementere, og forbedre, et potensielt kvalifiseringssrammeverk for slike systemer. Standarden kan også anses som en RAMS (pålitelighet, tilgjengelighet, vedlikeholdsvennlighet og sikkerhet) standard. RAMS-krav er viktige egenskaper for ytelsen til systemer, og RAMS vurderinger er viktige verktøy i enhver kvalifiseringsprosess.

Denne masteroppgaven sikter derfor mot å bidra til det pågående arbeidet med å implementere et rammeverk for teknologikvalifikasjon i Statens Vegvesen, ved å foreslå et rammeverk for kvalifisering av instrumenterte sikkerhetssystemer tilknyttet rørbrukonseptet. Konseptet blir for øyeblikket vurdert som en løsning for å krysse Bjørnafjorden. Rammeverket sikter mot å bygge på flere tilnærminger og samtidig implementere prinsipper fra systems engineering og IEC 61508. Fokus har blitt lagt på overførbarhet mellom et rammeverk for instrumenterte sikkerhetssystemer, og et rammeverk for kvalifisering av hele brukonsepter.

For å forstå de grunnleggende prinsippene for teknologikvalifisering, inneholder denne oppgaven en grundig gjennomgang av de forskjellige tilnærmingene til teknologikvalifisering. Dette inkluderer de mer etablerte anbefalte praksisene, som DNV-RP-A203 og API-RP-17N. Med et fokus på instrumenterte sikkerhetssystemer, er IEC 61508 presentert og de potensielle bidragene fra standarden mot kvalifisering av slike systemer diskutert. Det ble identifisert at den sentrale sikkerhetslivssyklusen fra standarden har likheter med en kvalifiseringsprosess og innehar flere elementer som kan supplementere et kvalifiseringsrammeverk.

For å tilpasse rammeverket mot Statens Vegvesens praksis, har sentrale aspekter og utfordinger for implementering av et kvalifiseringsrammeverk i Statens Vegvesen blitt identifisert og diskutert. Mangelen på RAMS-styringsrammeverk i etaten ble identifiserti som en nøkkelutfordring for å implementere et risikobasert rammeverk for kvalifisering av ny teknologi. Rollen og omfanget av et slikt rammeverk er en annen utfordring som må adresseres i forkant av en potensiell impementering.

Basert på utfordringene i Statens Vegvesen, sentrale aspekter innen RAMS og IEC 615008, og de etablerte tilnærmingene til teknologikvalifisering, er det introdusert et rammeverk for kvalifisering av instrumenterte sikkerhetssystemer. Rammeverket inneholder noen nye metoder og tilnærminger som hvordan krav kan stilles og hvordan vurdere modenheten til teknologi.

Rammeverket er demonstrert på et vanntåkesystem for å undertrykke brann i rørbrukonseptet planlagt over Bjørnafjorden. For å forstå omgivelsene og de operasjonelle forholdene for et slikt system, er det inkludert en beskrivelse av rørbrukonseptet og dets risikobilde.

Contents

Chapter 1

Introduction

One of the challenges in today's engineering and product development is to ensure that new technology and systems are considered safe and inherent the different attributes considered desireable. With new solutions, which potentially affect a lot of people, it is important to reduce the uncertainty related to the development of the technology and document that the technology will have an acceptable performance during its lifecycle.

Qualification of new technology (or systems) has become an important discipline within application areas that have strict requirements to safety and/or reliability, and where new technology is not adequately covered by established rules, standards, and practices. The first structurized methods were developed within the space industry, followed by the defence industry and oil and gas sector. Now, qualification of new technology has been identified as a key discipline to decision-making and project development management in the Norwegian Public Road Administration (NPRA) for the project "Ferry-free E-39".

1.1 Background

In 2010 the Norwegian Department of Transport and Communications commissioned the Norwegian Public Road Administration (NPRA) to investigate the potential effects for trade and industry, regional employment and settlement patterns of eliminating eight ferry connections along the western corridor (E-39) between Kristiansand and Trondheim. This also includes investigating and exploring the technology required for the fjord crossings. The overall aim is to

replace all the ferry connections and upgrade the entire route within twenty years.

With vast depths of up to 1300 meters and long distances of over 5 kilometres, the crossings of the western Norwegian fjords are no easy undertaking. The nature of the crossings requires new solutions which break the frontiers of existing bridge technology. This challenges how the NPRA traditionally manages and plans their road design projects. In order to make robust decisions regarding design solutions and overall concept selection, a systematic process of assessing and managing the many uncertainties related to the fjord-crossing concepts has been identified as a key supplement to the risk and uncertainty management for the project. For this purpose, a technology qualification programme (TQP) should be implemented to assure that the new bridge solutions are *fit for purpose* and have the required attributes before they are put into operation.

One of the fjord crossing concepts being considered for the crossing of Bjørnafjorden is the Submerged Floating Tube Bridge (SFTB). Bjørnafjorden has variating depths of up to 550 meters and a span of over five kilometres, making conventional bridge and tunnel solutions impossible to realize. A SFTB combines bridge, tunnel and offshore technology to enable a fixed fjord-crossing connection. The concept has already been evaluated as feasible. However, there are several uncertainties related to the fulfillment of objectives such as cost, safety, reliability and serviceability.

It has already been identified that the safe operation of SFTBs requires installation of dedicated safety-related systems that employ electrical/electronic/programmable electronic technology (so called "safety-instrumented systems"). Many of these systems may be considered unproven (in technology and/or application area), and will require a systematic and structured process of qualification before deemed safe to install.

Reliability, availability, maintainability, and safety (RAMS) requirements are key attributes of system performance, and RAMS assessments are therefore key tools in any qualification process. Many industry sectors, including their regulating bodies, have adapted IEC 61508 (or its' section specific versions of the standard) as a framework for design and operation of safety-instrumented systems. The scope of these standards go beyond the scope of a technology qualification process, but standards on qualification of new technology, like e.g. DNV-RP-203A and API-17N, represent an important supplement and support for many phases of the lifecycle.

A technology qualification programme has been identified as a key supplement to NPRA's project development management for the ferry free E-39 project. So far, few attempts have been made to adapt elements from IEC 61508 within this model. IEC 61508 may also provide a set of rules and requirements for safety instrumented systems, which is currently lacking in the NPRA. The main objective of this master thesis is hence to investigate and demonstrate how central aspects from IEC 61508 may support and supplement a technology qualification programme and the NPRA project development model by proposing a qualification framework for safety instrumented systems and demonstrating the framewok on a system relevant for a SFTB over Bjørnafjorden.

1.2 Objectives

The main objectives of this master thesis are to:

1. Identify and describe safety-instrumented systems expected to be needed in relation to the submergible floating tube bridge for Bjørnafjorden, and develop a risk model that illustrates how these systems interact in the sequence of events that may result in major accidents.

2. Identify and discuss links and (potential) interfaces between the scope, specific steps, phases, and requirements in IEC 61508 and NPRA practices, covering the project development model and the overall technology qualification program that has been adopted by NPRA

3. Propose an overall framework based on results from task 2 that may be adopted for qualification of safety-instrumented systems.

4. Demonstrate how the framework can be applied for a specific case study (i.e. for a safety-instrumented system decided upon in collaboration with the NPRA), including a discussion on how to:

    - Derive reliability and safety requirements, including safety integrity level(SIL).

- Assess the reliability of the selected safety-critical system in light of the SIL requirement
- Incorporate the treatment of uncertainty in the assessments and decision-making

5. Discuss the results and lessons learnt from adapting IEC 61508 for safety-instrumented systems for use in new strait crossing concepts, and identify and discuss ideas for further research.

1.3 Relevant Work

Qualification of new technology is a relatively young discipline. Among the more established guidelines on technology qualification are the recommended practices DNV-RP-A203 (DNV, 2011) and API-RP-17N (API, 2009). These frameworks are intended for the subsea oil and gas industry, but the principles are also valid for other applications. As a young discipline, technology qualification is a relatively unexplored topic in academia. Among the relevant contributions are: Rahimi and Rausand (2015); Mankins (2009); Samarakoon and Gudmestad (2011); Magtaggart (2012); Hother and Hebert (2005) and Sabetzadeh et al. (2011).

The subject of safety instrumented systems are well covered in academia. Lundteigen (2008), Lundteigen and Rausand (2009b), Rausand (2014), Liu (2014), Barnard (2013) and Hauge et al. (2009) are just some of the contributions within this field. The generic standard IEC-61508 (2010) is considered the main standard for regulation and development of safety instrumented systems. A lot of research have been conducted on the context of this standard, such as Smith and Simpson (2011); Lundteigen and Rausand (2009a), Lundteigen et al. (2009). No work, however, have been conducted on integrating elements of IEC-61508 (2010) in a qualification programme for new/novel technology (at least to the author's knowledge).

Johansen (2016) has proposed a framework for technology qualification of extreme fjord crossings regarding the ferry free E-39 project. This is, however, aimed at qualification of large bridge concepts and not safety instrumented systems.

1.4 Delimitations

The main focus of this thesis is qualification of safety instrumented systems. The thesis mainly focuses on the design and development phase, rather than the operation phase. The framework proposed in this thesis is influenced by the current needs and expectations from the NPRA, and relevant factors that may arise later in the development process may have been overlooked or excluded. To delimit the thesis, software requirements (IEC 61508, 2010, Part 3), and human and organizational factors are not considered. The case study only considers a low-demand (on-demand) system in a certain application setting (submerged floating tube bridge).

1.5 Structure of the Report

The rest of the report is organized as follows. Chapter 2 gives an introduction to the theory and methodology of technology qualification with a review of different qualification approaches. Chapter 3 narrows the qualification concept to qualification of safety instrumented systems (SISs) with an introduction to important principles, terminology and requirements of such systems. Chapter 4 provides an analysis of central aspects and challenges in the NPRA's work to introduce a TQP for both new bridge concepts and SISs. In Chapter 5, important attributes of a qualification framework is identified and a new framework for qualification of SISs in the NPRA is introduced. A case study of a fixed fire suppression system is described in Chapter 6 to demonstrate the framework introduced in Chapter 5. Chapter 6 also includes a description of the Submerged Floating Tube Bridge and the different SISs which is expected to be installed in the structure. A summary and recommendations for further work on the topic are provided in Chapter 7.

Chapter 2

Qualification of New Technology

Technology qualification may be described as a «structured process of providing evidence that a technology will function within specified operational limits and with an acceptable level of confidence» (DNV, 2011). The purpose is to reduce uncertainty and increase confidence in novel technology, not to simply obtain a "correct" estimate of the reliability of the new system. In addition to provide evidence, a technology qualification process may be used to compare, or scale, different technology solutions and provide documentation of technology maturity through the different development stages. Traditionally, technology qualification programmes (TQPs) have focused on reliability prediction in order to improve the reliability performance, but can in principle consider all types of system attributes and requirements (Johansen, 2016). To a company, a good technology qualification programme may help making sure that products, systems or technology, regarded as desirable to implement or produce, inhabits the required attributes and performance.

By new, or novel, technology, we understand any technology that is associated with some sort of uncertainties regarding the novelty of the technology itself (proven/unproven) and/or application area (known/unknown).

Table 2.1: Definition of new technology

	Proven	Unproven
Known technology		√
Unknown technoogy	√	√

A qualification process involves verification, which is the process of determining whether an

activity fulfills specified requirements according to objectives established in application standards, and validation which is the process of determining the appropriateness of specific data, assumptions and/or techniques. As such, verification and validation can, respectively, be seen as the answer to the two questions: Did we build the product right and did we build the right product?

2.1 Review of Approaches

Offshore oil and gas companies typically develop their own framework for qualification of new technology based on, or including, central aspects of standards such as DNV-RP-A203 (DNV, 2011) and API-RP-17N (API, 2009). Even if the NPRA does not necessarily view technology qualification in the same manner as the oil and gas industry, the basis for a framework applicable for road projects still needs to build on the same existing theories and methods for technology qualification. This section will present some of the most commonly applied standards and qualification approaches in the industry.

2.1.1 Technology and System Readiness Levels (TRL and SRL)

The Technology readiness level (TRL) concept was introduced in the 1970s and is central for technology qualification in the National Aeronautics and Space Administration (NASA) (Mankins, 2009). TRLs are levels used as a means to communicating the readiness or maturity status of a specified technology or system. The TRL system spans from TRL 1, which represents that scientific research has resulted in the observation of basic principles, to TRL 9, which represents that the actual technology or system has been "flight-proven" through successful operations. For a technology to go from one TRL to the another, the milestone objectives of the readiness level must be documented and approved. The different technology readiness levels are described in table 2.2 according to the description in Mankins (1995).

The TRL approach has been adopted for several applications, and various TRL scales and descriptions are used in the industry today. Besides NASA, the U.S Department of Defence (DOD), the U.S Congress' General Accountability Office (GAO), and most connectedly, the American Federal Highway Administration (FHWA) have adopted the approach (Mankins, 2009; Cheok

Table 2.2: Technology Readiness Levels. From Mankins (1995)

TRL	Definition	Description
TRL1	Basic principles observed and reported	Lowest level of technology readiness level. Scientific research starts to be translated into applied research and development. Examples might include paper studies of a technology's basic properties
TRL2	Technology concept and/or application formulated	Invention begins. Once basic principles are observed, documented and approved, practical applications can be invented. Applications are speculative and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytical studies
TRL3	Analytical and experimental critical function and/or characteristic proof of concept.	Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.
TRL4	Component and/or breadboard validation in laboratory environment	Basic technological components are integrated to establish that they will work together. This is relatively "low fidelity" compared to the eventual system. Examples include integration of "ad hoc" hardware in the laboratory.
TRL5	Component and/or breadboard validation in relevant environment.	Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so it can be tested in a simulated environment.
TRL6	System/subsystem model or prototype demonstration in a relevant environment	Representative model or prototype system, which is well beyond that of TRL 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness
TRL7	System prototype demonstration in an operational environment.	Prototype near, or at, planned operational system. Represents a major step up from TRL 6, requiring demonstration of an actual system prototype in an operational environment such as an aircraft, vehicle, or space
TRL8	Actual system completed and qualified through test and demonstration.	Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications.
TRL9	Actual system proven through successful mission operations.	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation. Examples include using the system under operational mission conditions.

et al., 2010). The FHWA uses the TRLs as a factor contributing to determine a Maturity Index (MI) which is a linear scale going from immature (0) to mature (1).

The traditional TRL concept can be seen as a measure of an individual technology, and not readiness of a system or how the technology integrates within a complete system. The main argument is that measuring technology and system maturity is a multidimensional process that cannot be performed adequately by a one-dimensional metric such as TRL (Yasseri, 2013). Hence, Sauser et al. (2006) have developed a more comprehensive readiness assessment with a System Readiness Level index (SRL index) and Integration Readiness Level index (IRL index) to describe the readiness on a system level and the integration maturity (see table 2.3 and 2.4). The approach was primarily developed to aid the U.S Department of Defense with development of complex weapon systems, where the standard TRL approach was not adequate. Knaggs et al. (2015) also studied the use of SRLs for developing fossil energy technologies.

The SRL approach proposed by Sauser et al. (2006) defines five maturity steps which is calculated from the individual TRLs and the interconnecting IRLs. The model uses matrix algebra to compute a SRL vector that quantifies the readiness level of a specific technology with respect to every other technology in the system (Sauser et al., 2008).

The specific SRL calculation model proposed by Sauser et al. (2006) has received mixed reviews. While some researchers acknowledge the value of the model as an effective support tool in different RD&D processes (Knaggs et al., 2015; Yasseri, 2013), others points to the mathematical flaws in the model as a potential source of misleading and harmful consequences of using the model (McConkie et al., 2013; Kujawski, 2013). The critics also argue that the simplicity of the model violates basic engineering principles by disregarding important system attributes such as cost and schedule, making the model potentially harmful for a system's development. It may be that system readiness, as a multidimensional concept, is too complex to be characterized by a single metric or overly simplified calculations, but the notion of a measurement that includes the integration maturity of the individual technologies interacting in a system perspective, may prove to be valuable in assessing the readiness of new complex systems.

Table 2.3: Integration Readiness Levels. From Sauser et al. (2008)

IRL	Definition	Description
IRL9	Integration is Mission Proven through successful mission operations.	IRL 9 represents the integrated technologies being used in the system environment successfully. In order for a technology to move to the TRL 9, it must first be integrated into the system and then proven in the relevant environment; thus, progressing IRL to 9 also implies maturing the component technology to the TRL 9.
IRL8	Actual integration completed and Mission Qualified through test and demonstration in the system environment.	IRL 8 represents not only the integration-meeting requirements, but also a system-level demonstration in the relevant environment. This will reveal any unknown bugs/defects that could not be discovered until the interaction of the two integrating technologies was observed in the system environment.
IRL7	The integration of technologies has been Verified and Validated with sufficient detail to be actionable.	Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.
IRL6	The integrating technologies can Accept, Translate, and Structure Information for its intended application.	IRL 6 is the highest technical level to be achieved; it includes the ability to not only control integration, but to specify what information to exchange, to label units of measure to specify what the information is, and the ability to translate from a foreign data structure to a local one.
IRL5	There is sufficient Control between technologies necessary to establish, manage, and terminate the integration.	IRL 5 simply denotes the ability of one or more of the integrating technologies to control the integration itself; this includes establishing, maintaining, and terminating.
IRL4	There is sufficient detail in the Quality and Assurance of the integration between technologies.	Many technology -integration failures never progress past IRL 3, due to the assumption that if two technologies can exchange information successfully, then they are fully integrated. IRL 4 goes beyond simple data exchange and requires that the data sent is the data received and there exists a mechanism for checking it.
IRL3	There is Compatibility (i.e., common language) between technologies to orderly and efficiently integrate and interact.	IRL 3 represents the minimum required level to provide successful integration. This means that the two technologies are able to not only influence each other, but also to communicate interpretable data. IRL 3 represents the first tangible step in the maturity process.
IRL2	There is some level of specificity to characterize the Interaction (i.e., ability to influence) between technologies through their interface.	Once a medium has been defined, a “signaling” method must be selected such that two integrating technologies are able to influence each other over that medium. Since IRL 2 represents the ability of two technologies to influence each other over a given medium, this represents integration proof-of-concept.
IRL1	An Interface between technologies has been identified with sufficient detail to allow characterization of the relationship.	This is the lowest level of integration readiness and describes the selection of a medium for integration.

Table 2.4: System Readiness Levels. From Sauser et al. (2008)

SRL	Acquisition Phase	Definitions
0.90 to 1.00	Operations & Support.	Execute a support program that meets operational support performance requirements and sustains the system in the most cost-effective manner over its total lifecycle.
0.80 to 0.89	Production	Achieve operational capability that satisfies mission needs.
0.60 to 0.79	System Development & Demonstration	Develop system capability or (increments thereof); reduce integration and manufacturing risk; ensure operational supportability; reduce logistics footprint; implement human systems integration; design for production; ensure affordability and protection of critical program information; and demonstrate system integration, interoperability, safety and utility.
0.40 to 0.59	Technology Development	Reduce technology risks and determine appropriate set of technologies to integrate into a full system.
0.10 to 0.40	Concept Refinement	Refine initial concept; develop system/technology strategy.

2.1.2 DNV-RP-A203

DNV-RP-A203 (DNV, 2011) is based on experience from the oil and gas industry and provides a general recommended practice (RP) for qualification of new technology. The guideline, developed by Det Norske Veritas (DNV), was first published in 2001 and the newest version, modified after ten years of experience, was introduced in 2011. The technology qualification framework introduced in the document is generic and might be applicable for qualification of both hardware and software technology. The guideline explains how a technology qualification programme (TQP) can be established. A technology qualification programme (TQP) is contextually contingent to the user/company/project and provides a framework for managing the qualification process with the overall aim to systematically reduce uncertainties and thus provide sufficient technical evidence for the technology. In this thesis, the term *framework* will be used for the same purpose. The framework outlines the qualification process and management principles of the qualification progress.

DNV-RP-A203 introduces a systematic qualification process that is risk-based. The basic technology qualification process consists of six steps:

1. Qualification basis, including identification and specification of technology functions, intended use and requirements, as well as the qualification objectives.

2. Technology assessment, including system decomposition and categorization of the de-

gree of novelty with respect to key uncertainties and significant challenges in the technology or application area.

3. Threat assessment, including identification of failure modes and risk evaluation.

4. Qualification plan, including the selection and development of the necessary qualification activities utilizing the appropriate qualification methods.

5. Execution of the plan, including collecting and documenting data.

6. Performance assessment, including review of evidence to demonstrate that the requirements and objectives are met, and to evaluate the level of confidence.

The framework reflects the iterative nature of the technology development and controls the activities through the development steps and milestones. As such, the overall qualification process is iterative and follows a stage-gate model. Each process ends with a concluding remark which indicates whether or not a stage in the framework has been reached. The process is repeated in all overarching phases of the development project (see figure 2.1). If the assessment shows that the technology does not meet the requirements and objectives stated in the qualification basis, the technology needs to be modified to achieve the objectives and requirements (DNV, 2011).

While the technology and system readiness levels (TRLs and SRLs) are means to quantify the development readiness of individual technologies and systems, DNV-RP-A203 (and API-RP-17N, see section 2.1.3) is concentrated around outlining the entire qualification process and developing a technology qualification programme. TRLs are also described in DNV-RP-A203 as a means of illustrating the development stage of a technology and map out the phases of a TQP.

2.1.3 API-RP-17N

The American Petroleum Institute (API) has developed a qualification procedure for the specific application of qualification for subsea equipment. The document (API-RP-17N) gives recommendations for the management of risk and uncertainties related to subsea system's reliability, technical risk and integrity. Current version, published in 2009, builds on 12 organizational key processes (KPs), where qualification of technology is one such key process.

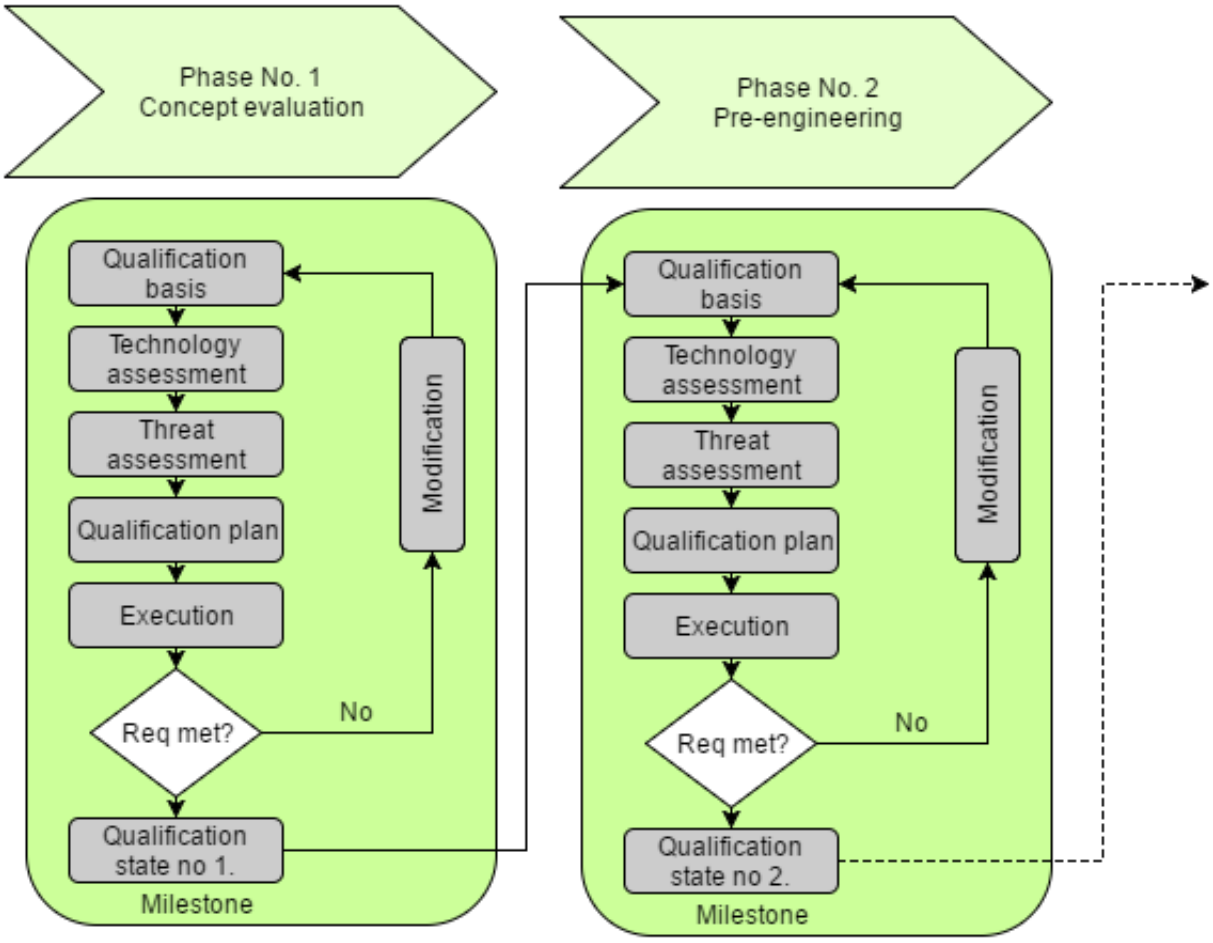

Figure 2.1: Illustration of the iterative qualification during the development phases. From DNV (2011)

The qualification process introduced in API-RP-17N is systematic and linked to the other KPs introduced in the document. The progress of the process is indicated by a methodical TRL-approach with eight levels going from TRL0, “unproven” to TRL7, “field proven”.

API-RP-17N recommends that all equipment to be used subsea, regardless of design, application or operation mode, should be subject to some sort of qualification. Similar to the DNV-RP-A203, the qualification process proposed in API-RP-17N is risk-based with a objective of managing the risk related to the new technology. The overall qualification process outlined in API-RP-17N is inspired by DNV-RP-A203 and the qualification process resembles the process presented in section 2.1.2. However, the process described in API-RP-17N is not so much of a separate process, but a process interacting with the other KPs described in the document (see figure 2.2).

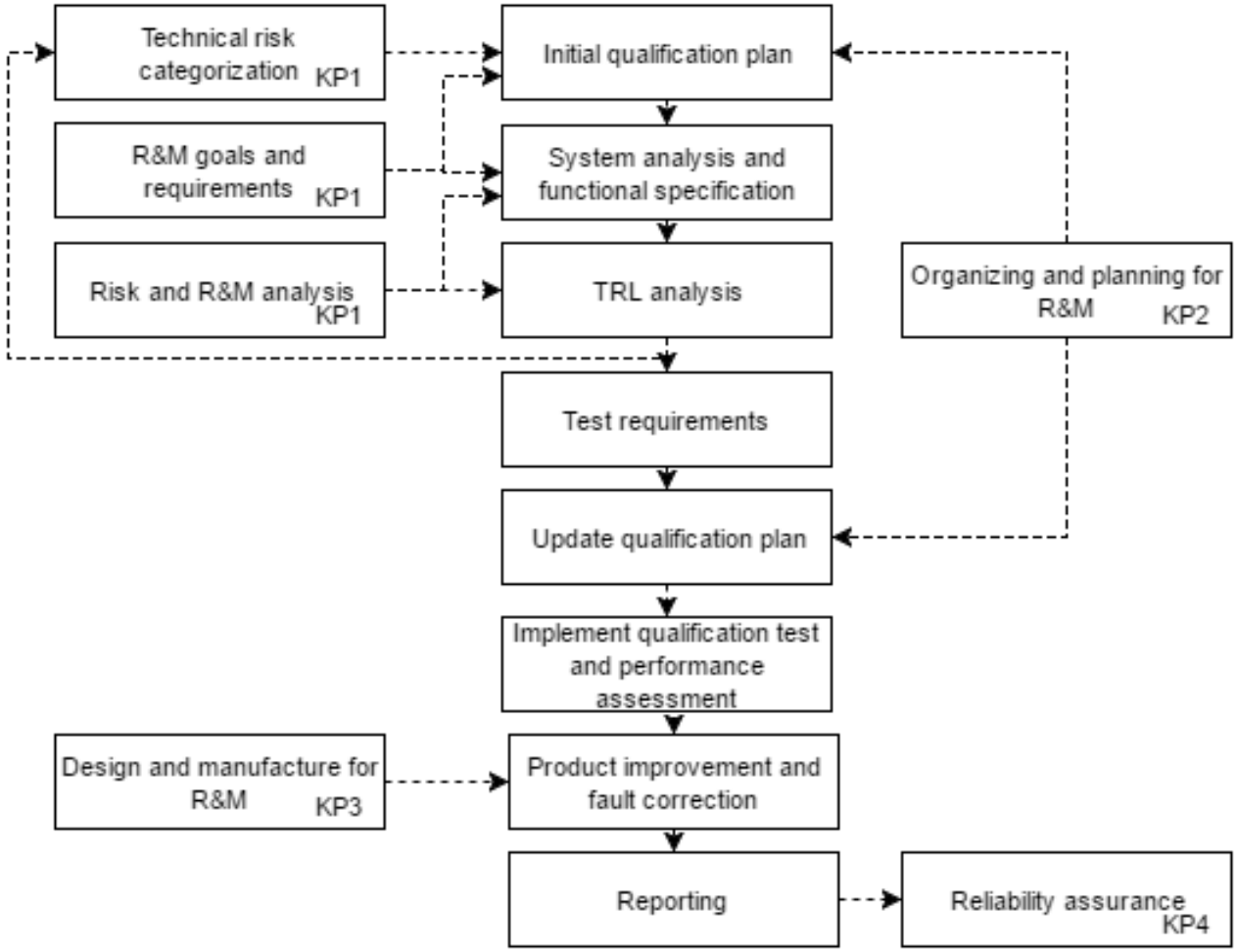

Figure 2.2: The outlined qualification process described in API (2009)

2.1.4 Other Approaches

Another TQP approach is discussed in Rahimi and Rausand (2015) which is integrated with the product development model of Murthy et al. (2008). The approach was aimed to overcome the weaknesses and shortcomings of other selected existing technology qualification approaches. The new presented TQP approach has six main steps that corresponds to the six first phases of Murthy's model (Rahimi and Rausand, 2015). It is argued that by using the model of Murthy et al. (2008), a more holistic development process may be developed for new safety systems.

SEMATECH (1995) builds on Motorola's IRONMAN methodology and provides a qualification framework directed towards the producers and users of semiconductor equipment. It provides methods for reliability experimentation and improvement. The guideline consists of three main parts: (1) equipment lifecycle and reliability improvement process; (2) the managerial aspect of implementing the process and controlling the improvement activities through the lifecycle; (3) the activities and methods to be applied in the reliability improvement process. The overall goal of the guideline is to minimize uncertainties to help make appropriate decisions and minimize the lifecycle cost (LCC).

NATO-AVT-092 (2009) presents an analytical qualification process for military aircrafts. The aim of the guideline is to speed up the required military systems using more analytical qualification methods and simultaneously increase the value of qualification testing.

Some companies, especially in the oil and gas industry, such as FMC Kongsberg, Statoil and Aker solutions, have developed their own TQP for their explicit application. These programmes are commonly based on DNV-RP-A203, but with own procedures introduced to best fit the company's strategy and operation.

2.2 Qualification Methods

Qualification methods are the actual ways to provide evidence for each identified failure mode, showing that the stated requirements in the technology qualification basis have been met. If the stated requirements are quantitative, then the methods to document fulfillment of the target requirement must also be quantitative. Qualification of technology can generally be performed in three different ways. Either by 1) analytical and numerical methods, 2) experimental methods

and physical tests, or 3) an integrated qualification combining 1) and 2).

2.2.1 Analytical Methods

Analytical qualification relies on analytical methods, carried out by appropriate technical software and/or expert judgment, to provide evidence. In recent years, several software solutions, like finite element (FEM) analysis, corrosion model software and other simulation software, have become increasingly advanced and reliable. By simulating scenarios based on estimated parameter values, evidence of potential problems may be revealed and visualized.

The biggest advantages of analytical qualification methods are the usage of non-physical models and the time efficiency. Detailed analyses by software require only the competence to use the software and a platform to carry out the analysis, while some physical tests might require suitable facilities and equipment which might be expensive. The downsides with analytical methods are the uncertainties related to how correct the model represents reality and how correct the estimates parameters and values used in the analysis are. Although a 100% representative digital model cannot be achieved, the analytical method has contributed making qualification easier and more time-efficient in many cases. Analytical software is, as such, often used to qualify complex and expensive equipment, but in cases where analytical methods do not provide the necessary or required evidence, qualification by physical testing must be carried out.

2.2.2 Experimental Methods (Qualification by Testing)

Experimental methods or physical testing are the most traditional means to provide evidence through qualification and is usually carried out when analytical methods are not sufficient. For hardware technology, testing is carried out on a physical prototype. The prototype may be a simplification of the product one wishes to qualify, but the vital elements essential to the technology must be present and with the same level of dependability. Testing is carried out to the extent of the uncertainty of the technology. The results of testing are also called empirical results. The major disadvantages with physical testing of a prototype are the high expenses and time effort compared to analytical qualification. A test programme should be developed in such

a way that it provides the necessary evidence to reduce the uncertainty of the technology in question to a level determined to be acceptable.

Qualification by testing is also sometimes referred to as quantitative qualification

2.2.3 Integrated Qualification

The combination of analytical qualification and qualification by testing is often described as integrated qualification.

Larger and more complex systems may not be directly subject to qualification by a particular qualification method. In such cases a combination of the two method may prove to be an appropriate way to provide the necessary qualification evidence. Due to the cost and time commitment associated with testing, only elements that cannot be qualified through analytical methods, is qualified through testing. Remaining elements are subject to analytical qualification. This implementation minimizes the necessary qualification cost and time usage.

Other ways of combining the two methods are also possible. Some cases present challenges related to monitoring of the physical tests. Such cases may be scenarios dealing with high pressure, temperature, force, etc. If a satisfactory analytical model does not exist it is possible to conduct tests at a lower pressure, temperature, force etc. and then use the results to build a analytical model with a satisfactory reflection of the real situation. The technology in question may then be qualified using the analytical model. It is also possible to make use of both methods on the same case in parallel to evaluate the same problem. This approach can be used in high budget projects when it is essential to minimize the uncertainties and ensure a high level of confidence.

2.3 Qualification Process

The DNV-RP-A203 document presented in section 2.1.2 provides a systematic risk-based approach to qualification of new technology. The flow chart in figure 2.3 illustrates the qualification process compromising of six main steps as described in DNV-RP-A203. The feedback loop of the process imply that the process has an iterative nature. Modifications to improve safety, performance, longevity and cost are considered throughout the process. For traceability of the

conclusions along the way, each step shall be sufficiently documented.

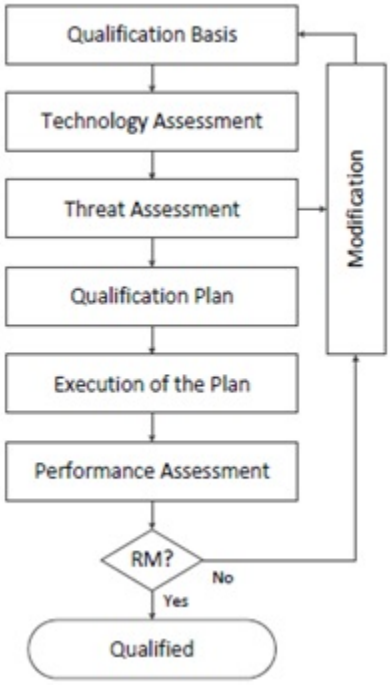

Figure 2.3: Flowchart illustrating the steps of the qualification process. From DNV (2011)

2.3.1 Technology Qualification Basis

The qualification basis is the first step in the process, and the information that forms the foundation for the qualification is stated here. The purpose is to provide a common set of requirement criteria to against which all qualification activities and decisions will be assessed. Among important activities in this first step are to describe the technology, define what use and environment the technology is intended for, and specify its required functions, acceptance criteria and performance expectations. The requirement specification and performance description shall, as far as possible, be expressed quantitatively. The requirements stated in the technology qualification basis shall be fulfilled through the remaining steps in the qualification process.

2.3.2 Technology Assessment

The main objective of the second step in the process is to assess the technology degree of novelty. Important activities in this step include technology composition analysis, technology cat-

Table 2.5: The degree of newness of technology.

Experience with the operating condition	Level of technology maturity		
	Proven	Limited field history or not used by company/user	New or unproven
Previous experience	1	2	3
No experience by company/user	2	3	4
No industry experience	3	4	4

egorization, and identification of the main challenges and uncertainties related to the technology. Technology composition analysis is a way to decompose the technology to system and sub-system levels. The functions and interactions between the different elements in technology is identified and mapped to get a complete understanding of the novel technology.

The next step is to categorize and classify the novelty of the technology. A categorization should account for uncertainties regarding the operation history of the technology itself (proven/unproven) and the uncertainties connected to the application area (new/known). The categorization method presented in DNV-RP-A203 is illustrated in table 2.5.

The numbers in the categorization represent the degree of uncertainty related to the technology.

1. No new technical uncertainties (proven technology).

2. New technical uncertainties.

3. New technical challenges.

4. Demanding new technical challenges.

Technology classified in category 1 is considered proven, and evidence can be provided without a full qualification process. Technology classified in category 2, 3 or 4 are categorized as new technologies with increasing degree of uncertainty. Elements falling into these categories shall be qualified by providing evidence according to the recognized methods for qualification, tests and analyses. The last step in the technology assessment is an identification of the main challenges and uncertainties related to the technology. This may be done by carrying out a HAZID (HAZard IDentification) to increase the understanding of the unproven technology.

2.3.3 Threat Assessment

The technology identified as novel in the previous step is followed-up with a threat assessment. The objective of the threat assessment is to identify and assess the failure modes of concern and their associated risks. Several methods and analysis tools may be used for this purpose such as: FMECA (Failure Mode Effect and Criticality Analysis), HAZOP (Hazard and Operability study), FTA (Fault Tree Analysis), SWIFT (Structured What-IF checklist) and OPERA (Operational Problem Analysis) . Some of these methods may be more applicable than the others, depending on the scenario. The most common, still, is perhaps the FMECA. The FMECA is a systematic review of all the components, assemblies and subsystems to identify the failure modes, causes and effects of such failures. The qualification basis and the technology decomposition serves as input to the analysis.

The failure modes' possible consequences and likelihood of occurrence are also assessed. The likelihood of occurrence, or frequencies, of the failure modes are estimated based on reliability data bases, previous test records or other approved sources. In cases where data may be lacking, estimates can be assigned by expert judgment. The possible consequences are identified based on expert judgment, and ranked according to severity.

To assess the risk, it is common to categorize the different failure modes in a calibrated and suitable risk matrix. An example of such a matrix is shown in figure 2.4. The failure modes are categorized in the risk matrix based on the ranked severity of consequence and likelihood of occurrence. It is usual to define three, or more, areas in the risk matrix to rank the associated risk of the failure modes. The categorization indicates which failure modes that need further attention in the qualification process.

2.3.4 Qualification Plan

The qualification plan is developed to reduce the uncertainties and reduce the risks related to the different technology elements. Main activities include selection of suitable qualification methods as described in section 2.2, planning the activities to ensure reliable evidence meeting the requirements stated in the qualification basis, and developing a schedule for the qualification execution. It is important that the qualification methods chosen reflects the risk reduction

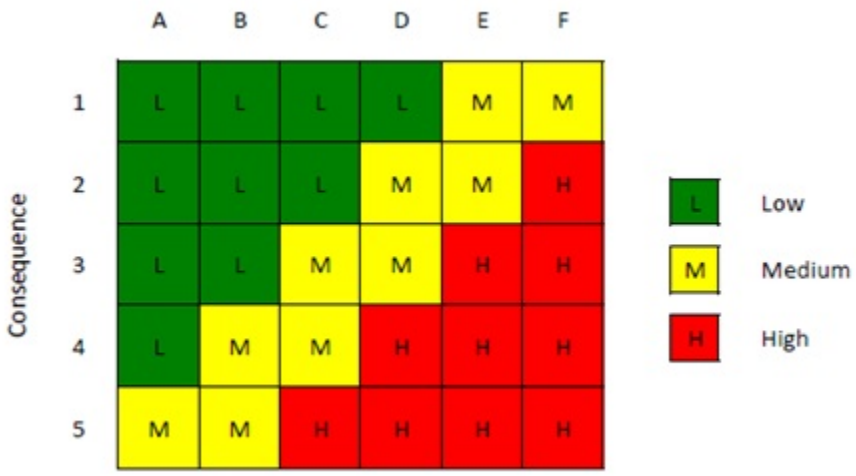

Figure 2.4: Example of a risk matrix

needed for the different failure modes categorized in the previous step. Focus should lie on the most critical failure modes identified in the threat assessment.

The qualification plan should outline a stage-gate model that reflects the iterative nature of the qualification process. Milestones in the execution should be specified and success criteria for evidence collection need to be established. A qualification plan may contain activities that cover several project phases. The plan must then be updated at every phase to include redefined requirements. The requirements can be redefined in respect to precision, scope or level of detail.

2.3.5 Execution of the plan

After successfully developing the qualification plan, the plan needs to be carried out. This step is usually the most resource and time consuming step in the qualification process, and emphasizes the need of a well-developed qualification plan. In the execution step, all qualification activities identified in the qualification plan is carried out, and generated results are collected and appropriately documented. The quality of the results should also be evaluated to ensure reliability.

If additional failure modes are identified during the execution step, these needs to be evaluated recorded and documented.

2.3.6 Performance Assessment

The last step in the process is a performance assessment of the technology to give a statement regarding the readiness of the technology and its elements. If a technology is categorized as qualified, it shall be confirmed that the risk and uncertainty connected to the technology and its elements are reduced to an acceptable level and meeting the requirements stated in the qualification basis. If the technology cannot be judged as proven, further qualification methods and activities may be identified. It may also be the case that the technology cannot be qualified at this point and needs to be addressed at a later time after more research and development have been invested in the technology.

2.4 Uncertainty Assessment

Uncertainty may be defined as "...the imperfect knowledge about the individual aspects of a system as well as the overall inaccuracy of the output determined by the system" (Rausand, 2014). The term is used with many different connotations in different contexts. Related to technology qualification, uncertainty implies risk for the technology's developers, manufacturers, vendors, operators and end-users, and the goal of technology qualification is to reduce these uncertainties through the provision of evidence. To document uncertainties it can be useful to categorize them by origin and influencing factor. Uncertainty may, basically, stem from two main causes, the lack of knowledge about the technology and the natural randomness. These types of uncertainty are often referred to as epistemic and aleatory uncertainty, respectively.

- Epistemic uncertainty: Uncertainty owed to lack of knowledge about the technology
- Aleatory uncertainty: Uncertainty owed to the natural randomness or variation

When more information and knowledge are being gathered about the technology, the epistemic uncertainties will be reduced. Aleatory uncertainty, however, cannot be reduced due to its origin in uncontrollable factors. As such, this categorization is useful to determine which uncertainties we can control and manage, and which we cannot.

Epistemic uncertainties can further be categorized according to the influencing factors. The uncertainties related to new technology assessments are also connected to the system analy-

ses and assessments performed in the process. The factors contributing to these uncertainties are a combination of parameter, model and completeness uncertainties. *Parameter uncertainties* owes to the relevance, amount and quality related to both the parameter input and output values. *Model uncertainties* owes to the fact that all models used are inevitably a simplification of the reality. All models involve some assumptions and simplifications that contribute to the overall uncertainty. *Completeness uncertainty* owes to factors deliberately or unconsciously overlooked or excluded, in addition to the factors that is truly unknown.

Chapter 3

Qualification of Safety Instrumented Systems

In order to achieve and maintain satisfactory risk levels in many industries, safety-instrumented systems are relied upon to carry out the necessary risk reducing functions. Failures of these systems may lead to injuries, fatalities, material and financial asset loss, and environemental pollution.

To ensure that these systems provide the necessary protection and inherits the required properties, safety and reliability assessments are central for the selection and qualification of SISs. The stated requirements are given in regulations and standards. Many industry sectors, including their regulating bodies, have adapted IEC 61508 (or its' section specific versions of the standard) as a framework for design and operation of safety-instrumented systems.

This chapter will give a brief introduction to the most relevant terms and definitions related to safety instrumented systems, and present central aspects of IEC 61508 which may be shown to be relevant for qualification of safety instrumented technology.

3.1 Safety Barriers and Classifications

Our public safety is increasingly provided for by different safety barriers. Such barriers are of vital importance to, for example, the oil and gas industry, the military sector, transportation, and shipping industry to prevent hazardous events for occurring and mitigate the consequences

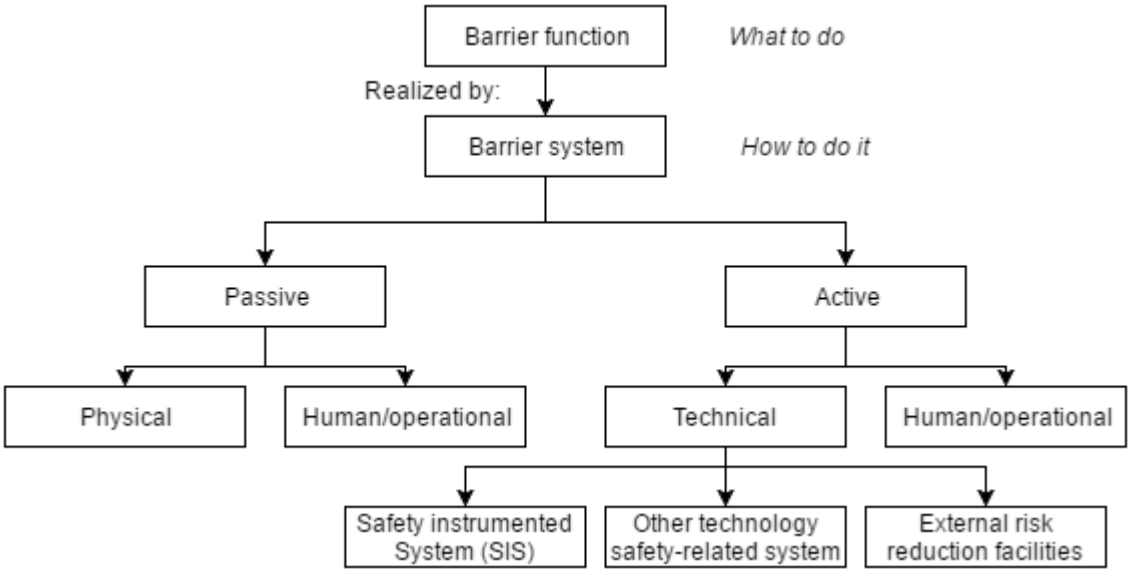

Figure 3.1: Classification of safety barriers. From Sklet (2006)

of unwanted events. Examples of safety barriers include: led walls in radiology departments at hospitals, emergency shutdown systems, fire and evacuation training, blow-out preventers and firefighting systems. A literature review shows that there is no universal and commonly accepted definition of the term (see CCPS (2001); Duijm et al. (2003); Harms-Ringdahl (2003); Hollnagel (2004); Sklet and Hauge (2004); Kecklund et al. (1996); Johnson (1980)). Sklet (2006) defines safety barriers as: "... all physical or non-physical means planned to prevent, control, or mitigate undesired events or accidents". A safety instrumented system (SIS) is a type of safety barrier. However not all safety barriers are SISs.

Safety barriers can be classified in several different ways depending on what dimensions to emphasise. The barriers may, for instance, be classified according to function (prevent, control and mitigate) or according to the source of the barrier (technical, administrative, etc.). Sklet (2006) also proposes a classification of safety barriers that is intuitive and applicable in many different scenarios (see figure 3.1). The classification also shows some important characteristics about SISs. From the classification it can be seen that SIS are classified as technical and active safety barriers.

Safety barriers are also referred to as defences, safeguards, countermeasures or protection layers

3.2 Function and System

Safety-critical systems are of vital importance to, for example, the oil and gas industry, the military sector, transportation, and shipping industry to prevent hazardous events for occurring and mitigate the consequences of unwanted events. Whether or not a system is safety-critical depends on the possible consequences of its failure. If the failure of the system can result in consequences that are judged to be unacceptable, we define that system as safety-critical. A SIS is a safety critical system that employ, at least to some extent, electrical, electronic, or programmable electronic (E/E/PE) technology.

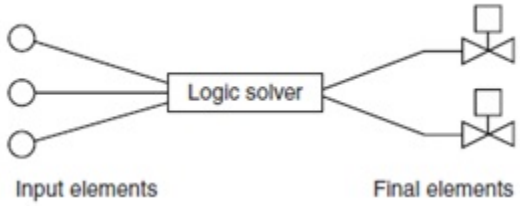

Figure 3.2: Illustration showing the elements in a SIS

A SIS may typically be split into three main subsystems, as illustrated in figure 3.2. The system is composed of input elements/detectors, a logical solver, and actuating/final elements. The logic solver may in some cases also be humanly controlled, such as a control centre. Together, these elements carry out one or more safety instrumented functions (SIFs) to bring, or keep, the equipment or facility in a safe state if a specific hazardous events occurs. It is noted that a SIS may perform one or more SIFs, and not all safety functions related to the equipment/facility one wants to protect are SIFs. The reliability of a SIS, however, is always related to its required safety instrumented functions and how well the system carries out these functions.

An example of a SIF in the SFTB case would be “to extract toxic air and smoke in case of a fire to prevent people in the tunnel being exposed to choking hazards”. This safety instrumented function is carried out by the ventilation system in the SFTB by switching its mode from fresh air supply mode to smoke extraction mode.

3.3 Failures

Failures and failure modes are two of the most important concepts when assessing the performance of any safety instrumented system. A failure is defined as "the termination of the ability of an item to perform its required function" (IEV-191-04-01). After a failure, the item will be in a fault state. For SISs, the required functions are related to keeping the safety level, and a failure of a SIS will affect the ability to maintain such a level. A failure mode is a description of a fault and describes how we can observe that an item is unable to perform the required function(s). An example of a failure mode for a valve can be “fails to open”, or “fails to close”.

Different failures may have different effect and consequence on the SIS, SIS-subsystems, humans, structure, environment etc., and a common way of classifying different failures is according to these effects and consequences. SIS failures may initially be classified into two main categories (Hauge et al., 2009).

- Dangerous (D) failures: Any failure that brings the item into a state where it cannot perform its safety function(s).
- Safe (S) failures: Any failure that does not bring the item into a state where it cannot perform its safety function(s).

Failures are also categorised according to their detectability as “detected” or “undetected”.

- Detected: Failure that is detected by automatic diagnostic testing (D)
- Undetected: Failure that is not detected by automatic diagnostic testing (U)

By diagnostic testing we mean an automatic partial test that uses built-in self-test features to detect faults. A failure commonly detected by diagnostic testing is for example, “loss of signal”. By combining the different failure categories, we get four different failure classes:

1. Dangerous undetected (DU)
2. Dangerous detected (DD)
3. Safe detected (SD)
4. Safe undetected (SU)

3.4 IEC 61508

IEC-61508 (2010) is a generic international standard published by the International Electrotechnical Commissions (IEC). The standard serves two main purposes, where the first is to aid and facilitate the development of sector specific versions. The second purpose is to serve as a guideline and provide the basis for specification, requirements design, operation and maintenance related to SISs where no sector specific version exists. As an application-independent standard, the IEC 61508 is of great relevance when assessing new technology, and although the standard is focused on systems involving E/E/PE technology, there should exist no reason why the standard could not also be applied in respect to "other technologies" used to provide risk reduction (Smith and Simpson, 2011). As an example, IEC 61511, which is the oil and gas specific version of IEC 61508, directs users back to IEC 61508 when dealing with design and qualification of new safety instrumented technology

The standard is comprehensive and divided into seven parts. The initial three parts (part 1 - 3) are normative parts which present the requirements for the SIS, while the remaining four (part 4 - 7) are supporting documents providing procedures, examples and other instructive annexes to the standard.

Part 1: General requirements

Part 2: Requirements for E/E/PE safety-related systems

Part 3: Software requirements

Part 4: Definitions and abbreviations

Part 5: Examples of methods for the determination of SIL

Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

Part 7: Overview of techniques and measures

3.4.1 The Safety Lifecycle

The standard is based on a lifecycle approach with 16 different lifecycle phases. The lifecycle provides a logical and systematic structure to the activities and requirements for the system.

This approach gives a traceability from the definition of necessity for protection, to the implementation and follow-up phase. Each phase has defined objectives and elementary activities with inputs and outputs to ensure ease the verification and validation at different points in the process.

The lifecycle, as illustrated schematically in figure 3.3, can be split into three main phases. The first main phase (phase 1-5) is the analysis phase where safety functions are identified, and requirements for the system are derived and stated. In this first main phase risk analyses are conducted and reliability requirements are allocated on the identified failure modes of the system. The second main phase (phase 6-13) is the realization which focuses on design and fabrication of the SIS according to the requirements identified in the first main phase. The last main phase (phase 14-16) is the operation, maintenance, modification and follow-up phase. These phases are intended to ensure that the system performance is maintained and meets the stated requirements throughout the lifetime of the system.

3.4.2 Functional Safety and Safety Integrity Requirements

The initial main phase of the lifecycle leads up to the functional safety requirements, stating what the system is required to do, and the safety integrity requirements, stating how well the SIS is required to perform. The safety integrity requirements may also be viewed as the likelihood of a safety function being performed satisfactorily. Risk assessments play a key role in developing the functional safety and safety integrity requirements. The hazard analysis leads to the functional requirements for safety (i.e. the safety functions) and the risk quantification assessment yields the safety integrity requirements (i.e. the safety integrity or performance level). The safety integrity requirements are determined by comparing the necessary risk reduction to the desired risk level or risk acceptance criteria. As such, the standard has a risk-based approach. Both are essential to ensure that the system provides the necessary protection to maintain a given safety level. The requirements may, together with the prerequisites and assumptions used to form the requirements, be documented in a safety requirement specification (SRS).

Safety integrity is presented in IEC 61508 as a measure of how well a safety function shall perform. The standard distinguishes between four different safety integrity levels (SIL), where SIL 1 is the least reliable, and SIL 4 is the most reliable. A SIL requirement provides restrictions

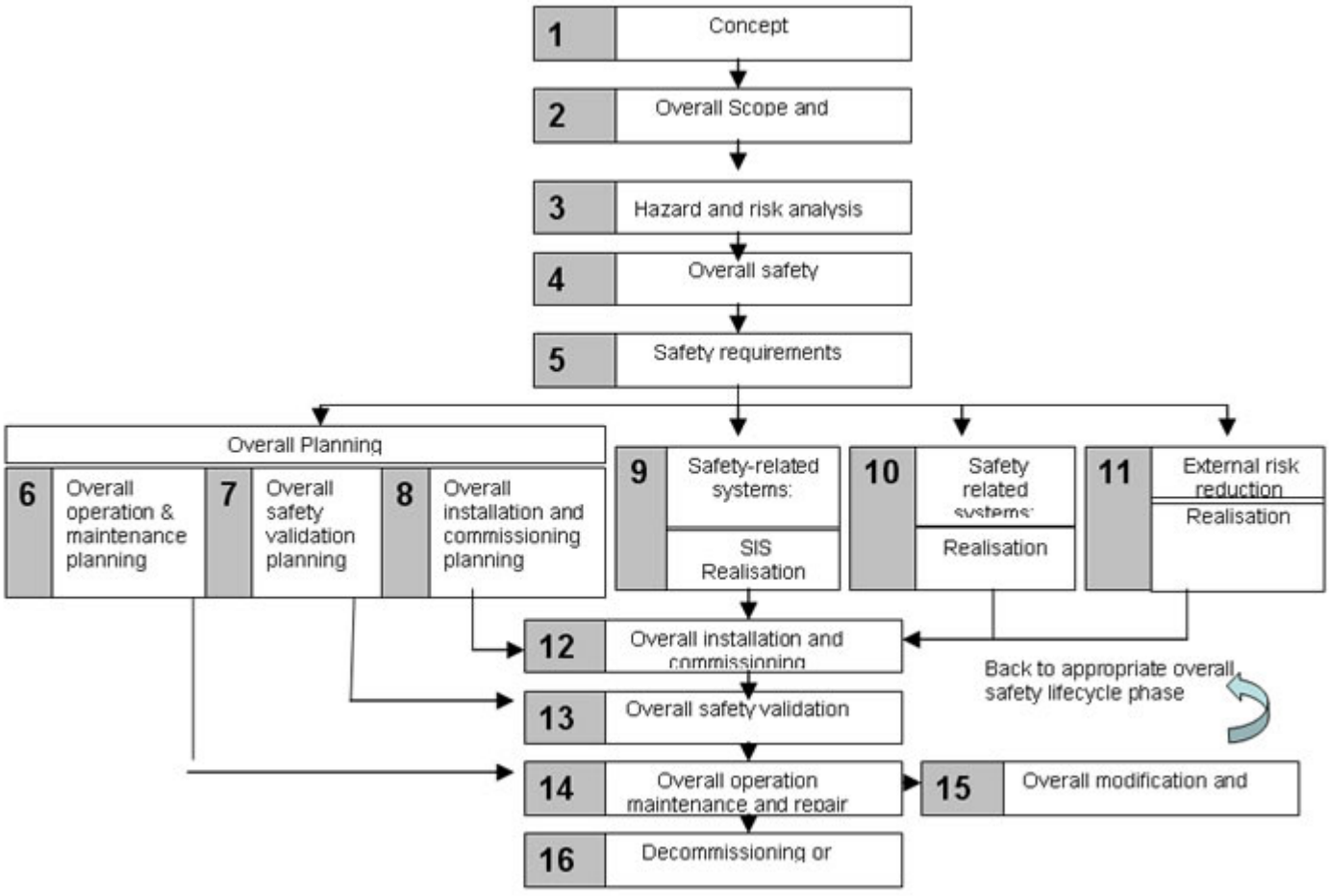

Figure 3.3: The safety lifecycle. From IEC-61508 (2010)

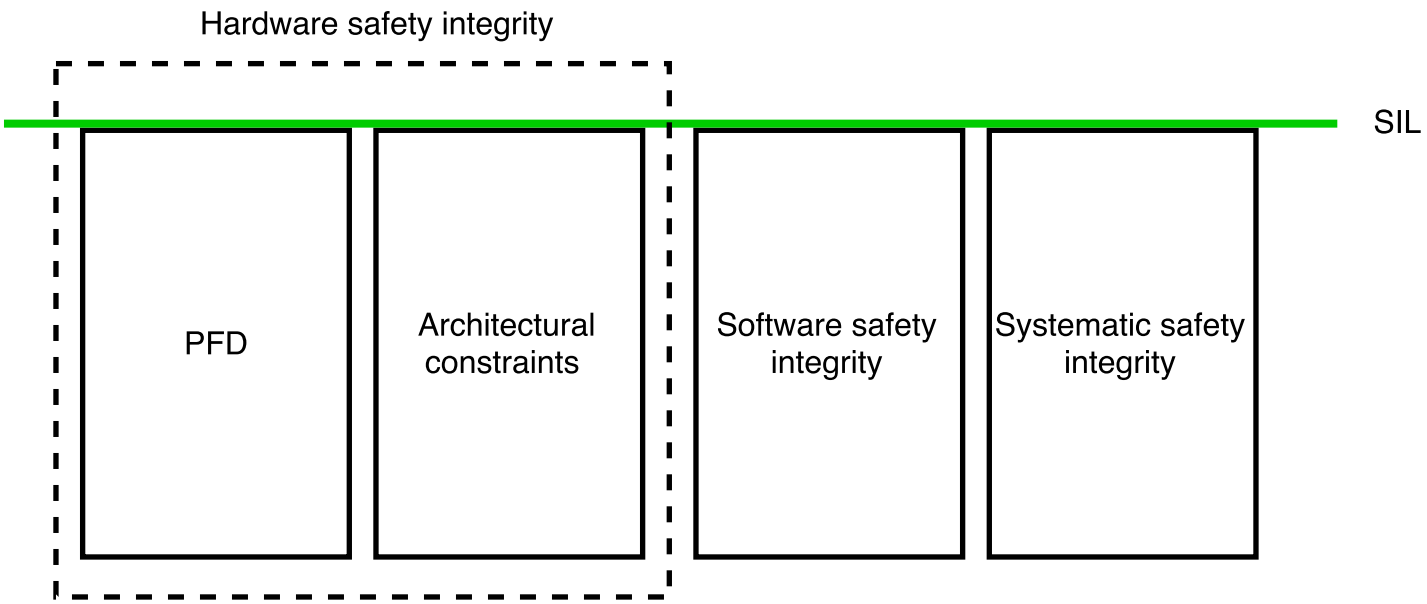

Figure 3.4: Illustration of safety integrity and SIL. Inspired from Lundteigen (2008)

and guidance towards the selection and development of hardware, software, procedures and work processes. The overall SIL requirements are specified in terms of either:

1. The risk reduction required to achieve tolerable risk, or
2. The tolerable hazardous event rate to meet the tolerable risk

SIL requirements are, according to IEC 61508, split into three parts: Hardware, software and systematic safety integrity. For a system to meet a given SIL requirement, all parts must demonstrate achievement of the specified SIL. This implies that if a SIF meets the hardware safety integrity of SIL 3, it cannot be claimed to comply with this SIL unless the software and systematic safety integrity meet a SIL 3 requirement. Hardware safety integrity is comprised of two different parts. The first part addresses the quantitative requirements, including calculation of probability of failure on demand (PFD) or probability of dangerous failure per hour (PFH), depending on demand rate of the system. The second part is architectural constraints is a more qualitative method which deals with achieving a sufficient robust system architecture without relying too hardly on reliability calculations alone. The different safety integrity categories are illustrated in figure 3.4.

For the quantitative requirements, two different measures of reliability are used. Systems in the defined low-demand mode (demanded less than once per year) are SIL categorized using

Table 3.1: SIL requirements.

Safety integrity level	PFD	PFH
SIL4	10^{-5} to 10^{-4}	10^{-9} to 10^{-8}
SIL3	10^{-4} to 10^{-3}	10^{-8} to 10^{-7}
SIL2	10^{-3} to 10^{-2}	10^{-7} to 10^{-6}
SIL1	10^{-2} to 10^{-1}	10^{-2} to 10^{-1}

probability of failure on demand (PFD), while systems defined as being in high or continuous demand mode are SIL categorized using probability of dangerous failure per hour (PFH). This discrimination is mostly because PFD has been shown not to be a suitable measurement for high-demand mode systems systems (Liu, 2014). The different SILs and corresponding PFDs and PFHs are listed in table 3.1.

3.5 Other RAMS requirements

Qualification of new technology is usually centred around reliability aspects of the technology, that is to qualify the reliability performance (the item or system's ability to carry out a specific function). Although reliability is important regarding qualification of SISs, the concept of technology qualification can be extended such that the technology is qualified with respect to several attributes. Besides reliability and safety, attributes such as availability, maintainability and testability are aspects influencing the technical safety.

3.5.1 Operation availability

Operation availability can be defined as the ability of an item to perform its required function at a stated instant in time or over a stated period of time (Rausand, 2011). The availability of a system or equipment is not only affected by failures, but also unintended operation (spurious trips), testing and maintenance. The unavailability of the safety system and its functions will contribute to lowering the protection performance of the system, and must be assessed as such. The unavailability may also cause the entire plant, construction or equipment the safety system is installed to protect to be shut down. This is highly relevant for infrastructure constructions like tunnels. If the entire ventilation or automatic incident detection system in a system is unavailable it is most likely that the entire tunnel will be shut down as a safety measure.

What sort of measurements, requirements and targets one should state regarding the systems and functions, depend on the operation, or demand, mode of the systems, in addition to what sort of failures that are related to them. The ventilation system in a tunnel, for instance, operates continuously to provide fresh air and ensure a tolerable level of pollution. The availability of this system will be measured by the number of failures to the system (single fans or subsystems of fans that must be operational to give sufficient coverage of the tunnel) and downtime related to the failures. The loss of availability will primarily cause traffic and health related problems. The same system must also act on demand in case of a fire or explosion in the tunnel to extract smoke and toxic fumes. This functionality must have different reliability and availability measurements and targets. Loss of availability will, in this case, reduce the safety level on demand. Under a demand, the ventilation system is also required to function a certain time period given a design fire intensity. This illustrates how demand mode impacts the choice of suitable availability targets

It is important to also state requirements and targets for the availability of the new safety related technology in a qualification process. Such requirements must take into consideration, not only the unavailability related to the reliability of the system, but also testing, spurious trips and maintenance.

3.5.2 Maintainability and testability

Maintainability is a feature related to the design of the system and describes how easy or difficult it is for an item to be maintained or repaired. This feature, just as safety, reliability and availability, is interconnected and dependent on the other RA(M)S features of the system. Maintenance is defined as the technical and administrative actions intended to retain an entity in, or restore it to, a state where it can perform its required function (IEC-60050-191, 1990). The maintainability of an item can significantly affect the availability and the lifecycle cost of the equipment. As such, maintainability must be considered as one of the requirement attributes when qualifying new technology.

Maintainability and testability requirements are, just as availability requirements, dependent on the demand mode of the system. Systems operating on continuous demand will perhaps be tested to see if the capacity or performance is maintained. For example, an engine that

runs continuously would be tested to see if the engine still produces the required effect. The maintainability is perhaps also more important for continuous systems, and needs more attention, due to the constant operation and associated downtime. For on-demand systems, testability also involves testing the required safety function to see if, and how, the system reacts in the occurrence of a demand, in addition to the performance of the function. The time and easiness of this attribute influences the systems overall protection capacity. As such, maintenance and testing are key activities to ensure that the SIS attains and upholds the desired performance.

3.5.3 IEC 61508 for Technology Qualification

This section will dicuss how the scope, and different requirements, aspects and phases from IEC 61508, can be of relevance in respect to qualification of new technology. Some of the main similarities and interfaces between the IEC standard and the different technology approaches, introduced in chapter 2, will be discussed, and aspects from IEC 61508 that can supplement a qualification framework will be identified.

Risk-based

The first important parallel between IEC 65108 and the qualification approaches is that they share a risk-based foundation in their efforts to address performance targets and requirements. This means that both the methods for stating reliability and safety integrity requirements in IEC 61508, and the qualification processes as described in DNV-RP-A203 and API-RP-17N, are rooted in risk analyses and assessments. The qualification processes in DNV-RP-A203, API-RP-17N and the safety lifecycle per IEC 61508 all involve an early risk analysis phase with the same objective; identifying failure modes for the system or technology.

Requirements

Another important aspect is how the methods for stating and allocating functional and safety integrity requirements in IEC 61508 can be used to form and develop a qualification basis in the qualification process. Safety integrity levels may be considered the same as what a qualification process calls “a desired confidence level” (DNV, 2011). The desired confidence level is stated

in the qualification basis, and the qualification effort shall determine whether or not the necessary level of reliability and other performance measures has been reached to meet the selected confidence level or safety integrity level. Other measures such as safe failure fraction (SFF) and spurious operation rate (λ^{SO}) may also be stated as requirements in the qualification basis.

Safety Lifecycle as Qualification Guideline

The safety lifecycle approach, which the IEC 61508 standard is based upon, can in itself be used to qualify new safety instrumented technology. The standard provides methods to derive and state both functional safety and safety integrity requirements, in addition to verification methods to quantitatively verify that the equipment and testing meets these requirements.

Systematic, Documentation and Operational phase

The IEC 61508 standard's systematic approach towards stating requirements and assessing functional safety can be a key supplement for a qualification framework. Especially for qualification of safety instrumented systems. The standard also has a well-established set of requirements for documentation throughout the development phases. A well-functioning qualification framework should also incorporate requirements for documentation, and can follow the requirements stated in IEC 61508. Another aspect of IEC 61508 that can supplement a qualification framework is the focus on the operational phase, which the qualification approaches usually to some extent have little focus.

Chapter 4

Technology qualification and RAMS in the NPRA, central aspects and challenges

The NPRA has adopted technology qualification as an overall approach for ensuring and demonstrating that the different fjord crossing concepts being considered in the ferry-free E39 project satisfies the necessary requirements. The project, which involves development of completely new bridge design concepts, challenges the way the NPRA traditionally addresses their road projects. This also includes risk and uncertainty management. As a way to implement a systematic, structured and holistic mind-set towards managing risk and uncertainty, a technology qualification framework has been identified as key tool for decision-making in the NPRA.

The NPRA has mainly focused on a combination of the approach in DNV (2011) and a TRL scale approach to develop a qualification framework for the E-39 project.

Several challenges must be faced in order to implement a qualification framework in the NPRA. The framework must be tailor-made and adjusted to fit into the general operation and development practices in the agency. The scope and role of the framework must also be defined. This chapter will outline some of the central aspects concerning an implementation of such a framework in the NPRA and some key challenges for qualification of the concepts considered for the E-39 project. Some thoughts and recommendations from the author on the different challenges are also included.

4.1 Defining Role and Scope of Technology Qualification

Technology qualification is in all aspects new to the NPRA, and a central challenge in the development of a qualification framework is to define what role, or place, the framework should have in operations and development projects. The work of adapting a qualification framework in the NPRA is still in an early stage, and different expectations exist within the agency concerning what sort of role such a framework should play and what the scope should be (Johansen, 2016).

An important task early in the development of a qualification framework is to clearly define the NPRA's needs in order to define and delimit the concept of technology qualification for the NPRA. One of the incentives for implementing a qualification framework in the NPRA is to achieve a more systematic and holistic mind-set towards risk and uncertainty. Foremost, the motivation is to have a systematic approach towards ensuring that the fjord crossing concepts inherent the desireable attributes and meets the necessary requirements. The framework must also be systematic in respect to documentation and demonstration to build confidence in concepts. This is particularly relevant in the early phases of technology development projects in order to empower strong decision-making. By looking at the need and motivation for the framework it is easier to define the scope and characteristics of a qualification framework. Like any other implementation of a new concept, it is important with unambiguous and clear-cut definitions of key terms. For example, the definition of what is considered proven, or unproven, technology. Different assessments might conclude differently on this matter because of dissimilar interpretations of the same definition.

This might be one of the main problems related to technology qualification. Programmes, approaches, frameworks, processes and definitions are often too fuzzy and indistinct, but at the same time based on solid and sensible principles it is hard to disagree with. For the NPRA, who employs a large number of contractors and suppliers, it is crucially important to at least have an unambiguous and unmistakeable foundation in form of definitions.

Johansen (2016) points to several important aspects to address when developing a framework for technology qualification with respect to the E-39 project. A central part of the paper is concentrated around delimiting and defining technology qualification to differentiate the concept from similar operations and processes. Among the highlighted features are:

- Focus on qualifying the systems, not only new/novel technical components or subsystems. A wide-ranging approach is desirable. The object of qualification is the technical systems, not the technology development process. This involves assessing the interfaces and interactions between the different components and subsystems constituting the system

- A clear distinction between technology qualification and quality assurance. Technology qualification stresses risks, not just quantitative requirements, and strives to produce a measurable statement of confidence in the finished product. Technology qualification processes and activities are in itself subjects to quality assurance and control. Quality assurance may be seen as reactive process (ensure that the right activities have been done correctly), while technology qualification may been seen as a proactive process (ensure that right activities will be done correctly).

- The distinction between a qualification framework and project management frameworks. The idea is not that technology qualification should drive the development processes, but provide inputs and decision arguments in such processes.

- Technology qualification should not be seen as an overall risk-based decision-making framework, but as a key tool to make risk risk-based decisions.

- RAMS (reliability, availability, maintainability and safety) assessments can be used to raise confidence in technology development, but are not the same as technology qualification. Technology qualification involves the entire development process, not only the assessment of RAMS-performance. The qualification process addresses uncertainties in the RAMS performance of the new technology, while RAMS management and assessment methods supplement the qualification process with methods to establish acceptance criteria.

As such, technology qualification is not to take the role as an overarching risk, quality, management or development framework, but as a development process tool giving inputs and decision basis to other, more general, project processes.

Another central aspect to consider is which attributes of the systems that should be subject to qualification. Conventionally, TQPs have been concentrated around, and related to, the reliability features of the technology(the ability of an item or system to carry out a specific function). However, reliability can be a complex concept, and there are more than one definition of reliability (see Ben-Haim (1995) and Ben-Haim and Elishakoff (1995)).

When dealing with extreme fjord crossing concepts, it is understandable that other attributes of the system may be included in the qualification process. The fjord crossings involve special uncertainties and challenges, which may make the scope of existing frameworks for technology qualification too narrow. In such a way, the traditional concept, or scope, of technology qualification may need to be extended. Among the different attributes that may be included are:

- Structural Reliability
  - Probability of failure of entire systems, elements and components
  - Life length
- System reliability
  - Probability of failure of systems and components
  - Interaction and dependability between systems
  - Life length
  - Fail-safe
- Availability and uptime
  - Planned and unplanned unavailability
  - Vulnerability in respect to failures
  - Durability
- Maintenance, maintainability and testability
  - Preventive and corrective maintenance
  - Detection of failures
  - Cost of maintenance
  - Testing and inspection opportunities
- Risk and safety

  - To the structure
  - To the public
  - To the operation and maintenance personnel
  - Accident management
  - Vulnerability
- Environmental impact
  - During construction
  - During operationial life time
  - During refurbishment and maintenance
  - During decommissioning
- Potential
  - For upgrades
  - For other functionalities and usage
  - Other exploitations

This being said, it is the opinion of the author that a clear distinction should be made between technology qualification as a tool to build confidence in a concept/system, and a complete tool for selection and assessment of different concepts. This does not mean that a technology qualification cannot give valuable input to a more overarching concept evaluation framework. Maturity and readiness assessment may be important aspects in such a evaluation, but should not be the sole method of conclusion.

If the concept of technology qualification drifts too far off from all other industry practices and notions of the concept, it may become difficult to ensure mutual understanding with contractors and knowledge exchange between other technology qualification actors may become challenging. Hence, technology qualification should not be made too complicated and resource demanding. In addition to the reasons mentioned above, it is important that the concept is compressed enough to ensure sufficient quality of the technology qualification deliveries.

4.2 RAMS

A central part of any qualification framework is to show conformity with various performance targets and requirements. These requirements can often be classified as RAMS performance requirements. RAMS engineering as a discipline can be applied to technical systems as well as road and critical infrastructures. A newly introduced highway can be regarded as a newly-introduced system interfacing with other existing systems and compromising several subsystems. RAMS engineering and assessment are necessary in all phases of the overall lifecycle of the system.

Even though the Norwegian National Rail Administration (NNRA), and many other international railway organizations have addressed the introduction of RAMS management in an effort to improve the operational effectiveness, the NPRA has limited experience working systematically with implementing RAMS management and engineering principles.

Based on the railway specific standard of IEC 61508 (EN-50126, 1999) the NPRA has started to develop some guidelines and work papers to address RAMS aspects in road engineering and projects. A manual for RAMS management for road tunnels has also been developed, but the document focuses mainly on the maintenance perspective and does not address a complete RAMS approach (NPRA, 2015).

It is the opinion of the author that the limited insight within the NPRA regarding RAMS management and engineering might hinder a potential development of a technology qualification framework. A well-established framework for RAMS management would have aided the development by giving guidelines towards establishing and verifying performance requirements. A RAMS framework would also provide an unambiguous approach towards addressing minimum safety levels (risk accept criteria), and methods for assessing the performance of components, subsystems and entire systems in light of such safety levels.

4.3 Project Development Model

A qualification process must be addressed prior to, and in parallel with, the overall project development process. This implies that the project development model needs to be suitable and adequate to act as a base for an efficient and practical qualification process. Such an approach

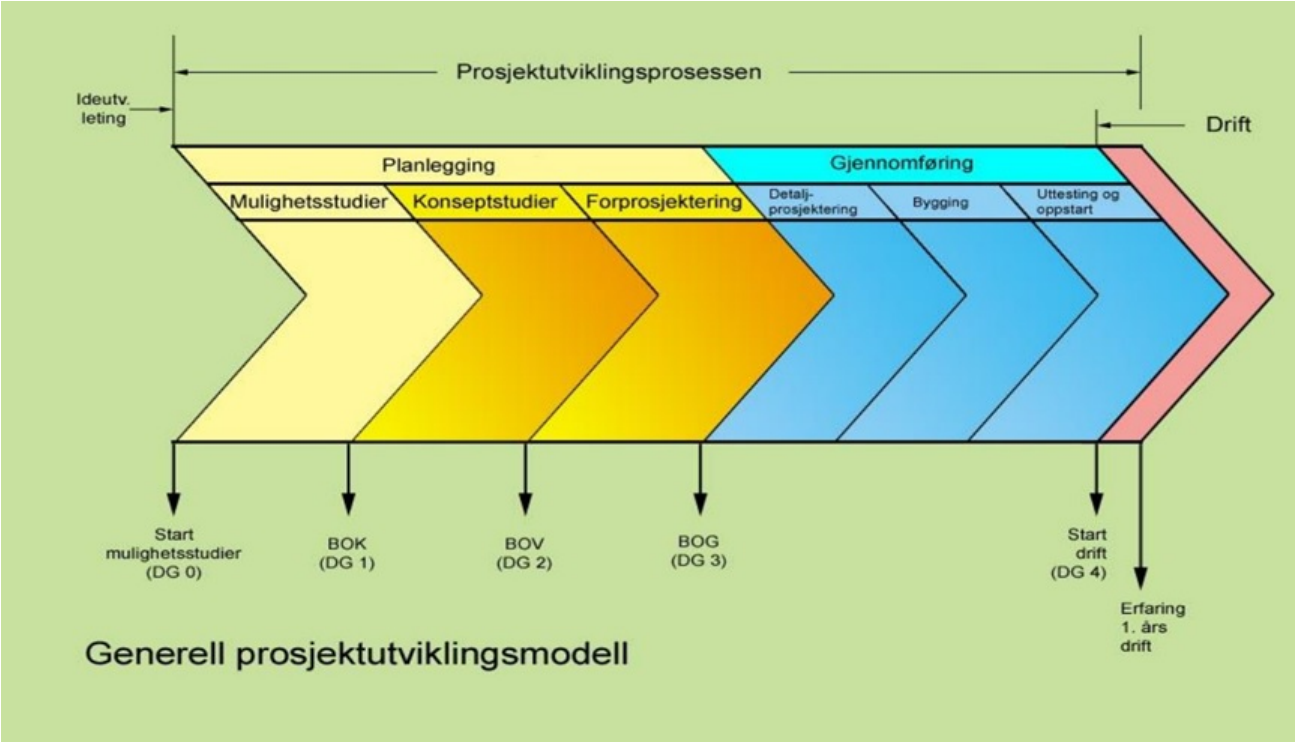

Figure 4.1: The project development model. From NPD (2013).

makes the qualification process functionally linked to the different key stages, phases and decision gates in the development model. The NPRA has two main manuals, or guidelines, for project management and planning, namely V710 “Project Overview Planning” (NPRA, 2000) and V760 “Management of Road Projects” (NPRA, 2012). These manuals are comprehensive, but outlines no uniform and clear-cut project development model to which a qualification process may be based upon. A new development model has therefore been proposed based on the general project development of the Norwegian Petroleum Directorate (NPD) with decision gates that contain political and technical content (NPD, 2013) (see figure 4.1). The model described by the NPD is fairly general, but may be adjusted to fit the NPRA’s needs and acts as a unifying functional phase model. Most important for the NPRA is the alignment of critical planning milestones, such as municipal sector plan and zoning plan, and decision gates in the project development model. A modified model is presented as part of the proposed framework for qualification of safety instrumented systems in chapter 5.

4.4 Standards and Requirements

Technology qualification is all about building confidence in the technology solution by showing compliance with various stated requirements and performance targets. A special challenge for qualification of the fjord crossings in the E-39 project is the combination of bridge, tunnel and offshore technologies. The combination implies that rules and standards from all the mentioned fields are relevant. This constitutes a challenge with respect to development of qualification basis. The design basis of the strait crossing concepts is based upon standards including; NPRA manuals, Eurocode and NORSOK standards. This patchwork of rules and design regulations creates uncertainty with respect to both potential deficiencies and inconsistencies, in addition to how applicable the requirements and regulations are in an overall system-perspective

There are also differences between the different rules and standards relevant for the strait crossing concepts. While some of the standards, like the standards adapted from the oil and gas sector, contain both specific functional requirements and quantitative performance requirements, other documents, such as the NPRA manuals, are mainly descriptive in nature. It would seem rational that this difference between the standards would mean that they could complement each other, but this is not the case given that the standards cover different issues. The NPRA manuals, which constitute much of the design requirement foundation, primarily describe specific solutions, rather than what functions or qualities the different solutions should hold. Nor is it always clear what sort of prerequisites that form the basis of the stated requirements. An illustrating example may be found in NPRA manual N500 “Road Tunnel Engineering” (NPRA, 2014). The technical requirements for tunnel ventilation cover, for instance: maximum noise level from the fans, how long the fans should be functioning given a fire intensity and requirements for air quality. Requirements regarding, for instance, failure frequency of different failure modes are nowhere stated in the manual. Neither on system nor component level.

A framework for technology qualification for the NPRA and the E-39 project should clearly state what are considered applicable rules, requirements and performance targets for a qualification basis, or a good description on how to develop them. The qualification basis is the foundation for all the later activities in a qualification process and is the benchmark against which the success of the performance of the technology is measured. Hence, emphasis should

be put on assuring a categorical requirement specification policy.

4.5 Breaking Down the Fjord Crossing Concepts

Another central challenge concerning qualification of the extreme fjord crossing concepts concerns how to assess the entire concepts on a system level, and how to decompose the different elements. The different bridge concepts can be categorized as systems composed mainly of subsystems/elements that are proven in other application fields. An example to illustrate is this composition for the SFTB is the truss towers designed to connect the floating pontoons to the main tubes. This concept is similar to various jacket structures for offshore platforms. However, further decomposition of these systems may reveal new or unproven components, like a new connection solution between the tube and the truss towers.

This implies that there exists a challenge when breaking down the concepts into smaller and more manageable elements. When breaking down a system like this, uncertainties also arises related to the functional interfaces and interactions on a global system level. A possible solution to address this challenge might be to implement a form for interaction and system readiness level (IRL and SRL, see section 2.1.1) assessment in a technology qualification framework.

4.6 Other Implementation Challenges

The development of a well-adjusted framework for technology qualification is only one of the challenges related to implementation of technology qualification in the NPRA's technology development projects, like the E-39 project. The technology qualification process represents a relatively high time and resource consumption. As all government allocations, this extra expense must be defensible through the potential gains regarding the level of confidence and safety of the technology. Another central challenge is to alter the mainly descriptive mind-set, or non-functional perspective dominating the current operation, to a systematic and functional approach. To change a well-established mentality in an organization, such as the NPRA, is no easy undertaking, and may involve several complications.

Chapter 5

Framework for Qualification of Safety Instrumented Systems

5.1 Properties of the Framework

By studying the basic principles and objectives of technology qualification, functional safety per IEC 61508, and the NPRA's needs and practices, several key aspects can be identified and combined to form a qualification framework for safety instrumented systems. This section will present the key principles and properties of the technology qualification programme introduced later in this chapter.

The framework for technology qualification of safety instrumented systems in the NPRA builds on the following principles and properties:

A combination of approaches :

To best achieve a qualification programme suitable for the NPRA and safety instrumented systems, different aspects from different qualification approaches have been combined. This includes a maturity-oriented approach building on the technology, integration and system readiness levels (TRLs, IRLs and SRLs) (Sauser et al., 2006, 2008), and a systematic and process-oriented approach inspired by DNV (2011). The purpose is to form a framework building on the most attractive features from the different approaches, and yet ensure a practical and cost-efficient approach.

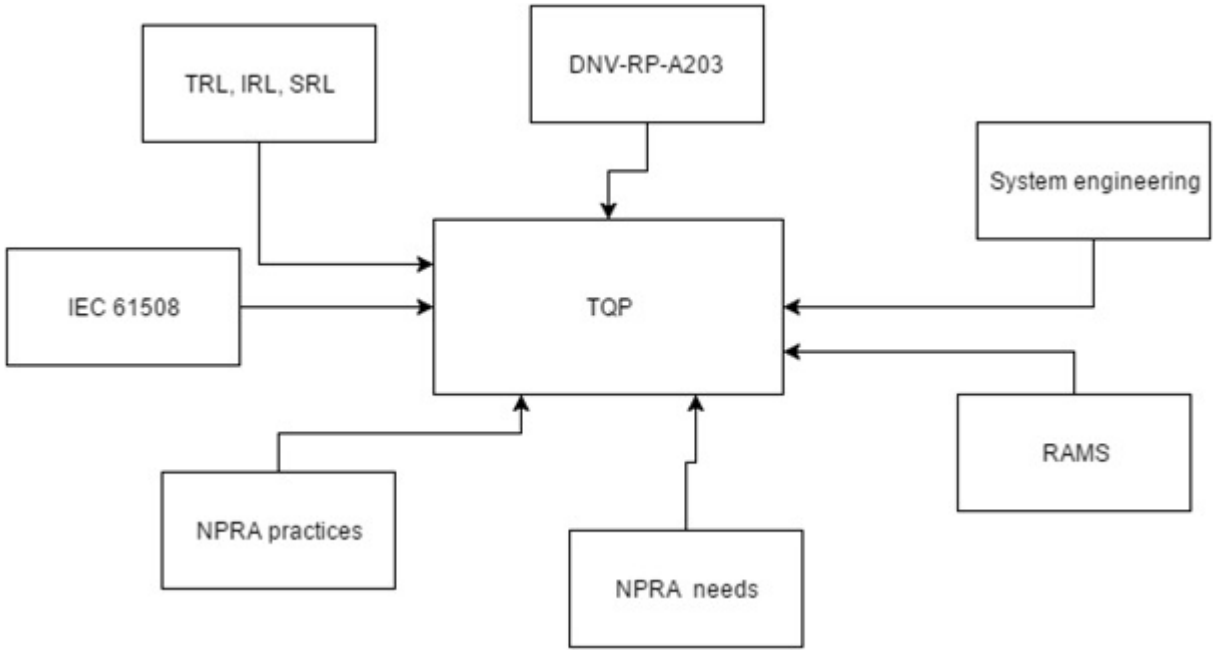

Figure 5.1: Illustration of the elements giving inputs to the qualification programme

Inspired by the safety lifecycle and system-engineering principles :

To be applicable and specific for safety instrumented systems, the qualification programme is primarily developed based on the analysis phase of the safety lifecycle per IEC 61508, covering specifications of safety requirements, design and development of safety features. The framework also considers systems engineering principles, such as system function analysis, system structural analysis and system complexity management (Johansen and Rausand, 2014), that can be applied to any system, even intricate and complicated ones (Kossiakoff et al., 2011).

Directly aligned with the new project development model :

To ensure optimal functionality of the framework, the qualification progress and the SMLs, which indicates the maturity of the system, are interlinked with the different key stages, phases and decision gates in the project development model (see section 4.3). It is imprtant to establish for each phase what level of maturity is considered "mature enough" to reach the phase objectives. This is important to identify the needs for modification in the design as early as possible (Rahimi and Rausand, 2015). It also makes it more clear what the qualification programme needs to deliver at different points in the development

process to provide the necessary decision support at each phase.

Risk-based and RAMS-oriented :

Both IEC 61508 and DNV-RP-A203 are focused around a systematic identification, and assessment, of hazards and risks. For the NPRA to be confident in any safety critical system, it is important that the decisions and overall process have addressed risk, and proved the concepts to meet the safety levels and be safe to the public. A risk-based approach involves a methodical identification of hazards and uncertainties, analysis of causes and consequences, and assessment with suggestions to risk and uncertainty reducing measures. It is important to view risk from a holistic RAMS perspective considering how the different RAMS attributes affect each other. Overall RAMS management will be able to provide inputs to the qualification programme, and the qualification programme can be seen as an integral part of a RAMS framework in the NPRA.

Proactive :

The qualification process shall be an integrated part of the design and development with early involvement in the development process. Analyses, tests and assessments in the qualification process will provide the basis and inputs for design solutions and requirements.

Model-based :

To deal with the complexity of systems, a model based approach is important. Models shall be developed on different levels (operational, system, component) to understand the different inputs and outputs of the systems, and how safety instrumented systems operate and interact with other systems to keep a safety level according to the principles of system architecture (Blanchard, 2008; Martin, 1996). A model based approach that provides a better understanding of the system and will facilitate a system qualification process, not only qualification of different elements or components. What models to use for describing the system depends on the nature of the system and its complexity.

Unambiguous :

An important feature of the framework is that it provides clear-cut and distinctive defini-

tions. It provides specific propositions to what sort of models, analyses and requirement prerequisites that can be considered valid. The purpose is to provide a framework that can be applied for qualification of all safety instrumented systems in the NPRA, and reduce possible misinterpretations and confusion.

Not just reliability based, but still not all-encompassing :

The framework considers several system attributes subject to consideration in addition to the traditional reliability focus. The purpose is to include more attributes is to provide additional confidence in the systems by gaining a more holistic view of the different contributors to uncertainty. Relevant attributes for SISs are primarily related to the different RAMS properties. It has also been focus on not making the framework "all-inclusive". The qualification programme shall be part of the design and development process, but not be a complete management tool for selection and assessment of the systems.

Iterative :

The qualification process is composed of several clearly defined steps described in a flow chart. With each defined stage in the development process, the process is repeated with an increasing level of confidence.

5.2 Qualification Framework

This section presents and outlines a proposition for a new framework for technology qualification of safety instrumented systems in the NPRA. The framework reflects the properties described in section 5.1. The framework will provide some new definitions and practical models. It is important to specify the terminology of system, sub-system and components used in the framework for safety instrumented systems. This is illustrated in figure 5.2.

5.2.1 Introduction to New Concepts in the Qualification Framework

Uncertainty Registers

An uncertainty register is similar to a risk register commonly used in oil and gas industry. A distinction is made between an uncertainty register on the component level, and on the system

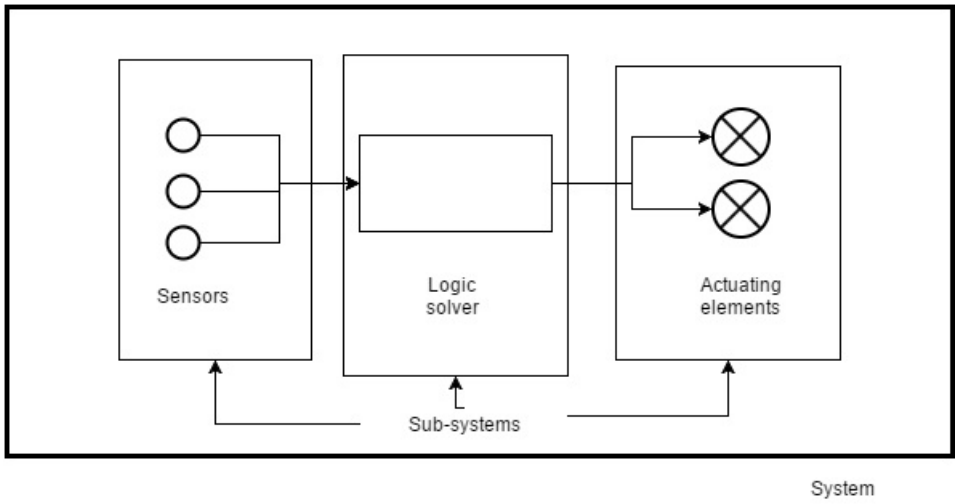

Figure 5.2: Illustration showing the classic definition of system, sub-system and elements for safety instumented systems

level. The registers contain an identification of uncertainties with descriptions and are “living” documents which are updated throughout the development process. The objective of the qualification process is to mitigate or eliminate the uncertainties in the uncertainty registers.

The register on the component level should include information about the following

- Description of the uncertainty
- Cause of uncertainty
- Effects of uncertainty
- Degree (probability and criticality)
- Relevant mitigation strategies

Table 5.1 shows an example of an uncertainty register on the component level.

Based on the component uncertainty register, a separate uncertainty register shall be compiled on the sub-system level. The register on the sub-system level should include information on more general uncertainties and uncertainties due to interfaces and interactions between the components. The purpose of compiling uncertainty registers at both levels (component and sub-system) is to first assess the uncertainties independently on the component level, and then assess the uncertainties from a broader perspective taking into account dependencies between

Table 5.1: Uncertainty register example.

ID	Description	Cause	Effect	Probability	Criticality	Mitigation measures
U-1	Uncertainty regarding fire resistance of AID camera casing	New operational conditions, not tested for fire of larger dimensions, design errors etc...	Reliability and safety function impaired, large fires will not automaticcaly be detected etc...	Small	Large	Conduct tests of higher fire magnitude, good design documentation, etc...

the uncertainties. Important aspects of the uncertainties may be overlooked by not looking up and assessing the situation from a wider perspective. To achieve the necessary perspective, the break-down used in the uncertainty assessment shall reflect the system structural analysis done in step 2 of the qualification process.

Novelty Classification

Based on the uncertainties identified and documented in the uncertainty registers, an overall evaluation shall be made regarding the novelty of the technology on a sub-system level. The purpose is to identify which sub-systems that need an full qualification process, and which sub-systems that only require a basic qualification process. The novelty classification also functions as a tool to compare and scale different sub-systems and solutions. This framework proposes a definition and method for categorizing the technology based on the procedure described in DNV (2011).

The novelty of the system is based on the total uncertainty associated with the technology. The classification should be based on the components with the highest uncertainty degree in addition to the degree of the uncertainty identified on a sub-system level. A proposed rule for this purpose could be to add a quantified measure to the degree of uncertainties and summing up the total uncertainty for each sub-system.

A technology might be considered novel due to uncertainties concerning the “newness” of the technology itself and its application area. A new categorization matrix for classification of technology novelty is proposed. The matrix is an extended version of the categorization table

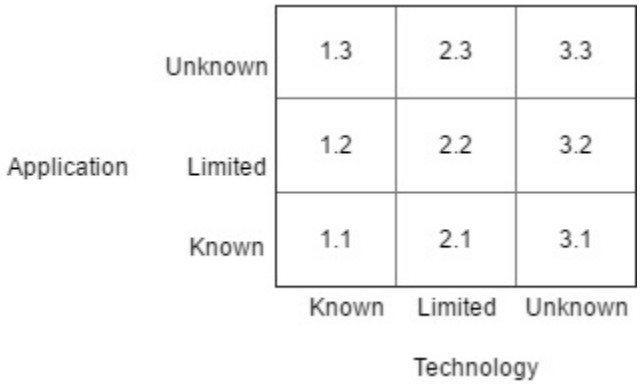

Figure 5.3: Extended classification table/matrix for novelty classification

in DNV (2011) (shown in section 2.1.2) with the same dimensions. The new classes of novelty are introduced to give further and more detailed inputs to the qualification plan. The approach in DNV-RP-A203 does not distinguish the classification between the dimensions (e.g. a classification of "3" does not fully explain if the uncertainties stem from the application, degree of novelty, or both). It is the opinion of the author that knowing more specifically where the novelty of the technology is rooted would be helpful towards development of a qualification plan.

In this categorization only category 1.1 is considered proven technology. To more precisely categorize the technology, and reduce the chance of misinterpretations, a definition of what is known, limited and unknown is introduced:

Technology :

Known: Well-known technology with documented field experience and well-defined structure. The technology is well-covered in acknowledged standards.

Limited: Technology with a limited field history, partly covered by acknowledged standards, or not fully documented or specified.

Unknown: No documented field history, not covered in acknowledged standards, not established as safe by evidence or demonstration.

Application :

Known: The user has previous experience with the technology in operation. The technology is proven in the given environmental and operational conditions.

Limited: The user has limited experience with the technology. It is proven in similar environmental and operational conditions.

Unknown: Technology is new to the industry and has no history in the given, or similar, environmental and operational conditions.

Basic Qualification Process

The basic qualification process is a simplified qualification procedure for sub-systems regarded as proven according to the novelty evaluation. It is important to not neglect these sub-systems in an overall evaluation, since the interaction between the sub-systems must also be taken into consideration. The basic qualification process should at least include the following activities:

- Verification and validation of potential previous qualifications and certifications considered relevant for the specific application and user.
- A novelty screening to ensure that the novelty/maturity is unchanged.
- Collection of documentation of evidence and field history of the technology.

Integration Maturity Levels and System Maturity Levels (IMLs and SMLs)

The integration maturity levels (IMLs), inspired by the integration readiness levels (IRLs) indicates how the sub-system interacts with the other sub-systems to carry out a certain SIF. This is a scenario-dependent (dependent on the environmental and operational conditions) measure which gives input to the overall system maturity level (SML). The purpose of including a IML scaling for the sub-systems is to address the integration aspect of the SIS's development more thoroughly and contribute to the objective of viewing the qualification from a overall system perspective. The idea is that a IML is assigned to every "direct link" between the sub-systems. For a SIS, this can be explained quite straightforward:

A IML is stated for the integration between the sensor/detection sub-system and logic controller sub-system, and another IML is stated for the integration between the logic controller sub-system and the final/actuating sub-system

Table 5.2: Integration Maturity Level.

IML	Definition	Requirements
IML1	Interaction and interface identified with sufficient detail to describe and specify how the sub-systems relate to each other.	The lowest level of integration. Evidence exist to describe how the sub-systems influence each other as parts of a larger system.
IML2	Compatibility (communication) between the sub-systems exist and can be sufficiently specified.	IML2 represents that the sub-systems can communicate interpretable data. This level ensures that the sub-systems can interact efficiently through the communication connection
IML3	Compatibility between the sub-systems involves control.	The specific information sent between the sub-systems are identified and specified. The information flow is sufficiently detailed to map how the sub-systems interacts to carry out specific functions in different operation conditions
IML4	Integration is verified and validated with sufficient detail. Integration qualified.	This involves evidence showing that the sub-systems have demonstrated sufficient compliance with integration and performance requirements. The sub-systems have been observed functioning together in the relevant environment with a sufficient level of confidence.

The system maturity levels are inspired by the system readiness levels (SRLs) (Sauser et al., 2006, 2008), and the technology maturity levels (TMLs) introduced in Johansen (2016). Unlike the SRLs, but similar to the TMLs, the SMLs are not quantitatively calculated. The system is rated a system maturity level on background of a collective evaluation of the results from the qualification process, other relevant inputs, and the IMLs. The SMLs are linked to the different decision gates and design phases in the project development model. It is the intention that the SML is to substitute TRL/TML as an indication measure to a technology/system's maturity. The choice to include the term *system* is deliberate to emphasize the need of a system perspective.

Four different IMLs and five different SMLs are defined for this framework. The IMLs and SMLs are presented in table 5.2 and 5.3. The IML and SML scales in this framework are described for the purpose of qualifying SISs, but there should exist no reasons why the idea of IMLs and SMLs could be modified and used for qualification of entire bridge concepts or "other systems". All requirements stated in the SML table (table 5.3) applies to the entire system.

A SML4 indicates that the system is proven and ready to be implemented. The connection between the decision gates in the project development model and the SMLs are illustrated in

Table 5.3: System Maturity Level.

SML	Definition	Requirements
SML1	System concept defined	• System functions and interactions defined and described. • Interfaces with other systems described. • Environmental and operational conditions described. • Basic Risk reducing and RAMS performance properties described. • Risk reducing and RAMS performance requirements demonstrated analytically. • Design basis established.
SML2	System concept specified and validated	• System functions and interactions specified and demonstrated • Interfaces with other systems shows compatibility (IML2 is reached). • Risk reducing and RAMS performance requirements are defined, calibrated and validated. • Methodology validated numerically/experimentally. • Environmental and operational conditions known and analyzed. • Construction principles and implementation plan recognized.
SML3	Design and Integration validated	• System requirements allocated and validated analytically or experimentally. • Integration successfully tested in laboratory conditions • Construction and implementation plan specified and validated. • System design verified by function/performance testing in relevant environment.
SML4	System Accepted	• System requirements and acceptance criteria has been verified internally and by third party with a sufficient level of confidence. • Integration qualified. IML4 is reached • Construction and implantation plan approved by the NPRA.
SML5	System constructed and installed	• System constructed in compliance with requirements and construction specifications • System successfully implemented and integration verified by operation test
SML6	System proven in operation.	• System has been proven to function according to the safety and reliability requirements over a period of a year. • System has been proven to function satisfactory in a real demand situation. • Potential improvements have been documented.

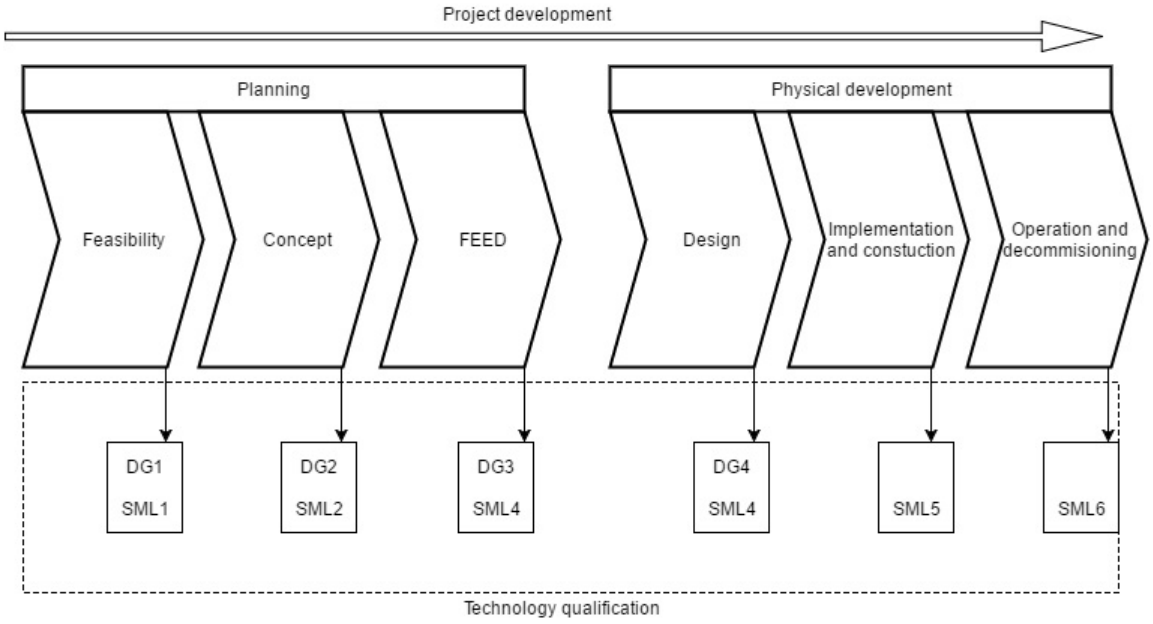

Figure 5.4: Illustration showing the decision gates in relation to the project development mode and the SMLs

figure 5.4. The project development model in figure 5.4 differs slightly from the general model described in NPD (2013) and the model suggested in Johansen (2016). The development model and the links with the decision gates and SMLs takes primarily into account the qualification of SISs, but can be modified to serve as a general development model for bridge, tunnel and other road projects in the NPRA. Only SML1 to SML4 are directly connected to decision gates in the development model. This is however an example model and the model presented in figure reffig16 does not necessarily reflect the realistic development scenario in the NPRA.

The different decision gates for development of safety instrumented systems are defined as shown in table 5.4

5.2.2 Practical Approach

The flow chart in figure 5.5 illustrates the steps in the new proposed qualification process for safety instrumented systems in the NPRA. The general qualification process is adapted from DNV (2011), but with some adjustments to make the qualification process more focused on qualifying safety instrumented systems and better suited to be applicable for the NPRA. This

Table 5.4: Decision gates.

DG	Description
DG1	Decision about need for system
DG2	Decision about choice of system concepts
DG3	Decision about detailed concept choice
DG4	Decision on implementation

includes inspiration from the safety lifecycle per IEC 61508, the framework for technology qualification of extreme fjord crossings proposed by Johansen (2016), the SRL approach described by Sauser et al. (2006) and RAMS engineering theory. The process has an iterative nature with an internal feedback loop. At each decision gate in the process is repeated with an increasing level of precision. This implies that the system must be "qualified" at each milestone in the project development model according to the newly introduced system maturity level (SML) requirements (see section 5.2.1).

The initial risk analyses and assessments, and the established rules and regulations, provides the point of departure for the qualification process. The risk analyses and assessments, or the rules and regulations, underlines the need for the safety instrumented functions and systems, and determines risk reducing performance required of the system.

The main steps in the qualification process are described as follows:

1. Initial Assessment of Qualification Foundations

An important first step in the qualification process is to identify uncertainties related to the qualification process itself. For the NPRA, much of the uncertainty is not related to the "technical qualification", but to the novelty of the qualification foundations. These uncertainties affect the viability of the process and must be addressed prior to the "technical qualification process".

The objectives of this step is to determine uncertainty and novelty related to:

Standards and requirements

For any systems subject to qualification, it is important to have a sufficient basis of standards and requirements that forms the acceptance criteria for the qualification. Uncer-

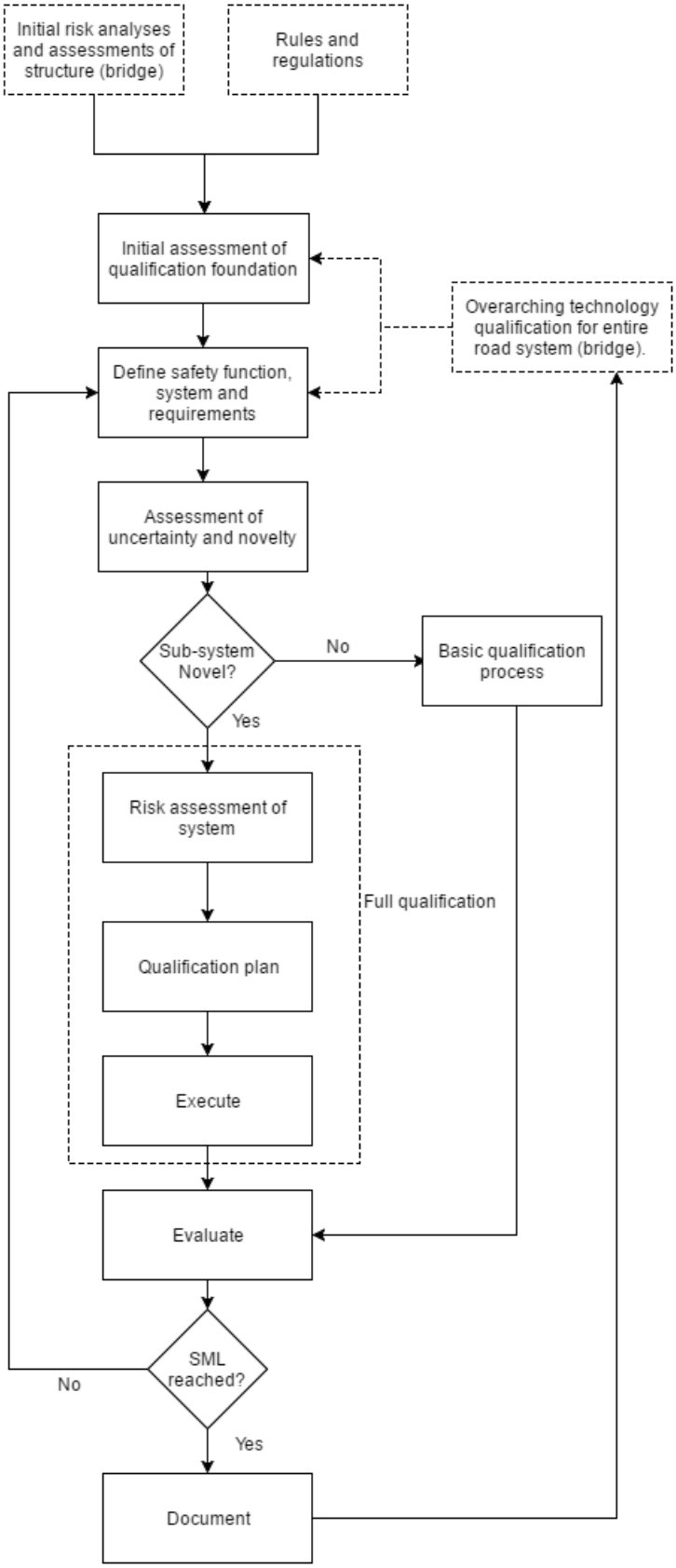

Figure 5.5: Process of technology qualification

tainties may rise from the appropriateness of the requirements, or potential omissions or inconsistencies. This can be summarized into the question "Are we able to state the relevant requirements for the system?". An example, is to be able to develop and state risk acceptance criteria for the system. Today, there is no clear-cut and uniform principle regarding this in the NPRA. For a risk-based qualification programme, this is something that needs to be addressed in advance of the technical qualification.

Environmental and operational conditions

Uncertainties related to technology or system might be owed to the technology being used in new environmental and operational conditions. However, the system's environmental and operational conditions, and how they may change over the system's lifetime, might also be subject to uncertainties. For the ferry-free E-39 project, there exist several uncertainties regarding the environmental conditions for the new extreme fjord crossing concepts. The bridge concepts also makes up the environment for the different safety instrumented systems to be implemented. Sufficient information and understanding of the environmental operational conditions are important to facilitate the rest of the qualification process.

Analyses and methodologies

Another aspect that needs to be considered is the uncertainties related to the system analyses performed throughout the qualification process. This applies to the basic data used in the analyses, and the models and methods themselves. Before the different analyses, models and methods are applied, the uncertainties related to how certain it is that the models and methods can provide appropriate evidence must be addressed. How much experience the NPRA has with the analyses and methods also must be assessed to determine how much third party or hired expertise that is needed to carry out the qualification.

2. Define Safety Function, System and Requirements

The first and most important step in the technical qualification process is to develop the fundamental basis for the rest of the steps in the process. This first step has two main objectives:

1. Define/redefine the safety system's structure, safety function(s), demand mode, boundaries, sub-system and component interfaces, and environmental and operational conditions.

2. Define/redefine and establish functional and non-functional performance requirements and acceptance criteria.

The first objective involves a complete description of the system. To start with a system description is inspired from the safety lifecycle per 61508. The system shall be described through text, illustrations, flowcharts, diagrams and other relevant documents. Models shall be complied to understand the inputs and outputs of the system and sub-systems according to the model-based approach described in section 5.1. The descriptions and models shall contain the functional safety requirements, stating what the system is required to do, and give sufficient understanding of the system to enable all the other activities in the qualification process, such as the risk assessment, to be satisfactorily carried out. The functional safety requirements shall contain what sort of hazards the system protects against and how it works to carry out these functions.

The second objective shall express the performance requirements stated for the system and components. For safety instrumented systems, the following quantitative performance requirements should be stated:

- Average probability of (dangerous) failure on demand (PFD_{avg}) (on-demand systems/functions)
- Average frequency (per hour) of dangerous failures (PFH) (Continuous demand systems/functions)
- Spurious trip rate (STR)
- Useable lifetime requirements (e.g. 20 years)
- Dimensional and conditional design requirements (Temperature, humidity, etc.)
- Demand length requirements (e.g. must provide protection for 1 hour, etc.)
- Activation time (on-demand systems)
- Operational availability

An overall safety integrity requirement in the form of a safety integrity level (SIL) should be stated. The safety integrity requirements can be derived from the sector specific versions of IEC 61508 or other database collections such as OREDA, given that the system or component are covered in such documents. If the system or component is not covered in the sector specific standards, new requirements must be stated and allocated in accordance to the methods and guidance in IEC 61508. Several different methods can be used for this purpose:

- Overall risk criteria
- Risk graph (calibrated)
- Layers of Protection Analysis (LOPA)
- Event tree analysis

The preferred method for projects in the NPRA should be to derive SIL requirements from an overall risk criteria. This method draws on the risk identified in the initial risk assessment of the road structure (bridge). The initial risk does not take in to account the different risk reducing measures and safety barriers. The SIL requirement is derived from the risk reduction needed to meet the risk acceptance criteria. Figure 5.6 illustrates the relationship between initial risk, risk accept and necessary risk reduction in form of SIL requirement.

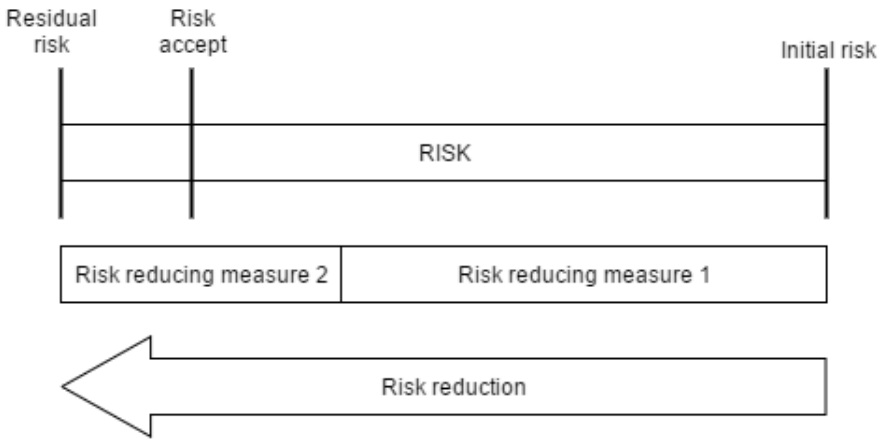

Figure 5.6: Initial risk, risk accept and risk reduction

3. Assessment of Uncertainty and Technology Novelty

The third step in the process is an assessment step to evaluate the uncertainties and novelty related to the technology on both component and sub-system level (see section 5.2.1). Two main task shall be conducted:

1. Uncertainty registers shall be compiled.

2. The technology shall be evaluated according to a novelty classification

The uncertainty registers shall contain identification and description of the various uncertainties related to the technology on component and system level. Based on the uncertainty registers, an evaluation of the technology novelty shall be conducted on a sub-system level. The sub-system shall be evaluated and categorized according to classification matrix illustrated in figure 5.3, which is an extension of the evaluation table in DNV (2011). Along with the categorization, a justification of the evaluation should be described and documented.

If the sub-system is classified as novel (all except 1,1), the rest of the full qualification process shall be followed. However, if the sub-system is classified as 1.1, the sub-system does not require a full qualification process, and can be evaluated according to a basic qualification process (see section 5.2.1).

4. Risk Assessment

The sub-systems identified as novel in the previous step shall undergo a risk assessment to identify all failure modes of concern and their associated risk. The objective is to provide a basis for prioritizing risk- and uncertainty reducing efforts. The risk assessment shall include the following steps:

1. Identify hazards and failure modes connected to the components and sub-system. This is done by carrying out established methods such as Preliminary Hazard Analysis (PHA), Hazard and Operability Analysis (HAZOP), and Failure Mode Effects and Criticality Analysis (FMECA).

2. Assess the risk according to consequence severity and likelihood of occurrence. This can be done by classifying the failure modes according to a risk matrix. Risk- and uncertainty-

reducing measures shall also be identified for the specific failure modes.

The risk assessment shall be documented and stored in a risk register similar to the procedures in the oil and gas industry. The risk registers are used in the oil and gas industry to segregate the identified critical risks and failure modes. They are used by asset managers as a tool to keep track of and manage the risks throughout the project lifetime (Hasle et al. (2009)). The risk register is a living document and is updated throughout the rest of the qualification process.

5. Qualification Plan

The next step is to develop a qualification plan based on the results from the three previous steps and the SML requirements (see table 5.3). The aim is to reduce all uncertainties regarded as critical and which is connected to the critical risks and failure modes. The qualification plan should contain an identification of all the relevant and appropriate qualification activities and a prioritizing of the different activities. Selection of appropriate qualification methods (analytical, experimental or integrated) to be used is also assessed in the qualification plan.

The plan should be detailed with schedules, activities, methods, responsibilities, documentation needs and resource requirements. In addition, success criteria of the qualification process, to evaluate the potential success of the qualification, shall be established. For safety instrumented systems, an evaluation from a third-party qualification process is required. The plan must also account for the third party's involvement in the process. The amount of involvement throughout the process from a third party depends on the situation, but for safety instrumented systems a third party is expected to at least quality assure and validate the qualification process.

6. Execute the Plan

The sixth step involves carrying out and evaluating the activities identified and planned according to the developed plan. The results of the tests, experiments, analytical analyses and other evidence creating activities shall be documented and assessed according to uncertainty and sensitivity.

The sub-systems and components shall undergo activities to determine performance, and level of integration internally and with other systems.

The evidence from the qualification activities, together with other relevant inputs from, for instance quality assurance assessments, technical assessments and other development processes, shall be collected and documented.

7. Evaluate the System

The seventh and final step is to perform an evaluation of the safety instrumented system and determine whether or not the system- and SML-requirements have been met. The evidence collected shall be assessed to determine if the system satisfies the functional safety and safety integrity requirements with an acceptable level of confidence.

An IML is assigned to the sub-systems based on the results from the qualification process. The IMLs are assigned to provide input regarding integration maturity to determine if the SML has been reached for this stage in the development. IMLs are not connected to the project development, but ensures a method for taking into account the integration between sub-systems in the final evaluation.

It shall be demonstrated that the system achieves the requirements stated to reach the next SML. If the SML requirements are reached, the milestone in the development phase has been reached, and the entire process is iterated in the next phase towards the next milestone in the project development model. If the SML requirements have not been reached, the process is evaluated and potentially iterated to reach the development milestone.

Chapter 6

Case Study

This chapter will demonstrate the qualification programme, introduced in chapter 5 , addressing a water mist fire suppression system for the SFT over Bjørnafjorden. The chapter contains an introduction to the SFTB concept and a description of the concept's risk picture. This includes a HAZID and a simplified risk model to show how the SISs function and interact in the sequence of events that may lead to major accidents. The water mist fire suppression system was chosen for the demonstration becuse it represents a completely new system to the NPRA, and may hence best illustrate the qualification progamme introduced in this thesis.

Since no SFTB has ever been realized, or any fixed firefighting system implemented in Norway, the necessary information about water mist systems for this specific application has been gathered from regular road tunnels and similar systems installed offshore and in other countries.

6.1 Submerged Floating Tube Bridges

6.1.1 Introduction to the Concept

The submerged floating tube bridge (SFTB), sometimes referred to as an Archimedes bridge because of its usage of Archimedes' law, is a tubular structure designed to lead road traffic over water crossings. The structure weighs roughly the same as the surrounding water and floats at a certain depth, allowing surface water traffic to pass without the risk of colliding with the tube.

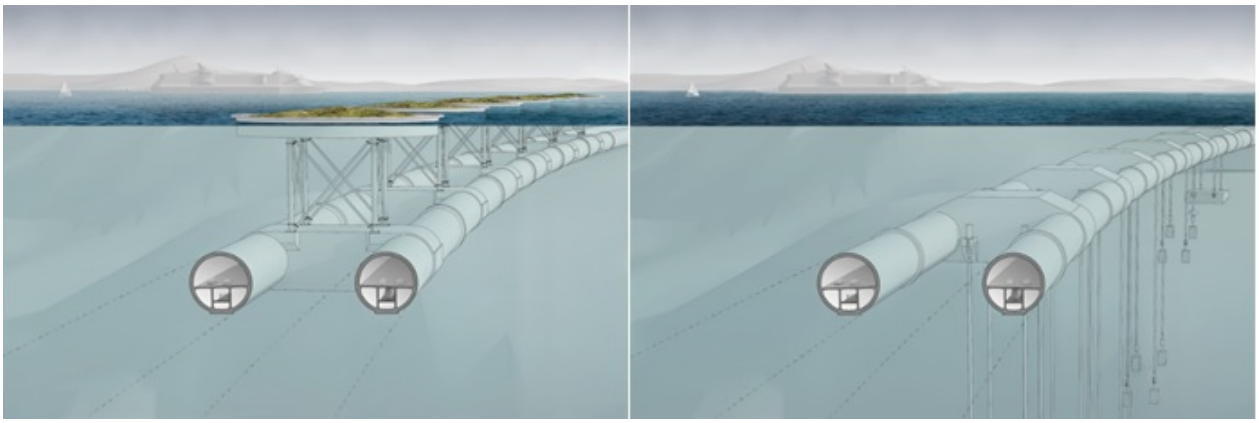

Figure 6.1: Illustration showing the two different anchoring solutions, pontoons to the left and tethers to the right (Olav Olsen, Reinertsen, Norconsult, Snøhetta)

The negative or positive load caused by the weight difference between the structure and the displaced water is carried either by tethers anchored to the seabed, or by floating pontoons on the surface (see figure 6.1).

The concept combines bridge, tunnel and offshore technology to make crossings feasible, where traditional bridge and tunnel solutions are not possible to realize. The nature of the SFTB makes it an ideal solution in deep waters, where underwater tunnel solutions are impossible, and over long crossings, where suspension bridges cannot be constructed. This makes the SFTB ideal for the extreme fjord crossings related to the ferry-free E39 project. The concept also has the advantage of being submerged, leaving no significant visual impact on the environment, and minimizing the risk of ship collisions.

6.1.2 History

Underwater tunnels are by no means a modern concept. However, constructing a safe SFTB is most definitely not the same as constructing a safe carved or immersed underwater tunnel. Although never realized, the idea of a submerged floating tunnel is not modern. The concept was first proposed and patented in Britain by MP and naval architect E.J Reed as early as in the 1880s (Tveit, 2010). Through the years, the concept has been further developed and has been assessed as a viable option on several occasions both in Norway and internationally. However, only recently, due to the great improvements achieved in offshore and deep sea technology the last thirty years, have the numerous problems that hampered the realization of this kind of struc-

ture been solved. The feasibility of the SFTB as a concept for fjord crossing was proven in the Høgsfjord project. The concept showed great potential, but the project was stopped due to "local political reasons" (Larssen and Jakobsen, 2010) before realization. Now the potential of an SFTB has again been recognized in Norway as way to successfully complete a ferry free coastal highway from Kristiansand to Trondheim. The SFT concept is considered for four of the total eight fjord crossings along the new projected E39:

1. Bjørnafjorden
2. Sognefjorden
3. Storfjorden/Sulafjorden
4. Halsafjorden

6.1.3 SFTB for the Crossing of Bjørnafjorden

The crossing of Bjørnafjorden is one of eight crossings along the E39 under consideration. The fjord is approximately five kilometres wide and 500 metres deep at the deepest point. The width and depth makes the crossing impossible to realize with traditional bridge and tunnel concepts. The NPRA pursues the development of a permanent link over the Bjørnafjord through parallel studies comprising both floating and submerged floating bridge concepts.

Several instances claim that the submerged floating tunnel is mature enough to be tested on a full scale scenario like the Bjørnafjord (Garathun, 2015). However, there are still several uncertainties related to the fulfillment of a submerged floating tunnel. The uncertainties relate to the novelty of the technology as well as their integration with the environment in the 100-year perspective requirement. In addition to technical uncertainties, the SFTB also faces uncertainties regarding investment cost.

The assessment study for the SFTB is carried out by the design group REINERTSEN, Dr. Techn. Olav Olsen and Norconsult with support from marine operation specialists from Aker Solutions. The proposal for Bjørnafjorden is based on two parallel tubes with crossing horizontal bracers. The bracers shall, apart from provide stiffness to the structure, facilitate evacuation

routes between the two main tubes. Both pontoon and tether anchoring are assessed as viable solutions.

6.1.4 Risk Picture for the SFTB

Two of the main reasons to why the SFTB concept never has been realized are owed to uncertainties connected to the concept. Firstly, there exists a great deal of uncertainty related to the lifecycle of the SFTB project. Taking into account the large investment and development cost, and the long construction time, many unexpected factors may contribute to hidden risks being revealed during the project-planning, design, construction and operation phases. Secondly, many technical and safety challenges still contribute to the uncertainty connected to the concept. The overall aim of the NPRA is to design strait crossing concepts that fulfill the same risk acceptance criteria as regular road tunnels and bridges. In other words, the SFTB needs to operate under and maintain the same safety level as an underwater tunnel or regular bridge.

A SFTB must face hazards related to bridge, tunnel and offshore solutions. For example, the SFTB shares the hazards related to the confined space and fires, just as regular road tunnels, and ship collisions to the pontoons, similar to a floating bridge. The consequences and frequencies of hazardous events related to confined space are usually dependent to where in the tube/tunnel the event occurs. It is common to divide the tube/tunnel into different zones (see figure 6.2). It may therefore be stated different requirements for safety barriers in the different zones.

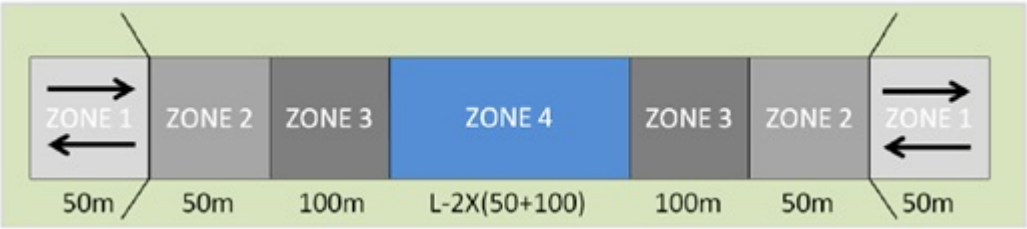

Figure 6.2: The division of tunnel zones in the NPRA. From NPRA (2014)

In order to identify the necessary safety instrumented functions for the submerged floating tunnel, a HAZID may be carried out. As mentioned in chapter 3, a HAZID leads to the functional requirements i.e. what sort of safety functions is required.

Several HAZIDs have been conducted in the feasibility study and development work related

to SFTBs for Bjørnafjorden and Sognefjorden. The analyses have been prepared by the design group responsible for the SFTB concept and consider both the installment and operational phase of the SFTB. For the purpose of this thesis, a compilation of only the relevant identified hazards has been made. Due to the specific objective of this HAZID, which is to identify safety instrumented functions, only the operational phase has been considered. The findings are presented in Appendix B.

Several different safety instrumented systems are identified in the HAZID as potential safety barriers to maintain a safe operation. Many of the systems are conventional tunnel systems, and some are specific SFTB systems. Central to all the systems is that they share a connection through either the manually operated SFTB control centre or through the central SFTB control system. The simplified diagram in figure 6.3 shows the different systems. In a wider perspective it can be argued that all the systems serve as either input/detection elements or actuating elements with the control system and control system functioning as a logic solver

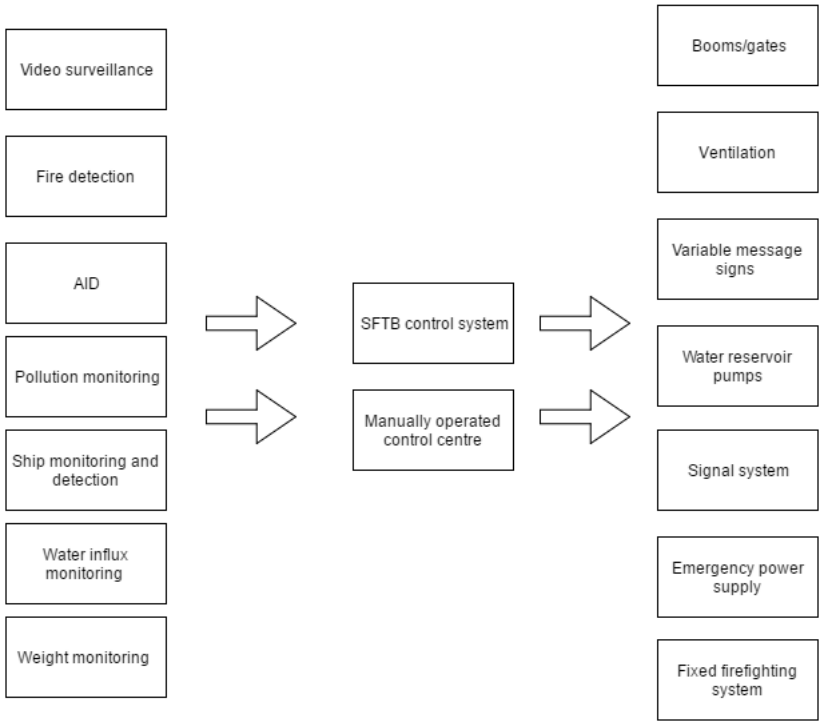

Figure 6.3: Illustration of the interaction and connection between the different safety systems identified

To illustrate how the systems function, and how these systems interact in a sequence of events that may lead to accidents, a simple example is presented.

For SFTBs, as for tunnels, a fire inside the tube is a potential catastrophic event. The flowchart in figure 6.4 illustrates an example of how the systems are designed to function in the scenario of a fire in the tube.

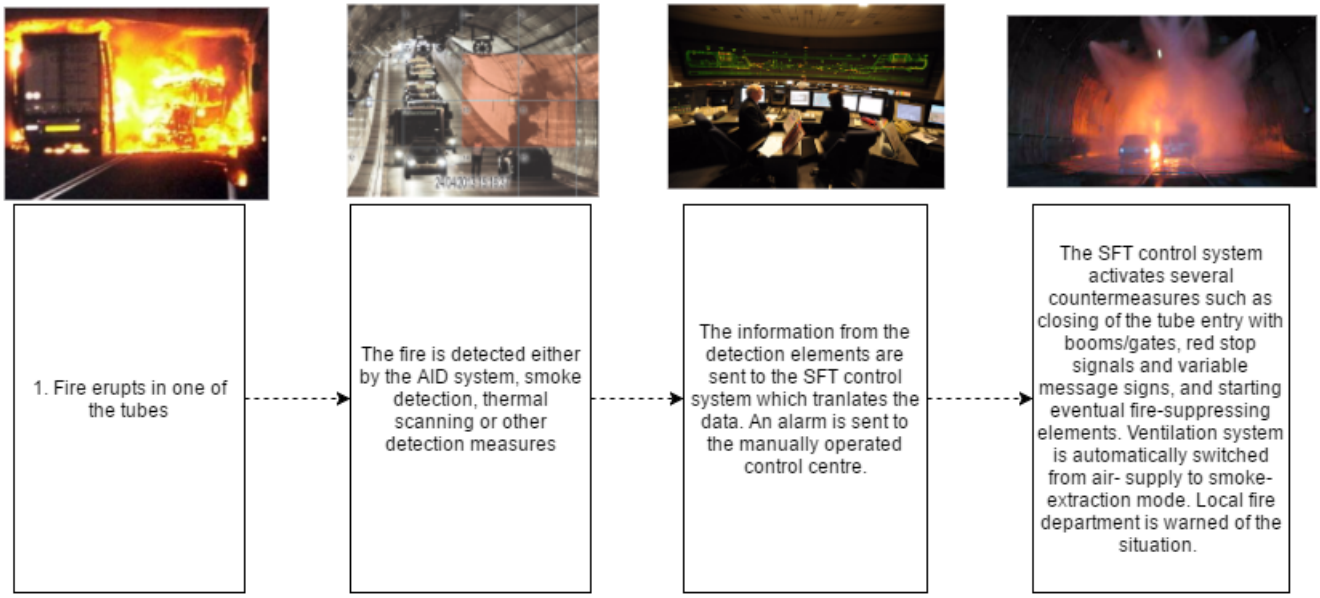

Figure 6.4: Illustration to show how the safety instrumented systems interacts in the case of a fire in a tube

6.2 Description of a fixed high pressure mist-type fire suppression system

One of the systems identified in the HAZID as a potential safety measure, was a active firefighting /fire suppression system. A fixed firefighting system that uses water droplets to suppress a tunnel fire has never been installed by the NPRA in Norway. In Japan and Australia, conventional sprinkler and deluge systems have been in use in tunnels since the 1960s. In recent years, to develop more effective and cost-effective solutions, systems using high pressure water mist technology have received increased attention (Kratzmeir and Lakkonen, 2008). Several studies have been conducted to evaluate the system's effectiveness as a safety measure towards controlling and mitigating the consequences of fires in regular road tunnels (see Setoyama et al. (2004); Mawhinney and Back (2016); Kratzmeir and Lakkonen (2008); Starke (2010)). The effect of deluge has also been tested with medium to full-scale experiments by SINTEF National

Fire Research Laboratory in Norway. The experiments show that release of water mist deluge reduces the global average heat load and is effective in preventing fire from spreading to adjacent vehicles (Wighus, 2012). The European research project UPTUN and the research project SOLIT, funded by the German government, have also conducted tests, specified some requirements and studied the interaction between a water mist fire suppression system and other safety system such as passive fire protection and ventilation.

The water mist fire suppression system is similar to a sprinkler system. However, the nozzles of a water mist fire suppression system are dry upstream and connected to the fire water pipe main with a deluge valve that is opened on demand. The water mist systems in regular road tunnels are typically designed as open nozzle deluge-type systems divided into sections of approximately 30-50 meters. The water supply is designed so that three sections can be activated simultaneously. The fire detectors are intended to accurately locate the source of fire, and automatically activate the water mist system in the section where the fire is located in addition to one section upstream and one section downstream.

The use of a high-pressure system (range from 60-120 bar) has advantages for the application in SFTBs due to the small-diameter piping needed, reducing the impact of the water mist system on the architecture. Not all the pressure is needed in the nozzles (around 50 bar). High-pressure water mist systems can utilize electric motor- or diesel engine-driven, positive displacement (PD) pumps to achieve the necessary system pressures. This is in contrast to traditional centrifugal fire pumps used in regular fire protection systems. Water mist systems have been installed in highway tunnels up to 10km (Mawhinney and Back, 2016).

The entire system structure is built up as a traditional safety instrumented system with fire-detectors, a logic solver, and actuating elements (see figure 6.5). For the application in SFTBs it is reasonable to assume that a potential water mist system will employ the same fire-detection technology used in regular road tunnels in Norway. Norwegian road tunnels rely primarily on 2D- video detection with image interpretation to identify everything from traffic accidents to fires (NPRA, 2013). The tube is divided into sections with adequate surveillance coverage. The cameras constantly scan every section to identify irregularities. The SFTB control system, similar to a regular road tunnel control system, will act as the logical solver, interpreting the signals from the video detectors and activating the water mist sub-system. The system can also be ac-

tivated from a manually operated SFTB control centre if a manually fire alarm pull station is activated in one of the tubes. The operator will then assess the situation and activate the water-mist system manually. The scenario with manual starting of the water mist sub-system is not treated in this case-study.

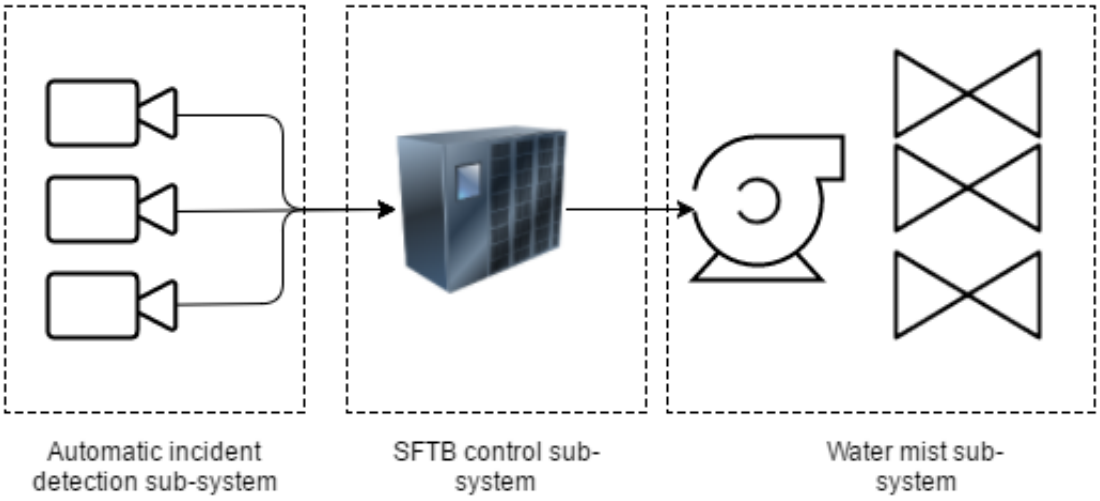

Figure 6.5: Illustration of the different sub-systems making up the water mist fire suppression system

The main objectives of a fixed mist-type firefighting system are to:

- Suppress and cool down the fire.
- Prevent fire spread in the direct vicinity of the fire.
- Protect the tube/tunnel structure and its facilities; and
- Support and facilitate other firefighting activities.

The basic safety instrumented function of the system can be defined as:

- Detect and suppress the fire in the tube by applying high pressure water mist to cool down the fire, preventing the fire from spreading, and protecting the structure and the users from heat, smoke and toxic gases.

6.3 Qualification of a fixed high pressure mist-type fire suppression system

This section will demonstrate the qualification framework introduced in chapter 5. The case-study will not be able to reflect all the attributes and principles important to the framework, since many of the attributes and principles are linked to the entire development time line of the project. Hence, the objective of this section is not to "qualify" a fixed high pressure mist-type fire suppression system for the submerged floating tube bridge, but to demonstrate and highlight some of the important aspects of the framework introduced. Emphasis has been laid on how to specify, derive, allocate and assess safety requirements including safety integrity levels.

There are currently no regulations in the NPRA stating that SFTBs should be equipped with fixed firefighting systems. Hence, the need for such a system must be derived from an initial risk analysis.

1) Initial uncertainty assessment of the qualification foundations.

The first step in the qualification process is to identify and assess the uncertainties related to carrying out the qualification.

Standards and requirements:

As mentioned in chapter 4, the NPRA does not have an unambigious approach, or principle, towards stating overall risk acceptance criteria. This means that the results from the risk analyses cannot be compared to the criteria for acceptable risk. In other words, the agency have no structured guidelines addressing how technical systems contribute to the overall risk picture for the road infrastructure. Nor does the NPRA have any stated performance requirements for such systems. One solution would be to adapt the rules and standards from the Norwegian oil and gas industry such as NORSOK-S-001 (2008) and OLF-070 (2004) which address performance and functional requirements for water mist fire suppression systems in offshore facilities. How appropriate these rules and standards are for the application of the SFTBs and uncertainty with respect to potential shortcomings must be assessed. However, most importantly, there is a need for a principle for stating risk acceptance and balancing the risks, risk reducing measures and benefits.

Environmental and operational conditions:

The environmental and operational conditions for a water mist fire suppression system in a SFTB will largely resemble the conditions in regular road tunnels. No explicit uncertainties should be related to this factor. However, since the SFTB concept is a completely new concept, the design basis must be detailed enough to sufficiently describe the environmental and operational conditions for the systems designed to be implemented in the SFTB. As such, the environmental and operational conditions may change coinciding with the development of the SFTB concept.

Analyses and Methodologies:

To assess and qualify a safety instrumented system such as the water mist fire suppression system, different system analyses must be carried out throughout the process. The lack of experience data, and the appropriateness and experience related to the models contribute to the uncertainty for the process. An example would be the different methods to derive SIL requirements (risk graph, LOPA, etc). It must be assessed if the methods are feasible, and eventually which method is the most appropriate. Due to the fact that the NPRA has little experience with RAMS analyses, it would be reasonable to assume that to reduce the uncertainty related to the entire qualification process, a high degree of involvement by third party consultants. The limited access to data must also be considered. This includes data such as failure rates, demand rates etc.

2) Define safety function, system and requirements

System and function specification:

The safety function of the fixed firefighting system is described in section 6.2.

- Detect and suppress the fire in the tube by applying high pressure water mist to cool down the fire, preventing the fire from spreading and protecting the structure and the users from heat, smoke and toxic gases.

To carry out this function, the system needs to be comprised of three main sub-systems:

1. Fire detector sub-system
2. Logical solver (control system)
3. Water-mist sub-system

The water-mist sub-system, which is the actuating system, will again be comprised of:

1. Submerged water pumps to supply water
2. Booster Pump(s) to build up the necessary pressure in the water pipe main
3. The water pipe main going along the tube
4. Valves (one for each section of the tube)
5. Nozzle heads which transforms the water into mist

No requirements exist regarding the arrangement and voting of pumps for the tunnel application (at least to the author's knowledge). However, the Norwegian offshore standard NORSOK-S-001 (2008) states that the pump arrangement on offshore installations shall be at least 4 x 50% or 3 x 100%, where 100% refers to the largest fire area. For a SFTB, where all the fire areas are the similar, it is assumed that a 2 x 100% arrangement is sufficient with a pump system located at each shore.

The flow chart in figure 6.6 illustrates the water mist sub-system used in this demonstration.

The system is categorized as a low-demand, or on-demand, system, meaning that it will be activated on a demand (fire). It is assumed that the demand rate will be considerably less than once per year. The system should be designed such that testing can be performed automatically and in full-scale. Once a year, the different water mist sections of the tube should be activated one at the time to fully proof test the system.

Performance requirements

Fixed firefighting systems are not covered by the NPRA manuals. However, several generic standards exist for water mist systems. These standards can provide basic design requirements such

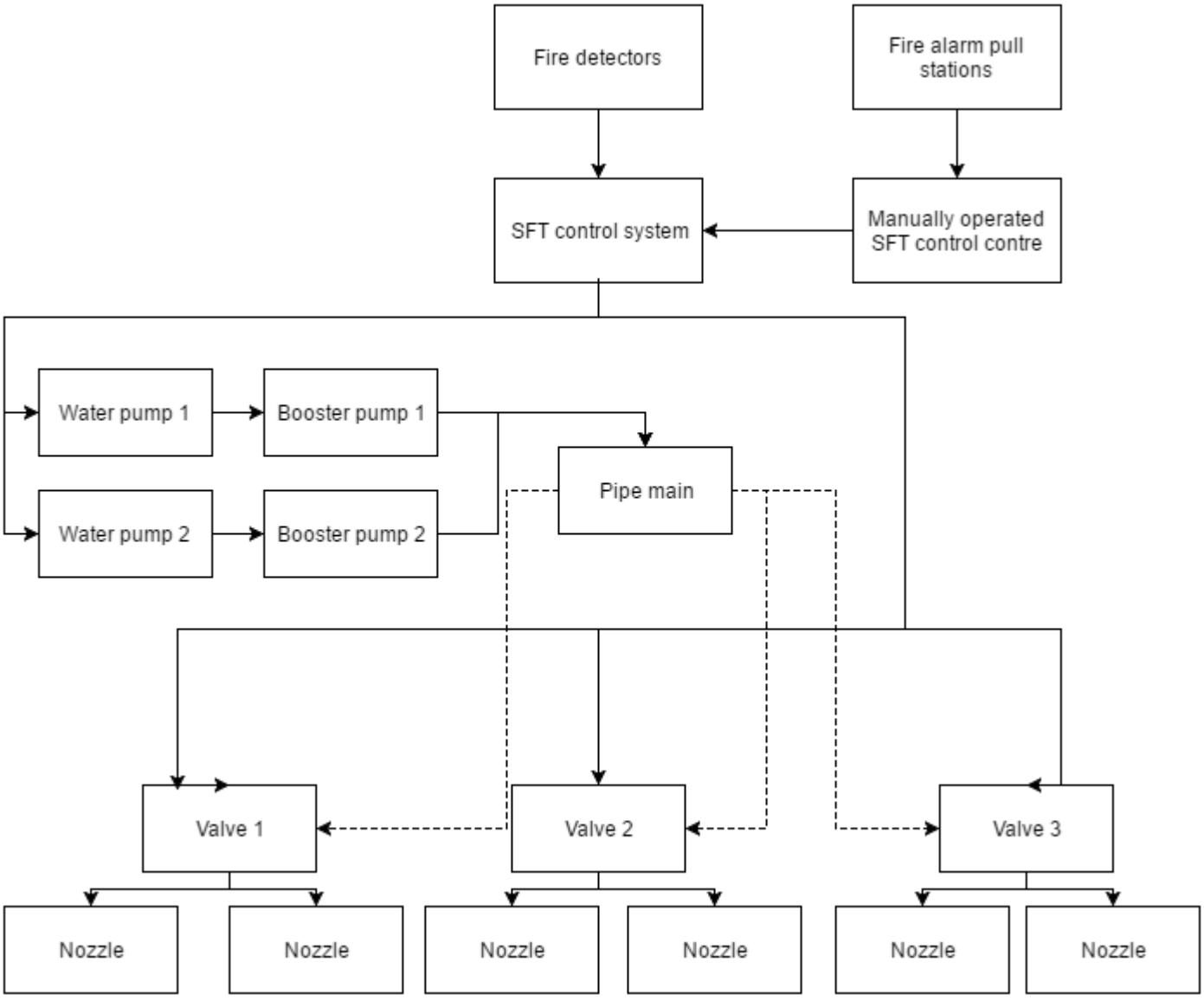

Figure 6.6: Flowchart of the water mist sub-system

as size of the water supply, droplet size and distance between sprinkler heads. These standards include: EN 12259-1, EN 14972, NFPA 20 and NFPA 750. None of the standards do, however, address the performance requirements of water mist systems. Hence, performance requirements must be derived from the risk analyses, and by design criteria for tunnel fires stated in NPRA's manuals. The SIL requirement for the water mist system can be deduced from the risk analyses by the following methods:

1. Overall tolerable risk
2. Risk graph(calibrated)
3. LOPA (Layers of protection analysis)
4. Event tree analysis

For the water mist system, it might be reasonable to derive SIL requirements through a calibrated risk graph. Due to the fact that the NPRA does not have an established principle in respect to risk accept criteria, the method of deriving SIL requirements from overall tolerable risk is impossible to realize. The risk graph should not be made too sophisticated, but may take into account the consequence, number of people in the tunnel, and the probability of escaping, in addition to the demand rate. It could be argued that LOPA, could also be considered a valid method, since it takes into account other risk reducing measures, but the simplicity of the risk graph makes it a valid choice in this demonstration. The standard risk graph is shown in figure 6.7 and the description of the calibrated risk parameters are classified in table 6.1. To calibrate a risk graph without stating risk acceptance criteria can be challenging, but is not impossible. Ideally should the calibrated parameters reflect the risk acceptance criteria of the user (Torres-Echeverria, 2015). The calibrated values and parameters shown in 6.1 are based on classification of regular tunnel fires adapted from NPRA (2014) and suggestions from the author.

For the water mist system, it is reasonable to go the path: Cd – Fa – Pa – W1, yielding a SIL2 requirement for the water mist system. This is also in compliance with OLF 070 which also states a SIL2 requirement for the safety function "release fire water/deluge".

Table 6.1: Description of calibrated risk parameters

Risk parameter	Classification	Notes
C) Consequence Related to number of fatalities and magnitude of fire C = No. fatalities x Magnitude	C_a - No fatalities C_b - range 0.01 -0.1 C_c - range 0.1 - 1 C_c - range >1	Vulnerability = Magnitude of fire Small fire = V1 = 0.01 (0-20MW) Medium fire = V2 = 0.1 (20-50MW) Big fire = V3 = 0.5 (50-100MW) Catastrophic fire = V4 = 1 (> 100 MW)
(F) Occupancy People in the tube	F_A - 0-100 people behind the fire when the fire erupts F_B - > 100 people behind the fire when the fire erupts	
(P) Probability of avoiding the fire	P_a - adopted if all the conditions in column 3 are satisfied P_b - adopted if one or several of the conditions in column 3 are not satisfied	Pa should be selected if all the following are true: 1. The SFTB control centre should be aware if the SIS fails 2. Independent measures are provided to close off the tube and enable persons to escape 3. Activation time for the SIS is less than 3 minutes
(W) demand rate	W1 - < 0.1 per year W2 – 0.1 – 1 per year W3 > 1 per year	

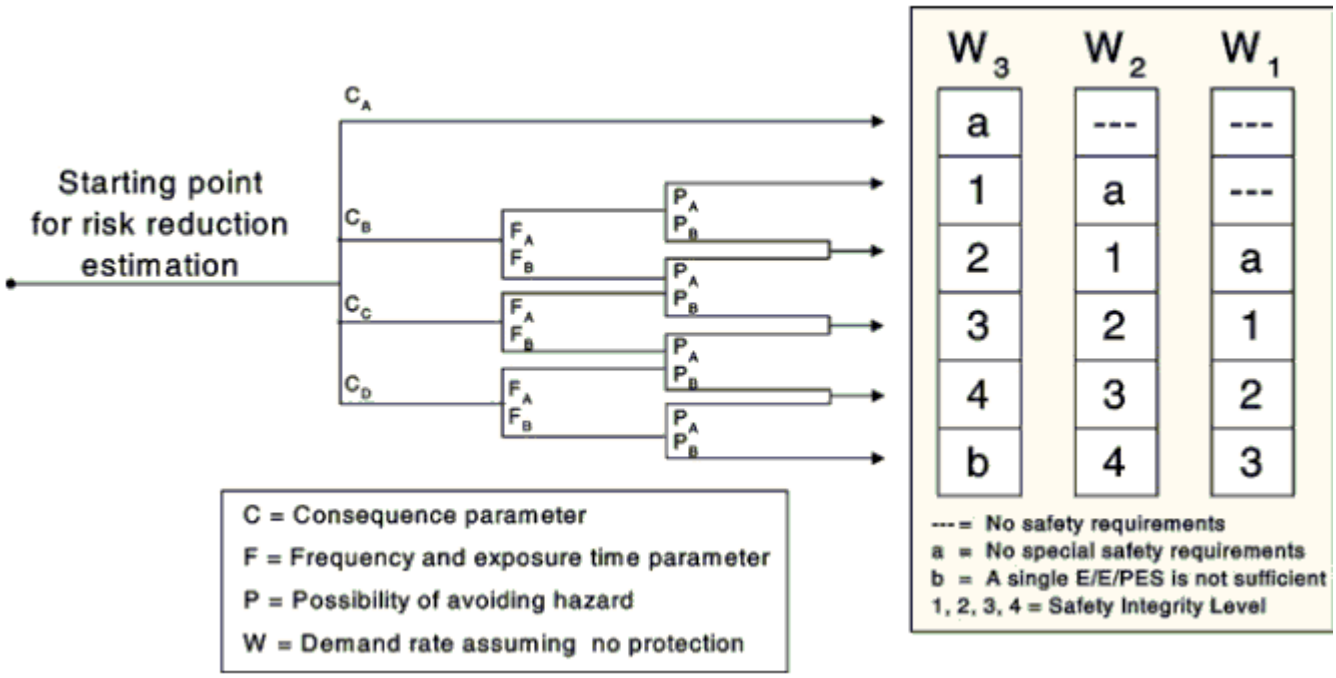

Figure 6.7: Standard risk graph

A SIL2 requirement, according to IEC 61508, indicates that the average probability of failure on demand (PFD) of the safety function shall be $0.001 < PFD < 0.01$. The PFD of the system is determined by the total PFD of the sub-systems.

$$PFD^{\text{system}} = PFD^{\text{Detectors}} + PFD^{\text{Control system}} + PFD^{\text{water mist sub-system}}$$

When a SIL requirement for a specific SIF has been allocated, the SIL requirement has to be broken down to requirements for the sub-systems. A commonly accepted distribution of the SIL requirement is (Rausand, 2014):

Sub-system	Percentage
Sensor subsystem	35%
Logical solver subsystem	15%
Final element subsyste	50%

If the water mist system spuriously activates, the visibility in the tunnel will be severely decreased, increasing the potential for traffic accidents. This, in addition to the time to restore the system and the cost of spurious trips, a maximum allowable spurious trip rate should be stated. This can be expressed as a spurious trip level (STL) which is calculated via probability of fail-safe

Table 6.2: Selected requirements

Parameter	Requirements
SIL requirement for safety function	SIL2
Design life for detectors and control system	10 years
Design life for tubes, nozzles, pump and valves	25 years
Spurious trip level	STL2
Demand length	40 minutes for one section
Activation time	3 minutes
Test interval (τ)	1 year

of the safety function. To further reduce the probability of spurious trips, the automatic video detection camera should run a total of two interpretation cycles before sending the signal to the control centre. As such, the video detection system has an integrated 2oo2 voting. The demand length requirements must be stated on the basis of scientific studies done on the duration it takes for the water mist system to suppress the design fire, and the estimated time until the local fire departments can react to the fire. In Japan, where sprinkler/water mist systems are required in all road tunnels over 500 metres, it is required that the water supply must be sufficient for 40 minutes of operation for one section of 50 metres. The Japanese have also stated requirements regarding the activation time of the system. To minimize spurious trips, errors and confusion by tunnel operators, the activation time was set to 3 minutes for a uni-directional tube (Liu et al., 2007).

In manual N500 (NPRA, 2014) for road tunnels in the NPRA, under chapter 10 concerning requirements for technical equipment, it is stated that "lifetime shall be assessed for every individual component based on lifecycle cost". For the electronic components it is reasonable to have relatively short lifetime due to the rapid technology development. New components today might be outdated in few years. For more structural components, such as piping etc. a longer expected lifetime may be stated. A summary of selected different performance requirements for the water mist system example is shown in table 6.2.

3) Assessment of uncertainty and technology novelty

To assess which of the sub-systems or elements that involves new, or novel, technology, uncertainty registers are compiled on both component and sub-system level. The system is broken

down as shown in figure 6.6 with three sub-systems.

No complete assessment will be carried out for the purpose of this demonstration, but an example uncertainty register is demonstrated for the longitudinal pipe element in the water mist sub-system.

Table 6.3: Uncertainty register example.

ID	Description	Cause	Effect	Probability	Criticality	Mitigation measures
U-1	Uncertainty regarding clogging of longitudinal pipe along the tube	Length of the tunnel, calcareous deposits, biofouling, corrosion, etc...	Water will not reach correct outlet, pressure may build up and rupture the pipe, the pump may be overloaded, etc...	small	high	X-ray inspection of the pipe, annual testing, pressure testing, filters to remove foreign particles. , etc...

The uncertainty registers should be constructed by a multidisciplinary team. Persons with experience and knowledge of similar systems should participate to reveal all the uncertainties related to the various components and sub-systems. Based on the uncertainty registers, the three different sub-systems of the water mist system shall be evaluated regarding novelty according to the table illustrated in figure 5.3.

The automatic incident detection sub-system is well known to the NPRA and has been used in very similar conditions. The concept is also very well covered in NPRA's report on automatic incident detection in tunnels (NPRA, 2013). Even though the video detection previously has encountered problems with false alarms and calibration errors, it is reasonable to categorize the automatic incident detection system as 1.1 (proven technology)

The SFTB will be controlled by an automatic control sub-system similar to the tunnel control system installed in all Norwegian tunnels over three kilometres. These systems are also well-known to the NPRA, and well covered in several NPRA documents such as the ITS guideline and N500 manual for road tunnels. The operational and environmental conditions inside the SFTB

are approximately identical to the conditions experienced in regular road tunnels. Hence, it will be reasonable to categorize the SFTB control sub-system as 1.1 (proven technology).

The water mist sub-system however, are new to the NPRA. The sub-system has been used for regular tunnels internationally, but the SFTB application area may include several new challenges and uncertainties for the water mist sub-system. The sub-system is covered in some standards, such as the NFPA standards and offshore application standards, but none addresses the application of such a system in a tunnel or SFTB application. A reasonable categorization of the water mist sub-system would be a limited application and technology rating; 2.2.

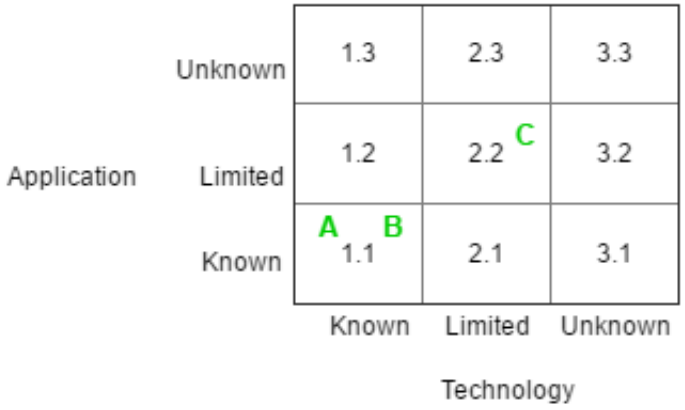

Figure 6.8: Classification of the three sub-systems. A = automatic incident detection sub-system, B = tunnel control sub-system, C = water mist sub-system

This means that the water mist sub-system requires a full qualification process, while the detection and control sub-systems only require a basic qualification process. The interaction between the sub-systems will be evaluated as part of the end evaluation of the process.

4) Risk assessment

For the water mist subsystem, a risk assessment is carried out. Since the sub-system involves flow of water and pressure, it may be reasonable to perform a HAZOP analysis to systematically identify the hazards related to the sub-system. The HAZOP should be carried out by a group of experts to explore how the system may deviate from the intended design and generate operability problems (Rausand, 2011).

The identified hazards also need to be risk evaluated according to frequency and severity via a risk matrix (see figure 6.10). This may be integrated in the HAZOP worksheet or conducted in

No.	Study Node	Deviation	Possible causes	Possible consequences	Existing barriers	Proposed improvements
1	Spray nozzles (flow)	No flow	Clogging of nozzles, clogging of pipelines, valve closed, no water pressure, no water supply	No water to cool down and suppress the fire	Inspection and maintenance of nozzle heads, X-ray of pipeline, annually full scale test of system	Use fjord as water supply, filter water to prevent clogging, etc.
2		Less flow	Nozzle or pipeline partly clogged, valve partly closed, too low pressure,	Too little water to sufficiently cool down and suppress the fire, the fire is cooled down too slowly	Inspection and maintenance of nozzle heads, X-ray of pipeline, annually full scale test of system	filter water to prevent clogging, install pressure monitor, etc.

Figure 6.9: Example of a HAZOP worksheet for the water spray nozzles

a separate exercise. The two hazards identified in the HAZOP in table 6.9 can be classified as follows:

Table 6.4: Ranking failure mode according to risk

Hazard	Freq	Sev	Risk classification
No flow	Remote	Critical	Undesirable
Less flow	Occasional	Critical	Undesirable

The risk matrix should be calibrated to the system under consideration. In this way, the different hazards and failure modes can be assessed to provide a basis for prioritizing risk and uncertainty reducing efforts.

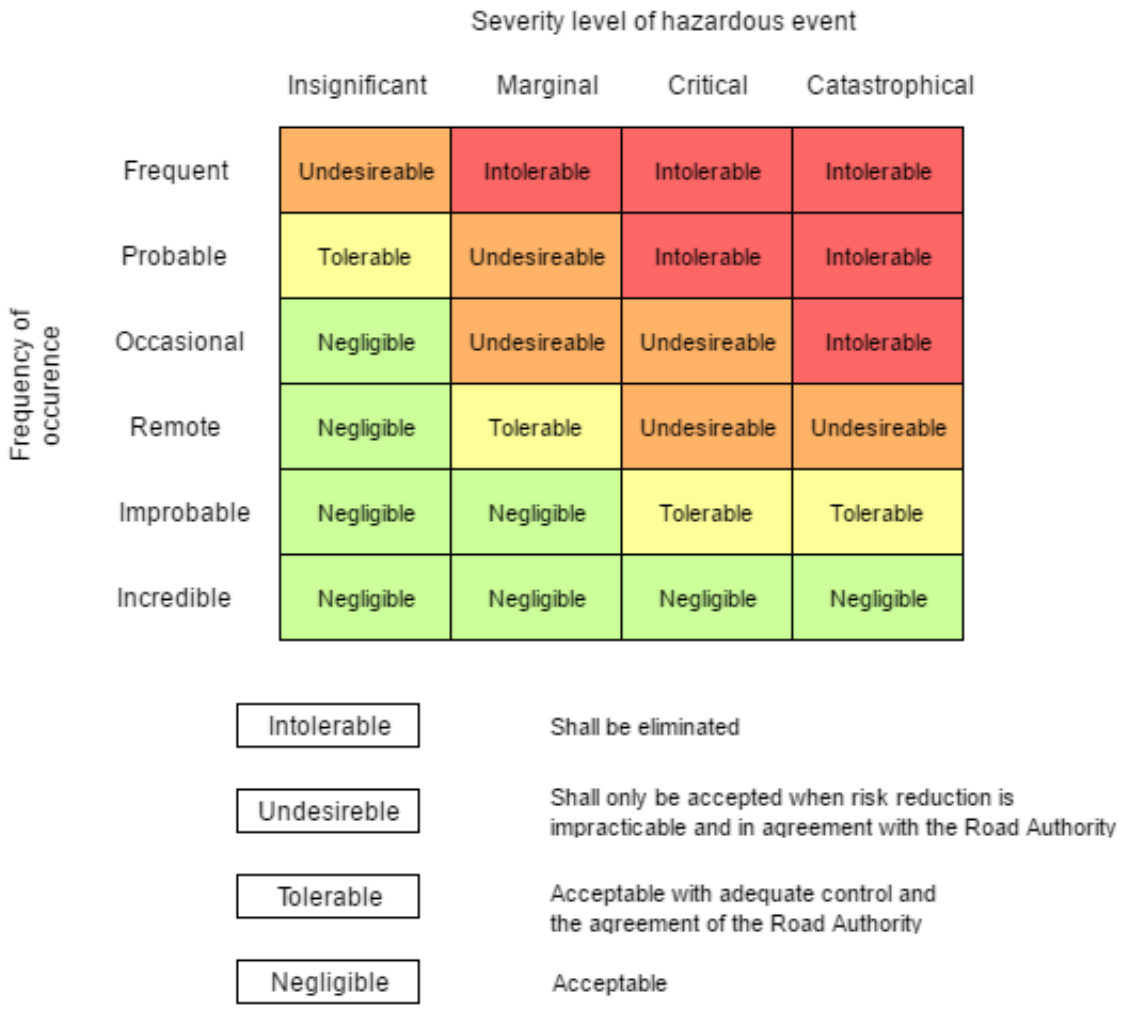

Figure 6.10: Risk matrix. From EN-50126 (1999).

5) Qualification Plan

The aim of the Qualification Plan is to develop a strategy where confidence is built towards the requirements stated in the first step of the qualification process. This is managed by reducing the uncertainties and by providing sufficient documentation to the failure modes of concern. The qualification plan for the water mist sub-system can be organized into separate verification activities according to the different attributes and functions of the sub-system. For instance:

A) Verification of water supply

B) Verification of pressure build-up and distribution

C) Verification of flow

D) Verification of mechanical reliability of components

E) Verification of interaction with SFTB sub-system

These verification activities can be organized as work packages and be scheduled according to a milestone plan. The specific activities and qualification methods (see section 2.2) to be carried out must be decided upon by a team of experts. To verify the flow of water it could be relevant to both analyze a computer model of the system to look at the fluid dynamics of the system working at high pressure. It could also be relevant to construct scaled-down test facility to physically test the liquid distribution properties of the system at low pressure. High pressure scenarios can be impossible to verify by physical tests. The two qualification methods should then be compared, and are verified when the test and computer analysis correspond.

Besides from the different verification activities, analyses for the sub-system must be planned and documented in order to provide evidence towards the requirements and acceptance criteria. This may include, for the water mist sub-system, LCC-analysis, operation availability analysis, PFD_{avg} analysis and other relevant analyses identified under this step. These analyses may use data generated or gathered under the execution step of the process.

6) Execution of the Plan

All the verification activities identified in the qualification plan should carried out in the execution of the plan. The starting point and the length of each activity should follow the milestone

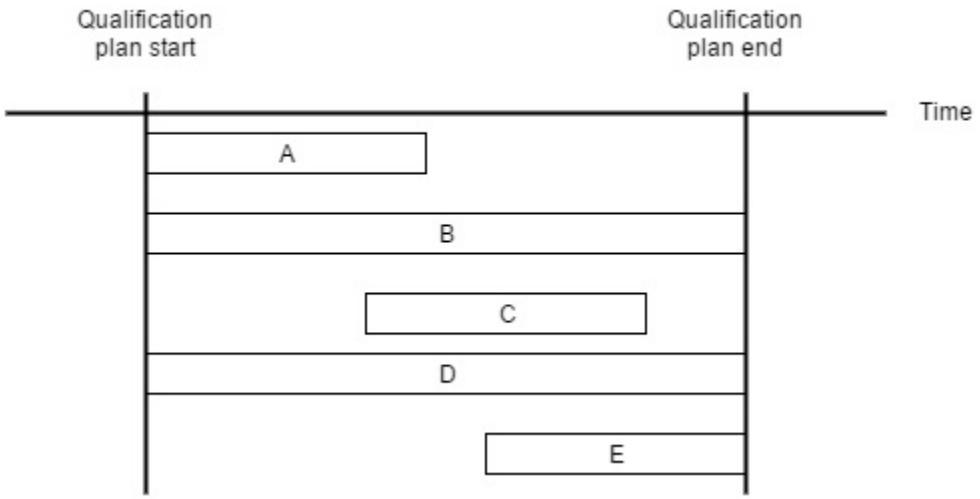

Figure 6.11: Example schedule

plan, illustrated in figure 6.11. Throughout the execution of the plan, the documentation of the qualification is essential to ensure traceability and evidence to the technology. The execution of an activity shall always be aimed to provide evidence towards the stated requirements stated in step 2.

7) Evaluation

In the evaluation, the documented qualification evidence, obtained through the execution of the plan, shall be compared with the technology- and requirement specifications stated in the technology qualification basis. All including sub-systems, including the sub-systems subject to the basic qualification basis, shall be ranked according to the IML scale. For the water mist system, there are three sub-systems interacting. Two IMLs must evaluated:

1. The interaction level between the automatic incident detection sub-system and the SFTB control sub-system

2. The interaction level between the SFTB control sub-system and the water mist sub-system

Since the automatic incident detection sub-system and SFTB control sub-system are assumed (in this demonstration) to have documented and qualified interaction, the IML between the SFTB control sub-system and the water mist sub-system will be the limiting integration factor.

An example will be to rank interaction 1) as IML4, while interaction 2) as IML2. This is of course dependent on the results from the execution step.

An evaluation shall also be made to rank the entire system according to the SML scale. The SML ranking must consider the lowest IML ranking (IML2 in this example), and the degree of confidence obtained through testing and analyses of data. The entire system would be considered qualified (SML4) when the evidence generated and gathered throughout the qualification process meets all requirements stated in step 1 of the qualification process with a sufficient level of confidence. In cases where the system does not meet these requirements, a modification loop can be used for trying to meet the requirements. This means that the water mist system must show compliance with a SIL2 requirement, and the other requirements stated in step 2.

Since the water mist system is a SIS, it required that a third party verifies the process and the obtained results, as well as the evaluation.

This demonstration will not conclude on whether or not a water mist system might be considered qualified or not. No qualification evidence has been obtained, but some important aspects of the qualification process have been highlighted to hopefully better demonstrate how such a qualification programme works in practice.

Chapter 7

Summary and Recommendations for Further Work

7.1 Summary and Conclusions

Implementing new technology with strict requirements and expectations regarding safety and reliability requires a systematic and structured qualification programme. This master's thesis has addressed an implementation of such a qualification programme in the Norwegian Public Road Administration (NPRA) for the project "Ferry-free E-39".

To meet the main objective of this thesis, which is to propose a qualification framework for SISs with respect to the situation in the NPRA, an extensive knowledge of concepts and terminology for technology qualification is necessary to achieve compliance. Chapter 2 describes the basic concept of qualification of new technology with a review of different acknowledged approaches and principles. The chapter also describes the different qualification methods and the standard qualification process introduced in DNV-RP-A203.

Chapter 3 introduces the concept of safety instrumented systems (SISs) and describes some central aspects concerning assessment of such systems. IEC 61508 is introduced as the main standard for regulation and development of SISs. Central aspects such as the safety lifecycle, functional safety and safety integrity requirements are discussed. The chapter also briefly discuss how IEC 61508 may be of relevance when addressing qualification of new technology. Several links were identified.

In order to understand the specific challenges and considerations regarding technology qualification in the NPRA, a study of project and development management in the agency is provided in chapter 4. Several challenges, like the lack of uniform RAMS management guidelines, lacking knowledge regarding requirements elicitation and uncertainty regarding the role and scope of technology qualification, was revealed.

The main delivery of this thesis is presented in chapter 5 as a qualification framework aimed at implementing SISs for the extreme fjord crossing concepts assessed in the Ferry-free E-39 project. Several different key principles and aspects was identified to make the framework applicable for the NPRA and to show how principles from IEC 61508, System's Engineering and technology qualification can be combined in such a framework. The framework is presented as a technology qualification programme with some new definitions and practical models, in addition to a practical approach describing the qualification process.

To further show how such a qualification framework can be utilized, a demonstration of a water mist fire suppression system intended for the submerged floating tube bridge (SFTB) over Bjørnafjorden is provided in chapter 5. The chapter introduces the SFTB concept and briefly assesses the risk picture of the concept. A HAZID was compiled to identify the different SISs expected to be needed for the SFTB over Bjørnafjorden, and a basic risk model was developed to show how these systems interact in the sequence of events that may result in major accidents. Emphasis is laid on how to derive SIL requirements and assess the reliability of the system in light of these requirements.

7.2 Discussion

Several different links and interfaces between the scope, specific methods, phases and requirements in IEC 61508, NPRA practices and the technology qualification approach adopted by the NPRA were identified. Due to the risk-based and reliability approach found in IEC 61508, several elements from the standard have a high transferability towards the development of a qualification programme for SISs. However, it is the opinion of the author, that the exercise of constructing a new technology qualification framework/programme for the NPRA based on the identified links, should be carried out as a multidisciplinary exercise. It is, surely, a weakening that the

framework presented in this thesis has primarily been developed by a single person. The result is that the framework lack the necessary specificity to directly be useful to the NPRA. However, it is the author's opinion that important aspects, challenges and principles identified in this thesis ought to be thought-provoking and useful for risk management and the efforts done towards qualification of new technology in the NPRA.

Another aspect to consider, is the relevance of such a framework to the NPRA. The Ferry-free E-39 project is still in its initial development stages. Considerations towards SISs and technical system is usually made later in the overall development process. As such, the framework might be of more relevance later in the project. In addition, the framework should have a high transferability towards the work being done to establish a technology qualification framework for the new extreme fjord crossing concepts. The transferability is natural, since much of this thesis have been influenced by the work on implementing a qualification programme for entire bridge concepts. The author has also taken this into account when developing the framework.

The selection of the water mist fire suppression system for the case study is based on the fact that this is an actual new system, and that this should give a better reflection of the central principles in the qualification framework.

7.3 Recommendations for Further Work

Based on the author's experience during the preparation of this thesis, some topics recommended for further work are:

- A study should be initiated to identify what aspects of the qualification framework proposed in this thesis that have high transferability to the qualification of extreme fjord crossings in the NPRA.
- Improve the qualification framework by making it a more multidisciplinary exercise involving both managerial and technical perspectives.
- The issue regarding RAMS and risk management within the NPRA should be addressed to better facilitate technology qualification in the agency. A more holistic view on risk in road project should be attained. In order to make this happen, a more functional mind-set

is necessary. This also includes how to address functional safety requirements regarding safety critical systems. The future will, surely, see increasing use of such systems to maintain the safety level on roads and aid the NPRA towards the vision of "zero fatal accidents on Norwegian roads".

- Official regulations and NPRA manuals should be updated, or be established, to include more functional performance requirements for technical systems. As per now, the requirements stated are mainly descriptive.

Appendix A

Acronyms

AID Automatic Incident Detection

API American Petroleum Institute

DG Decision Gate

DNV Det Norske Veritas

E/E/PE Electrical, Electronic, Programmable Electronic

FEM Finite Element Method

FMECA Failure Mode Effect and Criticality Analysis

FTA Fault Tree Analysis

HAZID Hazard Identification

HAZOP Hazard and Operability Study

IEC International Electrotechnical Commission

IML Integration Maturity Level

IRL Integration Readiness Level

ITS Intelligent Transport Systems

KP Key Process

LCC Lifecycle Cost

LOPA Layers of Protection Analysis

NPRA Norwegian Public Road Administration

OPERA Operational Problem Analysis

PFD Probability of Failure on Demand

PFH Probability of Failure per Hour

PHA Preliminary Hazard Analysis

RAMS Reliability, availability, maintainability, and safety

SFTB Submerged Floating Tube Bridge

SIF Safety Instrumented Function

SIL Safety Integrity Level

SIS Safety Instrumented System

SML System Maturity Level

SRL System Readiness Level

SRS Safety Requirement Specification

STL Spurious Trip Level

SWIFT Structured What-IF Checklist

TQP Technology Qualification Programme

TML Technology Maturity Level

TRL Technology Readiness Level

Appendix B

HAZID

This HAZID is a compilation of the different risk analysis and HAZIDs worked out for the SFTB concept. The HAZID only considers the operational phase of the SFTB and only includes the hazardous event relevant for identifying safety systems. The risks are ranked according to the risk matrix presented in figure B.1. It is noted that several other hazardous events and hazards are relevant for the SFTB concept, and only a handful is included in this HAZID.

Table B.1: HAZID with some relevant hazardous events

No.	Hazardous event	Causes	Risk Freq	Risk Cons	Risk RPN	Possible Consequences	Risk Reducing Measures
1	Structure weighing too much or too little	Water leakage, Erosion of concrete, Poor workmanship, Weak joints, Design Errors, Marine growth	1	5	6	Structural damage, Flooding of the lanes, Weight overload, Collapse,	A well structured maintenance strategy, Simple and robust design, Regularly inspections, Systems for measuring influx of water, Design to survive partial water filling, Booms/gates and signals for closing of the tube entrances, Pump system to remove water, Weight monitoring, Variable message signs
2	Ship collisions to the pontoons	Pontoons poorly marked, Wrong navigation from the ship (human error), Technical error on ship Ship not aware of structure	2	3	5	Damage to tube if weak link is not functioning as planned, SFT is closed down	Dedicated ship surveillance and control centre, Making the pontoons visible over long distances, Redundancy of pontoons
3	Power shortage in the tubes	Failure in wiring, Power is cut externally by mistake	1	3	4	No visibility, Traffic accidents, Loss of oxygen supply	Emergency power supply, A well structured maintenance strategy for power supply, Good communication with local authorities, Good mapping of power supply and grid
4	Fire/explosion in the tube	Technical errors in vehicles, Collisions, Electrical failures, Overheated brakes, Leakage of hazardous cargo	3	5	8	Injuries, fatalities and structural damage	Emergency power supply, Ventilation with smoke extraction, Automatic incident detection system, Gates/booms and signals to close off entrances, Sufficient escape routes, Fixed firefighting system, Variable message signs
5	Traffic accidents	Obstructions in the road, Low visibility, Inattentive driving (human error), Sudden change of light	4	3	7	Injuries, fatalities and structural damage	Automatic incident detection, Variable message signs, Pollution monitoring, Signals and Booms/gates to close of the tube, Emergency ramps, Good traffic control, Automatic traffic controls.
6	Too high pollutant level in the tunnel	Emission from vehicles, Fires, No air draft in the tunnel, confined space	2	2	4	Health problems for motorists, Poisoning, Traffic accidents	Correct dimensioned Ventilation system, Avoid queues, Pollution monitoring, Surveillance of traffic in the tunnel.

Figure B.1: Risk matrix

Bibliography

API (2009). *API-RP-17N Recommended Practice for Subsea Production System Reliability and Technical Risk Management*. American Petroleum Institute, 1st edition. Recommended Practice.

Barnard, G. S. (2013). *Safety Instrumented Systems*, pages 555–592. Wiley-VCH Verlag GmbH & Co. KGaA.

Ben-Haim, Y. (1995). A non-probabilistic measure of reliability of linear systems based on expansion of convex models. *Structural Safety*, 17(3):91–109.

Ben-Haim, Y. and Elishakoff, I. (1995). Discussion on: A non-probabilistic concept of reliability. *Structural Safety*, 17(3):195–199.

Blanchard, B. S. (2008). *System Engineering Management*. Wiley & Sons inc, 4 edition.

CCPS (2001). *Layer of Protection Analysis: Simplified Process Risk Assessment*. Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York.

Cheok, G., Franaszek, M., Itai Katz, A. L., Saidi, K., and Scott, N. (2010). Assessing technology gaps for the federal highway administration digital highway measurement program. *FHWA Grant DTFH61-09-X-30011, NISTIR 7685*. Construction Metrology and Automation Group, Building and Fire Research Laboratory.

DNV (2011). *DNV-RP-A203, Qualification of New Technology*. Det Norske Veritas, Høvik, Norway, 2nd edition. Recommended Practice.

Duijm, N., Madsen, M., Andersen, H., Hale, A., Goossens, L., Londiche, H., and Debray, B. (2003). Assessing the effect of safety management efficiency on industrial risk. *ESREL 2003*.

EN-50126 (1999). Nek en:50126 railway applications - the specification and demonstration of reliability, availability, maintainability and safety (rams). Norsk Elektronisk Komite.

Garathun, M. G. (2015). Verdens første rørbru kan stå ferdig i 2025. *Teknisk Ukeblad*. Retrievied from http://www.tu.no/artikler/verdens-forste-rorbru-kan-sta-ferdig-i-2025/275689.

Harms-Ringdahl, L. (2003). Assessing safety functions—results from a case study at an industrial workplace. *Safety Science*, 41(8):701 – 720.

Hasle, J. R., Kjellén, U., and Haugerud, O. (2009). Decision on oil and gas exploration in an arctic area: Case study from the norwegian barents sea. *Safety Science*, 47(6):832 – 842. Occupational Accidents and Safety: The Challenge of Globalization / Resolving multiple criteria in decision-making involving risk of accidental loss.

Hauge, S., Lundteigen, M. A., Hokstad, P., and Håbrekke, S. (2009). Reliability prediction method for safety instrumented systems, pds method handbook 2010 edition. SINTEF A13503.

Hollnagel, E. (2004). *Barriers and accident prevention*. Ashgate Publishing, Aldershot, Hampshire, UK.

Hother, J. A. and Hebert, B. J. (2005). Risk minimization by the use of failure mode analysis in the qualification of new technology - recent project experience. In *SPE Annual Technical Conference and Exhibition,*. Society of Petroleum Engineers. SPE-96335-MS.

IEC-60050-191 (1990). International electrotechnical vocabulary. chapter 191: Dependability and quality of service. International Electrotechnical Commission.

IEC-61508 (2010). Functional safety of electrical/electronic/programmable electronic safety-related systems (e/e/pe, or e/e/pes). International Electrotechnical Commission.

IEV-191-04-01. Dependability and quality of service. international electrotechnical vocabulary online database. Available on line: http://std.iec.ch/iec60050. Access date: 05/05/2016.

Johansen, I. L. (2016). Technology qualification of extreme fjord crossings. In *Preeceedings of the ASME 2016 35th International Conference on Ocean, Offshore and Arctic Engineering*. Norwegian Public Road Administration. OMAE2016-54419.

Johansen, I. L. and Rausand, M. (2014). Defining complexity for risk assessment of sociotechnical systems: A conceptual framework. *Journal of Risk and Reliability*, 228(3):272–290. Department of Production and Quality Engineering, Norwegian University of Science and Technology, Trondheim, Norway.

Johnson, W. G. (1980). *MORT safety assurance systems*. Occupational Safety and Health Series. Marcel Dekker Inc, New York.

Kecklund, L. J., Edland, A., Wedin, P., and Svenson, O. (1996). Safety barrier function analysis in a process industry: A nuclear power application. *International Journal of Industrial Ergonomics*, 17(3):275 – 284.

Knaggs, M., Ramsey, J., Unione, A., Harkreader, D., Oelfke, J., Keairns, D., and Bender, W. (2015). Application of systems readiness level methods in advanced fossil energy applications. In *Procedia Computer Science 44 (2015)*, volume 2015 Conference on Systems Engineering Research, page 497 – 506. National Energy Technology Laboratory,.

Kossiakoff, A., Sweet, W. N., Seymour, S. J., and Biemer, S. M. (2011). *Systems Engineering Principles and Practice*. John Wiley & Sons, Inc, Hoboken, NJ, second edition.

Kratzmeir, S. and Lakkonen, M., editors (2008). *Road tunnel protection by water mist systems: implementation of full scale fire test results into a real project*, volume Proceedings from the Third International Symposium on Tunnel Safety and Security, Stockholm, Sweden. Swedish National Road and Transport Research Institute (VTI).

Kujawski, E. (2013). Analysis and critique of the system readiness level. *IEEE Transactions on Systems Man and Cybernetics*, 43(4).

Larssen, R. M. and Jakobsen, S. E. (2010). Submerged floating tunnels for crossing of wide and deep fjords. *Procedia Engineering*, 4:171–178.

Liu, Y. (2014). Discrimination of low- and high-demand modes of safety-instrumented systems based on probability of failure on demand adaptability. *Journal of Risk and Reliability*, 228(4):409–418.

Liu, Z. G., Kashef, A., Lougheed, G., and Kim, K. (2007). Challenges for use of fixed fire suppression systems in road tunnel fire protection. *Fire Research Program, Institute for Research in Construction*. Ottawa, Canada.

Lundteigen, M. A. (2008). *Safety instrumented systems in the oil and gas industry: Concepts and methods for safety and reliability assessments in design and operation*. PhD thesis, Norwegian University of Science and Technology.

Lundteigen, M. A. and Rausand, M. (2009a). Architectural constraints in {IEC} 61508: Do they have the intended effect? *Reliability Engineering & System Safety*, 94(2):520 – 525.

Lundteigen, M. A. and Rausand, M. (2009b). Reliability assessment of safety instrumented systems in the oil and gas industry: A practical approach. *International Journal of Reliability, Quality and Safety Engineering*, 16(02):187–212.

Lundteigen, M. A., Rausand, M., and Utne, I. B. (2009). Integrating rams engineering and management with the safety lifecycle of iec 61508. *Reliability Engineering and System Safety*, 94:1894–1903.

Magtaggart, R. (2012). Technology qualification: Recommended practice for subsea applications. *Oil and Gas Journal*, 110(10):A38–A41.

Mankins, J. C. (1995). Technology readiness levels: A white paper. *Advanced Concepts Office*. Office of Space Access and Technology.

Mankins, J. C. (2009). Technology readiness assessments: A retrospective. *Acta Astronautica*, 65(9–10):1216 – 1223.

Martin, J. N. (1996). *Systems Engineering Guidebook: A Process for Developing Systems and Products*. CRC Press.

Mawhinney, J. R. and Back, G. G. (2016). *Water Mist Fire Suppression Systems*, chapter 46, pages 1587–1645. SFPE Handbook of Fire Protection Engineering. Springer New York. ISBN: 978-1-4939-2564-3.

McConkie, E., Mazzuchi, T. A., Sarkani, S., and Marchette, D. (2013). Mathematical properties of system readiness levels. *Systems Engineering*, 16(4). Wiley Periodicals, Inc.

Murthy, D. N. P., Rausand, M., and Østerås, T. (2008). *Product Reliability: Specification and Performance*. Springer.

NATO-AVT-092 (2009). *NATO AVT-092 - Qualification by Analysi, Certification par analyse*. NATO.

NORSOK-S-001 (2008). Norsok s-001 technical safety.

NPD (2013). *Implementation of projects implemented on the norwegian shelf*. Norwegian Petroleum Directorate, Oslo. Norwegian Petroleum Directorate.

NPRA (2000). *V710 Project Overview Planning*. Norwegian Public Road Administration. Vegdirektoratet.

NPRA (2012). *V760 Management of Road Projects*. Norwegian Public Road Administration. Vegdirektoratet.

NPRA (2013). *AID i tunnel, Teknologisammenligning*. Oslo. Norwegian Public Road Administration, Vegdirektoratet.

NPRA (2014). *N500 Road Tunnel Engineering*. Norwegian Public Road Administration. Norwegian Public Road Administration.

NPRA (2015). *Manual V729: VEG-RAMS Premisser for planlegging, prosjektering, bygging og rehabilitering av vegtunneler*. Norwegian Public Road Administration. Vegdirektoratet.

OLF-070 (2004). Guidelines for the application of iec 61508 and iec 61511 in the petroleum activities on the continental shelf.

Rahimi, M. and Rausand, M. (2015). Technology qualification program integrated with product development process. *International Journal of Performability Engineering*, 11(1):03–14. Department of Production and Quality Engineering, Norwegian University of Science and Technology, Trondheim, NORWAY.

Rausand, M. (2011). *Risk Assessment, Theory, Methods and Applications*. Statistics in practice. John Wiley and Sons Inc, Hoboken, NJ.

Rausand, M. (2014). *Reliability of Safety-Critical Systems: Theory and Applications*. Wiley, Hoboken, NJ.

Sabetzadeh, M., Falessi, D., Briand, L., Alesio, S. D., McGeorge, D., Åhjem, V., and Borg, J. (2011). Combining goal models, expert elicitation, and probabilistic simulation for qualification of new technology. In *2011 IEEE 13th International Symposium on High-Assurance Systems Engineering (HASE)*, pages 63–72, Boca Raton, FL.

Samarakoon, S. M. S. M. K. and Gudmestad, O. T., editors (2011). *On the necessity of technology qualification in the offshore wind energy industry*, volume ASME 2011 30th International Conference on Ocean, Offshore and Arctic Engineering. Faculty of Science and Technology, University of Stavanger, Norway.

Sauser, B., Ramirez-Marquez, J., Verma, D., and Gove, R. (2006). From trl to srl: The concept of systems readiness levels. In *Conference on Systems Engineering Research, Los Angeles, CA, April 7-8, 2006*, Hoboken, NJ 07030. Stevens Institute of Technology.

Sauser, B., Ramirez-Marquez, J. E., Magnaye, R., and Tan, W. (2008). A systems approach to expanding the technology readiness level within defense acquisition. *International Journal of Defense Acquisition Management*, 1:39–58. ISSN 1940-3445.

SEMATECH (1995). *SEMATECH Qualification Plan, Guidelines for Engineering*. SEMATECH, Inc.

Setoyama, S., Ichikawa, A., Shimizu, K., Gunki, S., and Kimura, T. (2004). Effective operation of water spray systems for a tunnel fire. *Tunnel Management International*, 7(2):47–50. ISSN: 1463-242X.

Sklet, S. (2006). Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries*, 19:494–506.

Sklet, S. and Hauge, S. (2004). *Probabilistic Safety Assessment and Management: PSAM 7 — ESREL '04 June 14–18, 2004, Berlin, Germany, Volume 6*, chapter Reflections on the Concept of Safety Barriers, pages 94–99. Springer London, London.

Smith, D. J. and Simpson, K. G. L. (2011). *Safety Critical Systems Handbook: A Straightforward Guide to Functional Safety: IEC 61508*. Elseveier Ltd, The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, UK, third edition.

Starke, H. (2010). Fire suppression in road tunnel fires by a water mist system – results of the solit project. In *Fourth International Symposium on Tunnel Safety and Security*, Frankfurt am Main, Germany.

Torres-Echeverria, A. C. (2015). On the use of lopa and risk graphs for sil determination. *Journal of Loss Prevention in the Process Industries*.

Tveit, P. (2010). Submerged floating tunnels (sfts) for norwegian fjords. *Procedia Engineering*, 4:135–143.

Wighus, R. (2012). Active fire fighting systems. evaluation of the sintef medium- and large-scale tests 1999-2001. Trondheim, Norway. SINTEF NBL as.

Yasseri, S. (2013). Subsea system readiness level assessment. *International Journal of the Society for Underwater Technology*, 31(2):77–92.