University of Stavanger

Faculty of Science and Technology

MASTER'S THESIS

Study program/ Specialization: Master in Risk Management – Offshore Safety	Spring semester, 2013 Open / ~~Restricted access~~
Author: Aleksander Matland	…… (Writer's signature)

Faculty supervisor: Terje Aven

External supervisor(s): Vidar Kristensen (Petroleum Safety Authority Norway)

Title of thesis: Suggestion of a new definition of risk in the Frameworks Regulations: possible implications for the process of establishing fire and explosions loads to be used as a basis for design

Credits (ECTS): 30 SP

Key words: design accidental load, dimensioning accidental load, DAL, risk analysis, ALARP	Pages: 41 + enclosure: 5 Stavanger, 14.06.2013 Date/year

Summary

The Petroleum Safety Authority Norway has suggested an update of the definition of risk in the regulations that concerns the health, safety and environment for Norwegian petroleum operations. The prevailing definition of risk, given in the guidelines to Section 11 in the Frameworks Regulations, is that “Risk means a combination of probability and consequence” (Petroleum Safety Authority Norway, 2011c). The suggestion for a new definition is that: “Risk means the consequences of the activity with associated uncertainty” (Petroleum Safety Authority Norway, 2013). This thesis will not address the wide range of potential implications of the new definition, but focus on the process of establishing accidental loads from explosions and fires that a facility shall be designed to withstand. This thesis suggests some principles and ideas related to two new methods of establishing the fire and explosion loads that an installation should be able to withstand, that will be in compliance with the suggested new definition of risk. The suggestions acknowledges that the accidental loads cannot be selected based alone on results from quantitative risk analyses, and that there are uncertainties that have to be assessed that is not reflected on computed probabilities and expected values.

In addition, it is shown in this thesis that there is confusion surrounding the terminology used to describe these loads, and a suggestion is given on how to clear up this confusion.

Preface

This thesis has been written during spring 2013 at the PSAs offices in Stavanger, and represents the completion of my M.Sc. in Risk Management. Writing the thesis has been a valuable experience, and I have gained valuable insights into the regulatory system that regulates the Norwegian petroleum activities.

I would like to thank my supervisor at the faculty, Professor Terje Aven, for always replying quickly and providing good feedback. I would also like to thank Vidar Kristensen, who worked at the PSA when I started my thesis, for letting me write the thesis at the PSA and for contributing with good guidance and feedback.

Stavanger, June 2013

Aleksander Matland

Content

1 Introduction

1.1 Background

The background for this thesis is a suggested update of the definition of risk in the HSE regulations for Norwegian petroleum activities. The prevailing definition of risk, given in the guidelines to Section 11 in the Frameworks Regulations, is that "Risk means a combination of probability and consequence" (Petroleum Safety Authority Norway, 2011b). The suggestion for a new definition is that: "Risk means the consequences of the activity with associated uncertainty" (Petroleum Safety Authority Norway, 2013).

The new definition may lead to several changes in the regulations and in the way the petroleum industry understands, analyze and manage risk. This thesis will not address the wide range of possible implications of the new definition but focus on the process of establishing accidental loads from explosions and fires that a facility shall be designed to withstand.

Loads to be used as basis for the design of a facility are today typically stipulated by the use of a risk analysis, and are typically close connected to the loads that will appear with an annual frequency of 10^{-4}. The main reason for this is the requirement stated in Section 11 in the Facilities Regulations (Petroleum Safety Authority Norway, 2012c). These loads are presented in a DAL-specification, where DAL is an abbreviation that may be interpreted as dimensioning accidental load, or design accidental load.

1.2 Problem

If the definition of risk is changed, how will it affect today's practice of establishing accidental loads from explosions and fires? Will today's practice be in compliance with the updated regulations, and if not – which changes will appear? Today's close link of the accidental loads and the $1*10^{-4}$ frequency is of many thought to be unfortunate. There are several other requirements in the regulations that have to be fulfilled, so if the accidental loads are established mainly on one requirement this would not be in accordance with the authorities' intentions in the regulations.

The abbreviation DAL is today being interpreted as either dimensioning accidental load or design accidental load, and these two terms are being interpreted differently in the industry. This confusion surrounding terminology is unfortunate, and should not be necessary.

1.3 Purpose

The purpose of this thesis is to suggest some principles and ideas related to new methods of establishing accidental fire and explosion loads that an installation should be designed to withstand, that will be in compliance with the suggested new definition of risk. In addition, a suggested interpretation of the terms DAL, design accidental loads and dimensioning accidental loads will be given to clear the confusion surrounding the terms.

1.4 Outline of thesis

This thesis is organized as follows. Chapter 2 is a summary of the different interpretations of the abbreviation DAL and the terms design accidental load and dimensioning accidental load. Chapter 3 is a brief summary of the relevant requirements for the establishment of fire and explosion loads that an installation should be designed to withstand. In chapter 4, the existing definition of risk and

the suggested new definition of risk are presented and briefly discussed. Today's process of establishing accidental fire and explosion loads is described in chapter 5, followed by suggestions related to two methods that could be used for establishing these loads in line with the suggested new risk definition in chapter 6. Finally, the thesis ends with a discussion and a conclusion in chapter 7 and 8, respectively.

2 Dimensioning accidental load, design accidental load and DAL

The accidental loads from fires and explosions that a facility are designed to withstand is typically gathered in a DAL-specification. The abbreviation DAL is however not clearly defined. The regulations do not use this abbreviation at all, but the standards NORSOK Z-013 and NORSOK S-001 defines DAL as "dimensioning accidental load" (Standards Norway, 2010) (Standards Norway, 2008). In several DAL-specifications the abbreviation DAL is defined as "design accidental load" and in the book "Offshore Risk Assessment by Vinnem (2007) the abbreviation is defined as "design accidental load".

This would of course not be a problem if the terms design accidental load and dimensioning accidental load had a clear definition that was generally agreed upon. This is however not the case. The following definitions illustrate the variation related to how these terms are understood:

The Norwegian version of the Facilities Regulations: "Dimensioning accidental load: An accidental load/action that the facility or a function shall be able to withstand for a defined period of time." (Petroleum Safety Authority Norway, 2012c)

The English version of the Facilities Regulations: "Design accidental load: An accidental load/action that the facility or a function shall be able to withstand for a defined period of time." (Petroleum Safety Authority Norway, 2012c)

NORSOK S-001: "dimensioning accidental load (DAL): most severe accidental load that the function or system shall be able to withstand during a required period of time, in order to meet the defined risk acceptance criteria." (Standards Norway, 2008)

NORSOK Z-013: "design accidental load: chosen accidental load that is to be used as the basis for the design

Note 1 The applied/chosen design accidental load may sometimes be the same as the dimensioning accidental load (DAL), but it may also be more conservative based on other input and considerations such as ALARP. Hence, the design accidental load may be more severe than the DAL.

Note 2 The design accidental load should as minimum be capable of resist the dimensioning accidental load (DAL).

dimensioning accidental load DAL: most severe accidental load that the function or system shall be able to withstand during a required period of time, in order to meet the defined risk acceptance criteria

Note 1 DAL is normally defined based on DAE.

Note 2 The dimensioning accidental load (DAL) are typically generated as a part of a risk assessment, while the design accidental load may be based on additional assessments and considerations.

Note 3 The dimensioning accidental load (DAL) are typically established as the load that occurs with an annual probability of $1*10^{-4}$." (Standards Norway, 2010)

As seen above, the regulations use both the term design accidental load and dimensioning accidental load and define them similarly, depending on whether the Norwegian or English version is read. That the regulations use both the terms dimensioning and design accidental load depending on whether the Norwegian or the English version of the regulations is read is unfortunate, and certainly

does not help to clear any confusion. The NORSOK S-001 defines and uses only the term dimensioning accidental load, but specifies that this is closely connected to the defined risk acceptance criteria, a specification that is not seen in the regulations. NORSOK Z-013 defines dimensioning accidental loads similarly to the NORSOK S-001, but specifies that the risk acceptance criteria used typically is an annual occurrence of the load of $1*10^{-4}$.

Compared to the other standards and regulations mentioned above, revision 3 of NORSOK Z-013, issued in 2010, defines the term design accidental load as well, and states that this should be the "final" load, and that this load could be more severe than the load that occurs with an annual probability of $1*10^{-4}$ based on for instance ALARP-considerations or other inputs.

This could be seen as an acknowledgment of that when establishing the accidental loads that an installation should be able to withstand, the NORSOK Z-013 standard has previously only focused on the loads occurring with the annual probability of $1*10^{-4}$, which is not in line with the regulations as can be seen by the definitions of dimensioning accidental load/design accidental load in the regulations.

The attempt to clear the confusion surrounding the two terms in the newest revision of NORSOK Z-013 is reasonable. The definition of the term design accidental load in NORSOK Z-013 can be interpreted similar to the definition found in the regulations, and underlines that the accidental loads that an installation or facility should be designed to withstand must be based on more than just results from a QRA. If the two definitions in NORSOK Z-013 are followed up by other standards, and the Norwegian version of the Facilities Regulations changes the use of dimensioning accidental load to design accidental load, at least the theory would be consistent.

However, this is a bit cumbersome. Considering that the two terms design accidental load and dimensioning accidental load are very similar, and that it makes sense to say that an installation shall be dimensioned to withstand loads and designed to withstand loads, some confusion surrounding the two terms seems inevitable. That confusion seems inevitable is also the case for the abbreviation DAL, considering that both the terms can be abbreviated to the abbreviation DAL.

The easiest solution would be to define both of the terms in a similar way, similar to the definition found in the Facilities Regulations or similar to the definition of design accidental load in NORSOK Z-013. This way, both of the terms would in theory have the same meaning and none of them would be associated with the load that occurs with the annual probability of $1*10^{-4}$. The definitions should be similar to the suggestion below:

Dimensioning accidental load/design accidental load: An accidental load/action that the facility or a function shall be able to withstand for a defined period of time (Petroleum Safety Authority Norway, 2012c).

If the wording from NORSOK Z-013 should be used, it would look like this:

Dimensioning accidental load/design accidental load: chosen accidental load that is to be used as the basis for the design (Standards Norway, 2010).

Defining the terms as suggested above, this would further underline the fact that the loads that an installation or facility is designed to withstand should be based on more than just calculated

probabilities. These definitions would also make sense with the new definition of risk, as it will be shown later in this thesis that a change of definitions will demand that the selection of accidental loads must be based on more than calculated probabilities and expected values.

Since the term design accidental load in the NORSOK Z-013 can be interpreted similar to the definition from the regulations, this is the term that will be used for the rest of the thesis. The term dimensioning accidental load or the abbreviation DAL will not be used, unless when citing from standards. The term that will be used for the rest of the thesis will therefore be design accidental load, meaning the accidental load/action that the facility or a function shall be able to withstand for a defined period of time.

3 Norwegian legislation and industry standards

The regulations that concern health, safety and the environment in petroleum activities at the Norwegian Continental Shelf consist of the Framework Regulations, and four supplementary regulations. The four supplementary regulations are the Management Regulations, the Facilities Regulations, the Activities Regulations and the Technical and Operational Regulations.

The Framework Regulations provide a framework for petroleum activities for among other things responsibility, risk reduction-principles, principles relating to health, safety and the environment and provisions on working hours (Petroleum Safety Authority Norway, 2011a).

The four supplementary regulations contains overarching requirements relating to health, safety and the environment, and requirements regarding risk reduction, barriers, management elements, resources and processes, analyses and measuring, handling of nonconformities and improvement (Petroleum Safety Authority Norway, 2011a).

In addition to the five regulations, the Petroleum Safety Authorities Norway (PSA) has developed five guidelines connected to the different regulations. These guidelines are not legally binding per se, but they are developed to give the reader the best possible understanding of what the authorities wish to achieve by means of the regulations (Petroleum Safety Authority Norway, 2011a).

The different regulations are mainly built on functional requirements, meaning that the requirements should express what the supervisory authorities wish to achieve with the requirement, but not in detail how it should be achieved (Petroleum Safety Authority Norway, 2011a). In addition to these functional requirements, a couple of specific requirements are found in the regulations, and these are requirements that specifically states how they should be fulfilled. Normally, the functional requirements are elaborated in the guidelines, where it is stated how the requirements are recommended to be solved. This is typically done by pointing to recognized norms or industry standards.

The NORSOK standards are examples of the latter, and they are developed by the Norwegian petroleum industry to as far as possible replace oil company specifications and serve as references in the authorities' regulations (Standards Norway, 2008).

The foundation in the safety regime present for the oil- and gas-industry in Norway is to a large degree built on the principle that the different operating companies are fully responsible for being in compliance with the regulations. The principle is today based on internal control, which means that the authorities supervises the industry by ensuring that the operating companies have adequate management systems for ensuring that their operations are performed in a safe way, according to the regulations (Aven & Vinnem, 2007).

3.1 Requirements regarding the establishment of the design accidental loads from the regulations

The requirements relevant for the establishment of design accidental loads are found in the different regulations and standards. The regulations have some functional requirements that are relevant for the design accidental loads and some specific requirements that have to be implemented. Some of the functional requirements points to different standards, where NORSOK S-001 and NORSOK Z-013 contains the most relevant requirements on how to stipulate the design

accidental loads. The most central requirements or parts of requirements from the regulations regarding the design accidental loads will be mentioned here, for the entire sections see Appendix A.

Perhaps the most central requirement regarding the design accidental loads are found in Section 11 in the facilities regulations, where it states that "The loads/actions that can affect facilities or parts of facilities, shall be determined. Accidental loads/actions and environmental loads/actions with an annual probability greater than or equal to $1*10^{-4}$, shall not result in loss of a main safety function, cf. Section 7." (Petroleum Safety Authority Norway, 2012c) The guidelines to this section states that the NORSOK S-001 standard should be used for accidental loads/actions (Petroleum Safety Authority Norway, 2012a). The main safety functions are listed in Section 7 of the Facilities Regulations, and are listed below:

- Preventing escalation of accident situations so that personnel outside the immediate accident area are not injured,
- maintaining the capacity of load-bearing structures until the facility has been evacuated,
- protecting rooms of significance to combating accidents so that they remain operative until the facility has been evacuated,
- protecting the facility's secure areas so that they remain intact until the facility has been evacuated,
- maintaining at least one escape route from every area where personnel are found until evacuation to the facility's safe areas and rescue of personnel have been completed. (Petroleum Safety Authority Norway, 2012c)

Section 5 in the Facilities Regulations states that "The facility's areas shall be classified such that design and location of areas and equipment contribute to reduce the risk associated with fires and explosions." (Petroleum Safety Authority Norway, 2012c) In the guidelines this requirement is elaborated, and it states that this requirement "…entails that a) the facility's main areas shall be classified to separate high-risk areas from low-risk areas" (Petroleum Safety Authority Norway, 2012a). Section 30 in the Facilities Regulations states that "the main areas on facilities shall be separated by fire divisions that can withstand the design fire and explosion loads/actions" (Petroleum Safety Authority Norway, 2012c). The term main areas are not further elaborated in the guidelines, but NORSOK Z-013 states that the following main areas shall as a minimum be defined (when relevant):

- Accomodation (living quarter)
- Utility
- Drilling and wellhead
- Process
- Hydrocarbon storage (Standards Norway, 2010)

The specific requirements in the regulations that are of relevance to the design accidental loads are mainly found in the Facilities Regulations – for instance Section 29, Section 30, Section 31, Section 32, Section 33, Section 34 and Section 35 (see appendix A).

Further requirements in the regulations that are relevant for the process of establishing the design accidental loads are Section 11 in the Frameworks Regulations that contain risk reducing principles, and Section 4, Section 5, Section 9 and section 17 in the Management Regulations. In Section 11 in

the Frameworks Regulations an important principle for risk reduction is found, the Norwegian version of the ALARP-principle. The section states that the risk shall be reduced to the extent possible, beyond the regulations minimum level (Petroleum Safety Authority Norway, 2011c). Section 9 in the Management Regulations states that the operator shall set acceptance criteria for major accident risk and environmental risk – including loss of main safety functions (Petroleum Safety Authority Norway, 2012). The acceptance criteria shall also be used when assessing results from risk analyses (Petroleum Safety Authority Norway, 2012). Section 17 in the Management Regulations regards risk analyses, and states among other things that risk analyses shall be performed, and the results shall be part of the basis for making decisions regarding identification and stipulation of design accidental loads (Petroleum Safety Authority Norway, 2012).

The ALARP-principle is a well-known principle when discussing risk. ALARP is an abbreviation that stands for As Low As Reasonable Practicable, and means that the risk should be reduced to a level that is as low as reasonable practicable. A common interpretation of the principle means that there are three levels of risk. At the first level the risk is unacceptable, at the second the risk is in the ALARP-area, and at the third the risk is negligible (Vinnem, Haugen, Vollen, & Grestad, 2006). Further the principle means that a risk reducing measures should be implemented unless it can be proved that implementing the measure would give an unreasonably disparity between the cost and the risk-reducing effect (Aven, 2008).

In the Norwegian regulations however, the ALARP-principle is implemented without any lower limit where the risk is to be considered negligible. The principle is illustrated below:

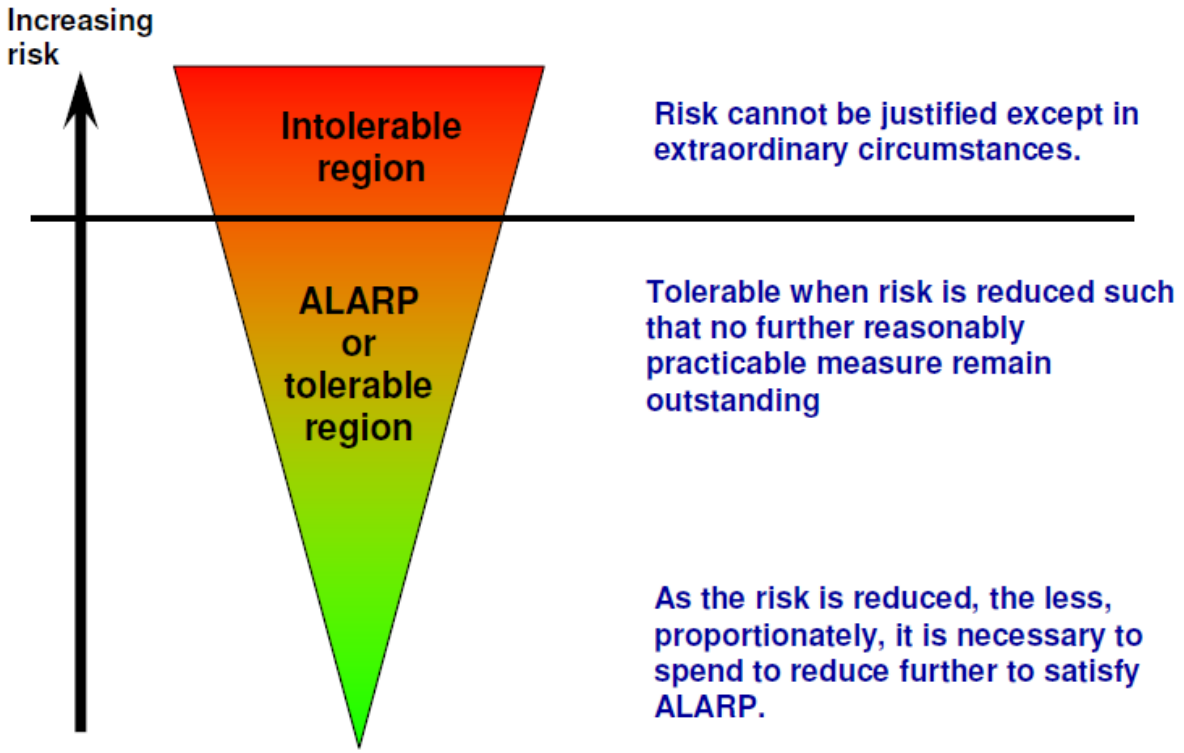


Figure 1 - The ALARP principle in the Norwegian regulations (Standards Norway, 2010)

3.2 Requirements from NORSOK S-001 and NORSOK Z-013

As mentioned above, the guidelines to Section 11 in the Facilities Regulations states that for accidental loads/actions, chapter 4.7 in the NORSOK S-001 should be used (Petroleum Safety Authority Norway, 2012a). This chapter states that the design accidental loads shall be established based on quantitative risk analysis and the comparison of estimated risk with risk acceptance and/or design criteria. The standard provides heat flux values to use for fires, and points to NORSOK Z-013 for a method for establishment of design explosion loads. The method for establishment of design explosion loads is found in Annex F in NORSOK Z-013, where the procedure for probabilistic explosion simulation is described. The details of how the establishment of the design accidental loads should be performed are described more thoroughly in chapter 5.

4 Definition of risk in the regulations

4.1 The existing definition of risk in the regulations

The existing definition of risk is found in the guidelines to the Framework Regulations where it says that "Risk means a combination of probability and consequence." (Petroleum Safety Authority Norway, 2011b) The definition is further elaborated with a subsection: "In the area of health, safety and working environment, this means a combination of probability of harm and the degree of severity of the harm in the form of fatalities, personal injuries or other health hazards, reduction in health condition or loss of financial assets. Risk of pollution means a combination of probability and consequence for the supply of solids, fluid or gas to air, water or the ground, as well as impact on the temperature, which is or can be harmful or disadvantageous for the environment." (Petroleum Safety Authority Norway, 2011b)

According to this definition, a description of risk should express information on the probability of events occurring, and probable consequences should the events occur. This definition is based on a quantitative approach, considering that it states that the use of probabilities is the only tool that should be used to assess risk (Aven & Vinnem, 2007). When expressing uncertainties probability-based analyses are used. How this is done depends on the interpretation of probability used by the assessor. There are primarily two ways of interpreting a probability, either as a relative frequency or as a measure of uncertainty about future events and consequences, seen through the eyes of the assessor and based on some background information and knowledge (Aven, 2010). The relative frequency interpretation sees a probability as the "relative fraction of times the events occur if the situation analyzed were hypothetically "repeated" an infinite number of times. The underlying probability is unknown, and is estimated in the risk analysis." (Vinnem, 2007) Which one of these two interpretations that the regulations are built on is not specifically stated in the regulations, but judging by the definition of risk, the other requirements in the regulations and the practice described in the NORSOK standards the relative frequency-interpretation is the prevailing one. In addition, according to Vinnem (2007), most professional analysts are trained in the relative frequency approach.

4.2 The suggested new definition

The following is the suggestion to the new definition, where the sentences mentioned in 3.1 will be replaced by the following:

"Risk means the consequences of the activity with associated uncertainty.
The term "consequences" is here meant as all the consequences the activity potentially may lead to. The term "consequences" are not only limited to the final consequences of the activity, such as for instance harm to or loss of human health and lives, environmental and material values, but does also include conditions and events that may result to or lead to this type of consequences. Consequences related to for instance major accidents means both unwanted events that potentially may lead to major accidents, those circumstances and factors that direct or indirect is of importance to whether the events will happen or not and the consequences if the events should take place. Consequences related to work-related illness and harm means both conditions and exposure that immediately or in longer term potentially may lead to illness or harm and the degree of disease or the harm in terms of deaths, personal injuries or other health-damages, reduction in health.

"Associated uncertainty" means uncertainty related to what the consequences of the activity may result in. Given the description of the consequences above, the uncertainty relates to for instance both what events may occur, how often they will occur, and to what damages on or loss of human life and health, environmental and material values the different events may result in.

The term "risk" relates to the activity, meaning a range of processes such as design of a facility, completion of a drilling operation or decision-processes related to a technical, operational or organizational change. The risk connected to the activity will in other words be dependent of the context one is facing, including the lack of knowledge, and whatever is being considered, planned and performed." (Petroleum Safety Authority Norway, 2013)

According to this definition, a risk description should contain information regarding the uncertainty regarding if events will occur and the uncertainty related to what consequences that potentially may occur. The main different from the existing definition is that the risk assessments become assessments of the uncertainties (Aven, 2010). However, these uncertainties will typically be described using probabilities, as it is a practical tool for doing so. The new definition will however mean that risk descriptions based on probabilities with a relative-frequency interpretation will not be sufficient (Aven, 2010). When probabilities are used to describe the uncertainty, a description of the background knowledge that the probabilities are built on is required.

4.3 Intentions behind the change

The guidelines to the five regulations are not legally binding per se, but the guidelines are developed to provide a deeper understanding of what the authorities mean by looking at the regulations and the guidelines together (Petroleum Safety Authority Norway, 2011a). The change of definition is in accordance with the international trends in risk research, and follows a pattern where more and more institutions and authorities change their definitions to include a broader focus on uncertainties, for instance the new definition of risk in ISO 31000 (ISO, 2009) or IRCG's definition of risk (International Risk Governance Council, 2008).

The intention behind the change of definition should thus be to clarify what the PSA mean in the regulations when they presents requirements regarding risk description and risk handling. The change from "risk means a combination of probability and consequence" to "risk means the consequences of the activity with associated uncertainty" is quite significant, and perhaps the clearest difference between the two is the lack of the term "probabilities" in the suggested new definition. This does not mean that there is a wish to avoid the use of probabilities to describe or calculate risk; it is more an acknowledgement of that risk should be more than a number calculated by using probabilities and expected consequences.

By just looking at the difference between the two definitions, this should be seen as a change of risk perspective from the PSA. This should have implications on the rest of the regulations, on industry standards and on references to industry standards when pointing to standards in functional requirements. However, changes will take time. Changing the regulations will take some time, and changes in the industry standards will take even more time – as they are not revised that often.

By looking at PSA publications the last few years, it is possible to set the suggested new definition of risk into context.

According to (Petroleum Safety Authority Norway, 2013), PSA recommends the oil- and gas-industry in Norway to further develop better tools for controlling major accident risk after the Deepwater Horizon accident and the industry's understanding and use of risk analysis is a subject that will be prioritized by the PSA throughout 2013.

In 2007, PSA published a letter to all the oil- and gas-companies operating at the Norwegian Continental Shelf, regarding what the PSA perceived as unacceptable use of risk calculations. One of the central points in the letter was the observation of use of risk calculations as an argument for setting aside specific requirements found in the regulations, and for selecting solutions that results in a poorer level of safety than the established minimum level (Petroleum Safety Authority Norway, 2007).

The latest version of the trends in risk level in the petroleum activity (RNNP) shows that there is room for improvement in the industry. Acting director of the PSA, Finn Carlsen, says among other things that (Petroleum Safety Authority Norway, 2013):

- We had a limited number of incidents, but those which did occur where serious. One event of that kind can unleash a disaster
- Its risk management must improve, and it must pay greater attention to managing risk associated with major accidents.
- Such incidents are characterized by a low probability that they will happen, but big potential consequences should they nevertheless occur.
- Even if their likelihood is low, we must plan for the unlikely happening, and not calculate or assess ourselves away from the problem.
- The industry must reverse the present trend now
- The barrier-related figures we see in the RNNP report aren't good enough. I'm talking about safety-critical barriers which fail to match recognized performance standards.
- The companies know there are barriers which don't function as they should, but do nothing about it. We can't have that. The companies must live up to their responsibilities here.

The three above-mentioned factors seem to reveal that the industry and the authorities do not agree upon what is correct handling of risk and how to perform risk analyses. A risk perspective that involves a focus on uncertainty, and that doesn't only focus on probabilities and consequences would have impacts on the handling of major accident risk. A major accident is defined in the guidelines to Section 9 in the Management Regulations, and is defined as "…an acute incident such as a major spill, fire or explosion that immediately or subsequently entails multiple serious personal injuries and/or loss of human lives, serious harm to the environment and/or loss of major financial assets." (Petroleum Safety Authority Norway, 2012b) Typically it is referred to as a situation characterized by a low probability and major consequences. Making decisions regarding the major accident risk without taking into account the different uncertainty-factors that may be "hidden" behind the probabilities and expected values calculated would not be in compliance with the suggested new definition of risk. In addition, the point that Finn Carlsen makes that the industry shouldn't calculate itself away from the problem even though the probability is low is interesting with respect to the design accidental loads, considering that further fire and explosion risk reducing measures are often disregarded if the installation already are designed to withstand design accidental loads that occurs with an annual probability of $1*10^{-4}$.

5 Today's practice of establishing design accidental loads with respect to fires and explosions

The design accidental loads describe the loads the installation in question should be designed to withstand. Installations are divided into several main areas, and design accidental loads must be established for all the main areas (Petroleum Safety Authority Norway, 2012c). The design accidental loads will have an impact on the layout, structure and choice of equipment and the need for additional measures (e.g. passive fire protection) that will have to be implemented, with respect to fire and explosion risk. Risk-reducing measures for fire and explosion may consist of many different measures, from changing the layout of the installation to applying passive fire protection on equipment and structural members. A more thorough list of risk-reducing measures is presented in chapter 5.2.1 and 5.3.1, for fire risk and explosion risk respectively.

The design explosion loads will be established for each main area based on the available amount of explosive materials, the layout and ventilation and the amount and type of equipment in the room that may generate turbulence. Similarly, the design fire loads will be established for each main area based mainly on the available amount of flammable materials and the time until depressurization.

Establishment of design accidental loads is relevant in two cases, either in the design process of a new facility, or in modification of existing facilities. There will be a significant difference between these two situations, but naturally also some similarities.

The major difference between the two situations is that when designing a new installation, the final layout is unknown. The design accidental loads will have to be established early in the design process, to know what loads the installation has to be designed to withstand. But later on in the final stages of design, or in the operations phase the congestion in the areas may deviate from the amount first stipulated. Norsok Z-013 recommends simplifying the procedure for calculation of the explosion risk to the design information available, and that the amount of equipment is based on equivalent areas in previous studies (Standards Norway, 2010).

The situation will be different when establishing/updating design accidental loads as a consequence of modification of existing installations. The congestion will be known to a larger degree, but some other interesting questions might be relevant. The existing risk level on the platform may not be in compliance with today's regulations depending on how old the installation is, due to the fact that new regulations are not given retrospective applicability on the Norwegian Continental Shelf (Aven & Vinnem, 2007).

The design accidental loads should according to NORSOK S-001 and NORSOK Z-013 be established based on a quantitative risk analysis (QRA), where the different contributors to fire and explosion risk should be identified. According to the regulations the operating companies should establish risk acceptance criteria that the calculated risk from risk analyses are compared with (Petroleum Safety Authority Norway, 2011c). The risk-acceptance criteria used when establishing the design accidental loads are often the requirement from section 11 in the Facilities Regulations, that the annual probability of occurrence for the design accidental loads shall be smaller than $1*10^{-4}$ (Petroleum Safety Authority Norway, 2012c). In addition, the design accidental loads must also be acceptable according to the other risk acceptance criteria that the operator has established (for instance PLL, FN-curves, FAR etc.). The specific requirements found in the facilities regulations regarding for

instance fire protection to the living quarter must be implemented, independent on the design accidental loads stipulated from the QRA results. ALARP considerations should also be performed in order to be in compliance with the regulations. The risk shall be reduced to the extent possible, and should at least in theory consist of the operator proving that additional risk reducing measures would be too expensive considering the risk reducing effect.

However, there are no clear requirements to how the ALARP-considerations should be performed or documented in the regulations or in the NORSOK standards. It has been shown that the understanding of the ALARP-principle varies quite a lot within the oil- and gas-industry in Norway (Vinnem, Haugen, Vollen, & Grestad, 2006). And according to Aven and Vinnem (2007), the present approach to risk analysis and evaluation is relatively mechanistic, which implies that it rarely is made much effort to further reduce the risk once the risk acceptance criteria are reached. If ALARP-evaluations are performed, possible risk reducing measures are identified, but quickly disregarded based on coarse cost-benefit analyses (Aven & Vinnem, 2007).

The way that the NORSOK standards describe the establishment of the design accidental loads are also implying that the ALARP-principle is not given much weight. The regulations point to NORSOK S-001 chapter 4.7 for establishment of the design accidental loads, and there it says that the loads "…shall be established based on quantitative risk analysis and the comparison of estimated risk with risk acceptance and/or design criteria" (Standards Norway, 2008). NORSOK Z-013 mentions that ALARP-considerations could lead to more severe design accident loads, but states that the foundation of the final loads should be loads stipulated from a QRA. In addition, when reading the Z-013 standard the main focus is on the QRA, and there is little mentioned on how the final loads should differ from the ones selected with the annual probability of occurrence of $1*10^{-4}$.

This should show that the focus on other requirements than the $1*10^{-4}$ is weak, but at least the newest revision of NORSOK Z-013 acknowledges this. The difference between the two standards could be due to the fact that the latest revision of the Z-013 standard was done in 2010, whereas the latest revision of the S-001 standard was done in 2008. It is hard to say just from NORSOK standards how the industry defines these terms, considering that revising a standard may take a long time, so it may not be "up to date" at all times. However, the NORSOK S-001 was last updated in 2008, so it should be realistic to assume that the methods presented are still quite representative for the industry.

The description of today's method will therefore not describe any ALARP-evaluations, even though some companies may perform these.

5.1 Fire loads

The procedure for establishing the design fire loads are found in NORSOK S-001, and consist of establishing the loads that will occur with an annual probability of $1*10^{-4}$. NORSOK S-001 states that "DALs shall be established based on quantitative risk analysis and the comparison of estimated risk with risk acceptance and/or design criteria" (Standards Norway, 2008) and that "Dimensioning load shall not cause loss of safety functions or escalation (locally)." (Standards Norway, 2008) For the fire/heat loads, the table found in Figure 2 is to be used, unless a probabilistic risk assessment of the fire risk is performed.

	Jet fire		Pool fire
	For leak rates m > 2 kg/s kW/m^2	For leak rates 0,1 kg/s < m < 2 kg/s kW/m^2	kW/m^2
Local peak heat load	350	250	150
Global average heat load	100	0	100

Figure 2 - Heat flux values (Standards Norway, 2008)

"The local peak heat load exposes a small area of the process segment or of the structure to the peak heat flux. The local peak heat load, with the highest heat flux, determines the rupture temperature of different equipment and piping within the process segment. The local peak heat load has marginal influence on the pressure profile within the process segment.

The global average heat load represents the average heat load that expose a significant part of the process segment or structure. The global average heat load provides the major part of the heat input to the process segment and, hence, affects the pressure in the segment." (Standards Norway, 2008)

According to Vinnem (2007), the main characteristics of a fire are heat loads, dimensions of fire and the duration of fire. If the table above is used, the only consideration to consider is the duration of the fire, which will be determined by how much flammable material that is available and the depressurization time, which is the time until the feeding of the fire has descended to a manageable level. The following factors will be important to consider, volumes of ESD segments and depressurization capacities and times (Vinnem, 2007).

As seen in the table above, there are two time segments to consider, first the time until the leak rate has descended to below 2 kg/s and then the time until the leak rate is between 0,1 kg/s and 2 kg/s. By considering the volumes of ESD segments and the depressurization capacities different fire scenarios will be studied, and the accumulated fire frequency as a function of duration will be calculated. First fires with different durations until the leak rate is below 2 kg/s will be presented with associated frequency per year, and the durations that will appear with a frequency of $1*10^{-4}$ will be selected as the design accidental load. The same exercise will be performed for the frequency of fires with durations until the leak rate is below 0.1 kg/s.

These two design fire loads will be calculated for the different main areas on a facility, and if the main areas are large enough several design fire loads may be calculated.

The design accidental loads for fires are thus a combination of deterministic and probabilistic methods. The heat flux values are given, but the duration the area has to resist the different values will have to be stipulated. The values shown in Figure 2 are somewhat conservative (Vinnem, 2007), but they are valid for use for all facilities unless specific fire analysis is performed.

5.1.1 Risk reducing measures with respect to fire risk

According to Vinnem (Vinnem, 2007) and ISO 13702 (International Standard Organization, 1999) relevant risk reducing measures for fire risk is:

- Installation layout

- Emergency shutdown systems and blowdown
- Control of ignition
- Control of spills
- Emergency power systems
- Fire and gas systems
- Active fire protection
- Passive fire protection
- Inspection, testing and maintenance

5.2 Explosion loads

Similarly to the establishment of design fire loads, the NORSOK S-001 states that "DALs shall be established based on quantitative risk analysis and the comparison of estimated risk with risk acceptance and/or design criteria" (Standards Norway, 2008) and that "Dimensioning load shall not cause loss of safety functions or escalation (locally)." (Standards Norway, 2008) The following two requirements are also stated:

- "Dimensioning explosion loads shall be established using a recognized method (e.g. NORSOK Z-013) and representative geometric explosion model. The loads shall be defined for relevant local horizontal and vertical area dividers (pressure and impulse from explosion and equipment (pressure/drag forces);
- Explosion loads shall also be defined for areas external to the initial explosion location (typical LQ, utility modules etc.);" (Standards Norway, 2008)

As seen above, pressure and impulse loads for walls and roofs have to be established, and pressure/drag forces for equipment. The rationale behind the drag forces for equipment is that the load that subjects equipment inside an exploding gas cloud will not directly be resolved by the explosion simulation code. To calculate this load a drag formula has to be used that references the flow conditions. (Bjerketvedt, Bakke, & van Wingerden, 1993)

The calculation of explosion loads on a structure and its response follows a similar series of steps to those used in fire analysis:

1. Calculation of releases of hydrocarbon
2. Calculation of explosion overpressure loads as a function of time
3. Calculation of structural response to the time dependent overpressure loads
4. Evaluation of secondary blast effects, such as missiles, etc. (Vinnem, 2007)

The establishment of design explosion loads is based on probabilistic evaluation, much more than the establishment of the design fire loads as everything will have to be simulated.

NORSOK S-001 points to NORSOK Z-013 for a recognized method for establishing design explosion loads. The following model is presented as the schematics of procedure for calculation of explosion risk:

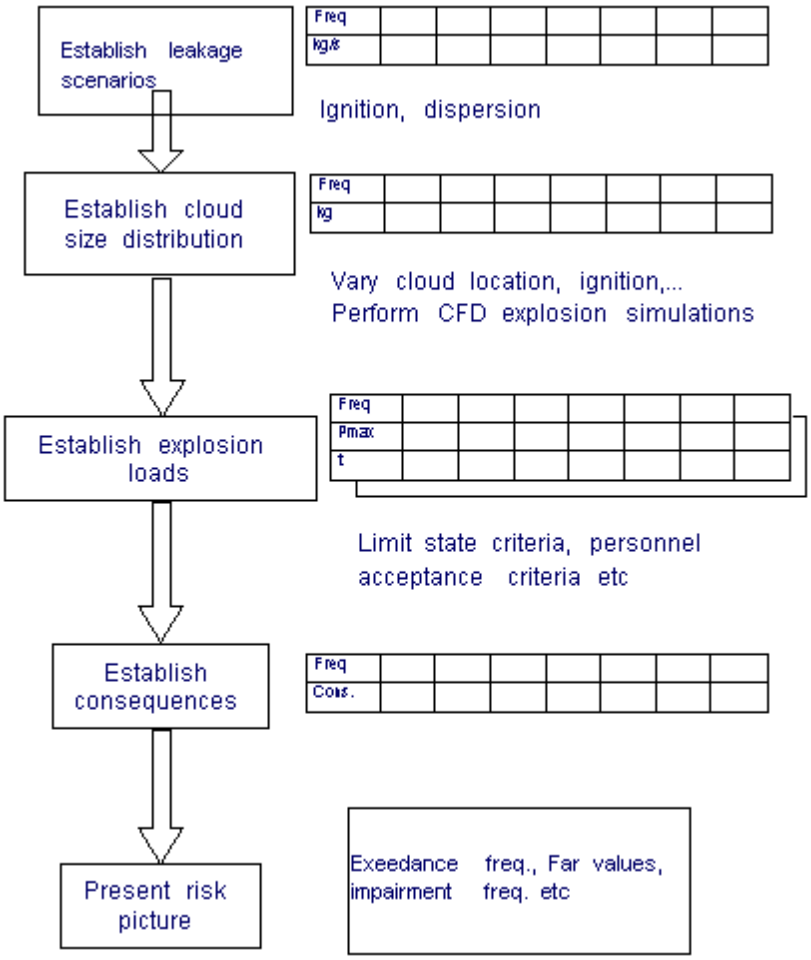


Figure 3- Schematics of Procedure for calculation of explosion risk (Standards Norway, 2010)

For selection of the design explosion load, the load that with an annual frequency of 10^{-4} will cause loss of a main safety function will typically be selected. To determine this load, a probabilistic distribution of explosion loads will be established using probabilistic risk assessment. The loads have to be calculated for the walls and roof in the shape of pressure and impulse from explosion, and for equipment as pressure/drag forces.

All of the parameters mentioned above, and other eventual parameters that are included in the evaluation has to be presented with their own probability distributions. The whole event sequence up to an explosion will have to be determined, and every event has to be given statistical values, so that it is possible to calculate probabilities for the different explosion scenarios. This is typically done by considering historical leak rates and historical failure rates, and converting these into probabilities. In the cases where there is little historical failure rates available, expert judgment will be used. In addition to rates, several phenomena have to be assumed having a certain outcome – and here assumptions must be made in order to be able to calculate the probabilities. For instance gas cloud sizes, ignition places etc.

5.2.1 Risk reducing measures with respect to explosion risk

When it comes to risk reducing measures for explosion risk, the following are listed by Vinnem (Vinnem, 2007):

- Prevent gas leaks through design, for instance reducing the number of flanges
- Prevent gas leaks from operations,
- Prevent ignitable concentration
- Prevent ignition
- Prevent high turbulence
- Prevent high blockage
- Install fire and blast barriers
- Activate deluge on gas leaks
- Improve resistance of equipment and structures

5.3 Strengths and weaknesses

5.3.1 Strengths

The most obvious strength with the practice of establishing design explosion and fire loads is that the process is well-established and pretty much straight-forward. It appears to be convenient, in the sense that it is easy for the oil- and gas-companies to know what to do to be in compliance with the regulations.

Another factor that contributes to making it convenient for both the companies and the oil- and gas-companies is that the regulations in its present state in practice give an answer to when the explosion and fire risk is low enough. By showing with a QRA that both the risk acceptance criteria for the total risk of an installation is met, and that the risk of impairment of main safety functions is below an annual probability of $1*10^{-4}$, the fire and explosion risk could be considered to be low enough. This seems to be a misinterpretation of the regulations, which demands risk reduction beyond the minimum level found in the regulations, but nonetheless it gives the operating companies a specific minimum risk level. In addition to knowing what risk levels to achieve with respect to fires and explosion, the regulations together with the NORSOK-standards also give a method for achieving these levels as the Facilities Regulations refers to the NORSOK S-001 for establishment of accidental loads (Petroleum Safety Authority Norway, 2012a).

Another strength is that the use of a QRA will give a thorough evaluation of the system in question. It will consider thousands of scenarios that involve multiple failures and increase the probability that complex interactions will be identified, among others (Apostolakis, 2004).

5.3.2 Weaknesses

5.3.2.1 Risk acceptance criteria

When establishing the design accidental loads, the loads should be developed through a QRA and compared with an existing risk acceptance criterion. The risk acceptance criterion that is used is normally the specific criterion given in Section 11 in the Facility Regulations that accidental loads with an annual probability of occurrence of $1*10^{-4}$ shall not result in loss of a main safety function (Petroleum Safety Authority Norway, 2012a). In addition the design accidental loads shall not contribute to the total risk of the installation in question being above the total risk acceptance criteria, which typically is in the form of PLL, FAR or F-n.

The idea of having a risk acceptance criterion before a risk analysis is performed may seem appealing. A QRA is performed, and either the risk is below the criterion or some risk-reducing

measures are implemented until the risk is below the criterion. It will make it easy for the decision-maker to know when the risk is low enough to be acceptable. However, this might be a solution that has more disadvantages than advantages. If the criterion is set before an analysis is performed, then it is natural that the focus is on showing that the risk is below this criterion, and potential risk-reducing measures might be overlooked. If there is an additional risk reducing measure that easily could be implemented, but that receives no attention due to the fact that the risk is judged to be below the risk acceptance criterion, then it should be clear that the risk acceptance criterion is not an ideal method.

5.3.2.2 QRA as a decision-making tool

Rae et Al (2012) says that "A risk practioner might say "the risk of an accident is 1*10^-8 per year if the estimated failure rates hold and the model is correct", meaning that significant work is required to monitor the failure rates and validate the model. Their audience might simply hear "the risk of an accident is 1*10^-8 per year"."

The use of QRA in establishing design accidental loads for fire and explosions will result in different fire and explosion loads with associated annual probabilities. However, the analysis will be built on quite a few assumptions. The whole event sequence that eventually leads to an explosion has to be analyzed, and all the different events have to be given probabilistic values. This is normally done by statistical analyses – where historical data is interpreted to probabilistic values. In addition, the starting points of the event sequence also have to be determined, and this may also give variations in the results. Where there is little historical data, expert judgment is used to obtain a statistical value.

The following aspects are among the ones that have to be analyzed (Vinnem, 2007):

- Location of the leak source
- Direction of gas jet
- Flow rate of the leak
- Wind direction and speed
- Performance of barrier elements, in order to limit size and duration of cloud

According to Vinnem (2007), the probability function will be established on the basis of the following uncertainties, among others:

- The actual location of the ignition point which may vary considerably and have a strong influence on the resulting explosion overpressure.
- The strength of the ignition source which may vary depending on the type of ignition source
- The volume of gas cloud
- The homogeneity of cloud
- The gas concentration in the cloud relative to a stoichiometric concentration

Whether or not a QRA is a scientific tool has been debated several times, but the general conclusion is that it's not if it relies heavily on historical data and if there is not a large amount of relevant data available (Aven, 2011). Historical leak rates are available on the equipment used in the oil-and gas-industry, but using historical data as representative probabilities for the future is a huge step (Aven & Vinnem, 2007). According to Aven and Vinnem (2007) many risk analysts does not acknowledge

this, and do not in practice separate between historical data and representative probabilities for the future. This could represent a problem in some cases, considering that there is always uniqueness present to the installation in question. Considering this together with the fact that there is a lot of equipment that all will have their own leak rates for instance, the uncertainty connected to if the historical data represents the future should be considered relatively large. Combining this again with the other different assumptions, the size of the leak, the flow rate, the location of the leak source, the wind, the size of the gas cloud, the time until detection, the possibility of ignition and so on, the precision level is not very sharp.

All these factors will contribute to the fact that a QRA of fire and explosion risk will not give similar results when performed by different assessors, the result is expected to vary as shown in for instance (Rein, et al., 2009).

This does not mean that a QRA shouldn't be used in the process of establishing design accidental loads, or in analyzing the total risk of an installation. A QRA is still an excellent tool for examining an installation and getting insights into possible failures in complex systems. But the fact that a QRA as all other ways of examining risk will have its strengths and weaknesses has to be acknowledged. Judging if a risk is acceptable or not based alone on if the results of a QRA imply that the risk is below $1*10^{-4}$ would seem to be a misinterpretation of what a QRA is.

Another weakness of today's practice that should be mentioned is that it is too easy for the decision-maker to make the decision. By simply referring to the results of a risk analysis and selecting the design accidental load, the decision will be less thought through than if the decision-maker would have been presented results from assessments of the strength of the background knowledge, surprises that may occur and other analyses.

5.3.2.3 Uncertainty

Perhaps the clearest requirement to the representation of uncertainty is found in the Management Regulations, Section 17, where the requirements for a risk analysis are stated. Second subsection reads "necessary assessments shall be carried out of sensitivity and uncertainty." (Petroleum Safety Authority Norway, 2012) In the guidelines to this section it is stated that NORSOK Z-013 normally can be used to fulfill the requirements for risk, with a few additions where one of them is "uncertainty shall be assessed and highlighted." (Petroleum Safety Authority Norway, 2012b)

However, few further requirements are presented on how to assess and highlight the uncertainty. Uncertainty in risk description is a subject that has received a lot of attention in the last years, and is a much debated subject in the field of risk. Uncertainty is a term that covers a lot of different fields, and several definitions and descriptions exist.

With the existing regulations and the existing risk-thinking in the oil- and gas-industry the uncertainty is typically expressed quantitatively, and in connection to the result of a QRA, as a pure statistical value. However, one uncertainty-factor is the strength of the background knowledge. As shown earlier, a number of assumptions and simplifications have to be made in order to be able to calculate the design accidental loads. How strong the background knowledge that the assessor uses to stipulate the statistical values on is, is difficult to present quantitatively.

The strength of the background knowledge may still have a large impact on the calculations, if the background knowledge is weak. This could be crucial, but this uncertainty appears to be given little or no attention in today's practice of establishing design accidental load. This could of be explained if the assessors and decision-makers have a traditional perspective of risk as a combination of probability and consequences.

Another reason behind considering the treatment of uncertainty as a weakness when considering the establishing of design accidental loads, is due to the fact that a requirement regarding risk analyses is that it (among other things) shall "identify and stipulate design accidental loads" (Petroleum Safety Authority Norway, 2012) and "be appropriate as regards providing support for decisions related to the upcoming operation or phase" (Petroleum Safety Authority Norway, 2012). With today's relatively weak focus on uncertainty regarding whether or not the design accidental loads for instance is acceptable regarding the $1*10^{-4}$ criteria, there is a question on how good the support for the decision-maker is, without a thorough evaluation of the knowledge the QRA is based on.

5.3.2.4 ALARP

As mentioned earlier, a version of the ALARP principle is found in the regulations. This principle is well-known and often used in risk management – and is a logical way of handling risk. However it doesn't appear to be given much weight by the different companies, possibly because there are no further requirements on how an ALARP-evaluation should be performed and documented. The ALARP-evaluations is performed with great differences among the companies, and the tools for assessing if a risk is ALARP varies as well (Vinnem, Haugen, Vollen, & Grestad, 2006). The ruling principles when establishing design accidental loads is the requirement regarding loss of main safety functions and that the risk should be below the risk acceptance criteria, and as shown in chapter 5.3.2.2, such requirements does not encourage to further risk reduction once the "goal" is achieved.

Aven and Vinnem (2007) use an example of modifying an existing platform, where the operating company claimed that ALARP evaluations had been performed, but without any documentation to prove it. The authorities were not satisfied with the resulting increase in risk on the platform, but had no legal basis for acting (Aven & Vinnem, 2007). This should be another example of the industry and the authorities interpreting the regulations differently.

Another important point is to determine when the ALARP-evaluations should be performed. For the different risk-reducing measures for fire and explosion risk, it is obvious that they will be relevant in different stages of the design-process. If the ALARP-process is started too late, some of the risk-reducing measures that concerns design, layout and structural strength will be too expensive to be considered implemented. The fact that the QRA is the basis for the establishment of the design accidental loads today implicates that the ALARP-evaluations are not performed early enough.

5.3.2.5 Peer-review

The importance of a QRA being peer-reviewed is a factor that is underlined by many. For instance Apostolakis, when presented with criticism of the QRA as a tool, he claims that the QRA should be peer-reviewed (Apostolakis, 2004). He states that "insights from QRAs should not be used in decision making unless they have been subjected to a peer review by independent experts." (Apostolakis, 2004) This is also a weakness with today's practice. Judging by the difference in views on risk between the industry and the PSA, the mechanistic way the industry threats risk calculations, and

the fact that design accidental loads are often based on a QRA alone implies that the decision-maker not always checks to what degree the analysis has been peer-reviewed.

5.3.2.6 Future phases

Another weakness with today's practice is that the results are not always followed up into the next phase (Petroleum Safety Authority Norway, 2013). This is somewhat connected to the other weaknesses. Considering a QRA stipulating design accidental loads, and that these are based on a number of assumptions and simplifications, it would be natural for these assumptions and simplifications to be followed up to see if they still make sense in the future phase – at least for the assumptions and simplifications that the assessor is the least sure of. But if the assessment on how certain the assessor is on the different assumptions and simplifications are not performed, or this is not being acknowledged by the decision-maker, then it is hard to imagine that this will be followed up in the future.

If the result from the process of establishing design accidental loads is that the installation will withstand a load that will occur with a low probability, this will give little or no usable information to the next phases. The interesting point should be how the different barriers should be monitored in order to keep the risk level as it was intended.

6 Suggestion of two methods to establish design accidental loads that will be in compliance with the new definition of risk

Today's method of establishing the design accidental loads starts with a QRA and comparison of results from the QRA with relevant risk acceptance criteria. The criterion used is normally that the annual occurrence of the design accidental loads shall be below $1*10^{-4}$. In addition to this, the specific requirements in the guidelines have to be fulfilled, independent of results from any risk analysis. The requirement that the risk shall be reduced further to the extent possible should in principle also be fulfilled, but these evaluations are often coarse and performed in a mechanistic way where possible improvements are identified but disregarded quickly based on a cost-benefit analysis (Aven & Vinnem, 2007). It has been shown that the use and understanding of the ALARP-requirement differs quite a lot between different operating companies on the Norwegian Continental Shelf (Vinnem, Haugen, Vollen, & Grestad, 2006).

Going from today's perspective of risk to the suggested new perspective of risk should mean that the assessment and description of risk should focus less on calculated expected values, and more on holistic assessments considering the context that the risk is involved in. Such a perspective of risk would mean that today's method of establishing design accidental loads will have to change, in order to be in compliance with the new definition. According to Aven and Vinnem (2007), such a perspective should be reflected by:

- Focusing on different actors' analyses and assessments of risk
- Addressing aspects of the uncertainties not reflected by the computed expected values
- Acknowledging that what is acceptable risk and the need for risk reduction cannot be determined simply by reference to the results of risk analyses
- Acknowledging that risk perception has a role to play in guiding decisions-makers; professional risk analysts do not have the exclusive right to describe risk.

In addition it should be clear that probabilities alone is not enough to describe the uncertainties, and that it should be acknowledged that there is a level of subjectivity connected to every risk analysis. If the PSAs focus on major accident risk is taken into account as well, accidental loads that have a low probability but high consequences should also be assessed.

How this new definition will be interpreted in the industry, and how it will be followed-up from the PSA will in the end determine how big the changes regarding the establishment of design accidental loads with respect to fire and explosions will be. As mentioned earlier the regulations are judging by the shape of its requirements built on a relative frequency interpretation of risk, so further changes in the regulations should be expected. Potential changes could be for instance removing or editing references to standards that are not updated with the new definition of risk, and some requirements on how uncertainties should be treated. Changes could also be expected to see in the requirement regarding the use of risk acceptance criteria, as this requirement has received criticism over the past years. According to Aven and Vinnem (2007) many experts of risk analysis are skeptical to the use of such pre-determined risk acceptance criteria, and the PSA has also raised critical questions on the topic. The criticism can be summed up in two points, the first being that the use of a pre-determined risk acceptance criteria leads to the focus of a risk analysis being to show that the risk is below the criteria. The second point regards the fact that there is a lack of tools with the necessary precision to justify having a pre-determined risk acceptance criterion (Aven & Vinnem, 2005).

In chapter 6.1.1 and 6.1.2, some principles and ideas related to two new methods are suggested in order to deal with the new definition. The first resembles the one used today in the sense that it uses a QRA as the starting point and uses a risk acceptance criterion to select the design accidental loads. The difference from today's method will be that a qualitative assessment of the strength of the background knowledge that the probabilities are built on is performed, in addition to assessments of surprises that may occur compared to the QRA-result, so-called black swans. The results from these assessments will have implications on the selection of the design accidental loads, and the ALARP-evaluation of choosing more severe loads. In addition to giving a better foundation to make a decision regarding the design accidental loads, this method will provide information that should be useful in the operating phase. The methods for assessing both the background knowledge and the black swans are based on a paper of Aven (2013).

Whereas the first method involves the use of a risk acceptance criterion, the second method will not. Instead it will try to capture the intentions in the regulations, by regarding the stipulated risk level in the regulations as a minimum level and focus on achieving further risk reduction below this level. In addition it will try to capture the messages given from the PSA regarding the focus on major accident risk. The main focus will be to design the installation for as high design accidental loads as reasonable practicable.

6.1 Method 1, today's practice with a sharper focus on uncertainties

This method will resemble today's practice of establishing the design accidental load in the sense that it uses a QRA as the starting point and compares the risk against the risk acceptance criterion, which in this case will be that the design accidental loads should have an annual probability of occurrence below $1*10^{-4}$. The difference from today's method will consist of qualitative assessments of the strength of the background knowledge in order to address the aspects of uncertainty that is not reflected by the calculated expected values, and an assessment of potential surprises that may occur compared to the risk picture stipulated by the QRA. The selection of the design accidental loads will be a decision made by the decision-maker, where the strength of the background knowledge and the potential surprises that may occur are taken into consideration. In addition, ALARP-evaluations should be performed, based on the results from the assessment of the strength of the background knowledge and the potential surprises.

6.1.1 Assessment of the strength of the background knowledge

The following methods are based on a paper by Aven (2013).

The five uncertainty-factors listed by Vinnem (2007) that among others will be present in a QRA that evaluates explosion risk will be used as an example on how the background knowledge will be evaluated.

- The actual location of the ignition point which may vary considerably and have a strong influence on the resulting explosion overpressure.
- The strength of the ignition source which may vary depending on the type of ignition source
- The volume of the gas cloud
- The homogeneity of the gas cloud
- The gas concentration in the cloud relative to a stoichiometric concentration

The focus of the evaluation of the strength of the background knowledge should be on the important factors for the result of the QRA. All of the assumptions and simplifications will not have the same effect on the results of the QRA, some will be more important than other.

The importance of this evaluation should be to identify the most important assumptions/simplifications, and present an evaluation on how certain the assessor is that the assumptions/simplifications made are reasonable.

Using the five assumptions that have to be performed to express the explosion risk as examples, each and one of them should be evaluated using the methods below.

6.1.1.1 Coarse evaluation of the strength of background knowledge

If one or more of the conditions to the left of the table is true, the knowledge regarding the assumption is considered weak. If all the conditions to the right of the table are considered true, then the knowledge regarding the assumption is considered strong.

For cases that lie in between the two different categories in the table, the assumptions may be considered to have a medium strong knowledge.

Table 1 - Method for assessing the strength of the knowledge (Aven, 2013)

The knowledge is weak if one or more are true	The knowledge is strong if all are true
The assumptions made represent strong simplifications	The assumptions made are seen as very reasonable
Data are not available, or are unreliable	Much reliable data are available
There is lack of agreement/consensus among experts	There is broad agreement/consensus among experts
The phenomena involved are not well understood; models are non-existent or known/believed to give poor predictions	The phenomena involved are well understood; the models used are known to give predictions with the required accuracy

The five uncertainty-factors that are used as examples here should be evaluated after the principles above, and the results should be presented to the decision-maker. However, it may be hard for the decision-maker to know what to do if the assessors state that the knowledge regarding the assumption of how large the volume of the gas cloud will be is weak, as this method doesn't say anything of the consequences of this assumption being wrong.

6.1.1.2 A more detailed evaluation of the strength of background knowledge

Another, more detailed method that involves the consequences is presented by Aven (2013), and is here shown for the example regarding the volume of the gas cloud.

Three events are defined where the first is that the gas cloud is twice as large than what assumed, the second that the gas cloud is ten times larger than what assumed and the third that the gas cloud is 50 times larger than what assumed. A crude risk assessment should be performed of the three events, considering the magnitude of the deviation, the probability of this magnitude to occur, and the effect of the change on the consequences. The score categories used for the assessment could be high, medium or low. After this, a judgment on how strong the knowledge behind the score categories assigned is, using strong, medium or weak categories. If the strength of the knowledge is

judged to be weak or medium, the score assigned should be moved up from one category to another, unless it's already given the highest score.

Table 2 - Assigned risk score for the assumption regarding the volume of the gas cloud, and the events of the volume being twice as big, ten times as big or 100 times as big as the volume assumed – considering both the probability, the consequences and the strength of the knowledge.

Assigned risk score	High	x		
	Medium		x	
	Low			X
		2	10	50
	Deviation magnitude			

As seen, this method will also include the consequences of an assumption being wrong. This is different from the first method shown, and provides the decision-maker with extra information. If an assumption is made with weak background knowledge, but the consequences of it being wrong is relatively small – it is not as important as an assumption made with weak background knowledge, but larger consequences if it turns out to be wrong.

If such an evaluation is performed and presented to the decision maker along with the results from the QRA, it will give valuable information on how solid the results are in a format that should be easily understandable.

6.1.2 Assessments of black swans

When making a decision regarding the design fire and explosion loads, the decision-maker decides how much the installation in question should be able to withstand. When making such a decision, the decision-maker should receive information regarding surprises that may occur, so-called black swans. How likely is it that accidental loads more severe than what the installation are built to withstand may occur? The consequences of such loads occurring may be devastating, so to highlight this part of the risk picture in particular makes good sense. In order to have a risk picture that is as complete as possible such an assessment should be performed. This would also make sense, considering that adopting the new risk perspective would be an acknowledgement of that there is a level of subjectivity involved with a risk analysis.

Potential surprises that may occur compared to results from a risk analysis is typically divided into two groups, unknown unknowns and surprises that may occur compared to the beliefs of the assessors and experts used in the assessment (Aven, 2013). The unknown unknowns are as the term says, surprises that may occur that are not known, so these are hard to assess in this setting. The assessments will therefore concentrate on the first group.

Aven (2013) presents a method for assessing these surprises. The first step consists of creating a list of risk events that has been judged to have a low risk assessed with respect to probability, consequences and strength of knowledge. For instance an explosion with a following fire that escalates to the neighboring areas.

When this list is created it should be assessed by another analysis team than those who performed the first risk assessments, in order to give room for creativity and obtaining an objective approach. The assessments should give "a review of all possible arguments and evidence for the occurrence of

these events" (Aven, 2013). Such arguments and evidence could for instance consist of referring to accidents that has happened earlier, or it could challenge assumptions made in the original risk assessment by referring to expert's judgments that says otherwise.

The list of events assessed together with the belonging evidence and arguments from the assessment is delivered to the decision-maker, together with the risk events that has been given the highest risk score according to the assigned probability, consequences and strength of knowledge (Aven, 2013).

When selecting design accidental loads, the same method as described above should be used on the accidental loads that are described from the QRA with a probability of occurrence lower than $1*10^{-4}$. If the decision-maker originally wants to select the load that occurs with an annual probability of $1*10^{-4}$ it should be of interest to analyze the events that leads to the loads that occurs with for instance a probability of $5*10^{-5}$, $1*10^{-5}$, $1*10^{-6}$ and so on. If the external analysts find some of these scenarios to be more likely than first thought, this should be essential information for the decision-maker before making the final decision. The reason for this is of course the potential consequences if accidental loads occur that are more severe than the installation in question is designed to withstand. This would provide the decision-maker with important information regarding major accident risk. The major accidental risk is typically events with low probability and high consequences, and both with the new definition of risk and PSAs focus on the subject should imply that such an assessment should be performed.

6.1.3 Decision

Compared to today's method, the selection of design accidental loads should take into considerations the strength of the background knowledge and the assessments of the black swans. Using the risk-acceptance criteria as today, the risk should be below $1*10^{-4}$, but depending on the results of the assessments mentioned above additional risk-reducing measures should be implemented. The ALARP-requirement should also be paid attention to.

The use of a risk acceptance criterion similar to selecting the loads that occurs with an annual probability of $1*10^{-4}$ will first of all mean that loads with a calculated probability of occurring higher than $1*10^{-4}$ never should be selected as design accidental loads. Loads that occur with an annual probability lower than $1*10^{-4}$ could be selected, but considerations of the strength of knowledge should be taken into account. A more describing procedure is suggested below, based on (Aven, 2013).

1. If a load is selected as a design accidental load and has a probability of occurrence that is clearly below $1*10^{-4}$, then it should be considered ok unless the strength of knowledge is weak.
2. If a load is selected as a design accidental load that has a probability of occurrence just below $1*10^{-4}$, it should be considered to be ok if the strength of knowledge is considered strong.
3. If a load is selected as a design accidental load that barely or with a small margin is below $1*10^{-4}$, and the strength of the knowledge isn't considered to be strong then it should not be considered acceptable and design accidental loads with a lower probability of occurrence should be chosen.

As for the ALARP-evaluations there are no guidelines in the regulations on how these should be performed, but somehow the costs of designing for more severe design accidental loads have to be assessed against the benefits or the effectiveness of the risk reduction. A method is described below, based on Aven (2013).

1. The design accidental loads selected should be more severe than suggested by the risk acceptance criterion if the cost of doing so is considered to be small
2. The design accidental loads selected should be more severe than suggested by the risk acceptance criterion if formal cost-benefit analyses/cost-effectiveness analyses show that the measures is justifiable
3. If the two points above suggests that the design accidental loads should not be more severe, the results of the assessments of the strength of the background knowledge and the black swans should be considered. If the strength of knowledge is poor or medium or if selecting more severe design accidental loads could reduce the black swan risk then extra considerations should be made with regards to selecting more severe design accidental loads.

6.1.4 Flow chart method 1

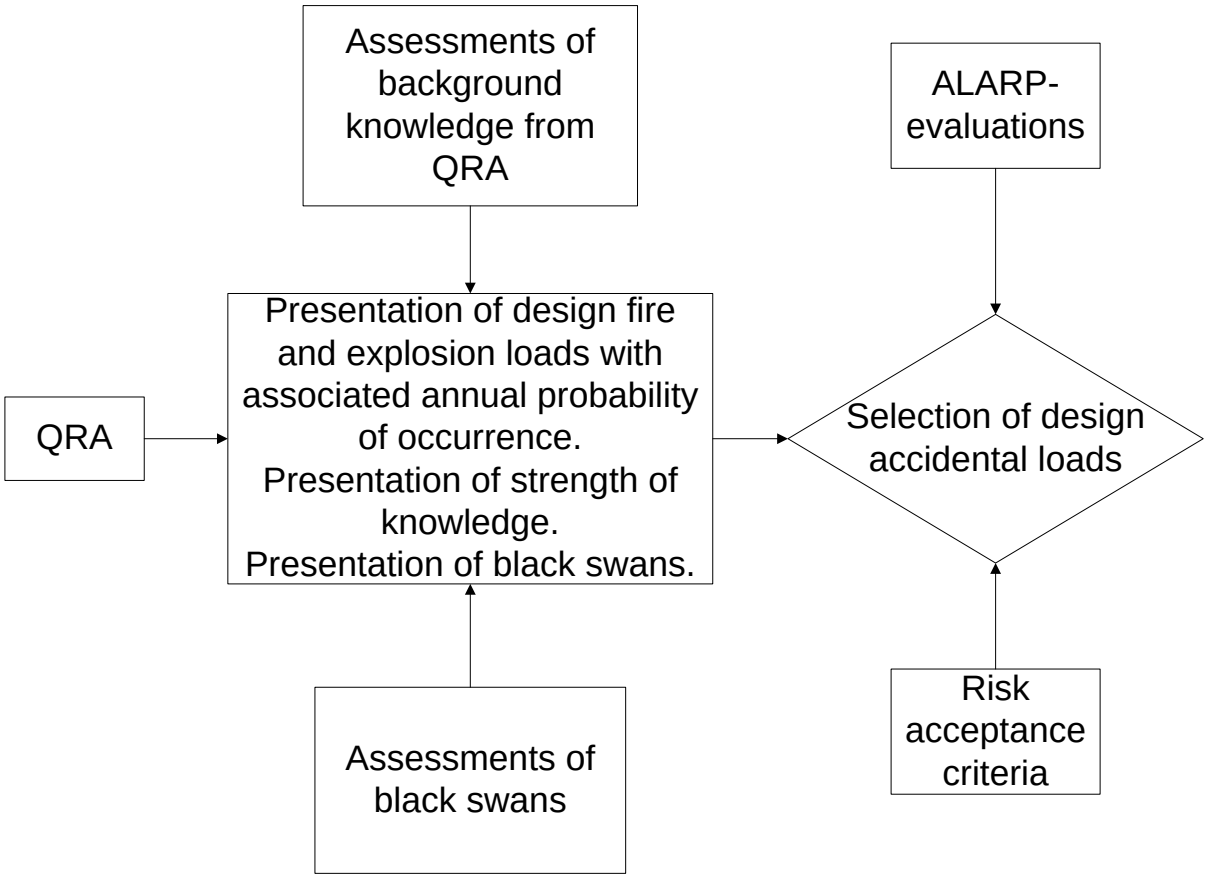


Figure 4 - Method 1, today's method with an elaborated assessment of background knowledge and black swans

6.2 Method 2, establishing design accidental loads without the use of risk acceptance criteria

Whereas the first method selects the design accidental loads by using as a pre-determined risk acceptance that the risk should be below $1*10^{-4}$, this method will avoid the use of a pre-determined criterion. The method will instead have a continuous focus on reducing the risk to the extent possible. The reason for not focusing on a risk acceptance criterion is the criticism that has been raised against the use of such a pre-determined criterion that determines when the risk is low enough. This criticism can be summed up in two points, the first that when having a pre-determined criterion the main focus of a risk analysis may end up to be on showing that the risk is below the limit, and not on obtaining the best risk reduction possible. The second point that has been criticized is that there is a lack of precision in the risk analysis tools available, making it hard to show that the risk is below a certain level (Aven & Vinnem, 2005).

6.2.1 Foundation

Instead of establishing loads that are acceptable compared to a pre-determined risk acceptance criterion, this method will have as a foundation to select as severe fire and explosion loads that it would be feasible to design the installation in question to withstand. The method will in other words focus on reducing the fire and explosion risk to the extent possible, as required by the version of the ALARP principle in Section 11 in the Framework Regulations (Petroleum Safety Authority Norway, 2011c). The goal should be for the decision-maker to select as high design fire and explosion loads as reasonably practicable.

This will be the prevailing principle for establishing the design accidental load. By using this principle from the beginning, the resulting structural strength and the early layout should be chosen to reduce the risk to the extent possible. Making decisions regarding design accidental loads so early in the design phase may be considered hard, since the final layout and the final amount of equipment in the installation in question may be unknown. However, this uncertainty should not be an excuse for not making a decision and the same uncertainty is present today when using a QRA to stipulate the loads. Except for the requirement regarding the use of risk acceptance criteria, the rest of the requirements regarding the establishing of design accidental load from the regulations should be fulfilled.

6.2.2 Starting point

A worst-case scenario is suggested as a starting point. What is the possible longest duration of a fire before it is depressurized to an acceptable level, and what is the highest possible explosion loads. The worst-case scenarios are normally not feasible to design against (Vinnem, 2007), but this should serve as the starting point. The idea is to move downward from the worst case, and find an area where the loads start to be feasible to design against. The evaluation of the descending levels from the worst-case scenario could be done by coarse qualitative evaluations, where the benefits and disadvantages are described briefly. At least in the beginning it will be obvious that the disadvantages will be too large considered against the benefits. When it is harder to discard a level based on a coarse qualitative evaluation, the area where the design accidental loads should be chosen from will appear.

From this area several alternatives should be suggested, so that the decision-maker would have several alternatives to choose from. The generating of alternatives for a decision is considered to

encourage a more thorough decision, where a broader spectrum of benefits and disadvantages is studied.

6.2.3 Decision support

The decision process should be supported by different analyses, both quantitative and qualitative. When a set of different alternatives are to be chosen from, and the goal is to find the design accidental loads that is as high as what is reasonably practicable to design against, different analyses should be used to support a decision. It should be mentioned that considering that this method does not use any risk acceptance criterion, the analyses performed as decision-support should be more thorough than in method 1.

As mentioned earlier, the first levels downwards from the worst-case scenario could be discarded with reference to coarse, qualitative assessments. These evaluations should be possible to do with coarse, qualitative assessments due to the fact that the industry in general has a vast experience in designing installations to withstand fires and explosions. During the forty years with oil- and gas-operations in Norway the industry and authorities have gained experience in how to design safe installations. This is underlined in PSAs publication Safety – Status and Signals, where it is said that "the industry now has detailed information on what's required to build a facility in a safe and robust way, and that the industry knows pretty well everything about designing a process plant to help prevent leaks or to limit their consequences if they happen." (Petroleum Safety Authority Norway, 2013)

Based on this it should not be too hard to discard the most severe accidental loads based on general good engineering experience and coarse qualitative assessments of the costs compared to the risk reduction achieved.

When the level is reached where it is harder to discard the loads based on coarse assessments, different alternatives should be generated. The decision on what loads to choose should be based on ALARP-evaluations. As mentioned earlier a variation of the principle is found in the regulations, but no guidelines on how the ALARP-evaluations should be performed. The HSE in the UK have a few guidelines. The HSE states that in many cases reference to "good practice" will suffice as an assessment. Good practice is further defined to as "those standards for controlling risk that HSE has judged and recognized as satisfying the law, when applied to a particular relevant case, in an appropriate manner." (HSE, 2013) It is further explained that what good practice should be is discussed and decided with relevant stakeholders. If good practice is not sufficient, the HSE recommend using common sense and exercising professional judgment as the next step. If the decision needs more support, a quantitative approach is recommended where cost-benefit analyses are recommended. However, it is underlined that such analyses will be associated with many assumptions and associated with a lot of uncertainties, so decisions should never be made with reference only to cost-benefit analyses.

There are a number of analyses that might be helpful for the decision-maker to make the final decision. The importance should be to compare the benefits and disadvantages of the different alternatives. These could be related to feasibility, conformance with good practice, economy, strategy considerations, risk, social responsibility, etc. (Aven & Vinnem, 2007). Expected cost per expected saved statistical life could be computed, to present differences between the alternatives in

terms of effectiveness, the expected net present value may be calculated and these should all be presented with associated sensitivity analyses (Vinnem, 2007).

A QRA should be an important contributor to the selection of the design accidental loads. Even though it has some disadvantages, it is still an excellent tool for having a thorough examination of the installation in question. It will provide decision support by giving an assessment of the annual probability of the different loads and it will be useful in order to suggest risk-reducing measures with an associated risk-reducing effect.

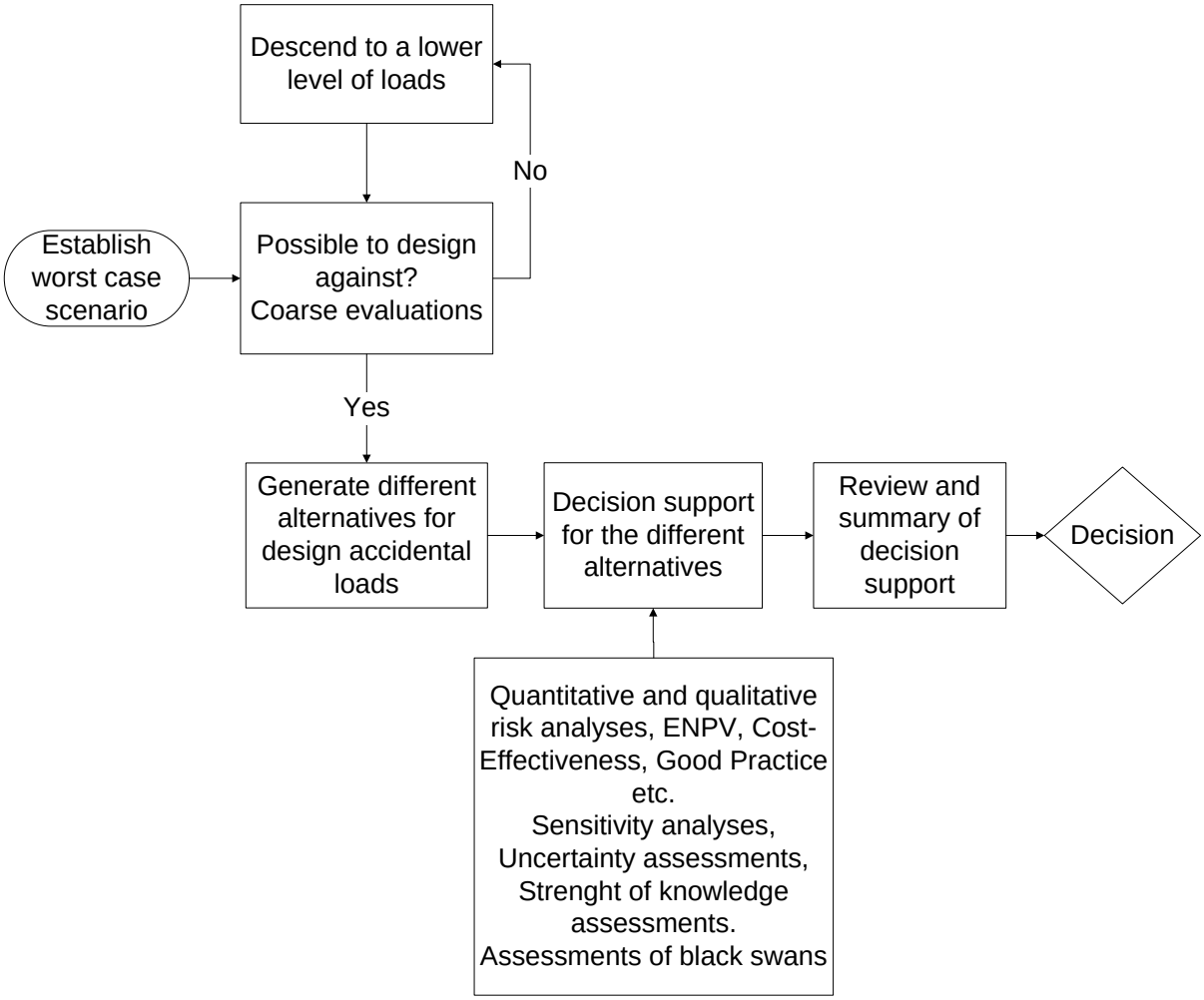
The limitations and constraints of the different analyses should be described, and when it comes to extensive, quantitative analyses as for instance the QRA and ENPV-analyses, the strength of the background knowledge should all be assessed according to one of the methods described in 6.1.1.

The assessments of potential surprises should also be performed as described in chapter 6.1.2 as decision support, in order to give the decision-maker information of the robustness of the selected design accidental loads.

6.2.4 Decision

The results from the different analyses for the different alternatives should be summarized, with their associated pros and cons. That the different analyses all have strengths and weaknesses should be underlined, and assumptions, limitations and uncertainties influencing the results should be presented. The strength of the background knowledge involved in the different analyses should be reported along with the results, as well as the results from the assessment of black swans. The decision-maker should then review the results for the different alternatives and make a decision. By being presented by different analyses for different alternatives, it should give a broad specter of information to make the decision on. The decision should still be made on the principle of that the installation should be designed to be able to withstand as high design accidental loads as reasonable practicable.

6.2.5 Flow chart method 2



Figur 5 - Method 2, establishing design accidental loads without the use of risk acceptance criteria

7 Discussion

7.1 Design accidental loads, dimensioning accidental loads and the abbreviation DAL

The main source of the confusion surrounding the three terms design accidental load, dimensioning accidental load and the abbreviation DAL is obvious. The terms design accidental load and dimensioning accidental load are very similar, and they can both be abbreviated to DAL. To avoid different use of the three terms seems like an impossible job. However, that does not mean that definitions in standards and regulations should not be consistent with each other. That the Facilities Regulations defines the term design accidental load and dimensioning accidental load similarly, depending on whether the English or Norwegian version is read is unfortunate and can probably be explained by a typo that should be fixed. Considering that the NORSOK Z-013 has included the term design accidental load as the "final" load that includes for instance ALARP-evaluations it would be natural to change the term dimensioning accidental load to design accidental load in the Norwegian version of the Facilities Regulations.

The suggestion made in chapter 3 to define both the terms similar to either the definition in the Facilities Regulations or similar to the definition of design accidental load in the NORSOK Z-013 standard will not be a good suggestion if there is a need in the industry to have one term for the load that appear with an annual probability of $1*10^{-4}$ and one for the "final" load. If this is the case, then the NORSOK Z-013's definitions should be implemented in the NORSOK S-001 standard as well, and eventually the confusion should be less than now.

However, if the suggested new definition of risk is implemented in the regulations, it would underline the point that the design accidental loads should not be based on QRA-results alone, and then the need for having two definitions should be even smaller than today.

7.2 Implications of the new risk perspective

The new definition represents a change of perspective on risk in the regulations. Judging by today's definition of risk, the general wording of the regulations and the industry practice represented by the different standards the present view on risk is traditional in the sense that computed probabilities and expected values are considered to be sufficient when analyzing and describing risk. The new definition will have implications on this, but how these implications will look like will depend on the follow-up from the PSA and the interest from the industry. Several changes in the regulations should be expected, for instance changing of requirements or removal of referrals to different industry standards. It is hard to predict how the changes will be and when they will occur, as changes often takes time. However, as shown earlier in this thesis today's practice of establishing design accidental loads is a good example of a practice that will have to change in order to be in compliance with the new definition.

To find ways of establishing design accidental loads that builds on the strengths of today's method and manages to capture the dimensions of uncertainty that is not focused on today is not that hard. The uncertainty is not some mystical object that is hard to describe, it should be relatively easy to express by the risk assessors, at least in a qualitatively way.

Both of the methods suggested in this thesis will make it harder for the decision-maker to let risk analysts make the decision in practice. This should be considered to be positive as it will mean that the decision-maker receives a more realistic risk picture. On the other hand it will demand that the decision-maker is willing to prioritize safety. The problem is rather to find a way to make sure that the decision-maker involves this uncertainty in the decision process, and takes the necessary precautions in case the background knowledge for some essential assumptions is weak.

This could be a challenge judging by the apparent different views on risk between the industry and the PSA, as mentioned in chapter 4.3. The non-compliances that the PSA discovers in their audits and the letter sent concerning misuse of risk analyses (Petroleum Safety Authority Norway, 2007) shows that the problem is complex. However, implementing the suggested new definition of risk should be a step in the right direction.

To observe how the PSA will follow up the suggested new definition, if it is implemented, in order to make the industry change the mechanistic approach to risk that is seen today will be interesting. As for the methods suggested in this thesis to establish the design accidental loads, some requirement regarding documentation of the different additional assessments would be necessary in order to ensure traceability later on.

The main difference between the two different suggestions made in this thesis is the use of risk acceptance criteria. As mentioned earlier the use of risk acceptance criteria has been criticized by several experts in the field earlier, and lately the PSA itself has been critical to the subject (Aven & Vinnem, 2007). However, whether or not any changes on the use of such a criterion will appear is not certain. Even though the PSA have been critical to the subject, it still has long traditions and is well integrated in both the regulations and the industry. It is therefore not a given that the requirement will be changed due to the new definition.

Another challenge associated with the additional assessments described throughout chapter 6 is that it will demand a precise level of communication. It is important that the relevant information regarding for instance the strength of the background knowledge and risk of surprises is communicated to the decision-maker in a precise way. This will demand more from both the assessors and the decision-maker, than what is necessary in today's practice.

7.2.1 Method 1, today's method with an elaborated assessment of uncertainty and surprises that may occur

As today's method, this method also uses a QRA as a starting point that will stipulate a set of accidental loads. The design accidental loads should be chosen among these loads as long as they are below the risk acceptance criterion. It differs from today's method by including assessments of the strength of background knowledge that the resulting loads presented from the QRA are built on and potential surprises that could occur. It acknowledges that there is a subjectivity involved with any analysis and that assessment of the strength of background knowledge and black swans will give important information to the decision-maker. The given information should be used when making decisions regarding ALARP-evaluations and the final design accidental loads. In addition, especially the assessments of strength of the background knowledge, will give the decision-maker the opportunity to either increase the knowledge about certain phenomena or know what factors of the system that has to be given extra attention during the operation phase.

The interesting part is what the decision-maker will do with this additional information in practice. If the procedure described above is performed, then the process should be within compliance with the regulations and with the suggested new definition of risk. The decision-maker could of course still select the design accidental loads that will correspond to the $1*10^{-4}$ criteria even though the results are associated with weak background knowledge. Just as the decision maker could make a coarse ALARP-evaluation today, and ignore risk-reducing measures if the design accidental loads are ok according to the risk acceptance criterion. Further requirements on how these evaluations should be documented and performed should be developed in order to ensure that the quality of the decision will be better than it is today. How and if this is done will as mentioned earlier depend on future follow-up from the PSA or the industry itself.

Another interesting point is that such a method will demand more from the decision-maker than what is demanded today. Such a method would "force" the decision-maker to make the decision alone instead of in practice let a risk analyst make the decision.

This method uses risk acceptance criteria in the same shape as it is done today. There may still be a chance that the focus will be on showing that the risk is below the risk acceptance criterion instead of obtaining the most robust solution possible. In addition, if the requirements regarding the risk acceptance criterion stays as today, the argument that the tools available for analyzing risk today lacks the necessary precision will still be valid. However, these two potential weaknesses will always be the case as long as a method involves the use of a pre-determined requirement.

Perhaps the most apparent weakness with such a method is that as long as the process of establishing design accidental loads starts with a QRA, it is a chance of overlooking ALARP-evaluations early in the design process. This could mean overlooking the potentially most effective risk-reducing measures, namely layout and structural strength, considering that decisions concerning these two factors are made early in the design process.

7.2.2 Method 2, establishing design accidental loads without the use of risk acceptance criteria

This method uses establishment of the worst-case scenario as a starting-point. Descending from the worst-case scenario, and ending up with the design accidental loads that the decision-maker means is as severe as reasonably practicable. As a result the major accident risk should be minimized and the installation should be robust. Monitoring of the risk level and the different implemented risk-reducing measures is required in the operating phase, but this will be necessary independent on how the design accidental loads are established.

The main difference between this method and method 1 is that this method does not involve a risk acceptance criterion. By using this method, the focus should be on risk reduction from the very beginning of the design phase, and thus ensuring that the potentially most effective risk-reducing measures are taken into consideration.

By not using a risk acceptance criterion the different analyses used in the decision support is thought to be more extensive than in the method that uses risk acceptance criterion. This will make it even "tougher" for the decision-maker to make a decision, which should lead to additional motivation for not letting the decisions in practice be made by risk analysts alone. This could be seen both as positive and negative. The positive aspect would be that the decision-maker receives broad

information, and is given a best possible description of the risk picture. The weakness is due to the lack of a risk acceptance criterion. A minimum level of risk will not automatically be present, so the decision-maker must be willing to prioritize safety in order for such a method to give good results. This also underlines the point that the decision-process should be documented such that any discarded alternatives must be documented with the reason for not implementing. As for the first part of the process, to descend from the worst-case scenario to the level where different alternatives are generated, it could also be a possibility that too low loads are selected as the starting point. However, using general good engineering practice should at least make sure that these loads are not lower than other similar facilities. Documentation of this process as well should be done. In case superficial decisions are made, this will be visible in the documentation.

8 Conclusion

8.1 DAL

That the Frameworks Regulations defines the term design accidental load in the English version and the term dimensioning accidental load in the Norwegian version, and that the definitions of these two terms are similar is probably an unfortunate typing error, and should be corrected in a future update of the regulations.

If it is found necessary and useful to have two different terms regarding the loads that an installation should be able to withstand, one for the loads that occurs with an annual probability of $1*10^{-4}$ and one for the final loads after extra considerations, then the definitions in NORSOK Z-013 makes sense. There the term DAL is defined as "Dimensioning accidental load", and is explained as the load that typically will appear with an annual probability of $1*10^{-4}$. The term design accidental loads on the other hand, is defined as "the chosen accidental load that is to be used as the basis for design", and is further explained as a load that sometimes may be the same as the DAL, but can be larger.

However, it is argued in this thesis that there should not be necessary to have two terms, and that this will not be the easiest way to clear the confusion surrounding the two terms.

Instead it is suggested to define both the terms dimensioning accidental loads and design accidental loads similarly as the definition in the Facilities Regulations. The definition for both terms should then be "an accidental load/action that a facility or an installation shall be able to withstand for a defined period of time." This would be a better way to clear the confusion, and focus on the message that should be considered important both with respect to the intentions in the regulations and the suggested new definition of risk, namely that when establishing design accidental loads it is not enough to establish the loads that occurs with an annual probability of $1*10^{-4}$ alone.

8.2 Establishing the design fire and explosion loads with the new definition of risk

It has been shown in the thesis that today's practice of establishing design fire and explosion loads will not be in compliance with the suggested new definition of risk. It will have to change if the new definition of risk is implemented in the regulations.

The implementation of the new definition of risk will mean that computed probabilities and expected values are not sufficient to describe risk alone. Uncertainties hidden in the background knowledge will have to be assessed, as well as the risk of surprises compared to the produced risk picture.

Some principles and ideas related to two methods for establishment of design fire and explosion loads that will be in compliance with the suggested new definition of risk have been suggested.

The first method resembles today's method, as it uses a QRA as a starting point and compares the results with a risk acceptance criterion. In addition, assessments of the background knowledge that the QRA is built on will have to be performed, as well as independent assessments of the risk of accidental loads occurring that is larger than the design accidental loads.

The second method does not use a risk acceptance criterion. It uses the worst-case scenarios as starting points, and this combined with ALARP-evaluations should give robust installations where the fire and explosion risk is reduced to a level the decision-maker feels is as low as practicably possible. A QRA will still be performed along with other analyses, that all will have to be assessed with respect to background knowledge. In addition the risk of surprises in the form of accidental loads occurring that is larger than the design accidental loads should be performed independently here as well.

9 References

Apostolakis, G. E. (2004, June). How Useful Is Quantitative Risk Assessment? *Risk Analysis: An International Journal* (3), ss. 515-520.

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

Aven, T. (2013, July). Practical implications of the new risk perspectives. *Reliability Engineering and System Safety* , ss. 136-145.

Aven, T. (2011). *Quantitative Risk Assessment - The Scientific Platform.* Cambridge: Cambridge University Press.

Aven, T. (2008). *Risk Analysis - Assessing Uncertainties beyond Expected Values and Probabilities.* Chichester: John Wiley & Sons, Ltd.

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

Aven, T., & Heide, B. (2009). Reliability and validity of risk analysis. *Reliability Engineering and System Safety* (94), ss. 1862-1868.

Aven, T., & Vinnem, J. E. (2005). On the use of risk acceptance criteria in the offshore oil and gas industry. *Reliability Engineering and System Safety , 2005* (90), ss. 15-24.

Aven, T., & Vinnem, J. E. (2007). *Risk Management - With Applications from the Offshore Petroleum Industry.* London: Springer.

Bjerketvedt, D., Bakke, J. R., & van Wingerden, K. (1993). *Gas explosion handbook.* Bergen.

Borg, A., & Njå, O. (2012, February). Concept of validation in performance-based fire safety engineering. *Safety Science* , ss. 57-64.

HSE. (2013). *HSE.gov.uk*. Hentet mai 21, 2013 fra http://www.hse.gov.uk/risk/theory/alarpglance.htm

International Risk Governance Council. (2008). *www.irgc.org.* Hentet mai 23, 2013 fra http://irgc.org/wp-content/uploads/2012/04/An_introduction_to_the_IRGC_Risk_Governance_Framework.pdf

International Standard Organization. (1999). *Petroleum and natural gas industries - Control and mitigation of fires and explosions on offshore production installations - Requirements and guidelines - ISO 13702 .* International Standard Organization.

ISO. (2009). *Risk management - Principles and guidelines.* Standard Norge.

Norwegian Technology Centre. (2001). *NORSOK standard Z-013 Risk and emergency preparedness analysis.* Oslo: Norwegian Technology Centre.

Petroleum Safety Authority Norway. (2011a, 03 31). *Basic knowledge about the regulations offshore and onshore*. Hentet 01 15, 2013 fra http://www.ptil.no/regulations/basic-knowledge-about-the-regulations-offshore-and-onshore-article7746-87.html

Petroleum Safety Authority Norway. (2012a). *Guidelines regarding the Facilities Regulations.* Stavanger: Petroleum Safety Authority Norway.

Petroleum Safety Authority Norway. (2011b). *Guidelines regarding the Framework Regulations.* Stavanger: Petroleum Safety Authority Norway.

Petroleum Safety Authority Norway. (2012b). *Guidelines regarding the Management Regulations.* Stavanger: Petroleum Safety Authority Norway.

Petroleum Safety Authority Norway. (2013). Høringsutkast veiledning til rammeforskriften 2013. Stavanger: Petroleum Safety Authority Norway.

Petroleum Safety Authority Norway. (2013). *Safety - Status and Signals.* Stavanger: Petroleum Safety Authority Norway.

Petroleum Safety Authority Norway. (2012c). *The Facilities Regulations.* Stavanger: Petroleum Safety Authority Norway.

Petroleum Safety Authority Norway. (2011c). *The Frameworks Regulation.* Stavanger: Petroleum Safety Authority Norway.

Petroleum Safety Authority Norway. (2012). *The Management Regulations.* Stavanger: Petroleum Safety Authority Norway.

Petroleum Safety Authority Norway. (2007, December 20). *www.ptil.no*. Hentet 03 21, 2013 fra http://www.ptil.no/news/unacceptable-use-of-risk-calculations-article3639-79.html

Petroleum Safety Authority Norway. (2013, April 25). *www.ptil.no*. Hentet 05 16, 2013 fra http://www.ptil.no/news/rnnp-2012-identifies-need-for-action-article9300-79.html?lang=en_US

Rae, A., McDermid, J., & Rob, A. (2012). The Science and Superstition of Quantitative Risk Assessment. *Proceedings of PSAM 11 & ESREL 2012.* Helsinki: International Association of Probabilistic Safety Assessment and Management, IAPSAM.

Rausand, M. (2011). *Risk Assessment .* New Jersey: Wiley.

Rein, G., Torero, J. L., Jahn, W., Stern-gottfried, J. R., Desanghere, S., Lázaro, M., et al. (2009). Round-robin study of a priori modelling predictions of the Dalmarnock Fire Test One. *Fire Safety Journal* .

Standards Norway. (2008). *NORSOK standard S-001 Technical Safety.* Standards Norway.

Standards Norway. (2010). *Norsok Standard Z-013 Risk and emergency preparedness assessment.* Standards Norway.

Veland, H., Amundrund, Ø., & Aven, T. (2013). Foundational issues in relation to national risk assessment methodologies. *Journal of Risk and Reliability* .

Vinnem, J. E. (2007). *Offshore Risk Assessment.* London: Springer.

Vinnem, J. E., Haugen, S., Vollen, F., & Grestad, J. E. (2006). ALARP-prosesser - Utredning for Petroleumstilsynet.

10 Appendix A

10.1 Requirements from the Framework Regulations (Petroleum Safety Authority Norway, 2011c)

Section 11

Risk Reduction principles

Harm or danger of harm to people, the environment or material assets shall be prevented or limited in accordance with the health, safety and environment legislation, including internal requirements and acceptance criteria that are of significance for complying with requirements in this legislation. In addition, the risk shall be further reduced to the extent possible.

In reducing the risk, the responsible party shall choose the technical, operational or organizational solutions that, according to an individual and overall evaluation of the potential harm and present and future use, offer the best results, provided the costs are not significantly disproportionate to the risk reduction achieved.

If there is insufficient knowledge concerning the effects that the use of technical, operational or organizational solutions can have on health, safety or the environment, solutions that will reduce this uncertainty, shall be chosen. Factors that could cause harm or disadvantage to people, the environment or material assets in the petroleum activities, shall be replaced by factors that, in an overall assessment, have less potential for harm or disadvantage.

Assessments as mentioned in this section, shall be carried out during all phases of the petroleum activities.

This provision does not apply to the onshore facilities' management of the external environment.

10.2 Requirements from the Management Regulations (Petroleum Safety Authority Norway, 2012)

Section 4

Risk Reduction

In reducing risk as mentioned in Section 11 of the Framework Regulations, the responsible party shall select technical, operational and organizational solutions that reduce the probability that harm, errors and hazard and accident situations occur.

Furthermore, barriers as mentioned in Section 5 shall be established.

The solutions and barriers that have the greatest risk-reducing effect shall be chosen based on an individual as well as an overall evaluation. Collective protective measures shall be preferred over protective measures aimed at individuals.

Section 9

Acceptance criteria for major accident risk and environmental risk

The operator shall set acceptance criteria for major accident risk and environmental risk.

Acceptance criteria shall be set for:

a) The personnel on the offshore or onshore facility as a whole, and for personnel groups exposed to particular risk,
b) Loss of main safety functions as mentioned in Section 7 of the Facilities Regulations for offshore petroleum activities,
c) Acute pollution from the offshore or onshore facility,
d) Damage to third party.

The acceptance criteria shall be used when assessing results from risk analyses, cf. Section 17. Cf. also Section 11 of the Framework Regulations.

Section 16

General requirements for analyses

The responsible party shall ensure that analyses are carried out that provide the necessary basis for making decisions to safeguard health, safety and the environment. Recognised and suitable models, methods and data shall be used when conducting and updating the analyses.

The purpose of each risk analysis shall be clear, as well as the conditions, premises and limitations that form its basis.

The individual analysis shall be presented such that the target groups receive a balanced and comprehensive presentation of the analysis and the results.

Criteria shall be set for carrying out new analyses and/or updating existing analyses as regards changes in conditions, assumptions, knowledge and definitions that, individually or collectively, influence the risk associated with the activities.

The operator or the party responsible for operating an offshore or onshore facility shall maintain a comprehensive overview of the analyses that have been carried out and are underway. Necessary consistency shall be ensured between analyses that complement or expand upon each other.

Section 17

Risk analyses and emergency preparedness assessments

The responsible party shall carry out risk analyses that provide a balanced and most comprehensive possible picture of the risk associated with the activities. The analyses shall be appropriate as regards providing support for decisions related to the upcoming operation or phase. Risk analyses shall be carried out to identify and assess contributions to major accident and environmental risk, as well as ascertain the effects carious operations and modifications will have on major accident and environmental risk.

Necessary assessments shall be carried out of sensitivity and uncertainty.

The risk analyses shall

a) identify hazard and accident situations,
b) identify initiating incidents and ascertain the causes of such incidents,
c) analyse accident sequences and potential consequences and
d) identify and analyse risk-reducing measures

Risk analyses shall be carried out and form part of the basis for making decisions when e.g.:

a) classifying areas, systems and equipment,
b) demonstrating that the main safety functions are safeguarded,
c) identifying and stipulating design accidental loads,
d) establishing requirements for barriers,
e) stipulating operational conditions and restrictions,
f) selecting defined hazard and accident situations.

Emergency preparedness analyses shall be carried out and be part of the basis for making decisions when e.g.

a) Defining hazard and accident situations,
b) Stipulating performance requirements for the emergency preparedness,
c) Selecting and dimensioning emergency preparedness measures.

10.3 Requirements from the Facilities Regulations (Petroleum Safety Authority Norway, 2012c)

Section 5

Design of facilities

Facilities shall be based on the most robust and simple solutions as possible, and designed so that

a) They can withstand the loads/actions as mentioned in Section 11,
b) Major accident risk is as low as possible,
c) A failure in one component, system or a single mistake does not result in unacceptable consequences,
d) The main safety functiosn as mentioned Section 7 are maintained,
e) Materials handling and transport can be carried out in an efficient and prudent manner, cf. Section 13,
f) A safe working environment is facilitated, cf. Chapter IV,
g) Operational assumptions and restrictions are safeguarded in a prudent manner,
h) Health-related matters are safeguarded in a prudent manner,
i) The lowest possible risk of pollution is facilitated,
j) Prudent maintenance is facilitated.

Measures to protect facilities against fires and explosions shall be based on a strategy.

The facility's areas shall be classified such that design and location of areas and equipment contribute to reduce the risk associated with fires and explosions.

Areas occupied by personnel, or where safety-related equipment is located, shall not be exposed to waves with an annual probability greater than $1x10^{-2}$.

Section 7

Main safety functions

The main safety functions shall be defined in a clear manner for each individual facility so that personnel safety is ensured and pollution is limited.

For permanently manned facilities, the following main safety functions shall be maintained in the event of an accident situation:

a) Preventing escalation of accident situations so that personnel outside the immediate accident area are not injured,
b) Maintaining the capacity of load-bearing structures until the facility has been evacuated,
c) Protecting rooms of significance to combating accidents so that they remain operative until the facility has been evacuated,
d) Protecting the facility's secure areas so that they remain intact until the facility has been evacuated,
e) Maintaining at least one escape route from every area where personnel are found until evacuation to the facility's safe areas and rescue of personnel have been completed.

Section 11

Loads/actions, load/action effects and resistance

The loads/actions that can affect facilities or parts of facilities, shall be determined. Accidental loads/actions and environmental loads/actions with an annual probability greater than or equal to 1*10^-4, shall not result in loss of a main safety function, cf. Section 7.

When stipulating loads/actions, the effects of seabed subsidence over, or in connection with the reservoir, shall be considered.

Functional and environmental loads/actions shall be combined in the most unfavourable manner.

Facilities or parts of facilities shall be able to withstand the design loads/actions and probable combinations of these loads/actions at all times.

Section 29

Passive fire protection

Where passive fire protection is used, this shall be designed such that it provides relevant structures and equipment with sufficient fire resistance as regards load/action capacity, integrity and insulation properties during a design fire load/action.

When designing passive fire protection, the cooling effect from fire-fighting equipment shall not be considered.

Section 30

Fire divisions

The main areas on facilities shall be separated by fire divisions that can withstand the design fire and explosion loads/actions and, as a minimum, satisfy rating H-0 if they can be exposed to hydrocarbon fires.

Rooms with important functions and important equipment, as well as rooms with a high risk of fire, shall be separated from their surroundings with fire divisions with a fire rating corresponding to the fire type and the design fire and explosion loads/actions to which they would be exposed.

Penetrations shall not weaken the fire divisions. Doors in fire divisions shall be self-closing.

Section 31

Fire divisions in living quarters

The living quarters shall be protected by fire divisions that, as a minimum, satisfy fire rating

a) H-60 for external walls facing a process or drilling area and which may be exposed to fire from these,
b) A-60 for other external walls,
c) A-0 for external walls on the living quarters that are located on a separate facility at a safe distance from production or drilling facilities, and for external walls on the emergency quarters on simpler facilities with accommodation, if these quarters are separated from the production or wellhead areas with a main fire division that, as a minimum, satisfies fire rating H-0.

The internal design of the living quarters shall be such that it limits the spread of fire.