Henrik Tehler[1]

Henrik Hassel[2]

A GENERAL FRAMEWORK FOR RISK ASSESSMENT USING SCENARIOS

Abstract: In the risk field the number of risk assessment methods is enormous. In order to ensure that these methods are applied in a way that is suitable for the particular risk problem at hand, it is argued that a firm understanding of basic risk assessment principles is crucial. This document therefore presents a general framework for risk assessment, which builds on a scenario-based definition of risk. The main components of risk assessment is briefly introduced and the idea is that the framework should be used in parallel to specific methods for addressing risk management issues.

Key words: Risk Analysis, risk assessment, risk evaluation, general framework

[1] Professor, Division of risk management and societal safety, Lund University, Box 118, 221 00 Lund, Sweden, henrik.tehler@risk.lth.se

[2] Associate Professor, Division of risk management and societal safety, Lund University, Box 118, 221 00 Lund, Sweden, henrik.hassel@risk.lth.se

1. A GENERAL FRAMEWORK FOR RISK ASSESSMENT

1.1. Background and aim of the paper

Risk assessments are performed in many different contexts ranging from industrial safety, transportation, project management, investments, disaster management and urban planning. In order to perform risk assessments in these different contexts, a wide range of methods exist. These methods have different areas of application as well as different advantages and disadvantages. In order to ensure that these methods are applied in a way that is suitable for the risk problem at hand, it is argued that a firm understanding of basic risk assessment principles is crucial. This paper will therefore present a general framework for risk assessment that describes the most important risk assessment principles. The framework can hence be used as a structure for how to analyse risk in a variety of settings. It also helps to point out what is important to consider when performing a risk assessment – *regardless* of which specific method that are used.

The idea of learning about basic risk analysis principles *before* learning specific methods is based on our experience from research and education. We have seen that if too much focus is placed on the methods, without a good foundation of risk theory and key risk principles, the students and the practitioners may lose sight of the underlying purpose of doing the analysis in the first place. As a consequence they may fail to apply the methods critically. This may in turn reduce the quality of the applications and hence lead to risk-related decisions of lower quality.

Another advantage of developing a general framework for risk assessment is that it can provide a common language and common understanding of key risk concepts and key components of a risk assessment. This is especially important since most contemporary applications of risk assessments are conducted in settings where multiple stakeholders, analysts and organizations are involved in more or less joint efforts of analyzing and managing risk. Having a common conceptual understanding is such a setting is therefore likely to be a success factor.

1.2. Need for risk assessments

All aspects of life, business and society are associated with risks that may lead to negative consequences for people's health, the economy, the environment, or other societal values. Decisions concerning risk are taken continuously by people and organizations but most often it is done without any formal risk assessment. This may be due to the stakes not being that high or the uncertainties being rather small. However, in cases where stakes are high, uncertainties large, number of people potentially affected large, etc. there may be reasons to adopt a more systematic and formal process to try to understand the risks that a system of concern is exposed to. In these circumstances, formal risk assessments can provide an explicit and transparent information basis that decision makers can make use of when balancing the different objectives in a decision situation. The risk assessment can both provide insights into how high the total risk levels are but also to highlight what the main risk contributors are which can guide decisions of how to reduce risk. Finally, the assessment process can *in itself* be fruitful by creating a common understanding, i.e. integrating various competencies and perspectives, stimulating reflection and creating mental awareness.

The need of risk assessments are increasing today. The reasons for this are manifold – here three will be mentioned. First, societies and people are generally more concerned with the risks they are exposed to today compared to before and hence the demands for risk assessments are increasing. Secondly, the technological development goes faster and faster, and many technologies that are being developed are associated with the potential of causing catastrophic consequences – artificial intelligence, genetically modified crops, nuclear power and nuclear weapons to mention a few. Finally, global societal and human-induced natural changes, including climate change, globalization, urbanization, may quickly give rise to new or changed risks which means risk assessments must be performed to decide on proactive actions to adapt to and/or to mitigate these risks.

2. DEFINING RISK – LAYING THE FOUNDATION FOR EFFECTIVE RISK MANAGEMENT

To establish a framework that facilitates collecting, sharing, and analyzing information related to risk in a context where multiple stakeholders contribute and influence the processes is a challenge. Nevertheless, the challenge would be even greater if we could not agree on what the focus of our attention, risk, really is. Therefore, an important step towards such a framework is to define what is meant by risk in such a way that different stakeholders can accept and understand the definition. It is also important that the chosen definition of risk provide enough guidance on how different actors should describe and analyze risk in practice. Because if not, communication difficulties between actors may arise possibly leading to risk assessments and decisions of lower quality.

A large number of definitions of risk exist in the literature – see Aven [1] for an overview. Most of these definitions involve some aspect of *uncertainty* and *negative consequences* that may occur in the future. However, several of the definitions are too vague to provide the necessary concrete guidance noted above. A good general starting point for a framework for risk assessment is the definition suggested by Aven and Renn [2] “Risk refers to uncertainty about and severity of the consequences (or outcomes) of an activity with respect to something that humans value”. This definition highlights uncertainties, negative consequences and the fact that human values play a crucial role in defining what is seen as a negative (and positive) consequence. To operationalize the definition further the concept of scenarios can be used. A scenario is a possible future chain of events that may or may not occur in the system of interest, i.e. it expresses an uncertainty about the future course of events. Scenarios are good to use when communicating information concerning risk since they are descriptions of possible events in the world and thus they are concrete and usually easy for people to understand, as opposed to abstract concepts such as risk. In addition, typically, uncertainty is also described by attaching a probability to the scenario – but other ways of expressing the uncertainty exist (see Flage et al. [3] for an overview of ways to describe uncertainties).

The definition of risk that is used in the present framework consists of a combination of the three concepts mentioned above (scenarios, uncertainty, negative consequences) formulated in terms of three questions:

- What can happen?
- How likely is it?
- What will the consequences be [for something humans value]?

Thus, according to this definition "risk" is the answer to these questions [4-6]. The implication of defining risk in this way is that when performing a risk analysis the aim is to answer the questions concerning a specific system in a specific context. The three questions can then become a "language" that different actors use when they share information on risk issues. Furthermore, this definition provides flexibility as it can be used along with a great variety of different methods for risk analysis. The definition is applicable as long as the results from using the methods can be presented in terms of the three questions.

Finally, since the concept of risk is dependent on values it is impossible to say that there is such a thing as an "objective" risk assessment. However, as Slovic [7] points out "…danger is real, but risk is socially constructed", which means that the potential devastating events that are the focus of the assessment are real in the sense that they may happen in the future, i.e. an earthquake can destroy a city or you can get hit by a bus when crossing a street. But the key point is that when we talk about risk it is a concept that we construct, i.e. it does not exist independent of human beings since it is humans that attach values to certain outcomes.

From a risk assessment perspective, this does not pose a serious problem. A risk assessment does not need to claim that it is objective to be useful. In fact, the whole idea of a risk assessment is to bring together the available facts (which might be called objective but that also might be contested for risk problems associated with high uncertainties and conflicting goals), judgements/assumptions/logical reasoning concerning the world (since objective facts, such as long-term statistical records, are typically not available for everything of interest in a risk analysis) and values to construct a basis for a decision, and therefore it is better to view a risk assessment as a set of arguments concerning risk rather than something that is objective. Transparency in those arguments then naturally becomes crucial.

3. OVERVIEW OF THE FRAMEWORK

In Figure 1, an overview of the framework can be seen. The framework should be read from the bottom up with the logic that each step of the framework build on the foundation provided by the step below. At the same time, in actually performing a risk assessment there might well be iterations back and forward between the different steps since new insights might arise and new choices made that may influence a previous step.

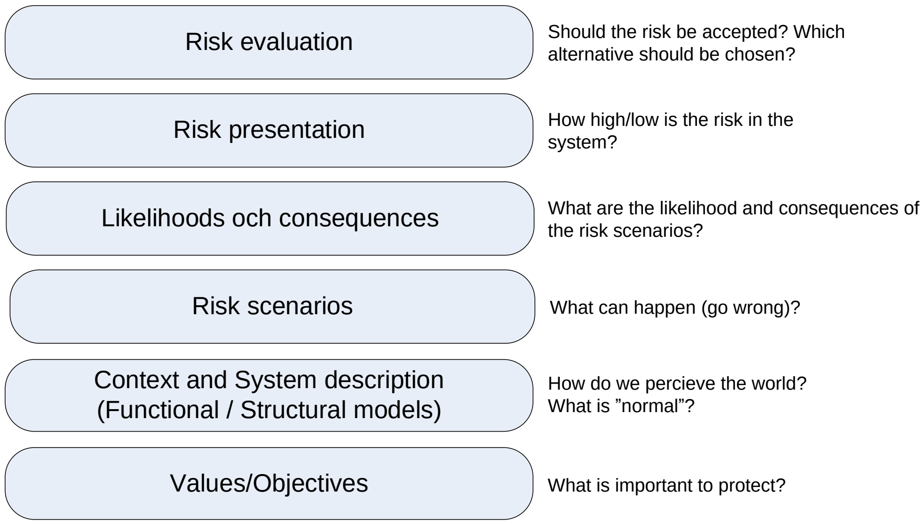


Figure 1. Overview of the genereal framework for risk assessment.

4. VALUES – WHERE IT ALL STARTS

Keeney [8] writes that "Values are what we care about", and values are very important for risk assessment. In fact, if we did not care about anything there would be no risk. Put differently, if there were nothing that we wanted to protect[3] there would be no negative consequences irrespectively of what happens in the world, e.g. floods and earthquakes. Unfortunately, values are often taken for granted, i.e. one assumes that everyone share the same values. This might be true in some cases, e.g. most people agree that protection of human life is important. In addition, there might be cases where risk assessments are performed due to a legislative requirement that essentially pre-determines what values should be addressed by the analysts (i.e. the values are defined by some decision makers outside the risk assessment process). However, there are also many situations where it is not the case – especially when the risk assessment address an issue where there are tensions, goal conflicts, etc. In addition, typically a risk analysis cannot address what everything single person cares about (as it would become extremely broad) which implies that delimitations have to be made concerning which values to address in the assessment.

From a risk assessment perspective it is important to note that there is nothing "objective" about values. It is an "expression of preferences among alternatives based on tradeoffs and priorities" [9]. Values are hence inherently subjective or intersubjective, and it is therefore very difficult to claim that an analysis of risk has objective properties. Obviously, some aspect of the analysis might be considered objective but there are parts

[3] Some definitions of risk are also concerned with positive outcomes, then a risk assessment is not only focused on what someone want to protect but also what want to achieve.

that are not. This constitutes a key challenge for anyone working with risk assessment since it excludes the possibility of talking about the "true risk". Instead, the focus in risk assessments should be on trying to use both facts and values to produce a transparent, clear and logically consistent analysis of the risk in a specific system such that the analysis can be used by others in their effort to manage risk [10]. A consequence of this is that any risk assessment following these general guidelines should clearly state which values that have been guiding the work with the analysis and the reason for choosing those values.

Examples of values are "Protection of the life and health of the population", "Protection of the functioning of society", etc. However, often these statements are too vague to be useful in determining how serious a specific *risk scenario* (see below) is and therefore they need to be made more concrete. This is done by specifying the *objectives* that reflect the values. An objective constitutes a way of determining the seriousness of a specific risk scenario. The primary requirement for the objectives is therefore to allow any risk scenario that can be identified to be estimated in terms of its seriousness using the objective(s) in question – i.e. to estimate the negative consequences. For example, a risk scenario that involves a serious flood is difficult to evaluate using only the value "Protection of life and health of the population". Should, for example, seriously injured persons be considered when evaluating the scenario? Should psychological effects of losing friends and family in the event be considered? There are many other such questions that arise when one tries to use vaguely formulated values to evaluate risk scenarios and it becomes even more difficult when one focuses on values such as "Protection of the function of society". Instead, one needs to use concretely formulated objectives to specify how the seriousness of the risk scenarios should be determined. In the flood example, one could specify that the seriousness should be estimated by the number of fatalities due to the scenario (flood) in question. In reality, one might require an even more detailed definition of how to determine if a fatality is caused by the flood, or not.

How to determine which values to focus on in a risk assessment depends on the context in which the assessment is performed. If, for example, it is performed due to a legislative requirement, which e.g. often is done for high-risk industries, these are often specified in the legislative text. If the risk assessment is performed in a company (without a legislative requirement) it would make sense to base the values on the preferences of the management board. Finally, if the assessment is done in a societal context, such as for a municipality, it makes sense to try to reflect the values and views of the population or from the democratically elected decision makers.

5. CONTEXT AND SYSTEM DESCRIPTIONS – A WAY TO COMMUNICATE HOW WE PERCEIVE THE WORLD

When performing a risk assessment and in particular when communicating the result of it to others (usually in the form of a report) it is very important to include a description of the system of interest and the context in which it is situated. Note that "system" does not mean "technical system" but can be any context in the world for which we are interested in analyzing risk, e.g. a local community. Roughly, the "system" constitutes of structures and functions affecting the risk picture that the decision makers have possibilities to influence. For example, in an industry this would typically be everything within the factory premises. The context, on the other hand, constitutes the external environment of the system that cannot be influenced as easily by the decision makers (but still affects the risk picture for the system). For example, in an industry this could constitute the external power supply system, surrounding residential areas, etc. ISO 31000:2009 [11] provides additional details on what could be regarded as system and context.

The reason(s) why it is so important to include descriptions of system and context is that when humans perceive the world we see different things of different complexity. Consider, for example, the way a geologist would describe a mountain range compared to a downhill skier. Most likely, they will provide quite different descriptions of the same mountain range, and these different descriptions would most likely give rise to risk assessments with different focus. Furthermore, in many cases a more complete picture of the system can be developed by combining the knowledge and perspectives from different people (e.g. a behavioral expert, chemical engineer and a fire safety professional).

In a risk assessment, one can distinguish the part where the context and system is described from the part where different risk scenarios are identified, described and analyzed. The first part can be said to be concerned with “the actual”, i.e. how things are right now, whereas the other is concerned with “the potential”, i.e. with how things might be in the future. The essence of a risk assessment is the second, i.e. “the potential”, but if information concerning the output of a risk assessment is to be accurately communicated within and between various organizations, one also needs to describe the current state of the system for which one is doing the assessment. In addition, a good starting point for identifying risk scenarios is often a description of the current, normal or success scenario of the system as it provides a baseline from which deviations may arise. The concept of success scenario will be further addressed in the next chapter about risk scenarios.

The type and content of the system description and the level of detail are dependent of the purpose of the assessment and the resources available for the assessment. As a rule of thumb, one should describe the system and the context using at least the same level of detail as one plan to use when describing risk scenarios. For example, if one is planning to describe consequences in terms of number of fatalities, i.e. the values used as a basis for the assessment is protection of human life, one should at least describe how many people are living in the area of concern and how population densities differ in the area. Moreover, if one aims to describe the effect of different risk scenarios for different part of, for example, a community one should describe how the parts differ in terms of their vulnerability to the risk scenarios in question. One example of this is if you intend to describe the fatalities due to floods in different areas of a community, it is probably a good idea to include a description of how the elevation of the land differs between the different areas. Hence, if it is realized that the risk scenario descriptions become too rough based on a particular system description, then one may have to go back and add more details to the system description.

As is obvious from these examples, there is not a single objective way of describing systems and their contexts. One has to make choices regarding what to include and what to exclude from the assessment, i.e. one have to make simplifications as reality contains an infinite number of variables and details. Another choice is whether it is the system as it looks at the time of the assessment that should be analyzed or if future changes or trends should be taken into account (e.g. demographic changes, climate changes, etc.). In addition, the values that are chosen as basis for the assessment will affect the system and context description. For example, an assessment focusing on environmental consequences would need to describe a municipality differently compared to an assessment that focus on fatalities due to traffic accidents.

There are two main types of system models that one can use when describing a system. One is called a structural model and the other a functional model. The structural model shows relations between different elements that are important in the system. The functional model illustrates some type of dynamics, i.e. things are happening and activities performed. A typical structural model of a city is a map and for an organization it could be an organization chart where the relations between various parts of the organization (such departments or employees) can be seen. Another example is a piping and instrumentation diagram in an industry displaying components such as valves, pumps and tanks. A typical functional model in the context of an organization would be a model of one of the business processes, e.g. the stages of project from the start to the finish. For an industry, a functional model could describe the various stages of the manufacturing process, such as first heating, then mixing and finally cooling of chemical reactants.

In addition to being useful as a tool to identify risk scenarios, the models are also useful when working with the risk assessment since they can be used as a means of communication within the team performing the assessment – essentially to create a common understanding of the system and to integrate various perspectives of the system. In addition, they are useful when the assessment is finished and needs to be communicated to others since they can facilitate the understanding of the system, context and delimitations made by persons not involved in the assessment itself.

To increase the possibility for persons not involved in the risk assessment to judge the quality of the assessment it is important to describe how one arrived at the description of the system and context, not just the final description itself. This concern is similar to that of reliability and validity concerns when communicating research findings in general. For example, you might claim in your assessment that the majority of the people in a community are fishermen and dependent on their ability to fish for their livelihood. However, when someone else should use the report they will wonder what basis for the claim you have since it will influence their ability to use the results, much in the same way reliability and validity issues will influence other researcher's ability to use research results. Therefore, one should take care when describing the context or system of interest and not only describe the final system model, e.g. a map, but also describe how one arrived at the description, e.g. the method used. There are many ways of arriving at a description of the context and often one does not think of this as following some specific "method". However, from a quality perspective it is important to describe how one did it, even though one did not use a formal method, e.g. describe from where one got the information that was used, etc.

6. RISK SCENARIOS – HOW WE DESCRIBE THE BAD THINGS THAT CAN HAPPEN

Risk scenario is a term that is used to denote a chain of event that may lead to something that is undesirable according to the values/objectives that are used as the basis for the analysis. Many methods for risk analysis focus on risk scenarios in one form or another. In fact, the main "product" of using many of the more common methods for risk analysis is a list of risk scenarios that may happen in the system of interest. This list of possible risk scenarios is the answer to the first question in the definition of risk used here, i.e. "What can happen?".

To illustrate risk scenarios so-called state space diagram can be used. A state space diagram presents how the state of a system changes over time – i.e. how variables describing the system (y- and x-axis) change over time, where a change is illustrated by a line in the diagram. Since most systems, particularly complex ones, can be described by a large number of variables the 2-dimensional state space diagram is just used for illustration purposes. A starting point for the illustration of a risk scenario is the success scenario, S_0, which displays the desirable scenario, i.e. what one want to happen in the system (see Figure 2a). Any deviation from the S_0-scenario is then a risk scenario and the goal of the risk assessment is to identify the risk scenarios that can occur.

A risk scenario always have some initiation where the state of the system starts to deviate from what is desirable. This can be an internal event, such as the failure of a component, or it could be an external event, such as the occurrence of an earthquake. This event is referred to as an Initiating Event (IE) – see Figure 2b. The risk scenario then evolves until it is possible to estimate the negative consequences, e.g. it should be possible to estimate the number of fatalities if that consequence dimension reflects the underlying values/objectives, which means that it has reached an End State.

A single Initiating Event can of course give rise to multiple different End States depending on a number of different factors and circumstances that the analyst are uncertain of at the time of the assessment. It could be whether protective barriers will function or not (e.g. whether the water sprinkler system will work during a fire or whether the Early Warning System will work during an earthquake). But it can also be about the timing of the event (day or night; summer or winter) or any other circumstance that is uncertain but will affect the negative consequences. Hence, an initiating event gives rise to a tree of scenarios with a number of different branches where each branch represents a risk scenario (see Figure 2c)

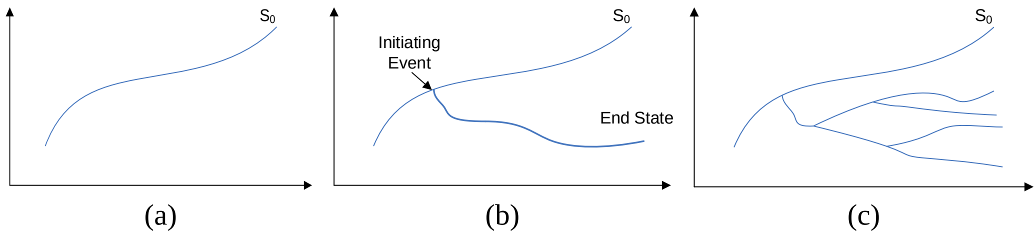


Figure 2. Illustration of risk scenarios. In (a) the success scenario is illustration, in (b) the initiating event and end state is illustrated and in (c) the branching of risk scenarios are illustrated.

In reality, the number of risk scenarios is approaching infinity since in theory a scenario can be specified in an extremely detailed way. In a practical setting, it is rarely possible to go into too many details as the available time and resources put an upper limit to the number of scenarios that can be managed. In addition, the benefit of analyzing two scenarios that are very similar in their characteristics is also minor. This means the number of scenarios must be reduced by defining a representative set of scenarios that together *cover* all scenarios that can occur in reality.

The process of reducing the number of scenarios to include in an assessment can be guided by a number objectives or ideals:

1. The set of scenarios should have a *suitable level of detail*. This has to do with the balance between describing scenario in a too rough way and too detailed way. A rule of thumb is that the risk scenarios included in the analysis should be specified with enough detail to allow for sufficiently accurate consequence estimations. For example, the scenario "flood in the city of Malmö" would not be specified in enough details as e.g. the flood severity (extent of water level rise, duration, etc.) is not specified. Hence, consequence estimations would be associated with too large variation to be meaningful and the scenario therefore need to be subdivided. At the same time, the number of scenarios must be manageable, given the available time and resources, since the more detailed/numerous the scenarios become, the more resources it takes to estimate their likelihoods and consequences. Therefore, scenarios must sometimes be clustered together to form a broader scenario cluster. The exact meaning of what is a suitable level of detail will in the end vary depending on the purpose of the assessment and the needs of the decision makers – if the assessment is a first, preliminary qualitative assessment then broader scenarios should be defined. But if it is an in-depth, quantitative assessment then scenarios should be specified in more detail

2. The set of scenarios should be *complete*. This means that the risk scenarios included in the analysis should strive to cover/represent all future scenarios that can occur in reality – otherwise it would simply not provide a complete picture of the risks and hence provide underestimations. Again, this does not mean that the risk analysis must include detailed descriptions of each and every future possible

risk scenario. This is unrealistic since those scenarios that actually do occur can be described in almost infinite number of ways. Instead, it means that it should be possible to assign each future potential scenario to one of the identified risk scenarios; i.e. each risk scenario described in a risk analysis always constitutes a class of more detailed scenarios. For example, the risk scenario "pipe rupture" would cover numerous more detailed scenarios (e.g. pipe rupturing at different locations, at different times, with different hole sizes, etc.). However, it should be noted that it is impossible to know for sure whether a risk analysis has actually covered all relevant risk scenarios (there are always surprises, especially if the system of interest is highly complex). However, using methods and procedures that stimulates broad and creative identification of scenarios is one recommendation. Another recommendation is to include a broad set of participants with complementing competencies in the risk identification phase and to learn from past events in the system of interest as well as from other similar systems. A third recommendation is to always include a scenario called "other risk scenarios" to remind oneself that there are always scenarios that have not been included. In the end, a risk analyst must be humble when it comes to the ability to cover everything and to try to compensate for the fact that some scenario may be left out by adding safety margins and make conservative assumptions.

3. The set of scenarios should be disjoint, i.e. *mutually exclusive*. This means that there should be no actual future scenarios that can be described by more than one risk scenario in the risk analysis. A trivial example is of one has identified two earthquake scenarios: one with magnitude 6-8 and one with magnitude 7-9. Then an earthquake with magnitude of 8 would be described by both risk scenarios in the analysis which means that the scenario is double counted when the likelihood of the scenarios are estimated and which in turn gives an overestimation of the risk. Note that, some methods for risk assessment if used correctly, such as event trees, automatically give rise to a mutually exclusive set of scenarios.

4. The risk level should *neither be over- nor underestimated*. In the process of reducing the number of scenarios, the goal should be not to distort the risk level, i.e. the estimated risk should remain the same even though the number of scenarios have been reduced. This can be done by first making sure that the likelihood is estimate for the *whole scenario cluster*. For example if the scenario Flooding of 2-4 m is defined, the likelihood should be estimated for any flooding of between 2-4 m rather than e.g. estimating the likelihood for a 3 m flood. Secondly, when the consequences are estimated this should be done for the average consequences for the cluster of more detailed scenarios that is part of the scenario description. E.g. for the 2-4 m flood an average case of let us say 3 m flood should be the basis for the estimation.

A number of strategies can be used in the process of reducing the number of scenarios to include in the risk assessment:

1. If the negative consequence of a scenario is insignificant (e.g. acceptable independent of the likelihood) then it can be ignored.
2. If two or more scenarios are very similar, in terms of consequences, then they can be clustered.
3. Parameters that do not have a particularly large influence on the negative consequences can be fixed at their mean values.
4. For parameters that do significantly influence the negative consequences but that can take on many or infinite number of values then only choose a few possible values that cover both smaller and larger consequences (of course unless the computational cost of using more/all values is small).

7. ESTIMATING LIKELIHOODS – COMMUNICATING UNCERTAINTY TO OTHERS

Risk assessment concerns describing potential future negative events and there is uncertainty associated with which scenario that actually will occur. Likelihood estimation is one way of characterizing this uncertainty – although there are other ways as well (see Flage et al. [3] for an overview). Estimating how likely certain events are is often perceived as one of the more difficult tasks in a risk assessment. Nevertheless, it is one of the most important ones simply because if it is left out the risk assessment cannot be called risk assessment anymore since uncertainty is such an important part of the concept of risk – it constitutes the second of the three risk questions that were previously stated. However, one should not make the mistake and associate likelihood estimation strictly with the quantitative estimations of probabilities. There are other ways of estimating and describing likelihood. Some of these techniques will be described here.

In general, different information sources can be used as a basis for likelihood estimations. Ideally, the estimation can be completely based by using experiences from what has happened in the system historically. With enough observations, it would be possible to calculate the relative frequency of different possible events, which then give rise to objective measures of likelihood. However, in reality this data is rarely available for the system of interest. Some past experiences might exist but they are typically limited both when it comes to the amount of data, e.g. the system has only been operational for 5 years where perhaps only a few incidents have occurred), and also when it comes to the relevance of the data. For example, the system or context of the system may have undergone changes making historical data not fully applicable for current or future conditions. This further means that other information sources often have to be used. One such source is the use of logical models. A logical model, such as an event or a fault tree, is developed from knowledge about the behavior of a system and by linking the event one wants to estimate the likelihood for to other events that are easier to estimate the likelihood for (e.g. where there are more data available). Finally, often expert judgements also have to be used to make likelihood estimates; however, it should be noted that people, including experts, are a rather unreliable source of information as we are affected by many psychological bias [12]. Combining different information sources and improving the estimates as more experiences and knowledge is gained is recommended.

When selecting how to estimate likelihood one must consider the purpose of the estimate, i.e. what properties do you want the estimate to have. Based on such properties one can distinguish four different types of likelihood estimates that are commonly used in risk assessments: (1) verbal descriptions of likelihood, (2) a qualitative ordinal (ranking) scale, (3) a semi-quantitative ordinal (ranking) scale, and (4) a quantitative cardinal scale. In the present context, an ordinal scale express order, e.g. one can say that event A is more likely than event B, but one cannot express how much more likely event A is compared to event B. Using a cardinal scale one can express order, and one can express how much more likely an event is compared to another. Thus, in selecting a way of expressing likelihood one needs to determine what is necessary in the context one is working. For example, do you need to be able to order events in terms of likelihood?

In determining which type of likelihood expression to use one could investigate the benefits and drawbacks of the four types.

7.1. Verbal descriptions of likelihood

A verbal description of likelihood means that the assessment contains statements of the type “Scenario A is not likely”, “Scenarios B is very unlikely”, etc. In some contexts, such statements are common, and they usually do not require much effort to produce. On the other hand, from a risk governance perspective they are not suitable since the meaning of words like “unlikely” differ depending on the person using the word and the context in which it is used. Therefore, it becomes problematic to communicate estimates of likelihood between persons and organizations. Moreover, because words are perceived differently depending on the context in which they are used it is not possible to establish a rank order among various scenarios based on their likelihood estimates. This problem can to a certain extent be alleviated by establishing a dictionary that can be used to “translate” words into quantitative statements. However, in that case the procedure matches type 3, semi-quantitative ordinal (ranking) scale. In the present context, it is therefore not recommended to use only verbal descriptions of likelihood.

7.2. A qualitative description using an ordinal (ranking) scale

Instead of relying on the use of words when expressing likelihood, one can establish a relative ranking scale that can be used to communicate how likely various scenarios are estimated to be in relation to each other. A common type of scale for this is a five step-scale, i.e. the likelihood is expressed using a number between 1 and 5, where 1 represents the least likely scenario and 5 the most likely. Often each of the steps on the scale is associated with a short verbal description, such as “Likely”, “Unlikely”, “Very likely”, etc. However, note that the difference compared to category 1 (Verbal descriptions of likelihood) is that the present category involves establishing an ordinal scale to be used. Category 1 does not involve establishing such a scale but the person using the likelihood estimates have to interpret the meaning of the word without the guidance of such a scale.

The benefits of using a qualitative ordinal scale are that it is fairly easy to use, and people usually feel comfortable using it. Moreover, it also allows the analyst to express order in terms of likelihood among the risk scenarios that have been identified. This is useful when it is time to analyze the risk since one can then identify scenarios that are both estimated to have a (relative) high likelihood of occurring and involves (relative) significant consequences if it should occur.

Notwithstanding the positive aspects of using a qualitative ranking scale, there are some considerable drawbacks, especially when considering that a risk assessment is supposed to be useful for others than the ones that produced it. When one person, group or organization produces an estimate of how likely an event is using a qualitative ordinal scale one can compare different risk scenarios to each other using the estimates. However, that can only be done if the assessments of the risk scenarios' likelihoods have been performed in the same risk analysis. Thus, one cannot compare a risk scenario that was identified in an analysis of, for example, earthquake risks, and compare it to a scenario that were identified in another risk analysis of, for example, flood risk. The reason is that even though the same ordinal scale is used in the two risk assessments the context in which the estimates are produced are different and that will influence the meaning of the different steps on the scale, e.g. what is "Unlikely", "Very unlikely", etc. A consequence of this is that one should be very careful when comparing the likelihood of two risk scenarios that were identified and assessed in two different contexts (analyses).

Another apparent drawback of the qualitative ordinal scale is that it becomes difficult to use the result as a basis for decision making concerning risk reduction. Consider, for example, the possibility of implementing a measure that is estimated to reduce the likelihood of a serious risk scenario from "Very unlikely" to "Extremely unlikely". How much resources is it worth to spend on accomplishing this? Using this type of ordinal scale hence provides very limited guidance to a decision maker when faced with such questions.

7.3. A semi-quantitative description using an ordinal (ranking) scale

One step towards alleviating the potential difficulties that a decision maker using the result from a risk assessment might face is to introduce some type of quantitative measure but still keep the ordinal scale. This could be done by associating each of the steps in the scale with a point estimate of the frequency (number of occurrences per year) or a frequency interval. Consider the following scale, for example:

1. Extremely unlikely – less than once every 10.000 year
2. Very unlikely – once every 1.000 year
3. Unlikely – once every 100 year
4. Likely – once every 10 year
5. Very likely – more than once every year

The difference between this scale and the qualitative description using an ordinal scale is the addition of the frequencies associated with each of the steps. This implies, one might argue, that the scale is in fact cardinal. However, since the scale is rather rough in the sense that it usually only contains a limited number of steps (e.g. five) and that the uncertainties associated with the quantitative estimates usually are substantial it is most often used as an ordinal scale (that is why we call it semi-quantitative). The benefit of introducing the quantitative estimates is that it gives a common point of reference for judgements performed in different contexts. In that respect, it increases the possibility of comparing estimates performed in different context by different people. Moreover, since the quantitative estimates are associated with the different steps it provides a rough possibility of providing a decision maker with information concerning how much resources it is worth spending on reducing, for example, the likelihood of one risk scenario from Unlikely to Very unlikely.

While the introduction of quantitative descriptions is positive from many perspectives, it also has some drawbacks. First, not all people are comfortable using numbers when estimating how likely certain events are, especially if the likelihood of them is very small and/or uncertainties are large. Secondly, sometimes the use of numbers can give an impression that the persons doing the analysis are much more confident in their assessment than they in fact are. Although these problems are difficult to address, it might help to explain why numbers are used and also to clarify that estimates using numbers are still estimates that are produced by some assessors (based on their knowledge, experience and judgments). Explicitly communicating uncertainties associated with the estimates can also be a way of conveying the level of confidence to decision makers.

7.4. A quantitative cardinal scale

While a semi-quantitative description using an ordinal scale is useful in many respects, using a quantitative cardinal scale, for example estimating frequencies (usually number of events per year) or probabilities (from zero, meaning the event with certainty will not occur, to one, meaning the event will occur for sure), provides an even better opportunity for communicating information regarding the likelihood of risk scenarios. Some ways of presenting risk are also contingent on quantitative estimations of likelihood (and consequence). Obviously, the estimates produced are still not objective since they reflect the assessors' assumptions and judgments concerning the occurrence of certain events in the future. Nevertheless, expressing likelihood using frequencies opens up new possibilities of using the estimate in the management of risk since it allows for mathematical and statistical operations.

One advantage of using frequencies to express likelihood is that you can easily communicate how uncertain you are concerning the estimate in question by using intervals. For example, assume that you have estimated the occurrence of a flood with a certain characteristics to occur once every 50 year. However, the information that you are basing your estimate on, e.g. interviews or flood data, might indicate that the frequency might well be as low as once in 100 years and as high as once in 20 years. In that case you might want to provide information on this uncertainty and one way of doing it is by expressing the frequency as 0,02 per year (once every 50 years) and also adding an interval to the estimate, e.g. 0,02 [0,01 – 0,05] per year. Such intervals can be very useful when communicating uncertainty and they are also a prerequisite for being able to perform a sensitivity analysis.

8. ESTIMATING CONSEQUENCES – HOW BAD WILL IT BE?

In answering the last question of the definition of risk, "What will the consequences be?", one needs to use the values and objectives on which the analysis is built as a point of departure. Only then can one receive guidance on how to assess the consequences of the various risk scenarios. Furthermore, consequence dimensions can be natural or constructed dimension [13]. A natural dimension is something that can actually be observed after an event has occurred, at least in theory. Examples include number of fatalities (measuring damage to life) and damages in Euros (measuring economic loss). Constructed scale is used in cases there are no natural scales that can be used as a good representation for the underlying values/objectives. Constructed scales are often qualitative such as "Large disturbances in critical societal functions" or "Minor public distrust in public authorities".

In principle one can classify the way to express consequences in much the same way as the one used to describe different ways of estimating likelihood. Thus, the approaches can be classified as (1) Verbal description of the consequences, (2) A qualitative description using an ordinal scale, (3) A semi-quantitative description using an ordinal scale, and (4) quantitative estimates on a cardinal scale. Since the various approaches have been described in the section above the description here will be brief.

1. Verbal description of the consequences

If each risk scenario's consequences are described without use of any scale for ranking or doing cardinal comparison, then the usefulness for risk management decisions is limited. Although it is important to describe the potential consequences of the risk scenarios as detailed as possible one should not forget to also provide an assessment using some type of scale that makes comparison among scenarios possible.

2. A qualitative description using an ordinal (ranking) scale

Consequences due to various risk scenarios are often described using a five-step scale with qualitative descriptions of the various steps. For example "Minimal", "Minor", "Major", "Serious", "Catastrophic". From a risk assessment perspective, such consequence estimates have the same properties as the likelihood estimates using the same type of ordinal scale (see above).

3. A semi-quantitative description using an ordinal (ranking) scale

Sometimes the qualitative descriptions of the steps used to classify consequences due to risk scenarios are complemented by quantitative values. Since consequences can be measures along many different dimensions (which depends on the values that are used) one usually has to establish one separate scale for each dimension. One example of such as scale is illustrated below (involving fatalities). Other relevant consequence dimensions might be livelihood issues, economic impact, environmental impact, etc.

1. Minimal – No fatalities
2. Minor – 1 to 5 fatalities
3. Major – 6 to 20 fatalities
4. Serious – 21 to 100 fatalities
5. Catastrophic – more than 100 fatalities

4. A quantitative cardinal scale

Instead of using a scale with rather limited number of categories, as the one illustrated above, one can instead use a quantitative cardinal scale to describe the consequences of various risk scenarios. Depending on which values and objectives that one use in the analysis the unit of measurement will differ. Some common units are: number of fatalities, dollars, number of seriously injured persons and damaged area (environmental damage).

9. RISK PRESENTATION – MAKING THE ANALYSIS USEFUL FOR DECISION MAKING

Since the number of risk scenarios can sometimes be substantial the scenarios and their associated estimates of likelihood and consequences needs to be processed further to facilitate risk understanding and evaluation, i.e. deciding if the risk is acceptable or not. To reduce the scope and complexity of the information that one needs to consider when performing the evaluation one usually transforms the answer to the three questions into some kind of risk presentation. A risk presentation is thus a way of compiling the information from the risk analysis into a more suitable and useful basis for decision-making.

At a general level, it is possible to distinguish two types of information that may be relevant to present from a risk analysis. Firstly, one is often interested in the total risk level for the system of interest since such information can be used as a basis for decisions concerning risk acceptability and/or for comparisons with other risks. Secondly, one may also be interested in understanding major risk contributors such as what elements, components, or scenarios contribute the most to the total risk of the system. Such information can for example direct efforts to reduce the risk. Sometimes the term importance measure is used to refer to contribution of an element to the risk level or importance of an element for safety. Below we will only further describe the first type of information. More information about importance measures can be found in [14].

There is a vast number of ways to present risk. Typically, there are large differences between different application areas. In this document, some general *type* of ways to present risk will be described rather than going into detail when it comes to exactly how to construct some particular risk measure or metric.

9.1. Point values/index

The most compressed way of presenting risk is using a point values or a single index, i.e. compressing all information from the risk analysis (multiple scenarios, likelihoods and consequences) into a single value. The most common such measure is the expected consequences, such as expected number of fatalities per year in a system of interest – also referred to as Potential Loss of Life (PLL). This measure can be calculated if a quantitative cardinal scale is used for the estimations and it is calculated by multiplying the likelihood and consequence for each scenario and then summing these products. If the expected number of fatalities during a year is 5 persons it means that over a long period of time, say 50, years one expects 250 persons (5 * 50) to die due to the risk in question. The expected value says nothing about if there is one major event with 250 fatalities or if there are multiple smaller events in the time period. Nevertheless, the expected consequences is a very common way of presenting risk because it is fairly easy to estimate and it is a convenient way of compiling all the information from the various risk scenarios into one number. Obviously, that also means that you also lose a lot of information when you use only one value to represent many risk scenarios.

Note that a wide array of other point values can be used to present risk, such as Value at Risk (VaR - often used in finance), and Fatal Accident Rate (FAR – often used in occupational health). See [15] for more information about risk measures in terms of point values.

9.2. Risk matrix

Slightly more information can be gained from presenting the likelihood and consequence of scenarios separately. Most commonly, a risk matrix is used for this purpose. The risk matrix uses a grid structure to present the estimated likelihood and consequences for each risk scenario. Various risk matrixes might look different and have different types of scales for likelihood and consequence (ordinal ranking scale or semi-quantitative ranking scale) and different number of categories, but the general principle of application is the same, see Figure 3 for an example. In the matrix, risk acceptance can also be indicated by coloring the matrix as can be seen in the figure.

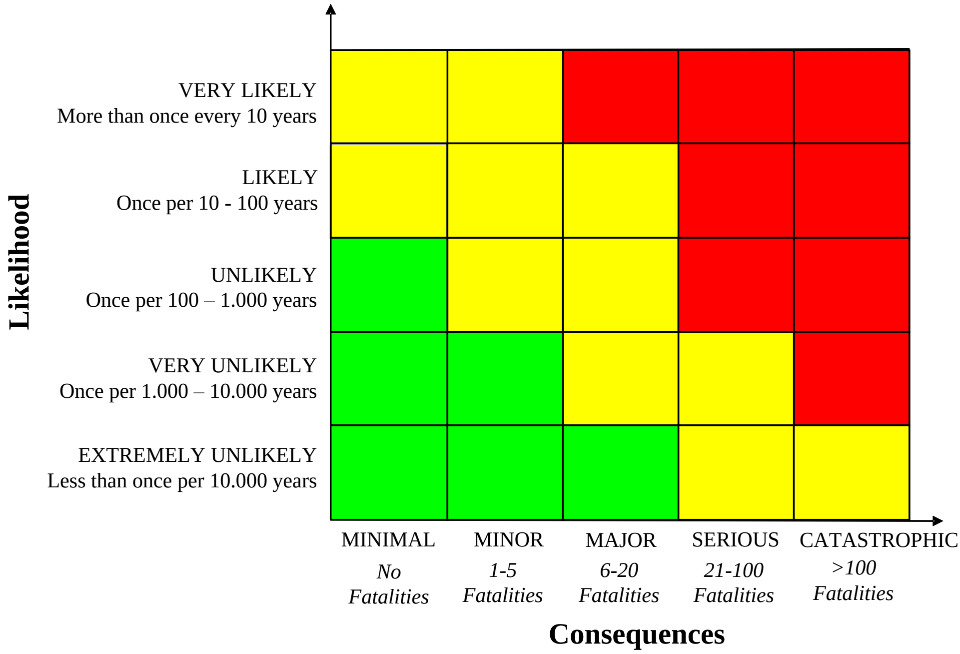


Figure 3. Example of a risk matrix

In the matrix each scenario is plotted, which means there are as many dots in the matrix as there are scenarios. This can to some extent provide an overview of the risk in the system and also which scenarios contribute most to the total risk; however, no aggregation is made of the scenarios into a total risk level. Furthermore, if the likelihoods and consequences estimated using a quantitative cardinal scale then a continuous likelihood-consequence diagram can be used (i.e. instead of for example a discrete number of categories such as 1-5). See Duijm [16] for more information about risk matrices and Ale et al. (2015) [17]for more information about probability-consequence diagrams.

9.3. Maps

Sometimes you are interested in presenting a geographic representation of risk, for example to determine if there are some specific areas that are subjected to high levels of risk. One, of many, ways to present risk geographically is the location specific individual risk. The individual risk at a specific geographic location is the same as the likelihood of dying for a (hypothetical) person that is assumed to stand at the same location for a whole year. It can be estimated for any hazard that has a clear geographic connection, e.g. floods, earthquakes, mudslides. In estimating the individual risk, one must have information on which geographic areas that are affected by each of the possible risk scenario. More specifically, the contribution to the total individual risk from each risk scenarios have to be calculated and then aggregated for all scenarios that affect a particular location. See CCPS [15] for more information about how to calculate individual risk.

9.4. Graphs

Graphs and diagrams can also be used to convey risk information. Compared to a point value, a graph can of course convey more information about the risk but at the same time be more difficult to interpret, especially by people with limited previous knowledge about risk assessment. One common way to present risk information is using probability/frequency distributions.

Neither individual risk, nor the expected consequences provide information concerning the seriousness of the specific risk scenarios. Individual risk does not consider whether there are any people exposed at all (instead, it focus on risks connected to geographical locations that may or may not be populated). Using those two ways of presenting risk one cannot see whether the total risk level is made up of very unlikely risk scenarios but with very high consequences or if it is the result of very likely risk scenarios with relatively limited consequences. This information can be important for making decisions concerning the acceptability of risk and therefore a way of presenting risk called FN-curve has been developed and used extensively.

An FN-curve shows an estimate of how often (frequency) N people or more will die due to a specific risk. In that way it is in fact a Complentary Cumulative Distribution Function (CCDF) which is a common method to display statistical data. See [15] for more information about how to construct FN-curves.

10. RISK EVALUATION – SHOULD WE ACCEPT THE RISK OR DO SOMETHING ABOUT IT?

When a risk analysis has been completed and the results presented both in terms of the answer to the three questions and in terms of some type of risk presentation one can continue by performing a risk evaluation. According to ISO 31000:2009 [11] for risk management Risk evaluation is a "process of comparing the results of a risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable". How you perform risk evaluation is much connected to the presentation of risk that you have employed in your analysis. However, on a more general level it is possible to distinguish between two general types of approaches to risk evaluation: rights-based approach and utility-based approach.

In the rights-based approach the focus is completely on the risk level. In its simples version a comparison is made with some level of risk that has been decided (by some decision makers) to be the limit between what is acceptable and unacceptable. If the risk level from the performed risk assessment is lower than the limit, the risk can be accepted. In reality, there are several challenges both when it comes to setting the unacceptability limit as well as how to account for the, sometimes large, uncertainties associated with the risk assessment results. See [18] for more information about risk acceptability criteria.

In the utility-based approach, it is acknowledged that the risk level is not the only aspect affecting risk acceptability. There might be benefits associated with a risky activity as well as other drawbacks associated with the activity. Determining acceptability is then accomplished by comparing all benefits with all drawbacks. If the drawbacks are greater than the benefits, the risk is not accepted. The most common method for doing this is the well-known cost-benefit analysis (CBA). The rights-based and the utility-based approach can also be combined which is for example done in the Tolerability of Risk (ToR) framework used by the British Health and Safety Executive [19].

11. FINAL REMARKS

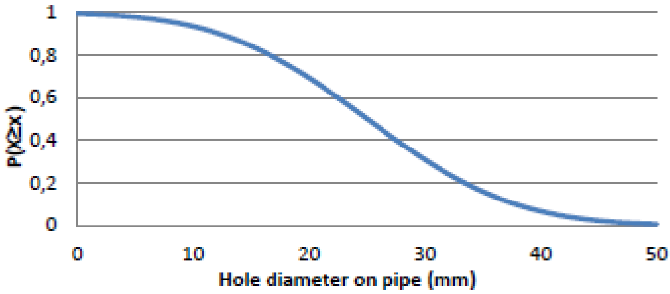
This document has presented a general framework for risk assessment; however, it is merely an brief introduction to the main concepts of risk and components of risk assessment. However, there are additional topics that have not been addressed in depth in this document. Two such topics are sensitivity and uncertainty analysis. Sensitivity analysis concerns analyzing to what extent a change in a single input data parameter give rise to changes in the output (are the changes significant or can the same conclusions be drawn) and uncertainty analysis aims to display how uncertainties in several input parameters and models used give rise to uncertainties in output data (such as risk levels). Applying sensitivity and uncertainty analysis techniques improves the decisions and provides a better basis for communicating the results of the risk analysis (what one knows and also what one does not know). The present document do not address risk treatment and sensitivity/uncertainty analysis in detail but some basic information can be found in [3, 11].

A final remark is the importance of good documentation and reporting. Performing a good risk assessment is obviously an important part of good risk management. However, if the result from risk assessments fails to be communicated to the relevant stakeholders and decision-makers much of the potential benefits of conducting systematic risk assessment work is lost. The most important aspect of good reporting is transparency. When describing the context, the assessments of likelihood and consequences, etc. you need to include descriptions of what the basis for those assessments/descriptions are. This can be information from scientific literature, reports, statistics, etc. but it can also be expert judgments, information received in focus group sessions, at interviews of various stakeholders, etc. It is of vital importance for the quality of the assessment to also include description of how one arrived at the estimates that are used in the assessment. Note that it is also important to describe how the analysis group reasoned when coming up with the assessments.

QUESTIONS

1. What does it mean to specify values/objectives in a risk assessment and how does this affect the risk assessment process?
2. What does it mean to perform a risk assessment that is *complete*?
3. What does a *suitable level of detail* mean when it comes to modelling risk scenarios?
4. Make a suitable selection of *three*hole sizes (for a tank leak in a chemical industry) from the diagram below that would fulfil the requirements of

completeness, suitable level of detail and non-overlapping scenarios. Also assign a probability to the hole sizes.



REFERENCES

1. Aven, T. (2012). The risk concept—historical and recent development trends. *Reliability Engineering & System Safety*, 99: p. 33-44.
2. Aven, T. and Renn, O. (2010). *Risk Management and Governance: Concepts, Guidelines and Applications*. Heidelberg: Springer.
3. Flage, R., Aven, T., Zio, E., and Baraldi, P. (2014). Concerns, Challenges, and Directions of Development for the Issue of Representing Uncertainty in Risk Assessment. *Risk Analysis*, 34: p. 1196-1207.
4. Kaplan, S. and Garrick, B.J. (1981). On The Quantitative Definition of Risk. *Risk Analysis*, 1(1): p. 11-27.
5. Kaplan, S. (1997). The Words of Risk Analysis. *Risk Analysis*, 17(4): p. 407-417.
6. Kaplan, S., Haimes, Y.Y., and Garrick, B.J. (2001). Fitting hierarchical holographic modeling into the theory of scenario structuring and a resulting refinement to the quantitative definition of risk. *Risk Analysis*, 21(5): p. 807-819.
7. Slovic, P. (2001). The Risk Game. *Journal of Hazardous Materials*, 86: p. 17-24.
8. Keeney, R.L. (1992). *Value-Focused Thinking, a Path to Creative Decisionmaking*. Cambridge: Harvard University Press.
9. Otway, H. and von Winterfeldt, D. (1992). Expert Judgement in Risk Analysis and Management: Process, Context, and Pitfalls. *Risk Analysis*, 12(1): p. 83-93.
10. Hansson, S.O. (2010). Risk: objective or subjective, facts or values. *Journal of Risk Research*, 13(2): p. 231-238.
11. ISO (2009). *ISO 31000:2009 - Risk Management - principles and guidelines:* . Geneva: International Organization for Standardization.
12. Montibeller, G. and von Winterfeldt, D. (1995). Cognitive and Motivational Biases in Decision and Risk Analysis. *Risk Analysis*, 37(7): p. 1230-1251.
13. Keeney, R.L. and Gregory, R. (2005). Selecting Attributes to Measure the Achievement of Objectives. *Operations Research*, 53(1): p. 1-11.
14. Nökland, T.E. and Aven, T. (2013). On Selection of Importance Measures in Risk and Reliability Analysis. *International Journal of Performability Engineering*, 9(2): p. 133-147.

15. CCPS (2000). *Guidelines for Chemical Process Quantitative Risk Analysis*. 2 ed. New York: Center for Chemical Process Safety, American Institute of Chemical Engineers.
16. Duijm, N.J. (2015). Recommendations on the use and design of risk matrices. *Safety Science*, 76: p. 21-31.
17. Ale, B.J.M., Burnap, P., and Slater, D. (2015). On the origin of PCDS – (Probability consequence diagrams). *Safety Science*, 72: p. 229-239.
18. CCPS (2009). *Guidelines for Developing Quantitative Safety Risk Criteria*. New York, : Center for Chemical Process Safety, American Institute of Chemical Engineers.
19. HSE (2001). *Reducing risks, protecting people - HSE's decision-making process*. Norwich: Health & Safety Executive.