Reliability Engineering and System Safety 191 (2019) 106553

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

How the distinction between general knowledge and specific knowledge can improve the foundation and practice of risk assessment and risk-informed decision-making

Terje Aven[a,*], Vidar Kristensen[b]

[a] University of Stavanger, Norway
[b] Wintershall Norge, Stavanger, Norway

ABSTRACT

There is an increasing awareness and recognition of the importance of reflecting knowledge and lack of knowledge in relation to the understanding, assessment and management of risk. Substantial research work has been initiated to better link risk and knowledge. The present paper aims to contribute to this work by distinguishing between different types of knowledge: general knowledge and specific knowledge. For example, in relation to an offshore installation, the former captures knowledge about what could happen and why on offshore installations in general, whereas the latter covers more detailed knowledge related to the specific installation of interest and its operation. Risk management is viewed as the process of making sure that the general knowledge is sufficiently and efficiently used, including the identification of the specific knowledge needed, and ensuring that we have sufficient specific knowledge and control when assessing risk and making decisions. In the paper, we present a risk management framework built on these ideas and knowledge distinction. This framework clarifies interactions between the two knowledge bases, and how these bases can be used to improve the foundation and practice of risk assessment and management.

1. Introduction

Consider the challenge of managing the risk related to the design and operation of a technical system, for example an offshore petroleum installation. Two fundamental strategies are commonly adopted for this purpose: i) the use of risk assessments (risk-informed strategy) and ii) the use of robust/resilient arrangements and measures (founded on the cautionary/precautionary principles [8,33,37]). Simplified, we can say that the latter is justified as a result of the limitations in the former: the risk assessments' lack of ability to properly reflect all aspects of risk [5]. These limitations are to a large extent about revealing uncertainties and lack of knowledge. We have some knowledge about the events and relevant systems and components; yet, there are always uncertainties. To meet these, we implement risk management systems. The aim of these is to control the risks, prevent the occurrence of incidents and accidents and/or to limit their consequences.

In practical (real-life) situations, there is also a third, supplementary strategy to i) and ii), which may be labelled 'risk-based requirement strategy'. This strategy is typically used when the knowledge is strong – the situations considered are well-understood and there is nothing new or unusual about the system or activity under study. Experience, statistical analysis and traditional risk assessment may have been used to establish the 'risk-based requirement strategy'. The idea is reflected in standards, for example the risk-related decision-making framework by ISO 17776 [20]. In this standard, the 'risk-based requirement strategy' is labelled 'good practice' and is added to the other two basic risk management strategies (assessment techniques) referred to above.

Depending on the decision context considered, these three management strategies are, to varying degrees, adopted. With strong knowledge and minimal uncertainties, the 'good practice' approach is justified, whereas, if the values at stake are high and the uncertainties are large, all three strategies are required. For other situations, with fewer uncertainties, the cautionary and precautionary strategy ii) is not given the same weight.

To illustrate this discussion, consider the offshore industry in Norway. In the early years of this industry, there was little knowledge about the hazards and potential accidental events that this industry faced. Risk assessment methods were introduced, and they matured as the industry expanded, contributing to increasing the general knowledge about the associated risks. The industry also gained knowledge about the safety and control measures needed, and how to design and operate the facilities in a safe manner. It learned from successes, failures, near misses and accidents.

To a large extent, today, the same hazards remain on an offshore facility as in the early days. The main difference is the increased general knowledge about the hazards and an increased general knowledge on how to manage them.

* Corresponding author.
E-mail address: terje.aven@uis.no (T. Aven).

https://doi.org/10.1016/j.ress.2019.106553
Received 4 March 2019; Received in revised form 28 May 2019; Accepted 26 June 2019
Available online 27 June 2019

Due to this increased general knowledge in the offshore industry, gained through experience, improvements and years of conducting risk assessments, the basic strategies i) and ii) have largely been replaced by a 'risk-based requirement' strategy with the use of codes and specific requirements that need to be met. An example of this is the specific requirements established for how to design and operate safety (barrier) systems. If these requirements are fulfilled, no further risk assessments are needed for the hazards and safety systems covered by the requirements.

However, when new technical concepts and arrangements are introduced, for example when moving the control rooms for offshore facilities from offshore to office buildings onshore, a more thorough and traditional risk assessment strategy, combined with a robustness/resilience strategy, is required.

We are led to a classification system, based on three types of risk management strategies:

a) Risk-based requirements strategy.
b) Risk assessments (risk-informed) strategy.
c) Cautionary (use of robust/resilient arrangements and measures) strategy.

In addition to strategies a–c), dialogue and discursive strategies need to be mentioned. These strategies use measures to build confidence and trustworthiness, through clarifications of facts, reduction of uncertainties, involvement of affected people, deliberation and accountability [33,36]. A successful example of the use of such strategies is the three-party dialogue introduced in the Norwegian petroleum industry, where formal collaboration is established between the industry, the unions and the authorities [11,12,27,34].

The practical implementation of a risk management system based on these strategies is, however, not straightforward. What are the conditions that must be fulfilled for a situation or activity to be classified as one of the 'risk-based requirements strategy'? When is the knowledge strong enough? When can we ignore the potential for surprise? Knowledge is basically justified beliefs [35], established on the basis of data and information, testing, argumentation, modelling, etc. The knowledge can be more or less strong, but that is based on judgements by someone, and these judgements can also be wrong. How should we take such aspects into account in the risk management? When is the robustness/resilience strategy actually justified?

The present paper aims to contribute to meeting these challenges. We seek to do this by making a distinction between two types of knowledge: 'general knowledge' (GK) and 'specific knowledge' (SK). For the above offshore example, the former type of knowledge relates to over 40 years of experience from the oil and gas industry, while the latter type of knowledge relates to concrete knowledge for the installation considered, for example concerning design features, operational constraints, targets and experience. Using these two types of knowledge, we formulate key features and requirements for the risk management, for example by stating that risk management is the process of making sure that the general knowledge is sufficiently strong to be used for the planning, procedures and requirements for the activity studied, and that we have sufficient specific knowledge and control at all times.

Based on the dichotomy between general knowledge and specific knowledge, as well as recent developments in risk science, the paper also aims to enhance the risk-related decision-making framework presented by ISO 17776 [20]. These developments relate to our understanding of the link between risk, uncertainties and knowledge, and how we can use this to improve risk assessment and management (see e.g. [5,15,36]). For example, conceptual frameworks have been developed, as presented in the new Glossary from the Society for Risk Analysis [35]. According to this glossary, risk associated with an activity, for example an investment or the operation of an offshore installation, can in its most general form be seen as comprising two basic features: i) values at stake: the consequences of the activity with respect to something that humans value and ii) uncertainties [35]. To describe these uncertainties, we are led to considerations of probabilities and knowledge. Probability is a measure for expressing the uncertainties, but it is just a tool – it has limitations. A probability is conditional on some knowledge, and this knowledge could be more or less strong and even erroneous. The Petroleum Safety Authority Norway has recently changed the definition of risk to highlight these two dimensions [31]. The ISO 31000 definition of risk (risk is the effect of uncertainty on objectives) can also be interpreted as a special case of this general formulation of risk.

Different types of risk management systems exist. On a general level, we have systems described in overall standards like ISO 31000 and ISO 17776 [20,21]. More specific systems are presented and discussed in the scientific literature, in textbooks and papers on risk management (e.g. [10,18,28,35]). Over the years, we have seen a gradual development of these, from pure probability-based risk assessment approaches to broader risk-management frameworks, highlighting both risk assessments and robust/resilient strategies. A main driver for this development has been the acknowledgement of the importance of uncertainties and knowledge for the proper understanding, assessment and management of risk.

An important source for this acknowledgment has been the insights developed over the last 20–30 years by the safety science literature (e.g. [14,19,32]). A key point made is that, for complex systems, full control of the risks cannot be achieved. Surprises will occur. If complexity is not fully acknowledged, the result will be blind zones and poor understanding of uncertainty [41].

Another source is the literature on black swans in risk management, which captures similar ideas, linking risk, knowledge and uncertainties [4,38]. It is argued that, if the risk assessment restricts its focus on probabilities, important aspects of risk could be covered or concealed, as the risk characterizations are conditional on some knowledge and this knowledge is associated with uncertainties and risk. Blacks swans are understood as surprises relative to this knowledge, for example so-called unknown knowns (some, but not the current analysts, have the knowledge) [4].

The paper is organized as follows. Firstly, in Section 2, we present a general, practical conceptual framework for risk management, which builds on these ideas and particularly the knowledge distinction referred to above. The aim of the framework is to provide clear guidance on how to think in relation to risk to properly manage it. Section 3 discusses the framework, pointing to both strengths and weaknesses (challenges) of the framework. Finally, Section 4 provides some conclusions. The work is to be considered a conceptual perspective paper, highlighting ideas and argumentation [7]. Examples are used to illustrate the concepts, principles and related discussion. The paper is based on both theoretical insights and extensive experience from practical risk management. More comprehensive cases studies showing in more detail how to implement and use the framework will be presented in coming papers.

2. Risk management framework

Risk management can be seen as all coordinated activities to direct and control an organization with respect to risk [21]. In this section, we present a framework, which gives the basic pillars for what these activities should be, using the ideas outlined in the previous section. These pillars capture:

1) Fundamentals related to the understanding of key concepts like risk, uncertainties and knowledge, and their interrelationship
2) The distinction between general knowledge and specific knowledge
3) A formulation of what risk management seeks to obtain, highlighting both successes and failures, and improvements over time
4) Risk management in different stages of a project

5) Using and controlling assumptions
6) Classifications of threats and risks
7) Decision-making, choice of alternatives and measures

2.1. Fundamental concepts

In this paper, risk is defined and understood in line with the ideas of the Glossary of the Society for Risk Analysis [35], also adopted by the Petroleum Safety Authority Norway, as referred to in the previous section. Risk has two main features: i) values at stake: the consequences C of the activity considered, with respect to something that humans value and ii) uncertainties U (what will these consequences be?). The term 'consequences' here refers to all effects of the activity, including the occurrence of hazardous situations and events A. For short, we write risk as (C,U), and (A,C,U) if we wish to highlight the events A. The C is then interpreted as the consequences of the activity given A. In the following, we will also refer to C as (RS, A, B, C), when we would like to highlight risk sources RS, events A, and barriers B [1]. We can, for example, think of a process plant example, where RS represents maintenance, A is a gas leakage, B the activation of an emergency preparedness system, and C the number of fatalities.

To make judgements about the magnitude or severity of the risk, these two dimensions, i) and ii), need to be assessed. We may choose, for example, to focus on the number of fatalities or the economic loss, and we need a way to measure or characterize the uncertainties. Following SRA [35], risk in its most general form can be described by (C',Q,K), where C' are some specified consequences, Q a measure or description of uncertainties, and K the background knowledge that Q is based on. The consequences C represent the actual consequences of the activity considered, whereas C' are those specified in the risk assessment. If an event A occurs which was not foreseen, it may not be covered by A'.

For Q, we recommend the use of probabilities P (including imprecise or interval probabilities), supplemented with judgements of the strength of the knowledge (SoK) supporting these probabilities [6]. As a concrete example, we can think about risk being described by 'severe leakage occurring' (A), the performance of some defined barriers (B), the number of fatalities (C), and related probabilities with SoK judgements. As mentioned in the introduction section, knowledge K in this setting means justified beliefs [35], established on the basis of data and information, testing, argumentation, modelling, etc. The background knowledge supporting the probabilities always needs to be added to the risk description, as the probabilistic results obtained by the risk assessment are conditional on this knowledge. For short, we refer in the following to a threat, meaning either a risk source RS or an event A.

2.2. The distinction between general knowledge and specific knowledge

Consider a specific activity, for example an offshore installation or a drilling operation. The knowledge K about the consequences C is divided into general knowledge GK and specific knowledge SK. The GK covers all knowledge available for related activities but not the specific one. It also includes knowledge about which specific factors/conditions are important for understanding and managing the risk related to the specific installation or operation of interest. The specific knowledge covers knowledge concerning the specific installation or activity alone.

In addition, we need to clarify whose knowledge we are referring to. We distinguish between three main categories: the analysts' knowledge, the total knowledge available when adding other experts' knowledge, and the decision-makers' knowledge.

Investigations following an incident or accident in an industry, like the petroleum industry, seldom reveal that there was a fundamental lack of knowledge about the relevant phenomena. Rather, the typical situation is that someone knew, but the knowledge was not shared/used in a way that prevented the incident or accident. We speak of unknown knowns: some, but not the relevant analysts or operators, had the knowledge [4]. Unknown unknowns, where nobody had the knowledge, are rare.

2.3. Aims of risk management. A model for risk-related decision-making

We define three states:

S: Successful realization of the activity, for example production as planned or increased production
I: Intermediate state (because of a threat, i.e. a risk source or an event)
F: A serious failure state, for example as a result of a major accident occurring.

Risk management is defined in relation to two possible situations:

i) That S is not achieved
ii) That F occurs.

For i), the key questions to ask are: what are the visions and goals defining S? What are the key instruments to be used to meet these visions and goals? How do we ensure that the system quickly returns to state S if it happens to visit state I; in other words, how do we ensure that the system is able to regain or restore performance (and even improve) in case of changes in the system (due to stressors, disturbances, opportunities), i.e. that the system is resilient? What are the main threats and risks related to not being able to obtain the S state?

For ii), the key questions are: how do we prevent this state F from occurring? What are the key instruments to be used? What are the main threats and risks of F occurring?

At first glance, the difference between i) and ii) may seem minor. However, it matters greatly whether the focus is on accident prevention or on not meeting some business objectives. Some events could lead to long periods of state I occurring, but with minor or no effect on the likelihood of a serious failure state F occurring.

The risk management tasks and responsibilities include:

- Make sure that the relevant actors have sufficiently strong knowledge about the (RS,A,B,C) – what could go wrong (that S is not achieved or F occurs) and why (necessary GK)
- Make sure that the necessary and right measures are in place – and that they are functioning as intended (necessary SK)
- Make sure that the relevant actors have sufficiently strong knowledge (GK + SK) to conclude that they are sufficiently sure that state S will be the normal state and F will not occur.

The general knowledge is the starting point for the risk management. If it is strong and has been reflected in relevant solutions and measures, we can focus on the specific knowledge. If not, the general knowledge needs to be strengthened and/or measures for ensuring that the knowledge is properly reflected in solutions and measures implemented. To evaluate the strength of the general knowledge, the risks related to unknown knowns is a key problem, as discussed in the previous section. Thus, although the general knowledge could be strong, we need to consider who knows what and how well they know/understand it.

The general knowledge provides a frame for understanding the specific knowledge related to the system or activity studied, concerning technical conditions, competences, experiences, training and exercises, planning and preparations, planning processes, etc. The specific knowledge needs to be 'transferred' back to the general knowledge, in order to make a decision on its criticality and to find the required and suitable measures. For example, if the test of a system or component during an operation results in a failure, we need to decide what should be done, by whom and when. We also need to decide what should be done if a test has been delayed/not performed. How long a delay can be

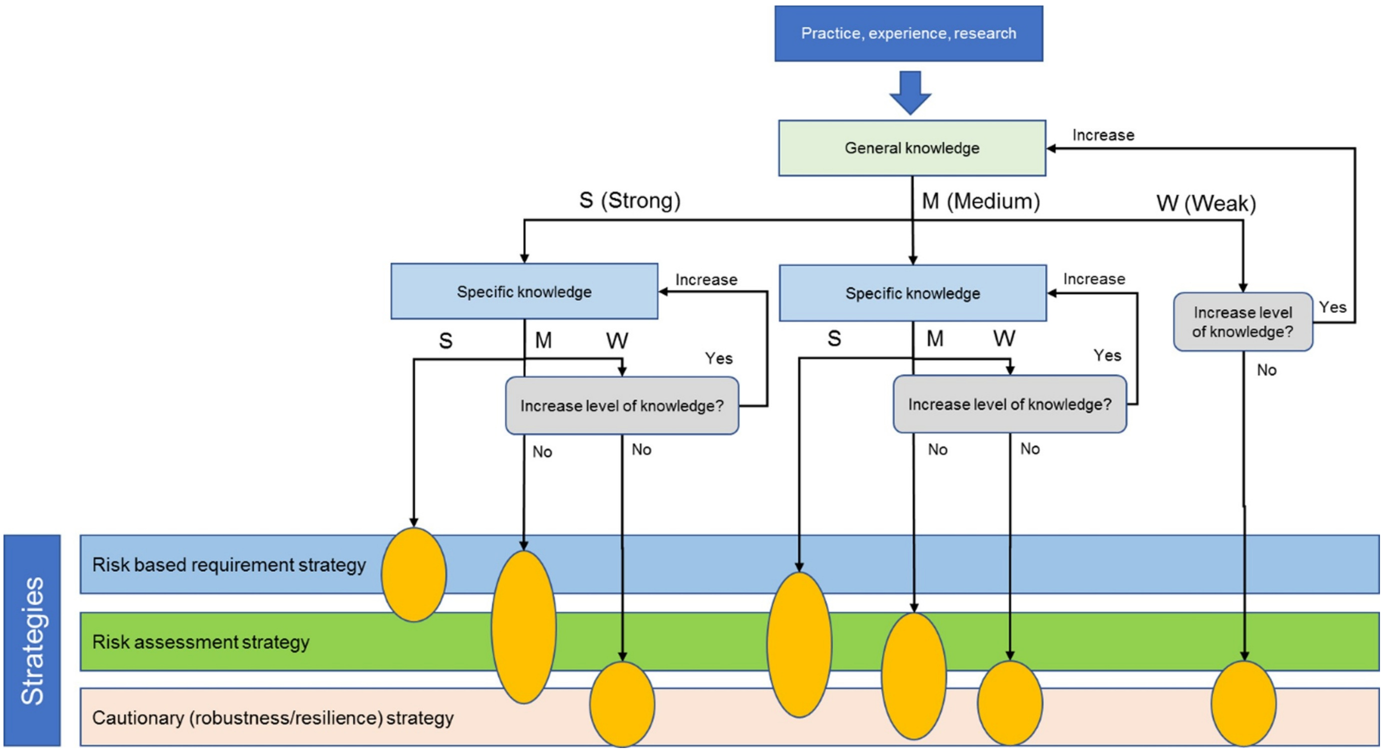

Fig. 1. A model for defining main risk management strategy, based on categorizations of general and specific knowledge.

accepted before it is no longer safe to operate? The general knowledge provides input to this.

Sufficient specific knowledge and control means a judgement that the risk associated with the activity is considered sufficiently low and is acceptable.

In Fig. 1, a model for selection of appropriate risk management strategies is presented, using the concepts of general and specific knowledge. It can be seen as a version of the framework presented by ISO 17776 [20]. A key message from Fig. 1 is that when the general knowledge (GK), as well as the specific knowledge (SK), is strong, risk-based requirement strategy a) can be implemented. If, however, the SK is weak (but the GK still strong), weight needs to be given to robustness/resilience, as the activity considered could have special features and there is a potential for surprises relative to the GK. Using feedback loops, the model allows for differentiations between situations where it is possible to increase the knowledge – for example by performing analysis, testing, modelling, decision-making and the use of assumptions (see Section 2.5) - and where this is not possible. If the GK is weak, a robustness/resilience-based strategy is always needed, as the SK has a poor foundation. If the GK is medium strong, risk assessments will provide useful decision support, expect in cases with weak SK. In the case of weak SK, the risk assessment will have rather limited information value and is therefore not highlighted in the model in Fig. 1.

When faced with a situation where the level of knowledge (GK or SK) is medium or weak, one should always consider the questions: Can, and if yes, should the level of knowledge be increased before a decision on the risk management strategies is made? This is founded on the thesis that increased level of knowledge will provide a better decision basis, and less costly (less conservative) risk management strategies and measures. Aspects to be included in such considerations could be: the timeframe (before the decision(s) has to be made), what can be done (consult with external experts vs. extensive research work needed?) and cost (will the increased knowledge be worth the cost needed to gain it?).

There are several other simplified features in this model. In fact, some types of risk assessments are always conducted. For instance, it is important to identify risks related to assumptions made, and, in the case of large uncertainties, risk assessment is a useful tool to systematize the knowledge available and identify knowledge gaps, although no attempts are made to quantify risk.

The model illustrated in Fig. 1 is to be considered as a conceptual model rather than a fixed process/evaluation, to be performed at for example specific times, with a fixed set-up for how it should be done. The main idea with the figure is to increase the reflection on the level of knowledge (GK and SK), and how the different levels should influence the selection of the risk management strategy/strategies to be used. “Unconscious” approaches or approached based on traditions (“we have always done it like this”) such as: always using the risk assessment strategy, without reflecting on whether the outcome will provide a better/needed decision support, and/or whether the input needed is available (i.e. sufficient level of SK in order to conduct the assessment), is not beneficial to any party. It can be considered a misuse of the decision-makers time and money, and it may jeopardize the importance of doing for example an extensive risk assessment when that is the suitable and best strategy.

2.4. Risk management in different stages of a project

For decisions at the early stages of a development project, the general knowledge provides the basis for the decisions. As the project develops, the specific knowledge becomes more important, and, in the operational stages, when making a decision about the operation of a system, the specific knowledge is central. However, in most situations, the general knowledge is important for placing the observations and measurements of the specific system in context, and the general knowledge provides this context, with its general theories, experiences, practices, etc.; the general knowledge will always provide guidance on how to understand and use the specific knowledge.

For example, at the early stages of an offshore development project, for proven development concepts such as fully integrated topside facilities and subsea tie-back developments, the general knowledge provides the basis for the identification of hazards, accidental events and the risk control measures (barriers) needed. To perform traditional risk assessments, starting by asking what can happen/go wrong, and thereafter continuing to assess why, how often, what will the consequences be, etc., will, for proven development projects, not provide any new knowledge. Thus, the main purpose of performing such assessments in such cases will not be to gain more insight about the risks associated with the concepts but to reproduce it (which could be relevant, in order to give the decision-makers this knowledge).

The general knowledge provides guidance on the need for risk assessments and the type of such assessments, including the methods and models that should be used.

A main strategy for managing the risk through different stages is to use and 'control' assumptions. In the early stages of a development project, the specific knowledge is weak, and assumptions are introduced as discussed in the following section.

2.5. Using and controlling assumptions as a strategy to deal with weak specific knowledge

Consider a case where strong or medium strong general knowledge exists (e.g. fires in buildings). A specific building is to be constructed. The developers want to get the building up as fast as possible, but they do not yet know what the building will contain when it is completed. Whether it is going to be used for housing, partly housing and partly offices/industry or only industry purposes, they do not know.

The building's main load-bearing structure, the divisions between the floors, the construction materials, the firefighting equipment, etc. will to a large extent be governed by what the building is going to be used for (due to, for example, regulatory requirements). So, do the developers have to wait until the building is fully rented out before they can start the building process?

No, they need to make some decisions, and these are often formulated as assumptions, for example that the building is going to be a flexible housing/office building, and that only the lowest floors shall have the possibility to be used for either housing or offices, while the rest of the building is going to be used only for housing.

To choose the combined housing and office concept for the building would most likely eliminate the possibility of allowing future industry activities in the building. This is a risk the decision-makers must take into consideration when they decide on the type of building they want to build.

Using a traditional risk assessment approach, one may argue that details related to the final building, i.e. its combination of flats, offices and/or industry activities, need to be in place in order to conduct a proper hazard identification, risk characterizations and evaluations. In other words, the building needs to be specified in detail before it can be assessed properly. When such detailed specifications cannot be made (due to lack of knowledge), assumptions can be used in order to continue the project. The alternative is to stop or delay the project. Such assumptions can for example relate to the overall features of the building, as discussed above, and, for example, the load capacity of walls, in the case of fires and/or explosions. As modifying, for example, the load-bearing structure or the fire divisions will be very costly (often impossible) after the building is finalized, the choice of assumptions is critical.

Fig. 2 presents a simple model for how to use assumptions in the risk management by considering differences in the level of general and specific knowledge, refining the scheme in Fig. 1.

If the general knowledge is strong but the specific knowledge is medium and weak, the use of assumptions (which will often be decisions that limit the flexibility in the way forward) will allow for a shift towards more weight given to the a) and b) strategies, 'risk-based requirement strategy' and risk assessment strategy, for example from a mainly cautionary approach to a combined risk assessment and a partly cautionary approach, if the general knowledge is strong and the specific knowledge is weak, or from a cautionary/risk assessment approach to a combined 'risk-based requirement strategy', risk assessment and cautionary approach, if the general knowledge is medium and the specific knowledge is medium.

A key feature of this approach, based on assumptions to compensate for lack of specific knowledge, is that the decision-makers ensure that the assumptions are fulfilled (e.g. making sure that industry activities are not allowed in the building in the future, in the building example presented above). There will always be risk related to the assumptions actually being met in practice.

The above analysis shows how the framework reflects time. As an illustrating scenario think about a project where the special knowledge at an early development stage is weak, but a key assumption is made which clarifies the scope and goals of the project. The result is that the uncertainties are reduced and the specific knowledge increased. In another case, the further detailing of the project could lead to the discovery of a technical problem, and consequently reduced specific knowledge. The problem triggers some analysis, modelling and testing, and the specific knowledge is strengthened. Through this process, the generic knowledge could be the same, but we could also think about a situation where the identified problem generates some more fundamental research which then improve the general knowledge.

2.6. Classifications and judgements of the severity of threats and risks

Threats and risks are classified according to three categories: High, Medium and Low. The category 'High' is typically associated with an unacceptable risk, requiring additional measures in order to proceed, whereas 'Low' is typically associated with an acceptable risk, where no additional measures are needed. The 'Medium' category is associated with situations where the risk is acceptable but additional measures should be implemented if possible. Management considerations are needed to decide which measures to implement.

To classify a threat or the risk as High, the following criteria need to be considered (minimum one of these criteria applies):

a) The risk is judged to be high when considering consequences and probability
b) The risk is judged as high, considering the potential for severe consequences and significant uncertainty (relatively weak knowledge)
c) Lack of robustness/resilience
d) Weak general knowledge about (RS, A, B, C)
e) Weak specific knowledge about (RS, A, B, C)
f) Strong general knowledge about undesirable features of (RS, A, B, C)
g) Strong specific knowledge about undesirable features of (RS, A, B, C)

For example, the risk is classified as *High* if a critical failure on the Blowout Preventor (BOP has been revealed through testing, by reference to a), c) and g).

We can also classify the risk as *High* if the BOP has not been tested, with reference to b), c) and e).

In the former example, we argued according to what we know and, in the latter, to what we did not know.

Analogously, we can define criteria for *Low* (all relevant criteria apply):

h) No potential for serious consequences
i) The risk is judged to be low when considering consequences and probability, and supporting knowledge is strong
j) Solid robustness/resilience
k) Strong general knowledge about (RS, A, B, C)
l) Strong specific knowledge about (RS, A, B, C)

Medium applies to all other cases.

To evaluate the strength of the knowledge, we need to address issues such as [6,9,15]:

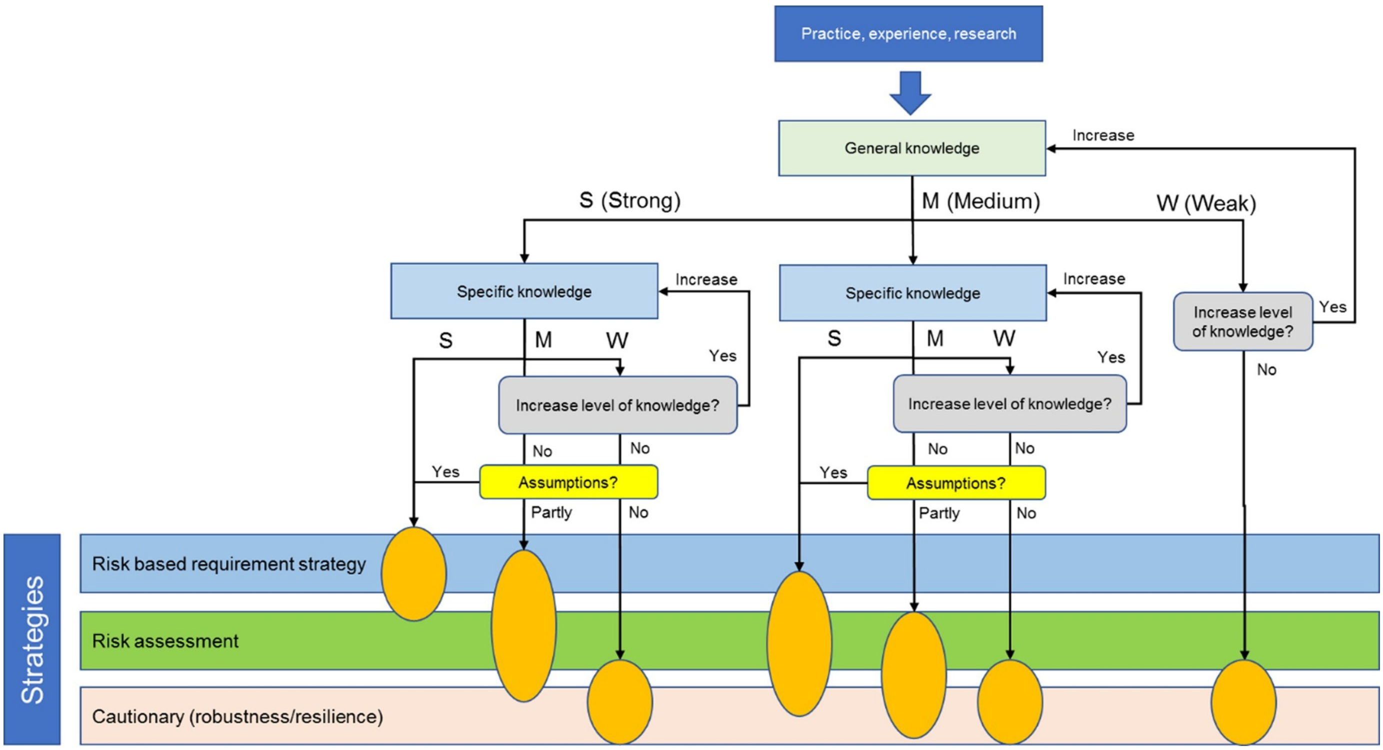

Fig. 2. Model of the use of assumptions in risk management, refining the ideas in Fig. 1.

- The reasonability of assumptions made
- The amount and relevancy of data/information
- The degree of agreement among experts
- The degree to which the phenomena involved are understood and accurate models exist
- The degree to which the knowledge has been thoroughly examined (for example, with respect to unknown knowns).

The last point relates to potential surprise issues like [13]:

- The possibility of unknown knowns (i.e. others, but not the analysis group, have the knowledge). Have special measures been implemented to check for this type of event (for example, the use of an independent review of the analysis)?
- The possibility that events are disregarded because of very low probabilities, although these probabilities are based on critical assumptions. Have special measures been implemented to check for this type of event (for example, signals and warnings influencing the existing knowledge basis)?
- Risk related to deviations from assumptions made (see the coming section)
- Changes in knowledge over time

Based on judgements of such issues, qualitative score systems can be developed (see [6]); see also the so-called NUSAP system (NUSAP: Numeral, Unit, Spread, Assessment, and Pedigree) [16,17,23–25,39,40].

Examples

How to make judgements about risk and use the general knowledge (GK) and specific knowledge (SK) depends on the situation considered. We consider three examples to illustrate this point:

1) A company buys a product from a manufacturer. There is no need to perform a probabilistic analysis and calculate risk metrics, as the company has well-documented strong GK in relation to the performance of the product, established on the basis of work done by the manufacturer, as well as operational experience with this type of product. The manufacturer has conducted a risk assessment of the product and implemented risk-reducing measures, and reference can also be made to practical use of the product, demonstrating its high reliability. The company has strong knowledge expressing that the reliability is high. However, there is always a potential for surprises, and the risk related to such surprises need to be addressed, through for example checks of key assumptions made.
2) In the above example, the manufacturer, on the other hand, may find it useful to use a probabilistic analysis to characterize the reliability and risks. Uncertainties and the strength of knowledge supporting this analysis need to be reflected. Bayesian analysis can provide a suitable framework for updating the probabilities, given new information.
3) In this final example, consider a situation where a product is used in a completely new context. The GK for the product may be strong, but it is not relevant for this new context. Hence, we are led to SK judgements. An analysis of what characterizes this new context compared to the standard one is conducted. This analysis may, for example, reveal that the new context involves a higher exposure level from a specific risk source. Measures will then be considered to meet this risk factor. Probabilistic analysis is not recommended, as the knowledge supporting the probabilities is so weak. However, qualitative probability judgements or interval probabilities could be useful to communicate experts' degree of beliefs: is this a likely event or not? Is it higher than 50%? Negligible probability?

These examples show that different situations call for different weights on the main components of a performance-uncertainty characterization. Compared to common risk assessment practice, the proposed framework has a stronger focus on the knowledge dimension.

2.7. Decision-making, choice of alternatives and measures

When facing many potential solutions and measures, we need to evaluate these. A key aspect to consider in relation to this is the manageability of a risk event (for example 'low oil price') or measures meeting this risk event, which is a concept that relates to how difficult it is to reduce the risk and depends on technical feasibility, time aspects, costs, etc. [6]. It is often informative to present a matrix with, for example, three categories (high, medium, low), based on manageability, on the one axis, and effect on risk, on the other. The latter axis relates to how large an effect the measures have on risk: consequences, probability and strength of knowledge; or how large an effect the risk event has on risk. Measures which score relatively highly on manageability and risk are clear candidates for implementation. Such matrices need to be used with care. For example, if the risk event considered for an oil company is 'low oil price', it may, at first glance, be tempting to express the manageability as low, leading to the conclusion that no measures are required. However, the risk is not only related to the price changes, equally important are measures implemented for meeting a low oil price, for example reducing operational expenditure. This risk event could therefore be classified as relatively high as regards manageability, and the main focus is on measures that could reduce the negative effects for the company if such an event should occur. In general, the following risk-reduction process is recommended [6]:

1 Implement measures in the case of High risks, as defined above.
2 If the costs are small, implement the measure if it is considered to have a positive effect in relation to risk and performance in a wide sense (Medium or even Low risk).
3 If the costs are significant, make an assessment of all relevant pros and cons of the measure. If the expected present value (or corresponding indices) can be meaningfully calculated, implement the measure if this value is positive.
4 Also consider implementing the measure if it generates a considerable positive effect on the risk and/or other conditions, for example:

- Reducing uncertainty, strengthening knowledge
- Strengthening the robustness in the case of hazards/threats, strengthening the resilience

The approach aims to balance the need for cost-effectiveness and being cautious in the face of threats with potential negative consequences.

2.8. An illustrating example

Consider a house development project during spring and summer, with an issue of radon risk. The owner has currently not been able to make proper radon measurements in the house as it needs to be measured in the winter. Based on a radon map, the owner observes that there are high radon concentrations in the area where the house is located. The general knowledge concerning radon risk is strong and the risk is judged high according to the scheme presented in Section 2.6, for example by referring to criterion f). The general knowledge recommends some protection barriers to be installed. The specific knowledge is judged to be rather weak, and to strengthen this knowledge the owner needs to defer the project some 6–9 months to make detailed measurements. The results of such measurements could potentially show that the radon exposure for the house is small, and no special protection is required. However, a delay of 6–9 is considered too costly for the owner, and the conclusion is that the protection barriers are installed on the basis of the general knowledge, in line with Fig. 1 which points to the cautionary principle and the implementation of robust/resilient measures.

3. Discussion

The distinction between general knowledge (GK) and specific knowledge (SK) to assess risk leads to a new type of approach. We find, however, similar ideas in the Bayesian method, where a prior distribution and the underlying probability model are established on the basis of generic knowledge and combined with observations and measurements representing specific knowledge, to produce an integrated distribution, reflecting the total knowledge. The Bayesian method has a strong theoretical foundation and can be useful in many cases to systematically update knowledge. The approach presented in Section 2 differs, however, from the Bayesian approach in many ways. First, it is a qualitative approach, not a quantitative approach as the Bayesian one. The strengths of quantitative analysis are well known, as are the weaknesses of qualitative studies. Probabilistic quantification and the use of Bayes' formula make it possible to systematically combine knowledge about unknown quantities and observations (measurements). Using qualitative approaches, the stringency of the probability theory is lost, and it is not possible to ensure the same level of coherency in judgements. However, quantification also has strong limitations. To use a probability to represent uncertainty means that important aspects of risk are not reflected: aspects that are important for being able to properly evaluate the significance of the risk and make the right decisions. The argumentation for this assertion is well known (see, for example, [3,15]) but, to quickly recap, a probability representing or expressing uncertainty is conditional on some knowledge, and this knowledge could be more or less strong and even erroneous. For the proper use of the risk assessment, it is not enough to only report the probability numbers, as these reflect 'conditional risk'. The assessment may, for example, be based on a belief that the system studied has some specified properties, but in real life it could in fact have others, and this can lead to negative surprises (see examples in [6]). The use of imprecise probability or interval probabilities [15] makes the transformation from knowledge to the probabilities more objective but does not eliminate the issue of the underlying knowledge being weak or wrong. Such intervals will also reduce the information value of the assessments, as the intervals seek to avoid incorporating analysts' judgements.

A probabilistic quantitative risk assessment produces a risk description (C',P|K) using the notation introduced in Section 2.1. The method presented in this paper describes risk using the triplet (C',Q,K). Thus, the knowledge supporting the uncertainty description Q is a part of the risk description. In (C',P|K), the probabilistic metrics are to be seen as conditional on some knowledge, whereas, in (C',Q,K), the knowledge is subject to scrutiny. The aim is not only to describe the strength of this knowledge but also to strengthen it when the knowledge is weak. An objective transformation of the knowledge from the evidence to the risk description is attractive and has a value, but the price paid is that the assessment becomes rather uninformative for the decision-makers if the evidence is not strong. We may, for example, have some signals indicating a failure in the system, but if we are not able to understand these signals they are of little importance. The proposed risk assessment method presented in Section 2 seeks to stimulate processes to strengthen the knowledge generation, where the knowledge is judged as weak, and also to reveal knowledge gaps, in particular unknown knowns. If the risk description at some stage of the analysis is (C',Q,K), the study at a later time could be (C',Q,K_1), where K_1 is stronger than K. The assessment may, for example, have revealed that an assumption used is questionable and should be replaced by a more nuanced analysis, adding new knowledge to the table. The split into general knowledge and specific knowledge can be useful in this respect. For example, it is important to distinguish between what are general knowledge gaps and what are specific knowledge gaps. The former case may trigger some generic research projects, whereas the latter case could lead to broader involvement of operational personnel in the risk assessment.

The subjectivity of the analysis must be acknowledged. The analysts may consider the knowledge to be strong, but they could be wrong. It is about beliefs and justifications of these beliefs. We know that scientists and analysts often have strong confidence in relation to their own knowledge, but history has shown that incorrect conclusions are made. The limitations of the method need to be taken into account in the risk management. These problems particularly apply to quantitative analysis but are also an issue when it comes to qualitative studies. The approach proposed in Section 2 seeks to meet this challenge through its checklists and reviews, but it is still based on judgements which could be wrong. The way of dealing with this challenge is to recognize the importance of robustness and resilience-based strategies. Such strategies constitute a main category of risk measures justified by the imperfection of the risk assessments, whether they are quantitative, qualitative or a mixture. All industries have built in some degree of robustness and resilience, but the risk assessment rationality is often seen as the superior one; see, for example, discussions in O'Brien [29], Pasman et al. [30] and Aven [2]. However, in the face of uncertainties, there is theoretical strong justification of the robustness and resilience-based strategies; see, for example, Renn [33] and Aven [8].

A main challenge with the approach presented in Section 2 is that it is based on qualitative judgements regarding what is high (medium, low) risk. Different analyst groups could come to different conclusions about the magnitude of the risk, as there is no clearly defined scale. However, the idea that such a scale exists can be disputed, as argued for in Section 2.1 (see also [15]) and, to be able to include all relevant risk aspects, we are faced with a dilemma. We either present a rather narrow risk description, based on risk numbers as the basis for the decision-making, which does not incorporate important aspects of risk, or we use a qualitative approach, which lacks scale precision but is more complete. Also, metrics based on quantification can be used to support the qualitative approach, but these metrics are not viewed as final results but input to the overall qualitative judgements to be made. To make a judgement that, for example, the risk is 'High', criteria as outlined in Section 2.6 are introduced. The judgement does not automatically prescribe a decision to act to reduce risk; considerations are needed to check for the feasibility of measures, costs, and other concerns, but commonly the classification 'High' leads to conclusions about unacceptable risk and the need for risk-reducing measures. This presumes, however, that the 'perspective' and 'references' of the analysis are clarified. For example, the perspective or reference for the conclusions could be overall technical criteria in the company and the industry, regulations, etc. In other cases, the study team includes managers with proper authority, and the conclusions could then also be influenced by the value judgements of these managers. Think of the planning of a technical operation on an offshore installation. Here, the decision-maker could be a part of the analysis team, and conclusions can be made about risk being too high and unacceptable, as a part of the assessment.

As mentioned by one of the reviewers of the original version of the present paper, it could be informative to use two independent analysis teams to confront the subjectivity of the approach. However, in practice there are always resource limitations, and it can be argued that this analysis framework is not more subjective than many other risk assessment methods. The key is to be open and clear about what the approach actually gives and how it should be used in the decision-making process. Subjective judgments can also be useful, and as highlighted above, the basic idea of the approach recommended is to build on robustness and resilience to deal with the limitations of the formal approaches, including subjectivity.

The approach presented is based on the split between generic knowledge and specific knowledge, but also about knowledge and lack of knowledge. Uncertainty is about lack of knowledge, and the risk concept highlights uncertainties. However, the traditional risk assessments often focus on the available knowledge. The probabilities assessed reflect the analysts' knowledge, not the lack of knowledge. When making judgements about the strength of knowledge, we also focus mainly on the existing knowledge. Lack of knowledge is more the issue when addressing potential surprises and the unforeseen. The presented approach also aims to give weight to this risk aspect. It represents a challenge, as it extends beyond the analysis as such, and it has traditionally not been given much attention in risk assessments. Recently, it has, however, been more emphasized − references to black swan types of events are relatively common today. How to best deal with this type of risk is not straightforward, as the issue cannot be solved by calculations. The presented approach in Section 2 highlights some tools in this regard, but there are many others that could be useful in relation to the approach; see, for example, Aven [4] and the references therein.

4. Conclusions

Using the dichotomy between general and specific knowledge, in this paper, risk management is viewed as the process of making sure that the general knowledge is sufficiently strong to be used for the planning, procedures and requirements of the activity studied, and that we have sufficient specific knowledge and control at all times. Based on this idea, in this paper, we present a framework that shows how risk can be evaluated and managed, giving due attention to potential surprises and the unforeseen. The framework builds on current risk science, which acknowledges the importance of using both risk assessment and robustness/resilience-based strategies to properly handle risk. In contrast to many other risk management frameworks, it is mainly qualitative, and it does not make a sharp distinction between assessment and risk descriptions, on the one hand, and the handling of the risk, on the other. The main focus is on the actions and decisions to be made, not on the risk characterizations as such. For the purpose of making the right decisions, detailed and nuanced risk descriptions are not always needed (refer to, for example, Lambert et al. [26] and Karvetski and Lambert [22]). The key is to identify the measures that are needed to make the activity safe and the risk tolerable/acceptable. Risk quantification can be useful in many cases to systematically assess risk-related information and knowledge, but qualitative judgements are always needed to be able to properly consider all aspects of risk of importance for the decision-makers. Qualitative judgements have their limitations, but they can still be useful. The challenge is to establish some suitable guidance on how to conduct these qualitative risk analyses. The present paper's main aim has been to provide such guidance, using the concept of general and specific knowledge.

Acknowledgments

The authors are grateful to two anonymous reviewers for their useful comments and suggestions to the original version of this paper. For Terje Aven this research was performed as part of the project Safety 4.0 which is funded by the Research Council of Norway under the PETROMAKS 2 programme, project number 281877.

References

[1] Amundrud Ø, Aven T, Flage R. How the definition of security risk can be made compatible with safety definitions. Proc Inst Mech Eng Part O 2017. Open Access.
[2] Aven T. Selective critique of risk assessments with recommendations for improving methodology and practice. Reliab Eng Syst Saf 2011;96:509–14.
[3] Aven T. Risk, surprises and black swans. New York: Routledge; 2014.
[4] Aven T. Implications of black swans to the foundations and practice of risk assessment and management. Reliab Eng Syst Saf 2015;134:83–91. Open Access.
[5] Aven T. Risk assessment and risk management: review of recent advances on their foundation. Eur J Oper Res 2016;25:1–13. Open Access.
[6] Aven T. Improving risk characterisations in practical situations by highlighting knowledge aspects, with applications to risk matrices. Reliab Eng Syst Saf 2017;167:42–8.
[7] Aven T. Reflections on the use of conceptual research in risk analysis. Risk Anal 2018;38(11):2415–23.
[8] Aven T. The call for a shift from risk to resilience: what does it mean? Risk Anal 2019;39(6):1196–203.
[9] Aven T, Flage R. Risk assessment with broad uncertainty and knowledge characterisations: an illustrating case study. In: Aven T, Zio E, editors. Knowledge in risk assessments. NY: Wiley; 2018.
[10] Aven T, Renn O. Risk management and risk governance. Springer Verlag; 2010.
[11] Aven T, Renn O. Improving government policy on risk: eight key principles. Reliab Eng Syst Saf 2018;176:230–41.
[12] Bang P, Thuestad O. Government-enforced self-regulation: the Norwegian case. In: Lindøe P, Baram M, Renn O, editors. Risk governance of offshore oil and gas

operations. Cambridge USA: Cambridge University Press; 2014.
[13] Bjerga T, Aven T. Some perspectives on risk management – a security case study from the oil and gas industry. J Risk Reliab 2016;230(5):512–20.
[14] Dekker S. Drift into failure. Kindle ed. Ashgate Publishing; 2012.
[15] Flage R, Aven T, Baraldi P, Zio E. Concerns, challenges and directions of development for the issue of representing uncertainty in risk assessment. Risk Anal 2014;34(7):1196–207.
[16] Funtowicz SO, Ravetz JR. Uncertainty and quality in science for policy. Dordrecht: Kluwer Academic Publishers; 1990.
[17] Funtowicz SO, Ravetz JR. Science for the post-normal age. Futures 1993;25:735–55.
[18] Haimes YY. Risk modeling, assessment, and management. 4th ed. New York: Wiley; 2015.
[19] Hollnagel E, Woods DD, Leveson N. Resilience engineering. Kindle ed. Ashgate Publishing; 2012.
[20] ISO (2016) 17776. Petroleum and natural gas industries − offshore production installations − major accident hazard management during the design of new installations.
[21] ISO (2018) Risk management guidelines. ISO/FDIS 31000:2017(E).
[22] Karvetski CW, Lambert JH. Evaluating deep uncertainties in strategic priority-setting with an application to facility energy investments. Syst Eng 2012;15(4):483–93.
[23] Kloprogge P, van der Sluijs J, Petersen A. A method for the analysis of assumptions in assessments. Bilthoven, The Netherlands: Netherlands Environmental Assessment Agency (MNP); 2005.
[24] Kloprogge P, van der Sluijs JP, Petersen AC. A method for the analysis of assumptions in model-based environmental assessments. Environ Model Softw 2011;26:289–301.
[25] Laes E, Meskens G, van der Sluijs JP. On the contribution of external cost calculations to energy system governance: the case of a potential large-scale nuclear accident. Energy Policy 2011;39:5664–73.
[26] Lambert JH, Karvetski CW, Spencer DK, Sotirin BJ, Liberi DM, Zaghloul HH, Koogler JB, Hunter SL, Goran WD, Ditmer RD, Linkov I. Prioritizing infrastructure investments in Afghanistan with multiagency stakeholders and deep uncertainty of emergent conditions. ASCE J Infrastruct Syst 2012;18(2):155–66.
[27] Lindøe P, Engen OA. Offshore safety regimes – a contested terrain. In: Nordquist M, More JN, Chircop A, Long R, editors. The regulation of continental shelf development. Rethinking international standards. Martinus Nijhoff Publishers; 2013.
[28] Meyer T, Reniers G. Engineering risk management. Berlin: De Gruyter Graduate; 2013.
[29] O'Brien M. Making better environmental decisions. Cambridge: The MIT Press; 2000.
[30] Pasman HJ, Rogers WJ, Mannan MS. Risk assessment: what is it worth? Shall we just do away with it, or can it do a better job? Saf Sci 2017;99(B):140–55.
[31] PSA-N (2019) Petroleum safety authority Norway. http://www.ptil.no/framework/category408.html#p11. [Accessed 23 January 2019].
[32] Rasmussen J. Risk management in a dynamic society: a modelling problem. Saf Sci 1997;27(2/3):183–213.
[33] Renn O. Risk governance. Coping with uncertainty in a complex world. London: Earthscan; 2008.
[34] Rosness R, Forseth U. Boxing and dancing: tripartite collaboration as an integral part of a regulatory regime. In: Lindøe P, Baram M, Renn O, editors. Risk governance of offshore oil and gas operations. Cambridge MA: Cambridge University Press; 2014.
[35] SRA (2015) Glossary Society for Risk Analysis, www.sra.org/resources. [Accessed 7 January 2019].
[36] SRA. Foundations of risk analysis 2015 Discussion note. http://sra.org/sites/default/files/pdf/FoundationsMay7-2015-sent-x.pdf. [Accessed 7 January 2019].
[37] SRA (2017) Risk analysis: Fundamental principles, www.sra.org/resources. [Accessed 7 January 2019].
[38] Taleb NN. The black Swan: the impact of the highly improbable. London: Penguin; 2007.
[39] van der Sluijs J, Craye M, Futowicz S, Kloprogge P, Ravetz J, Risbey J. Combining quantitative and qualitative measures of uncertainty in model-based environmental assessment. Risk Anal 2005;25(2):481–92.
[40] van der Sluijs J, Craye M, Funtowicz S, Kloprogge P, Ravetz J, Risbey J. Experiences with the NUSAP system for multidimensional uncertainty assessment in model based foresight studies. Water Sci Technol 2005;52(6):133–44.
[41] Årstad I, Aven T. Managing major accident risk: concerns about complacency and complexity in practice. Saf Sci 2017;91:114–21.