Abrahamsen Eirik Bjorheim

Aven Terje
University of Stavanger, Stavanger, Norway

Iversen Rune Sæbøe
Gassco AS, Haugesund, Norway

An integrated framework for safety management and uncertainty management in petroleum operations

Keywords

safety management, uncertainty management, petroleum operations

Abstract

In petroleum operations, the safety management and the uncertainty management have traditionally been completely separated functions. The two disciplines are to large extent based on different scientific pillars and it has been difficult to obtain an integrated approach. However, the recent introduction of risk perspectives highlighting the uncertainty component of risk has provided an improved basis for development of such an approach. By seeing risk as the two-dimensional concept covering events and consequences on the one hand side and uncertainties on the other, the content and boundaries of risk assessments are changed. The gap between the two disciplines can to large extent be bridged. The purpose of the present paper is to present and discuss an integrated framework for these disciplines and traditions, based on this risk perspective. An example is included to show the practical implications of the framework.

1. Introduction

In petroleum operations, the safety management and the uncertainty management have traditionally been completely separated functions. In the uncertainty management attention is usually given to technical attributes, such as reservoir conditions (reservoir volume, reservoir compositions, sand production, changes in well stream, etc.), drilling conditions (technology, maintenance, etc.), design conditions (technology, weight, etc.) and operational conditions (production assurance, modifications, etc.). Attributes related to safety, and in particular low-probability events with a potential of severe consequences, are normally not considered in uncertainty management. Such attributes are addressed by the safety management.

For many types of decision problems, both management functions provide important decision support. An example is given in Section 3. However, the two functions are to large extent based on different scientific pillars and it has been difficult to integrate the two functions to establish an overall, unified risk characterisation. The safety discipline typically produces frequency estimates of specific hazardous events, such as leakages causing fatalities [11], whereas the uncertainty discipline produces prediction intervals based on probability distribution quantiles, in addition to mean values. Furthermore, the safety discipline has a focus on risk acceptance criteria (limits of acceptable or tolerable risk), whereas the uncertainty discipline make top-10 and similar lists to rank the most critical uncertainty aspects. Why should the format of the risk description be that different? To improve the decision basis a common platform should be established that can give a unified set-up for dealing with risks and uncertainties. There is no reason why the uncertainty management and the safety management functions should have different perspectives on how to think when approaching risk and uncertainties, when the basic problem is the same – express and characterise risk and uncertainties.

In this paper we show that it is possible to bridge the gap between the two traditions and integrate them

into a common framework. The basic pillar of this framework is a risk perspective comprising the two dimensions: a) events and consequences and b) associated uncertainties (will the events occur, and what will the consequences be) [1], [2]. A key point is that uncertainty is the main feature of risk, and not probability and expected values. A probability is a tool used to express uncertainties, but it is not a "perfect tool". The probabilities and expected values could camouflage uncertainties, e.g. [2], [7], [9]. The assigned probabilities are conditioned on a number of assumptions and suppositions. They depend on the background knowledge. Uncertainties are often hidden in the background knowledge, and restricting attention to the assigned probabilities could camouflage factors that could produce surprising outcomes. By jumping directly into probabilities, important uncertainty aspects are easily truncated, meaning that potential surprises could be left unconsidered. We find also similar ideas underpinning approaches such as the risk governance framework [8] and the risk framework used by the UK Cabinet Office [4].
The framework is introduced in Section 2. It has been a main goal of this paper to show the practical implications of the framework, and an application example is presented and discussed in Section 3. Then in Section 4 we show how the results from the integrated framework can be presented to the decision-makers. Finally, in Section 5 we draw some conclusions.

2. An integrated framework for safety and uncertainty management

The basis for the integrated framework is the risk perspective introduced in the previous section. We formalise this by referring to risk as (A,C,U), where A denotes the events (often referred to as the initiating events), C the consequences of these events, and U the associated uncertainties U.
We may rephrase this definition by saying that risk associated with an activity is to be understood as [3]:
Risk is uncertainty about and severity of the consequences (or outcomes) of an activity with respect to something that humans value.
Severity refers to intensity, size, extension, scope and other potential measures of magnitude, and affects something that humans value (lives, the environment, money, etc.). Losses and gains, for example expressed by money or the number of fatalities, are ways of defining the severity of the consequences. It is important to note that the uncertainties relate to the events and consequences – the severity is just a way of characterising the consequences. The main features of this definition are illustrated in *Figure 1*.

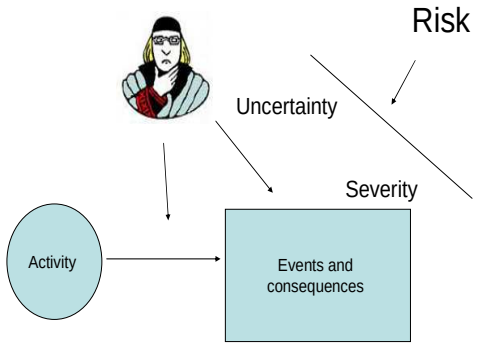

Figure 1. Illustration of the risk definition given in [1], [2], [3].

This perspective of risk acknowledges that risk cannot be adequately described and evaluated by reference to probabilities and expected values only. There is a need for seeing beyond these values. Computed probabilities and expected values are not objective quantities, but subjective assignments conditioned on the background information. Assumptions and suppositions are an important part of the background information. Hence we may characterise risk by (A, C, U, P, K), where P is the assigned probabilities and K the knowledge and background information the analysis is based on. Often we add a prediction of C, C*, in this description. The aim of safety management and uncertainty management based on this perspective on risk is to establish a risk picture covering all relevant dimensions of (A, C, C*, U, P, K).
In general, the risk picture should highlight the following aspects, in addition to presenting probabilities and expected values: 1) uncertainties in phenomena and processes and 2) manageability factors.
It is an aim to identify factors that could lead to consequences C far from the expected consequences EC. A system for characterising the associated uncertainties are outlined in [10]. This system reflects features such as the current knowledge and understanding about the underlying phenomena and the systems being studied, the complexity of technology, the level of predictability, the experts' competence, and the vulnerability of the system.
The level of manageability is related to the potential the organisation has to reduce risk and obtain desirable outcomes seen in relation to other concerns, in particular cost. Expected values and probabilities provide predictions for the future, but some risks are more manageable than others, meaning that the potential for reducing the risk is larger for some risks compared to others. By proper management, we seek to obtain desirable outcomes.

3. Case: Operation and design of flare & HIPPS systems

The flare & HIPPS systems represent an important part of the safety system on a petroleum plant. During different kind of pressure build-up and blow-down scenarios the flare system shall be able to release hydrocarbons in a safe manner, to avoid equipment rupture with subsequent fire and explosions. It is vital that these systems have a robust design, since they represent the last barrier if a situation comes out of control and overpressure occurs. If these systems do not have sufficient reliability, severe consequences may occur affecting people, environment, assets, production and reputation.

When existing plants are being expanded, it is important for the company to decide whether or not the flare & HIPPS system should be redesigned, and if it is redesigned what design that should be preferred. It is common today to use a risk based design according to the standards IEC 61508/615011 [5], [6]. By using this risk based approach, the standards themselves do not specify the design. Different design can be used as long as they comply with the company defined risk acceptance criteria.

Suppose that a processing plant is to be expanded with a new processing train. The company decides to perform the flare & HIPPS design based on a risk based approach according to IEC 61508/615011. This standard tells you that the design must satisfy the following requirements:

- yearly probability for overpressure above test pressure shall be less than $1x10^{-5}$
- yearly probability for overpressure above design/code pressure shall be less than 1×10^{-3}

To simplify, we assume that the company's decision problem is to decide whether or not a redesign of the flare & HIPPS system is required.

Following the common practice in safety management, the flare & HIPPS system used today is considered unacceptable and should be redesigned if the assigned probability for overpressure above test pressure exceeds the limit $1x10^{-5}$, or if the assigned probability for overpressure above design/code pressure exceeds the limit $1x10^{-3}$.

The assigned probabilities give useful insight to decision makers, but there is a need for a broader reflection of uncertainties. The point is that the above calculations express conditional probabilities. In mathematical terms this can be written like $P(A|K)$ where A may express the occurrence of overpressure above test pressure and K is the background information and knowledge. The background knowledge covers historical system performance data, system performance characteristics and knowledge about the phenomena in question. Assumptions and presuppositions are an important part of this information and knowledge. The background knowledge can be viewed as frame conditions of the analysis, and the produced probabilities must always be seen in relation to these conditions. A result of this is that a true objective value does not exist. There could be different values, and different analysts could come up with different values depending on the assumptions and presuppositions made. The differences could be very large. Hence uncertainty needs to be considered, beyond the assigned probability numbers.

A method that may be used as a type of uncertainty analysis is to perform an operational hazard and identification analysis (HAZID) early in the project stages, where one reviews how the flare & HIPPS systems are being operated at the plant today, to check compliance with the designers' view of how it should be operated. The HAZID should involve all relevant personnel, including control room operators, shift supervisors, operational and technical responsible engineers and leaders. The HAZID leader should be a skilled independent person, with both operations and specific engineering experience.

The scope of the HAZID may include formal identification processes, operation interviews and documentation reviews related to for example procedures, operating handbooks, and near miss data. After the HAZID is completed a report is issued and the findings/uncertainties may be divided into three categories: Human (M), Technical (T) and Organizational (O) issues.

The findings/uncertainties may be as described below for the three different categories (MTO), and they are factors that the safety analyst may not be aware of in a design situation when calculating the risk numbers and comparing them against the risk acceptance criteria related to the probability for overpressure at the plant.

Human issues (M)

<u>Competence and experiences</u>

The plant may be operated by a young team with limited experiences and/or being managed by inexperienced leaders on the different shifts. This will influence the overall risk picture, especially since the flare & HIPPS is a complicated system and strict procedures must be trained upon and followed.

<u>Living up to procedures</u>

This element has two dimensions:

1. The managers at the plant must make sure that the procedures are updated, and that they on a regular basis during the shift-periods are trained upon. The operation personnel must have easy access to the relevant procedures.
2. What is the Health, Safety and Environment (HSE) culture at the plant. If the HSE culture is bad, there may be a culture for taking short cuts and not operate according to the established routines and procedures. If the designer has assumed that the operation personnel follow strict routines, and are given credit for it in the risk calculations in relation to operator interventions during pressure build up situations, this creates an uncertainty factor.

Operator/simulator training

Especially if the plant is not equipped with inherent safe design, and the operators are a part of the pressure protection system, they need to follow strict routines and follow-up, requiring special training on regular basis.
At first we must expect that the personnel are aware of that they are a part of the overall safety system, and secondly frequent simulator training on different cases must be performed especially where the operators are a part of the safety systems. These conditions are assumed in the quantitative risk assessment but creates an uncertainty factor as in practice they could be satisfied to a varying degree.

Technical issues (T)

Input data in design calculations

It is important that the flare & HIPPS design is based on relevant data from the plant and the different vendors such as valve vendors, and that sensitivity calculations are performed in relation to for example reliability data for the HIPPS valves.
The safety analyst must have a clear understanding of how often the flare system is used for other purposes such as maintenance blowdown, as well as an overview of the flare availability if the Process Shutdown System and HIPPS fails and equipment are released to flare by their respective Process Safety Valves.

Barrier integrity

When having restriction related to the flare system capacity, HIPPS valves are used to block-in the different segments during an undesirable event. If one of the biggest processing units is filling up the flare capacity due to process shutdown and HIPPS failure, it is crucial that the surrounding boundary valves do not leak at the same time. This requirement may lead to higher flow rates entering the flare system, perhaps above design, and may lead to acoustic fatigue, overpressure and rupture. The different barrier valves such as Emergence Safety Valves and HIPPS valves may have an internal leakage due to dirt, tear and wear caused by frequent operation. Problems may also occur on the hydraulic system that operates these valves, such as dirt or bacterial growth. These uncertainty factors are not necessarily taken into account in the design situation.

Updated documentation

If the plant is being operated with a poor documentation system, this represents an uncertainty related to flare & HIPPS operations. Important and imperative documents such as flare & HIPPS operating manual and emergency preparedness documents are not adequately updated in conjunction with projects and studies. The safety analyst performing the risk analysis is probably not aware of the state of the documentation system.

System dynamics

The probabilistic analyses performed to check whether you are within the risk acceptance criteria does not usually include flare system dynamics. During flare situations high gas velocities may occur, and the consequence may be acoustic fatigue in the piping system, leading to possible rupture and gas leakage. The static flare calculations that often are used may not be robust enough, in relation to the actual blowdown scenario.

Flare back pressure

If the Process Shutdown System and HIPPS fails and flaring from Process Safety Valves on large units such as gas export compressors occurs, the flare back pressure increases up to a certain level. At this level some process equipment on other parts of the plant operating at lower pressures, may not be able to release to flare. The flare back pressure is so high that the Process Safety Valve will not be able to open.

Escalation risk

If there is a significant physical distance between the different process systems, one only needs to meet the risk acceptance criteria per system and not per plant.

Using such a philosophy it is easier to meet the risk acceptance criteria. Add all risk contribution would easier lead to exceedance of the risk acceptance criteria limit.
If there is a significant distance between the process systems, the risk of a jet-fire, escalating to the neighbour system may be considered low. However, it is based on theoretical calculations and one assumes that both the passive and active fire protection systems are working. If the flare system is strained, the lack of blow down capacity may give a higher escalation risk. Human errors during the manually performed blow down may also occur, causing an increased risk for escalation.

Stepwise plant development over an extended time period

This type of plant development can lead to a clash of different system characteristics. In this respect this may require that special precautions are made to accommodate a safe release of hydrocarbons, for instance related to blowdown time and flare back pressure.
The different development stages must be adequately aligned design wise, in order to perform safely in an overall flaring perspective.

Organisational issues (O)

Management of change, MOC

During the operating phase at a plant there may occur situations where one needs to operate different systems in another way than it was designed for. The flexibility in the plant with for example crossover piping between units, opens up this possibility. Operating in this "no-design" mode, may influence on segment volumes, blowdown time and flare capacity.
Temporary equipment may be hired in and temporary hooked up in the plant. An example is use of flexible hoses instead of fixed piping. And deviations from existing procedures will be necessary. If the management at the plant does not have a management of change system, that follow up and communicate these periodical changes in operation, this will represent a silent deviation that the safety analyst most probably will miss.

System responsible

The operation crew at the plant operates the flare & HIPPS systems with support from the operation and technical engineers at the plant. But who is the system responsible for the different systems, and who makes sure that the total system works as intended? The flare & HIPPS systems must be looked upon with a common understanding, since they are strongly linked together. The situation today is often that a process engineer at the plant is responsible for the flare system including piping, headers and knock-out drum, and a instrument engineer is responsible for the instrumented HIPPS valves. In such a situation it may be difficult to see the total picture, related to flare & HIPPS challenges and uncertainties.

4. Presentation of results and risk evaluation

From the above example we have seen that the probabilities (P) produced in safety management, should be seen in relation to uncertainties (U). The point is that probability is a tool to express uncertainty. It is however not a perfect tool, and we should not restrict risk to the probabilistic world. The probabilities are conditional on specific background knowledge (K), and they could produce poor predictions. Surprises relative to the assigned probabilities may occur, and by just addressing probabilities such surprises may be overlooked.
In the example above we have seen from the HAZID that there are many uncertainty factors. To better reflect the uncertainties to the management we recommend that the uncertainty factors should be classified within one of the three categories: high, medium or low.
The categorisation process should be based on some guidelines or criteria to ensure consistency. For the above example the following descriptions could serve as a guideline:

Low uncertainty:
All of the following conditions are met:
- The assumptions made in calculations of P are seen as very reasonable
- Much reliable data are available
- There is broad agreement among experts

High uncertainty:
One or more of the following conditions are met:
- The assumptions made in calculations of P represent strong simplifications
- Data are not available, or are unreliable
- There is lack of agreement/consensus among experts

Medium uncertainty:
Conditions between those characterising high and low uncertainty.

Note, that the degree of uncertainty must be seen in relation to the effect/influence the uncertainty has

on the risk indices considered. For example, a high degree of uncertainty combined with high effect/influence on the risk indices considered will lead to a conclusion that the uncertainty factor is high. However, if the degree of uncertainty is high but the risk indices considered are relatively insensitive to changes in the uncertain quantities, then the uncertainty classified in the diagram could be low or medium.

The information about both P and U may be presented to the decision-makers as done in *Table 1*. From *Table 1* we see that several uncertainty factors are classified as high. The uncertainty factor which is considered most important is "living up to procedures".

The assigned yearly probability for overpressure above test pressure is based on the assumption that the procedures are updated on a continuously basis, and that they on a regular basis during the shift-periods are trained upon. This is not necessarily the case. Changes in assumptions related to this factor will have high influence on the assigned yearly probability for overpressure above test pressure. The assigned probability may be considered to be as low as 10^{-4} (which is far above the risk acceptance criterion) even for small changes in the assumptions related to the factor "living up to procedures".

With no attention on the uncertainty dimension, we conclude that the risk is within the risk acceptance criteria. The calculated yearly probability for overpressure above test pressure $P(A_1|K)$ is less than 10^{-5} (and $P(A_2|K)$ is less than 10^{-3}). Taking the uncertainty dimension into account, the risk associated with the flare & HIPPS system used today may be judged unacceptable, even if the calculated probabilities are within the risk acceptance criteria.

Table 1. Presentation of both dimensions P and U.

Probability $P(A_1\|K)$	Uncertainty				
	Uncertainty factors		Uncertainty category		
	Main categories	Sub categories	High	Medium	Low
1×10^{-6}	Human issues (M)	Competence and experiences	x		
		Living up to procedures	x		
		Operator/simulator training		x	
	Technical issues (T)	Input data in design calculations			x
		Barrier integrity	x		
		Updated documentation	x		
		System dynamics	x		
		Flare back pressure	x		
		Escalation risk		x	
		Stepwise plant development over an extended time period		x	
	Organisational issues (O)	Management of change	x		
		System responsible		x	

5. Conclusion

The main purpose of this paper is to present an integrated framework for safety management and uncertainty management in petroleum operations. The basis for the integrated framework is a risk perspective that refers to risk as a two-dimensional concept covering events and consequences on the one hand side and uncertainties on the other. This perspective of risk acknowledges that risk cannot only be adequately described and evaluated by reference to probabilities and expected values, which is common in safety management. There is a need to assess uncertainties beyond expected values and probabilities. An example has been

included to show the practical implications of the framework.

References

[1] Aven, T. (2008). A semi-quantitative approach to risk analysis, as an alternative to QRAs. *Reliability Engineering and System Safety* 93, 76-755.

[2] Aven, T. & Renn, (2009). On risk defined as an event where the outcome is uncertain. *Journal of Risk Research.* To appear.

[3] Cabinet Office. (2002). Risk: improving government's capability to handle risk and uncertainty. Strategy unit report. UK.

[4] IEC 61508. (2000). IEC 61508, Functional safety of electrical/ electronic/ programmable electronic safety-related systems. International Electrotechnical Commision (IEC), Geneva. Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-Related Systems.

[5] IEC 615011. (2003). IEC 61511 Standard. Functional safety - safety instrumented systems for the process industry sector.

[6] Mosleh, A. & Bier, V.M. (1996). Uncertainty about probability: a reconciliation with the subjectivist view. *IEEE Transactions on Systems, Man and Cybernetics* 26: 303-310.

[7] Renn, O. (2005). Risk Governance. White paper no. 1. International Risk Governance Council. Geneva.

[8] Rosa, E.A. (2003). *The logical structure of the social amplification of risk framework (SARF).* Metatheoretical Foundations and Policy Implications. In: N. Pidgeon; R.E. Kasperson and P. Slovic (eds.): The social amplification of risk. Cambridge University Press: Cambridge, UK. pp.47-49.

[9] Sandøy, M., Aven, T. & Ford, D. (2005). On integrating risk perspectives in project management. *Risk Management: an International Journal* 7: 7-21.

[10] Vinnem, J.E. (2007). *Offshore risk assessment: principles, modelling and applications of QRA studies*. 2nd ed. Springer.