Activity-based risk analysis for process plant operations

Stein Haugen[1], Nathaniel John Edwin[2]

Jan Erik Vinnem[1], Olav Brautaset[2], Ole Magnus Nyheim[2], Tiantian Zhu[1], Vegard L. Tuft[2]

[1]Norwegian University of Science and Technology (NTNU), Trondheim, Norway

[2] Safetec, an ABS group company, Trondheim, Norway

Design of complex technical systems with potential for major accidents, such as nuclear power plants, offshore installations and high hazard process facilities, is often supported by quantitative risk analysis (QRA). This contributes to a safe design and optimized use of resources for controlling risk. QRA has been developed and improved over several decades for this purpose. In recent years, the offshore oil and gas industry in Norway has put significant effort into application of QRA also for supporting decisions in day-to-day operations of process plants. Several objectives have driven these attempts. One important objective is to ensure that major accident risk is taken into account in an adequate manner in daily operations. Another important aspect is to provide a basis for more consistent decision-making with respect to risk. However, success in meeting these objectives has been limited so far.

The MIRMAP project (Modelling Instantaneous Risk for Major Accident Prevention) attempts to address this issue in a systematic manner. The starting point has been the types of decisions taken in daily operation, compared to the types of decisions in a design project. Based on this, risk models have been developed which are intended to give up-to-date risk information with limited effort and sufficiently quickly to be available when the decisions are being made. In traditional QRA, focus in the modelling is on technical systems and layout and how the systems may fail. This is relevant in design, when there is scope for making changes to these aspects. However, in operation, the design is fixed and changes in the risk level are driven primarily by the activities taking place and how they may interfere with the technical systems. The risk analysis should therefore also focus on activities. This is a different approach compared to traditional QRAs.

The paper will describe the background to the project and an approach towards modelling the risk. Examples of representative activities are provided and how the risk associated with these are modelled. This includes how activities may influence the barriers in a plant and how activities may interact with each other to increase risk. Illustrative examples are provided and practical implications and feasibility are discussed.

Introduction

Design of complex technical systems with potential for major accidents, such as nuclear power plants, offshore installations and high hazard process facilities, is often supported by quantitative risk analysis (QRA). This contributes to a safe design and more efficient use of resources for controlling risk. Within the nuclear industry, this started in the 1970s, with the publication of the WASH-1400 report (Rasmussen et al., 1975). This was strongly criticised, but still formed the basis for later Probabilistic Risk Assessments (PRA) for nuclear power plants.

The oil and gas industry in Norway was also inspired by the nuclear industry and the first quantitative risk analyses were performed around 1980. The first studies and the first requirements were firmly aimed at supporting the design process. The first requirements from the Norwegian Petroleum Directorate (NPD), now the Petroleum Safety Authority, Norway (PSAN) were called "Guidelines for safety evaluation of platform conceptual design" (NPD, 1981) and specifically pointed to the early design phases of new installations. Over the 35 years since then, the QRA has been extensively developed as a tool for design, with detailed requirements being laid down in the NORSOK standard for Risk and Emergency Preparedness Assessment (NORSOK, 2010).

In recent years, the offshore oil and gas industry in Norway has put significant effort into the use of QRA also for supporting decisions in day-to-day operations of the oil and gas installations. Several objectives have driven these attempts. One important objective is to ensure that major accident risk is taken into account in an adequate manner in daily operations. Another important point is to provide a basis for more consistent decision-making with respect to risk. Success in meeting these objectives has however been somewhat limited so far.

There are several reasons for this, but one key factor is the nature of the risk models used in QRAs. The QRA models the relevant and identified hazardous events and accident scenarios. Any risk model will however be a simplification of the complete set of accident scenarios that can occur. Only a representative set of scenarios are modelled, and normally only explicitly model the factors which are important for the results and for the purpose of the model. This is where the background of the QRAs, as a tool for supporting design, becomes an important limitation.

In a QRA, the layout of the installation, the equipment and all technical systems that influence risk significantly is usually modelled explicitly. Thus, the QRA can guide the design process by pointing out what contributes most to risk, how changes in systems can reduce risk and how we can introduce improvements. However, in the design phase, operational details are not yet fixed and it is typically assumed that they will be some sort of "industry average" and therefore are modelled explicitly only to a limited degree.

An example to illustrate this can be gas leaks. Experience has shown that on the Norwegian Continental Shelf, more than 50% of the gas leaks are related to intervention in the process plant by operations or maintenance personnel (Haugen et al., 2011b);Vinnem and Røed, 2015). However, in the QRA, the frequency of gas leaks is dependent only on the quantity of equipment, not on the number of operations (NORSOK, 2010). The most important factor influencing the frequency of leaks is thus not modelled explicitly, but only taken into account implicitly through the use of historical leak frequencies.

In the design phase, we can argue that the QRA is developed to enable improvements in the design and technical systems, and that the operations is a more or less fixed "framework" for the risk calculation. However, in the operational phase, the situation is the other way round; the operations vary from day to day, while the technical systems and design is a more or less fixed context for the operations. This will also require a different approach to QRA, where the activities taking place in the plant are at the centre of the risk models. This is the starting point for the idea of an activity-based risk analysis.

The MIRMAP project (Modelling Instantaneous Risk for Major Accident Prevention) attempts to address this issue in a systematic manner. As indicated in the title of the project, the focus is on major accidents. The starting point has been the types of decisions taken in daily operation, compared to the types of decisions in a design project. Based on this, risk models have been developed which are intended to give up-to-date risk information with limited effort and sufficiently quickly to be available when the decisions are being made.

Another aspect that also is relevant for the applicability of the QRA is that risk in operation will vary from day to day and even from hour to hour. However, the QRA models average risk over a long period of time, usually for a "typical" year in the operation of the plant. As a basis for developing a design that can be safe "on average" over the lifetime of the installation, this is adequate. However, it will not support operational decision-making.

The main objective of this paper is to describe a method that has been developed to model risk in a more suitable manner for operational decision-making. The rest of the paper is structured as follows. In the next section, an overview over some relevant literature is provided. This is followed by a description of the method in Section 3, and a discussion of some key aspects in Section 4. In Section 5, conclusions are presented.

Background

A structured literature review was performed to study similar methods and applications of real-time risk analysis for decision support in different industries and settings. The review covers both practical and theoretical methods and concepts that are of relevance to real-time risk monitoring.

The concept of a real-time or living risk analysis has its beginnings in the nuclear sector. One such example is Risk Spectrum RiskWatcher (Knochenhauer, 2014) that is a software which uses event and fault trees to model systems and reflect the point-in-time risk based on the current system configuration and other relevant environmental factors. The availability of detailed event and fault tree models from the nuclear Probabilistic Safety Assessments (PSA) makes these models realistic to implement in practice. Another such example is RiskVu from Isograph that falls into this class of risk monitors. The main focus of these tools are plant and barrier condition and not the effect of maintenance activities and combinations of them (Yang et al., 2014). Another limitation of using the PSA models is that no other states or operations than those already included in the probabilistic models are considered by the real-time risk monitor.

The QRA for petroleum facilities model a limited number of parameters and therefore are of restricted relevance for operational decision-making. In light of this, several efforts were made in the oil and gas industry to extend existing QRAs in an attempt to operationalize them. A few of these efforts include the Barrier and Operational Risk Analysis (BORA) project (Aven et al., 2006) that focussed on barrier and operative issues to setup a basic risk influence modelling framework and the Operational Condition Safety (OCS) method (Sklet et al., 2010) that looked at human and organizational factors and their influence on barrier performance. The RiskOMT method (Vinnem et al., 2012) followed and built on the strengths of both the BORA and OCS projects and suggest an approach to risk influence modelling for updating the hydrocarbon leak frequency based on technical, operational and organizational factors. A significant limitation of all of these methods was the complexity and associated work to extend existing QRAs to fit with these approaches and make them relevant for real-time decision support.

Parallel to the BORA, OCS and RiskOMT work, a lot of research effort has also gone into developing indicator sets for major accidents to aid regular monitoring of trends within a system with major accident potential. For example, a review of literature on indicators (Sklet et al., 2010) shows that there is very limited work on approaches to establish and validate indicators. Haugen et al. (2012) provides a generic and systematic method to develop these indicator sets where a risk model links technical, operational and organizational factors and their underlying aspects (e.g. root causes, background factors etc.). These factors are measured (not necessarily completely) through indicators. Although not quantitative, this method provides a valuable foundation on how to systematically approach identification of relevant influencing factors and indicators.

In other related developments, the MARI method (Haugen et al., 2011a), also based on traditional risk models, uses causal chains to illustrate the influence relations between factors and a major accident event. Another method known as Hybrid Causal Logic (Wang, 2007) combines traditional risk analysis tools with Bayesian belief networks. This quantitative method was tested on the aviation industry as a case and Røed et al.(2009) discusses the relevance of the method for offshore risk analysis.

In the aviation sector, the Aviation System Risk Model (ASRM) (Luxhoej and Coit, 2006) combines the use of a human error taxonomy, probabilistic Bayesian Belief Networks and case-based scenarios to assess a relative risk intensity and develop a graphical profile of the updated risk measure in a risk matrix. Scenarios that provide the best risk reduction are selected and subjected to further drill down diagnostics to identify the critical causal factors that define the model performance. In the process industry, Storybuilder (Bellamy et al., 2013) is a tool that uses bow tie structures to graphically depict failures in barrier elements from prior occupational incidents and accidents. This is primarily intended as a systematic instrument to record barrier historical performance and not specifically for proactive use.

In the recent past in the oil and gas industry, a number of operators have developed their own proprietary software-based tools for better status and monitoring across their facilities. These tools promote integrated management of safety critical information (status of barriers, deviations, ongoing activities etc.) for better visualization, data management and reporting. Certain examples are iSee from ConocoPhilips (Etterlid, 2013), Total Risk from Shell UK (Schellings, 2013) etc. These tools provide users an overview of the safety critical activities and deviations at a facility and thereby provides a better decision basis, improved data accessibility and better transfer of experience.

The MIRMAP project attempts to build on some of the work existing in literature, adapt important aspects and overcome some of the limitations from existing methods.

Method description

Developing a practical model to measure transient risks in operations due to ongoing activities comprises of three main phases. Figure 1 illustrates these phases. The first phase involves defining the scope of the risk analysis and therein developing a generic risk model for the process plant or facility concerned. Phase 2 covers calibrating the generic model from phase one and scaling the model for actual use. Important aspects in this phase include identification of data sources and model quantification. Finally, phase 3 looks at providing suitable risk results from the risk model that are relevant decision support. This paper mainly covers the details from Phase 1 and provides a brief reflection on important aspects from Phase 2. This presentation does not cover aspects from Phase 3 – risk reporting and decision support. The examples in this section relate to a typical oil and gas process facility as this has been the focal point of the project and overall method development.

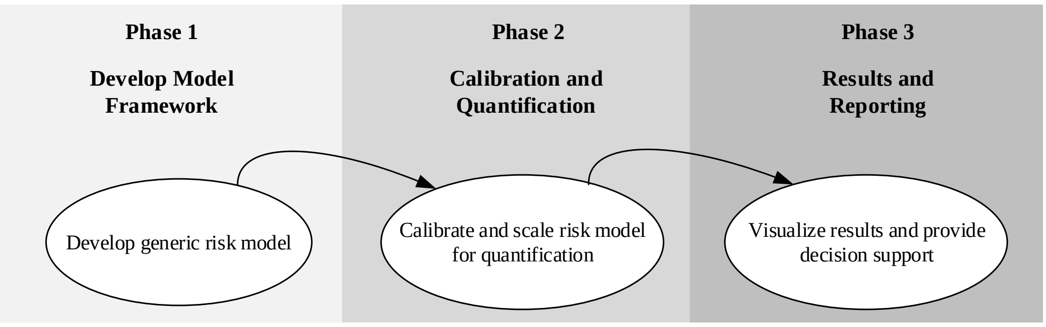
Phase 1
Develop Model Framework
Phase 2
Calibration and Quantification
Phase 3
Results and Reporting
Develop generic risk model
Calibrate and scale risk model for quantification
Visualize results and provide decision support

Figure 1 Outline of the three main phases of the method

Phase 1 – Develop Model Framework

This phase is a systematic seven-step process that first defines the scope of the activity-based risk analysis and lays the foundation for the development of a generic risk model for a process plant. Figure 2 illustrates these seven steps. The result from phase one is a generic activity-based risk model that provides a detailed description of the risk by thoroughly modelling the most significant process hazards, the means of protection and the various relevant factors that can influence or affect these means of protection.

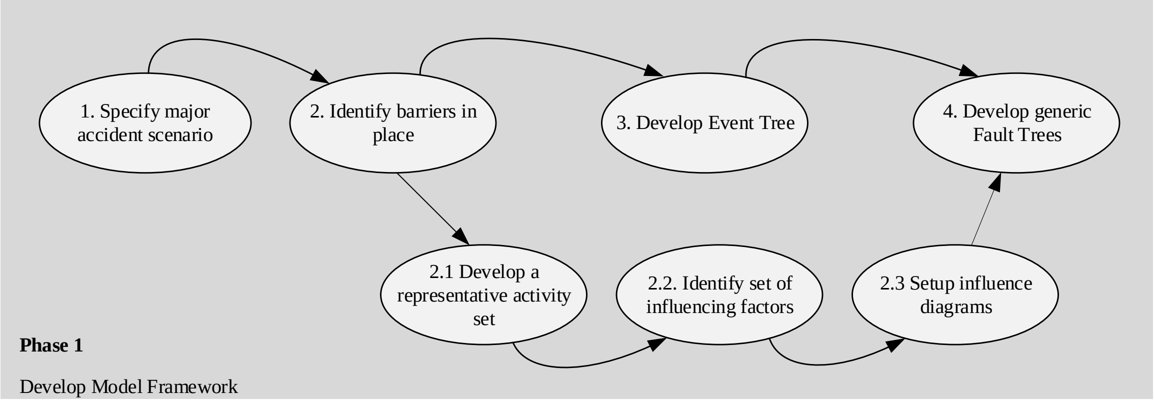
1. Specify major accident scenario
2. Identify barriers in place
3. Develop Event Tree
4. Develop generic Fault Trees
2.1 Develop a representative activity set
2.2. Identify set of influencing factors
2.3 Setup influence diagrams
Phase 1
Develop Model Framework

Figure 2 Illustration of phase 1 - develop model framework

Major accident scenarios and barriers

Steps 1 and 2 define the context and scope for the risk model. The design risk analysis or QRA that quantifies risk from various accident types for a process plant and is of valuable input to this step. For instance, for offshore oil and gas facilities, process leaks, blowouts and ship collisions are the highest contributors to risk (PSAN, 2014). These high-risk contributing scenarios are further analysed to study how daily operational activity affects this risk level. Only risks that vary dynamically with changing operational conditions are suited for real-time monitoring. Here, process leaks followed by ignition and escalation is the major accident scenario that stands out.

Several pre-designed layers of protection or barriers prevent the uncontrolled progression of an accident scenario. PSAN (2013) defines barriers as technical, operational and organizational elements which are intended individually or collectively to reduce possibility for a specific effect, hazard or accident to occur, or which limit its harm/ disadvantages.

Barrier systems form an integral part of each barrier function and comprise of concrete technical, operational or organizational elements that together realize the barrier function in its entirety. All relevant installed and available barriers functions, their constituent barrier systems and corresponding technical, operational and organizational barrier elements are identified and listed.

Figure 3 illustrates the four essential barrier functions for the process-leak event sequence and the associated accident scenario. For example, BF3 "Prevent Ignition" includes barrier systems such as ignition source isolation, control of hot work, ventilation systems etc. among others. Similarly, all the other barrier functions and their related barrier systems are identified for each major accident scenario shortlisted from Step 1.

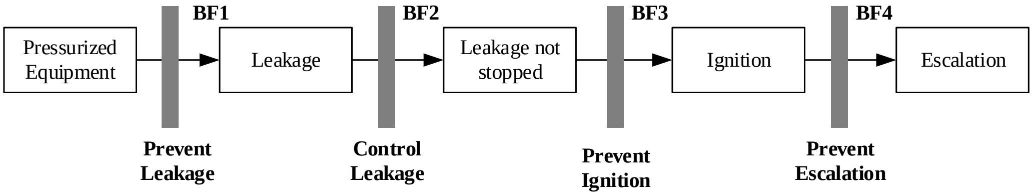

Figure 3 Barrier Functions for the "process leak" accident scenario

Representative activity sets

In daily operations, there is a significant amount of ongoing work. In addition, there are barrier impairments that either exist alongside this work or is caused by the work itself. Any work at a process facility can be broken down into a number of sub-tasks or "activities". For example, consider the recertification of a process safety valve (PSV). This job involves many such sub-tasks or activities such as isolation of the hydrocarbon segment, construction of scaffolding, reinstatement of the hydrocarbon segment etc. Step 2.1 identifies such a representative set sub-tasks or activities that are typical for the process plant at hand.

To simplify this process, it can be said that every activity or sub-task falls into one of two categories- 'Activity A1' that introduces a hazard that may affect the integrity of a barrier, or 'Activity A2' that represents a condition that directly impairs/weakens a barrier system/element. For instance, "disconnection of a gas detector" is an example of a category A2 activity that directly weakens/impairs gas detection. On the other hand, "critical lifting" is an example of a category A1 activity that introduces a hazard that can lead to a process leak due to dropped or swinging loads, an impairment to BF1. Table 1 lists a few further examples of representative activities and the barriers they affect.

In a similar fashion, through a thorough review of each barrier function and its associated systems and elements, all possible activities or conditions that may directly or indirectly represent or lead to an impairment or deviation in the barrier is identified. This exhaustive activity list may also correspond to different types of operational deviations for a process facility, for instance functional tests, ongoing maintenance work, alarms from condition monitoring services, possible notifications from the control system amongst many others.

Table 1 Examples of representative activities from each activity category A1 and A2

Activity Type	Activity Category	Description	Barrier Function Affected			
			BF1	BF2	BF3	BF4
A1. Activities that introduce a hazard that may affect a barrier	Work on hydrocarbon equipment	Includes all tasks related to isolation, execution and reinstatement of a hydrocarbon segment.	X			
	Critical lifting activity	Heavy lifts may damage structural integrity of process equipment through either falling or swinging loads.	X			
	Hot Work (Class A)	Work with equipment and tools that constitute an effective ignition source and may ignite an explosive atmosphere.			X	
	Hot Work (Class B)	Work that constitutes a potential ignition			X	

Activity	Activity Category	Description	Barrier Function Affected			
		source that does not fall under Class A.				
A2. Activities that directly weaken/impair a barrier	Impairment/Deviation on Process Safety Valves (PSVs)	PSVs provide pressure release capability for critical process vessels and equipment	X			
	Impairment/Deviation with Emergency Shutdown Valves (ESDVs)	ESDVs isolate and sectionalize the process in a fast and reliable manner limit the amount of HC released in a leakage.		X		
	Impairment/Deviation on fire detectors (automatic and manual call points)	Automatic fire detection detects fire by type (jet, flame, heat smoke) to initiate suitable action through the control system.				X
	Impairment/deviation in ventilation systems	Ventilation dilutes gas cloud concentration, reduce size of flammable gas clouds among other functions			X	

Influence factors and influence diagrams

Steps 2.2 and 2.3 involve identifying influence factors and understanding the influence relation between the factors and the activity concerned. The term Risk Influencing Factor (RIF) is commonly used in literature related to risk influence modelling. In the current context, a RIF is defined as an aspect of an activity that influences the changing risk level (Øien, 2001). These factors describe the nature and degree to which the RIFs affect the safe execution of the task with respect to major accident risk and thereby the risk level. Table 2 provides examples of RIFs for a selected A1 and A2 activity.

The direction of influence of the various RIFs with the activity and between each other is graphically visualised using influence diagrams. Arcs between the RIFs and the activity visualise this “cause-effect” or “dependence” relationship. Figure 4 illustrates one such simple representation for the activity from Table 2.

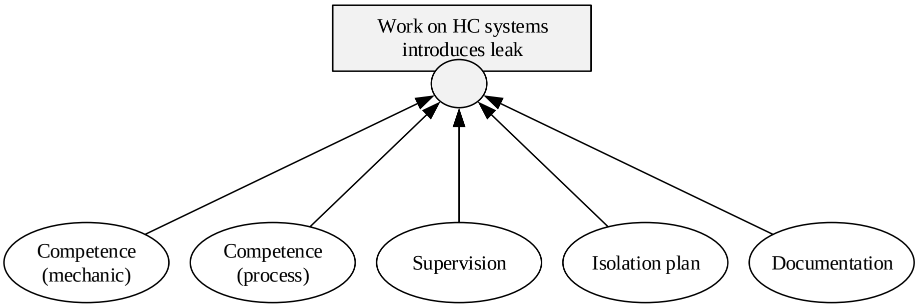

Figure 4 Influence diagrams connect the risk influencing factors and the activity

Table 2 Examples of risk influencing factors

	Type A1 activity	Type A2 activity
	Work on hydrocarbon systems – isolation	*Impairment/ deviation in gas detector(s)*
Influencing Factors	Competence (mechanical)	Redundancy
	Competence (process)	Compensatory measures
	Time pressure	
	Design/ HMI	
	Documentation	
	Isolation plan(s)	

Event Trees

Step 3 builds on the accident scenarios specified earlier in Step 2 to develop event trees for each scenario. Event trees describe the progression of the event sequence to various end consequences. An event tree starts with a hazardous event and splits at different stages in the structure. Each split represents a failure/success situation of pivotal events (functioning or failure of the barriers). The ordering of the pivotal events are made based on the occurrence of events in the accident sequence (refer Figure 3). The occurrence of each pivotal event is conditional on the occurrence of the previous. The progression of the event tree stops at the desired level of end consequence, for instance an escalation scenario. Each end consequence from the event tree is mutually exclusive and does not occur at the same time.

Figure 5 shows an event tree structure for the accident sequence introduced in Figure 3. For ease of interpretation and representation, barrier function 2 splits into sub-functions leak detection, isolation and depressurization. End consequences here are escalation scenarios on a scale of severity from C1 representing a controlled leak to C12 representing a leak followed by uncontrolled explosion.

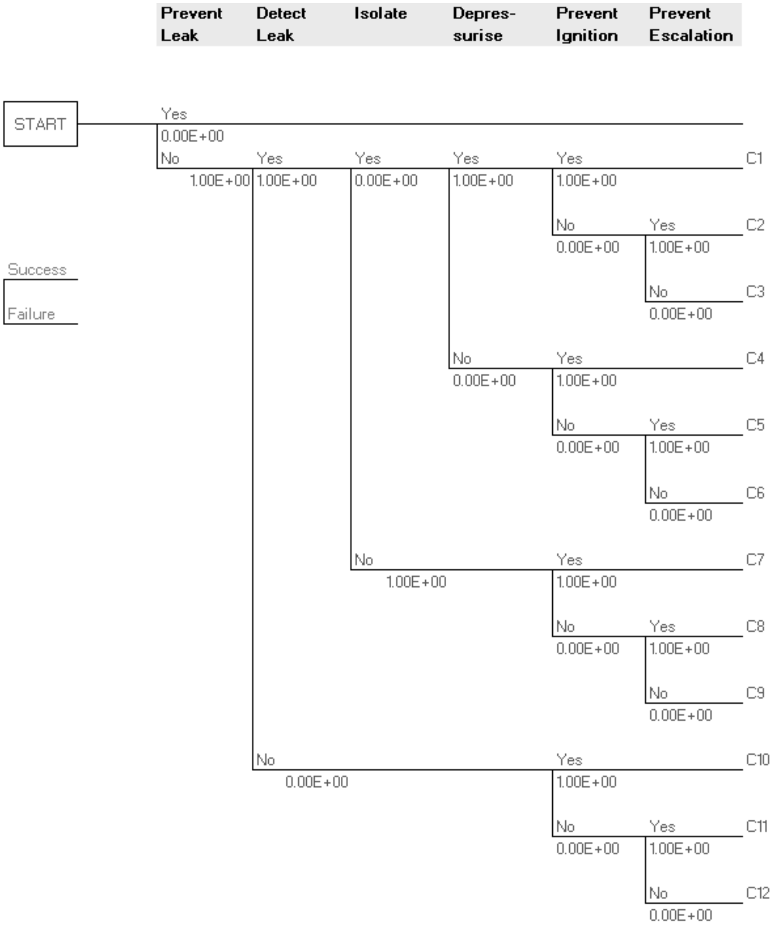

Figure 5 Event Tree Structure

Fault Trees

Development of fault trees for each pivotal event from the event trees covers Step 4. Fault trees are a top-down approach to failure analysis that starts from a potential undesired event and systematically goes through the various ways this happens. In other words, a fault tree models the failure of a barrier function as a function of individual or combined lower level failures or events. In this case, these low-level failures or events correspond to:

A1. Activities that introduce a hazard that may affect the working/performance of the barrier function – e.g. work on hydrocarbon systems, hot work, car traffic, excavation work etc.

A2. Activities that represent a direct barrier deviation/impairment – e.g. removal of emergency shutdown/process shutdown valve, disconnection of gas/fire detectors etc.

B. Issues with technical integrity – e.g. equipment degradation due to age, environmental conditions and other factors

C. Inherent design characteristics or deficiencies – e.g. limitations with regard to firewater capacity, limitations with coverage areas of gas/fire detection etc.

Including all relevant A1, A2, B and C factors as a part of the barrier fault tree models result in detailed and comprehensive activity-based fault tree structures that also cover design and technical integrity issues. Figure 6 illustrates one such excerpt of the fault tree "fail to prevent escalation" that covers failure in firefighting mechanisms – supply systems, manual and automatic fire fighting. For example, to illustrate how design factors are accounted for, the basic event "C: (hydrants/ monitors) effectiveness/ design limitations" accounts for the effectiveness or ineffectiveness of manual firefighting using water hydrants or monitors which is often restricted due to limitations in coverage etc.

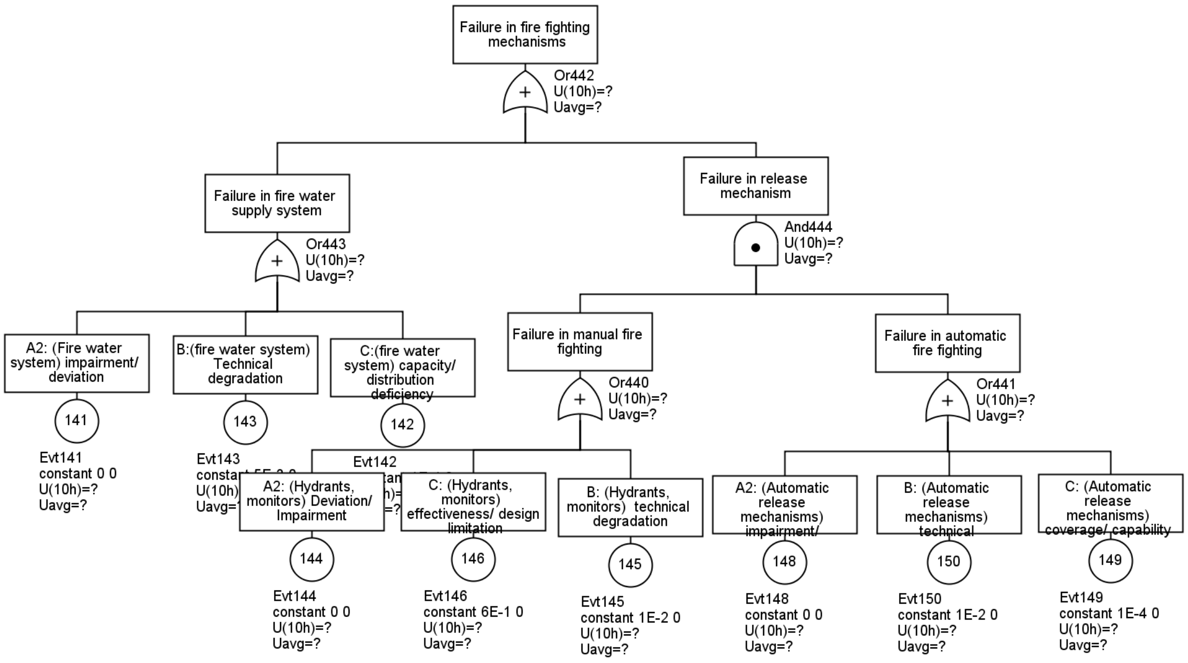
Failure in fire fighting mechanisms
Or442
U(10h)=?
Uavg=?
Failure in fire water supply system
Or443
U(10h)=?
Uavg=?
Failure in release mechanism
And444
U(10h)=?
Uavg=?
A2: (Fire water system) impairment/ deviation
141
Evt141
constant 0 0
U(10h)=?
Uavg=?
B:(fire water system) Technical degradation
143
Evt143
U(10h)
Uavg=
C:(fire water system) capacity/ distribution deficiency
142
Evt142
Failure in manual fire fighting
Or440
U(10h)=?
Uavg=?
Failure in automatic fire fighting
Or441
U(10h)=?
Uavg=?
A2: (Hydrants, monitors) Deviation/ Impairment
144
Evt144
constant 0 0
U(10h)=?
Uavg=?
C: (Hydrants, monitors) effectiveness/ design limitation
146
Evt146
constant 6E-1 0
U(10h)=?
Uavg=?
B: (Hydrants, monitors) technical degradation
145
Evt145
constant 1E-2 0
U(10h)=?
Uavg=?
A2: (Automatic release mechanisms) impairment/
148
Evt148
constant 0 0
U(10h)=?
Uavg=?
B: (Automatic release mechanisms) technical
150
Evt150
constant 1E-2 0
U(10h)=?
Uavg=?
C: (Automatic release mechanisms) coverage/ capability
149
Evt149
constant 1E-4 0
U(10h)=?
Uavg=?

Figure 6 Fault Tree Structure for “Failure in firefighting mechanisms”

Generic risk model

A run-through of all steps from the phase 1 produces a generic risk model as seen in Figure 7. In this model, event trees describe the selected major accident scenarios and activity-based fault trees model every pivotal event from the event trees. The lowest failure level on the fault trees are the individual activities and these link to influence factors via influence diagrams.

The various end consequences or sequences marked ES in Figure 7 are weighted together to define the risk measure. Weights between consequences are determined based on the potential for fatalities due to heat exposure, toxic gas, inability to escape etc. Therefore, the number of personnel or manning levels is an important parameter for the risk measure. This is a rather simple interpretation of the consequence aspect of the risk measure. Further discussion on this is provided in Section 4.

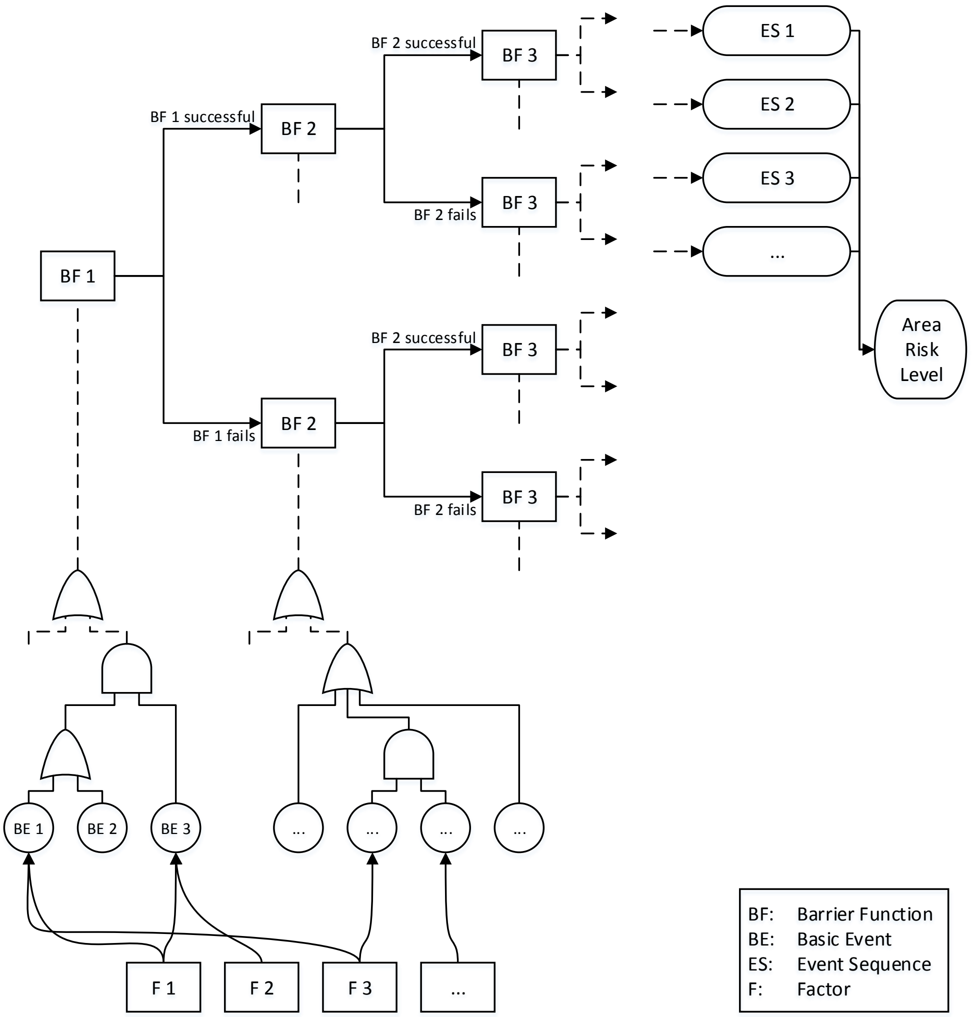

Figure 7 Overview of structure of the risk model

Phase 2 – Model Calibration and Quantification

This phase performs necessary modifications to the model – structural and numerical, to prepare the model for quantification of risk at the process facility.

It is common practice for hazardous process plants to be divided into different areas – for example, analysis areas, main areas, fire areas, construction areas etc. The need of these divisions arise due to various reasons – for instance, the analysis areas are created to help increase precision of the risk analysis, the construction areas are used for physical reference to locations across a facility etc. This step selects one such area classification for the risk model. Model configuration, further calibration and final quantification is performed based on the selected area classification.

Scaling the risk model involves selecting an area classification and modifying the risk model per area for the process facility. For example, consider the fault tree from Figure 6, while one area might have automatic firefighting, another area might have only manual firefighting. In such a manner, calibration involves removal of redundant or irrelevant lower level events or basic events from the fault trees based on the actual conditions in the given area. This thereby creates specific risk models tuned differently for each area of the process plant.

Calibrating the risk model per area requires identifying relevant data sources and setting the probabilities for the basic events for the fault trees. The widespread use of computerized solutions in current reporting practices for process industries means that the amount of available data is huge and available in a variety of formats. This is an advantage as well as a challenge at the same time. Section 4 discusses this in further detail.

Model quantification is inspired from the Hybrid Causal Logic (Røed et al., 2009) and RiskOMT (Vinnem et al., 2012) methods from wherein Bayesian belief networks integrate with the traditional event and fault tree quantification. The use of Bayesian belief networks provide an elegant way to model uncertainty in information by specifying probability distributions at the influencing factor level. These aspects are not detailed further in this paper.

The resulting risk model produces risk results per area of the installation, which together provides an overall risk picture at the entire facility.

Discussion

There are several points worth discussing related to the developed method. These are partly related to the application of the method in practice and partly to the theoretical aspects of the model. In the following, some of these key aspects are briefly described.

Focus in risk modelling

In a risk analysis context, risk is usually calculated as a combination of probability and consequence, essentially giving us a statistically expected consequence over a given period of time, normally a year. Common risk metrics, such as PLL (Probable Loss of Life), is an expression of an average or statistically expected consequence. This is a useful way of comparing alternatives when we have to make decisions about how to minimize future losses.

However, in an operational setting, the situation is slightly different. On a day-to-day basis, our focus is not just the statistically expected future consequence as expressed through the risk measure; we are primarily concerned about how to avoid accidents. The goal each day is to complete operations without anyone being injured or killed and it follows from this that we want to be able to complete all planned activities without accidents occurring. This means that apart from only looking at the risk, it is the probability of accidents that is an important parameter.

This clearly is of relevance in the approach to the modelling of risk as this simplifies the consequence modelling somewhat and puts our main effort into modelling the probability. It can probably also be argued that in many cases, the probability is more sensitive to day-to-day variation in a plant than the consequence. Clearly, it is not always like this, but as a general rule this probably holds true in many cases. Because of this, the method also focuses more on probability and looks at consequence for additional perspective to the risk picture.

Effort to develop risk models

First of all, it is quite clear from the method description that the effort required to develop a comprehensive risk model like this will be quite extensive. There are three different modelling techniques used, fault tree analysis, event tree analysis and Bayesian belief networks, and each method has to be applied to all types of activities in a plant that has an impact on major accident risk. It is not hard to envisage that this requires a considerable amount of work and it may be questioned whether the effort is cost-effective. We will not discuss the question about cost-effectiveness, but may point out a couple of issues that are relevant.

Practice in the offshore industry has been to update the QRA for offshore installations with regular intervals and the risk assessment standard NORSOK Z-013 describes criteria for updating (NORSOK, 2010). This has required extensive work for each update, in particular has detailed consequence modelling using CFD (Computational Fluid Dynamics) tools been resource demanding. The purpose of this has been to ensure that up-to-date risk models have been available for decision making in operations. In our opinion, the need for doing this is significantly reduced if models like we describe in this paper are developed instead. Considerable savings in cost can thus be achieved.

Another aspect of this is that it may be possible to develop risk model “templates” for a large variety of activities. Many activities will be similar, if not identical, from one plant to another, and most influencing factors and other related aspects will also be similar. Thus, with a library of models covering the most common activities as a starting point, developing a risk model for a specific plant will partly be a question of picking relevant models, modifying these, and putting this together. Clearly, there will be aspects which cannot be handled in this way, but we do not foresee that all details of all models will require development from scratch each time.

Availability of data

Availability of data is always an issue in risk analysis. Within the offshore industry, data collection has been ongoing for many years and this covers most of the key risk drivers. A well-known example is the OREDA database (SINTEF and NTNU, 2015). We are therefore in a fortunate situation with access to recognized databases to support risk quantification. Adopting a modelling framework as suggested in the method description represents a challenge with respect to data in at least two ways:

1) The model needs to be updated more or less continuously (e.g. daily) and data must be available in such a way that they can be “harvested” into the model automatically

2) The type of data required is partly of a different nature in comparison to the mainly technical information used in QRAs.

To take the easy part first, some input from the QRA will also be applied in this method. As long as a QRA is available, extracting this data should be relatively easily and in the long term, we can also envisage that QRAs are reported in a manner which makes it even easier to extract relevant information. This information from the QRAs is more or less static, that is this information typically can be gathered from the QRA once (or at least with long time intervals) and applied without changes for a long period (months or even years).

However, information about activities and risk influencing factors change on a daily basis and must therefore be updated daily. This includes information about types of activities, number of activities, where they are taking place, how many people are involved, who is involved etc. In addition, daily updated information about status of safety critical systems is also required. This includes information about systems/components that have failed, maintenance status, systems out of operation etc. This will not necessarily change as rapidly as the activities, but changes sufficiently often to require daily updating.

The implication of this is that the data collection must be automatic. Manually gathering all this information and inputting this into a computer tool for calculating risk would be way too work intensive to make it feasible and cost-effective in practice.

Interestingly, a lot of the information that is required is typically available in two key systems that are used in most plants already, namely the maintenance management/planning system and the work permit system (in many cases these may also be integrated). Provided automatic transfer of information from these systems to a computerized risk tool is possible (or that the risk model is implemented as a module in the maintenance management system), it is realistic to get updated information on a frequent basis.

The fact that some of the information is of a different nature as compared to what we normally use in QRA is not necessarily a problem in itself. However, the fact that the information is not necessarily available in a readily accessible format and updated regularly in electronically makes data collection a challenge.

The availability of data is a key issue for successful implementation of a model such as this, but as pointed out above; our experience is that a lot of the information is available and can be used. It is more a matter of adapting to this way of thinking and making an effort to make the data available in a suitable manner. This is a one-time effort provided automatic data transfer could be arranged and is in our view this is possible to achieve.

Practical application

We have so far not been very specific about how a tool like this can be applied in practice, except that it is a tool to support day-to-day decision-making in process plants. In the case study, we have concluded that this is a tool that can be used to support primarily the planning process. The tool can rank individual activities, identify high risk activities that need additional attention and suggest possible risk reducing measures. This can be useful early and all through the planning process until a final decision is made to approve execution of an activity. Therefore, this tool should contribute to reduce the need to postpone or even stop activities late in the planning process.

The tool can also be used to evaluate the effect of combining activities, and highlight possible interaction effects that contribute to increased risk (e.g. performing work that can lead to leaks and hot work in the same area and at the same time). These can also be identified early in the planning process and potential problems can thereby be addressed and fixed early in the process.

Both of these uses will contribute not just to reduce risk but potentially also to improve the planning process, reducing the need for late rescheduling and thus potential inefficiencies in the use of resources.

We have not so far considered potential uses during work execution. During the execution phase itself, it is hard to foresee that formal risk assessment will have a significant role in decision-making. Here, it is more a question of the workers experience, their knowledge of the systems and activities and of course, their knowledge of what the risks are. This then forms their basis for decision-making. Decisions in a setting like this will primarily be about whether to proceed with an activity or not, or whether to proceed with a different plan or not. One could envisage that if alternative plans are being considered, a formal risk assessment could be of help. However, at present, we have difficulties seeing how this can be kept up-to-date as the work progresses and is therefore not likely to be realistic. Also, there will be significant issues of trust – that is, will the workers trust a tool that tells them whether it is safe to proceed or not, or will they rely on their own knowledge and experience?

A more general aspect of practical application of this model is the balance between complexity (and completeness) of the model versus the ability to produce results in time and the trust that the personnel involved in the planning process will have in the model. It is likely that there will be a lot of compromises necessary to develop a model that works in practice. This needs to be carefully weighed against what we lose through simplifications and if we reach a point where the model is not useful anymore.

Presentation of results

Part of the project is also to look into how the result presentation can be improved, to support better decisions. This is still ongoing, but some important principles have been laid down as a basis for the model development.

We have used inspiration from the description of fast and slow thinking by Kahneman (2011) as a “model” for how we want the risk model to work. Fast thinking relies very much on simple decision rules and heuristics, enabling us to make quick decisions. On the other hand, slow thinking implies a more comprehensive deliberation of key factors that influence our decision. For low risk activities, fast thinking can be applied, in the sense that standardised risk reducing measures are applied and simple decision-criteria are applied. There may even be a possibility that these decisions can be more or less automated. However, for high-risk activities, the aim is to “push” the decision-maker into slow-thinking mode by presenting more information about why the risk is high (the “risk driving factors”), not just the risk level as such. Of course, there is still a possibility that the decision-makers will focus only on a few of these factors and over time develop heuristics that help them stay in fast thinking mode. The idea is however to try to support the process of staying in slow thinking mode.

How the risk should be presented is also an issue that requires careful consideration. The traditional risk metrics that we use, such as PLL and FAR are all representations of statistically expected consequences. As pointed out earlier, this is not necessarily the most useful information for operational decision-making.

Uncertainty

PSAN's defines risk as "risk means the consequences of the activities, with associated uncertainty" (PSAN, 2015), which emphasizes the uncertainty as an important issue in risk assessment. It is therefore interesting to consider how the proposed approach considers uncertainty.

There is virtually no uncertainty about the circumstances and state of parameters that may influence risk, on the day the activity is due to be carried out. The competence of the crew is known, the weather conditions are known, technical status of protective systems (barriers) as well as any simultaneous activities they are all known. There is still some uncertainty about how the activity will be carried out, will there be any human errors, will any technical systems experience faults, etc. the uncertainty is nevertheless at its minimum.

When the work was planned, maybe a year ahead, or three months ahead, there was more extensive uncertainty about competence levels of involved crew members, weather conditions, state of all barrier systems, simultaneous activities. This span of uncertainty in aspects that influence the risk levels is covered by the proposed methodology through the probability distributions of the RIFs.

Another aspect of uncertainty is the extent to which there are unknown hazards or threats that have not been included in the risk assessment, so-called 'unknown unknowns' (Haugen & Vinnem, 2015). We would on the other hand argue that hazards related to leaks of hydrocarbons are well known, although there may be unknown causal mechanisms that have not been revealed yet. It is nevertheless considered that 'unknown unknowns' may be disregarded in a risk assessment of operations that may affect the probability of leaks from the process systems. On the other hand, if a full risk assessment of the plant in question was performed, the risk associated with 'unknown unknowns' should be considered explicitly.

Weaknesses in the theoretical modelling

It is argued above that operational activities likely affect the probability of major accidents and not so much the consequences of such occurrences. If ventilation conditions are altered, either due to the presence of scaffolding or tarpaulin, the spread of gas clouds in the area changes. While this aspect has been considered partially in the model, the detailed impact of this on the consequence (due to change in explosion pressures and other mechanisms) is not focussed upon. The proposed approach therefore has a very limited consideration on explicit modelling of the consequences of accidental events. Any more sophisticated consideration of consequences (for instance through CFD modelling) would most likely affect the computation time severely. Significant increase of computational time would most likely affect the usability of the methodology drastically, because it will be required that the effect of changes to input parameters can be seen almost instantly.

Conclusion

In the MIRMAP project, we have developed a conceptual method for analysing risk in an operational setting, to provide decision support related to major accident risk for day-to-day decision making in process plants. A key to the project has been that we have taken a step back to look at the decisions that we need decision support for and what these decisions require in terms of information about major accident risk. The method that has been developed is still at the conceptual stage and has not been implemented in practice. However, based on the work done so far we believe this is a fully feasible approach that can provide useful information. There are challenges that need to be overcome, e.g. availability of data, and there are also uncertainties, e.g. related to how much work is actually required to develop useful methods. Clearly, if the work is too extensive and implies too high cost, it may be questioned if this is worthwhile.

The project will continue approximately for another year, focusing on application to practical problems. This is expected to give more information about the practicality and feasibility of the method, but our preliminary conclusion is that this is a promising approach.

Acknowledgement

The authors wish to acknowledge the Norwegian Research Council for their financial support to the MIRMAP project, No. 228237/E30, funded by PETROMAKS2.

References

Aven, T., Sklet, S., Vinnem, J.E., 2006. Barrier and operational risk analysis of hydrocarbon releases (BORA-Release): Part I. Method description. J. Hazard. Mater. 137, 681–691. doi:10.1016/j.jhazmat.2006.03.049

Bellamy, L.J., Mud, M., Manuel, H.J., Oh, J.I.H., 2013. Analysis of underlying causes of investigated loss of containment incidents in Dutch Seveso plants using the Storybuilder method. J. Loss Prev. Process Ind. 26, 1039–1059. doi:10.1016/j.jlp.2013.03.009

Etterlid, D., 2013. iSee - visualization of HMS related factors.

Haugen, S., Seljelid, J., Mo, K., Nyheim, O.M., 2011a. Major Accident Indicators for Monitoring and Predicting Risk Levels. Society of Petroleum Engineers.

Haugen, S., Seljelid, J., Nyheim, O.M., Sklet, S., Jahnsen, E., 2012. A generic method for identifying major accident risk indicators. Presented at the 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference, Curran Associates Inc., Helsinki, Finland, pp. 5743–5752.

Haugen, S., Vinnem, J.E., Seljelid, J., 2011b. Analysis of causes of hydrocarbon leaks from process plants. Society of Petroleum Engineers.

Kahneman, D., 2011. Thinking, fast and slow. Macmillan.

Knochenhauer, M., 2014. Risk expression and modelling in risk monitors - using RiskSpectrum RiskWatcher as an example.

Luxhoej, J.T., Coit, D.W., 2006. Modeling low probability/high consequence events: an aviation safety risk model, in: Reliability and Maintainability Symposium, 2006. RAMS '06. Annual. Presented at the Reliability and Maintainability Symposium, 2006. RAMS '06. Annual, pp. 215–221.

NORSOK, 2010. Risk and emergency preparedness analysis. NOROSK Stand. Z-013 Rev 3, 16–8.

NPD, 1981. Guidelines for safety evaluation of platform conceptual design. Oslo.

Øien, K., 2001. Risk indicators as a tool for risk control. Reliab. Eng. Syst. Saf. 74, 129–145.

PSAN, 2015. Regulations relating to health, safety and the environment in the petroleum activities and at certain onshore facilities (The framework regulations).

PSAN, 2014. Trends in the risk level on the Norwegian Contintental Shelf (NCS) - main report (in Norwegian).

PSAN, 2013. Principles for barrier management in the petroleum industry.

Rasmussen et al., 1975. Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants [NUREG-75/014 (WASH-1400)]. US Nuclear Regulatory Commission.

Røed, W., Mosleh, A., Vinnem, J.E., Aven, T., 2009. On the use of the hybrid causal logic method in offshore risk analysis. Reliab. Eng. Syst. Saf. 94, 445–455.

Schellings, D., 2013. Total risk approach. Society of Petroleum Engineers.

SINTEF and NTNU, 2015. OREDA – Offshore and onshore reliability data handbook, 6th ed. Trondheim, Norway.

Sklet, S., Ringstad, A.J., Steen, S.A., Tronstad, L., Haugen, S., Seljelid, J., Kongsvik, T., W\a erø, I., others, 2010. Monitoring of human and organizational factors influencing the risk of major accidents, in: SPE International Conference on Health Safety and Environment in Oil and Gas Exploration and Production. Society of Petroleum Engineers.

Vinnem, J.E., Bye, R., Gran, B.A., Kongsvik, T., Nyheim, O.M., Okstad, E.H., Seljelid, J., Vatn, J., 2012. Risk modelling of maintenance work on major process equipment on offshore petroleum installations. J. Loss Prev. Process Ind. 25, 274–292.

Vinnem, J.E., Røed, W., 2015. Root causes of hydrocarbon leaks on offshore petroleum installations. J. Loss Prev. Process Ind. 36, 54–62.

Wang, C., 2007. Hybrid causal logic methodology for risk assessment. ProQuest.

Yang, J., Yang, M., Yoshikawa, H., Yang, F., 2014. Development of a risk monitoring system for nuclear power plants based on GO-FLOW methodology. Nucl. Eng. Des. 278, 255–267.