SAFETY SCIENCE Monitor

Issue 1 2011

Article 6 VOL 15

INVESTIGATION OF INCIDENTS IN SYSTEMS DESIGNED OR DEVELOPED ON THE BASIS OF RISK ANALYSES

OVE NJÅ
University of Stavanger

GEIR SVERRE BRAUT
Stord/Haugesund University College

SUMMARY

The use of risk analyses for planning and maintenance purposes has increased in recent decades. Not only has this been the case in the industry and transport sectors, but risk analyses have gained increasing popularity also for societal planning purposes, e.g. in local community development and emergency preparedness.

The overall aim of risk analyses is to reduce the number of undesired incidents and their potential outcomes. But since risk is a phenomenon with stochastic properties, we cannot expect even the best performed risk analysis to guarantee absolute risk control and no unexpected, undesired incident or negative outcome.

Up to now scant interest has been shown in how prior risk analyses are dealt with in subsequent incident investigations. Accident investigations often criticize involved parties for not having carried out risk analyses, especially assessments that could have prevented the accidents. We regard this as a narrow interpretation of what risk management can provide. Analyses of root causes and background variables during an incident investigation process must be seen as representations of investigators' preconceptions of good safety management principles, regarded as acknowledged practice. It is a misconception to regard highlighted background risk management variables as true explanations of accidents. To emphasize the constructivist interpretation of a risk analysis we propose to use the notion risk image instead of risk picture, which is the term commonly used today.

Keywords**:** Risk analysis, accident investigation, risk image

1. INTRODUCTION

When major accidents or adverse events occur it is quite common for society to respond by setting up an incident investigation, through an ad hoc committee or permanent investigation boards or public supervisory bodies. In future, it is likely that such investigation processes will increasingly have to deal with incidents in systems that also have been an object of prior risk analyses.

The aim of this article is to discuss from a theoretical point of view how incident investigation processes can approach incidents preceded by relevant risk analyses and even criticize or challenge the established risk picture. The theoretical perspectives will be illustrated by material from investigation reports and other relevant comments on four specific incidents, cf. Table 1.

The present organization of industries and public services reflects past history and traditions, both within the specific sector as well as society at large. This imprint of history also applies to risk regulation and risk

management practices. Written and unwritten requirements and expectations have great impact on how organizations and their members act, including where safety issues are concerned. Such cultural and historical factors may be used to challenge the results of probabilistic risk analyses. These contextual conditions may possibly also restrict a sensible use of the results of risk analyses.

Despite cross-sectoral differences there seems to be a common trend towards the principle of self regulation. This is very clearly seen in the petroleum sector (Lindøe & Braut, 2009), and also increasingly in other sectors such as the health services (Braut, 2003). The report to the President after the Deepwater Horizon accident may be read as a proposition for moving the US regulatory regime from a prescriptive regime to more regulated self-regulation (Graham et al., 2011).

The current regulatory situation in the petroleum sector in Norway will be used as a frame for the discussion in this article, although we shall also draw on examples from the railway sector. The regulatory regime in the railway sector has partly copied the regulatory stance from the petroleum sector.

1.1 The Norwegian oil and gas industry

In many aspects the oil and gas industry has been a pioneer in the development of safety management systems. In Norway this sector has also been used as a model for developing new regulatory regimes in other sectors.

The petroleum regulatory regime includes risk management as a premise for loss prevention activities, and subsequent accident investigations as a learning tool after incidents or accidents.

1.1.1 The safety regulation regime

The Norwegian petroleum safety regime builds on the basic principle of the licensees' (oil companies, refineries) full responsibility for ensuring that the petroleum activity is carried out in compliance with the conditions laid down in the legislation, not least the requirement for practice according to prudent and sound standards based on up-to-date knowledge, cf. the Act of 1996 relating to petroleum activities (Petroleum Act) Sections 9-1 and 10-1.

Since 1985 the safety regime has been founded on the principle of internal control. The initial requirements in the Act of 1985 have been continued in the current Act of 1996, cf. Petroleum Act, Section 10-6. The authorities' supervisory activities are therefore aimed at ensuring that the management systems of the licensees cater adequately for the safety and working environment aspects of their activities.

The initial petroleum legislation dating back to the 1960s and 1970s was technically oriented, with detailed and prescriptive requirements for safety management as well as technical solutions. The authorities, represented by the Norwegian Petroleum Directorate (NPD) and from 2004 the Petroleum Safety Authority (PSA), have gradually modified the legislation in the direction of functional requirements.

New regulations regarding the implementation and use of risk analyses came into force in 1990, and new regulations on emergency preparedness appeared in 1992. Both these regulations focused on the risk analysis process aimed at preventing major accidents. The regulations were further developed and a revised set came into force in 2002. The current revision is dated 2010 and came into force in 2011.

The purpose of the risk analyses is to provide a decision-making basis for determining appropriate solutions and risk reducing measures. According to the regulations it is the operator’s responsibility to define safety objectives and risk acceptance criteria. The objectives express an ideal safety level, thereby ensuring that the planning, maintenance and the further enhancement of safety in the activities become a dynamic and forward-looking process.

Accidental events must be avoided (any actual accidental event is unacceptable). This means that risk is kept as low as reasonably practicable (ALARP), and attempts are made to achieve reduction of risk over time, e.g. in view of technological development and experience. The need for risk reducing measures is assessed with reference to risk acceptance criteria. The acceptance criteria and the basis for deciding them are to be documented and auditable.

The current regulations state that the operator shall formulate acceptance criteria relating to major accidents and to the environment. The acceptance criteria shall be used for evaluation of results from the various quantitative risk analyses (QRAs) and shall be given for:

a) personnel on the installation as a whole, and for personnel groups (that are) particularly exposed to risk,

b) loss of main safety functions,

c) pollution from installation.

The Norwegian system is claimed to represent a relatively 'mechanistic' approach to risk analysis and evaluation, implying a narrow focus on satisfying the risk acceptance limits, usually with no or small margin (Aven & Vinnem, 2005). Planning of onshore facilities, such as refineries, must take the EU Seveso II directive into consideration, which obliges the operator to address third party risk.

1.1.2 Accident investigation requirements

Accident investigation in the Norwegian oil and gas industry is regulated by Section 10-10 of the Petroleum Act and subsequent regulations. In the case of serious accidents the Ministry may appoint a specific committee for inquiry (ad hoc), in which sufficient legal, nautical and technical expertise must be ensured.

Furthermore, Section 20 of the regulations of 2010 relating to management of the petroleum activities (Management Regulations) requires that:

The responsible party shall ensure that hazard and accident situations that have occurred and that may lead to or have led to acute pollution or other harm, are recorded and examined in order to prevent recurrence.

This is similar to the text of the regulations of 2001. The guidelines to Section 20 of the Management Regulations issued by PSA recommend that (2011):

The investigation should, inter alia, clarify:

a) the actual course of events and the consequences,
b) other potential courses and consequences,
c) existing non-conformities to requirements, approaches and procedures,
d) human, technical and organizational causes of the situation of hazard and accident, as well as in which process and levels the causes may be found,
e) which barriers have failed, the causes of barrier failure and, if applicable, which barriers should have been established,
f) which barriers have functioned, i.e. which barriers have contributed to prevent a situation of hazard from developing into an accident, or which barriers have reduced the consequences of an accident,
g) which actions should be taken in order to prevent similar situations of hazard and accident.

These guidelines for accident investigation provide great flexibility in choice of accident modelling and subsequent emphasis on risk increasing factors and behaviour prior to the incident.

1.2 General relevance

Even though other industries differ from the petroleum sector, the concept of high reliability organizations (HRO) seems to prevail as the ideal. This is evident e.g. in the rail transport sector. In Norway as in other countries, this approach to safety has been adopted by far more loosely coupled systems and sectors than those for which it was originally developed (US Navy, Air Traffic Control, nuclear energy production), see for example (La Porte & Consolini, 1991; Marone & Woodhouse, 1986; Reason, 1997; Roberts, 1989). As a consequence, enterprises express safety philosophies that require continuous learning and improvement processes in which they reflect critically on risk in their own systems, subsystems, units and components and draw on experience from undesired incidents in this reflection.

The safety regime described above is supposed to ensure that safety is continuously improved. It is not easy to claim that enterprises managed on the basis of risk analyses are safer than enterprises regulated in accordance with other (regulatory) strategies. We contend that investigators' preconceptions about these questions may influence the content of accident investigations and thus the explanatory factors addressed.

Andrew Hopkins, an Australian sociologist, has studied two major petrochemical accidents, Longford (1998, Exxon) and Texas City (2005, BP), as well as the mining accident in Gretley (1996, Oakbridge). He expresses his scepticism towards risk management at the Texas City refinery in this way: *"The best way to ensure safety in matters such as trailer location (in which most of the people died, our remark) is to devise a rule*

beforehand, rather than allowing decisions to be made on the basis of individual risk assessment. The latter approach is likely to introduce confirmation bias and to result in less competent risk assessments." (Hopkins, 2010, p. 44).

Our discussion is rooted in doubts and questions similar to those of Hopkins. We link our scepticism to theories of risk management and learning in order to make specific suggestions for further discussion and development of current investigation practices in situations where risk managed enterprises are being investigated.

2. HYPOTHESIS AND METHODOLOGY

Our hypothesis is that investigators and commentators, when it comes to background causes, are free to apply their own understanding of good safety management principles. They do not necessarily take into account or validate prior performed analyses and the conditions under which such analyses were made—hence the phenomenon "What You Look For Is What You Find" (Hollnagel, 2010; Lundberg, Rollenhagen, & Hollnagel, 2009) may dominate the investigations. In other words, investigators do not use prior risk analyses as an analytic framework for their investigation.

Although not necessarily a drawback for the learning process, it may be a serious mistake to interpret the explanations from the investigation reports as the ultimate and complete truth about the incident and its causes. Such underlying interpretations are even more important if the investigation results are used to place or argue moral or legal responsibility for the accident.

We have chosen the petroleum and railway sectors for our study because both are based on high-risk operations and technologies. Furthermore, the systems are relatively closed, as operations are limited to a restricted number of licensed companies and their employees. They may therefore be seen as systems that are possible to govern through procedures based on high reliability theory. These sectors have also been met by regulatory requirements for risk analyses in addition to regulatory requirements for performing accident investigations.

There are major differences in the chosen cases with respect to media coverage, number of fatalities, operational premises and (type of) companies involved. However, all the accidents had damage potential that could easily have made them much worse than experienced.

To pinpoint and discuss our hypothesis we introduce the four accidents depicted in Table 1.

Table 1. Selected incidents/accidents

Accident/Year	*Number of fatalities*	*Risk management focus in the investigation reports*
Petroleum sector		
Texas City Refinery, 2005	15	Yes
Gas leak Oseberg C, 2008	0	No
Railway sector		
Åsta, Røros-line, 2000	19	Yes
Alnabru/Sjursøya, 2010	3	Yes

The Texas City Refinery disaster occurred after a 60 metre distillation column was overfilled during start up after maintenance. The condensate was discharged from a tall vent stack and an explosive vapour cloud formed and ignited by an idling motor vehicle nearby. 15 people were killed and almost 200 injured (Hopkins, 2010).

The gas leak at Oseberg C platform in the North Sea occurred during hydraulic leak test after change-out of a solenoid valve for a well manifold valve. The valve opened unintentionally for less than 1 second. There was a pressure differential of 70 bars over the valve. This caused rupture of a 2" equalizing line between the test manifold and the production manifold and subsequent hydrocarbon leak from the production manifold. The production process was shut down automatically and all personnel mustered according to plan (PSA, 2009; StatoilHydro, 2008).

The Åsta train accident occurred when a southbound diesel powered passenger train from Trondheim heading for Hamar on the Røros line collided with a northbound diesel powered passenger train (engine car and

steering car) at Åsta on a single track line. A major fire immediately broke out in the forward area of both trains, and a few minutes later fire broke out in the first carriage of the southbound train. 19 persons were killed (NoU, 2000).

The Alnabru/Sjursøya train accident occurred when a set of empty cargo wagons started to roll out from a marshalling yard and by means of gravity ran uncontrolled for several kilometres before derailing at the buffer stop at the end of the track. Unsuccessful attempts were made to derail the wagons before they reached the end of the track. The incident resulted in three fatalities in addition to four injured persons and severe damage to buildings (AIBN, 2011).

We restrict our scrutiny to the investigations as presented by the selected authors and reports. We have not taken into consideration other documents related to the incidents, for example the Baker report (Baker et al., 2007) on the Texas City refinery disaster. Our analysis therefore cannot be regarded as a corrective to the truth about the described incidents, which are merely used as aids for our theoretical discussion.

Case studies have been criticized for their lack of scientific rigour and generalizability. Despite the complexity of framing case studies, we claim that case study approaches are perhaps the most important means for generating knowledge about learning from accidents. This kind of knowledge is highly dependent on contextual and practical experience. Comparative case study designs are beneficial because they enable analytical treatment of various subsequent variables for the purpose of improving modelling, cf. Yin (1994), Kaarbo & Beasley (1999), Andersen (1997), and Flyvbjerg (2004) for further discussion about case studies.

We have read the chosen documentation closely in order to clarify the authors' main lines of approach and how they model the accidents. Their presentations must be seen through the lens of the authors and the contribution they wish to make in the aftermath of the accidents.

Our analysis seeks to reveal how the authors deal with the following issues: risk analysis and modelling of a risk picture; risk management and blaming, shaming and learning.

3. FINDINGS RELATED TO RISK ANALYSIS AND RISK MANAGEMENT

3.1 The Texas City disaster

Hopkins (2010) has devoted an entire chapter to the topic "Blindness to major risk". His main concern in regard to the Texas City incident was BP's confusion of occupational safety hazards and major process safety hazards. Issues such as lost time incidents were highly prioritized by the refinery management, whereas process safety hazard issues were downsized in the organization, with no real spokesmen to provide informed input in the decision making forums. Throughout the entire book he addresses three critical decisions in terms of risk management:

1. Unsuccessful replacement of the vent stack with a new flare assembly. The risk assessment was used to inhibit the change-out.

2. Fatal location of trailers during maintenance. Hopkins criticizes the risk assessment made by the local staff as being insufficient and erroneous, not taking major process accident scenarios into consideration.

3. Inadequate start up procedures of the distillation column. In this case risk analyses were not carried out as a basis for the procedures.

In order to substantiate these sharp-end failures, Hopkins demonstrates several contextual conditions as cost-cutting independent from considerations of the system operational conditions, reward systems isolated from process safety performance, decentralized decision making without a superior holistic framework guiding decisions, lack of collective mindfulness and mindful leadership, a blaming culture, inability to learn from accidents within or outside the company, failure to successfully implement an HRO culture programme and finally a supervisory authority in the role of passive spectator.

3.2 Oseberg C gas leak

Neither the reports from the internal (StatoilHydro, 2008) nor the external (PSA, 2009) investigations are clear about the level of risk control or safety to be achieved. The internal report refers to the total risk analysis (TRA) for Oseberg C in the context of ignition likelihood for a gas leak of 20 kg/sec. The authors use the

likelihood assignment to argue that the probability of a fire or explosion with escalation was non-existent, given approximately the same conditions as were observed on Oseberg C. In addition, the internal investigators ascertained that no reliability analysis of unintended and sudden valve opening was required by regulation. The investigators recommended that operational risk should be discussed as part of the work permit in order to ensure common understanding amongst supervisors and technicians.

The external report perceived the work preparations before the valve change-out as a violation of the regulations and claimed that the operational risk analyses were insufficient due to:

- No risk assessment of work on a valve with 70 bar differential pressure.
- Consequences of sudden opening of valve were not considered.
- No coordination of simultaneous work on the system.
- No discussion with supervisor prior to safety critical work.

3.3 Åsta accident

The Groth commission found that the Ministry of Transport and Communications had initiated a risk analysis in 1990 with the aim of assessing the safety level in rail transport. In regard to the owner of the infrastructure, the Norwegian National Railway Administration (NNRA), the commission harshly commented: "*In practical terms the experience transfer and measures after previous accidents have been weak. Recommendations after the Tretten accident (27 killed in 1975) and the Nordstrand accident (5 killed in 1993), and subsequent recommendations from risk and safety reports, made by ….., have not been followed up in a systematic and controlled way. Important recommendations encompassing audiovisual alarms at the rail traffic centres and automatic train control development on all lines have not been carried out and no compensating measures have been installed to replace these recommended safety measures* (p. 131)",

The Groth commission concludes (NoU, 2000, p. 203): *The Norwegian National Rail Administration should have conducted more risk analyses over the last few years in the light of the changes introduced that affected safety. Furthermore, a risk analysis should have been conducted of the safety level on the individual section of a line, including the Røros line. A risk analysis would have shown that the safety level on the Røros line was far from adequate. Whatever the direct cause of northbound train 2369 incorrectly passing the exit signal at Rudstad station on 4 January 2000, our examination of the reasons why it happened at all, and why the situation was not discovered and stopped at an earlier stage, has revealed a basic lack of a systematic approach to safety issues, particularly within the Norwegian National Rail Administration, whose responsibility it is to ensure that the overall safety of a section of a line is acceptable.*

The NNRA was finally blamed and given a penalty of NOK 10 million (2001), not for the accident itself but because of its lack of an adequate safety management system.

3.4 Alnabru/Sjursøya runaway train

The investigation report refers to six prior risk analyses with some relevance to the accident (AIBN, 2011).

One of them (from 2001) identified as a possible hazard: *Brakes not engaged for rail car and it rolls onto the main track at Alnabru South.* AIBN in their preliminary report gives this comment upon this analysis: *The report shows that the analysis team was split in its view of whether or not this was a realistic incident and priority was therefore not given to identifying appropriate measures. It is also evident from the report that the basis for hazard identification was normal slipping of rail cars to the directional tracks. Activities such as parking of wagon sets in the A tracks, shunting in additional rail cars while the wagon set was parked in an A track and reserving wagon sets past the access brakes do not appear to have been included in the basis for the analysis.*

A second analysis from 2004 was never finished. Analyses from 2000, 2006 and 2008 gave some indications on a possible hazard like what happened in the accident. Two of them (2006, 2008) suggested possible barriers or actions, but the suggestions were not followed up.

Another analysis from 2001 was more concerned with presenting an overall picture than analysing the conditions at the marshalling yard in detail, even though it identified uncontrolled rolling stock as a hazard.

The report from AIBN states that the infrastructure at Alnabru has been under continuous adjustments and changes for several years.

In addition it is mentioned that limited risk analyses have been performed related to all reports and applications on alterations of railway infrastructure. But those analyses were only related to the specific changes and thus did not show how the impact of the changes on the total level of risk at the marshalling yard. AIBN recommends that focus for mapping of risk in an area as here should be more concentrated upon thorough analyses of barriers related to working processes than upon determination of quantitative aspects related to possible "top events". Considerations on probabilities and consequences may not be able to catch the complex risk picture at the marshalling yard, they claim. AIBN also claims that important information on safety related experiences are transferred as narratives on the work place more than through formalized reporting channels.

4. ACCIDENT INVESTIGATION OF RISK MANAGED ENTERPRISES

4.1 Risk picture or risk image for managerial purposes?

The aim of a risk analysis is to give a description of possible threats and hazards that may give rise to undesired consequences. The causal relationship between threats and hazards and consequences must be understood and explained. The validity of the analysis cannot be better than the validity of the causal explanations given.

When there is doubt related to the possibility of a chain of events occurring, as e.g. in the first risk analysis from 2001 of the marshalling yard at Alnabru, this doubt must be handled in a prudent way. Disagreement between the analysts must be seen as possible lack of validity of causal chains. In itself this is a potential source of risk. Hopkins (2010) reveals distrust in risk assessment in his discussion of trailer location decision through the confirmation bias phenomenon. This view is further increased by his call for more prescriptive rule compliant risk regulation principles and rules for decision making in the hazardous industries, (Hopkins, 2011). Stephen Watson (1994) provides a completely different view on probabilistic safety assessments. He recommends that in the risk analysis process the analysis should base discussions about risk, both at the executive decision levels and within operational environments prior to decisions, very much in line with Habermas' thinking on planning and decision making. Perhaps the latter is easier to operationalize in a Scandinavian context where the balance between authorities, employers and employees is more even than in the rest of Europe and the western world.

Lack of agreement on risk may lead to an unclear risk picture and further to lack of conformity in systems and procedures and even to perception of threats and hazards during operational activities. In the Alnabru case the analysis and the analysis process from 2001 did not reveal any risk treatment activities, raising questions as to whether the risk assessment was given priority at all.

The notion of a risk picture may also give rise to a false sense of truth. A picture is commonly understood as a visual representation of something that may be regarded as a fact or a truth, at least something that can be observed objectively. As risk analyses aim to depict the future, of which we do not know the fact or the truth, the notion of a risk picture may be misleading. Possibly a better notion would be a risk image. By using the word image we contend that it becomes clearer that the result of a risk analysis is a sensible construction, based upon the best available knowledge at any time. A risk image may then be the mental representation for contemporary managerial purposes, something that can be imagined.

The images produced by risk analyses must be kept under almost continuous scrutiny by the responsible leaders. Risk management based upon non-updated risk analyses or analyses with lacking relevance is not necessarily better than risk management based upon no formal analysis. Here it may be important to be reminded of the warnings on possible oversimplification given by the Columbia Accident Investigation Board (2003, p. 181).

In view of this it is difficult to see that train handling on a marshalling yard according to procedures based upon risk analyses made several years ago, under other operational circumstances and with unclosed disagreement on hazards, justifies being called analytic based risk management.

4.2 Blame, shame or learning

In an investigation there is a critical relationship between the normative assessments of individual or organizational performance and the presented explanations on the causes and the development of the accident. As soon as the investigator makes a direct or indirect assumption that a person might have been negligent and made a possible mistake it can be regarded as a moral judgment which might stop further investigation on the causes and development of the incident. Finding an explanation requires the investigator recurrently to ask "why"-questions in order to reveal contextual factors further back in the causal chain.

Hopkins (2010, pp. 121-122) describes this eloquently, and he advocates that blaming should be avoided in investigations. However, he is a strong proponent of a deposition system as seen in the US, which confronts the responsible persons with lawyers and the sufferers. Hopkins seems to believe that such a potential pressure upon company leaders would oblige leaders to learn. Although Hopkins has not defined what he means by the concept of learning, it is implicit that since the time of the Texas City disaster, managers and employees had not learnt. Hopkins draws on the fact that similar accidents had happened elsewhere, both at refineries owned by BP and at refineries outside the company. In spite of this BP had not made any changes to the design and procedures of the Texas City refinery.

The point of interest is not merely the presence or absence of prior analyses. In our view the managers should neither be evaluated nor judged on the fact that the incident occurred, but on how they had been able to construct and follow up a relevant risk image that could support them in the continuous efforts to reduce risk.

The Åsta case. The Norwegian National Railway Administration (NNRA) was made a scapegoat for the Åsta accident. According to the investigation commission NNRA had not absorbed, and showed an almost reluctant attitude to, the concept of "modern safety management". Modern safety management was said to be risk based, and according to the commission modern risk management requires that risk analyses should govern all phases and areas of railway activities. Apparently this was well-founded, judging by NNRA's own comments to the public report.

The Norwegian State Railways (NSB BA), the train transport operator, was spared criticism because they had carried out some risk analyses. The quality of those analyses was however never questioned by the commission (Njå, 2002), neither were the decisions made at the political level challenged by the commission.

The Groth commission (NoU, 2000) may be suspected of having an underlying view of risk analyses as instruments capable of revealing possible future incidents, as if the risk pictures presented were valid representations of the future truth. But if, on the other hand, risk analyses are to be used as platforms for managerial decisions it is not the risk analysis in itself that is of value. The value of a risk analysis in this perspective must be judged according to how far it gives a sensible risk image for managerial actions.

Thus there may be a close coupling between risk analyses for managerial purposes and risk analyses aimed at learning. When dealing with previous risk analyses, investigators should evaluate how these instruments have been used in establishing a risk image in the organization and how this risk image has been used for managerial decisions and employee education and reflection (Braut & Njå, 2009).

4.3 The role of risk assessments in the aftermath

Hopkins (Hopkins, 2010) and Perrow (Perrow, 1984) both criticize risk analyses because they were unable to predict the upcoming incident and encouraged less safe solutions, seen retrospectively. In our view this is not the most sensible way to regard the potential benefits of risk analyses. If this perspective on risk analyses is also shared by investigators we would expect future investigations to seriously question the role and value of risk analyses for risk managerial purposes.

None of the investigations we have studied did put total risk analyses performed (in the organization itself or by the owners) under scrutiny to see how the analyses had influenced the design of the systems. The preliminary investigation report of the Alnabru/Sjursøya-accident goes some way towards addressing the prior analyses. Neither of the investigations has focused on the intersection between managerial decisions based upon prescriptive requirements (including agreed standards as well as legal and economic frames) and functional requirements based on probabilistic analyses of risks performed before the accident. The scrutiny of prior risk analyses to be performed in an investigation should also take into account these superior perspectives. Failure to do so may mean that corporate risk analyses will soon prove to be the documentation that helps to make the manager the scapegoat of any accident.

4.4 Pitfalls to be avoided in accident investigations of risk based regulated enterprises

It is certainly sound practice in the aftermath of incidents to critically challenge the previous decisions. But to assume a different outcome, given other prerequisites, seems unreasonable, beyond mere rhetoric, if we presume the probabilistic nature of accidents.

With the benefit of hindsight the two important questions investigators should try to answer are:

1. How was the information on relevant risks available before the incident dealt with by managers and employees?

2. What new knowledge generated by this incident is of a general nature or specific to this incident and/or this organization?

Both these questions put under scrutiny not only the prior dispositions of the investigated organizations, but also the presumptions of the investigators. For an investigation to be of good quality we recommend that investigators be explicit about their own views on the potentials and limitations of risk analyses, and about how they judge the analyses made and subsequent actions taken by the organization under investigation.

When attempting to answer these questions investigators must try to reveal how the organization at different levels has responded to risk related experiences generated through daily operations, not least how it has responded to warnings from inside or outside and situations perceived as "fateful moments" by the employees (Giddens, 1991). Without this basis in daily, practical work, the risk analytic approach may turn out to be more of a bureaucratic exercise than a living instrument for reducing risk.

5. CONCLUDING REMARKS

Ellinor Ochs (1997) describes narrative as: "It is our cares about the present and especially about the future that organize our narrative recollection of past events". In this paper we have scrutinized the investigators' power as narrators of the "true" stories. In an accident inquiry the initiating interest is, of course, to reveal the truth about what really occurred and why the accident took place. But to reveal the "truth", i.e. all facts of the accident, is practically impossible.

In a risk management system based on risk acceptance limits, the operator needs to demonstrate to the authorities that the limits have been met. This is often achieved by referring to the risk results, and involvement by the authorities is sometimes rather superficial.

With an ALARP approach, this also implies that authorities' involvement needs to be stronger. ALARP requires continuous updating of the risk image. The authorities, as supervisory bodies before a possible accident as well as investigators after an accident, must therefore concentrate on how the organizations establish and continuously maintain and make use of a valid risk image. The reflections and discussions on this risk image both among the employees and on managerial level are probably more important than the risk image itself. The ALARP demonstration is more comprehensive than merely inspecting risk results. For authorities to review an ALARP demonstration, an extensive evaluation process will normally be needed to determine if a sufficiently wide search for alternatives (e.g. possible risk reducing measures) was taken, and whether arguments relating to gross disproportion are valid. This means that more effort is required on the part of the authorities.

However, we are not necessarily proponents of updating the concept risk analysis (also defined as total risk analysis - TRA), as often required by guidelines, e.g. (NORSOK Z-013, 2001; NS 5814, 2008). Such updating processes are cumbersome, expensive and rigid, reflecting the models and assumptions of the TRA. It is very rare for personnel at different levels in the organization to be familiar with the contents of the TRA, not even among top level management. The total risk analysis should be considered as a snapshot of risk provided as a contribution to major decisions on facility design. In the operational phase there must be structures that enable risk images to become integrated, risk images that reflect experiences at the particular facility as well as comparable facilities elsewhere. Collective mindfulness requires risk assessment tools that are adapted to the emerging decision problems, and not the converse that decisions have to be adapted to the TRA. Supervisory bodies must demand explanations on how risk images, both holistic and specific, are developed, what they contain and how they are applied within the organization, rather than asking how often the TRA is updated.

Our main hypothesis was that the investigators' preconceptions of good safety management would dominate the investigations. We conclude that our empirical data support this view, but different approaches are found in the literature. Andrew Hopkins based his criticism upon his evidence collected in the vicinity of "bad decisions". The Groth commission and the PSA related their view to regulations and risk management guidelines. Hopkins sees the balance between risk based and prescriptive based regulations as a pendulum in which he advocates stronger emphasis on prescriptive regulation (Hopkins, 2011). One might expect that organizations with highly professional personnel with clear tasks in a well structured environment need less prescriptive regulations, but it is also possible to argue that some values are so important that they should be protected and supported by prescriptive regulations and clear norms. A prescriptive regulatory regime must at least make allowance for continuous development on the basis of contemporary and relevant scientific knowledge. In the same way corporate risk analyses must not be confined to the presentation of a static, once-upon-a-time picture of the risk in an enterprise.

The Groth commission has not argued for, or substantiated its opposing or alternative views on risk management. It is accordingly difficult to assess how they assess the expected performance of a safety management system within the enterprises investigated.

The report from AIBN on the Alnabru/Sjursøya-accident criticizes the use of risk analyses in mainly three directions: Firstly the lack of establishing an updated picture of the total risk, secondly the lack of analyses of possible barriers and thirdly they doubt the ability for quantitative analyses to catch the complexity of the risk picture. These deficiencies may be interpreted as serious obstacles for establishing a well functioning system for risk governance.

As risk analyses presume to say something about the future, it is difficult to see that any particular risk analysis can be judged as right or wrong. At least it cannot be done alone on the basis of hindsight as to what really happened in the aftermath of the analysis. That said, risk analyses can still be judged as good or bad.

We contend that a good risk analysis, for either managerial or for learning purposes, must possess the following properties:

1. The analysis must *invent* a risk image based on up to date knowledge and subsequent attempts to construct valid causal relationships between identified and shared opinions on threats and hazards and connected consequences.

2. The analysis must encourage *sharing* of the risk image among the relevant actors, and give them the opportunity to comment upon identified threats and hazards as well as connected consequences.

3. The analysis must establish a platform for *continuing development* of the risk image so that the risk image depicts the current operational situation in a valid way.

All four cases selected for this study encompass formulations of risk analysis and risk management. In the investigations discussed here the investigators' understanding of risk analysis and risk management gets a prominent role. In the Texas City case, risk management practices relating to the three fatal decisions were discussed and partly criticized, but not the contents and the possible consequences of the TRAs as planning, decision making and design tools. The investigators of the Åsta accident and the Oseberg accident criticized the lack of previous risk analyses and risk management activities, but did not relate the potential of such analyses to the specific incidents.

ACKNOWLEDGMENT

The work in this article is part of the ACCILEARN project, which is financially supported by the Norwegian Research Council, SAMRISK program. The support is gratefully acknowledged.

REFERENCES

AIBN. (2011). Rapport om jernbaneulykke med vognstamme i utilsiktet drift fra Alnabru til Sydhavna 24. mars 2010 [Alnabru – Sydhavna accident]. Lillestrøm: Accident Investigation Board Norway.

Andersen, S. S. (1997). Case-studier og generalisering: forskningsstrategi og design [Case studies and generalisation: research strategy and design]. Bergen: Fagbokforlaget.

Aven, T., & Vinnem, J. E. (2005). On the use of risk acceptance criteria in the offshore oil and gas industry. *Reliability Engineering & System Safety, 90*(1), 15-24.

Baker, J. A., Bowman, F. L., Erwin, G., Gorton, S., Hendershot, D., Leveson, N., et al. (2007). *The Report of the BP U.S. Refineries Independent Safety Review Panel*: The BP U.S. Refineries Independent Safety Review Panel.

Braut, G. S. (2003). Public legislation and professional self-regulation: quality and safety efforts in Norwegian health care. In M. Hatlie & B. J. Youngberg (Eds.), *The patient safety handbook.* Boston: Jones and Bartlett.

Braut, G. S., & Njå, O. (2009). Learning from accidents (incidents). Theoretical perspectives on investigation reports as educational tools. In R. Briš, C. Guedes Soares & S. Martorell (Eds.), *Reliability, Risk and Safety. Theory and Applications* (pp. 9-16). London: Taylor & Francis Group.

CAIB. (2003). *Report Volume I*. Washington DC: Columbia Accident Investigation Board.

Flyvbjerg, B. (2004). Five misunderstandings about case-study research. In C. Seale, G. Gobo, J. F. Gubrium & D. Silverman (Eds.), *Qualitative Research Practice*. London: Sage.

Giddens, A. (1991). Modernity and self-identity: self and society in the late modern age. Stanford, Calif.: Stanford University Press.

Graham, B., Reilly, W. K., Beinecke, F., Boesch, D. F., Garcia, T. D., Murray, C. A., et al. (2011). *Deep Water. The Gulf Oil Disaster and the Future of Offshore Drilling. Report to the President*. Washington DC: National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling.

Hollnagel, E. (2010). *On How to (Not) Learn from Accidents*. Paper presented at the Ulykkesgranskning og læring [Accident investigation and learning]. Retrieved from http://www.uis.no/getfile.php/Konferanser/Presentasjoner/Ulykkesgransking%202010/EH_AcciLearn_short.pdf

Hopkins, A. (2010). Failure to learn: the BP Texas City refinery disaster. Sydney: CCH Australia Limited.

Hopkins, A. (2011). Risk-management and rule-compliance: Decision-making in hazardous industries. *Safety Science, 49*(2), 110-120.

Kaarbo, J., & Beasley, R. K. (1999). A practical guide to the comparative case study method in political psychology. *Political Psychology, 20*(2), 369-391.

La Porte, T., & Consolini, P. M. (1991). Working in Practice but Not in Theory: Theoretical Challenges of High Reliability Organizations. *Journal of Public Administration Research and Theory, 1*(1), 19-47.

Lindøe, P. H., & Braut, G. S. (2009). Risk regulation in the Norwegian petroleum industry: Robustness and changing methods of operation. In R. Briš, C. Guedes Soares & S. Martorell (Eds.), *Reliability, Risk and Safety. Theory and Applications* (Vol. 3, pp. 2247-2253). London: Taylor & Francis Group.

Lundberg, J., Rollenhagen, C., & Hollnagel, E. (2009). What-You-Look-For-Is-What-You-Find - The consequences of underlying accident models in eight accident investigation manuals. *Safety Science, 47*(10), 1297-1311.

Marone, J. G., & Woodhouse, E. J. (1986). *Averting Catastrophe: Strategies for Regulating Risky Technologies*. Berkeley: University of California Press.

Njå, O. (2002). *Issues and judgements in accident investigation*. Paper presented at the The International Emergency Management Society (TIEMS), Waterloo, Canada.

NORSOK Z-013. (2001). Risk and emergency preparedness analysis, *Rev. 2*. Oslo: Norwegian Technology Centre.

NoU. (2000). *Åsta-ulykken, 4. januar 2000. [The Åsta accident, January 4th, 2000]* (No. Report NoU 2000: 30, submitted to the Ministry of Justice and Police by the government appointed committee on November 6th 2000). Oslo: Ministry of Justice and Police.

NS 5814. (2008). Krav til risikovurderinger [Requirements for risk assessment]. Oslo: Standards Norway.

Ochs, E. (1997). Narrative. In T. A. van Dijk (Ed.), *Discourse as Structure and Process*: Sage Publications.

Perrow, C. (1984). Normal accidents : living with high-risk technologies. New York: Basic Books.

PSA. (2009). Hydro carbon leakage on Oseberg C 12.9.2008 [Hydrokarbonlekkasje på Oseberg C]. Stavanger: Petroleum Safety Authority Norway.

PSA. (2011). *GUIDELINES REGARDING THE MANAGEMENT REGULATIONS*. Retrieved from http://www.ptil.no/getfile.php/Regelverket/Styringsforskriften_veiledning_e.pdf.

Reason, J. (1997). Managing the risks of organizational accidents. Aldershot: Ashgate.

Roberts, K. H. (1989). New Challenges in Organization Research: High Reliability Org anizations. *Industrial Crisis Quarterly, 3*(2), 111-125.

StatoilHydro. (2008). Oseberg C. Gas leakage from pressure equalizing line 12.09.2008 [Gasslekasje fra trykkutjevningslinje]. CONFIDENTIAL. Stavanger, Norway: StatoilHydro.

Watson, S. R. (1994). The meaning of probability in probabilistic safety analysis. *Reliability Engineering and System Safety, 45*, 261-269.

Yin, R. K. (1994). *Case study research: design and methods*. Thousand Oaks, Calif.: Sage.