DET NORSKE VERITAS (USA), INC.
Division Americas
1 International Blvd.
Suite 1200
Mahwah, NJ 07495
Tel: 201-512-8900
Fax: 201-513-8901
http://www.dnv.com

United States Department of Interior
Att. Regulations and Standards Branch
Bureau of Ocean Energy Management, Regulation and Enforcement
381 Elsen Street, MS-4024
Herndon, VA 20170-4817

Your ref.:	Our ref.:	Date:
	ASTUSBECO111114-1	11/14/2011

Revisions To Safety and Environmental Management Systems, Docket BOEM-2011-0003

Dear Sir or Madam:

DNV is a global provider of services for managing risk, with safeguarding life, property and the environment as our purpose. Organized as an independent and autonomous foundation with no proprietors, DNV balances the needs of business and society, based on its independence and integrity.

DNV serves a range of high-risk industries, with a special focus on the maritime and energy sectors. In addition, DNV has expert knowledge in pipeline safety, renewable energy (especially wind and solar), and climate change.

DNV has been authorized by governments and national authorities to provide services in countries worldwide, including independent investigations, audits and surveys, especially within in the area of advanced technologies.

Established in 1864, the company has a global presence with a network of 300 offices in 100 countries, and is headquartered in Oslo, Norway. Our prime assets are the knowledge and expertise of its 9,000 employees from more than 80 nations. In the US, DNV has more than 700 employees, of which about half are based in Houston. DNV has operated in the US since 1898.

DNV has reviewed the proposed rule for "Oil and Gas Sulphur Operations in the Outer Continental Shelf – Revisions to Safety and Environmental Management Systems and appreciates this opportunity to comment on the proposed regulatory amendment.

- The six new requirements: Stop Work Authority, Ultimate Work Authority, Employee Participation, Reporting of Unsafe Work Conditions, Independent Third Party Audits and Job Safety Analysis may contribute to increased effectiveness of Safety and Management Systems.
- Section 250.1902. DNV does not believe, however, that the proposed regulations fully draw upon the learning and best practices from Process Safety Management to handle

low-frequency, high-consequence events, which often become large disasters. Process safety requires more than a Safety and Environmental Management System (SEMS) and the 6 new elements. DNV proposes that the regulations should also require that safety critical elements, their performance requirements and the barrier management for all operations must be identified, described and managed based upon process safety management principles. This will effectively address the low-probability, high consequence events which management systems do not fully consider. Process safety in some geographic areas, such as the North Sea, has improved greatly as more emphasis is placed on safety critical elements. For example, an auditor review of safety critical elements should consider the functionality, the date and results of the last inspection and test, maintenance records, and site and facility specific training for personnel. DNV recognizes that a Safety Case is necessary to identify the safety critical elements.

- Section 250.1911. Job Safety Assessments (JSA) are more related to occupational safety than process safety. For example, the JSA for a welding job typically considers safety for the individual and others. The larger risks, such as a pipeline break or vessel burst, or the consequences of disabling safety barriers are not typically evaluated as they would be in a safety case. The JSA may require that the fire alarm system is disabled during x-ray examinations, but without a safety case, it is not likely that the JSA will also consider the larger impact of disabling a key safety barrier.
- Section 250.1920 (a). DNV recommends that BSEE consider more sophisticated techniques than audit techniques of API RP 75 to verify implementation of the SEMS. The International Safety Rating System protocol considers both the requirements for each element of the SEMS and, equally important, scoring guidelines. For example, where the SEMS requires a safety meeting, the ISRS would detail what items should be included in the safety meeting agendas, the frequency for the meetings and a quantitative scoring system for each. Best practices and recommendations for improvement are embedded in the scoring system.
- Section 250.1926. DNV recommends that BSEE's approval of auditors and organizations recognizes the benefits of large independent organizations to conduct audits. It is beneficial for auditors to be part of a larger competent organization, for larger organizations to provide proper training, for larger organizations to maintain global records and data bases, and for larger organizations to provide a wider number of auditors with additional competencies. In addition, larger organizations also have first-hand knowledge and experience with global trends, best practices and technology. DNV further recommends that the requirements to avoid a conflict of interest are clarified so that completely separate persons within an independent third party organization may conduct either audits or develop and maintain a SEMS, but not both.
- Section 250.1926 (c). DNV proposes that independent third party auditors and organizations are pre-approved by BSEE rather than singular nomination and approval actions. This will prevent delays to the audit process, allow the necessary flexibility for last minute changes or to add specialized competence to the audit team.

- Under National Environmental Policy Act of 1969 (FR 56691 (c)), there is a claim that SEMS will improve OCS safety, but it is not clear how much and if the improvement will be in occupational safety, process safety or both. In DNV's opinion, the main focus of SEMS is occupational safety, not process safety. DNV notes that OSHA 1910 has improved occupational safety, but not process safety. Indeed, if process safety is not explicitly addressed, process safety improvements are not achieved.

Enclosure (1), Achieving Excellence is Process Safety Management Through People, Process and Plant is submitted to provide additional information about process safety.

Enclosure (2), Key Aspects of an Effective U.S. Offshore Safety Regime, is submitted to provide recommendations for an effective U.S. Offshore Safety Regime, including a blend of prescriptive and performance based regulations and balancing risks, controls and conditions to achieve safe offshore operations.

Enclosure (3), OTC OTC-20415-PP, Barrier Diagrams the Next Stage for Enhancing Offshore Operations Safety is submitted to describe how process safety may be improved by using bow tie risk management tools.

Thank you for your consideration. I will be pleased to provide any additional information.

Yours faithfully
for DET NORSKE VERITAS (USA), INC.

Blaine Collins
Director of External Affairs

Enclosures - 3

ENCLOSURE (1)

ACHIEVING EXCELLENCE

in Process Safety Management through people, process and plant

While tremendous progress has been made within occupational safety and environmental emissions, the hydrocarbon processing industry has not yet managed to reduce the occurrence of major accidents. Solving this critical issue will require a clearer understanding of potential root causes and of managing incidents.

[AUTHORS]

Graham Bennett
TITLE Director, DNV Energy
DESCRIPTION Segment Director Refining and Petrochemicals. Specialises in refinery risk management and Process Safety Management
EMAIL graham.bennett@dnv.com

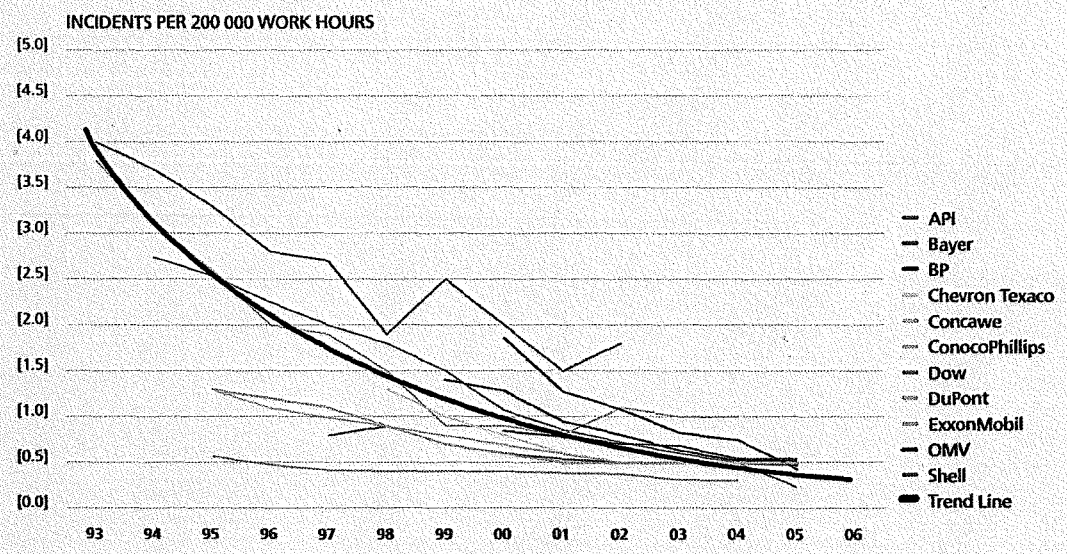
Iain Wilson
TITLE Project Manager Risk Intelligence Centre, DNV Energy
DESCRIPTION Principal Consultant with extensive experience of safety engineering, risk assessment and risk management in the oil, gas and process industries
EMAIL iain.wilson@dnv.com

We live in an age where satellite communications, the internet, and 24 hour rolling news media can instantly broadcast incidents to the rest of the world. Anyone involved in the hydrocarbon processing industry will recognise this reality. Today, perhaps more than ever, the industry finds itself the subject of a wide range of legislative requirements, and under increasing scrutiny from society at large. Much of the legislative burden and the adverse publicity have come about as a result of a series of well-publicised accidents that have occurred in both the refining and chemicals sector, and the recent high profile investigations into the culture of this industry that have followed (Ref. 1). In this article we will examine some of the underlying trends relating to those accidents, identify lessons to be learnt, challenge some existing paradigms, and identify opportunities for the future.

The persistent challenge of major accidents

Over the last 10 to 15 years, the downstream process industries around the world have made tremendous improvements in the areas of occupational (personal) safety and environmental emissions. Standard industry measures such as Lost Time Injuries (LTI), or Recordable Accident Rates (RAR) all show dramatic reductions in incident rates, with industry leaders in the USA and Europe showing reductions of 50 to 75% in reported rates. *Figure 1* shows how the industry

Figure 1. **RECENT TREND IN REPORTABLE INCIDENTS**

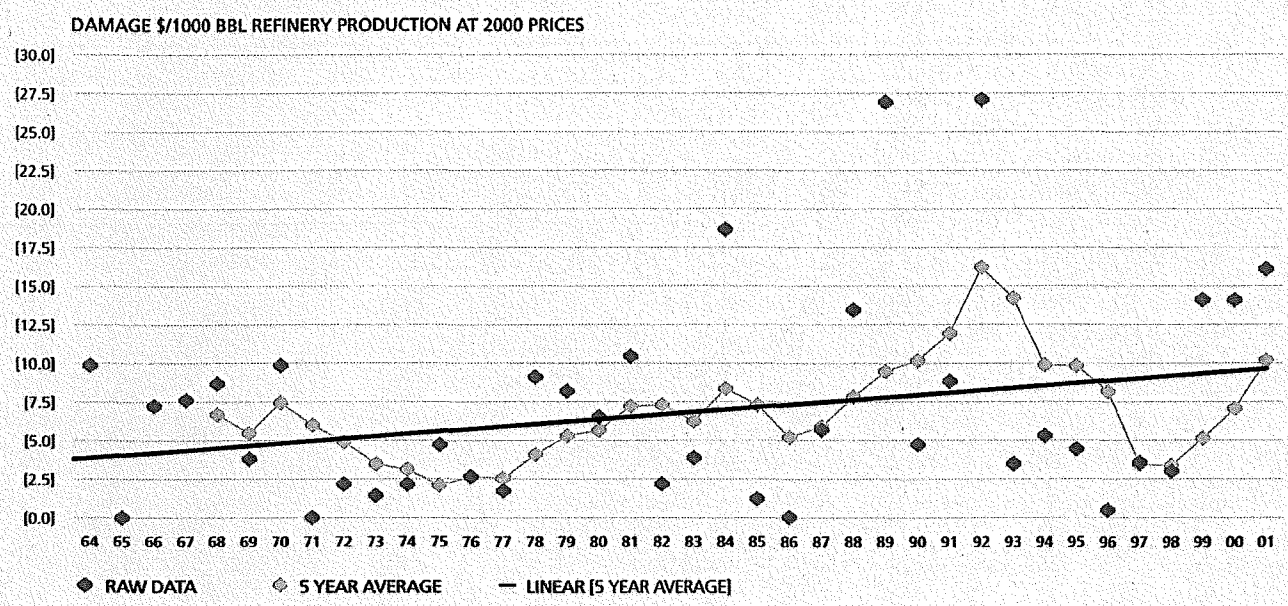


The source: Analysis of company public reports completed by DNV.

has improved its performance in Total Recordable Injuries (TRI) over the last 15 years. The low levels of recordable lost time incidents and the need for a more significant measure to monitor trends, have led many companies to start using Medical Treatment Cases (MTC) as an indicator of how well they are performing in managing occupational risks. The industry quite rightly deserves to be congratulated for its achievements in this respect.

When examining major accident events over the same period however, a very different picture emerges. Unfortunately, the industry has continued to experience large scale, process related accidents, resulting in fires, explosions or releases of toxic, or ecotoxic materials. An analysis of refinery losses conducted by DNV (Ref. 2) reviewed over 400 refinery accidents over a 40 year period, and showed a trend of rising losses over the period (with all values normalised to year 2000 values, and to refining capacity in terms of number of barrels processed). *Figure 2* is derived from this work and shows how the refining industry has performed in terms of its annual losses arising from major accidents. Note that the data used for the graph does not yet include the final costs of incidents such as Texas City or Buncefield. The graph takes into account the frequency of events, their associated costs, and the change in refinery capacity over the same period. Losses are expressed in terms of US$ per thousand barrels of distillation capacity. Some very costly single accidents tend

Figure 2. **HISTORICAL TREND IN REFINERY MATERIAL DAMAGE COSTS**



"In the last 3 years alone, the total loss from refinery and petrochemical incidents around the world has exceeded US$1 billion."

to obscure the picture, so a 5 year moving average plot has been added to the graph to indicate the trend. A linear fit to the annual cost data on the graph also shows a rise over the period. The data analysed in the report also indicates that for every major release event, resulting in asset damage, there are several events that resulted in lost production opportunities or significant plant downtime that are not included in the insured loss figures of the graph.

In the last 3 years alone, the total loss from refinery and petrochemical incidents around the world has exceeded US$1 billion. Many of these incidents did not involve fatalities or even serious injuries, but did result in significant production losses and asset damage. A review by the UK Health and Safety Executive (HSE) of accidents in the UK (Ref. 3) gives examples of cases where the business interruption costs are more than twice the costs associated with the asset damage. This review also found that 17 out of the top 20 highest financial loss cases in the UK resulted in no fatalities. This does not of course suggest that we should be complacent about fatality risks. It just serves to remind us how the use of injury/fatality statistics alone can disguise underlying trends in incident rates and costs.

Understanding cause and effect relationships

Much effort has been expended in identifying, recording and investigating 'smaller' events such as those which result in property damage only, or those

that are sometimes called 'near miss' events which cause no loss, but only through providence. The theory is that these smaller events are the precursors to the major accident hazards that industry is aiming to eliminate. Whilst this theory is accurate for occupational events, the level of understanding of the cause and effect relationships in major hazard events has largely been insufficient to change the number or scale of major accident events in recent times.

In fact, despite the intense focus on safety in the process industry over many years, the number of major accidents continues to be significant. In 2005, DNV set up a database to track and record accidents and incidents in the process industry. Since its inception there have been over 1,800 incidents recorded, which include:

INCIDENT TYPE	NUMBER RECORDED
Loss of containment	*745*
Fire	*538*
Explosion	*369*
Environmental release off site	*44*

Which led to the following consequences:

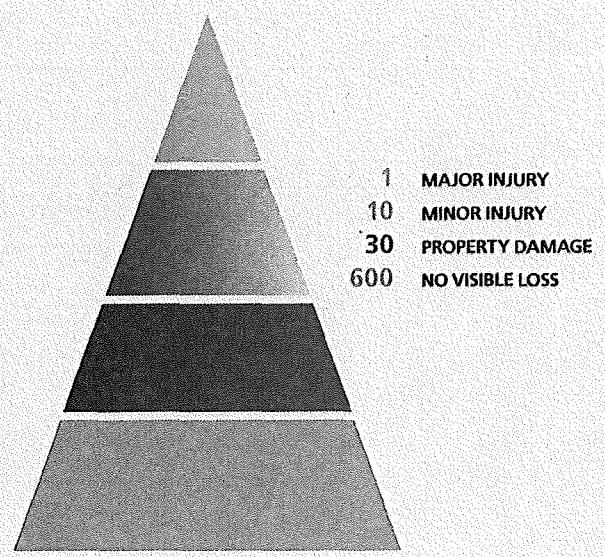
CONSEQUENCE	NUMBER
Loss of life/injury	*169**
Site evacuation	*114*
Regulatory fine	*674*
Production downtime > 10 days	*219*

*These 169 incidents resulted in injury to 721 people, 155 of the events resulted in loss of life (a total of 298 deaths).

Considering that there are around 600 operational oil refineries worldwide, the above data suggests a major loss of containment occurring on average once every 3 years and a major fire occurring once every 5 years on each facility.

A review of the number of incidents and trends for industries other than refining and petrochemical is contained in Appendix I.

Figure 3. **TYPICAL ACCIDENT PYRAMID**



"The understanding of the number, nature, reliability and effectiveness of these barriers is the essence of process safety management."

The hypothesis driving improvement efforts over many years has been the concept of a predictable ratio of incident outcome severities often referred to as an 'accident pyramid'. *Figure 3* shows a standard accident pyramid.

Conventional wisdom has suggested that by acting to shrink the base of the pyramid, the values at the apex will also decrease in proportion, as illustrated in *Figure 4.*

Unfortunately the lack of understanding of the different mechanisms which contribute to both low consequence and major accident events has resulted in a reality more closely represented by *Figure 5.*

Figure 4. **DESIRED ACCIDENT PYRAMID**

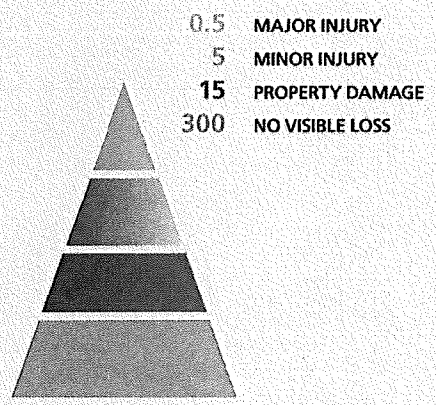
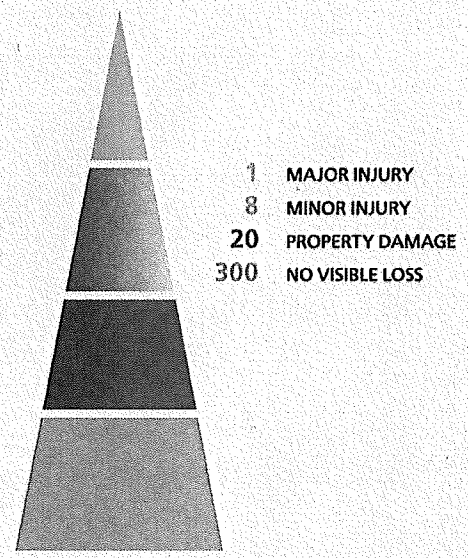


Figure 5. **ACCIDENT PYRAMID WITH OCCUPATIONAL SAFETY FOCUS**



Focus on occupational safety has reduced the smaller events, but the major accidents, driven by process safety shortcomings, continue to occur.

Managing process safety requires a different approach

The Centre for Chemical Process Safety (CCPS) (Ref. 4) defines Process Safety Management (PSM) as: 'The application of management principles and systems to the identification, understanding and control of process hazards in order to prevent process related injuries and incidents'.

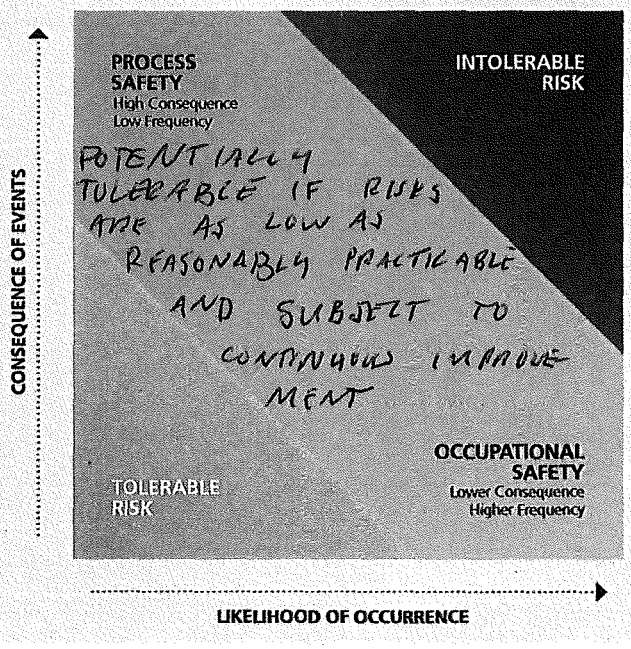
A more concise definition could be: 'Keeping the process fluids inside the piping and equipment'.

Managing process safety is significantly different from, and more difficult, than managing occupational safety. The relationship between likelihood and consequence is very different as illustrated in *Figure 6.*

The management of process safety is more problematic than managing occupational safety for a number of reasons:

- Major process events are (fortunately) outside the range of experience of most people. In order for a process safety event to occur, a number of 'barriers' need to fail. This leads to an incomplete or inadequate 'mental model' of the complex pathways to the event and the development of the event once it occurs. By contrast, occupational incidents such as slips, trips and falls are familiar to all, and the causes and outcomes are readily imagined. As a result, hazard review teams frequently underestimate frequency and consequence of process safety events.
- Due to the complexity described above, specialist tools are required both to establish the potential pathways and to evaluate the potential frequency and consequence of incidents.
- Process safety scenarios can have potentially catastrophic consequences which, due to factors such as 'Risk Aversion' and 'Dread', may require significant risk management intervention despite extremely low likelihood of occurrence.

Figure 6. **RELATIONSHIP BETWEEN OCCUPATIONAL AND PROCESS SAFETY**



- Major process events have significant business impacts and can threaten the viability of the enterprise, although the true costs of a major event are not always understood by hazard review teams.

Process safety management is complex because it must encompass:

- Many drivers – reputation, strategic plans, license to operate
- Many interfaces – functions, stake holders, systems
- Many resources – people, knowledge, finance
- Many times – a lifecycle approach

It is essential to take a holistic view of the management of major accident hazards by recognising that all areas of the business – from HSE, to asset management and supply chain management – have critical roles to play in ensuring Process Safety Management.

Understanding how barriers work

The only way in which process safety can be successfully managed is by developing a clear understanding of the potential causes, development and outcomes of each scenario.

The concept that accidents occur as a result of a chain of events rather than a single action has been recognised since Heinrich's Domino Theory (Ref. 5) was published in 1931. This concept has been used in various forms for purposes such as incident investigation and has evolved to encompass modern management concepts and technology.

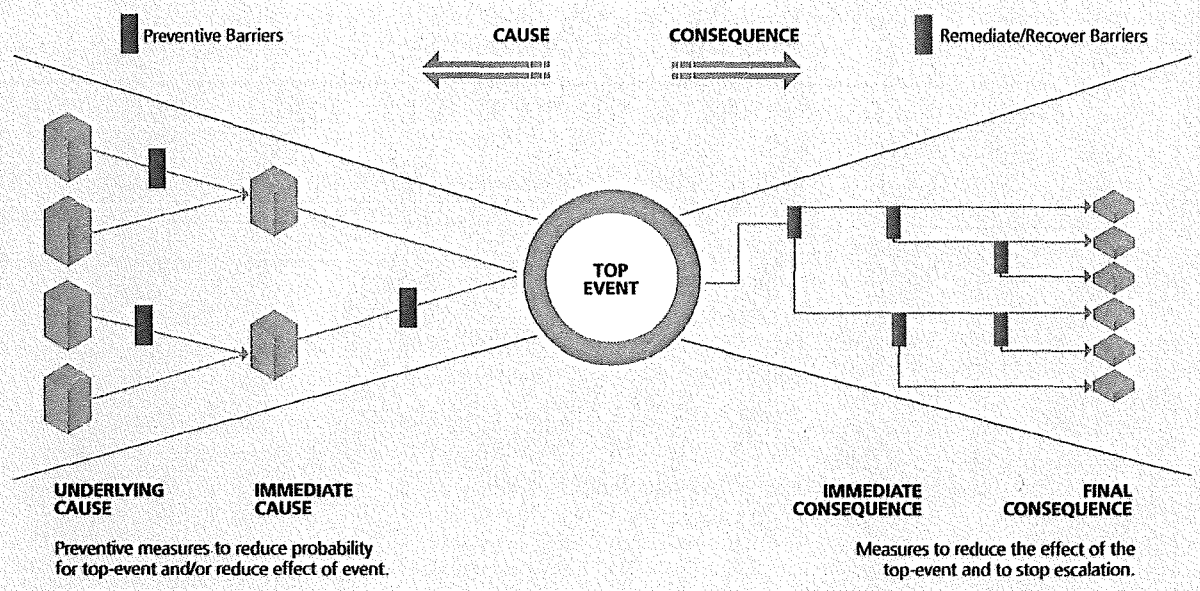
In order to represent the managing factors relating to any potential incident, the Domino theory can be combined with the more recent but similarly framed formulation of the 'Swiss Cheese Model' by Reason in 1990 (Ref. 6). The representation of the hazard management process is known as a 'Bow Tie' and is illustrated in *Figure 7.*

Bow ties reflect the multiple causation analysis of the domino theory by considering underlying and immediate causes and also by considering the multiplicity of potential outcomes. Also, part of this system are barriers which exist within the system to manage the hazard. They are integrated into the process to illustrate how plant, process and people interact to prevent, detect, control, mitigate and recover from the incident. The Swiss Cheese model is applied in the recognition that none of the barriers are either 100% reliable or 100% effective. In reality, barriers rarely fail completely, they degrade over time. Failures are usually readily detectable, it is the degradation effect that is harder to detect and manage, and requires greater management vigilance as a result.

The understanding of the number, nature, reliability and effectiveness of these barriers is the essence of Process Safety Management. In DNV we sometimes refer to this as solving the PSM P3 puzzle of People, Process and Plant. As with any puzzle, the PSM puzzle can appear daunting, but with a few simple rules, and some guidance, it can be solved.

Existing major hazard management is largely focussed on the maintenance of protective systems. Classical Quantitative Risk Assessment (QRA) approaches emphasise the consequence aspect rather than the frequency aspect, as the industry has historically been poor in collating good quality leak frequency data. As a result, many protection systems have

Figure 7. **BOW TIE MODEL**



been developed and installed to mitigate the consequences of an event. A more holistic approach should however place equal emphasis on driving improvements in integrity management, developing effective leadership and achieving a solid understanding of the hazards of the plant and equipment. The effectiveness of such a system should be monitored using a combination of leading and lagging indicators.

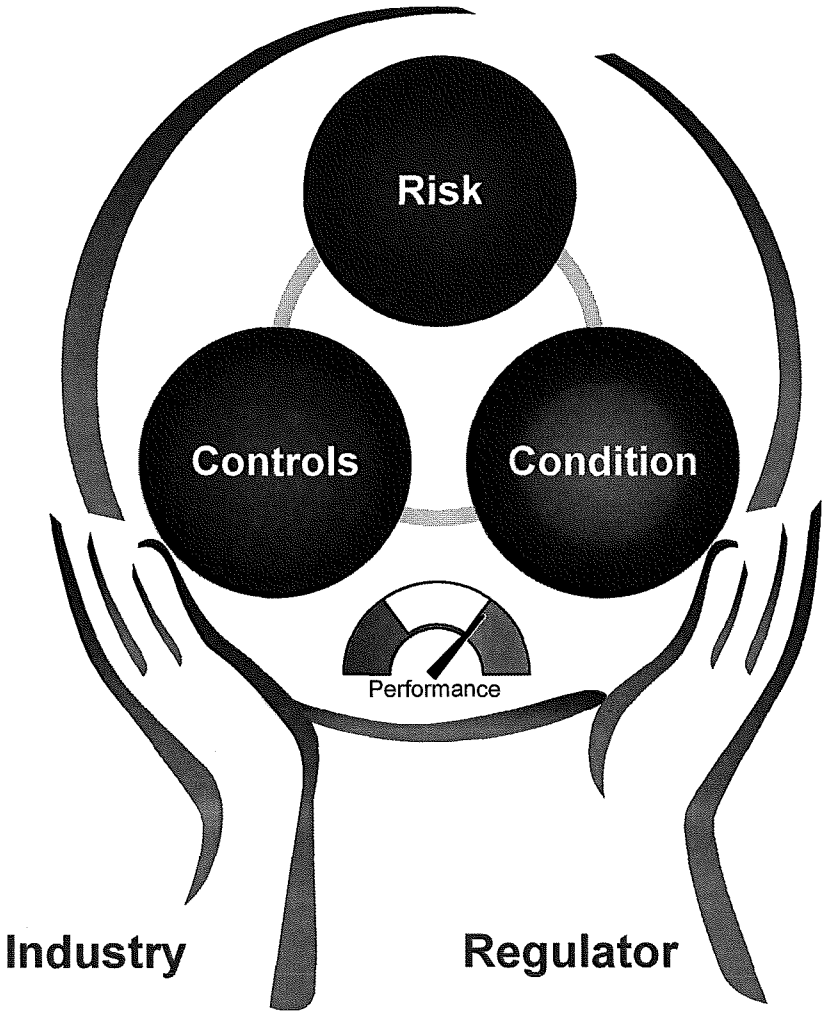
Applying an integrated approach

Issues related to the management of major accident hazards will not be solved overnight. It will require the industry to adopt a more integrated approach to the management of major accident hazards, which considers not just the consequences of failure, but also the likelihood of failure, and the factors influencing event likelihood and development. Asset integrity management, management systems, inherently safer designs, and organisational factors will all need to be improved if the industry is to learn the lessons from the occupational safety achievements, and translate them into process safety improvements.

References

1. The BP US Independent Refineries Independent Safety Review Panel, Jan. 2007 (The Baker Report)
2. DNV (2002), 'Accident Risks at Onshore Process Plants Based on Historical Data' for DNV Safety Health & Environmental Risk Management, Internal Project, October 2002.
3. Fewtrell P, 'A Review of High Cost Chemical/ Petrochemical Accidents since Flixborough 1974', IChemE Loss Prevention Bulletin, April 1998 no. 140.
4. CCPS, 'Guidelines for Auditing Process Safety Management Systems', 1992
5. H.W.Heinrich, 'Industrial Accident Prevention: A Scientific Approach', 1931
6. J. Reason, 'Human Error', 1990

ENCLOSURE (2)



Key Aspects of an Effective U.S. Offshore Safety Regime

DET NORSKE VERITAS

Key Aspects of an Effective U.S. Offshore Safety Regime

	Page
1. Introduction	1
2. Objective of an offshore safety regime	2
3. Performance-based supplemented by prescriptive regulation	2
4. Consideration of technology, organization and people	3
5. Clear roles and responsibilities	4
6. Enforced identification, reduction and control of risks	4
7. Shared performance monitoring	5
8. Practical and economic feasibility	5
9. A step change for major accidents	5
10. Balance between risk, control and condition	6
11. Conclusion	7
Appendix on risk models	8
About DNV	12

1. Introduction

Major accidents lead to a review and revision of current practices and regulations with the objective of avoiding similar or other major accidents in the future. This also appears to be the case after the tragic Deepwater Horizon blow-out accident and subsequent oil spill. This paper presents DNV's view on key aspects of an effective offshore safety[1] regime. The paper is meant as a contribution to the on-going discussion on how to improve safety and environmental protection during offshore oil and gas exploration, development and production. The paper supports and complements the recommendation for a more systematic approach to safety and environment in the U.S. Department of the Interior (DOI) report on "Increased Safety Measures for Energy Development on the Outer Continental Shelf" (May 27, 2010).

DNV[2] believes that a *step change* can be achieved with respect to prevention and mitigation of major accidents through an effective and efficient safety regime for offshore energy exploration, development and production. Such a safety regime must be risk-informed, balancing the inherent risks with the benefits for society and must possess the following characteristics discussed in this paper

- Performance-based supplemented by prescriptive regulation
- Consideration of technology, organization and people
- Clear roles and responsibilities
- Enforced identification, reduction and control of risks
- Shared performance monitoring
- Practical and economic feasibility
- Balance between risk, control and condition

DNV has world wide experience within risk management in the offshore energy and maritime industries. DNV advises regulators on offshore safety regulation as well as executing key functions on behalf of authorities and industry in order to safeguard life, property and the environment. This paper does not present the many ways in which the key aspects could be implemented within law and regulation or how they are effectively institutionalized, or which roles are best managed by governmental agencies and which by

[1] Safety in this paper often covers all aspects related to health, safety and the environment (HSE)

[2] Det Norske Veritas (www.dnv.com) is a global foundation with the purpose of safeguarding life, property and the environment. DNV is the leading company for oil & gas risk assessment globally. It was founded in 1864 in Norway and currently has 9.000 employees, of which about 10% are based in North America. See also Appendix II.

independent or private organizations. The paper does, however, highlight issues and methodologies that DNV believe regulators should take into account when promulgating new legislation.

2. Objective of an offshore safety regime

Oil and gas will constitute the major part of the U.S. energy supply in the foreseeable future despite on-going and needed efforts in developing renewable and other alternative energy sources to meet our energy demand and limit carbon emissions. In addition, deep water exploration and production of oil and gas will continue to be a vital part of our oil and gas supply. Because of this, additional focus on managing risk of deep water activities is needed to prevent consequences such as those from the Deepwater Horizon accident.

Following a major accident we have an obligation to review and revise as needed the offshore safety regime under which oil exploration and production takes place with the objective to

- Ensure that exploration and production activity is done safely and in a sustainable manner, and
- Assure all stakeholders – foremost the public – that activities that pose a threat to life, environment and property are properly controlled

DNV believes that a safety regime for offshore energy exploration and production must ensure that

- Life, environment and property are protected in an effective, consistent, transparent and predictable way; both for those directly affected and involved in offshore operations, but also for those otherwise affected by an accident, such as fisheries, recreation and the whole ecosystem
- Risks are properly evaluated and all prevention and mitigation measures are identified
- Control measures are implemented and maintained by all parties in accordance with mandatory risk assessments as well as what is prescribed by regulation
- Conditions of safeguards, facilities, procedures, personnel and organizations are continuously monitored throughout the lifetime for proper functioning and compliance with all regulatory requirements and to assure that risks do not increase
- Technical innovation and efficiency improvements can be implemented safely and responsibly

3. Performance-based supplemented by prescriptive regulation

The safety regime must benefit from all learning of the past. This is the traditional way of developing safety regulations where previous events lead to new knowledge and additional regulation that prescribes a set of requirements for industry to follow. In most cases, however, regulators and industry do not regularly revise and upgrade procedures, rules and regulations, as the collective knowledge of how to operate safely increases (e.g. Baker Panel[3] findings after Texas City). More often, a major disaster becomes the trigger to update regulations that have been proven to be insufficient.

Every major accident at sea has been followed by new regulation, from maritime oil spill accidents such as Exxon Valdez, Erika and Prestige to offshore oil and gas accidents such as Alexander Kielland, Piper Alpha and now Deepwater Horizon. The same is the case in the chemical process industry where accidents in Bhopal, Seveso, Pasadena Texas and Texas City led to new US and EU regulations. The potential weakness from such regulatory development is that issues of the moment rather than long term sound policy become dominant and that all focus is on the specific event and root causes with insufficient focus on other possible, future hazards.

An offshore safety regime based on prescriptive regulation has the advantage of being relatively easy and simple to implement and follow up but has the weakness that it may not prevent new types of accidents that may appear in the future and it often prevents innovation due to its specific, prescriptive rules and

[3] The Baker Panel was established to investigate safety management systems and safety culture after the Texas City disaster – they laid out many important concepts for enhanced major accident prevention

requirements. It may also limit operators' dedication and understanding of responsibility as well as proactive initiatives to increase the safety level beyond compliance. This is particularly important in the deep water offshore arena where new technologies and techniques to improve production and safety and also reduce costs are being constantly developed, but by their nature may introduce potential new risks.

To be able to account for new types of events and to allow for needed innovation and new technology in the future, performance-based (also referred to as functional-based or goal-based) safety regimes have been introduced in several countries. In these, performance requirements and acceptance criteria are specified and industry must document that their specific solutions meet such requirements, e.g. in terms of acceptable risk levels. The advantage of performance-based regulation is that solutions for the problem at hand can be developed free of specific prescriptions. The regulation will include comprehensive safety – or HSE – cases that document how all risks (including novel risks) for the specific facility, operational conditions and location will be prevented or mitigated. A challenge of a pure performance-based regulation is that it may require more analysis and documentation to be done in each individual case to verify that performance goals are met. It also requires a competent and active regulator.

The current safety regime for the U.S. Gulf of Mexico is largely a prescriptive regulation with no requirement for safety cases[4] to be performed. The offshore safety regimes in the UK and Norway, for example, are of the performance-based type where safety cases (UK) or detailed risk assessments (Norway) must be presented to the authorities who review and accept - rather than approve - these before implementation. Once accepted, operations not in conformance with the safety case is an offence.

DNV believes that an offshore safety regime based on a performance-based regulation requiring safety cases including risk assessments *supplemented* by required or recommended specific prescriptive regulation for *selected* areas is the most effective regime model. Areas that may be addressed by prescriptive regulation are typical facilities, components and situations where experience exists. The prescriptive regulation may include specific requirements supplemented e.g. by API standards and class societies such as DNV Offshore Codes.

The safety regime must ensure a safe operation of the offshore facility throughout its lifetime. The safety case performed at the design stage must be implemented in the actual operation of the offshore installation and not just end as a document on a bookshelf. Furthermore, the offshore installation may be modified, it will degrade over time, external loading conditions on structure or process system may change, and the operator and crew may change. Each such change of condition must be monitored and documented as a safety case update as part of the regulated process for ensuring a safe operation.

4. Consideration of technology, organization and people

A complex system such as an offshore drilling or production platform performs safely and reliably only when

1. The technical facility is fit for purpose and works as intended
2. The people operating the facility are trained and competent, also as regards safety culture, and
3. The organization is defined so decisions are made and safe procedures are followed as planned

Within chemical process plants these aspects are often referred to as plant, process and people which all must be fit for purpose and performing accordingly for the process plant to perform safely.

When root causes are identified for major accidents, it generally turns out to be a combination of several factors that lead to the accident – and often a combination of technical, human and organizational failures. Even when it at first appears that it was a technology failure, the root cause analysis may reveal that organizational or human failures e.g. during modifications or maintenance in reality lead to the failure.

[4] A Safety Case is a documented, facility specific, safety and environmental program that identifies all hazards, estimates risks and demonstrates how these are prevented or mitigated to a stringent target level of safety, merging both prescriptive and facility specific requirements. All safeguards are documented, their required performance defined, owners assigned, and means to keep functional at all times specified (e.g. maintenance, competence, etc), and providing a transparent means to verify the conditions.

Organizational and human factors are the dominant root cause factors and together often estimated to constitute up to 80% of the causes for major accidents.

In summary, it is critical that an offshore safety regime properly accounts for technological, organizational and human factor defenses – or barriers[5] – in the prevention and mitigation of accidents throughout the lifetime of the offshore installation.

5. Clear roles and responsibilities

An effective offshore safety regime must ensure that clear roles and responsibilities are established between all parties involved. In particular, the role and responsibility between authority and operator is important. The performance-based regime has been preferred by a number of authorities not least because of its very clear split of responsibilities, where authorities define performance goals and acceptance criteria and the operator has the responsibility to ensure that these performance goals are met. The aim is to force the operator and contractors to take an active role and not lean on authorities to ensure safety. In such a regime the authorities will normally not approve the operator's plans but only review and accept them.

In a prescriptive regime the authorities define implicitly the performance by prescriptive requirements and will furthermore typically approve the operator's plans, in some cases including detailed operations. Although the operator normally will be defined in the regulation to carry the liability for the operation, matters may become unclear if something goes wrong and the authorities have both given specific requirements for the facilities and operation plans as well as approved their implementation. Also, the responsibilities between parties may also vary between different pieces of the regulation. The choice of the performance-based model is therefore natural when authorities want to minimize own risk and liability.

6. Enforced identification, reduction and control of risks

DNV believes that risks such as those related to offshore drilling and operation can only be properly managed if the risks are known and understood by the operator (and subcontractors to operator) of the facility. Therefore, a key element in an offshore safety regime is that all parties are required to take an active role on undertaking holistic risk assessments for a specific installation through which preventive and mitigating means are identified and where all factors mentioned above are included in the safety and environmental models. Furthermore, the regime must ensure that such risk management is maintained throughout the life of the installation and continuously kept up to date to prevent deterioration of barriers that prevent and mitigate risks.

DNV believes that the frequency of major accidents only can be significantly reduced by identifying the risks and the factors influencing these risks through quantified risk assessment where the effect of preventing and mitigation measures can be directly evaluated and compared. This is the means that have been introduced in other industries such as nuclear and aerospace and which have proven successful in reducing major accidents. As mentioned, the current offshore safety regime for the U.S. Gulf of Mexico does not require risk assessment and safety cases to be established. IADC has, however, a recommended approach for a safety case for mobile drilling units. DNV believes that such requirements with extensions must be introduced in the future regulation so that all risks are evaluated throughout the lifetime of the offshore drilling and production activities, including design, construction, installation, operations, maintenance, adaptation of new technologies, modifications and decommissioning.

It should be noted that some operators in the US Gulf of Mexico already perform risk assessments due to their own corporate governance and based on experience from other safety regimes in the world. Furthermore, the challenge of handling an unlimited liability for operators can be met through a systematic risk management approach where active prevention and mitigation barriers are monitored and managed throughout the lifetime.

[5] The term barriers is here used interchangeably with controls or safeguards, which are any technical, human or organizational feature interrupting an accident sequence – either stopping it or reducing its likelihood or consequence or both.

7. Shared performance monitoring

DNV believes that performance monitoring of all factors influencing a safe operation should take place throughout the life time of the facility. The monitoring should include the actual risks updated regularly, the condition of the facility, people and organization as well as the condition of all barriers preventing and mitigating accidents. Such performance monitoring would be a continuous assessment of the total integrity of the operation and ensure that, for example, barriers do not deteriorate.

The performance monitoring should be shared – fully or partly – with all parties participating in the operations such as partners and subcontractors in order for all to benefit from the knowledge of the actual condition. Part of the performance monitoring could be reported as online information to authorities and regulators as part of their oversight function.

8. Practical and economic feasibility

After a major accident there can be a tendency to establish a significant amount of new regulation where all elements may not have an equally good balance between investment and benefits to society. It is important that new regulation is practical and economically feasible in addition to ensuring sufficient safety and environmental protection. DNV recommends that the effectiveness of new regulation should be assessed on basis of a risk assessment where the reduction of risks (reduction of expected loss) due to the new or modified regulation is compared with the investment needed to implement the new or modified regulation.

As has been seen with the Deepwater Horizon accident it can be important that equipment from other parts of the world can be brought into the Gulf without any delay when needed. The regulation in the U.S. Gulf of Mexico should therefore be aligned with international regulation for offshore oil and gas exploration, development and production. Specific requirements needed for the local conditions such as risk of hurricanes should be established and met in addition.

9. A step change for major accidents

DNV believes that a step change for major accidents can be achieved, i.e. that the risk can be reduced by a factor of 10 by use of risk management. The oil, gas and process industries have achieved significant improvements over the past 20 years in occupational safety and limited spills or pollution incidents because companies' safety and environmental management have focused on and measured progress in these areas. However, major accidents in safety, structural failures, explosions and environmental pollution have been more resistant to improvement (e.g. major accidents onshore: Texas City[6] and Longford Australia, and offshore: Piper Alpha and the Montara blowout).

After the Three Mile Island accident, the nuclear industry achieved a step change using better tools, namely formal Probabilistic Risk Analysis, new audit structures from the Institute of Nuclear Power Operations and stricter regulations. The Offshore industry in the UK and in Norway, following two major disasters with more than 100 fatalities each in the 1980's, has also achieved an improvement by using safety cases and quantified risk assessments. Also the aviation sector has been successful in reducing major accidents.

There are important lessons to be learned from these achievements:

- When seeking a step-change, a holistic approach to address technical, procedural, human and organizational and cultural aspects is essential
- A detailed quantified safety and environmental model is necessary to underpin operational decision making to prevent major accidents

[6] Texas City refinery explosion 2005; Longford Australia gas processing facility fire 1998; Piper Alpha North Sea rig explosion and fire 1988, Montara oil well blowout off Northern Territory 2009 – particularly well documented and studied accidents amongst many

10. Balance between risk, control and condition

In the North Sea offshore industry and the commercial nuclear power industry, a detailed risk model is established and, from this model, all hazards are identified and managed to a level commensurate with the risks. In the offshore energy industry, all risks would include at least all safety and environmental risks from topsides infrastructure, subsea arrangements and downhole. This approach has the benefit of being able to reduce risks as they become directly known and the approach therefore provide additional and higher levels of safety and environmental protection.

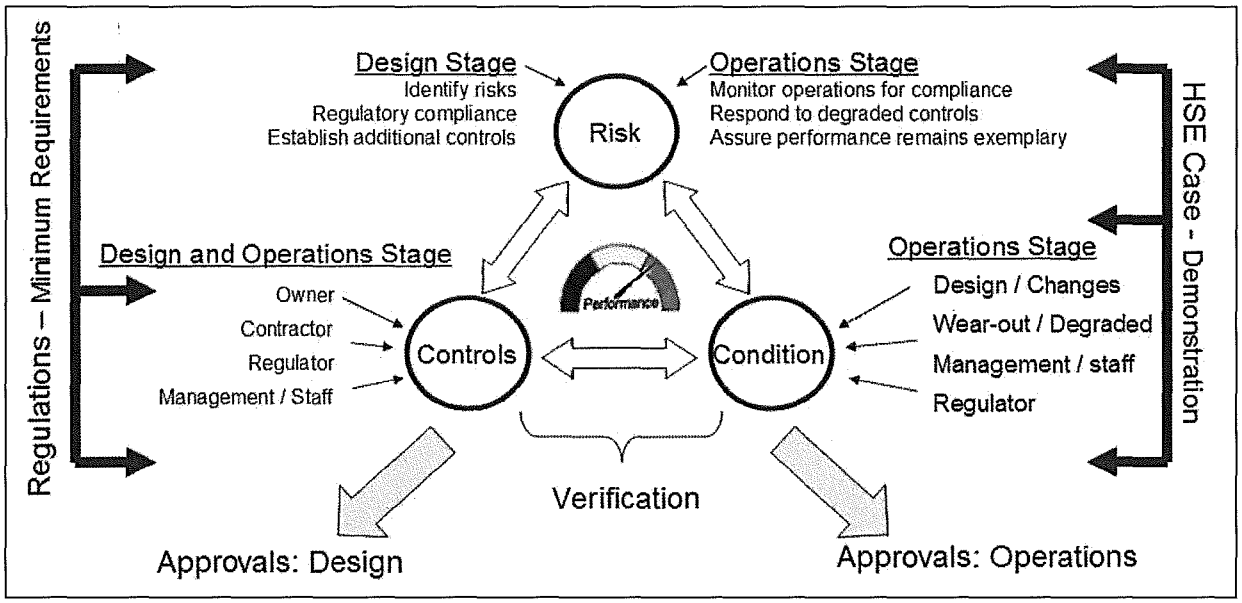


Illustration of the elements Risk, Control and Condition in a risk-informed offshore safety regime

A risk management approach is characterized by three main elements

1. ***Risk: The risk model[7] is the foundation of a safety case***

   - The operator must identify of all risks ranging from high frequency, but small consequences to rare major events with significant consequences, ways and means to prevent these accidents and how to respond if prevention fails. The barrier model – mentioned further in the appendix – is an effective technique to understand prevention and mitigation systems, equipment and operating procedures.
   - The engineering and maritime design must meet current regulations and standards and the safety case must describe the basis for the design and operation.
   - The risk model must have a sound basis and detail. To achieve a step change it must in the design stage be quantified to cover safety and environment risks on the topsides, subsea and downhole. Subsequently, operations procedures may rely on, or require, more qualitative risk models.
   - The risk model is used to establish the required performance of all critical aspects (technical, human and procedural) and these performance standards would be used for verification.

[7] The concepts of a risk model are outlined further in the annex to this paper

2. ***Controls: Effective mechanisms for control must be implemented***

- Ensure that regulatory requirements and safety case commitments are achieved in practice, are documented and communicated to all offshore and onshore staff and contractors
- Ensure that modern safety & environment management system and process safety and safe drilling operations culture programs are in place to institutionalize success and to prevent short term financial Key Performance Indicators from increasing longer term threats
- Verification by an independent, competent party as a key control mechanism both during design and operations

3. ***Condition: The sound condition of all elements must be continuously monitored***

- Complex systems are subject to degradation or failure from the moment of entering service. Processes must be in place to maintain equipment and to ensure that systems meet the required performance standard throughout the life time
- As well as the technical systems may degrade, this is also the case as regards working culture, organization and human competences which must be included in the condition monitoring processes
- Changes in system, organization or people must be assessed, managed, controlled and documented before implementation, with effective processes for returning critical equipment to its current state after temporary changes

It is important to have the right balance between the three elements risk, control and condition. A safety regime which has focus in only one or two of the elements will lead to ineffective risk management. A prescriptive regime focuses typically on control and condition but less on risk.

11. Conclusion

DNV believes that an effective and robust safety regime for offshore energy exploration, development and production must be risk-informed and must possess the following characteristics

- Performance-based supplemented by prescriptive regulation
- Consideration of technology, organization and people
- Clear roles and responsibilities
- Enforced identification, reduction and control of risks
- Shared performance monitoring
- Practical and economic feasibility
- Balance between risk, control and condition

DNV believes that the introduction of a risk management approach as basis for a new regulatory regime within U.S. waters will significantly improve the safety of offshore oil exploration and production. It will meet the public expectations for assessment of all risks as well as accommodate further development in offshore exploration and drilling safety and environmental protection.

DNV believes that it is critical to maintain and use a living quantifiable safety and environmental risk model to support decision making to prevent major accidents. A holistic model is needed that addresses all aspects affecting the safety, such as technical, procedural, human and organizational and cultural aspects.

This paper is intended to introduce the concept of a risk informed approach to safety and environmental regulations, and does not attempt to describe the concept comprehensively. DNV will be pleased to assist and contribute to the discussion and development of an improved offshore safety and environmental regime for the United States.

Appendix

Risk models

A risk model is a formal review of all threats to safety and the environment. Although complex in execution, the basic principles are simple and shown in the figure below. Because of its conceptual simplicity, however, the importance and complexity of asking the critical questions in the analysis of what can go wrong is often underestimated. This analysis needs to be undertaken both from a holistic perspective and from a detailed perspective on technology, people and organization. Therefore, the assessment requires a dedicated and tailor made approach and can not be undertaken by simple checklists or other standardized approaches.

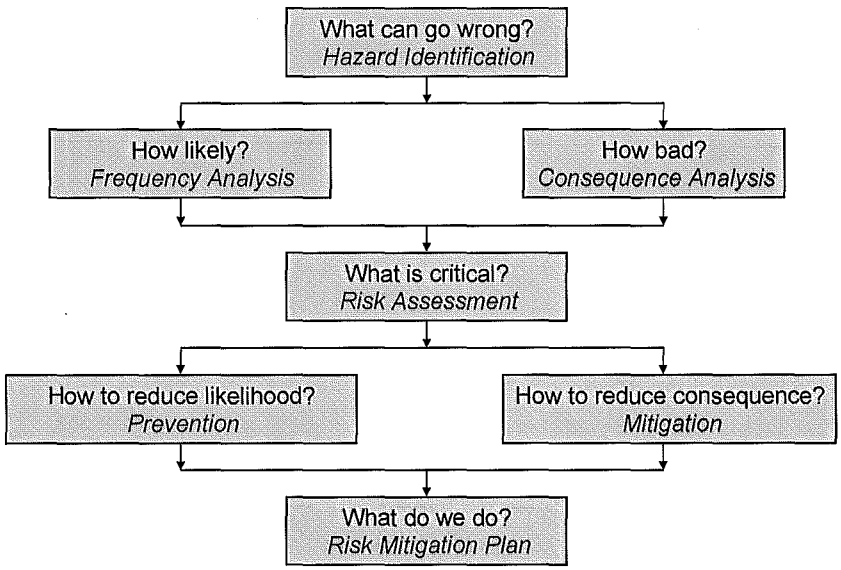


Illustration of the risk assessment and mitigation identification process

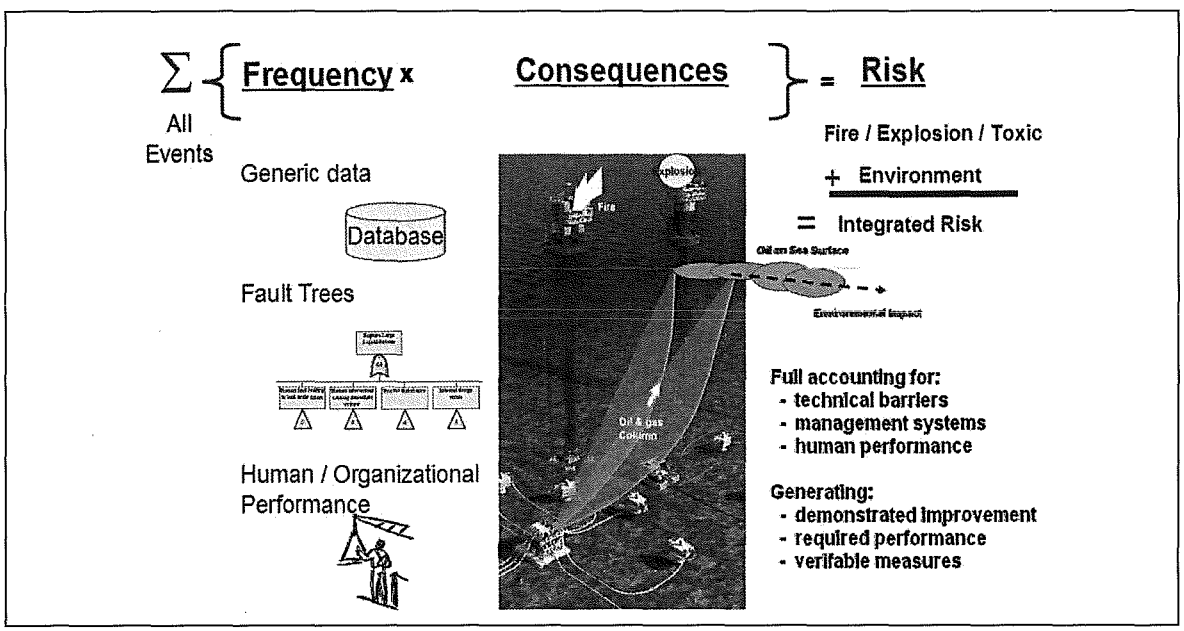


Illustration of a holistic, quantitative risk model for offshore installation

Two risk models should be established, one for the Safety Case during the Planning Stage and one for the Operations Stage as briefly outlined in the following.

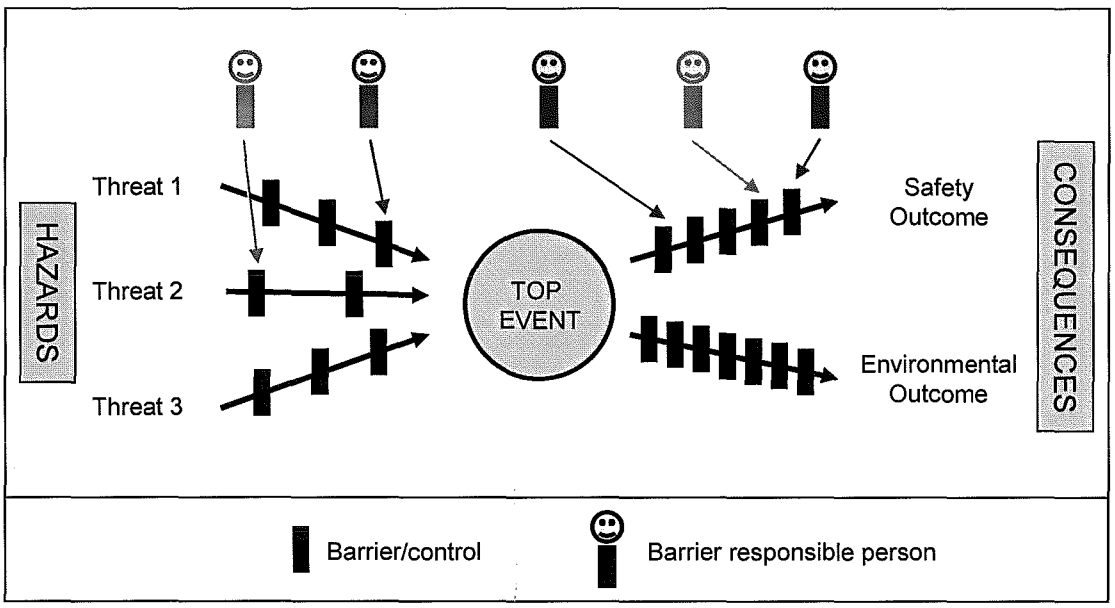
Planning Stage Risk Management

The Planning Stage risk model includes quantified risk assessment (QRA) that uses detailed engineering studies and human performance models to identify all risks and demonstrate how they are prevented and, if an event occurs, mitigated. The figure above illustrates such a holistic, quantitative risk model. Within offshore facilities, there has traditionally been a focus on safety due to fire and explosion on the topside. A holistic model should also include e.g. environment and downhole related risk as illustrated in the figure.

A QRA is a risk model that quantifies key aspects of risk and – importantly – allows for the demonstration of risk reduction by the application of defined safeguards. In many ways, a QRA is similar to a Nuclear Probabilistic Risk Assessment (PRA), except that the numerical approach is a little different (discrete versus probabilistic) and the range of events examined is much broader for the offshore industry while the PRA focuses mostly on the single event of potential reactor meltdown.

Operations Stage Risk Management

The Operations Stage risk model captures all the findings and requirements and translates these into easily understood terms and documents that can be effectively managed and driven into a positive process and safety culture during operations. The documentation will likely consist of a combination of a qualitative barrier diagram approach (often termed a "Bow Tie", see figure below) for foreseen threats and an operational version of the QRA model described in the previous section to address unforeseen issues. The nuclear industry uses also such an operational approach in utilizing the PRA model.



Bow Tie barrier model showing critical barriers (controls).
Prevention barriers are on the left and mitigation barriers on the right.
Each barrier should have a responsible person - only some of these are illustrated.

Most accidents (e.g. Bhopal, Texas City) have been demonstrated to be due not to an unforeseen threat, but due to a known threat adequately addressed by regulations and company requirements, but where the

safeguards have been allowed to degrade over time (technical, human or organizational). The Chemical Safety Board investigations have shown the same to be true in other serious U.S. accidents (e.g., recent explosion at Imperial Sugar, Georgia).

Thus, a vital output of the Operations Stage risk model is that it be maintained up-to-date to provide a clear understanding of the current status of all barriers and how they affect risks, when these have degraded what must be done to return the system to a safe state, and ensure that all company staff, contractors and regulators are aware of the barrier status at all times in daily operations.

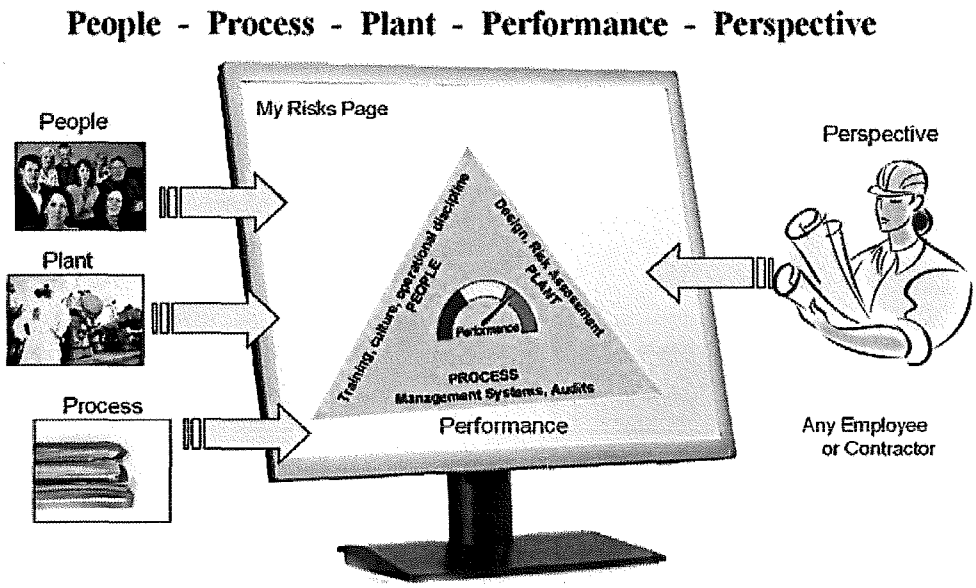
Verification and improvements through audits, reviews and inspections

Regular audits during operations of the risk management system are vital. Important areas that need to be addressed are the management system, the process safety and organizational culture, seamless processes across company staff, contractors and sub-contractors, offshore and onshore as well as the status of all barriers. Also the readiness of prevention barriers must be included, such as emergency and mitigation measures e.g. for containment of oil flow from a well and reduction of oil spill in the ocean.

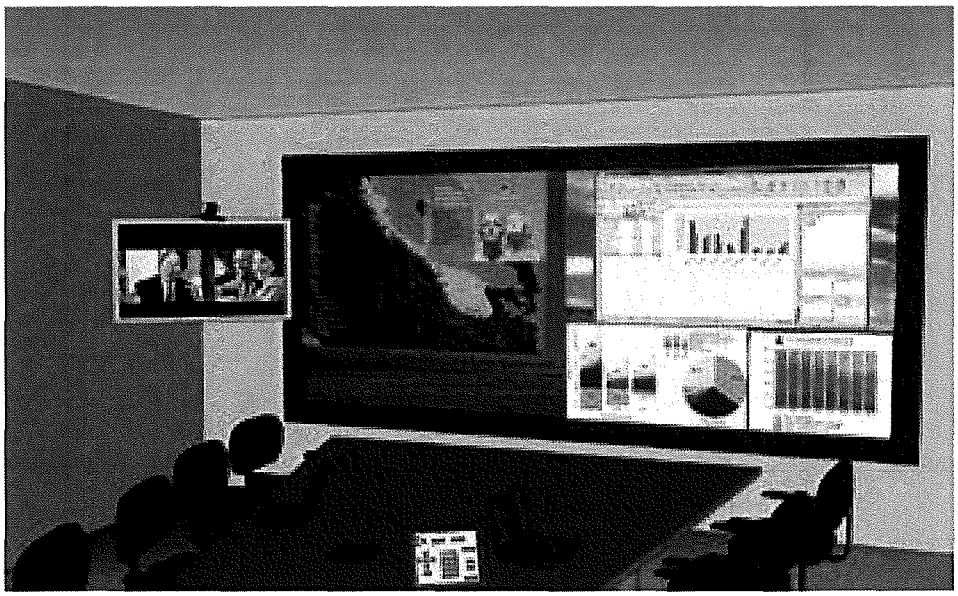
Management and staff reviews must in the same way be executed regularly in order to improve continuously. Finally, regular and in-depth technical inspection and verification of physical facilities are needed to ensure robust integrity.

Effective communication and decision making

Modern information and communication technology can be an effective support in sharing performance monitoring of risks and barriers as well as for making team-based decisions for critical situations in an integrated operations environment as illustrated in the figures below.



IT system can be used to communicate the current status on barriers and risk to allow everyone anywhere to access this information in real-time



Conference systems allow for "Decision Rooms" where offshore and onshore staff, contractors and regulators can meet in a common place for superior team-based decisions

About DNV

With the corporate objective of safeguarding life, property and the environment, DNV helps business and society to manage risks on basis of DNV's independence and integrity. DNV serves a range of industries with special focus on the energy and maritime sectors.

Established in 1864, DNV has a global presence with a network of 300 offices in 100 countries, and is headquartered in Oslo, Norway. As a knowledge-based company, DNV's prime assets are the creativity, knowledge and expertise of our 9,000 employees.

DNV is a global provider of services for managing risk, helping customers to safely and responsibly improve their business performance. As companies today are operating in an increasingly complex and demanding risk environment, DNV's core competence is to identify, assess and advise on how to effectively manage risk, and to identify improvement opportunities. Our technology expertise and deep industry knowledge, combined with our risk management approach, have been used to manage the risks in high-profile projects around the world.

DNV in USA

DNV opened its first office in USA in New York in 1898. Today DNV has 700 employees in USA with offices in Atlanta, Chicago, Columbus, Cincinnati, Detroit, Houston, Jacksonville, Long Beach, Boston, Miami, Norfolk, New Orleans, New York, Portland, Seattle, San Francisco and La Porte.

DNV's main activities in USA are within the energy sector, both within oil & gas exploration, development and production as well as within wind energy. DNV is engaged in verification, classification and asset risk management offshore in the Gulf of Mexico and within risk management of onshore pipelines and refining. DNV has a Deepwater Technology Center in Houston and a leading Corrosion and Materials Technology Center in Ohio focusing on management of degradable structures. The Technology Center in Ohio was a leader in the development of pipeline corrosion assessment standards referenced by US Federal Regulations. DNV is the largest independent consultancy within wind energy in USA.

DNV helps the maritime industry to manage risk in all phases of a ship's life through ship classification, statutory certification, fuel testing and a range of technical, business risk and competency-related services. DNV is among the top two classification societies for mobile offshore units. DNV is present in all maritime clusters in U.S. and our Global Cruise Center located in Miami supports our leading position in this sector.

DNV and Authorities

DNV works for and on behalf of more than 130 authorities as an authorized, notified or accredited body within classification of offshore structures and ships, within certification of management systems and products and within validation and verification of climate change projects on behalf of United Nations.

DNV is authorized by the US Coast Guard as a classification society, approved by Department of Interior as a Certified Verification Agent, accredited by ANSI-AQS National Accreditation Board for certification services and approved by US Centers for Medicare and Medicaid Services to accredit hospitals.

DNV Offshore Codes

The DNV Offshore Codes are a comprehensive set of documents in a 3-level hierarchy consisting of Offshore Service Specifications, Offshore Standards and Recommended Practices. The DNV Offshore Codes are referenced in a number of offshore safety regulations.

Published 22 July 2010

Det Norske Veritas USA Inc.
1400 Ravello Drive
Katy, Texas 77449
USA
Tel: +1-281-396-1000
Email: DNVHouston@dnv.com
www.dnv.com

Contacts

Global Service Director Robin Pitblado, robin.pitblado@dnv.com
Director of Operations Peter Bjerager, peter.bjerager@dnv.com
Director of External Affairs Blaine Collins, blaine.collins@dnv.com

ENCLOSURE (3)

OTC OTC-20415-PP

Barrier Diagrams the Next Stage for Enhancing Offshore Operations Safety

Robin Pitblado DNV Houston, Ravi Tahilramani DNV Abu Dhabi

Copyright 2010, Offshore Technology Conference

This paper was prepared for presentation at the 2010 Offshore Technology Conference held in Houston, Texas, USA, 3–6 May 2010.

This paper was selected for presentation by an OTC program committee following review of information contained in an abstract submitted by the author(s). Contents of the paper have not been reviewed by the Offshore Technology Conference and are subject to correction by the author(s). The material does not necessarily reflect any position of the Offshore Technology Conference, its officers, or members. Electronic reproduction, distribution, or storage of any part of this paper without the written consent of the Offshore Technology Conference is prohibited. Permission to reproduce in print is restricted to an abstract of not more than 300 words; illustrations may not be copied. The abstract must contain conspicuous acknowledgment of OTC copyright.

Abstract

Published data show that the O&G industry has been very successful in reducing occupational accidents, but not as successful in larger scale process safety accidents. The EU has pioneered an approach using barrier diagrams, called bow ties, to identify and communicate barriers effectively, and thereafter to manage these through life. In North America, IADC offers these as the basis for demonstration of safety for MODU facilities which travel between regulatory jurisdictions.

Ongoing safe operations in the UK and Norwegian offshore sectors have shown that comprehensive barrier management improves safety performance. However, communicating the information from hazard and risk registers and bow ties is essential to make sure that everyone understands the full set of barriers in use, their personal responsibilities, that these barriers are operational, and meet their effectiveness requirements.

This paper provides an example demonstration combining bow tie risk management tools with a Sharepoint interface for communications as applied for a large upstream company. Two versions were created – a simpler Pull interface and more complex Push interface.

Operations Safety Needs

It is clear that Process Safety – particularly preventing major accidents – is not yet a solved problem for the process industry globally. A prior paper (Pitblado, 2008) highlighted that while the industry has been very successful in reducing occupational accidents over the past 15-20 years, trends on process safety have been flat or even getting worse. In fact this very success can mislead site management into thinking that process safety is under control as the more frequent occupational incidents have reduced so much. Kleindorfer et al (2007) note that early hopes for process safety improvement have not occurred. The EPA published reduction in accident frequencies and impacts based on the combined effects of the OSHA PSM standard and the EPA RMP Rule was estimated to be 75% of the baseline accident/impact rates over the first 5 years of implementation. In fact no statistically valid reduction was found.

Following the Texas City accident, the Baker Panel (2007) identified many problems with today's implementation of Process Safety Management (PSM) programs and with Process Safety Culture, not only in BP but the whole industry. The CSB identified similar issues in its assessment (CSB, 2007) as well as important technical integrity issues, beyond the terms of reference of the Baker Panel.

In the USA, two major regulations address process safety, OSHA 1910.119 Process Safety Management and the EPA Risk Management Plan regulations (part of the Clean Air Act amendments). These are broadly similar regulations, but OSHA focuses on onsite personnel and EPA focuses on offsite impacts. These regulations have been relatively static since their development in the late 1980's and early 1990's, and enforcement has been less emphasized until after the CSB recommendations to OSHA. A National Emphasis Program is addressing the enforcement issue now for refineries falling under OSHA regulations (Lay et al, 2009).

In the EU, by contrast, the primary regulations are driven by the EU Seveso Safety Case Directives and these have been more dynamic, being updated several times in response to the ongoing series of events. The Seveso Directive is implemented differently in every EU country, and thus local incidents also drive regulatory changes (e.g. in France after the Toulouse explosion and in Belgium after the Antwerp pipeline explosion).

In general, design stage process hazard analyses and risk assessments have resulted in designs that are safe to operate. Newer ideas of inherent safety are slowly being introduced as well. Purely qualitative PHA's are being extended with more quantitative techniques, either LOPA – Layers of Protection Analysis (CCPS, 2001) which is a simplified QRA or full Quantitative Risk Assessment (CCPS, 2000) for the highest hazard chemicals. Changes to facilities are also reviewed well using these techniques.

Thus the problem is not that facilities are unsafe due to design, but that incidents tend to happen due to safeguards included in the design – technical, administrative or human, which are allowed to degrade over time. Reasons are complex and rarely due to deliberate intent or risk taking, but serious process incidents are rare and the rationale for many safeguards may be lost over time and the continuous activities to keep them functional may not occur. Normalization of deviance is an important issue in this regard.

Barrier Based Methods

Current hazard identification tools (e.g. HAZOP, PHA, etc) do identify hazards and key controls for those, but for time reasons, the identification teams rarely record more than the top 2-3 controls. These studies are particularly looking for unprotected hazards and once the team judges sufficient controls are identified, no further documentation occurs. In reality there can be many more than 2 or 3. Thus current tools do not record the full range of controls and thus the process safety management system is not directed to ensuring they are all working.

The use of barriers to manage risks is well established. The nuclear industry has been using a formal Defense-in-Depth concept since the late 1960's – and this was fundamental to preventing the Three Mile Island accident from becoming a disaster. Prof Reason in a well known assessment of major accidents has developed a Swiss Cheese model to demonstrate accident causation and the role of multiple but imperfect safeguards in their prevention. In his model (Reason, 2000) uses several slices of swiss cheese, each with many holes, being challenged by threats – which are spears trying to pass through all the slices. Intuitively, the more slices (the safeguards) and the smaller the holes (a measure of their effectiveness), then the safer the system.

It is now believed that formal definition of barriers and thereafter ongoing monitoring of their status is a key means to ensure ongoing safety. The North Sea suffered two very serious incidents in the 1980's – Alexander Kjelland in 1982 (123 fatalities) and Piper Alpha in 1987 (167 fatalities) where key safeguards failed and greatly increased the consequences of those accidents. The UK regulations were updated to adopt the safety case approach (based on the EU Seveso Directive) but added extra weight to the safeguards. Risk assessments must be used to identify Safety Critical Elements (the key safeguards / barriers), their performance requirements (necessary to attain the low risk objective), and a written scheme (the ongoing maintenance, inspection and competence regimes) to keep those safeguards functional through life.

Major accidents are rare, but in the 20+ years since Piper Alpha there has been no major disaster in the North Sea. That is not to say that challenges are not occurring. The UK maintains the Hydrocarbon Leak Database of all leaks in the UK sector and there remain a large number of events every year – but declining in number, particularly the more serious ones (Pitblado, op cit).

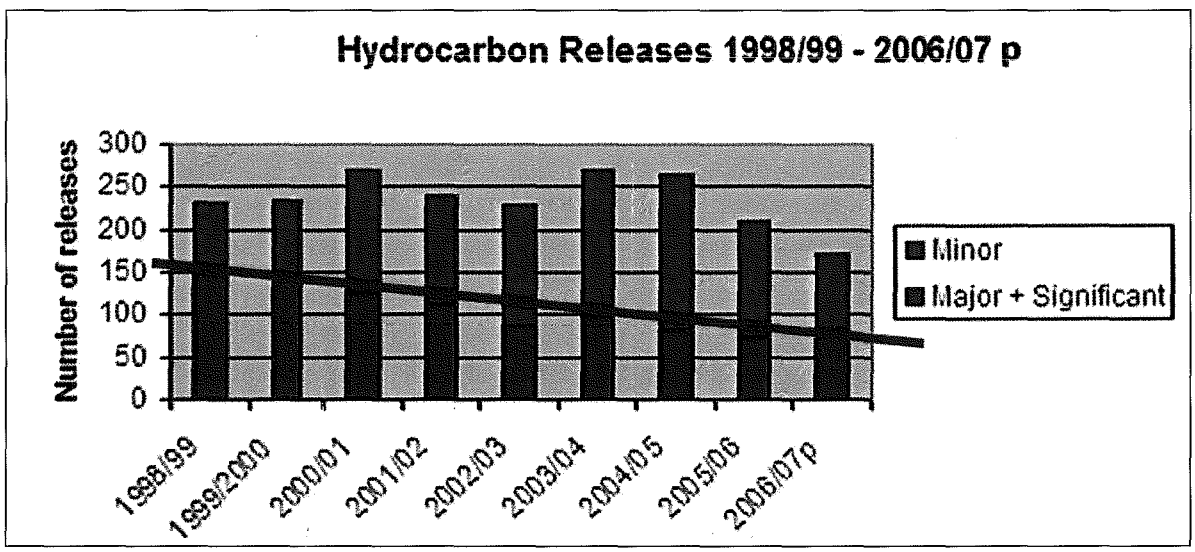


Figure 1. Number of Release events in UK Sector of North Sea (HSE HCRD database)

In 2007 there were two very serious initiating events – one on the Visund Platform in the Norwegian sector and one on the Rough Platform in the UK sector. The former event released over 900kg/s into the platform – but all, the safeguards worked – ignition controls, gas detection, ESD systems, blowdown and no ignition occurred. On the Rough platform the release was 400kg/s and ignition did occur, but again the safeguards worked and the event was limited. Both of these had the potential to be total losses if the safeguards had failed. Ingvarson and Strøm (2009) describe an effective lifecycle barrier audit process used in the Norwegian sector by StatoilHydro. Thus initiating events still occur in the North Sea but the better management of safeguards has to date prevented their escalation into disasters.

The importance of managing barriers is as important onshore as for offshore. An analysis of the Bhopal accident shows that there were 8 barriers included in the original design (hardware and administrative) to prevent or mitigate a runaway reaction of MIC caused by water ingress. The local site allowed all 8 to go out of service or become degraded. A similar analysis of the Texas City disaster shows 12 barriers were included in the design and all 12 had become degraded. Thus a design stage QRA may show a facility to be safe and to meet a risk target, but if the barriers are allowed to degrade, then risks can greatly increase.

Two types of risk assessment can be defined for high hazard facilities:

- a design stage risk assessment (e.g. HAZOP + QRA) focusing on a short list of controls and quantitative results (separation distances, firewall ratings, firewater demand, risk target attainment)
- an operations phase risk assessment (e.g. bow ties) focusing on a more complete definition of critical controls, and definition of ownership, effectiveness, and means to keep operational through life

A methodology for barrier definition and risk assessment, using the swiss cheese model, was developed in the Netherlands in the 1990's. This approach, called Bow Tie Risk Analysis was pioneered into the process industry by Shell (Zuijderduijn, 2000). They have implemented this as an integral part of their Hazard Management and Effects Program (HEMP) applied to all sites upstream and downstream, globally. An EU sponsored research project, ARAMIS, investigated means to adopt bow ties as a standard part of the EU Safety Case regime and the results of this work are presented in a special issue of the Journal of Hazardous Materials (Salvi and Debray, 2006). In Norway, a similar method, titled "Barrier and Operational Risk Assessment" is being used as a means to enhance process safety (Aven et al, 2006).

The bow tie approach obtains its name from the graphical display of controls in the form of multiple threat controls on the left hand side, reaching a central event, and then expanding to multiple outcomes or effects with mitigation controls on the right hand side. The central event can be thought of as the Top Event in a Fault Tree and most often for process safety this will be a large loss of containment event. In concept terms the Bow Tie diagram is shown in Figure 2.

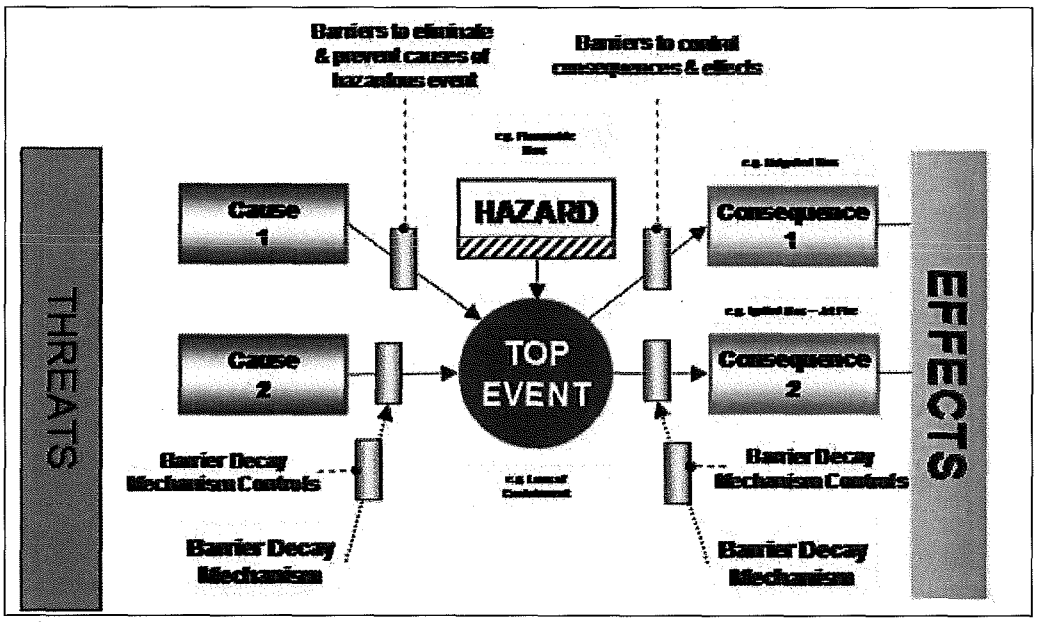


Figure 2. Bow Tie diagram concept

Each arm in this figure represents a pathway thought which an accident can occur. In the diagram only one barrier or control is shown on each arm – in practice there are many, often 6 or more controls. A barrier for the purposes of Bow Tie is more extensive to those in LOPA which is more restrictive as it seeks to generate a quantitative result. DNV prefer the definition

of Sklet (2006) which defines barriers / controls as: "Safety barriers are physical and/or non-physical means planned to prevent, control, or mitigate undesired events or accidents". This definition permits the full range of hardware, administrative and people controls to be documented and assessed.

Controls can be thought of in Fault Tree terms as an AND gate with two inputs: a demand (the threats progressing through the system) coupled with Control Fails. The control that fails allows the threat or outcome to progress to the next control or its ultimate outcome. With this model in mind, then it is clear that further analysis can give reasons why the control might fail and this is shown in Figure 2 as a Barrier Decay Mechanism (also known as an escalation factor). The Fault Tree combinations are shown for clarity in Figure 3. If this is Routine Inspection as the control, then the gate would represent Inspection fails. A barrier decay mechanism development might take this further and show why Inspection might fail – e.g. planned inspections delayed or cancelled, inspector not competent, inspection equipment faulty, or inspection technique not suitable.

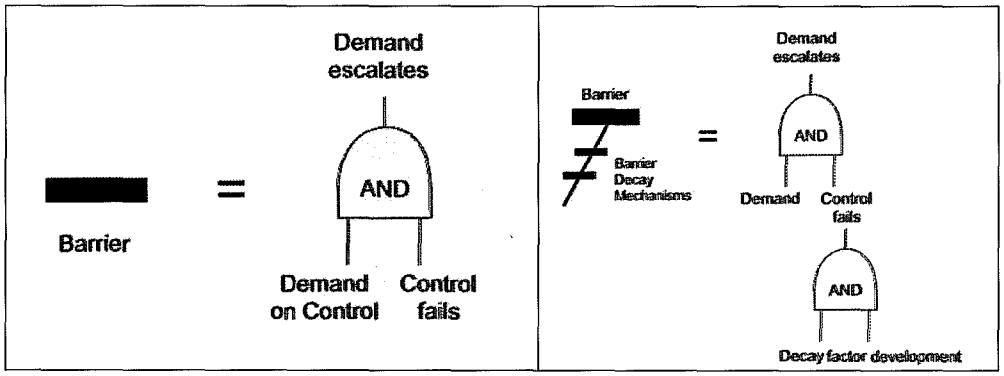


Figure 3. Fault Tree representation of barriers / controls

Real bows can become large and complex. An example extract bow tie (Figure 4) shows the level of detail that might be presented and this is just for the threat side for 10 identified threats leading to a central loss of containment event. The text in this figure is not intended to be read.

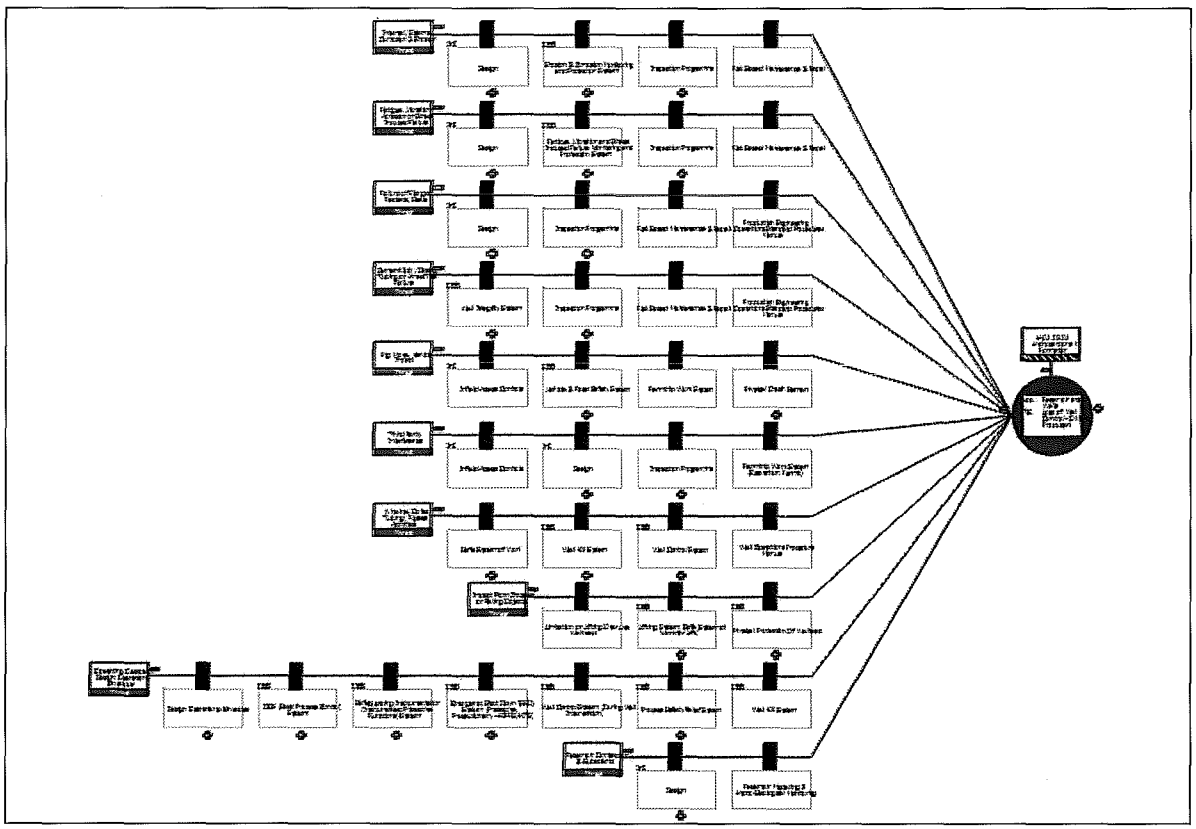


Figure 4. Typical real bow tie for process facility

Case Study: Web-Based Solution for Integrated Risk Management

In the following case study, an approach to effective risk management was to use integrated database sharing information technology to communicate and manage facility and process risks throughout an organization. A bow tie database and along with the company's HRR were both incorporated into this web-based solution. This was achieved by using Sharepoint 2007, a Microsoft tool which allows for workgroup information sharing and workflow management.

Earlier versions of SharePoint (through Sharepoint 2003) were primarily used as document libraries and offered basic functionalities and features such as support for SQL (structured query language) servers and web-based interface. The newer versions, SharePoint 2007 and 2010 consist of products and software elements that have web browser based collaboration functions, process management modules, search modules and a document-management platform. It has a web portal interface which allows for more graphics, point and click, RSS (really simple syndication) feeds, wiki's, blogs, community of practice support and offers an enhanced search function with the capability of triggers for notifications. SharePoint2007 fully integrates with MS Office and can link to external databases such as SAP or bow tie software. Databases in Excel, Access and SQL are also supported with the standard features.

By using Sharepoint it was possible to create HSE and barrier information websites in two formats, a 'pull' site and 'push' site. Both were developed and deployed for a large oil and gas operator in the Middle East. The 'pull' site is a more traditional document sharing system where users query the database through an intuitive web interface and get the SHE risk information they are authorized to access. The interface is easy to use but requires the user to extract the information needed from the bow tie database by filling in a query form that asks for the plants and hazards of interest. The 'push' site on the other hand is much more user-friendly as it is customizable to meet the specific job requirements or activities of the end user. Through a more advanced interface, the 'push' site recognizes the user upon login and generates pre-programmed user-specific information. Various permission levels were created to allow user groups to see only information pertaining to their job responsibilities or tenure level within the company (e.g. technicians, supervisors, managers, directors). The following screen shots explore in more detail the push site features and capabilities.

Home page

An objective for the creation of the web-based tool was to assist the operator in meeting HSE targets / close-outs by integrating project management elements. The built-in features of Sharepoint does support basic project management task typical for small projects. Moreover, for larger complex projects that use MS Project, tools are available that will export essential fields from MS project into Sharepoint which will then display the information on the web-based interface.

The push web-based HSE and barrier management solution is accessed through a standard web browser. The homepage, customized for the user, promotes some of the important and most frequently used tasks (see figure 4).

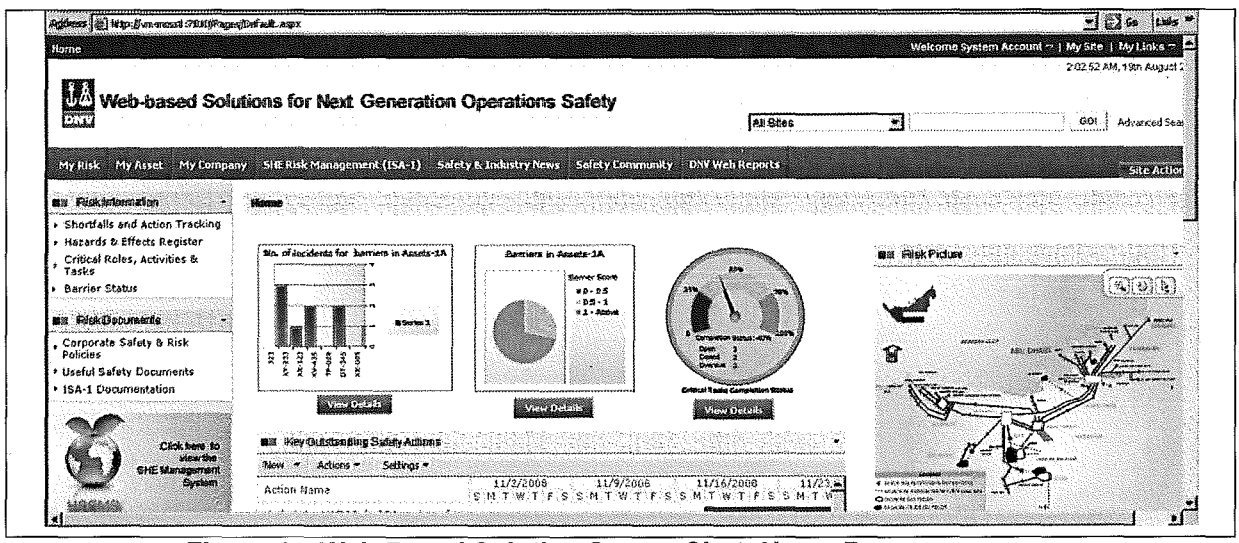


Figure 4 – Web-Based Solution Screen Shot: Home Page

Shown in the middle is a dashboard with a graphical representation of key information contained in the bow tie database pertaining to the users' KPI's (i.e. number of incidents per barrier, health of barriers and critical outstanding tasks). Another option for a graphical representation can be the display of a bow tie diagram showing barrier status. On the right side of the homepage a geographical map of the company's assets, with zoom-in and pan-around, gives traffic light indicators showing the overall risk picture. This live map allows the user to jump to site specific information (e.g. hazard and risk register). The left side of the homepage displays links to key information (Risk Information) and documents (Risk Documents). For this

project, the links under Risk Information consisted of: Shortfalls and Actions Tracking, Hazard & Effects Register, Critical Roles, Activities and Tasks, Barrier Status. RSS news feeds and news alerts are also displayed on the home page.

Navigational Structure

On top of the home page, a persistent navigation menu enables the user to reach any section of the HSE web-based solution which has been customized and segregated at different levels:

- Individual level (My Risk) – job responsibilities (standards and procedures), their personal barrier responsibilities, safety performance, key performance indicators (KPI), action status and competence training.
- Site level (My Asset) – HSE management system, project status, critical safety actions, barriers and performance monitoring
- Company level (My Company) – Corporate safety and risk policies and documents, asset maps, safety culture, corporate incident metrics.
- Knowledge Sharing - SHE Risk Management information, HSE incidents, operations safety projects, incident investigations results
- Industry level (Safety and Industry News) – announcement, newsletters, industry news, conferences and training courses.
- Community level (Safety Community) –.Journals, Conferences, SHE blogs, SHE Wikis, SHE Quiz, Safety Survey, Media library and video collection.
- Web Reports – Generation of bow tie reports, statistical charts, hazard and effects risk registers based on information from the bow tie database.

At the individual level ('My Risk' tab), the information is highly personalized. Upon login the systems has recognized the individual and built-in features within Sharepoint facilitate the viewing of activities and scheduled tasks with start and end dates in Gantt chart format (see figure 5). Because it's fully integrated with MS Office and MS Outlook, calendars can be viewed and updated through the web-based interface or MS Outlook. This makes keeping track of project tasks and outstanding activities relatively easy. Not only does the system list the user's barriers and the critical tasks but it also indicates the approvals required. Other specific information related to the individual's job responsibilities such as procedures, manuals and other useful documents are also made available. For instance, a senior electrical technician would see under 'My risk' electrical SOPs (standard operating procedures), electrical craft newsletters and an electricians' blog.

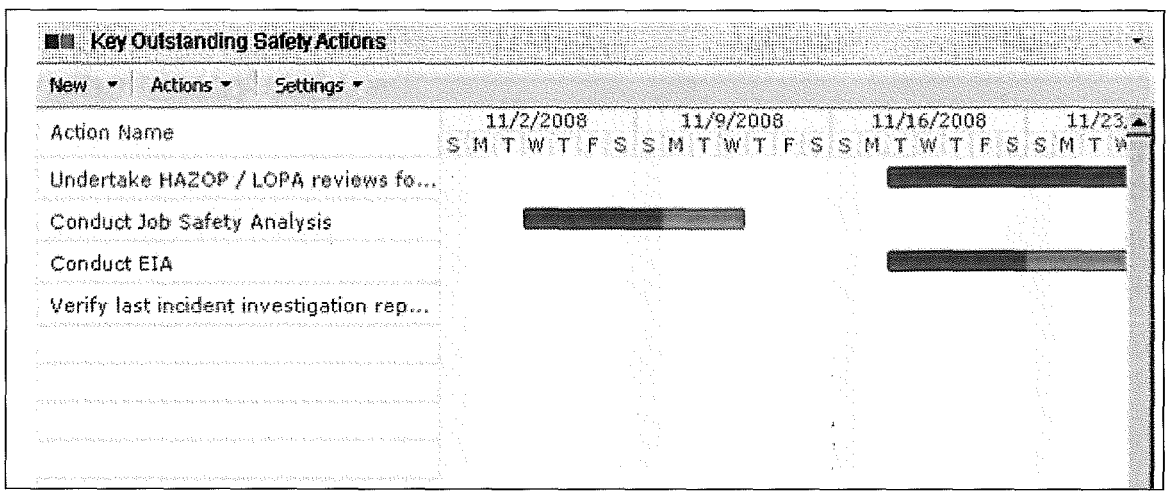


Figure 5 – Web-Based Solution Screen Shot: HSE Action Management

At the site level ('My Asset' tab), the information is more broad and encompasses the entire site/facility where the user is located. The features at this level include viewing the HSE management system for the specific site and access to important information for operations safety such as emergency response plans, performance monitoring charts, project status reports, critical safety actions, key barriers and barriers status. Figure 6 illustrates the listing of barriers for a specific asset. The health rating or score of each barrier is shown along with a record of the number of incidents associated with that barrier. Additionally, notes can be recorded and viewed facilitating information sharing amongst staff.. At the company level ('My Company' tab), the website presents data for the whole enterprise. Typical information such as introduction to the company, map of assets, corporate safety and risk policies and documentation are accessible to the user. In addition, a general

operational risk status of the company is shown and links allow the user to view the corporate incidents metrics and safety culture metrics.

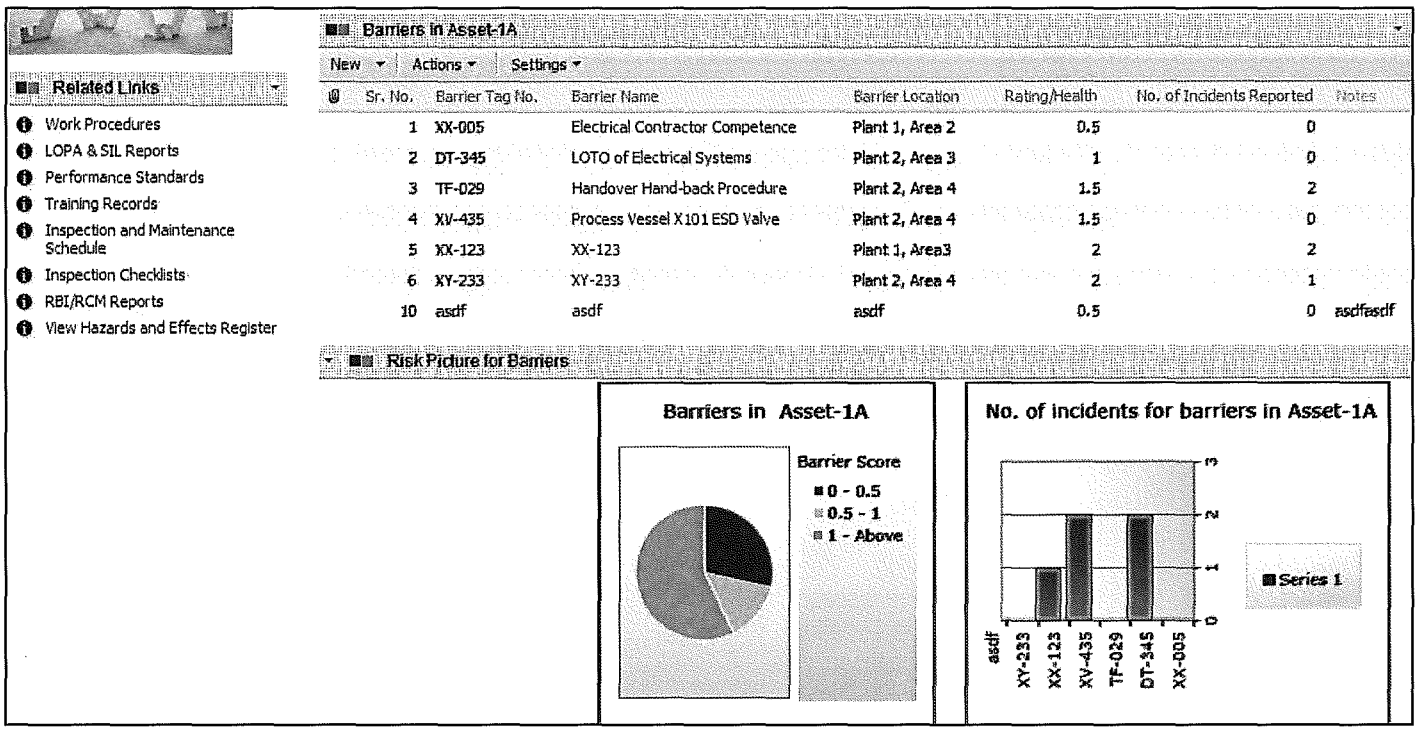


Figure 6 – Web-Based Solution Screen Shot: My Asset -critical barrier health and related links

The information contained at the industry level ('Safety and Industry News' tab), keeps the user up-to-date with HSE news and related events. One of the features is a shared calendar to view training courses and conferences relevant to the user's interests and needs. The calendar implemented for this project has the option of segregating courses and conferences by city or region. Other features include announcements and newsletters (company or third party which users can signup for). Under the community level ('Safety Community' tab), a variety of web-based tools are available such as RSS feeds, SHE wikis, SHE blogs, online quizzes and surveys. For this project, the push HSE website solution supported the delivery of online quizzes. Customized quizzes and test can be administered to assess employee competency and identify training needs.

Access to Database via Web Reports

With Sharepoint all HSE documents, reports or general working document can be stored and accessed for review, updates or on-going project work. This allows teams to share files and facilitates the work process for major projects. A neat feature of the developed HSE web-based solution is the capability to generate reports on the fly within the web browser. The information from the bow tie database is accessed from the web reports section. Through a series of intuitive query fields, selected one at a time, the web-based tool allows the user to filter the database for the desired information to report. For instance, the user can generate a list of shortfall and remedial actions plans (RAP) for one or more sites. After choosing the location, the shortfalls can be viewed by hazard or activities. Figure 7 shows the query screen where the search parameters are chosen to generate a shortfall and RAP report. In this illustration, the shortfalls are selected to be viewed by activity. One or more activities can be selected at once with the option of sorting them with a target date range (i.e. start and end date for that given task). Note that a check box for overdue shortfalls if selected would generate a list of tasks which should have been completed by the current date. Once generated the report lists the shortfall, the priority and target date for the activities, the owner and the remedial action plan.

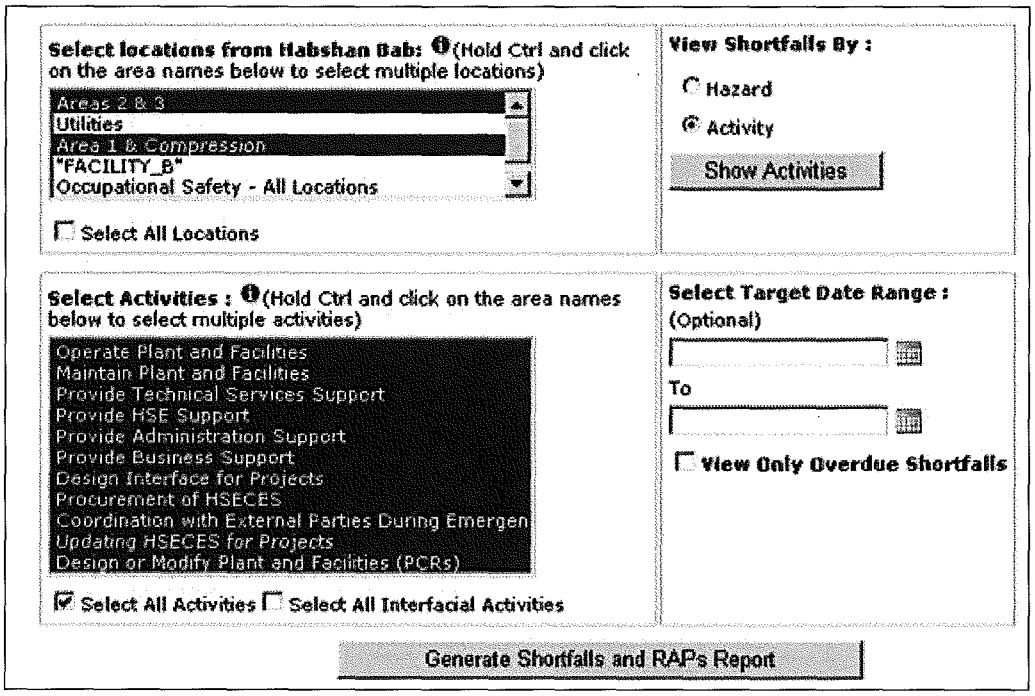
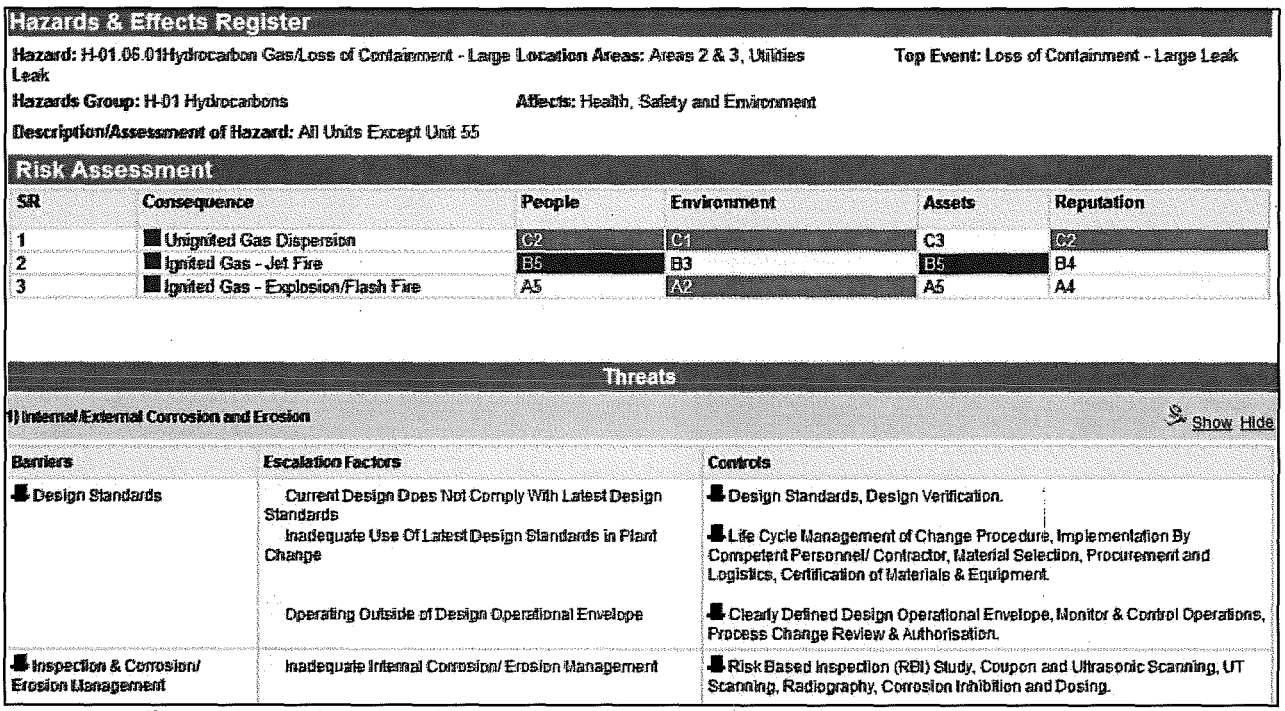


Figure 7 – Web-Based Solution Screen Shot: Shortfalls and Remedial Actions report

Another example is the generation of a hazard and effects register report that can be for one or a number of sites. The user selects the site(s) or unit(s) of interest within the site, the hazard category (H, S, and E) and the hazard group (e.g. hydrocarbons, toxic gas). The example of a report is illustrated in Figure 8.



Hazards & Effects Register

Hazard: H-01.06.01Hydrocarbon Gas/Loss of Containment - Large Leak **Location Areas:** Areas 2 & 3, Utilities **Top Event:** Loss of Containment - Large Leak

Hazards Group: H-01 Hydrocarbons **Affects:** Health, Safety and Environment

Description/Assessment of Hazard: All Units Except Unit 55

Risk Assessment

SR	Consequence	People	Environment	Assets	Reputation
1	Unignited Gas Dispersion	C2	C1	C3	C2
2	Ignited Gas - Jet Fire	B5	B3	B5	B4
3	Ignited Gas - Explosion/Flash Fire	A5	A2	A5	A4

Threats

1) Internal/External Corrosion and Erosion — Show Hide

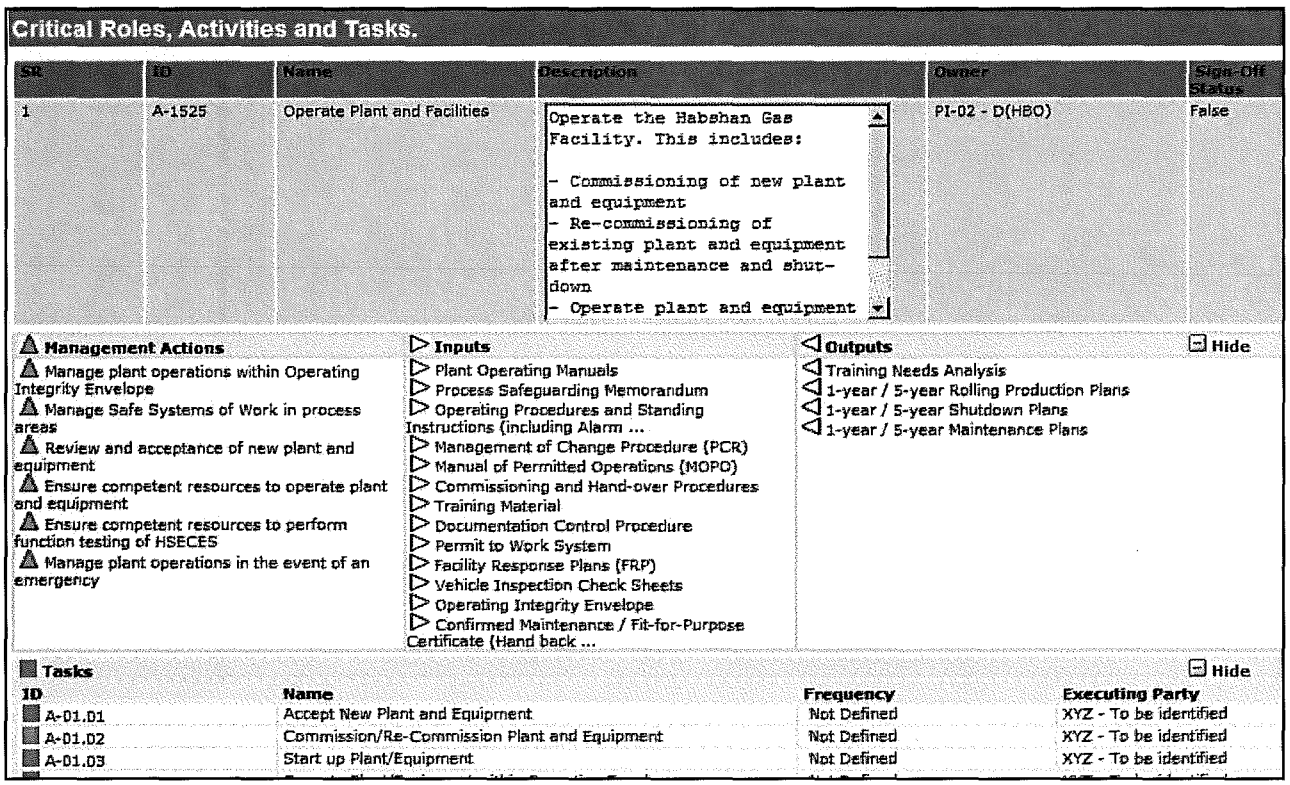
Barriers	Escalation Factors	Controls
Design Standards	Current Design Does Not Comply With Latest Design Standards	Design Standards, Design Verification.
	Inadequate Use Of Latest Design Standards in Plant Change	Life Cycle Management of Change Procedure, Implementation By Competent Personnel/ Contractor, Material Selection, Procurement and Logistics, Certification of Materials & Equipment.
	Operating Outside of Design Operational Envelope	Clearly Defined Design Operational Envelope, Monitor & Control Operations, Process Change Review & Authorisation.
Inspection & Corrosion/ Erosion Management	Inadequate Internal Corrosion/ Erosion Management	Risk Based Inspection (RBI) Study, Coupon and Ultrasonic Scanning, UT Scanning, Radiography, Corrosion Inhibition and Dosing.

Figure 8 – Web-Based Solution Screen Shot: Hazard & Effects Register Report

The hazard and effects register report is formatted as per the company's requirements. As depicted above, the first section of the report page provides a summary of the selections made to obtain the report. The subsequent section presents the risk assessment of the selected hazards based on the organization's actual risk matrix. In the last section (Threats), the full set of threats with their barriers, escalation factors and consequences can be viewed. Since the bow tie database is updated regularly

by its owner, everyone on the site has access to the latest barrier status and information. All reports can be printed, converted to PDF or e-mailed directly from the web browser.

Another feature also included in the web report section is the ability to generate reports for critical roles, activities and tasks (CRAT) for any specific position or job title. This feature allows the user to generate on demand, an electronic real-time report showing HSE critical activity and its corresponding management. Figure 9 gives an example of a CRAT report generated for the operations manager position of a specific plant (like the other reports previously described, the CRAT report can be site specific).



Critical Roles, Activities and Tasks.

SR	ID	Name	Description	Owner	Sign-Off Status
1	A-1525	Operate Plant and Facilities	Operate the Habshan Gas Facility. This includes: - Commissioning of new plant and equipment - Re-commissioning of existing plant and equipment after maintenance and shut-down - Operate plant and equipment	PI-02 - D(HBO)	False

Management Actions

- Manage plant operations within Operating Integrity Envelope
- Manage Safe Systems of Work in process areas
- Review and acceptance of new plant and equipment
- Ensure competent resources to operate plant and equipment
- Ensure competent resources to perform function testing of HSECES
- Manage plant operations in the event of an emergency

Inputs

- Plant Operating Manuals
- Process Safeguarding Memorandum
- Operating Procedures and Standing Instructions (including Alarm ...
- Management of Change Procedure (PCR)
- Manual of Permitted Operations (MOPO)
- Commissioning and Hand-over Procedures
- Training Material
- Documentation Control Procedure
- Permit to Work System
- Facility Response Plans (FRP)
- Vehicle Inspection Check Sheets
- Operating Integrity Envelope
- Confirmed Maintenance / Fit-for-Purpose Certificate (Hand back ...

Outputs Hide

- Training Needs Analysis
- 1-year / 5-year Rolling Production Plans
- 1-year / 5-year Shutdown Plans
- 1-year / 5-year Maintenance Plans

Tasks Hide

ID	Name	Frequency	Executing Party
A-01.01	Accept New Plant and Equipment	Not Defined	XYZ - To be identified
A-01.02	Commission/Re-Commission Plant and Equipment	Not Defined	XYZ - To be identified
A-01.03	Start up Plant/Equipment	Not Defined	XYZ - To be identified

Figure 9 – Web-Based Solution Screen Shot: CRAT Report

The report gives a description of the role and responsibilities associated with the position and management actions along with a list of inputs, outputs and specific tasks. The frequency, executing parties and deadlines for each task are also presented. This is a useful document for conducting internal audits to check and monitor performance of personnel at all levels.

Improved Communication

The HSE and barrier management web-based solution improved communication of critical safety information between barrier owners and management. Status of key barriers is known; key actions identified and easily shared keeping everyone aware of the tasks to be performed. The HSE web reports assist in performance monitoring of both assets and people facilitating operations management.

The web-based solution has also provided an opportunity for site operators and supervisors to share knowledge with their peers working on similar challenges on other sites in the organization. For example, they can now refer to each others Remedial Action Plans (RAPs) for similar Hazards. Furthermore, they can effectively share knowledge through features such as Blogs, Wikis and Discussions, which not only encourage knowledge sharing but also document the shared knowledge for others to benefit in future.

Due to the streamlined nature of the solution with organization's operational safety processes, the required safety information and alerts are available in 'real time' to supervisors, superintendents and HSE managers at corporate head office. On the other hand, personnel working on sites no longer have to dedicatedly write voluminous periodic reports to their supervisors. All operational safety critical information is thus systematically available in real-time across geographically dispersed assets, which can be accessed using a standard web browser. Reporting features such as viewing overdue shortfalls has created an increased sense of awareness and responsibility at all levels in the organization.

An ancillary benefit was that the web-based nature of the solution has also helped the organization meet one of its HSE goals of reducing paper usage.

Conclusion

Effective operational risk management requires the constant monitoring of the performance and status of critical safety and operational systems hence the importance of barriers and barrier management. Barrier based approaches, such as Bow tie diagrams, are recognized and recommended to help industry meet operational safety objectives. Compared to traditional PHA methods like HAZOP or QRA, the visual aspects of bow tie diagrams makes them a more effective tool for safety training and communicating the complete risk picture to personnel. They shows the relationship between, threats, barriers, hazards and the potential outcomes. Furthermore they clearly indicate barrier ownership and thus emphasize barriers relating to major risks that may have a relatively lower likelihood of occurrence and thus tend to fall below people's consciousness due to other more urgent demands. Paper based bowtie diagram reports are good initially but ultimately are filed and are not easily accessible, and thus not effective for continuous barrier status monitoring and upkeep. The use of a web-based interface solution is a powerful vehicle for communicating to everyone on a company intranet all the critical safety information from a continuously updated bowtie database. The HSE 'push' website allows access to information which is often hard to share or hidden to individuals.

References

Baker Panel (2007), The BP U.S. Refineries Independent Safety Review Panel. Chairman James A. Baker III. Available from BP.

CCPS (2000), Guidelines for Chemical Process Risk Assessment, 2nd Edition, Center for Chemical Process Safety, AIChE, New York.

CCPS (2008), Guidelines for Hazard Evaluation Procedures, Center for Chemical Process Safety, AIChE, New York.

HSE (2006), Heath Safety Executive Information sheet: Guidance on Risk Assessment for Offshore Installations, Offshore Information Sheet No. 3/2006.

IADC (2009), Health, Safety and Environment Case Guidelines for Mobile Offshore Drilling Units, issue 3.2.1, May 1, 2009.

ISO Standard 17776 :2000, Petroleum and natural gas industries, Offshore production installations, Guidelines on tools and techniques for hazard identification and risk assessment.

Lee's (2005). Loss Prevention in the Process Industries, Hazard Identification, Assessment and Control, Volume 1, DR S. Mannan.

Oil and Gas UK (2009), Accident Statistics for Offshore Units on the UKCS 1990-2007, Issue 1, April 2009.

Pitblado R (2008). Global Process Industry Initiatives to Reduce Major Accident Hazards, Mary Kay O'Connor Process Safety Conference, College Station, October.

Pitblado R (2009) Risk Communications: Web-sites for Barrier Diagrams and Process Safety, Mary Kay O'Connor Process Safety Conference, College Station, October.

Reason, J. (2000) Human error: Models and management. British Medical Journal, 320: 768-770.

Salvi O and Debray B (2006) A global view on ARAMIS, a risk assessment methodology for industries in the framework of the SEVESO II directive, Journal of Hazardous Materials 130, p187–199.

Sklet S (2006) Safety barriers: Definition, classification, and performance. Journal of Loss Prevention in the Process Industries 19, 494–506.