Dynamic Barrier Management – Managing Safety Barrier Degradation

Pitblado R[1]., Fisher M[2]., Nelson B[1]., Fløtaker H.[3], Molazemi, K.[3], Stokke A.[3]
DNV GL
1 – 1400 Ravello Dr, Katy TX, USA; 2 – Applicon House, Exchange St, Stockport UK; 3 – Veritasveien Høvik Norway

Safety barrier management is an important activity to maintain or reduce process safety risk of an operating facility. Barriers can be hardware (e.g. relief valves) or human (e.g. permit procedures) or a combination of both (e.g. manually actuated ESD system). Barriers are normally fully functional after installation or commissioning when all equipment has been tested and all staff trained, and the facility risk will be at or better than target level, as the design risk assessment this will have assumed some barrier failure probability. However, barriers degrade at different rates, and these degradations start to increase facility risk. Some barrier failures can increase risk dramatically, especially where barrier dependencies exists. Conventional barrier management applies fixed inspection and maintenance intervals to these with the intent to return these to full functionality and the risk to target, but take no account of dependencies.

Dynamic barrier management uses the full suite of information available, including direct and indirect indicators of barrier performance to infer barrier status in near real-time. This can be through a smart combination of inspection, preventive maintenance, audit, sensors, process control, and near-miss or incident records, and big data concepts. Barrier maintenance can then be planned optimally based on quantitative barrier importance to risk control, in a manner similar to risk based inspection (RBI). Higher Importance barriers (i.e. risk affecting) would be assigned higher priority than other barriers. This can achieve better safety at lower cost than current barrier management processes.

Keywords: Barriers, Risk, Safety Management, Asset Management

Introduction

The barrier risk management approach has been in use in aviation, rail, and oil & gas industries for more than 15 years, and for even longer in the nuclear industry where it is termed Defence in Depth. The bow tie model extends this idea by creating a bow-tie shaped figure defining a central “Top Event” which in Oil & Gas terms would correspond to a loss of containment, a loss of structural integrity or a loss of control . Barriers located to the left of this (the Threat side) are termed Prevention Barriers, and those on the right (the Consequence side) are termed mitigation barriers. There is no current standard for the Bow Tie risk method, and many companies have their own internal bow tie procedures. Public method documents exist from CGE Risk (2013), DNV GL (2014) amongst others, and CCPS is currently working on a Guidelines text so that there will be a public standard in 2016.

The bow tie method links well to regulatory requirements in Europe for O&G and chemical facilities covered by the onshore Seveso Directive or the new EU Offshore Safety Directive (Zuijderduijn, 2000). Offshore regulations call for a risk assessment that defines safety critical elements (SCE), and for each of these to define required performance standards (PS) as well as a written scheme to specify the required maintenance, inspection and competence regimes to keep each SCE at its defined PS. Norway has issued a guideline on the management of barriers PSA (2013) highlighting these are not static and hence the need to manage barrier systems to keep them functioning at their desired performance level.

Zuijderduijn suggested that 10-12 well designed bow ties can capture most key barriers for a refinery, and that logic would also apply to offshore installations. Some other companies start with a basic set of bow ties but customize these for specific units, so staff can recognize their facility barriers and owners can be specific individuals rather than generic job titles.

Barriers degrade in service and unless suitable remedial actions are taken then risk levels will be higher than assumed from design, perhaps much higher if there are barrier dependencies. The basic shape of the solution is defined in Figure 1which shows the integration and decision process. This shows the sequence of data collection from multiple sources, the integration of this into an integrated database, a prediction of barrier status (from direct or indirect indicators), the impact of barrier status onto risk (quantitative or qualitative), and ultimately to decision support (for safety or operational efficiency purposes). The idea within this figure is described more fully in Section 3.3.

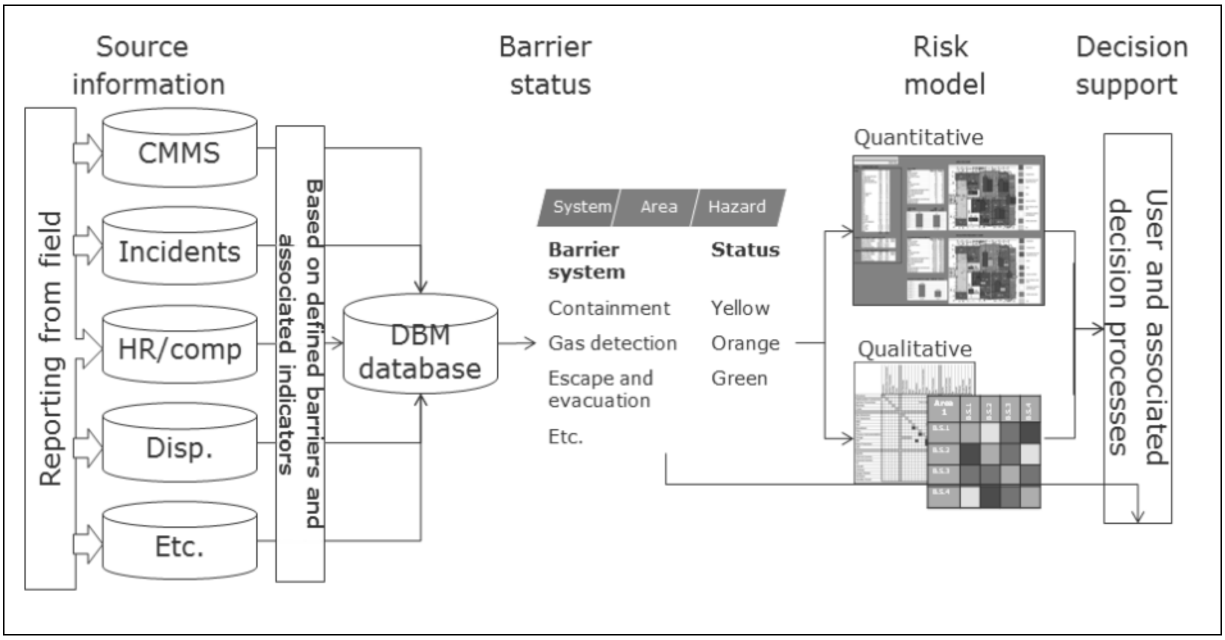

Figure 1. Concept for Dynamic Barrier Management

Definitions

The Norwegian PSA (2013) defines a barrier as: Technical, operational and organizational elements which are intended individually or collectively to reduce the possibility for a specific error, hazard or accident to occur, or which limit its harm or disadvantages. This definition is broader than an independent protection layer in LOPA or in UK safety case regulations for a safety critical element.

A "static barrier" is a barrier with assumed constant performance (its pfd: Probability of Failure on Demand). This is achieved by a predetermined inspection, maintenance, and competence regime.

A "dynamic barrier" is a barrier with some performance degradation rate. This is measured typically with predetermined inspection, maintenance and competence regimes. The current state of the barrier is used in routine operational decision making and a flexible system of maintenance corrects the degraded state back to the desired performance level or introduces some additional equivalent barrier to return the risk to the desired target level. The term dynamic is used as sometimes a barrier can perform above its expected performance.

Barrier degradation is not a simple or constant factor. There are inherent degradation rates with fast, medium and slow time constants. Some typical degradation rates are given in Table 1.

Table 1. Example barrier degradation rates

Degradation Rate	Typical degradation rate	Example barriers
Fast	Less than 1 year	Procedural barriers (e.g. procedures without refresher training) Most human barriers Active barriers (e.g. gas detection, emergency lighting)
Medium	1 year – 5 years	Safety documentation Process containment – subject to more rapid corrosion Active barriers (e.g. flare systems, Emergency Shutdown systems)
Slow	5+ years	Active barriers (e.g. relief valves) Process containment – subject to normal corrosion rates Passive barriers (e.g. tank dikes, firewalls)
Static	Life of facility	Separation distances (provided these are maintained by planning)

It is useful to explain why gas detection, ESD valves and relief systems have different characteristic degradation times from the above examples. Gas detectors are continuously active and subject to changing atmospheres and the sensor heads can degrade. It is sometimes observed that 1 or 2 detectors in an array can be out of service, pending maintenance – this degrades but does not fail the system. ESD valves are continuously powered (to stay open), but otherwise do no action until power is removed in an emergency – they do not need to maintain a calibration and are closed by stored energy. Relief valves are known to have low failure rates and 5 year inspection and recalibration intervals are typical.

The issue of barrier degradation can be characterized in Figure 2. This shows that at design time, all barriers are assumed fully functioning and that risk meets the corporate or community risk target. But over time in the example shown, Barrier 1 has failed and Barrier 3 is in an unknown condition (e.g. inspections and planned maintenance have not occurred). With dynamic barrier management, Barrier 1 is repaired and in this example Barrier 3 is replaced with an equivalent new barrier and the total risk is returned quickly to the target.

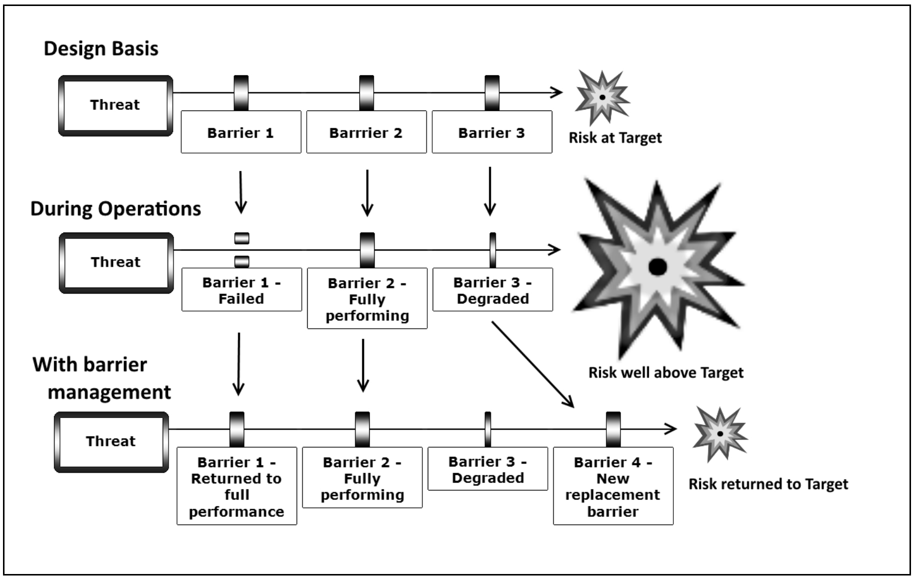

Figure 2. The issue of dynamic barriers and the need for dynamic barrier management

The concept of dynamic barriers and their impact on risk is shown in Figure 3. The left side of this figure shows traditional barrier management – barriers start initially at full capability and thus risk is at its lowest level, but risk rises in steps as individual barriers degrade. Downwards movement in risk indicates barriers have been repaired, but overall during operations the average risk is greater than the risk target as barrier repair is not necessarily focused on the most important barriers.

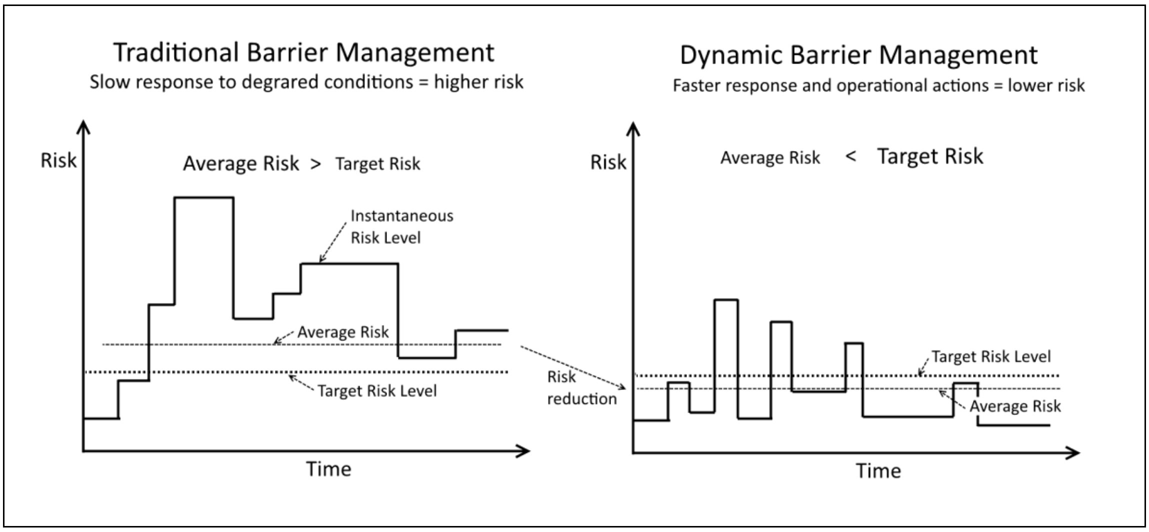

Figure 3. Relationship between Barrier Status and Overall Risk Level

The right side of the figure shows how risk levels might change with dynamic barrier management. Risk starts as before at the minimum when all barriers are functioning, and upwards movements correspond to barrier failures. But now a better system monitors barrier status and the most important barriers are prioritized for quick repair. The average risk is now below the risk target, which is the desired result.

Example Dynamic Barrier Management Strategies

While most companies adopt a fixed program for safety critical barrier inspection and maintenance, with little direct influence on daily operations, there are some interesting published examples showing how degraded barriers can be managed.

Permitted Operations

Detman and Groot (2011) describe an approach pioneered by Shell linking defined activities to required functioning barriers – called the Manual of Permitted Operations (MOPO). At its simplest, the approach maps all anticipated activities and defines the barriers that must be functional, in format similar to a cause and effect chart. A weakness of MOPO is that it assumes barrier status can be easily determined and it also assumes barriers are either working or broken, not degraded.

Cumulative Risk Modeling

Jackson (2013) describes a risk management tool used in BG that monitors changes in barrier performance during key activities. If barriers degrade (e.g. a safety device or key person is not available) then the risk goes up and this is compared to a target. The method is based on the swiss cheese model and degraded barriers are identified by automated linkage to risk assessments and inspection / maintenance systems, by manual linkage to safety overrides, and with reporting and reviews. A conventional green-yellow-red scoring system is used for decisions which are not automated. BG regards this tool as a powerful leading indicator for major accident hazards. There is not a strong risk model underpinning this approach however.

Statoil TTS and TIMP programs

DNV GL has worked closely with Statoil on the development of the TTS program (in English: technical condition of safety barriers). TTS was initiated around 2001 and was directly based on regular verification of key safety barriers. The method defined performance standards for all important safety barriers. These were all assessed in terms of their original design, their condition, and their operation and scored using a simple color-coded system – ultimately A – F ("A" means above requirements while "F" is failing).

More recently (Refsdal et al, 2013) describe an approach developed by Statoil and DNV GL for the Technical Integrity Management Program (TIMP) initiated in 2010 and has now been applied to 40 Statoil assets, onshore and offshore. It operates in conjunction with TTS. The purpose of TIMP is to provide an updated status of the technical integrity of barriers and production systems to ease decision making during e.g. operational and maintenance planning. It also ensures a common way of working across assets. The development of TIMP focused on 4 main elements:

- A competence scheme
- A work process with clear roles and responsibilities
- A methodology to promote an aligned evaluation of technical integrity
- A tool that captures and structure data from various information sources and presents it in a dashboard format

The key principle in the TIMP concept is to combine automatic data capture with manual evaluations from technical experts. TIMP supports a daily work process to manage the technical integrity of safety barriers and TTS verifies this every 5 years. The two tools provide a detailed mechanism to monitor and manage key safety barriers.

Electronic Safety Case Tools

There are multiple electronic safety case tools described in the literature, but many of these have a focus on ready availability and ease of updating, rather than a barrier performance focus. DNV GL has developed the e-Safety Case tool in Aberdeen and now being deployed for Dolphin and a safety case interactive tool developed for Gasco in Abu Dhabi.

While developed by different teams – these both have the objective of enhanced accessibility to safety case information and flagging of degraded barriers. The e-Safety Case can map and flag safety critical elements that have not met their performance standards according to the scheme of verification. The Abu Dhabi tool, implemented in SharePoint, delivers to all key individuals customized screens on a "push" basis highlighting their barriers and status of activities. This is superior to "pull" implementation where users need to search for such key personal information and responsibilities.

BSCAT Incident Investigation Tool

One of the potentially most fruitful sources of barrier status is currently also amongst the least used – this is incident information. A large facility may experience several actual loss events and over 100 near miss events annually. It is axiomatic that any accident or near-miss events mean that some barriers must have failed and presumably some must have worked – as there was not a disaster. Currently few investigation methods include barrier performance as an integral part of the investigation. The BSCAT tool (Pitblado et al, 2015) and the Tripod investigation approach developed by Reason and Hudson and used by Shell are exceptions.

BSCAT uses an incident bow tie showing all the barriers involved in an incident and which of those worked and which failed or performed below expectations (Figure 4). For each barrier that did not function properly a traditional SCAT root cause analysis (Systematic Cause Analysis Technique) is carried out.

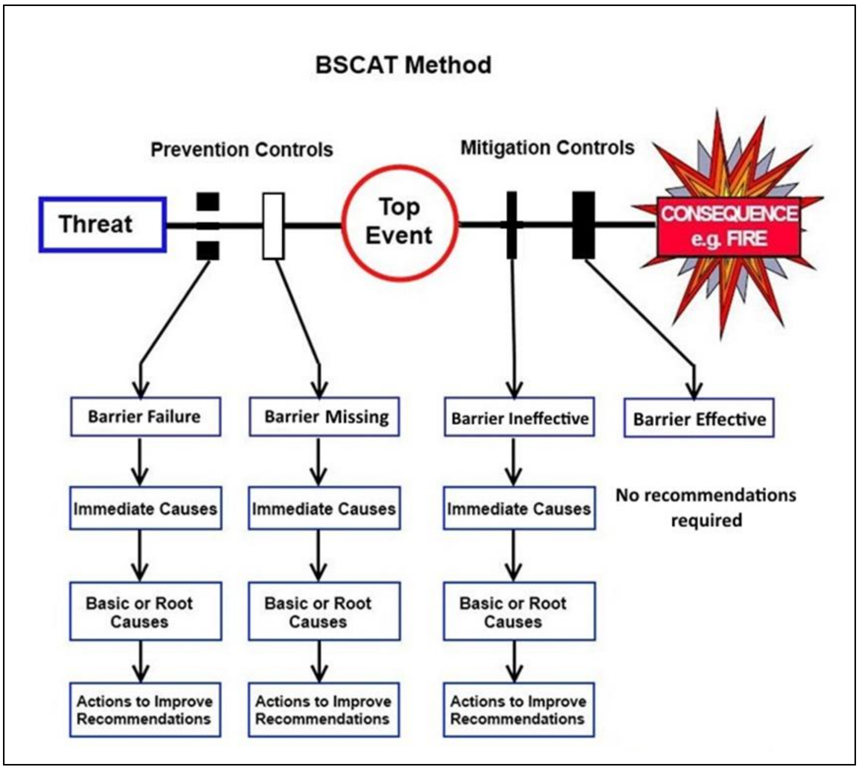

Figure 4. BSCAT methodology with symbols

This barrier failure information provides right-up-date status on all barriers involved in the incident. This includes information on barriers that can be hard to measure except during shutdowns (e.g. ESD valve functionality) or human systems that are incorrectly assumed to be working (e.g. just because training is completed). This information is more robust than scheduled measurements as the incident will have tested the barrier in a real scenario. It is particularly powerful as it provides direct measurements of barrier functionality, not limited by testing method.

Offshore Blowout Preventer Barrier Performance Tool

Nelson (2014) has described a novel approach for assessment of subsea blowout preventer performance. The 2010 Deepwater Horizon blowout event highlighted deficiencies with current BOP's – which itself is composed of multiple barriers (e.g. annular and shear RAMS, auto-breakaway shutdown, etc.). Current BOP designs utilize twin control pods (yellow and blue) to provide redundancy, but system level tests can mask single component failures before deployment, and battery rundown can disable elements (CSB 2014).

Safety Objective Trees are used as an extension to basic bow tie methodology. Safety Objective Trees have been deployed in the nuclear industry for many years and are focused on success attributes of systems rather than failures. The combination of the two methods allows to:

- Systematically identify information and instrumentation requirements
- Provide decision guidance to restore degraded or failed barriers or critical functions
- Develop an information architecture for decision support among offshore operators, industry groups, regulatory bodies, and the public

The method allows dynamic management of the BOP and allows better decisions as to when necessary to pull the BOP.

Dynamic Barrier Management Developments

Framework

A dynamic barrier management approach should not focus solely on safety, it should also integrate into operational and strategic decision making so that there is a holistic approach to barrier observation and management. A holistic model developed by the authors' company for the management of dynamic barriers is shown in Figure 5. This shows three separate calculation loops tracking the impact of barrier performance on risk levels – a baseline loop using initial barrier conditions but later updated for current status, a performance loop that focuses on barrier maintenance decisions, and a safety risk mitigation loop that focuses on operational safety decisions. The figure shows how degraded barriers increase risk (either quantitatively or qualitatively) and how risk can be returned to the risk target by operational decisions (e.g. delaying selected activities) or by maintenance decisions (e.g. repair strategy for degraded barriers). These decisions can both increase safety and decrease costs compared to current fixed interval strategies in a manner roughly equivalent to risk-based inspection. RBI is a proven technique that has been adopted very widely in the O&G and process industries.

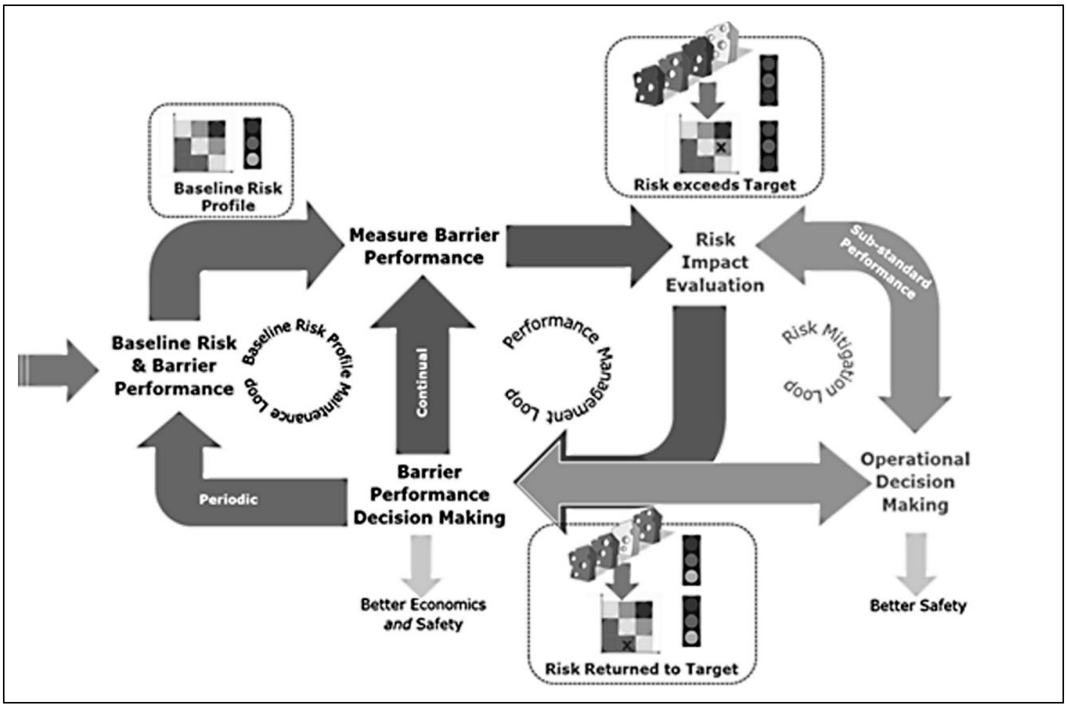
Baseline Risk Profile
Measure Barrier Performance
Risk exceeds Target
Risk Impact Evaluation
Sub-standard Performance
Baseline Risk & Barrier Performance
Baseline Risk Profile Maintenance Loop
Continual
Performance Management Loop
Risk Mitigation Loop
Periodic
Barrier Performance Decision Making
Operational Decision Making
Better Economics and Safety
Better Safety
Risk Returned to Target

Figure 5. Holistic barrier management with direct risk linkage for decision support

Barrier Management with Qualitative Risk Approach

SINTEF and the Integrated Operations Center in Norway has been working with partners (Conoco, BP, DNV GL) on a Risk Barometer approach that seeks to provide a real-time risk picture based on the status of barriers. They note that a typical North Sea offshore facility might have 2500 barrier elements that need to be tracked in a variety of database systems and administrative systems – SAP, Synergi, work permits, inhibit logs, etc. They propose tracking barrier status and a qualitative risk estimate defined between 0 -100, where 0 is nominal with all barriers fully functioning. Green – yellow – red risk categories are defined with nominal transitions at scores of 33 and 66. More rigorous thinking allowing for dependencies would reduce the transition scores to be 15 and 36 respectively. They also discuss a quantitative system where risk is directly linked to typical QRA results (FAR or PLL statistics), but this is judged more difficult. The risk result is used for daily and longer term decision making. No cost estimates are provided.

Barrier Management with Quantitative Risk Approach

The authors regard a direct linkage of barrier status to facility risk can provide for better management of barriers that enhances safety decisions while controlling or reducing barrier inspection costs.

Three problems commonly encountered with barrier management include: a lack of data for some barriers, poor understanding of data actually available, and over analysis of data. The lack of data is addressed through integration of several data sources as shown in **Error! Reference source not found.**. Some of these are conventional sources (e.g. CMMS – Computerized Maintenance Management Systems) but integrating this with incident data on barrier performance (Figure 1) , HR records for staff training and competence and process control system displays is less common and provides a richer indicator of current barrier status. Poor understanding relates to how decision makers use specialist system data. CMMS systems do not provide degraded barrier status in an easily understood format, only if the barrier is completely working or completely broken. Integrating several different datasets also provides context, for example a barrier test may be positive but it may fail in actual incidents. The final issue of over-analysis relates to exclusive use of one dataset directly without the integration of other datasets and thus a need to infer status without using the additional data available.

A newer technology for integrating large diverse datasets is termed “big data analytics” and this uses special database programs to interrogate and identify trends. This idea has been developed for major accident safety using High Reliability Organizations theory (Roberts and Bea, 2011) and they term this searching for “weak signals”. This is hard to do manually, but it is a good application for big data. Candidates for big data analysis might include for example SAP and Maximo for maintenance and inspection data, and Synergi for safety incident data. This idea is part of dynamic barrier management.

Simply searching for trends could be very time consuming and an optimization strategy is needed. This would focus attention on those barriers which contribute most to major accident risk reduction. Bow ties are qualitative figures and do not directly show the importance of individual barriers. The quantitative importance of barriers can be developed – in a generic sense for a typical offshore installation using Safeti Offshore – a modern example of a QRA tool (Bain et al, 2014). Since this tool relies on generic failure frequency data, it is better at defining the importance of mitigation barriers (e.g. gas detection, ESD, fire and blast walls, etc.) than it is for prevention barriers (e.g. corrosion protection, dropped object prevention, etc.). A qualitative barrier importance ranking system covering all Barrier Systems in NORSOK S-001 based on expert judgment is available from a major operator. The calculated quantitative importance for mitigation barriers is matched to equivalent qualitative rankings and based on this calibration the unknown preventive barrier quantitative importance's can be estimated. Once an estimate is available for all barriers then a strategy similar to that for risk-based inspection can be developed for barrier monitoring at design time. This strategy can be updated during operations using the big data analysis of the large volume of information being captured in the facility inspection, maintenance and incident recording systems.

Risk can be calculated in a detailed QRA model or in a simpler LOPA style model. In barrier terms

Risk = fn [Initiating event frequency *(pdf_1 *pdf_2 *…*pdf_n)* Consequence]

Here for a system with n barriers each with a probability of failure on demand: pdf_i

Prevention barriers affect frequency, mitigation barriers affect consequence (but non-linearly)

Barrier Importance can be defined as the impact on risk, based on barrier i status (where barrier status is defined in terms of its current pfd).

$\text{Importance}_{i} = (\text{Risk}_{1} / \text{Risk}_{0})$

given that $\text{Barrier}_{i,1} = \text{pdf}_{i,1} = 1.0$ (i.e. failed) and $\text{pdf}_{i,0}$ = design

Importance can be defined in other manners (e.g. Delta Risk/Delta Barrier), but this definition makes the Importance dependent on the initial reliability of the barrier (which can be SIL 1, SIL 2, or some intermediate reliability) and this makes comparisons of Importance more difficult compared to the definition proposed. But clearly SIL 2 barriers will generate greater impact to risk if they fail compared to SIL 1 or equivalent barriers.

If one conceives of a simple bow tie barrier diagram with one threat and one consequence and several barriers in between. If one of the barriers failed, a SIL 1 barrier – risk this would increase by 10x and if SIL 2 then by 100x. But risk is more complex than this. Typically there might be 10-20 bow ties, each with 5-8 threats – or 50-120 risk lines ending in a safety outcome. A single barrier failure here would increase the overall risk much less than considering a single risk line. The overall increase might be only 10%. Important exceptions to this are repeated barriers and dependent barriers.

Some barriers are repeated on many threat lines. This is especially common on mitigation barriers where the entire mitigation side is repeated many times (e.g. gas detection & ESD, ignition control, fire protection, and emergency response) for all loss of containment events. Prevention controls repeat less often but there are examples of this as well (e.g. work permit barrier, inspection system). Failure of a repeated barrier will increase risk much more than a single failure. In the limit, for example a mitigation barrier failed in every bow tie (e.g. fire protection system) – then the risk can increase by 10x or greater.

Dependent barriers are those whose operation is dependent on another barrier (e.g. if gas detection fails then subsequent safety barriers such as ESD, blowdown and ignition control will not operate quickly, as manual actuation would be required and this is too slow to prevent a major process safety incident for serious releases). If the design risk assessment treated these as independent mitigation barriers each with its own pfd, then the risk reduction in practice if gas detection fails will be much less then assumed.

Thus the impact of dependent barriers must be included in the QRA for quantitative approaches, or by means of a dependency table for the qualitative approach – as shown in Figure 1column for Risk Model.

The impact to risk can be directly calculated using the predefined Importance and accounting where relevant for repeated barriers or dependencies. Given the impact to risk, the operational safety decisions or asset performance decisions can be taken that reduce risk or optimize costs (as shown in Figure 1).

Conclusions

Barrier management is potentially the most powerful risk management approach that specifically focuses on major accident risks during the operations phase. The bow tie approach is commonly used to identify, structure and communicate barriers as a part of the barrier management. Typically 10-20 major accident bow ties can capture the most important barriers preventing or mitigating major accident events. These might contain 500+ barriers in total (and a larger number of individual elements), but not all of these will be unique, many barriers will repeat between different bow ties or in different arms of a single bow tie. While these figures are useful for the purpose of communications – they are poorer for ongoing operations as barrier performance is dynamic rather than static, and they are difficult to manage as identified by the PSA (op. cit.). For this reason, some form of dynamic barrier management, which monitors and accommodates barrier degradation is vital if major accident risk is to be properly controlled over the facility lifecycle. This is not simple as different barriers have their own characteristic degradation rates.

The paper has reviewed several systems used in the offshore industry by Shell, BG, Statoil, SINTEF, and DNV GL. These all provide some part of the solution but not the holistic result which is needed. A system which integrates multiple datasets is suggested. At design time, an initial barrier monitoring strategy can be developed which considers the importance of barriers in preventing or mitigating major accidents and then ranks these using a system similar to risk based inspection. During operations, real data becomes available. This would include: 1) inspections, audits and reviews; 2) sensor data and condition monitoring; 3) near miss and incident data; 4) maintenance and test records, and 5) personnel training and competence records. Several of these are contained in large database programs and in mixed formats and some form of big data analytics would enhance identification of relevant trends, the status of degradations, and weak signals indicating safety problems.

Dynamic Barrier Management has the potential to maintain major accident risk levels at their target throughout the life of the installation, allowing degraded barriers to be returned to their performance target more quickly and economically than is the current situation. A major benefit is also to alert staff and local management teams earlier to degraded barriers and how the risk levels are potentially increasing dramatically unless remedial action or alternative barriers are implemented. It also allows the facility Mechanical Integrity program to focus on the barriers that contribute most to risk reduction.

References

Astrup O.C., Wahlstrøm A-M., King T., 2015, A framework for addressing major accident risk in the maritime industry. SNAME 5th World Maritime Technology Conference. Rhode Island, Nov 3-7.

Bain B., Worthington D., Spitzenberger C., Falck A., 2014, Modeling the progression of an offshore hydrocarbon release accident, Mary Kay O'Connor Annual Symposium, Texas A&M University, College Station, Oct 28-30.

CGE Risk, 2013, BowTie Methodology Manual, Rev 14, available from CGERisk.com website.

CSB, 2014, Explosion and Fire At The Macondo Well, Investigation Report 2, US Chemical Safety and Hazard Investigation Board, Washington DC.

Detman D., Groot G., 2011, Shell's experience implementing a manual of permitted operations, 14th Annual Symposium Mary Kay O'Connor Process Safety Center, Texas A&M University, College Station, Oct 25-27.

DNV GL, 2014, Barrier and Bow Tie Diagrams – Methodology Manual. Risk Reliability and Human Factors Technology Leadership Group. Jan 14, 2014, rev 1. Available on request from Robin. Pitblado@dnvgl.com

Jackson, N., 2013, Cumulative risk modeling in BG, Piper Alpha 25 Conference, Aberdeen (18 Jun 2013)

Nelson B., 2014, Joint Industry Project - Decision Support for Dynamic Barrier Management, DNV GL 2015.

Pitblado R., Potts A., Fisher M., Greenfield S., 2015, A Method for Barrier-based Incident Investigation, Process Safety Progress Journal, 34 (4): 328-334.

PSA, 2013, Principles for barrier management in the petroleum industry, Norway Petroleum Safety Authority, available at PSA website (checked July 2015) http://www.ptil.no/getfile.php/PDF/Barrierenotatet%202013%20engelsk%20april.pdf

Refsdal I., Østby E., Børve O., Stokke A., 2013, A step change in managing technical integrity in the oil and gas industry - a case study from Statoil, Technical Conference at Total Center, Pau, France.

Roberts K.H., Bea R., 2011, Must accidents happen? Lessons from high-reliability organizations. Academy of Management Executive 15 (3):70-79.

Zuijderduijn C., 2000, Risk management by Shell refinery/chemicals at Pernis, the Netherlands. EU Safety Conference: Implementation of the Seveso II Directive, Athens, Greece.