CHEMICAL ENGINEERING TRANSACTIONS
VOL. 31, 2013
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at: www.aidic.it/cet
Guest Editors: Eddy De Rademaeker, Bruno Fabiano, Simberto Senni Buratti

ISBN 978-88-95608-22-8; **ISSN** 1974-9791
DOI: 10.3303/CET1331056

Advanced Safety Barrier Management with Inclusion of Human and Organizational Aspects

Robin Pitblado and William R. Nelson

DNV, 1400 Ravello Drive, Katy TX 77441, USA
Email: robin.pitblado@dnv.com

Recent major accidents have shown that the human element is not adequately treated in current risk assessments and during facility operations. A novel approach is described which combines barrier based risk assessment (the bow tie risk model) with a nuclear industry approach "Success Pathways" which provides more thorough treatment of human factors and organizational objectives. In operations, barriers are often degraded, and a system driving to near-real time barrier status has been developed which combines inspection, maintenance, audit and incident investigation methods. The Integrated Operations idea from Offshore Norway allows additional robustness to decision making.

1. Accident Trends

1.1 Occupational vs Process Safety

The Oil and Gas (O&G) and process industries have been very successful in improving occupational safety, but conversely less successful in improving process safety / major accident performance. These have been long duration trends in both areas (as shown in Figure 1) and this reinforces the recognition that occupational safety and process safety are different (Baker Panel, 2007) and require different approaches to drive positive results. The authors have developed Figure 1 using data for occupational safety taken from company annual reports and the 5 year loss statistics from Marsh (2011).

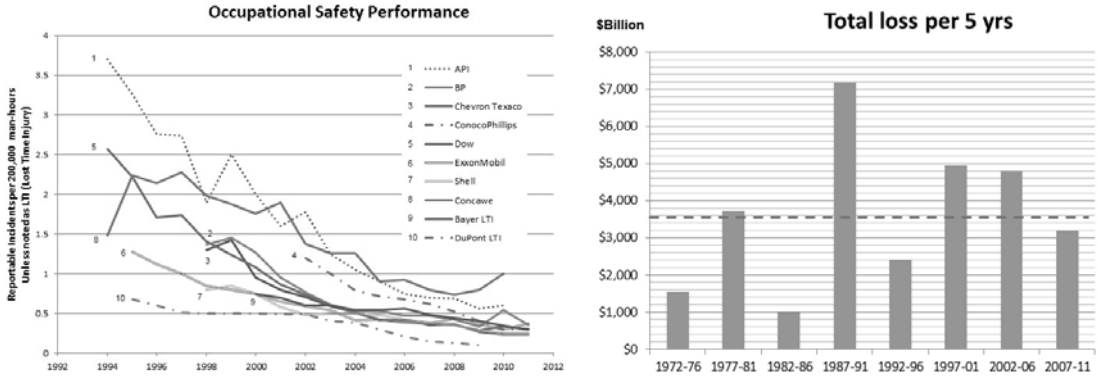

Figure 1: Comparison of Occupational Safety Performance with Process Safety Performance

2. Process Safety Risk Management Approaches

2.1 Barrier Risk Management (Bow Ties)

Several levels of risk approach have been applied to onshore and offshore O&G facilities. These range from simple Process Hazard Analysis (PHA) studies with risk ranking to very detailed quantified risk

Please cite this article as: Pitblado R. and Nelson B., 2013, Advanced safety barrier management with inclusion of human and organizational aspects, Chemical Engineering Transactions, 31, 331-336 DOI: 10.3303/CET1331056

assessment studies. Both these study types are well suited to addressing safety issues arising during design, but they are poorer for managing operational risks, and for these a barrier diagram approach, often termed bow tie diagrams has been more widely promoted. The EU ARAMIS Project examined the application of bow tie risk assessment to onshore process safety (Salvi and Debray, 2006) and the IADC (2011) recommends this approach to underpin HSE cases for offshore applications.

The bow tie risk model implements the so-called Swiss cheese model of Prof Reason. It shows threats as arrows continually challenging safeguards (i.e. barriers) and since these are not 100% reliable or effective, multiple barriers are required to assure to some level of risk that threats do not escalate to bad outcomes. The layout is standardized with threats positioned on the left passing through various prevention barriers and reaching the Top Event – which may in the process safety context be a loss of containment or a loss of control event. Further progression is possible through mitigation barriers to the ultimate outcome – which may be fire, explosion or other undesired outcome. A simplified diagram is shown in Figure 2.

In principle the bow tie risk diagram can address hardware, administrative and procedural controls, either on the main pathways as shown in the simplified diagram, or on separate branches called escalation factors. In fact the bow tie is a simplified representation of a fault tree diagram where each barrier is an AND gate with two inputs – a demand AND barrier fails. An escalation branch is just building out the barrier fails arm from an undeveloped event to one that is developed – showing the means in place to maintain that barrier. Thus if Inspection program was a main pathway prevention barrier, then the escalation pathway for inspection fails might have barriers such as appropriate inspection technique, adequate inspection interval, inspection device calibration, and inspector training and competence.

Thus properly developed, a bow tie diagram offers much of the qualitative capability of a fault tree diagram and it is this linkage that underpins the systematics of the approach.

A requirement of fault trees and thus of bow ties is an assumption of barrier independence. While technically or administratively this may be true, there are overarching organizational or cultural aspects that can degrade multiple barriers for common reasons (Hopkins, 2012).

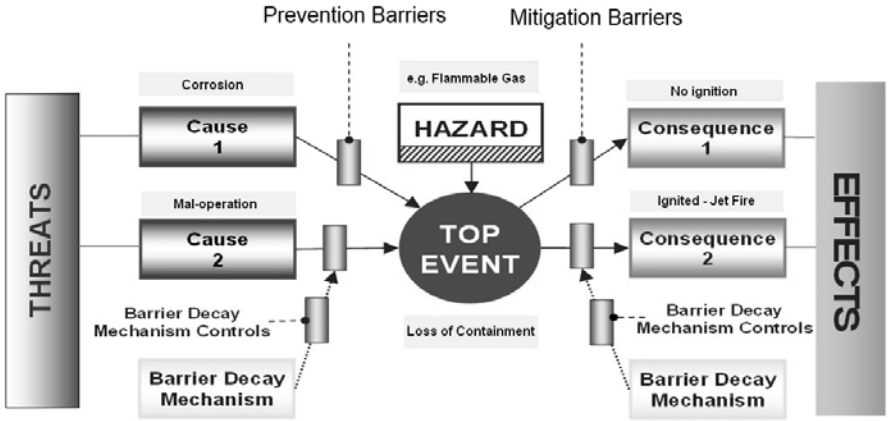

Figure 2: Example Bow Tie risk assessment diagram

An example might be a top management directive that no longer tolerates delays or overruns to projects. This can have the effect of degrading many barriers if their implementation or functioning requires time or resources beyond the current plan. What might appear to be a well-protected system with multiple barriers can in fact have many fewer if resources are not devoted to maintaining them. The bow tie, like the fault tree, is poor at capturing these overarching influences, but they important to overall system safety and a systems process is important (Leveson, 2011).

Thus an important aspect for barrier diagrams would be to include these overarching organizational drivers and to model them in parallel with conventional barriers.

2.2 Safety Objective Trees

The nuclear industry has long used a barrier management approach, termed Defence in Depth, to ensure that an adequate number of barriers protects against serious nuclear accidents. While not in the bow tie format, the approach includes many of those ideas and is built on PRA fault tree models. An extension to this includes a methodology termed Safety Objective Trees (Hanson, et. al 1990). They show important information about critical functions and the strategies or success paths for maintaining them or restoring them if they are challenged (see Figure 3). In this figure, the top level shows the overall safety objectives

– keeping the reactor core within the reactor vessel, maintaining the integrity of the containment building, and mitigating the dispersion of radioactive materials if they are released from the containment. The second level shows the critical functions for containment integrity – temperature control, pressure control, and mechanical integrity. The third level shows types of challenges or phenomena that could endanger the pressure control critical function. The fourth, mechanism level shows the specific types of physical phenomena that could challenge the critical function. And finally, the strategy level shows the available resources or success paths that are available to respond to a critical function challenge. The primary advantage of the critical function approach is that it is based on achieving essential safety objectives and critical functions, but does not depend on an accurate diagnosis of the event in progress.
All commercial nuclear plants in the US have developed accident management procedures that combine the event-based (or barrier) approach with the critical function approach. The combined approach allows for efficient response if the event can be diagnosed accurately, but provides additional protection of the critical function approach to ensure that the response is effective, and to implement a success path to restore the critical function.

2.3 Combining Barrier Models with Safety Objective Trees

After Macondo, it was recognized that the current approaches used in offshore drilling safety, while mostly successful, do allow for failures. The combination of the safety objective method with bow tie risk assessment appears to offer an important advance, combining all the benefits of both methods. It also breaks down industry “silos” and it combines the wealth of experience from the nuclear industry with the barrier methods from the process industries to form a much more robust system for incident assessment and management. The use of bow tie diagrams adds additional definition of the barrier concept to support the event-based element of assessment and response.

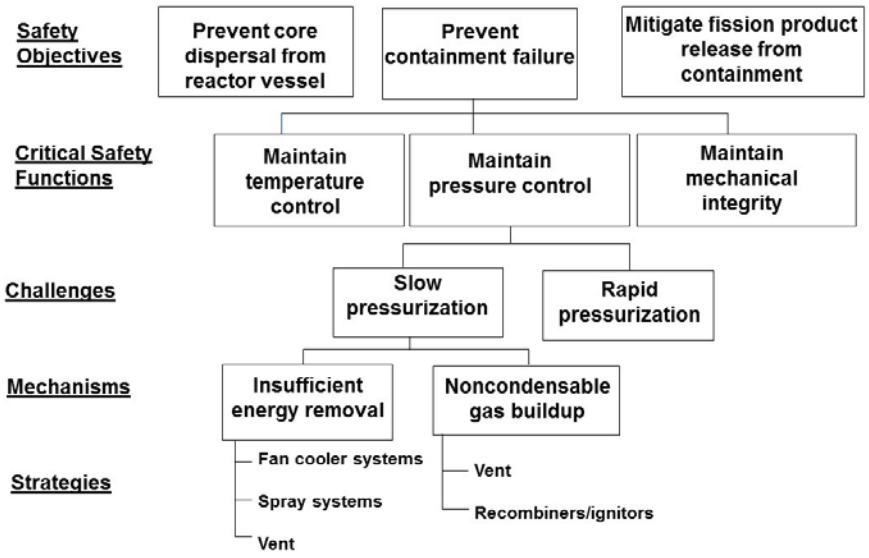

Figure 3. Example nuclear safety objective tree

3. Application to Drilling Safety

DNV is working to combine safety barrier methods with critical function methods such as safety objective trees to provide effective decision support for drilling safety, including well control and blowout prevention. Figure 4 shows conceptually how the two paradigms are combined to provide robust decision support for well control and blowout prevention. This concept can be thought of as analogous to the use of an automobile Global Positioning System (GPS) to navigate from the current location to the desired destination. The GPS performs these functions by providing information about current location, the availability of potential routes or pathways to navigate to the destination, and guidance in the form of “turn by turn” instructions to reach the destination.

Similarly, Figure 4 shows conceptually the process of moving from the current known location to reach the desired destination – i.e. achievement of the safety and performance goals. The horizontal axis of the

diagram represents the safety barrier approach, showing the presence of barriers to impede the progression of an event from a hazard to an accident. The vertical axis shows the maintenance of the critical functions and possible pathways for achieving performance and safety goals such as Continuous and Safe Production. The dotted circles illustrate examples of critical decisions that must be made to change the trajectory of the event to follow a pathway to achieve performance and safety goals rather than proceeding further along the trajectory towards an accident. This diagram also highlights the important human role to intervene in event sequences where barriers may be missing or degraded.

In order to support these critical decisions the following types of information are required:

- The current location in the 2-dimensional decision space, determined by process condition and status of plant equipment
- Health of the barriers
- Health of the critical functions
- Availability of success pathways
- Guidance for selecting a success pathway for maintaining the critical functions and achieving the safety and performance goals

Bow tie diagrams and safety objective trees are used to organize the information needed to determine the current location and provide guidance to select a pathway for responding to the current situation. To fully implement this concept in the offshore drilling or production environment will require the development of specific decision algorithms for the target application – e.g. well control and blowout prevention – and interface to actual instrumentation for the target processes and systems. Possible analytic tools such as Bayesian Networks (Pearl, 1988) are being investigated to capture the knowledge and the algorithms for understanding the health of barriers and critical functions and providing guidance for selecting an effective pathway for the situation.

DNV is currently working with the Norwegian Integrated Operations (IO) Centre to identify industry partners and pilot projects to implement and test this concept in the deepwater offshore environment. In general, Integrated Operations is the concept to establish on-shore operations centres to monitor and control offshore installations, both to increase efficiencies and to reduce offshore staffing. This environment will serve as an effective test bed for evaluating the safety and production benefits for the combined safety barrier and critical function approach.

The method is also being deployed with a US drilling company to identify technology innovations and improved methods for human-system integration that could substantially improve the safety of deepwater offshore drilling. The combined barrier and critical function approach is being used as the framework.

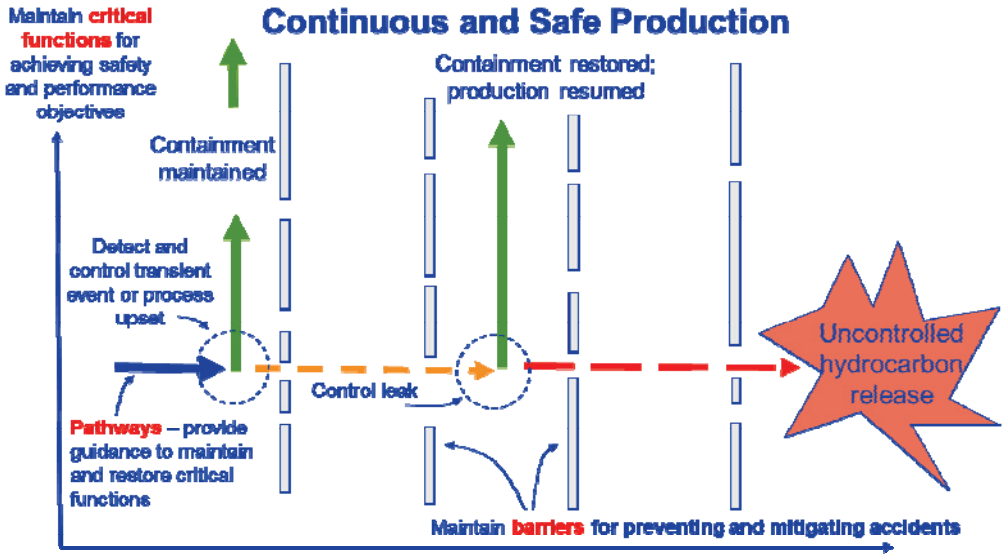

Figure 4. Combining safety barrier management with critical function methods

4. Knowledge of Barrier Status

4.1 Background

A key feature to managing barriers is knowledge of their current status. In principle technical, administrative and procedural controls can have realistic reliability / effectiveness targets. However, as noted above human factors and organizational influences can have overarching influences and lead multiple barriers to become subject to dependent failures.

Some companies have developed systematic approaches to operating only within pre-determined safety boundaries and this is based on all needed barriers being functional when activities are undertaken. Shell (Detman and Groot, 2011) describe a system called Manual of Permitted Operations, also known as Summary of Operational Barriers (SOOB), to map necessary barriers for all specified activities. These are derived from risk assessment bow ties and constructed by experienced operations staff. The list is like a cause and effect chart – with activities down the page and barriers across the top, a marked intersection means that that barrier is needed for that activity to proceed. This takes the operational decision away from the local site person who may be under pressure and who may not have a good appreciation of the potential risk associated – especially for rare major hazards, and places it instead with a process safety specialist. While the system does not prevent wilful non-compliance, it does provide very clear support for staff under pressure to resist activities that are unsafe due to degraded barriers. The system is also not specific the degree of degradation of a barrier to be considered non-functioning. For example if two gas detectors in an array of 50 are not functioning – can operations still proceed? That may be straightforward, but if the number were 20 and all were in one direction with respect to the wind – the answer may be different.

Prediction of such failures is difficult as accepted structural models showing the effect of human and organizational factors on barrier performance is not yet available. However, if barrier performance can be measured, then it will show such effects. For this to be useful, the measurement of barrier performance against its target needs to be current.

An example of selected barriers and information sources on status are provided in Table 1.

Table 1: Example Barriers and means to establish status

Barrier example	Means to establish status	How current
Inspection program	Audit	3 yearly audit is typical
Preventive Maintenance	Audit	3 yearly audit is typical
Inspection or PM item	Inspection result	External inspection frequency 6-12 months is typical – for some items internal inspections may be 5 years. PM as per manufacturer recommendations – may be several years.
Relief valve	Bench test	5 years
ESD valve	Actuation test	At unit shutdown (scheduled 2-5 years) or by disconnecting valve actuator more frequently – 6 months
Gas detection device	Calibration test	As per schedule – may be 6-12 months
Training course	Test certificate	Original date plus retraining interval (3 years)
Fatigue management	Audit	Annual
Work permit system	Audit and record review	Audits 3 years, record review maybe 3 months

As may be seen from this table, unless an item is physically broken and obvious to visual inspection, then the cycle time to determine the frequency can be 3-6 months at best and 3-5 years at worst. There are exceptions to this. SIL-rated items will have a specified probability of failure on demand (PFD), and a program to sustain the item at that level will be necessary – and this could involve more frequent measurements than implied by the table. Such programs are actually hard to implement in practice and many sites may not be able to demonstrate the specified “PFD”.

Thus establishing the current barrier condition is more of a challenge than is often recognized by approaches such as MOPO and SOOB.

4.2 Using Incidents for Barrier Status

Incidents unfortunately are still relatively common on large sites – and can number several hundred per year when near misses are included. Today incident investigations are often divided into simple and more

detailed based on actual or potential severity. Full root cause analysis using techniques such as TapRoot, MORT, 5 Why's, SCAT, etc. might be applied to the more severe category, but with simple analysis for minor incidents and most near misses leading only to direct causes. Neither of these broad approaches has a barrier focus. Root cause analysis is primarily seeking a management system deficiency, and direct cause is not necessarily barrier related. The Tripod method has a link to barriers, but it is very resource intensive and requires specialist skills.

A new method, DNV BSCAT™ (Pitblado and Fisher, 2010), has a direct focus on barriers. It is applied to the most relevant pathway in the risk assessment and the incident is examined in this context. The performance of every barrier is assessed (failed, degraded, worked but ineffective, successful) and where ineffective the full root causes are established. This approach has the advantage that every incident is examined in the context of the facility risk assessment and the performance of every relevant barrier is monitored. A typical bow tie pathway might have 5-7 main pathway barriers – to get to the final outcome, and near misses maybe half of this on average. If escalation factors are included those barrier counts might double. This every incident has the potential to deliver barrier status information on 8-12 barriers and near misses 4-6. If a site has 200 incidents per year, this means information on 1500+ barrier actions can be collected. Not all of these will be different barriers, but that means multiple barrier status measures are obtained on critical barriers (work permits, training, gas detection, etc.) as they appear in so many incident bow tie pathways. This compares with three yearly audit results on systems and 3-6 months on many safety systems.

Since barrier based operational strategies (e.g. MOPO) require current barrier status, it is the authors' view that investigation approaches focusing also on barriers and not just root causes must become the norm in the future if process safety is to improve.

5. Conclusions

The ongoing series of major accidents shows that current major accident management programs are not sufficiently effective. The barrier approach appears to offer additional focus on process safety during operations. It has been used in the offshore industry in the UK, driven by the Offshore Safety Case Regulations which require this focus – and major accident performance has improved. The nuclear industry also deploys a barrier defence in depth, but with an additional element to address better organizational objectives. This nuclear approach has been combined with the barrier approach for a drilling application and this appears promising. The organizational part addresses issues such as common organizational causes degrading multiple barriers simultaneously, which a traditional barrier model does not address. An important aspect is more up-to-date information on barrier status and the novel BSCAT investigation process, assessing barrier failures in incidents significantly improves this knowledge. Finally, the Integrated Operations approach, which creates strong operational teams with onshore and offshore staff, should permit greater real-time assessment of barrier status and hence deliver greater offshore safety.

References

Baker Panel, 2007, The BP U.S. Refineries Independent Safety Review Panel, <www.bp.com/bakerpanelreport>, accessed 10.01.2013.

Detman D., and Groot G., 2011, Shell's Experience Implementing a Manual of Permitted Operations, Mary Kay O'Connor Center Process Safety Symposium: Beyond Regulatory Compliance, College Station, Oct 25-27, 32-51.

Hanson D.J., Ward L.W., Nelson W.R., and Meyer O.R., 1990, Accident Management Information Needs, US Nuclear Regulatory Commission Report NUREG/CR-5513.

Hopkins, Andrew, 2012, Disastrous Decisions – the Human and Organisational Causes of the Gulf of Mexico Blowout, CCH Australia Ltd, Sydney.

International Association of Drilling Contractors (IADC), 2011, HSE Case Guidelines for Mobile Offshore Drilling Units, Issue 3.4 (1 Nov), Houston, TX.

Leveson N., 2011, Applying systems thinking to analyze and learn from events, Safety Science, 49, 55–64.

Marsh, 2011, The 100 Largest Losses 1972–2011, 22nd Edition, Marsh and McLennan Group, USA.

Pearl, J., 1988, Probabilistic Reasoning in Intelligent Systems, Morgan Kaufmann, San Francisco, CA.

Pitblado R.M. and Fisher M., 2010, Novel Investigation Approach Linking Management System and Barrier Failure, European Refining Technical Conference (ERTC), Barcelona.

Salvi O., 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, 187–199.