Creating an effective BowTie barrier based Process Safety Management System (and how to avoid getting tied up in knots in the process)

Ian Baulch-Jones, Lead Engineer – Asset Management Systems, E.ON Global Unit Generation
Paul McCulloch, Process Safety Specialist, E.ON Global Unit Generation
E.ON, Westwood Way, Westwood Business Park, Coventry, CV4 8LG, United Kingdom

This paper describes the challenges encountered and how they were overcome in building an effective BowTie barrier based process safety management system, capable of operating across multiple power generation technologies crossing national boundaries, that seamlessly answers the three key questions of process safety:

1) Do we understand our hazards and the risks associated with them?

2) Do we have controls in place to effectively manage the risks?

3) Do we know that our controls will be effective if required?

It is based on the Highly Commended IChemE 2014 Process Safety Award submission "Bringing New Life to Process Safety". In answering the three questions it challenges the blinkered use of the word safety when assessing process safety risk due to the narrow connotations that can sometimes be inferred from it. Instead it advocates a wider understanding of the commercial, environmental and regulatory consequences of events in order to quantify business risk and successfully engage with the wider business community to de-mystify process safety management and bring it to the table of effective business management.

Keywords: Safety, Process Safety, Hazard, Asset, Risk, BowTie / bow tie, Top Event, Barrier, Threat, Consequence, LOPA (Layers Of Protection Analysis), Audit, Presence, Performance, Compliance, Governance, Incident Investigation, HAZID / HAZOP,HSE (Health and Safety Executive)

The Challenge facing us? Understanding the business context

Background to what was required. How big is the Elephant?

E.ON is a large organisation operating internationally across a number of sectors related to energy. This paper describes the journey undertaken within the Power Generation arm of E.ON, specifically the fossil fuelled areas, although the methodology developed is now being adopted across all areas including Hydro and Renewables.

E.ON's power generation arm has grown internationally both organically and through acquisition, including assets from many former state run industries. The result was a pan-European portfolio of power generation capacity organised initially on a per country basis and more recently on a per technology fleet basis, with little cross over between the five technology fleets of:

- CCGT (Gas Powered)
- Steam (Coal Powered)
- Hydro (Water Powered)
- EC&R (Renewables)
- Nuclear

Our challenge was therefore to build an effective process safety management system capable of operating across multiple power generation technologies and crossing national boundaries and organisational cultures. It had to be simple to understand and use by personnel, yet provide powerful insights for management at all levels by creating a comprehensive and repeatable view of risk that can be used to target effective risk reduction via a transparent investment model based upon agreed risk reduction criteria. Finally it also had to be sustainable over the longer term by looking at the ongoing performance of key controls and the health of the underlying management systems that support them, forming a decision support tool where areas for improvement (either locally or on a pan-fleet level) are identified. In short it should:

1. Apply to all power generation technologies
2. Be easy to understand
3. Provide powerful insights for all employees
4. Produce a repeatable view on risks and the effects of risk reduction
5. Measure controls and the health of the underlying management systems that support them
6. Act as a decision support tool for improvement actions

What are we trying to achieve? Begin with the end in mind

How we approached the challenge. Forming the question in a language everyone can understand!

Just as all roads lead to Rome, so all roads in Process Safety now lead to whether you can answer the three questions for businesses posed by the Health and Safety Executive on the courtroom steps following the Buncefield trial[1].

From the Boardroom Down companies must ask themselves these questions:

1. Do we understand what could go wrong?
2. Do we know what systems are in place to prevent this from happening?
3. Do we have information to assure us that they are working effectively?

Taken in the round these three questions succinctly encapsulate what is meant by Process Safety Management. Many organisations will claim to be able to answer all three, but the ease of demonstrating adherence as you work from 1, to 2 and finally 3 changes until the evidence available in effectively answering question 3 to provide a high degree of assurance (whether it be to senior management or to the regulator) becomes actually quite hard once you start turning over the rocks and looking at what you find underneath.

However, the language contained within the three questions is a highly effective sound bite as it is:

- Short (three questions)
- To the point (aligned with risk assessment)
- Easy to understand (linking cause and effect) meaning that its message is easy to communicate across all levels of the organisation and its stakeholders. Process safety should not be shrouded in mystery or rituals, and for us we have built an entire process safety management system with "line of sight" to the three questions forming the back bone.

The answer's HAZOP, now what's the question? There has to be a better way!

Following several major Process Safety Incidents around the world in recent years a number of organisations in the high hazard arena, in an endeavor to demonstrate that tangible action was being taken, have gone down the route of HAZOPing everything in their portfolio. In the context of our project, however, we were sceptical about the practicalities and the benefits of adopting the HAZOP approach for a number of reasons:

- We believed that at a generic level most of our power stations were very similar, performed repetitive processes and operated similar controls
- The army of people required to HAZOP a portfolio of our size would not be able to adopt a transparently common methodology
- The process of HAZOPing everything would have taken a long period of time if it was to be carried out properly
- The potential improvements identified across the asset base would be difficult to rank against each other when competing for resources to give the biggest effective risk reduction (getting the biggest non-bang for the buck)
- Adopting a HAZOP approach would not systematically identify common risks and generate the synergistic improvements achievable in risk reduction when operating a fleet (portfolio) of assets
- HAZOPs generate high numbers of actions although it is often difficult to demonstrate that these have been closed out, leaving the organisation potentially vulnerable through discoverability and culpability should there be an incident at some future time
- The fact that a HAZOP may identify a barrier does not attest to the effectiveness of the barrier should it be called upon if an event occurs
- In order to be able to improve over time there was no effective way of linking incidents (be they real or potential, from internal or from the wider industry) back to HAZOPs in order to be able to assess actual levels of risk on plant

HAZOP was therefore rejected as the tool of choice for the challenge faced. Whilst it is still a valid tool in its own right (this paper is not intended as a HAZOP "bashing" exercise) it was believed not to be the right one for an operational process safety management system, as it gave a sub-optimal use of time and resources in answering the three questions across a portfolio of assets. This left us with the dilemma of what to use in its place. Thankfully an answer was at hand.

[1] Gordon MacDonald, Health and Safety Executive, 2010

Getting back to basics with Process Safety Management

How to eat an Elephant? One hazard at a time!

At the risk of sounding like a record that has got stuck in the same groove (a phrase from a technology of a bygone age that is making something of a resurgence) we focused all of our efforts on the insightful words of the HSE:

From the Boardroom Down companies must ask themselves these questions:

1. Do we understand what could go wrong?
2. Do we know what systems are in place to prevent this from happening?
3. Do we have information to assure us that they are working effectively?

The authors make no apologies for "banging the drum" with this message, as it has proved to be an effective rallying call within the organisation under which to galvanise all efforts under the Process Safety banner. To demonstrate why this is so effective, before we continue, let us examine what is being asked of us, as the three questions in reality pose nothing more than the five requirements from a risk assessment[2]:

- Identifying the Hazards
- Identifying who might be harmed and how
- Evaluating the risks from the identified hazards
- Recording
- Review and revision

As this project was focused on Process Safety rather than Occupational Safety it is important to understand some of the differences between them and the following taxonomy was used:

Personal Safety	Process Safety
High Frequency	Low Frequency
Low Complexity – simple cause, active failure	High Complexity – multiple active and latent failures
The agent is often the victim	The agent is often not the victim
Often personal experience (knowledgeable)	Rarely personal experience (not previously experienced)

Table 1 – Personal versus Process Safety

The conclusion we drew from this is that a far more complex and organisation wide approach is required when applying the ERICPD hierarchy of controls to Process Safety than to Occupational Safety:

- Eliminate the hazard
- Reduce or substitute the hazard
- Isolate or separate the hazard
- Control using a safe system
- PPE
- Discipline to follow operating procedures

The thread that runs through all of this, however, is hazard. Just as all journeys start with a single step, so all risks start from a hazard. The principles behind Occupational Safety risk assessments are well understood in business, and Process Safety should be no different. We were not starting with a blank canvas though as we were working with existing plants, meaning that we were effectively starting part way through the hierarchy of controls. Therefore, rather than coming up with a suite of Process Safety Metrics first (to answer Question 3) and working backwards (other than at the management controls level, e.g. Plant Modifications), the starting point should always be an understanding of what are your hazards (to answer Question 1) and working forwards through the steps. Otherwise management cannot demonstrate a "line of sight" back to the hazards that they are trying to control. There is no silver bullet panacea to this, and it is a very linear approach, especially as you have to demonstrate review and revision at the end (the HSE's third question and the elephant in the room for process safety management). Elephants are big creatures, but once you understand what your particular elephant looks like you eat it one hazard at a time, or you don't eat it at all.

[2] Management of Health and Safety at Work Regulations 1999, Approved Code of Practice, pages 9 to 11

How to demonstrate the five steps and ERICPD at a process plant level? Pre-requisites for tool selection

On page 3 we outlined why HAZOP was not the chosen tool. We therefore required a suitable alternative that possessed the capability of answering all three questions.

In short the authors do not believe that there is any one single tool that can answer all the three questions. If there is we would like to know about it. There were, however, a number of tools that provided some of the pieces to the jigsaw. Whilst there were pieces, it was the picture on the front of the virtual jigsaw box that we held in our minds eye that held the key to placing them together to form a coherent image that we could communicate across the organisation. Here we soon identified a number of "out of the box" tools that were being used as point solutions and not at the enterprise wide level, e.g.:

- HAZID
- Engineering Standards
- BowTie analysis
- LOPA
- Audit
- PT-Risk[3]
- Incident Investigation

Individually these tools were not enough, but collectively they could be moulded together to form an effective system that could:

- Identify the Hazards
- Identify the events leading to loss of control of the Hazards
- Identify the threats leading to the loss of control
- Identify the consequences resulting from the release of the hazard (safety, environmental, commercial, regulatory)
- Identify the barriers in place to prevent the threat from leading to the event
- Identify the barriers in place to mitigate the consequence of the release
- Identify the target effectiveness of the barriers to reduce the frequency of events to a tolerable level
- Identify the target effectiveness of the barriers to reduce the consequences to a sustainable level
- Communicate the requirements to both Engineering, Operations and to Management
- Check on the deployment of the requirements in the field
- Form the basis of continual ongoing improvement by linking to the results of incident investigation, whether real or high potential incidents
- Be used to influence future plant design

I.e. a Process Safety Management System, not a series of discrete activities tack welded together and called a Process Safety Management System.

Rather than re-invent the wheel we simply applied a unique combination of a number of previously disparate tools to create a holistic real world solution that acknowledges the competing and different pressures faced by the stakeholders involved in managing plant throughout the end to end lifecycle of the asset and the portfolio of assets within which it sits. We did this by combining a detailed knowledge of process safety management tools and techniques with leading management systems experience[4], seamlessly integrating it together using a simple yet powerful IT application to provide the platform to drive risk reduction. The management systems experience and the IT platform are essential as they provide the glue to bind everything together. Systems can degrade over time, or can be bypassed, and without this glue effective governance of the system would be impossible.

[3] PT-Risk (Power Technologies Risk) is a proprietary E.ON software tool for managing risk
[4] The authors' experience crosses a number of Management System Standards

Water, water everywhere, nor any drop to drink

People manage Assets, not Hazards. Process Safety Management Systems manage Hazards, not Assets.

Like the sailor from the Rime of the Ancient Mariner5 the issue for people working on a process plant is that they are surrounded by hazards, e.g. high pressure steam is all around you when you work in a power plant. They may therefore feel unable to directly influence the management of the hazard, and process safety then begins to become detached from the day to day routine. To follow the literary metaphor if you ask someone to manage High Pressure Steam you are effectively shooting the albatross and will have to helplessly stand aside and watch as the enthusiasm for the Process Safety Management system slowly dies before your eyes (management exhortations are not enough if there is no effective methodology to implement) and the albatross will be hung around the neck of management as a sign of their failure.

The reason for this is that managing a hazard can be an abstract concept for Engineers more used to managing assets:

1. You have specifications for assets
2. You have acceptance tests for assets
3. You have operating procedures for assets
4. You have alarms for assets
5. You have conditioning monitoring for assets
6. You have routine inspections for assets
7. You have routine maintenance for assets
8. You have outage (shut down) inspections for assets
9. You have outage (shut down) maintenance for assets

These are all preventive actions which should be aligned to maintaining control over the hazard. Once control over the hazard is lost, however, you are then into minimizing the consequences of the event:

a. You have detection systems
b. You have suppression systems
c. You have emergency response procedures
d. You have shut down systems

Whilst steps a to d are concerned with minimizing the impact of the hazard, they are all (with the possible exception of procedures) still related to physical assets, and they are all subject to requirements in steps 1 to 9 above.

Maintaining line of sight between Hazard and Asset. Keeping your eye on the ball

Identifying and placing the hazard at the centre of attention forms the initial identification step of the process, but can be too abstract a concept and lose its usefulness when concrete tasks need to be communicated to the workforce. There therefore needs to be a linkage (line of sight) between the hazard and the asset, and the process safety management system has to be built around the governance in ensuring that people manage the asset, and not around managing the hazard directly. Once this philosophy has been internalised it is as if the scales have been lifted from your eyes[6] and the solution at once becomes clear. This epiphany will transform your thinking on Process Safety. With the right tools the rest then becomes a handle turning process, working logically through the steps on page 4, until you have lain before you what it is you are supposed to be managing. The next step is therefore to stock your armoury of tools with the materiel required for the job in hand.

A bad workman always blames his tools! Selecting the right tools for the job

There is a saying that when the only tool that you have is a hammer, everything looks like a nail7. At the risk of raising a storm of controversy this has been one of the issues with HAZOP. It is a great tool in the right hands and for the right task, but it is not the tool for taking control over a Process Safety Management System as defined by the requirements on page 5. Here we decided on the use of BowTies as the workhorse of the system. Together with the ability to link incidents back to the original BowTie on which the hazard and its controls are defined, it not only allowed us to create a Process Safety Management System but, by building the system around assets, it also gives you the added benefit of an Asset Management System at the same time (effectively two management systems for the price of one). Sounds too good to be true but it isn't.

[5] Samuel Taylor Coleridge, Lyrical Ballads, 1798
[6] Paraphrasing the restoration of sight to Saul, Holy Bible, Acts, Verses 9 to 18
[7] Abraham Maslow, The Psychology of Science, 1966, developing am earlier statement by Kaplan

BowTie Analysis

A picture paints a thousand words, and BowTie diagrams are no different

Whilst no longer the height of sartorial elegance, there are no prizes for guessing how the name BowTie analysis was coined. It is not the intention of this paper to teach you about the detail of BowTies. Rather to explain how they have been used. However, to those unfamiliar with the concepts some background information is required in order to understand how the system ties (no pun intended) together. A BowTie diagram is essentially a Fault Tree and an Event Tree joined together through the event they either end in or begin with. Figure 1 explains the outline8.

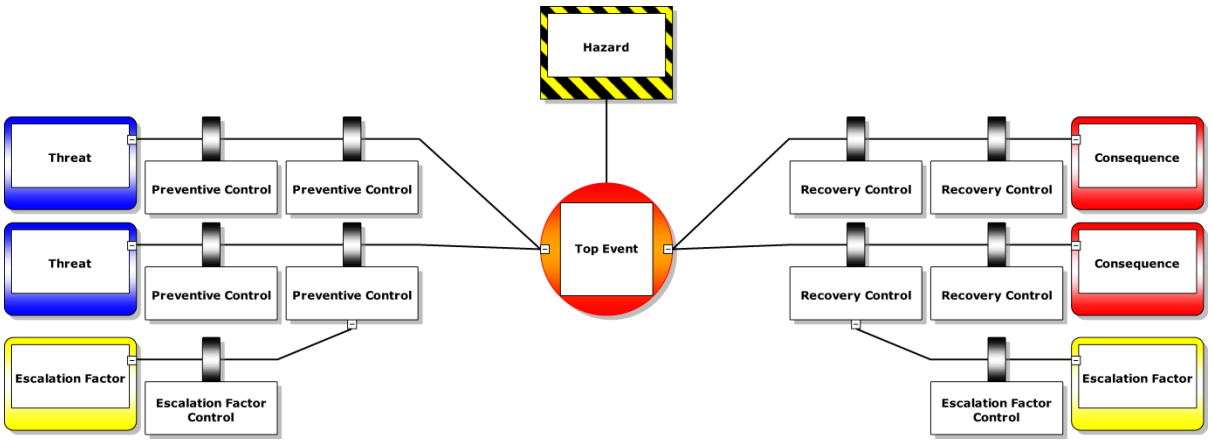

Figure 1 – The BowTie diagram framework

It is the authors' belief that this framework provides a springboard for answering all of the requirements detailed on page 5, once you understand the terms used:

- HAZARD (central point) – That which creates the risk should control be lost over it
- TOP EVENT (central point) – The point at which control of the hazard is lost
- THREATS (LHS) - Which unmitigated lead directly to the top event
- BARRIERS[9] (between the Threat & Event) - Which reduce the likelihood of the threat leading to the Event
- CONSEQUENCES (RHS) – The adverse results of the top event occurring
- BARRIERS (between the Event & Consequence) - Which mitigate the impact of the Event
- ESCALATION FACTORS (sub-barrier) – Those factors which could cause the barrier to fail

There are several key points to bear in mind when creating a BowTie but the two fundamentals are:

1. Get the centre section of the BowTie correct as this sets the scene for the rest of the diagram
2. Not to confuse the failure of a barrier with a Top Event, e.g. the failure of a DCS[10] is not the point at which control over the hazard is lost, but is more than likely a direct threat leading to loss of control

The distinction between quantitative risk assessment and qualitative risk assessment also has to be considered when using BowTies as they are primarily a qualitative risk assessment tool.

BowTies also educate people as they read them. It is the authors' experience that not only do they capture the corporate knowledge of the threats posed to an asset and how they are managed, but that they also help to bridge gaps between operations, maintenance and engineering staff as they build a common view on not just how the asset is operated and maintained but also why, and the potential impact of not doing certain things.

[8] Diagram courtesy of CGE Risk Management Solutions, the software supplier used by E.ON for their BowTies
[9] Usually categorised under the 3P's : Plant, Process and People (a barrier needs to sense, think and act)
[10] Distributed Control System

Where to start? Cutting the elephant into bite sized chunks

Introducing the Barrier Family sized portion

The starting point is the centre of the BowTie and we have defined our Hazards and our Top Events as follows:

Hazards

- Chemicals
- Flammable Materials
- Potential Energy
- Kinetic Energy
- Electrical Energy
- High Pressure
- High Temperature
- Low Temperature

Top Events

- Loss of Containment
- Uncontrolled Exposure
- Ignition in Storage
- Unplanned/Uncontrolled Ignition
- Loss of Control in Combustion System
- Loss of Integrity
- Loss of Control
- Unplanned/Uncontrolled Release
- Failed to Achieve
- Failure

Identifying the assets that relate to a hazard can be done by a HAZID[11] of the process and linking this to your plant identification system. Reverse engineering this exercise once you have finished is a good sense check to ensure that nothing has been missed out.

Taken together the failure of an asset captured by one of the Top Events listed may release several of the potential Hazards identified. Remember that Top Events can occur at any time, not just during normal operation, and anyone familiar with managing safety on a site with multiple hazards will know that there are multiple barriers in place to prevent or reduce the likelihood of things getting out of control.

As a simple rule of thumb the bigger the plant and/or the more complex the process, the more intricate the controls required until eventually a knot of Gordian complexity binds the plant together (sometimes called a Safety Case). The result of this complexity for BowTies can be that each threat line can contain many barriers, with the result that the diagram becomes very big, and the visual appeal due to the tool's simplicity is lost (together with the progressive loss of eyesight of those trying to read the diagram due to the small print required).

In order to overcome this and at the same time create a common language we have adopted the term "Barrier Family". These families are essentially "buckets" within which we can place similar types of control.

On the left hand side of the BowTie the (preventive) families are:

1. Operational Integrity (understanding the as built design)
2. Operating Procedures
3. Protective Devices
4. Alarms
5. Condition (Process) Monitoring
6. Routine Inspection and Testing

[11] HAZID – Hazard Identification, an analysis for identifying hazards

7. Routine Maintenance
8. Outage Inspection
9. Outage Maintenance

On the right hand side of the BowTie the (corrective) families are:

1. Operations
2. Detection Systems
3. Protection Systems
4. Spare Parts
5. Contractual Coverage
6. Engineering Recovery

Whilst Threats are specific to the Top Events that result from them, we have also standardised our Consequences under the following headings to further align the outputs from the BowTies to allow comparisons to be made between different areas of the business and priorities drawn up (based on their relative impact) as a result:

Cost Consequences

- Loss of Production
- Restricted Production
- Consequential Damage to Plant
- Liquidated Damages
- Recovery Expenditure
- Fire and/or Explosion

Safety Consequences

- Injury / Death

Environmental Consequences

- Damage to Environment

All barriers are equal, but some are more equal than others!

It is possible to define all the theoretical Barriers that could be in place for each Threat line in an ideal world to reduce the estimated frequency of the Top Event, and to identify which Barriers are must haves (Minimum) and which ones are nice to haves (Enhanced). The idea behind this approach is to align with the philosophy of ALARP[12], a concept at the heart of COMAH[13]. We have tried to adopt this philosophy for all of our asset BowTies, and they can be revised at a later date if additional potential Barriers are subsequently identified.

In order to be able to do this consistently internal standards need to be defined not only on how to capture and record the information for the BowTie, but crucially on how to validate this both technically and operationally (as there is more than one way to break things) before the final product sees the light of day at site. Here a process of drafting, peer review and site piloting (with a cross section of site staff) was successfully used, as the diagrams speak the language of engineering (internationally) and getting both engineering and site engagement was not a problem at any stage.

Whilst outside of the scope of this paper the goal posts for the selection of Minimum and Enhanced need to be clearly spelt out and understood internally so as to be consistently applied, e.g. company policy, regulatory requirement, industry standard, etc., as this effectively defines ALARP and therefore sets the risk appetite of the organisation. One tool that we have used to help better understand the relative merits of the various barriers here is LOPA[14], although care has to be taken over the independence of barriers when adopting the approach that we took.

You are now left with a series of bite sized chunks (BowTies) with which to return to the ubiquitous three questions. Within power generation the assets possess similar characteristics across sites. By linking individual assets with their associated hazards, a suite of asset related BowTie diagrams has been built (a de facto safety case for a power station).

[12] ALARP – As Low As Reasonably Practicable, weighing up a risk against what is needed to control it
[13] COMAH – Control Of Major Accident Hazards Regulations
[14] LOPA - Layer Of Protection Analysis

Plan, Do, Check and Act

Approach, Deployment, Effectiveness and Results (does it do what it says on the tin?)

Before we suffer from premature congratulation, however, we need to return to the three questions where the astute reader will have realised that we have not yet answered the second or third questions. A BowTie is only as good as the Management Systems that maintain its integrity. A diagram is a snapshot in time and the barriers it describes are likely to degrade over time and can be defeated either by malice or by ignorance. It can therefore be seen that the second of the three questions:

1. Do we know what systems are in place to prevent this from happening?

therefore also includes management systems, e.g. Management of Change, Competency, etc., as well as the physical barriers themselves. Moving on to question three we can also see that we need to check still deeper to be able to answer:

2. Do we have information to assure us that they are working effectively?

as to be effective a system needs to be:

- Defined
- Communicated
- Implemented
- Checked for deployment

and the:

- Actual outcomes versus desired outcomes reviewed
- Reasons for variances understood
- Appropriate corrective action taken to restore the desired outcomes

All we have succeeded in doing so far is to describe the world as it should be, not the as is, and we all know that we do not live in an ideal world. We therefore need to find a methodology to help us understand not only which sites have which barriers in place, but whether these barriers are being nurtured so that they will work as their designer intended. This is not an easy task if you do the maths across the fleet of fossil power stations:

- Seventy one sites
- Sixty BowTies per site (averaged as some are CCGT specific and some are Coal specific)
- Four hundred Barriers per BowTie (approximately)

Therefore with over 1,700,000 potential things to think about you very quickly come to realise that rather than having just one elephant to eat you have a herd of elephants, and you can see why HAZOP was not our tool of choice. If we were to close the control loop we needed to find a methodology for checking the deployment on site without bringing the organisation to its knees in the process.

We have built the capability to do this by working with our BowTie software supplier[15] to create an enterprise version of what has historically been a client piece of software, incorporating an audit module directly linked to the BowTie diagrams. As each Barrier has been created with its own unique:

- Question (based on the barrier)
- Expectation (what should be expected to be present on site to answer in the affirmative)
- Supporting Information (background to the requirements as the auditor may not be a subject expert)

Compliance against requirements is achieved by completing questionnaires on a web-based tool for assessing whether barriers are present. This is transparent to the sites so they understand exactly what the requirements are in advance, and can be completed over a period of time so as to reduce the burden on the site. The results are available at both a site level and at a central level. This survey measures barrier presence (does the barrier exist?).

Where gaps are identified these are then entered into a global risk register. Not all risks require investment to mitigate them but, where an investment is required, its effectiveness against other potential risk mitigations can be made and budget allocated where it is most effective across the portfolio.

Having a barrier present still does not mean it will operate effectively. Here a detailed set of additional barrier performance questions are asked against several key barrier families to generate leading process safety indicators to predict if a barrier will be effective on a site by site basis. By comparing barrier presence responses to those of barrier performance a better feel for the dependability of the barriers in place can be arrived at (to give a degree of assurance they are working effectively).

[15] CGE Risk Management Solutions

Learning from Incidents

Confirming that we answered Question 3 (hindsight is not an exact science)

Finally for question three if everything was working effectively then we would not have incidents. Unfortunately this is not the case!

Incidents whether actual or high potential continue to happen. Because of the infrequent nature of process safety incidents organisations must also capture their high potential incidents if they are to learn. Even assuming that they manage to capture the majority of them there is widespread doubt as to the effectiveness of organisations to learn from them[16], as how does an organisation learn?

Incident investigations produce recommendations but the organisation does not learn until it is has implemented them across the organisation (see the implementation life-cycle on page 10). This is easier said than done, but it is not impossible.

To assist us on this journey we realised early on that if we were going to create a model (for that is what a BowTie is) of our organisation capturing our barriers, then the results of incident investigations needed to be capable of being fed back into this model. Where the investigation revealed shortcomings in our world view then we could investigate why this was so, e.g.:

- Had we identified the threat on the BowTie?
- Did we have the barrier in place that we should have had?
- Did we have the barrier in place but it failed completely?
- Did we have the barrier in place but its effectiveness was different to that expected?

It would also tell us whether our other barriers had worked as expected. BowTieXP[17] has this capability through an add on called BSCAT[18] which gives us the facility to relate incident investigations back to the BowTie on which they sit, and allow us to see how things performed when needed.

BowTie diagrams can then be updated where required, and the information that they communicate conveyed to the sites both by updating the diagrams themselves and by updating the questionnaire surveys that describe the updated requirements. Based on the responses gaps against the updated requirements can be established and a coordinated cross company approach adopted, providing an informed opinion on the level of residual risk (to answer question three).

Potential Next Steps

Active Barrier Management?

So where is all this leading to?

The purpose of BowTies is to better manage risk. To do this they need to reflect the barriers that are in place and how they are managed. A plant, however, is not a static entity but is usually in a state of flux. Therefore if we are to understand the status of our plant at any point in time we need to understand whether the barriers are active or not in real time, and the impact of this on the safety of personnel and on the health of the asset. A decision has therefore to be taken as to whether the benefits of pursuing this active barrier management approach outweigh the costs. The reason for this is that it requires the integration of a number of other systems, some of which have a reputation within industry for not being very flexible, quick or cheap to customise or change.

Before we get to that point, however, we need to go down the learning curve of better understanding BowTies and how, by capturing our hazards and the events which cause them, they put us in a better place to attempt to answer the three questions. The authors' hope is that this paper will help set you off on your journey down this road.

Summary

Brining Risk to the Enterprise - the final frontier for Process Safety Management

BowTies have successfully created a common lexicon of risk management across power generation within E.ON spanning both power generation technology and geographical boundaries. This has not been achieved without considerable effort and now requires to be maintained and refined in order to demonstrate continuous learning and therefore further risk quantification and reduction.

[16] See any number of publications by Trevor Kletz

[17] BowTieXP - The BowTie software product from CGE Risk Management Solutions

[18] BSCAT – Barriers and Systematic Causal Analysis Technique (licensed from the DNV-GL methodology), comes as an additional module for BowTieXP, linking the causes of incidents with safety management systems and barrier based risk assessments

BowTies have proved to be a very flexible tool that can be applied to situations where a holistic understanding of cause and effect is required. Their potential scope is far wider that just high hazard industries and in this regard promise much in their potential as a tool of choice for wider risk management. Watch this space.