Standardisation of Bow Tie Methodology and Terminology via a CCPS/EI Book

Mark Manton, Principal Consultant, ABS Group, Warrington, UK

Martin Johnson, Principal Process Safety Engineer, BP, Sunbury UK

Robin Pitblado, Snr Vice President, DNV GL, Katy TX, USA

Charles Cowley, Project Manager, CCPS, London, UK

Tim McGrath, Process Safety Specialist, ZeroHarmHES, CA, USA

Ron McLeod, Consultant, Ron McLeod Ltd., Glasgow, UK

Rob Miles, Technical Director, Hu-Tech RMS, London, UK

Kiran Krishna, Principal Technical Safety Engineer, Shell, Houston, TX, USA

The Center for Chemical Process Safety (CCPS) issues books that have become the *de facto* best practise for process safety management globally. For example the CCPS issued the original LOPA book in 2001 and the Risk Based Process Safety book in 2007. We, the authors and members of the sub-committee advising on the content of the book, are now getting near to the end of a long process to write, develop, review, edit and issue a CCPS Concept book (prepared together with the Energy Institute) on the use of BowTies in risk management. The purpose of the book is to provide the basis for the chemical and process industries to move towards consistency in the approach adopted and terminology used when developing and using bowties. The book has been written by DNV-GL in the USA but with significant contributions from a sub-committee of over ten companies.

This paper and presentation will highlight the key recommendations, assumptions and improvements that CCPS are proposing for bowties, such as:

- Audience: key to bow ties is determining who is the audience for them, from the front-line operators through local management to corporate risk managers and senior management
- Barriers must be 'effective, independent and auditable' i.e. they must have the capacity to completely stop the threat from leading to the top event and must be independent of the threat and other barriers linked to a particular threat
- Barriers are either active or passive. If active, they must have separate elements to Detect what is going wrong, Decide on what to do about it and to Act to completely stop the threat from progressing further
- Barriers are now defined as: Passive Hardware, Active Hardware (all elements of detect-decide-act are hardware), Active Hardware+Human (elements of detect-decide-act are a mix of hardware and human), Active Human (all elements of detect-decide-act are human), and Continuous Hardware (only the act element is present, the detect and decide elements were determined during the design of the barrier)
- Degradation factors: barriers may fail, or degrade for various reasons. Previously these factors were called escalation factors, due the escalation of the risk due to the barrier failing.
- The "barriers" against degradation factors are referred to as "safeguards". Safeguards may not fulfil the barrier criteria of being 'effective, independent and auditable' or have all of the detect, decide, and act elements but will be more effective if these criteria are met.
- Human performance may be one element of a barrier but more usually, human and organisational factors will appear as safeguards preventing the degradation of barriers due to human error or other causes.
- The book also proposes standardisation on the meta-data associated with barriers such as barrier owner, the inherent, or as designed, strength of the barrier and barrier performance (the current condition or status of the barrier).
- Further chapters cover the process to develop bow ties, how to maintain them and how to incorporate human factors in bow ties (which is also addressed in another paper submitted to Hazards 27).
- Finally the paper includes a bowtie for a gasoline storage tank facility (*a la* Buncefield) to demonstrate the application of the recommended terminology.

It is hoped that the consistency in development and implementation of bow ties that will arise from use of the CCPS/EI book will improve their quality and application thereby reducing the risks in operating environments and less major accidents.

Keywords: bow ties, human factors, risk management, process safety, threat, hazard, consequence, barrier, degradation factor, safeguard, Buncefield, CCPS, EI

Introduction – Background to Bow ties and the CCPS/EI Book

The first mention of bow ties appears in ICI literature and some courses in Australia in the 1980's but they really took off after the criticisms contained in the Cullen Report in to the Piper Alpha disaster around the industry's understanding of the hazards and risks involved in oil and gas production in the North Sea. Shell took this to heart, further developed the bow tie concept together with the original software for bow ties, THESIS (The Health, Environment, and Safety Information System) and integrated the use of bow ties in to their process safety management systems. It is still a key element of their HSE assurance for capital projects. Many other companies and organisations have taken up the use of bow ties and included them in their management systems. An illustration of their widespread usage the frequent reference to bow ties in conference papers and other literature that address hazards and risks. Many companies have developed internal standards, charters or some form of guidance on what bow ties should look like, how to develop them and how to maintain them. Unfortunately these guides are generally not available publically so there has been no opportunity to compare the different sets of guidance to identify the good, the bad and the ugly amongst them.

The CCPS/EI workbook on bow ties is being developed by a committee of volunteers with a contract led by DNV GL and CGE. The committee members were asked for copies of their internal guidance on bow ties, bow tie development, etc. These were combined with internal knowledge and experience of the primary authors to prepare the first draft of each chapter. Comments were sought on these drafts from the committee members and extensive discussions held in multiple meetings to progress the workbook. The Energy Institute joined the effort to provide a particular focus on human factors throughout the book and a separate chapter on demonstrating human factors using bow ties (this topic is covered in detail in a separate Hazards 27 paper). The intent is the workbook will be issued as a joint publication of CCPS and the Energy Institute. The book is in its final compilation phase and will soon be sent out for Peer Review. CCPS aim to have the book published in 2017.

Guidance, both written and in the meetings, was received from companies and individuals with deep seated knowledge of bow tie development in BP, Shell, BHP-Billiton, DNV GL, ABS Group, Chevron, Husky Oil and human factors knowledge from the Energy Institute's subcommittee.

If you have particular experience in the development or use of bow ties and would like to volunteer to assist in the peer review then please let any of the authors know and we will put your name forward for consideration.

Audience for the Paper, Book and Bow Ties Themselves

This paper is intended to publicise the forthcoming CCPS/EI book to the attendees of Hazards27 and to commence the process that professionals adopt a common process terminology when developing and using bowties.

The key front line audience perceived by the authors are:

- Front-line Operators because they operate the plant that manages the hazard, makes use barriers and may be among the victims of a major accident event (MAE)
- Maintenance technicians who maintain the barriers to prevent the MAEs and could also be the victims of a MAE.
- Operations management, who need to understand their responsibilities for ensuring the organisational arrangements, infrastructure and resources to ensure the barriers can perform as intended. This category includes the Site Managers who, if an MAE occurs, will be the ones visiting the families of the deceased to explain what happened (and what they didn't do to prevent it).

Practically all of these groups struggle in wading through 100s of pages of a HAZOP output or a COMAH Report for the entire site. They want short, clear, preferably visual, overviews of the MAEs, the threat that could cause the loss of control of the hazard, the preventative barriers that prevent the event from occurring and the mitigations should the initial event occur. These are what good bowties deliver. Operators and technicians can use bowties to understand their roles in preventing MAEs. Managers can use them to understand what they and their organisation needs to put in place for barriers to function as intended. Good bowties can also serve as a tool to aid conversations between management and operators and technicians about their respective roles in preventing the MAEs

There will be other audiences and they will want different degrees of detail from the bow ties:

- Process Safety professionals: will be the group of people who provide detailed technical input and assurance to the site around their management of the process safety risks. They are probably also the on-site facilitators for developing new bow ties. They need more information regarding the barriers such as who "owns" them, what safety critical activities are associated with the barriers, the types of each barrier and their effectiveness. They also ensure that the bow ties align with site standards and norms for bow ties.
- This group might alternatively want the bow ties to give them a pictorial overview of the safety management system to aid understanding of how the processes and procedures in the management system relate to each other.
- Auditors (both internal and above-site auditors): bow ties can be used by auditors to test and review the site understanding of their risks and heath of barriers. Alternatively, for off-site auditors, the bow tie can be used with the site management to test their overall risk management of the site including plans to rectify deficient barriers and interim safeguards when operations continue with impaired barriers.

- The Competent Authority (CA). There are anecdotal comments that if sites operating in the UK include bow ties in their COMAH safety reports then this makes it easier for the inspectors who are reviewing the reports to understand the risks. It also gives the impression to the inspectors that the site understands the risks involved in their operations and that management is taking process safety seriously. This could potentially result in a cost saving by reducing the number of hours the CA charge the site to review their COMAH Reports.
- Non-UK regulators: some regulations demand the inclusion of bow ties. Bow ties developed off-line by desk-bound consultants offering the lowest price can lead to very generic bow ties that are only developed as a tick-box exercise. These would be of minimal value in preventing fatalities from MAEs.

A strength of bow ties comes from being a visual tool and for all barriers to be seen in one place and linked to each threat or consequence. Bow ties may be drawn on paper, using simple IT tools such as Visio or dedicated bow tie software. The advantage of using dedicated software is the ability to rapidly show different degrees of detail from the simple overview to a massive amount of information. This allows the same bow tie to meet the needs of the different audiences.

Once the audience for the bowties is decided then the number of bowties that will need to be developed follows logically. If the audience is operators and technicians then the desire will not be to cover each and every MAE but rather a representative set of the MAEs which will function to educate the audience and to inculcate a sense of chronic unease. In COMAH sites in the UK these would logically be the representative set for the COMAH report which should cover worst case scenarios but also a range of hazards, substances and processes (HSE, 2017). If the bow ties are developed during the design phase of a project with the audience being the process safety professionals then a far larger number of bow ties may be desired.

Elements of bow ties

Most of the elements of bow ties are well known the Hazards27 audience and you may be wondering about the need to cover such well-known ground. The reality was that arriving at these clear definitions took far more effort than we had ever imagined. We all "knew" the definitions but had minor and subtle differences in interpretation before we arrived at the definitions that will appear in the book (Figure 1). If you don't agree 100% with these definitions then please get involved and volunteer to Peer Review the book. It is now or never!

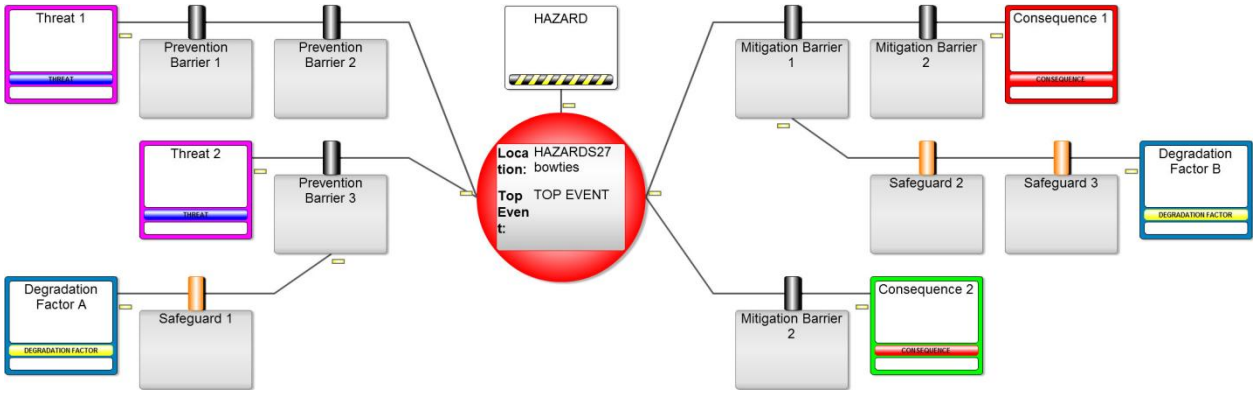

Figure 1: Standard terms for Bow ties

Hazard

Nothing new here, simply the standard HSE definition (HSE, 2016) that a hazard is any agent or operational situation that may cause harm, such as chemicals, electricity, working at height, etc. However, generic hazards lead to generic bow ties, so in bow ties include details on the scale and location of the hazard. So not "LPG" but "storing 50 tons of LPG in a bullet"; not "helicopters" but "transporting people 200 miles by helicopter from land to an offshore drill rig". In other words the same hazard can result in different bow ties depending on the circumstances such as storing, reacting, distilling or blending, etc. A further refinement can be bow ties developed for the same hazard and operation but during different activities from normal operations to start-up, shut-down or maintenance and repair.

Top Event

The moment when control over the hazard is lost, releasing its harmful potential (the 'oh no' moment). While the top event is the initial loss of control of the hazard there is still time to act to prevent or mitigate the consequences. For process hazards this is typically loss of primary containment (LOPC) but for a structural hazard is typically collapse of the structure be that a tank or offshore platform.

Consequences

As per the name itself, except we are only really interested in the worst credible scenarios if the top event occurs and there are zero barriers to mitigate the effects. One top event can have multiple consequences. Typically these are scored using corporate risk assessment matrices (RAMs) in terms of the effect on People (fatalities), Environment (major accidents to the environment), Assets (money, business loss) or Reputation (share price, licence to operate). As with the other elements the

preference is to define the consequence in sufficient detail, so not just “fatality” but “fatalities due to vapour cloud explosion from massive release of LPG”.

We mentioned consequences before threats. This was deliberate, reflecting the way bow ties should be built, see next chapter.

Threats

Threats are what they say they are, threats. So threats are similar to HAZOP causes, but with a few extra requirements for their use in bow ties, namely that their descriptions must be specific and sufficient and not just generic descriptions such as overpressure, overfilling, excess temperature, etc. A threat acting alone on the hazard must be enough to cause the top event to occur, without any help from another threat if there are no barriers in place. For a car driving bow tie “bad weather conditions” doesn’t really help to define the subsequent barriers. Is the bad weather due to excessive rain, high wind, fog, ice or something else? Each of these threats would lead to different barriers being defined. This also means that a threat cannot be the non-functioning of a barrier or absence of a barrier. For example, if the brakes fail on a car it cannot lead to a top event of loss of control if the car is standing still in a garage. The threat in this case is “driving at (high) speed”.

Also an “open valve” is a form of a failed barrier. Start-up operation is another non-specific threat. But the combined “starting operation with isolation valve(s) in incorrect position” becomes a valid threat.

Barriers

‘Prevention barriers’ on the left hand side of the bow tie are used to stop the risk event. They sit between the threat and the top event on the bow tie. ‘Mitigation barriers’ on the right hand side of the bow tie are used to stop, or significantly reduce, the severity of the potential consequences. They sit between the top event and the consequences on the bow tie.

Each barrier has to be ‘effective, independent and auditable’. They must have the capacity to completely stop the threat from leading to the top event or, if a mitigation barrier, significantly reducing or eliminating the consequence. Each barrier must be ‘independent’ of other barriers linked to a particular threat.

Grouping together equipment and tasks so that only ‘effective, independent and auditable’ barriers are represented typically limits the number of barriers on the bow tie to between 2 and 5 barriers on each threat or consequence leg. This has a major benefit that the bow ties is more easily understood so that management and operations do not gain a false sense of security that multiple barriers are in place when several of the barriers are not independent (i.e. if one barrier fails then another one will fail at the same time). Barriers are characterised as passive (e.g. crash barriers, bunds) or active. Active barriers are further subdivided in to *active hardware* (with an additional category of *continuous hardware* for the very particular type barrier, e.g. ventilation), *active hardware+human* and *active human* (Table 1). Active and human barriers must have separate elements of Detect, Decide and Act, i.e. Detect what is going wrong, Decide what to do about it and to Act to stop the threat from progressing further (Figure 2). The detect and decide elements are theoretically also present for passive and continuous barriers but only in the mind of the designer of the project/barrier when she considers that the threat may exist and decides to include the barrier in the design. These three terms are also called “sensor”, “logic solver” and “actuator” by some bow ties users but the committee preferred the simpler terms instead.

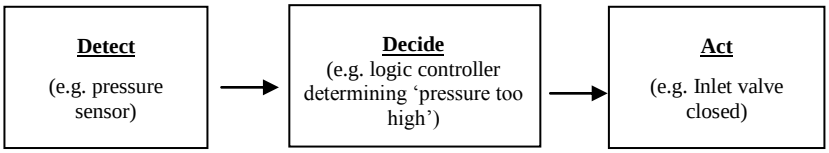

Figure 2: The Detect-Decide-Act model for active barriers

Some barriers in bow ties can be compared to Independent Protection Layers (IPLs) in Layer of Protection Analyses (LOPAs) although they may not meet the full criteria specified IEC 61511 (British Standards EN 61511-3, 2004).

The term Safeguards has been reserved for the degradation pathways (see below).

Table 1: Barrier Types and linkage to 'Detect', 'Decide' and 'Act' Component

Barrier type	Detect	Decide	Act	Description	Examples	Possible Barrier Owner
Passive Hardware	n/a	n/a	n/a	The barrier works by virtue of its presence	Bund, Blast wall, crash barrier, anti-corrosion paint	Head of Civil Department
Continuous Hardware	N/A	N/A	Technological	The barrier is always operating.	Ventilation system, Active corrosion protection"	Maintenance Manager
Active Hardware	Technology (e.g. pressure sensor)	Technology (e.g. logic controller)	Technology (e.g. Emergency shutdown valve)	All elements of the barrier are executed by technology.	Process control systems and Safety Instrumented Systems	Head of Instrumentation Department
Active Hardware+ Human	Technology (e.g. high-high level indicator and alarm)	Human (e.g. operator hears and responds to alarm)	Technology (e.g. Emergency shutdown valve) OR Human (e.g. operator manually shuts valve)	The barrier is a combination of human behaviour and technological execution.	Operator-activated ESD valve Gas alarm and decision by human to evacuate	Unit Operations Manager
Active Human	Human (e.g. operator walk around detect leak)	Human (e.g. decides to shut-down and isolate the equipment)	Human - but acting on technology (e.g. operator presses stop button or manually shuts a valve)	The barrier consists of human actions interacting with technology.	Operator detection and response (e.g. during structured walk-arounds)	Unit Operations Manager

When arranging barriers they should be drawn in a logical order reflecting their expected sequence of operation (i.e. the first barrier to stop the threat should appear first, etc. (see Figures 3 and 4)).

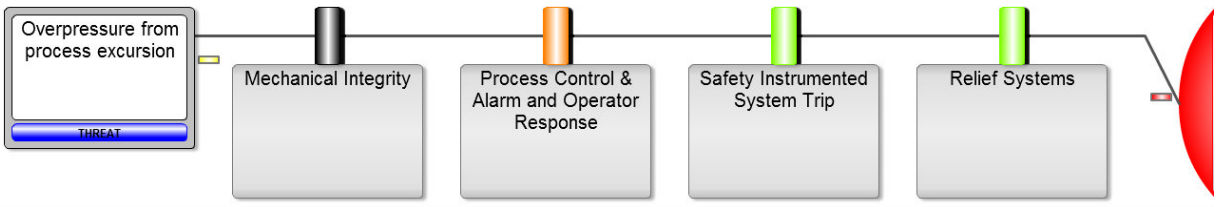

Figure 3: Typical Prevention Barriers on a single threat leg

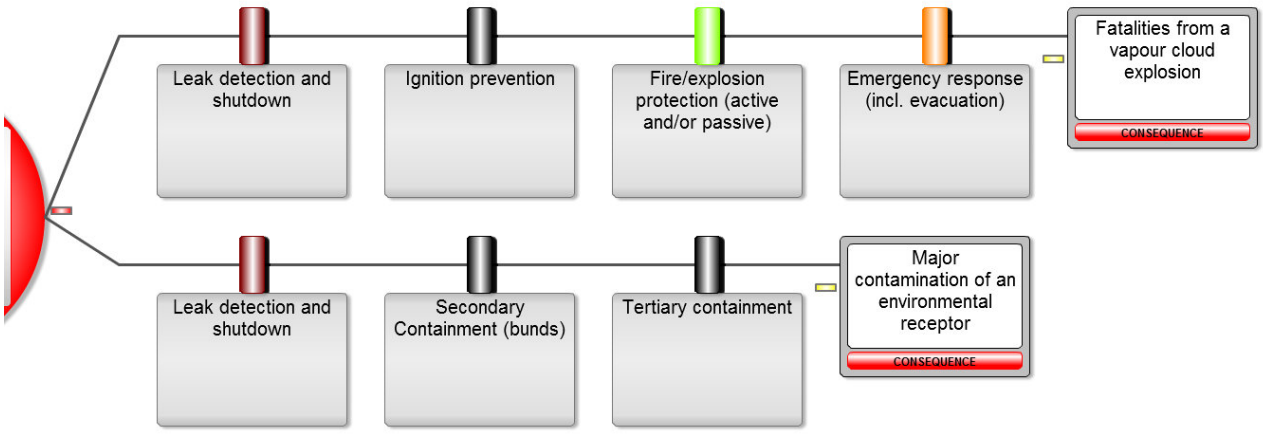

Figure 4: Typical Mitigation Barriers

Barrier meta-data

Besides the key elements that make up a barrier it is useful to classify them with further details, or metadata. The main meta-data are as follows:

Barrier type: see Table 1

Barrier owner. This will identify the single individual on site, or rather their role, who is responsible to assure that the barrier functions as it should. For example, the barrier owner for *active human* and *active hardware+human* barriers will often be the Operations Manager/Superintendent (Table 1) although these classifications will be site and company specific. Having a clear name per barrier will be of interest to the Site Manager to be assured that the barriers are being appropriately maintained. Auditors will also want to know who to interview about the different barriers.

Barrier Effectiveness/Strength. Whilst every barrier should fulfil the criteria of being effective, independent and auditable some barriers are better than others. To be effective it has to be "big enough", "strong enough" and react "fast enough" to stop the threat leading to the top event occurring or in mitigating the consequence. This can be seen as analogous to the size and thickness of the cheese within the 'Swiss cheese model'. Under the hierarchy of controls model the type of barrier tends to indicate its strength. In this model passive hardware are usually the strongest, followed by active hardware, then *active hardware+human*, with only one human element and finally *active human* with all elements being human.

These are important discussion points during the development of the bow tie. Factors affecting the inherent, or as designed, effectiveness/strength of a barrier may include some or all of these sub-categories:

- **Barrier Reliability:** This can be assessed qualitatively (e.g. high, medium or low; valid, partially valid and invalid; excellent, good, acceptable, poor and unacceptable/absent) or quantitatively (e.g. in terms of probability of failure on demand similar to a LOPA).
- **Barrier Adequacy:** whilst the goal is for all barriers to be fully effective, specific barriers might be included due to their importance even if not meeting a desired effectiveness target, particularly on the mitigation side of the bow tie (e.g. effective, partially effective, not effective or using a percentage estimate). For example an ammonia water curtain might only address 50% of wind directions and reduce ammonia impacts by only 70%.
- **Barrier Criticality**. In principle all barriers are important but some are more important than others. Factors determining criticality can include if the barrier is working to prevent a particularly prevalent threat or a critical consequence or if a barrier is used across multiple threat or consequence legs. Pressure relief valves might be determined to be critical as the last line of defence and in many jurisdictions having a functioning pressure relief valve is a legal requirement.

Barrier condition. This is important during operation, to give an indication of the status of the barrier against the design intent and whether the barrier has degraded over time. This can be seen as analogous to the size of holes in the cheese within the 'Swiss cheese model'; have they increased in size during operation? A three level system lends to the use of 'traffic lighting', for example:

- Green: in place, available and operating as per design
- Amber: in place and available but operating below its intended functionality
- Red: not available or significantly degraded.

Some companies have found it has been useful to also add two other categories: white where the barrier has not yet been assessed or no operational performance is available and black to designate either a barrier is not installed versus a standard design or where a barrier has been removed or not available on a long term basis (deactivated).

Degradation Factors and Safeguards

HAZOP, LOPA or other tools have conceptual similarities to a risk assessment via bow ties with hazards, causes, consequences, barriers/safeguards. Bow ties have three key differences to these other risk techniques namely, the:

- visual display of the hazards, threats, barriers and associated safeguards,
- interrogation of the barrier performance and, most importantly,
- recognition and analysis of factors that can degrade the barriers.

There will always be things that can cause a barrier to not work as intended. Degradation factors enable the team to further investigate why a barrier won't work as intended. In contrast, the barriers identified in HAZOPs and LOPAs are all assumed to work as intended (subject to semi-quantitative probabilities of failure on demand).

As with all elements, the CCPS/EI bow tie book recommends that the degradation factors be clearly described and specific - not just "the barrier fails". We need know how and why the barrier might fail. Will an "alarm and operator response" barrier fail because the alarm is broken and there is no system in place to detect this has happened or because the training and competence of operators is deficient so they do not respond, or respond incorrectly to the alarm?

> (Note: historically lines in the bow tie linked to barriers have been referred to as "escalation factors" because if the barrier fails then the risks will escalate. The sub-committee chose to call them elements that degrade the performance of the barrier, i.e. degradation factors.)

Degradation factors cannot lead to a top event. They can only lead to a barrier not functioning as desired. A frequent error in constructing bow ties is the inclusion of safeguards to degradation factors as barriers in the main threat or consequence line.

Safeguards

Safeguards lie along degradation pathways into that barrier where they help defeat the degradation factor. Safeguards should only appear on degradation pathways as they do not to prevent or mitigate a top event directly. Safeguards are not titled "barriers" to provide differentiation of terminology. Some safeguards can fulfil the requirements of a barrier but other may not because they may neither have the detect, decide and act elements nor the effective, independent and auditable requirements of a barrier. "Safeguards" allows the developer to reflect the role that softer issues play in the management of risk and assurance of barriers. Safeguard can also be used to incorporate softer issues such as human and organisational factors.

Two examples of degradation factors and safeguards preventing or minimising the degradation factor are shown in Figure 5.

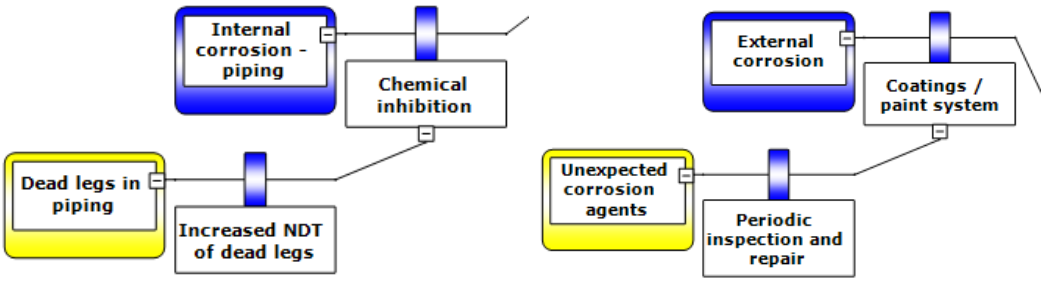

Figure 5: Example Degradation factors and Safeguards

Bow Tie Elements conclusion

The main substantive recommendation proposed by the CCPS/EI concept book is that bow tie terms become clearly defined. In the case of "barriers" that we remove the simple human factors descriptors such as "procedures", "training" and "competency" from being barriers by themselves on the main threatline pathway. This does not reduce their importance but because they cannot stop the trajectory between the threat and the top event they are not "barriers" by definition. They are, however, vital as safeguards to ensure the barriers perform as desired.

Another definitive conclusion within the sub-committee is the differentiation between "barriers" and "safeguards". Barriers must detect, decide and act and if the preventative measure cannot deliver all these then it becomes a "safeguard". So safeguards are all of the other things we do to prevent MAEs, such as ancillary equipment, processes, procedures, training, etc. These need to be present and working correctly to support the barriers.

Building bow ties

The CCPS/EI book contains a chapter providing clear guidance on workshops as a means of developing bow ties. The initial step is to develop a Terms of Reference document which documents the response to all of the key questions associated with the bow ties as listed in Table 2.

Table 2: Questions to be addressed in the Terms of Reference document for the Bow tie Development Workshops

Who is the sponsor of the workshop?
Who are the intended audience?
What is the purpose for the bow ties that will be produced?
What is the study scope?
Is there a prioritization of scenarios?
What method will be used to generate the threat lines to be considered? Selective high potential HAZOP threat lines or structured brainstorming?
How many scenarios (Top Events) to be considered?
Are there specific human factor related issues or concerns?
Which rule set and terminology will be used in the study?
Are there sufficient time and specialists team members available?
Who will be present in the workshop?
What consequences need to be assessed?
Which recording method will be used?
Which documents may be needed during the workshop?
How will action items identified in the workshop be addressed?

Developing bowties are similar to performing HAZOPs in that it is best to not develop them alone while sitting behind a PC screen. Rather, they are best developed by a team who understand the scenarios and the barriers and safeguards that may be used. A typical team for a bowtie workshop might include a bowtie session leader and scribe with experienced representatives from operations, maintenance, process engineering, mechanical engineering, process control & instrumentation, risk management and process safety.

The further guidance in the book is the order in which the bow tie should be built up during the workshop itself, namely:

- The starting point is obviously to identify the hazard, then the top event.
- Next identify the unmitigated consequences. It is advised to do consequences before threats as this helps team members dimension the event and later to better define the threats.
- Next comes the brainstorming session to identify all threats. Useful guidance while doing this is to use the MAEs identified in the major accident hazard management process and earlier HAZOPs, when available, i.e. those HAZOP threat lines that lead to damage to: People (fatalities), Environment (major accidents to the environment), Assets (money, business loss) or Reputation (share price, licence to operate).
- Identify barriers, both preventative and mitigation
- Identify degradation factors and their associated safeguards
- Finally when the outline of the bow tie is clear, go back and populate the metadata on the barriers as needed and where these were not included during the barrier identification and definition step

Bowties may be developed on paper or using specialist, or spreadsheet type, software displayed a screen during the workshop. An easy approach is to start with bow ties drawn on a large sheet of paper visible to the whole team and using sticky notes so barriers can be moved, grouped or re-designated as safeguards. In parallel, the scribe can copy the bow tie into the software so that when the paper version starts to get too complex the team can switch over to the electronic version. Bow tie workshops are highly iterative and it is likely beneficial to iterate at step 4. Only after the barriers have been fully defined does it make sense to add the degradation factors and safeguards.

Additional work is required after the bow tie workshop is complete. This will largely be done by a single individual, or small team, to ensure that the full benefit of the bow tie activities become embedded in the site. The overview of these activities, and the end-to-end process for bow ties and how they might sit within a COMAH regime framework is illustrated in Figure 6).

Some of the specific post-workshop activities include:

- Completing the metadata details on the barriers.
- Cross checking barriers against the site's Computer Maintenance Management System (CMMS) and safety critical equipment list.
- Ensuring all procedures and active human barriers identified in the bow tie are defined in a Standard Operating Practice and reviewed if they become a safety critical activity/task.
- Conducting Task Analysis on barriers that rely on human performance, or degradation actors associated with human error.
- Validating the outcome of the bow ties. Do the identified barriers meet the criteria of barriers? Are there performance standards associated with the identified barriers? Do the bow ties demonstrate an acceptable reduction of the risks to ALARP? Is LOPA and a cost-benefit analysis needed to provide the numerical demonstration that the risks are in the "Tolerable if ALARP region", or better?

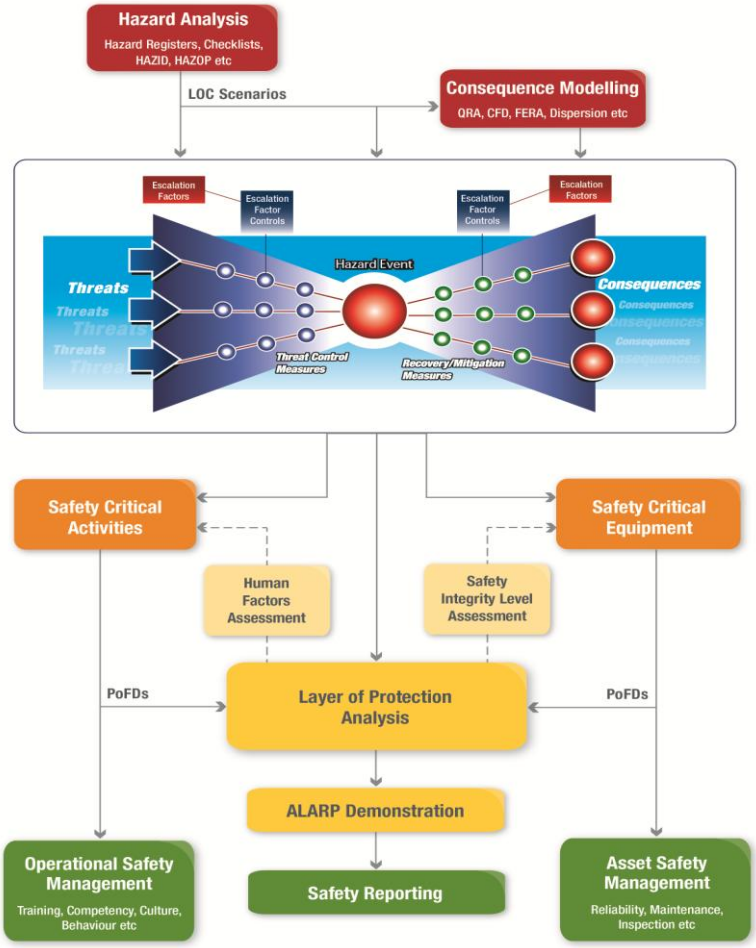

Figure 6: Schematic overview of the position of bow ties within a process safety management system

Managing Barriers and their Relationship to Risk Based Process Safety

There is a depressingly long list of major accidents that have occurred because the barriers that had been installed to prevent a MAE weren't maintained correctly and were not inspected or tested against performance criteria. Two recent and well-known examples include Buncefield, UK on 11th December 2005 and less than four years later on 23rd October 2009, a very similar incident at Caribbean Petroleum Corporation. At the Buncefield the tank overfill shut-off switch had been taken out of service a few months before the incident for maintenance (HSE, 2011) but not correctly returned to service (it was *de facto* configured to act as a low level shut-off rather than a high-high level shut-off). At the Caribbean Corporation there was no overfill shut-off switch installed and the tank level gauges failed frequently and their connections to the control room did not function (CSB, 2015).

Bow tie diagrams should be part of an ongoing risk management process. The creation of the original bow tie helps awareness of the hazard, threats, consequences and barriers but does not manage the risk. Barriers degrade continuously, at different rates for different barriers, and measurement of status will vary depending on barrier type and likely involve a combination of direct and indirect measurements. Sites therefore need a clear approach to ensuring that the barriers are correctly maintained. One of which would be for the local plant management team to meet periodically to review one bowtie each meeting. One of the key benefits of the bow tie is the visual representation of the condition of barriers and safeguards facilitating the discussion on the design intent or how degraded the barrier is. If the barriers and safeguards are provided with a colour code against condition one can quickly see if, for example, multiple or all the barriers on a single threat leg are degraded. The updated bow tie with barrier and safeguard condition is not an end to itself but provides input to the following questions:

- Is it safe to continue operations?
- Are immediate mitigations required to continue operations?
- Which barriers or safeguards should be prioritised for rectification to regain their design intent?

Occasionally the bow tie review can lead to the recommendation for additional barriers. Care should be taken in adding barriers unless the original design intent and assessment is shown to be deficient. If the current barriers are significantly degraded there is likely to be a structural problem with the organisation's maintenance, inspection and testing. Any new barrier is likely to suffer the same fate of also becoming degraded.

Given the questions above it is unlikely to be beneficial to create/use a barrier scoring systems as a single 'go, no go' decision process. The complexities of different barrier strengths, criticalities and current condition are normally too difficult to distil into a single numerical scoring system. In answering the questions above many other additional factors need to be considered such as; legislative requirements, manpower availability, spares available, time to engineer the corrective actions. The bow ties are one feed that management can use to decide if operation should continue and the immediate and longer term actions to strengthen (or add) barriers and safeguards.

The CCPS published the book on Risk Based Process Safety in 2010 (Center for Chemical Process Safety (CCPS), 2007) defines 20 elements that need to be managed for good process safety performance. The Energy Institute published their Process Safety Management Framework (Energy Institute, 2010) that covers the same ground, with some slight reordering of the elements. These describe the elements of a good process safety risk management programme such as Leadership through to asset integrity, management of change, etc. There is a direct link between bow ties and the PSM program. The latter all act as the safeguards to sustain all the barriers and ensure that they continuously operate at their desired performance level.

Bow tie Example – Gasoline Storage

The easiest way to fully understand the terms and construction of a bow tie is through studying an example. The book contains an in-depth overview of an example, namely the storage of gasoline in an atmospheric storage tank. This was chosen because it is well known and because of all of the well documented work done on this subject following on from the Buncefield incident, starting with the PSLG report (PSLG, 2009), continuing with the short (36 page) but detailed incident investigation report (HSE, 2011) and many guidance documents published under the auspices of the Chemical and Downstream Oil Industry Forum (CDOIF), in particular the "Other Products in Scope" guidance (CDOIF, 2012).

The simplest view of the bow tie is shown in Figure 7. Note how the hazard, top event, consequence and threat have all been defined. The intention with each is to comply with the guidance described above to be specific and sufficient. The threat is sufficient, if there are no preventative barriers present, to lead to the top event.

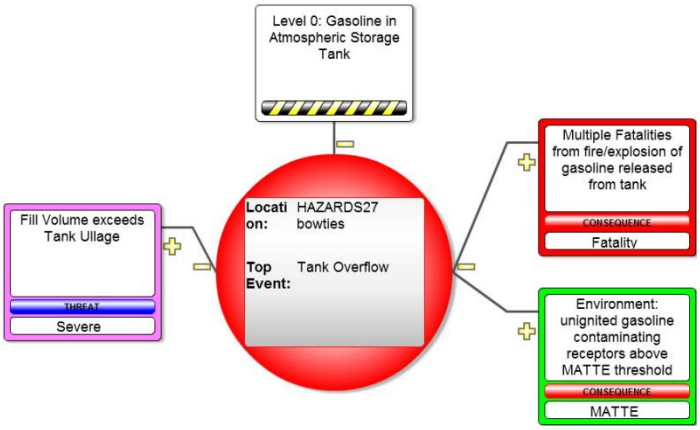

Figure 7: Simple overview of a tank overfill bow tie

Expanding the preventative barriers and showing the degradation factors and safeguards for one barrier leads to Figure 8. In this tank overfill example the three barriers are those identified in the industry guidance (CDOIF, 2012). The degradation factors that would prevent an "alarm and operator response" functioning correctly could be failures of the "detect" element (alarm failure) or failures of the "decide and act" elements (operators fail to respond appropriately to alarms). The safeguards for the alarm failure cover preventative and breakdown maintenance. The safeguards for the operator failing to respond appropriately cover the four possibilities for this failure from the operator not:

- seeing the alarm
- knowing how to respond
- being physically fit enough to respond or
- being mentally fit enough to respond

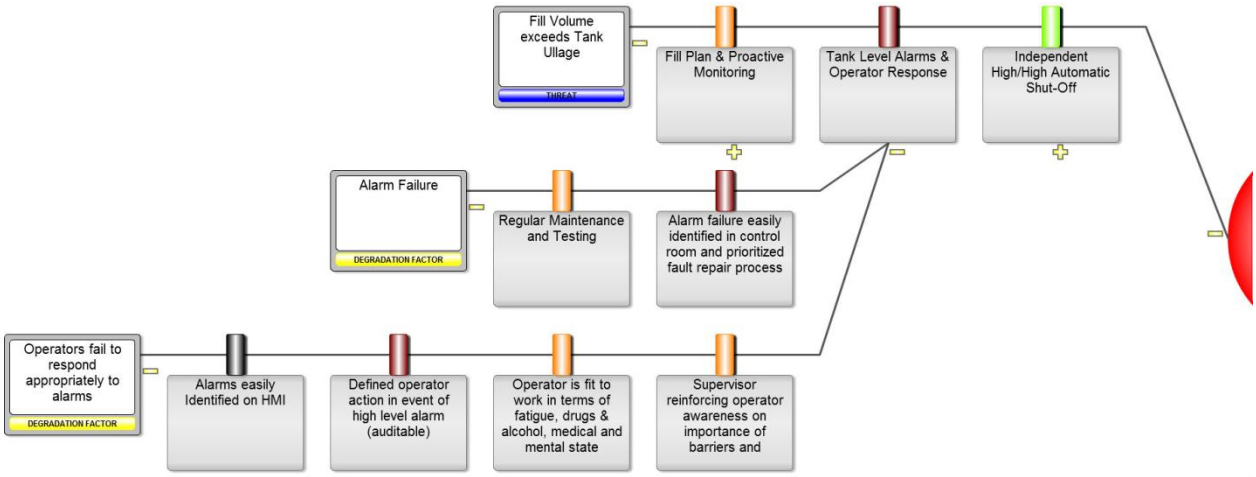

Figure 8: Preventative barriers and degradation factors for the tank level alarm and operator response barrier

After the top event has occurred and the tank is overflowing then the two main consequences depend on whether the gas cloud ignites or not. There were no fatalities in Buncefield due to the simple fact that no operators were in the area and no-one occupying the Maylands Industrial Estate at 06h01 on 11th December 2005, it being a Sunday morning. Buncefield was a useful reminder that passive barriers can fail. Buncefield led to environmental damage with bund failure from loss of the sealant between the concrete sections of the bunds, and between penetrating pipes and the bund walls due to the sealant melting in the presence of the burning gasoline allowing it to flow outside the bunds. Drains and soak-aways allowed the liquids to flow off-site (failure of tertiary containment) and to harm the local environmental receptors including a drinking water aquifer.

Another possible mitigation barrier is leak detection and shutdown. It has not been included in this example because it was not present in Buncefield and has rarely been implemented in gasoline tank farms in the UK. Guidance on such systems is available in another CDOIF report (CDOIF, 2013).

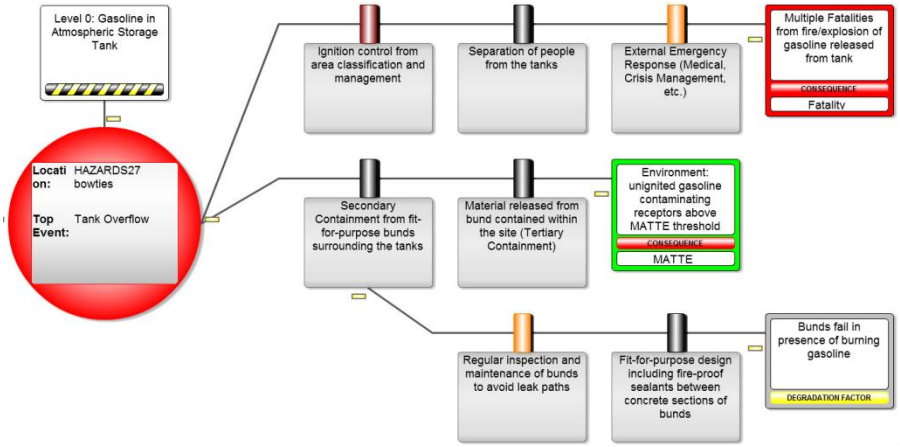

Figure 9: Mitigation barriers and some of their degradation factors

Conclusions

Bow ties have been around for quite a while and many have been produced and are in use by many companies. The quality of these bow ties varies from excellent to abysmal. A contributing reason to this variation is the lack of clear, agreed industry guidance on what constitutes best practise in developing and producing bow ties. Adopting the process and recommendations in the new CCPS/EI concept book should help industry address key deficiencies in previous bow ties such as:

- No quality criteria for barriers leading to a high number of barriers giving operations and management an artificial sense of security. Applying the suggested recommendations should generally give between 2 and 5 barriers on each threat leg.
- Safeguards against degradation barriers being included as barriers on the main threat or consequence legs.
- Safety management system elements being included as barriers for example, ‘training or competence’

The CCPS is the source of key process safety guidance from Risk Based Process Safety guidance and Layer of Protection Analysis for the chemical and process industries. Both of these books were, and still are, considered by many to provide the

definitive guidance on what constitutes best practice in these topics. It was therefore logical to continue this pattern to deliver what is hoped will become the definitive guidance on best practice in bowtie risk management. The book is in a near-final draft and should be issued in the second half of 2017. This paper summarises the key terminology, methodology and recommendations for bowtie users. This places great emphasis on clarity of the terms to be used in the bowties. The big advantage of bowties over other risk assessment approaches are i) the identification and analysis of degradation factors to understand how barriers can fail and the safeguards that need to be in place to prevent such failure and ii) the visualisation of barrier and safeguard condition in the operating phase.

The intention and hope from this book is to aid everyone when they develop bow ties to adopt a consistent approach that will deliver real value from the time spent in developing them. The bow ties should deliver what we want them to deliver, namely, a reduction in the frequency of major accidents leading to fatalities and environmental catastrophes. But bow tie development alone is not enough. Bow ties need to be live documents, reviewed and updated regularly and to not just sit on the shelf.

References

British Standards EN 61511-3. (2004). Functional safety - Safety instrumented systems for the process industry sector. Part 3: Guidance for teh determination of the required safety integrity levels.

CDOIF. (2012). *Other Products in Scope.* Chemicals and Downstream Industry Forum incl. Health and Safety Executive. Retrieved 2016, from http://www.hse.gov.uk/aboutus/meetings/committees/cif/resources.htm: http://www.hse.gov.uk/aboutus/meetings/committees/cif/pslg-other-products.pdf

CDOIF. (2013). *Guidance - Leak Detection.* Chemicals and Downstream Industry Forum - HSE. Retrieved from http://www.hse.gov.uk/aboutus/meetings/committees/cif/leak-detection-guide.pdf

Center for Chemical Process Safety (CCPS). (2007). *Guidelines for Risk Based Process Safety.* John Wiley & Sons.

CSB. (2015, October). *Final Investigation Report: Caribbean Petroleum Tank Terminal Explosion and Multiple Tank Fires.* Retrieved from http://www.csb.gov/caribbean-petroleum-refining-tank-explosion-and-fire/.

Energy Institute. (2010). *High level framework for process safety management.* Energy Institute.

HSE. (2011). *Buncefield: Why did it happen?* Retrieved from http://www.hse.gov.uk/comah/buncefield/buncefield-report.pdf

HSE. (2016, 12). *Controlling risks in the workplace*. Retrieved from http://www.hse.gov.uk/risk/controlling-risks.htm

HSE. (2017). *Risk analyses or 'predictive' aspects of COMAH safety reports guidance for explosives sites. Step 3: Selection of Representative Set for Detailed Assessment.* Retrieved February 6, 2017, from COMAH Safety Report Assessment Guides: http://www.hse.gov.uk/comah/assessexplosives/step3.htm

PSLG. (2009). *Safety and environmental standards for fuel storage sites.* Process Safety Leadership Group, Health and Safety Executive.