MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

18th Annual International Symposium
October 27-29, 2015 • College Station, Texas

Are You as Safe as You Think You Are?

Richard Rowe and Stephen Shaw
ERM
840 West Sam Houston Parkway North, Suite 600, Houston, Texas 77024
Richard.Rowe@erm.com and Stephen.Shaw@erm.com

Abstract

The use of the bowtie diagram has become widespread in the oil and gas industry as a communication and identification tool for hazardous events. The technique has proven to be very useful in the determination of safety critical equipment, when used in a simplistic manner. On the other hand, its complex applications extend towards developing and maintaining performance standards, procedures, etc.

The bowtie technique is used to record barriers – both preventive and mitigative. But having recorded barriers, it is useful to be able to take a view on how effective these barriers are, and how well you are protected from the identified threats and potential consequences. There are several tools available in the industry to estimate this quantitatively. Just like the known quantitative risk techniques, these methods come with their own set of complexities. For assessing barrier effectiveness, is this complexity needed?

This paper provides a qualitative methodology for estimating the effectiveness of barriers, which can be considered as a screening process that can both focus OPEX and identify areas where barriers may need to be reinforced or added to. The method accounts for a variety of factors such as safety measures being fail-safe, and the possibility of safety system overrides.

One of the major benefits of the bowtie technique is to assist in the development of key performance indicator metrics. It gives an insight as to how well protected a facility is against accident events and supports operational managers in making risk based decisions, e.g. making choices on how to focus OPEX spend.

With continued development of new sources for oil and gas production, the risk to surrounding public receptors has been a growing concern in the industry. Questions arise about how to best implement safeguards and position detectors, respond to emergencies, and better protect vulnerable areas, making a thorough understanding of risk key.

Introduction

Bowties are increasingly used as a means of communicating both the Threats can lead to an undesirable event (referred to as a “Top Event” which are generally the loss of control of a Hazard) such as a loss of containment of flammable liquids, and what this Top Event can lead to (Consequences), such as a pool fire leading to multiple fatalities. The Barriers that are provided to prevent Threats from leading to a Top Event; and Recovery Measures (often also referred to as barriers) provided to respond to the top event to prevent, limit the effect or respond to a potential Consequence are then added. Many, if not all barriers can be considered as safety critical systems, or elements.

In reviewing a bowtie, it has typically been difficult to gain a realistic appreciation of how effective the provided protection is against the identified threats, or how well equipped to respond to a top event to prevent or minimise the impact of a consequence. If a robust view of the effectiveness and hence adequacy of barrier (at least relatively) is available, this can give insight into the safety of the facility.

One approach, that of counting the number of barriers and recovery measures, has been used both explicitly and implicitly, since people tend to feel better protected if they can see multiple barriers and recovery measures on each threat and consequence line. This approach, however, is not effective and can provide a false sense of security. It also does not give any indication of which barriers are, for example, most vulnerable to being degraded if regular maintenance or testing is not performed on time (it also relies on people’s common definitions of what constitutes a barrier – which is often not accurate).

Pressures on operators to reduce OPEX require that budgets are used wisely, and the current approach to using bowties does not support this, nor in the authors’ opinion does it help with risk reduction.

Whilst this paper will focus on process safety related examples, the same challenges exist for environmental incidents. For the purposes of this paper, recovery measures are referred to as barriers (unless in it necessary to draw the distinction from barriers on the left hand side of a bowtie).

Overview of current practice

Bowties have become increasingly widely adopted as a communication tool, but they are not generally used in the design process (other than to record what is being provided), nor as a decision support tool to assist operational managers in managing risk. However, as their use has become more established, expanding their application would provide a clear view of the level of protection provided against major accident events, and provide a valuable decision making aid.

However, current practice in developing bowties is not consistent, with a number of variations in the conventions used when developing them. Whilst for some applications this may not present a problem, in the context discussed in this paper of barrier effectiveness assessment, consistency is essential.

Examples of the variations that exist are:

- Definition of top events – Most bowties adopt the approach that a Top Event is the loss of control of a Hazard, with the hazard being shown on the bowtie diagram above the top event. An example is shown in Figure 1:

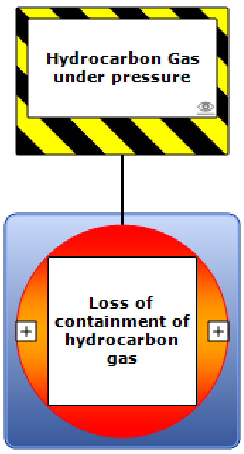

Figure 1 – Typical bowtie representation of a hazard and top event

This approach can be adopted at an asset level (e.g. loss of containment from the whole pressure containment envelope), or a system/module level (e.g. loss of containment in the gas compression module).

Another approach is to define the "hazard" as an activity such as top-hole drilling, and then have a Top Event representing a specific type of incident that could occur when conducting that activity, such as release of shallow gas. Defining the Top Event as, for instance, fire or explosion and the consequences as being fatalities, evacuation etc. has also been observed.

- **Barrier type** – There are two main approaches to what are shown as barriers on bowties:

1. Hardware barriers – where these barriers are physical in nature such as pressure containment systems, shutdown systems (this could include separation distance, as well as more obvious barriers). Procedures, human interventions and training/competency etc. (that collectively can be described as "soft barriers") that are required to activate and/or maintain a hardware barrier in suitable condition can be treated as escalation controls. These controls act to stop escalation factors that could undermine the functioning of the barrier.
2. A mix of hardware barriers and soft barriers, such as procedures, human interventions, competency/training etc.

This difference between these two approaches is illustrated in the two simple examples below.

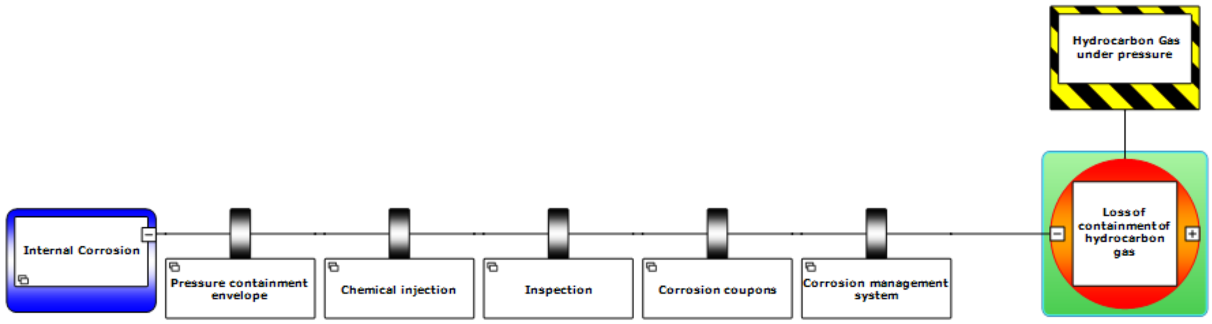

Figure 2 – Bowtie showing both hardware and soft barriers

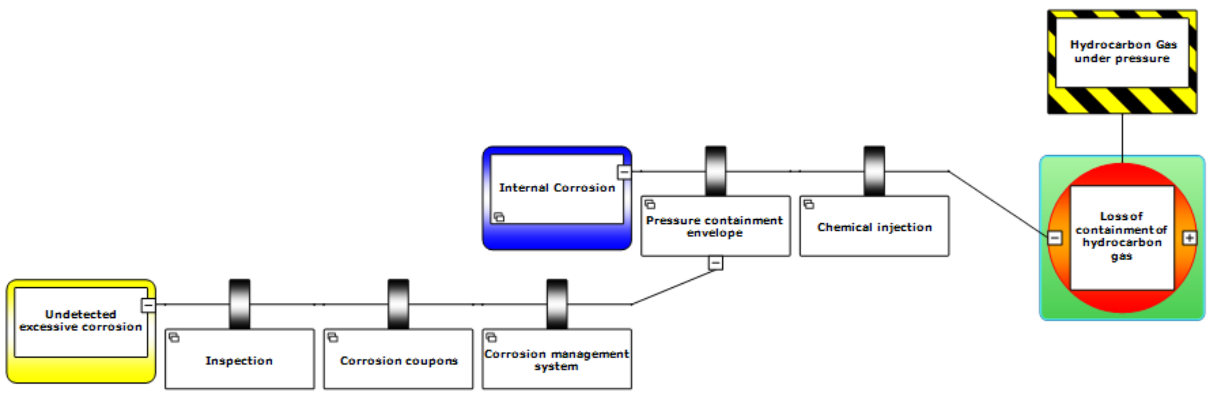

Figure 3 – Bowtie showing soft barriers as escalation controls

- **Barrier completeness** – It is common to see bowties where, for example, flame detectors appear as a barrier, with the ESD system and deluge as separate barriers. This approach can, however, lead to the perception that a facility is better protected than it actually is. An alternative approach (and in the view of the authors, a clearer one) is to only identify barriers that on their own are able to eliminate or significantly reduce the likelihood of a threat, or prevent or significantly mitigate a consequence. With this approach, it is clear that detection on its own is not a barrier, as it alone does not do anything to e.g. shut down the plant or sound an alarm. The combination of detection, processing of that information and some form of executive action (actuation) does constitute a barrier. This definition, referred to as being complete, is based on the principle that if any of three elements fails, then the barrier would not be effective. Some barriers by their very nature do not require these three components, as they are intrinsically passive in performing their role (such as a bund)

- **Barrier independence** – To gain a clear view of barriers they should also be independent i.e. they should not rely on other barriers to work, and should not have any common failures points or modes (e.g. having two types of flame detectors, connected back to a common fire and gas panel and subsequent actuation, does not constitute two separate barriers, as failure of the panel or the actuation would render both types of detectors ineffective). The authors have conducted barrier rationalisation exercises, where bowties have been simplified, so that component parts and non-independent barriers have been consolidated into barriers that are independent (in several cases reducing the number of barriers on a single threat line from over 10 to two or three). Some of these exercises have been greeted by the response, from experienced engineers plant operators and managers, that they now feel less assured of the safety of their facility (i.e. they had implicitly taken having lots of barriers as meaning they were well protected).

Note: Based on these principles, the two separate barriers shown in Figure 3 should be combined (carbon steel on its own will not stop the threat of internal corrosion – its corrosion allowance will, however, delay a loss of containment. Chemical injection on its own does not prevent a loss of containment - again, it can slow or halt corrosion, but must take into consideration the materials used in the containment envelope).

For the purposes of this paper the approach adopted is to define barriers as being hardware, complete and independent.

Barrier strength and effectiveness concept

For the purposes of this paper, bowties related to a generic gas processing plant or module are used. It is assumed that the gas being processed has a reasonable level of corrosivity (e.g. it is wet and contains some H_2S). It is also assumed, unless stated otherwise, that the process and equipment have been suitably designed and constructed.

The examples shown below demonstrate two different approaches to managing the threat of internal corrosion.

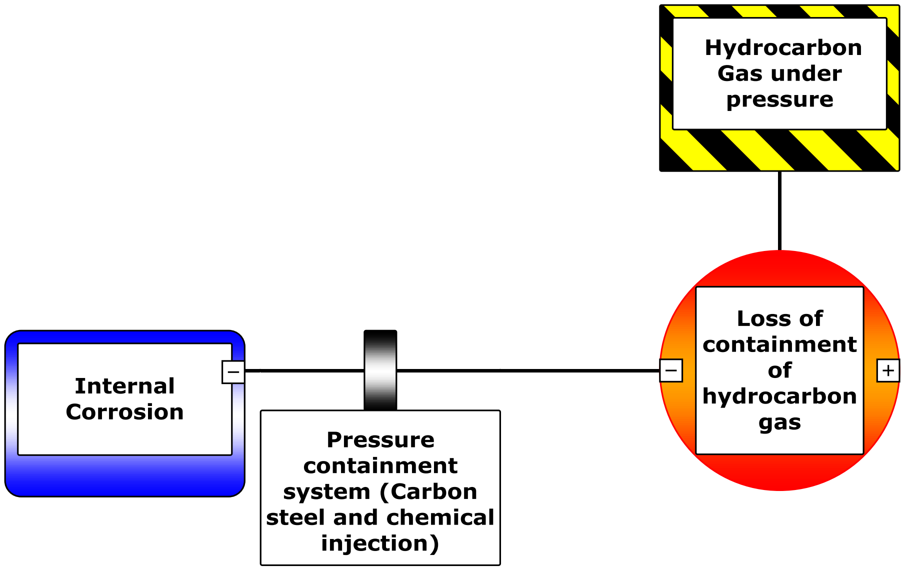

Figure 4 – Bowtie showing combined (complete) barrier

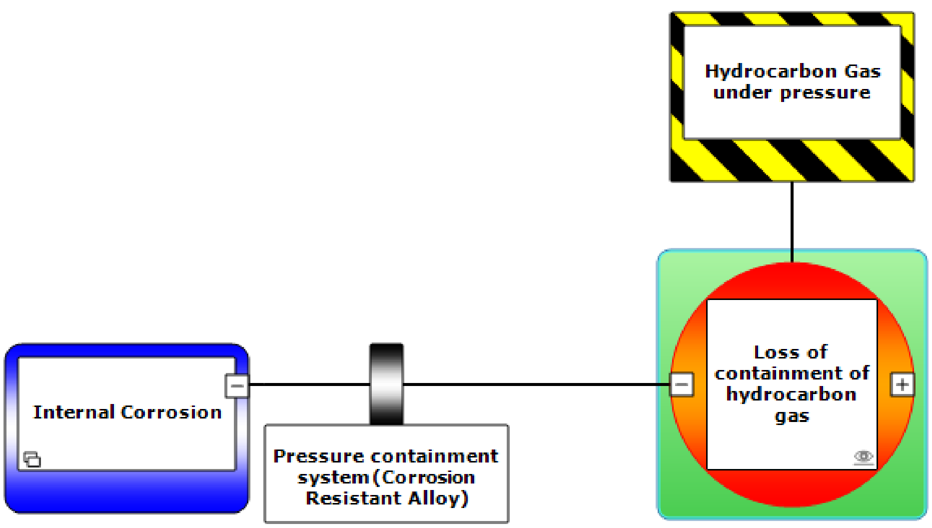

Figure 5 – Bowtie showing single effective barrier

In the first example (Figure 4), the pressure containment envelope barrier comprises both a carbon steel pressure containment system and chemical injection. The pressure containment system is vulnerable to internal corrosion, so whilst it may initially be fully effective as a barrier, it will degrade over time as any corrosion allowance is used, potentially rapidly. The second part of this barrier, chemical injection, is provided to reduce the corrosivity of the process fluid and hence protect the carbon steel. For this to be effective requires human intervention such as topping up chemical supplies, setting dossing rates, and maintaining the chemical injection system. Hence there are numerous ways that this barrier can be compromised.

In the second example (Figure 5), the pressure containment envelope is constructed out of a corrosion resistant alloy (CRA) (assumed to be appropriate for all anticipated process conditions). Provided that this is properly specified and that the process conditions do not deviate outside of the expected envelope, this barrier will be effective (against this specific threat) and should maintain its effectiveness, without the need for any further active controls or human intervention. In other words, this is a simple and passive barrier.

Whilst it is not always practical or financially viable to use CRAs in place of carbon steel and chemical dosing, in terms of which approach provides a stronger and more effective barrier, the use of suitable CRAs would generally be preferred as this is a more dependable or "effective" barrier. This introduces the concept of barrier effectiveness, which is a combination of whether a barrier can fully achieve its objective (strength), how reliably it can perform this task (referred in this paper to as readiness) and how much reliance is place on a given barrier (criticality).

There are a number of criteria that can be used to assess the strength of barriers and readiness, and these are considered below.

Criteria for assessing barrier strength and readiness

Barrier strength is defined in this paper as a measure of the ability of a barrier to prevent a threat leading to a Top Event, or in preventing a Top Event leading to an ultimate consequence. There are a number of criteria that can be considered as contributing to a barrier's strength. Examples include:

- Capacity, including its speed of response if it is an active barrier, e.g. whether a bund is sized to be able to contain the full spill volume that can be released or whether a pressure relief valve lifts in time to prevent an overpressurisation leading to loss of containment; its sizing/flowrate versus the required level of relief as a measure of capacity; or the speed of closure of an ESDV (its leak/passing rate being a capacity measure)

- Suitability e.g. how suitable a deluge system is in preventing escalation from a fire (may differ depending on the type of fire, with these being shown as different consequences on the bowtie).

Barrier readiness is a measure of how likely a barrier is to perform when required - this is a slightly different concept to traditional reliability or availability of equipment. Whilst readiness includes consideration of reliability and availability in the traditional sense it also considers e.g. the performance of procedural controls, human interactions, current condition and discoverability of failure modes. Examples include:

- Relative passive/active nature, i.e. how passive or active the barrier is. Passive barriers include bunds, PFP, natural ventilation and separation/layout, while active barriers include active fire protection, relief valves, interlocks and shut down systems

- Complexity, i.e. how simple or complex the barrier is. An ESD system (complete with detection, processing and actuation) and a Pressure Safety Valve (PSV) are both active barriers, but the ESD system is considerably more complex.

Barrier criticality

Barrier strength and readiness give a measure of the performance of a barrier, with the other important consideration being barrier criticality. This is an indication of how much reliance is placed on a barrier and how significant a given threat or consequence is considered. This includes consideration of the nature of the threat (which can range from e.g. loss of the facility with multiple fatalities on and off site down to a nuisance factor), how frequently the threat occurs or the proportion of time it is present, and how well supported the barrier is, by other strong barriers with good readiness.

A proposed set of criteria are presented in Table 1.

Table 1 – Proposed Criteria

Barrier strength		
Criteria	*Range*	
Capacity/Speed/ Redundancy	Exceeded/Fully redundant	Partial/No redundancy
Suitability	Intended role	Unintended role
Current condition	As new	Poor
Confidence in condition	Certain	Unknown
Barrier Readiness		
Criteria	*Range*	
Relative activity	Fully passive	Fully active
Complexity	Simple	Reliance on human action
Failure mode	Fail safe	Fail to danger or undiscoverable failure
Availability and use of overrides (including LOTO)	No overrides	Overrides available and regularly used
Barrier history	No history of barrier failure (good reliability and availability)	Poor history with repeated failures
Barrier Criticality		
Criteria	*Range*	
*Nature of threat/consequence	Catastrophic event	Nuisance factor
Frequency of threat/consequence	Constant	Rare
Reliance on this barrier	Multiple barriers with good strength and readiness	Single barrier or considered the main barrier

*As this paper has considered the use of this approach for major accident events that have serious or catastrophic consequences, this criteria will not be considered further here.

Other criteria may be applicable depending on the nature of the facilities being considered.

The ideal outcome when scoring against these criteria would be a high strength and readiness rating and a low criticality rating.

Considering the number of barriers, threats and consequences that would be considered for a typical facility, it is proposed that a qualitative approach is taken to the scales that are used (e.g. as in Table 1.), with a maximum of five values used for each criterion (rated from 0 to 4). Whilst it is suggested that a simple summation of ratings for each category (strength, readiness and criticality) may give a good indication of the overall "effectiveness" of the barrier, the use of weighting factors would be readily incorporated into this model and allows the model to be calibrated.

The overall barrier effectiveness rating is defined as:

$$BE_n = \frac{S_n + R_n}{C_n}$$

Where:
- BE_n = Barrier *n*'s overall effectiveness
- S_n = Barrier *n*'s strength rating
- R_n = Barrier *n*'s readiness rating
- C_n = Barrier *n*'s criticality rating

"Gatekeeper" criteria

Whilst it is considered that all of the above criteria are important, there are some that stand out as being "gatekeepers" that must achieve a minimum rating before any of the other criteria have much value.

These are Capacity (including speed and redundancy), Condition and the Use of overrides.

If a barrier does not have adequate Capacity, it does not matter if it is in good condition, simple, passive etc. As it will not be able to prevent/significantly reduce the likelihood of a Top Event, or prevent or significantly mitigate the effect of a Consequence.

Similarly, if it is known that a barrier's condition is such that it will not work, or if it is known that is has been overridden, then other factors' criteria become worthless. Hence a rating of zero against any of these three criteria would default the overall effectiveness to zero (by implication this is a dynamic measure for condition and overrides, as when the condition has been restored or the override removed, the barrier may have a rating).

The barrier effectiveness model therefore uses a (significant) weighting factor on the capacity/speed criteria to account for its importance. A weighting equal to the number of other numerator criteria is proposed and is used in this paper.

Example of rating a barrier's effectiveness

Taking as an example a hydrocarbon processing unit that takes feedstock from a high pressure source, and an overpressurisation threat line, Table 2 shows how PSVs could be rated. For evaluating the barrier strength, in this case it is assumed that, whilst the total relief capacity is acceptable, there are sections of the plant where relief capacity is marginal. The valves were all installed when the plant was new and are now four years old, and have not yet been re-certified/re-calibrated, so there are no grounds to be confident in the condition of the valves. Hence, a middle rating for condition and a low rating for confidence in condition is achieved. PSVs are a well understood piece of technology, but they are known to stick, thus attaining a middle rating for confidence.

Considering the barrier's readiness, whilst PSVs are not passive, they are self-contained and require no human intervention to operate, and as such a good rating is given. They are relatively simple, but can fail with a hidden defect (they can stick with no readily available means of detecting this). PSVs can also be overridden under a permit system, and the specific types of PSVs used have had good experience in many facilities.

For the criticality, it is assumed that this plant does have a significant overpressure threat that could lead to a major release of hydrocarbon gas. This threat is considered to be present several times a month when e.g. dryers are being switched over, and the PSVs are the main barrier against overpressure events.

Table 2 - Pressure Safety Valves Effectiveness Rating (Overpressure Threat)

Strength	***Rating***	***Weight***	***Weighted Rating***	***Readiness***	***Rating***	**Criticality**	***Rating***
Capacity	3	7	21	Relative activity	4	Frequency of threat/ consequence	1
Suitability	4	1	4	Complexity	4	Reliance on this barrier	2
Current condition	2	1	2	Failure mode	2		
Confidence in condition	3	1	3	Overrides	2		
				Barrier history	3		
Sub-Total			30		15		3
						Overall rating	**15**

In this example the overall barrier effectiveness rating is 15, which is low (the maximum available with this scoring system is 60, assuming that the denominator is 1). Whilst the exact ratings could undoubtedly be debated, this low rating should indicate to management that the recertification of these PSVs needs to be expedited and a test programme established to confirm that they are functioning as intended.

In the following example in Table 3, a corrosion resistant alloy pressure containment system is considered against the threat of internal corrosion. This achieves ratings higher than the PSV on a number of criteria (again, assumptions have been made as to the nature of the threat and the barrier's properties), but is a completely passive barrier. This achieves an overall rating of 9.2, which is considerably better than the PSV, but the difficulty in confidently ascertaining its condition and the level of reliance that can be placed on it prevent it from scoring higher. This is in turn compared with the carbon steel containment envelope and chemical injection (see Table 4.).

Table 3 - CRA Pressure Containment Envelope Effectiveness Rating (Internal Corrosion Threat)

Strength	*Rating*	*Weight*	*Weighted Rating*	*Readiness*	*Rating*	**Criticality**	*Rating*
Capacity	4	7	21	Relative activity	4	Frequency of threat/ consequence	4
Suitability	4	1	4	Complexity	4	Reliance on this barrier	2
Current condition	3	1	2	Failure mode	2		
Confidence in condition	3	1	3	Overrides	4		
				Barrier history	3		
Sub-Total			30		15		6
						Overall rating	**9.2**

Table 4 - Combined Carbon Steel pressure envelope and chemical injection Effectiveness Rating (Internal Corrosion Threat)

Strength	*Rating*	*Weight*	*Weighted Rating*	*Readiness*	*Rating*	**Criticality**	*Rating*
Capacity	4	7	28	Relative activity	4	Frequency of threat/ consequence	4
Suitability	4	1	4	Complexity	2	Reliance on this barrier	2
Current condition	3	1	3	Failure mode	2		
Confidence in condition	2	1	3	Overrides	2		
				Barrier history	***3***		
Sub-Total			37		14		6
						Overall rating	**8.5**

Multiple barrier effectiveness rating

The discussion above focuses on the assessment of individual (complete) barriers, however the overall effectiveness of barriers, on any given threat line or consequence line, is likely to be the primary focus of decision makers. As the definition of barriers used in this paper is of independent barriers (i.e. failing does not mean that the overall line of defense is overcome), the overall effectiveness rating can thus be evaluated as:

$OE_a = \sum_1^x BE_n$

Where: OE_a = Overall effectiveness of the barriers on a threat or consequence line
$_{1 \text{ to } x}$ = The barriers on the threat line being considered

This is illustrated in the following example.

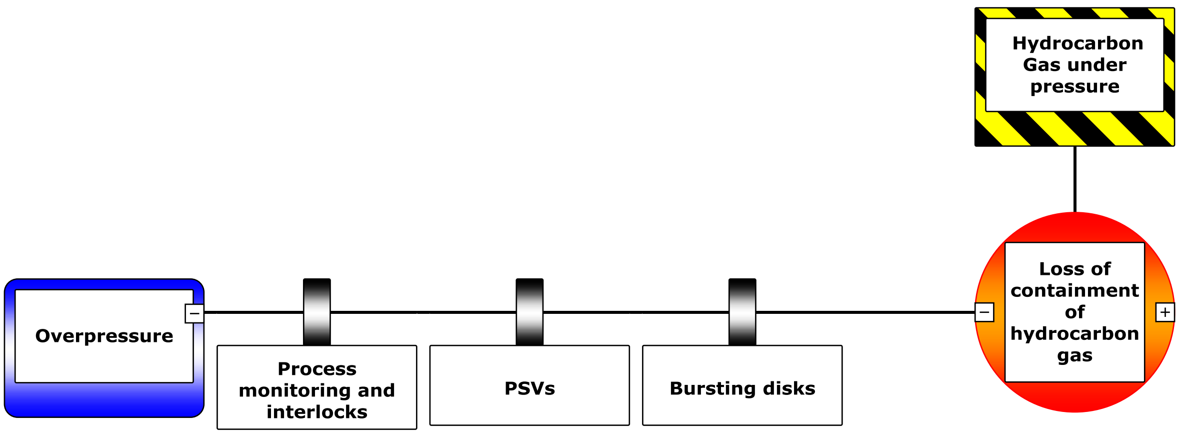

Figure 7 – Multiple independent barriers

Considering the example in Figure 7, we already have the effectiveness rating for the PSVs. Tables 5 and 6 show the ratings for the process monitoring and bursting disk barriers.

Table 5 - Process monitoring and interlocks

Strength	***Rating***	***Weight***	***Weighted score***	***Readiness***	***Rating***	***Criticality***	***Rating***
Capacity	2	7	14	Relative activity	2	Frequency of threat/ consequence	1
Suitability	2	1	2	Complexity	1	Reliance on this barrier	2
Current condition	3	1	3	Failure mode	2		
Confidence in condition	3	1	3	Availability and use of overrides	2		
				Barrier history	2		
Sub-Total			22		9		3
						Overall rating	**10.3**

Table 6 - Bursting disks

Strength	***Rating***	***Weight***	***Weighted score***	***Readiness***	***Rating***	***Criticality***	***Rating***
Capacity	4	7	28	Relative activity	4	Frequency of threat/ consequence	1
Suitability	4	1	4	Complexity	3	Reliance on this barrier	2
Current condition	4	1	4	Failure mode			
Confidence in condition	4	1	4	Availability and use of overrides	3		
				Barrier history	4		
Sub-Total			40		14		3
						Overall rating	**18.0**

The summation of the effectiveness ratings of these three barriers is:

$$OE_a = \sum_{1}^{x} BEn = \mathbf{15+10.3+18} = \mathbf{43.5}$$

This compares with the single barrier example for protection against an internal corrosion threat (where the effectiveness for the two cases considered in Tables 3 and 4 was rated at about 9 (8.8. and 9.2 for the two cases). So is this indicating that the barriers against overpressure are more than four times more effective than those for internal corrosion? Recognising that these ratings are for a hypothetical set of conditions, where there is a corrosive/wet gas, internal corrosion would typically be expected to be one of the dominant threats at some point in time. This, however, would not be the case initially when (for the carbon steel case) there would be a corrosion allowance that would provide increased effectiveness (in the example the rating for condition was relatively high as a fairly recent facility was being considered). This introduces the concept of barrier effectiveness over time and how this is not necessarily constant (hence the inclusion of Current condition and Confidence in condition).

Practicalities and criteria selection

To maintain this approach as a practical tool, the ratings are assigned in structured multi-disciplinary review workshops, where threat and consequence lines are considered in turn. Many barriers will appear on multiple threat lines, and the effectiveness of the barrier may not always be the same, so barriers should be re-rated for each threat and consequence line.

Contribution to managing assets throughout their lifecycle

This approach can be used throughout the lifecycle of a facility, from design to decommissioning. Whilst the role of bowties in design has generally been limited to the recording of design decisions, this approach provides a tool for considering the adequacy of barriers against different threats during design. This allows optimisation of the protection provided.

As a facility goes enters operation, this approach can provide a decision support tool to allow risk based decisions to be more effectively made and to allow operational expenditure to be focused on maintaining the facility's risk profile at acceptable levels (e.g. prioritising maintenance and inspection/testing on the most critical barriers).

It should be remembered that this approach provides a snapshot in time of barrier effectiveness. This can be kept current by identifying the data sources that would allow the recalibration of the ratings (based on the known condition and operational experience), which can then be readily mapped onto a dashboard to give operational managers a tool for assessing changes to the risk profile of their facility.

As a facility enters late life and possibly life extension, this approach can still be used to assess how ageing has impacted the effectiveness of barriers. Specific threats associated with late life (such as obsolescence of equipment and fatigue becoming a more dominant threat) can be used to reassign strength, readiness and criticality values.

Conclusions

The approach presented in this paper provides a practical means of developing a view of the level of protection that is provided on a facility and how this changes over time. It converts bowties from being a recording and presentation tool into a valuable element in risk based decision making.