Representing Human Factors in Bow Ties as per the new 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, Ron McLeod Ltd., Glasgow, UK

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

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 nearing the end of a long process to develop, write, review, edit and issue a CCPS/EI Concept book (prepared together with the Energy Institute) on the use of Bow ties in risk management. The final chapter of the draft book addresses representing human factors in bow ties, part of which is summarised in this paper.

In bow ties barriers are in place to stop the threat leading to the "top event" or to prevent the top event leading to catastrophes. These barriers are either passive barriers (e.g. crash barriers, bunds), continuous barriers (e.g. ventilation) or active barriers. Active barriers need to have separate elements to "detect" the threat, "decide" what to do about it and to "act" to stop the trajectory. This means that typical human factors aspects such as "training", "competence", "safety culture" or "leadership" cannot appear by themselves as barriers on the main threat line. Instead, they are <u>essential</u> to ensure the correct operation of the barriers. As such, they appear as safeguards on the degradation factors that affect a barrier.

Almost everyone agrees that a positive safety culture, process safety leadership, etc. are needed for the safe operation of a facility. There is, however, currently no clear way of demonstrating how these aspects prevent a major accident and possible subsequent fatalities. The approach described in this paper uses multiple layers of bow ties to demonstrate the clear link between these human factors and preventing major accidents. Sharing these bow ties with operators would support positive safety culture efforts.

There are four important premises addressing human factors in bow tie analysis:

In basic ("Level 0") bow ties, human error should preferably not be directly modelled as a threat that can lead to a top event. The threats are inherent threats arising from the operation.

Active barriers, with detect, decide and act components very often involve humans in one of the elements and so it is important to understand how these degrade the barrier

Mechanical failures and human errors can defeat or degrade these barriers. Safeguards are then needed to be put in place to mitigate the risk and to prevent this happening. The term "safeguard" is used to denote those controls not meeting the full requirements of an active barrier.

Most of the controls that organisations use to minimise human error cannot meet the criteria necessary to be considered active barriers in their own right (effective, independent and auditable). They are, nevertheless, very important safeguards to manage the risk from human error leading to degrading the performance of active barriers. Safeguards can range from local warnings and signs, the design and implementation of alarms and the human machine-interface (HMI) to control systems, through job design, operating procedures and cross-checking practices, to "Stop Culture" (the willingness of front-line personnel to stop work if they have any concerns over safety), Leadership, etc.

More detailed bow ties (referred to in this paper as "level -1", "level -2", etc.) can be developed that focus on understanding how those safeguards, the human and organizational controls, can themselves be degraded or defeated. Typically two levels will be needed (i.e. the top level, which identifies the main barriers, and level -1, analysing human error as a degradation factor for the top level barriers).

The paper uses a Buncefield-type scenario of overfilling a fuel storage tank to illustrate the application of this approach.

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

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

The Center for Chemical Process Safety (CCPS), part of the American Institute from Chemical Engineers (AIChE) have for a long while produced the definitive textbooks providing guidance on aspects of process safety from Risk Based Process Safety (CCPS, April 2007) to developing Guidelines for Implementing process safety management systems (CCPS, June 2016), etc. They responded positively to a proposal for a book on bow ties. In parallel to this effort, the Energy Institute's Human Factors

Committee had been working on the description of human factors in bow ties. The logical combination of these efforts culminated in the EI joining CCPS in sponsoring an additional chapter to the now CCPS/EI book specifically looking at representations of human factors in bow ties.

The bulk of the book covers the elements of a barrier management program, including how to create bow ties, and various uses of bow ties. It is summarised in a parallel poster being presented at Hazards 27. In the current draft there is a chapter addressing the human factors issues that need to be taken into account in developing and implementing bow ties and how to represent human factors using "layered" bow ties. That chapter is summarised in this paper and was written by a cross-section of human factors specialists from both industrial and regulatory backgrounds, as well as non-specialists with many years' experience addressing human factors issues in safety management systems. Current approaches to bow tie modelling rarely either capture the complexity of the human contribution to barrier systems, or recognize the range of factors that need to be managed to mitigate the risk from "human error".

This paper, and the associated chapter, presents a novel approach and ideas that are in the early stages of being implemented. Nonetheless, we feel that this approach will greatly enhance the overall understanding of human factors and provide a visual link on how managing human factors well will reduce the probability of fatalities from major accident events (MAEs).

While the thoughts and concepts presented here were being developed, there was a parallel activity within the Chartered Institute of Ergonomics and Human Factors (CIEHF). There was overlap in membership of the two committees so both arrived at comparable outcomes between this section of the CCPS/EI book and the CIEHF's "Human Factors in Barrier Management" White Paper (CIEHF, 2016).

Definition of Key Bow tie Terms

A more complete description of the elements of a bow tie, as presented in the CCPS/EI book, are covered in a separate paper. These are repeated here, in brief, for completion.

Hazard: anything that has the potential to cause harm, similar to the normal HSE definition

Top event: when things start to go wrong, the "oh no" moment. In the oil and gas industry, this is typically a loss of containment. For many other bow tie applications this is the loss of control.

Consequence: bow ties are not typically developed to describe trivial events. The consequences addressed are typically fatalities (e.g. caused by a vapour cloud explosion), a Major Accident to the Environment (MATTE) (e.g. from a leak leading to long-term harm to an environmental receptor), significant asset damage or harm to the corporate reputation (and so share price). They are typically classified using a corporate risk assessment matrix as the most severe consequences.

Threats: threats have the potential, if not inhibited, to lead to the top event. The non-functioning of a barrier is therefore not a threat because it cannot cause the top event to occur. Threats are therefore similar to those used in HAZOPs such as overpressure, excessive flow (in excess of the volume of a receiving tank), etc.

One picture tells a thousand words, so Figure 1 shows an example of the use of these terms for the case of possible tank overfill *a la* Buncefield.

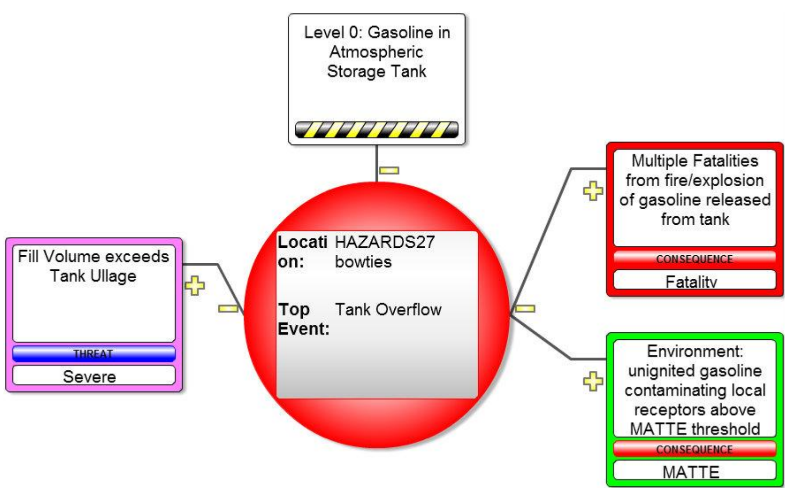

Figure 1: Representation of a potential Buncefield-type scenario in a bow tie

The other main elements of a bow tie, barriers, degradation factors and safeguards, will be discussed further background on human and organisational factors.

Human and Organizational Factors - Conventional Approach

The CCPS previously defined Human Factors as a discipline concerned with designing machines, operations and work environments to match human capabilities, limitations, and needs, i.e. emphasising ergonomics.

The UK Health and Safety Executive's dedicated web sub-site (HSE, 2016) consider that "human factors" help to avoid accidents and ill health at work and so provide a wider list of topics: managing human failures, staffing, fatigue and shift work, safety critical communications, human factors in design, procedures, competence, organisational change, organisational culture, maintenance, inspection and testing. This broader definition is the one used in this paper.

As described above, a "threat" is something that can lead to a top event if not prevented by a barrier. In bow ties human and organisational factors (HOFs) will generally be degradation factors, or 'threats', to stopping a barrier working as intended, rather than a threat on the main threat line. Why, because by themselves the HOFs generally do not have the ability to combine with the hazard to lead to a top event. HOFs will also be present as safeguards to prevent other degradation factors affecting a barrier. They cannot be hazards or top events.

Historically some bow ties have been developed with vague descriptions of human error and the barriers. Applying that approach, we would arrive at the bow tie shown in Figure 2 for our Buncefield-type scenario.

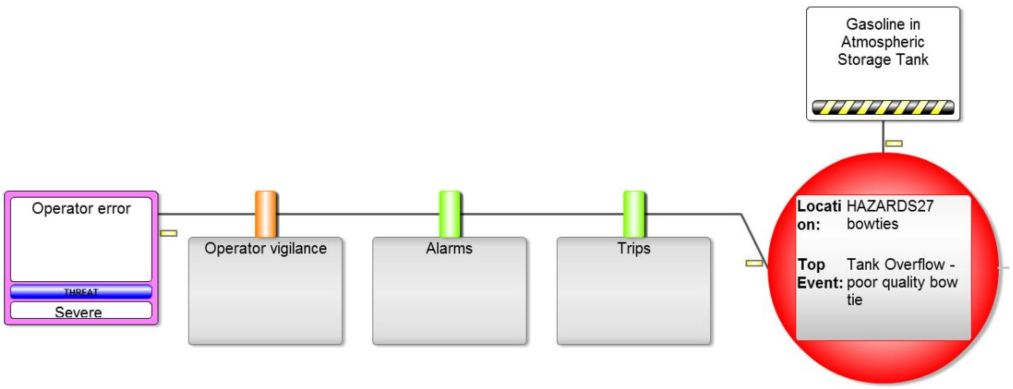

Figure 2: Poor quality bow tie in terms of both threat and barrier definition

Why this is wrong is clear when we review HSE guidance on human failure (HSE, 1999) (Figure 3) that follows the categories originally introduced by Reason (1990) and defines human failures as errors, violations, slips, lapses and mistakes whether intended or unintended actions.

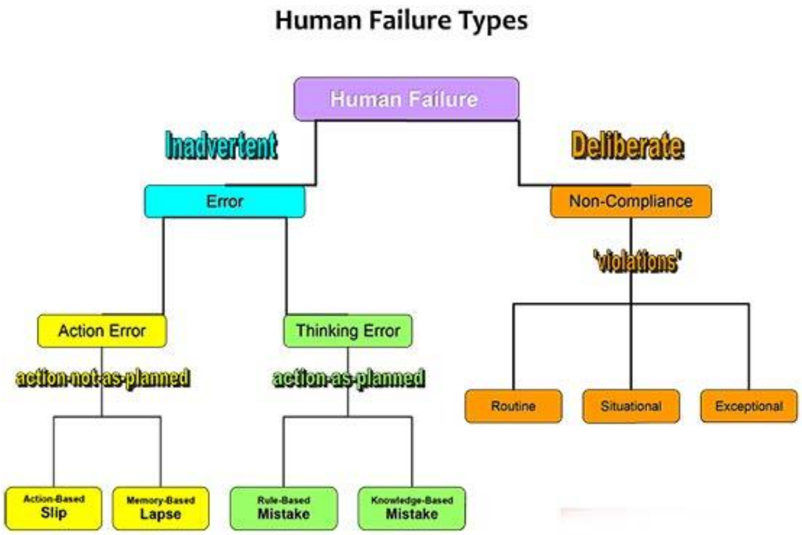

Figure 3: Types of human failures, as per HSE guidance (HSE, nd)

If we combine this description with the requirements that a threat, if not prevented by a barrier, has to lead to a top event, then it becomes clear that "operator error" is a very poor description of the threat. In this case, the threat instead comes from a flow of gasoline to the storage tank larger than its total ullage. The barriers in Figure 2 also do not comply with the definition for active barriers, i.e. to have elements to detect, decide and act and also to be effective, independent and auditable. Replacing the vague threats and barriers with those that comply with the CCPS/EI book recommendations leads to the alternative bow tie shown in Figure 4.

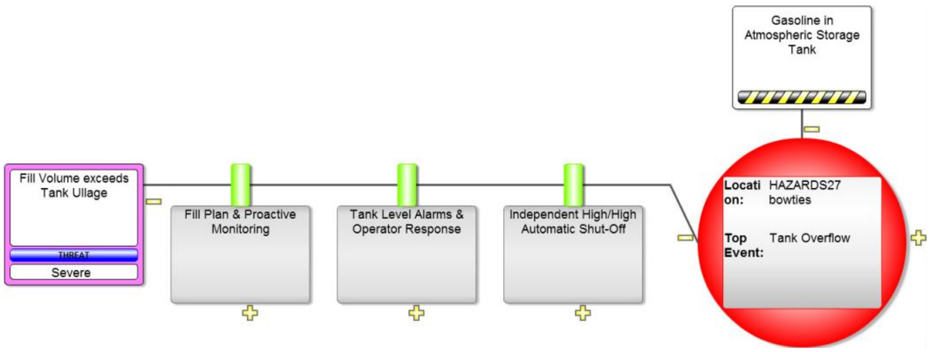

Figure 4: Better description of the threat for the example of tank overflow bow tie

Here the threat is now specific and the barriers meet the criteria laid out earlier for an active barrier. However, it does mean that all human factors, both positive and negative, have disappeared from this representation of the bow tie (e.g. the second barrier requires a human response with the operator taking action).

The human factors are still present for the case of potential tank overflow, but now they appear mainly as the factors that degrade the function of the barriers (i.e. "degradation factors", previously called "escalation factors" because they were escalating the risks) or as safeguards to prevent the degradation factors affecting the barriers (Figure 5).

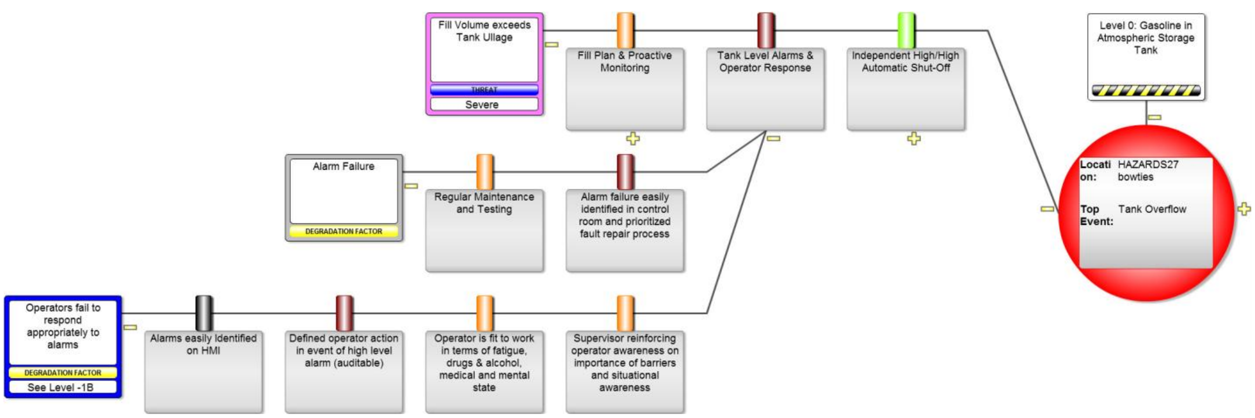

Figure 5: Human Factors appearing predominantly as degradation factors and safeguards

The tank level alarm and operator response barrier may fail in any of the three elements of detect, decide and act. Figure 5 shows some of the possible degradation factors. There may be others but we have restricted ourselves to just these two to demonstrate the concept. Here human factors appear as one of the two degradation factors (the operators not responding correctly to the alarm) but in most of the safeguards to prevent this happening. The message is then that operators are key to preventing tank overflows. Their contribution to preventing the catastrophe is far greater than the risks they introduce.

In summary, the guidelines on treatment of human error in basic bow ties are as follows:

1. Human error should not normally appear as a main pathway threat as it is too generic for meaningful barriers and the resulting barriers would probably not meet the standard required of being able on their own to terminate the sequence.
2. Very specific errors (e.g. valve opened too soon) can be main pathway threats, but this is not an ideal placement. As before, verify that barriers deployed can genuinely terminate the event.

3. Human error is better treated as a degradation pathway threat impairing a main pathway barrier and mitigated by a range of safeguards (e.g. training and competence of a particular task, stop work culture (that an operator will intervene), etc.). These safeguards enhance the reliability of the main pathway barrier. The human error threat would normally be defined in specific terms, not simply "human error".

"Multi-Level Bow Tie" Approach

Up to this stage, there has been nothing substantially new, although there has been a refinement and clarification in the thoughts and processes associated with developing bow ties and the definitions around threats and barriers. The bow tie in Figure 5 does touch upon some human factors elements but only with specific details describing operator actions as the safeguards to prevent the barriers failing. The useful question may now be to consider in more detail as to how and why, for example, the safeguard of "defined operator action in event of high level alarm" may not work as desired, i.e. are there degradation factors for this safeguard?

One of the main benefits of bow ties is to produce useful visual overviews of the potential major accident event (MAE). Adding a second level of degradation on the safeguards themselves will start to make the visual image much more complex and so defeat the whole idea of clarity and simplicity. Typically, only key degradation factors and safeguards are shown on the main bow tie to limit the complexity.

The preferred approach is therefore to create this additional analysis of HOF as a separate bow tie. The proposed approach is to call the main, top level bow tie 'Level 0' and for the separate bow ties that are delving in to the details of how the safeguards themselves degrade as a lower level or Level -1. In theory then it would also be possible to produce bow ties showing the degradation factors on the safeguards in the Level -1 bow ties as Level -2 bow ties, etc. but with diminishing returns of value to the organisation.

The concept of multi-level bow ties is shown schematically in Figure 6. The upper part of this figure is the Level 0, comprising all the basic bow tie main pathways (threat and consequence arms) and degradation factors and safeguards. Level-1 duplicates the degradation pathway shown here for Barrier 2 (only), but built out again as a basic bow tie. Thus the level 0 degradation pathway threat (Degradation factor A) becomes the level-1 main pathway threat, the top event becomes the hazard, and the new top event is the failure of Barrier 2. However, safeguards remain "safeguards" as they do not meet the requirements for a barrier.

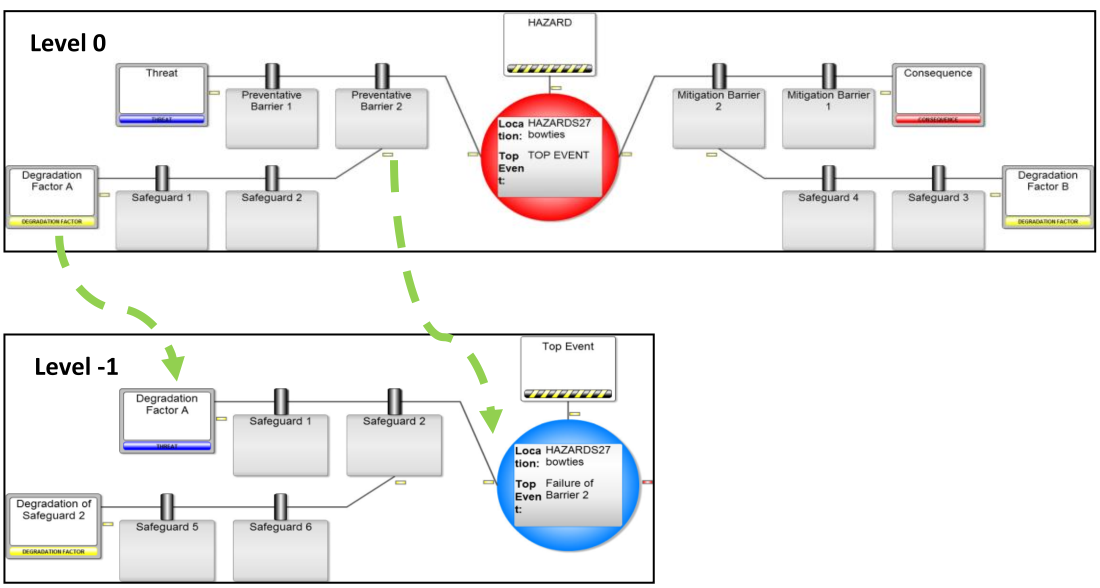

Figure 6: The concept of multi-level bow ties for Level 0 and Level -1

Next Level-2 repeats the process showing how Level-1 safeguards can degrade. The example here shows this for Safeguard (Figure 7).

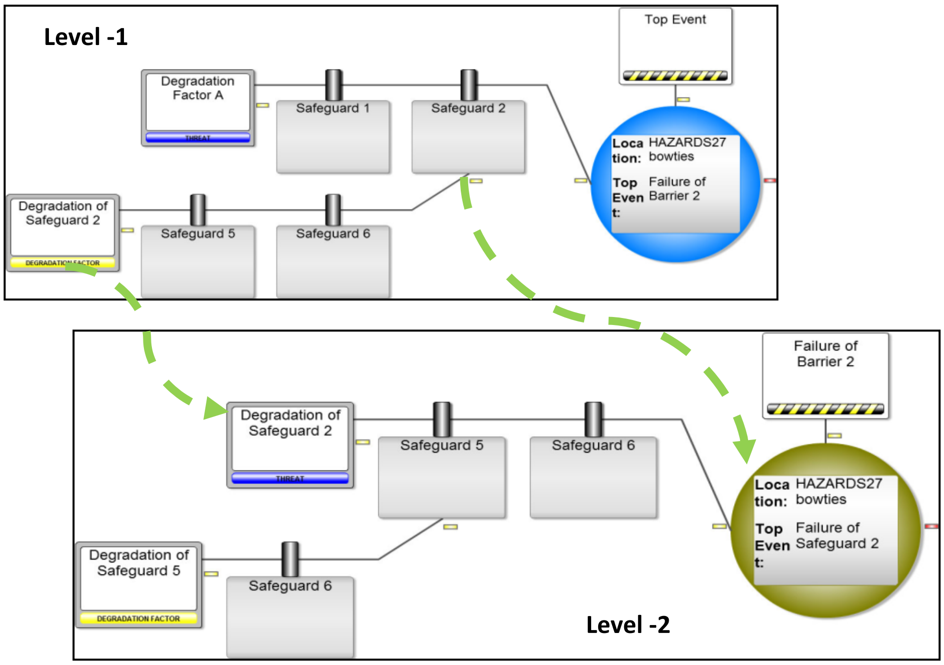

Figure 7: The concept of multi-level bow ties for Level -1 and Level -2

Level-2 may be a valuable addition because it will document the more generic human factor safeguards that are important, but might not show up in the more specific Level-1 build-outs. Some secondary safeguards might include leadership, fatigue management, competency, recruitment policies, drug and alcohol screening, safety culture assessments, etc.

Important premises with multi-level bow ties

Taking the above into account, the recommended approach for addressing human factors in bow tie analysis is based on four important premises:

1. In bow ties human error should not be modelled as a threat that can lead to a top event. Instead, attention should be focused on identifying the barriers that human error can defeat or degrade and on ensuring those barriers are as robust as they reasonably can be both to human error and to other degradation factors.
2. Human error will however frequently be identified as a potential degradation factor. When that is the case, it is important to understand both how the error can arise, and to ensure there are sufficient controls in place to mitigate the risk and to make the human error specific to the barrier being degraded (or safeguard being degraded in the lower level bow ties).
3. Organizations can decide for themselves whether to develop bow ties at a basic level (Level 0) where the first level of HOFs can be included as degradation factors and safeguards or if they see value in investigating the further layers of possible degradation in more detail of Level-1, Level-2, etc.
4. Most of the Human and Organizational controls used to mitigate human error cannot meet the criteria necessary to be considered barriers in their own right (for active barriers to detect, decide and act and to also be effective, independent and auditable). These factors are therefore considered as "safeguards", rather than barriers.

Application of Multi-level Bow Ties for Tank Overfill

Again, the easiest explanation of the concept may be to continue the example of the Buncefield-type bow tie for tank overfill. The Level 0 bow tie was shown in Figure 5, above. There we had identified two degradation factors for the Alarm and Operator Response barrier, namely failure of the detect action due to an unrevealed alarm, and failure of the combined detect and act elements due to improper response to the alarm by the operators. The "operators fail to respond appropriately to alarm" degradation factor had four safeguards:

1. alarms easily identified in the Human-Machine Interface (HMI) to ensure the operator can see the alarm
2. defined operator actions in response to high level alarm (auditable) to ensure the operator knows how to respond
3. checks to ensure the operator is physically capable of responding to the alarm (fit to work)
4. systems to ensure the operator is mentally and culturally able to respond appropriately (barrier awareness)

The corresponding Level-1 bow tie now considers the top event to be the failure of the Alarm and Operator Response barrier, the "threat" is now what was the degradation factor in the Level 0 bow tie and the previous safeguards now become the "barriers" in the Level-1 bow tie (Figure 8).

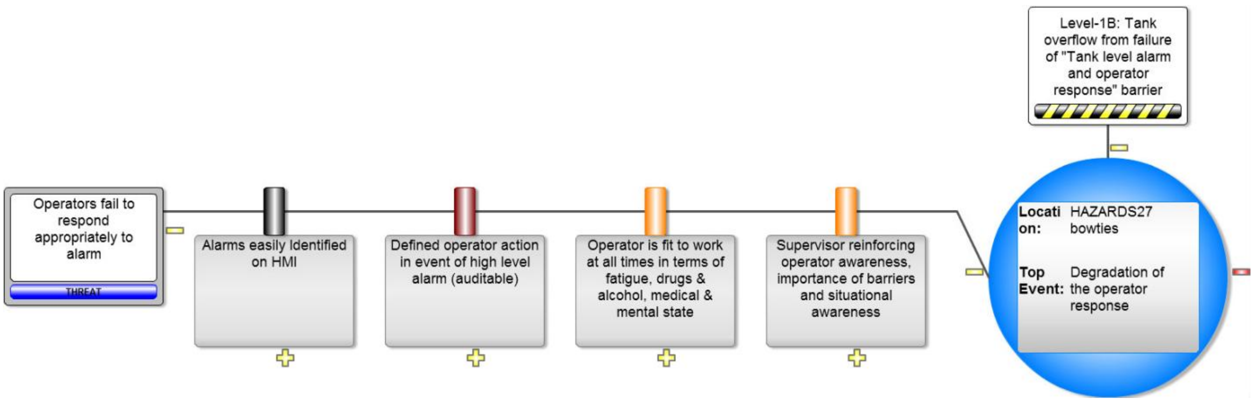

Figure 8: Level -1 bow tie investigating possible failure of the Alarm and Operator Response barrier

We now have the possibility to consider the degradation factors that could affect each of the safeguards in this Level-1 bow tie. These are shown separately in Figures 9 to 12 and then combined together in Figure 13. Note, only selective degradation factors have been shown in this example. These figures do not cover all degradation factors that could apply.

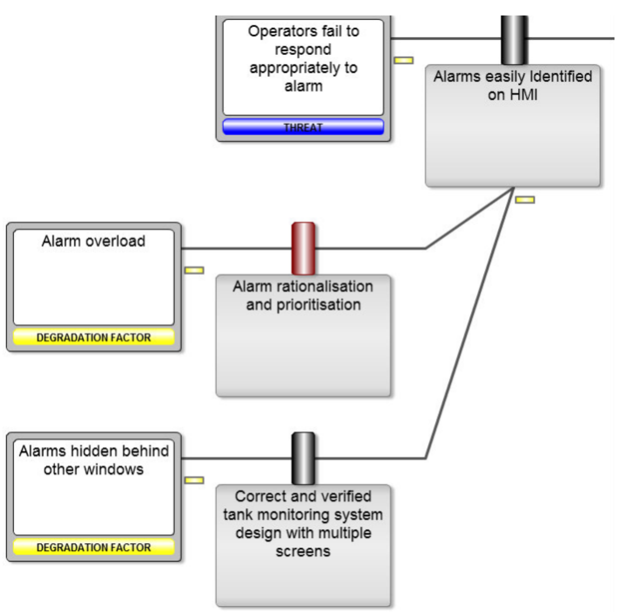

Figure 9: Degradation factors and safeguards to ensure the operator can see the alarm

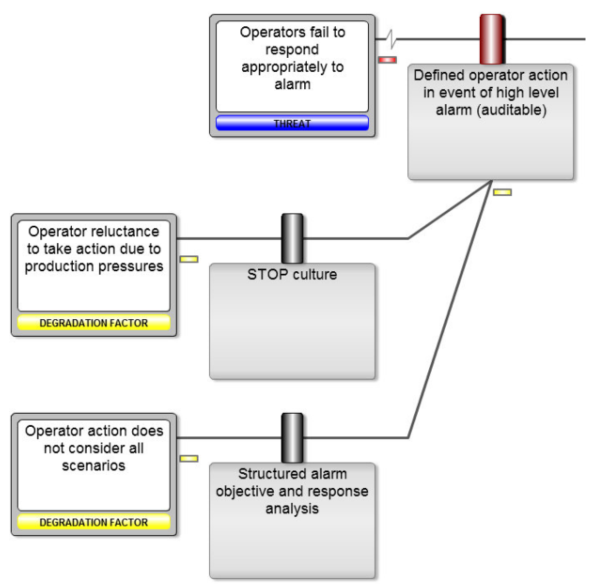

Figure 10: Degradation factors and safeguards to ensure the operator knows how to respond to the alarm

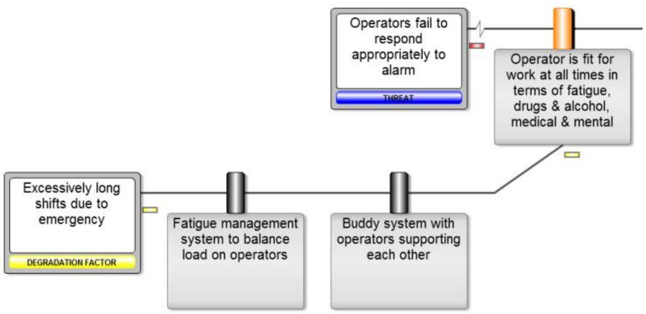

Figure 11: Degradation factor and safeguards so operator is physically and mentally fit to respond to the alarm

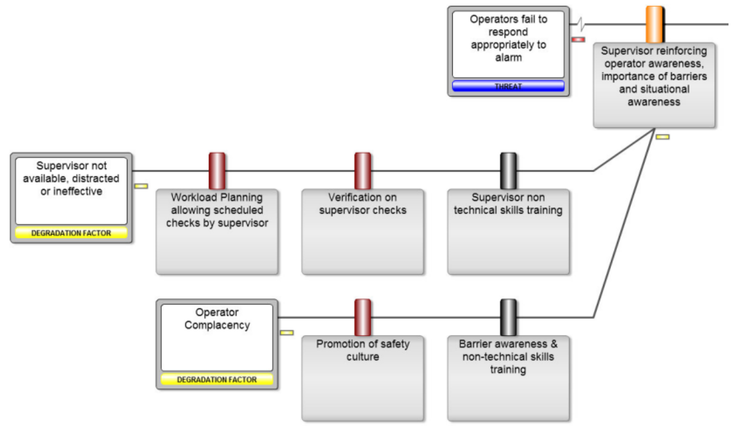

Figure 12: Degradation factors and safeguards to maintain supervisor's effectiveness and operator's predisposition to respond appropriately (barrier awareness)

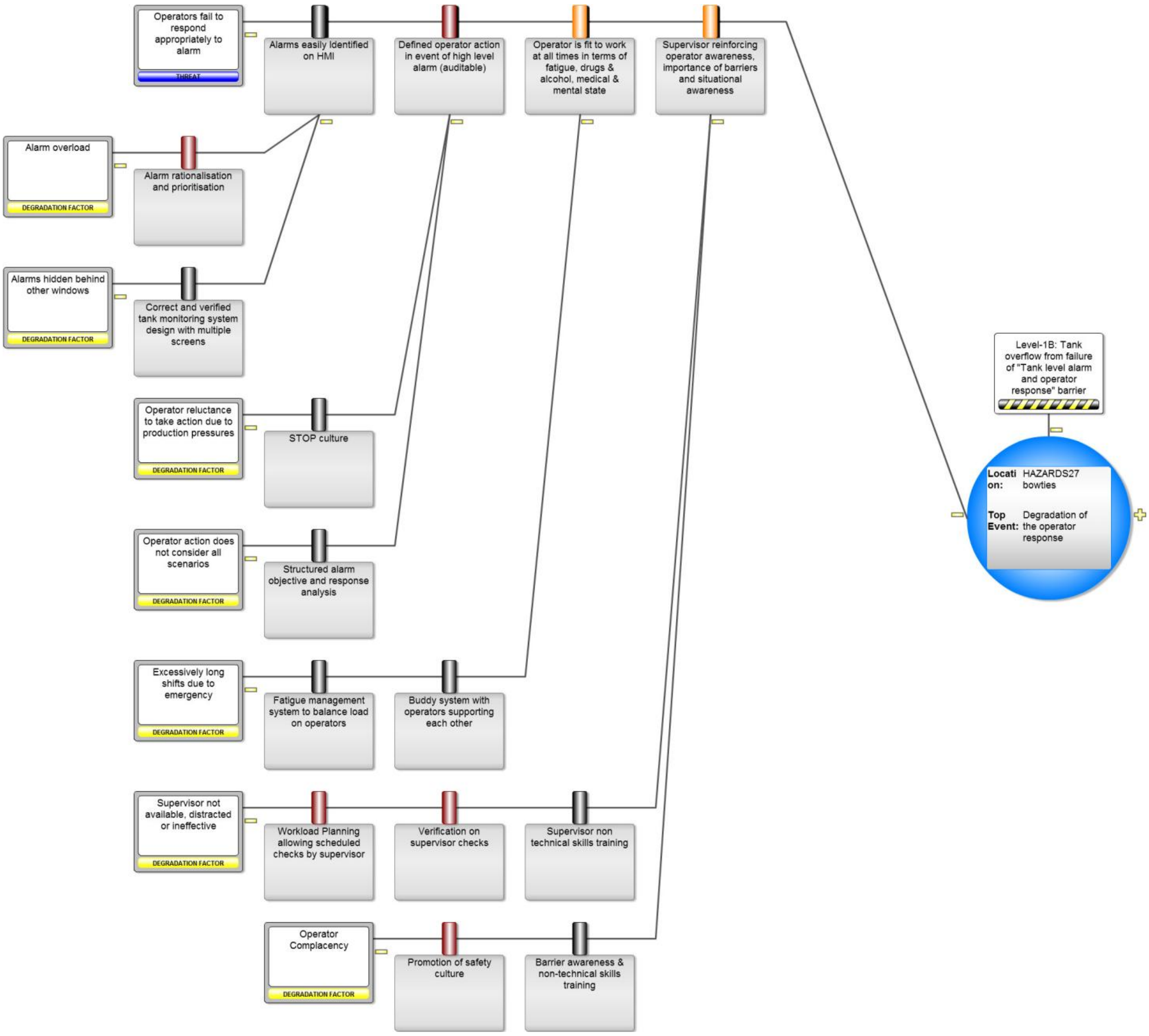

Figure 13: The fully expanded Level -1 for failure of operators to respond appropriately

Figure 13 does start to become complex but the real benefit is to now show how the soft human factors topics actually work as safeguards to prevent the worst case consequence of the VCE and fatalities, such as:

- Performing an Alarm Objective Analysis (a structured review of all alarms to document why they occur and what the operator response should be), with this outcome being logged in an alarm management system working with the Basic Process Control System (BPCS, also known as Distributed Control Systems or DCS)
- Alarm rationalisation processes to avoid operators not responding due to alarm overload
- STOP Culture driving operators to prioritise safety over production and so be willing to halt production if needed
- Safety culture to enhance a feeling of "Chronic unease" so that operators do not become complacent and stop responding appropriately to alarms
- HMI studies to ensure operators can easily access relevant alarms
- Supervision to ensure that operators maintain their vigilance and remain aware of their important role in preventing a MAE

We could easily have also expanded the other degradation factor for this barrier of an unrevealed alarm failure where maintenance and testing was identified as the safeguard. This would have allowed identification of the issues surrounding maintenance, documenting the degradation factors showing why it may not happen as and when required.

Beyond the Level-1, it would be possible to investigate deeper. We had identified that supervision is needed to maintain barrier awareness with safeguards of workload planning to allow sufficient time for supervision and verification checks on supervision. If desired we could investigate what may cause there to be insufficient supervision. As one can see there will come a point of diminishing returns.

Generic Human Factors Bow Ties

Many users of bow ties have in the past developed generic bow ties for human factors. These show generic human error threats such as fatigue, drug & alcohol, work overload and show all the programs deployed to reduce the likelihood of these threats. These lead to a top event of Human Error. However, the consequence side can be confusing as the barriers on this side depend on the actual operational situation. In addition, these so-called barriers are actually safeguards, as they mostly do not have the full functionality required of a barrier. Thus, the generic bow ties do not conform to the CCPS/EI book formal requirements for bow ties.

In many ways, the generic bow ties approach is similar to the idea of the Level-2 bow ties in the multi-level approach, but without the clear linkages to actual major accident events demonstrated in the multi-level approach.

Thus while it appears that Level-1 makes the bow tie more complicated, it does however show important safeguards not evident in the basic bow tie (level 0) and it avoids duplication for these more general safeguards.

Conclusions

The CCPS/EI is in the process of developing a bow tie book to provide industry-wide guidance on the structure and development of bow ties. The book also has an extensive chapter on incorporating human factors into bow ties. Key to that chapter is the concept of multi-layered bow ties.

Level 0 bow ties are the classical bow ties with threats potentially leading to a top event and ultimately catastrophic consequences. There are preventative barriers to prevent the top event occurring and mitigation barriers to reduce the consequences from the top event and to avoid the worst-case scenarios of fatalities and major environmental incidents. Degradation factors can prevent the barriers performing as desired and safeguards are present to prevent this happening.

Many of the safeguards are associated with human activities.

Level-1 bow ties start from Level 0 bow tie and investigate the degradation factors that could negatively affect the performance of the safeguards.

Because many of the safeguards contain human activities, the factors that will prevent humans acting appropriately will be the typical safety culture issues. By developing Level-1 (and, if needed Level-2) bow ties it is then possible to have a clear demonstration of why positive human factors behaviours, such as STOP culture, can lead to preventing a specific major accident event.

It is hoped that providing this clear link between the “motherhood and apple pie” topic of a positive safety culture to the actual MAEs that can occur at a facility will enable a better understanding in the minds of operators, etc. The hoped for outcome is that staff will self-motivated to perform these activities, rather than because of a simple fiat from on high.

Bibliography

CCPS. (April 2007). *Guidelines for Risk Based Process Safety.* ISBN: 978-0-470-16569-0: Center for Chemical Process Safety, Wiley.

CCPS. (June 2016). *Guidelines for Implementing Process Safety Management (2nd Edition).* Centre for Chemical Process Safety, Wiley.

CIEHF. (2016). *Human Factors in Barrier Management.* Chartered Institute of Ergonomics and Human Factors. Retrieved from http://www.ergonomics.org.uk/learn/barrier-management/

HSE. (1999). *HSG-48 Reducing Error and Influencing Behaviour.* Health and Safety Executive. Retrieved Jan 2107, from http://www.hse.gov.uk/pubns/priced/hsg48.pdf

HSE. (2016, December). *Human factors and ergonomics web site*. Retrieved from HSE Guidance: http://www.hse.gov.uk/humanfactors/

HSE. (nd). *Human Factor Types.* Health and Safety Executive. Retrieved Feb 2017, from http://www.hse.gov.uk/humanfactors/topics/types.pdf