CHEMICAL ENGINEERING TRANSACTIONS
VOL. 67, 2018
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.aidic.it/cet
Guest Editors: Valerio Cozzani, Bruno Fabiano, Davide Manca

ISBN 978-88-95608-64-8; **ISSN** 2283-9216
DOI: 10.3303/CET1867043

Sound Barriers Management in Process Safety: Bow-tie Approach According to the First Official AIChE - CCPS Guidelines

Luca Fiorentini *[a], Luca Marmo [b]

[a] TECSA S.r.l.
[b] Politecnico di Torino
luca.fiorentini@tecsasrl.it

Safety barrier-based management systems are widely adopted because of the advantages coming from the barrier approach. Different methods are available to implement it and the Bow-tie is one of the most recognized methodology. The Bow-tie method allows the risk analyst to have, in a single shot, the complex picture about the relations linking threats, preventive barriers, top events, mitigative barriers, consequences, and escalation factors. From this perspective, without a proper reference, there are significant possibilities to misuse the method and create confusion about the right role of each component of a Bow-tie diagram. This work intends to support the approach of the guidelines developed by the Center for Chemical Process Safety (CCPS) of the American Institute of Chemical Engineers (AIChE), to drive the analyst in the proper usage of the method, avoiding to misinterpret key elements like the human errors or the barrier failures, and helping in a congruent definition of the elements, thus resulting in a high-quality risk analysis and in a sound barriers management.

1. The barrier-based approach to process safety: the Bow-tie method

Bow-ties are a powerful graphical representation of a risk analysis, linking together, in a simplified definition, a fault tree (left-side) and an event tree (right-side) (Luca Fiorentini and Luca Marmo, 2018). The point of connection is the *Top Event*, i.e. an unwanted event that could happen because of the loss of control on the hazards (usually normally present to run the business). A *Top Event* may come from one or more *Threats:* to control them, *Preventive Barriers* are put in place. However, the *Top Event* is not yet the final scenario: indeed, a *Top Event* may result in one or more *Consequences*, i.e. incidental scenarios. To reduce their effects, *Mitigative Barriers* are put in place. The brief description here presented allows to draw the Bow-tie in Figure 1.

2. Contents of the AIChE - CCPS guidelines

Even if the definition of the main elements of a Bow-tie model strictly depends on the specific risk analysis (mainly on the business sectors and the goals of the analysis), there are some rules that the risk analyst should follow in order to properly apply the Bow-tie method, regardless its scope and objectives. The guidelines developed by the Center for Chemical Process Safety (CCPS) of the American Institute of Chemical Engineers (AIChE) provide some sound reference to follow, in order to reduce the risk of a misusage of this method (CCPS, 2017). The present Chapter briefly shows them. The formal definition of Bow-tie diagram, provided by CCPS, is the following: “A diagram for visualizing the types of preventive and mitigative barriers which can be used to manage risk. These barriers are drawn with the threats on the left, the unwanted event at the center, and the consequences on the right, representing the flow of the hazardous materials or energies through its barriers to its destination. The hazards or threats can be proactively addressed on the left with specific barriers (safeguards, layers of protection) to help prevent a hazardous event from occurring; barriers reacting to the event to help reduce the event’s consequences are shown on the right.”

Please cite this article as: Fiorentini L., Marmo L., 2018, Sound barriers management in process safety: bow-tie approach according to the first official aiche - ccps guidelines, Chemical Engineering Transactions, 67, 253-258 DOI: 10.3303/CET1867043

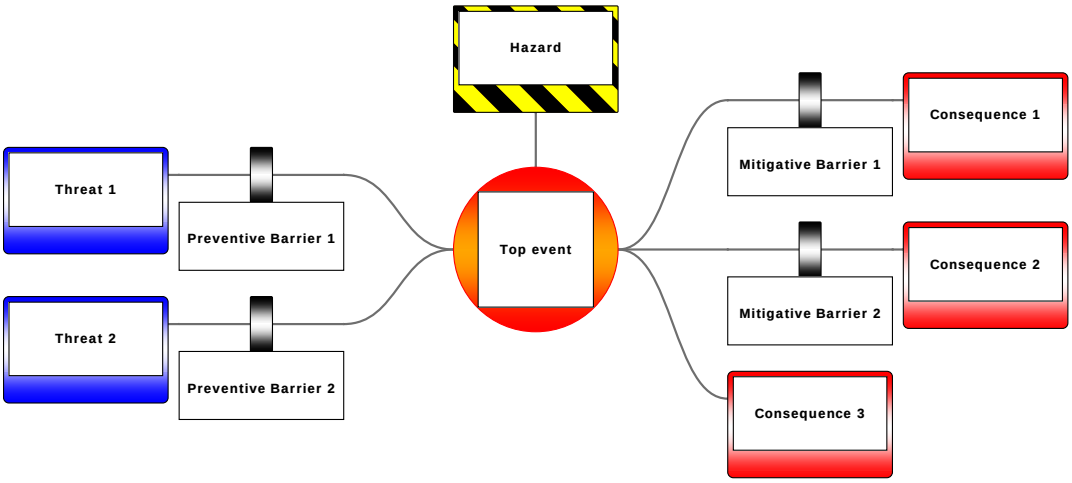

Figure 1: The basic structure of a Bow-tie model

2.1 Definition of Hazards and Top Events

Hazards are intrinsically part of the business: this is especially true in the process industry. It is fundamental to control them for safe plant operations, from installation to decommissioning, not only for the safety of human life, but also for the environment and the business-related risks, like asset integrity, business interruptions, and reputations. In the Bow-tie method, the very first step is providing a clear definition of *Hazards*. To do so, the risk analyst has to define the scope of his/her activities, asking how much in depth the analysis should go. For example, “Hydrocarbons” is a poor definition of *Hazard* in the process industry, whilst it may be sufficient for an industry there it is not supposed to deal with hydrocarbons. However, also in this case, it is always better to provide some detail in the definition of the *Hazard*. Thus, “Gasoline in a storage tank” is a better-defined *Hazard*: it is clear the nature of the hazardous substance and a further reason about its hazardousness is provided (it is in a storage tank). Other examples are shown in Table 1.
Top Events are the actualization of the loss of control on an *Hazard*. A loss of containment is a typical *Top Event* in the process industry. However, the clear definition of the *Top Event* is a precondition to execute a proper Bow-tie analysis: indeed, the definition of the *Threats* and the *Consequences*, i.e. the two parts of the bowtie (the fault tree-like structure on the left and the event tree-like on the right), strictly depends on how clear the *Top Event* is. A poor *Top Event* might result in a poor risk analysis as some case studies clearly demonstrate (Marmo et. al. 2013, Marmo et. al. 2012). For example, the loss of control on a pipeline containing lubes under pressure may result in a Loss Of Primary Containment (LOPC). This definition is generally enough to brainstorm about the possible causes and consequences of a LOPC, but the task is harder if a poorer definition was provided, like “Corrosion” (it is indeed a possible *Threat*), or “Release” (of what?) and so on. Other examples are shown in Table 2.

2.2 Definition of Threats and Consequences

The guidelines provided by the CCPS of the AIChE highlight the main features that the right definition of *Threats* and the *Consequences* should have to possess. First of all, *Threats* must be direct. This means that every identified *Threat* causes the *Top Event* directly. The multiple *Threats* need to be independent to each other: this requirement is fundamental when a LOPA analysis is run to quantify a Bow-tie in frequency: independency of the *Threats* results in an OR gate when combining their single frequency of occurrence to obtain the frequency of the *Top Event*. Credibility is also essential for *Threats*, since the definition of incredible causes may bring to overestimate the frequency of occurrence of the *Top Event*. The control over the credibility requires a sound and wide experience in the business sector: only senior analysts should perform this check also to avoid the exclusion of some non-happened causes. These features (being direct, independent and credible) can be replicated also for the consequences.

Barrier failures and Threats

A further request is advanced for *Threats*: they must not be barrier failures. This is often among the top causes of a failed application of the Bow-tie method. This confusion arises from the fact that the *Top Event* happens also because the barriers fail, and the risk analyst might erroneously think that, as a consequence, it

is caused by the barrier failures. This logic is obviously wrong. A *Top Event* happens because *Threats* exist and the preventive barriers fail. This means that the *Threats* and the barrier failures are separate phenomena in the risk analysis. This distinction really matters, since defining a *Threat* as a barrier failure hides the problem. In other words, if the failure of a control measure is considered equivalent to one of the causes of the *Top Event*, then it is no more possible to detect why the barrier failed, because it is assumed that it simply happens. This way of reasoning is responsible to weak the safety improvement process at the base of every risk analysis. For example, considering a LOPC as *Top Event*, the "lack of quality control" cannot be considered as a *Threat*, as well as the "ESD failed to act": they are failed barriers. Similarly, attention should be paid also in avoiding human error as *Threats* in technical Bow-ties, since real causes can be overlooked.

Table 1: Poor and better definition of Hazards

Poor Hazard	Better Hazard
Electricity	Electrical machine at > 440 V
Storage tank	Oil in storage tank
Oil	Oil under pressure
Helicopter	Transport personnel via helicopter to/from site
Chlorine	Pressurized chlorine (10 tonnes) in storage

Table 2: Poor and better definition of Top Event

Poor Top Event	Better Top Event
Slipping	Falling from height
Overflow	Gasoline escape from tank
Helicopter crash	Loss of control of helicopter
Random rupture	Loss of primary containment
Storm	Personnel exposed to catastrophic event

2.3 Definition of Barriers

Barriers are control measures put in place to prevent or mitigate an unwanted scenario. They intervention can be considered the result of the following sequence: to detect, to decide, and to act. Depending on the subjects performing these steps, it is possible to define five barrier types.

Barrier types

Passive Hardware barriers are those always present and functioning: they neither detect, decide, or act. They simply absorb or avoid transfer of energy. Examples are dikes, fences, or containment basins. They are always in place and become useful when the control over the hazard is lost.

Active Hardware barriers rely on the performance of a technical system. All the elements of the barriers (detecting, deciding, and acting) are executed by technology. The typical example is the automatic shut-down system, where a net of sensors is used to detect anomalies, and a logic controller is used to decide if the alarm thresholds have been reached, causing an effect (closure of an ESD valve, automatic activation of a fire system, and so on). On the contrary, when the path "detect-decide-act" is fully performed thanks to human intervention, then the barrier is "Behavioral" or "Active Human". In this case, a person, or a group of people, is responsible for detecting, deciding and acting. Checklists, inspections, maintenance, and procedures in general can be considered as "Active Human" barriers. These barriers are often misused or bad-defined in a Bow-tie. The CCPS guidelines suggest that they should be defined combining an action verb and a noun (e.g. Apply seat belt). The ownership must be clear and the control measures should be traceable, i.e. linked to the management system. The definition of "Active Human" barriers requires to define the specific target. Only the effective measures can be considered barriers, and this is true also for "Active Human" barriers: they must be capable on their own of preventing an event, within the required time. Moreover, their performance should be inspected and audited: in other words, they must be measurable.

When the human intervention is combined with technology", then the barrier is "Socio-technical". It is a mix an Active Hardware barrier and an Active Human barrier. A typical example is the human intervention after an alarm in control room: detection relies on technology (the sensors provoking the alarm), but the decision to act depends on the personnel in control room. Then, the action could be "push the red button, thus closing the valve". The risk analyst has to pay attention at this step: even if the actuation of the valve is permitted thanks to technology, the activation of the system relies on the human intervention of pushing the red button. So, when assigning the Probability of Failure on Demand of this barrier, the human contribution must be

considered both in the diagnosis and action phase. Finally, there are the “Continuous Hardware” barriers. They are always-acting technology measures, like ventilation system, or cathodic corrosion protection. For them, it is not possible to assign who detects and decides. The possible barrier types are shown in Table 3.

Table 3: Barrier types

Barrier type	Detect	Decide	Act
Passive Hardware	N/A	N/A	N/A
Active Hardware	Technology	Technology	Technology
Active Human	Human	Human	Human
Hardware + Human	Technology/Human	Technology/Human	Technology/Human
Continuous Hardware	N/A	N/A	Technology

Barriers validity

A barrier in a Bow-tie is considered valid if it is:

- Fully functional (the barrier is capable to prevent the *Top Event* or to mitigate a *Consequence,* functioning as intended, when intended with a measurable effect);
- Independent (the barrier has a direct, independent impact to the *Threat, Top Event,* or *Consequence*. Independency exclude those barriers sharing common cause/mode failures);
- Auditable (the barrier can be evaluated to verify its expected performances).

Validity criteria are useful to determine if the developed Bow-tie has the minimum requirement to be properly assessed or quantified using LOPA analysis. For example:

- Fire and gas detection: it is not a valid barrier. This definition is limited to the “detection” box and needs to be improved clarifying who decides and what is the resulting action, otherwise it is not clear how this barrier should reduce the risk in a measurable way;
- Training, competency: it is not a valid barrier. It can be used to better describe another barrier, representing elements supporting it, but cannot be considered itself a barrier, remaining unclear its direct effect on the risks. Instead, a critical task may require training or competency to be performed: training and competency are part of that barrier;
- Audit: it is not a valid barrier. It is not clear what are the actions after audit has been performed;
- Emergency Shut Down: even if it is understandable, a high standard of barriers definition requires to be consistent and use a verb. For example: “deploy the ESD”.

2.4 Degradation factors and degradation controls

During a hazard identification analysis, like an HAZID, what-if, checklists, *Degradation Factors* may be discovered. They are threats for barriers, affecting their effectiveness. For example, a water firefighting system could be threatened by the interruption of the electrical energy supply, causing the pumps to stop. Another example may be a safety procedure which is impossible to carry out under certain weather condition. To protect barriers from the *Degradation Factors*, also known as escalation factors, *Degradation Controls* are put in place. They can be defined as secondary barriers, protecting the primary barriers of the Bow-tie. Back-up systems as secondary source of energy are typical examples of *Degradation Controls*, like the diesel emergency generators or the emergency pumps. Sometimes, it is natural to consider the “barrier-supporting” controls, including training, inspection and maintenance, as *Degradation Controls*. However, in order to improve the readiness of the Bow-tie models and reduce the size of the whole picture, especially when multi-level *Degradation Factors* are used (i.e. a further *Degradation Factor* for a *Degradation Control*) it is suggested to add them as label under the relevant primary barriers, showing immediately what the required activities to support them. This approach takes also into account the fact that training, inspection and maintenance are “barrier-supporting” controls, and not barrier themselves. The definition of the *Degradation Factors* follows the rule adopted for the *Threat*s. For example, if “PSV” is the primary barrier, then “no PSV” is not a clear *Degradation Factors.* A better definition could be “PSV removed for service”, and a *Degradation Control* could be “Redundant PSVs”.

3. Barrier management

Once defined the barriers in a Bow-tie model, it is fundamental to ask some key questions helping in the development of the barrier management program. First of all, it is crucial to determine the barrier condition at a specific time. It is not intended as the “inherent strength” of the barriers, nor its as-designed effectiveness (usually summed up using the FARSI - Functionality, Availability, Reliability, Survivability, Independency -

criterion). At this stage, the risk analyst considers if barriers are degraded, not in place, or working as intended. Table 4 shows some possible barrier conditions.
Once identified the barrier conditions, the risk analyst should understand if the current risk level is acceptable (or, at least, tolerable), or if more barriers are needed to make it safe to continue, planning the remedial actions and prioritizing them. The barrier management requires the knowledge of the barriers at three different levels: the element, the system and the function of each single barrier. This zoom-out on the contents is similarly proposed for the management level: from barrier management to process safety management, to risk management, to corporate governance. In such a wide scale of intervention, an integrated approach to process safety, and barrier management in particular, requires integrated tools of analysis, capable to combine and share audit data with risk analysis, incident data with risk assessment, documents with management systems, in a multi-relations database where effectiveness, corrective actions, owners, target dates, acceptance criteria, accountabilities, criticalities, types, categories, and descriptions are taken into account. Beyond the tools, it is the method supporting this approach that really counts: it is the Bow-tie method. The integrated approach also enables an easy overlapping of the Bow-tie method and the LOPA analysis, allowing to quantify the resulting diagram adding frequencies and probabilities, whose values are taken under control thanks to the multi-relations database and the integrated approach to safety.
Process safety management systems rely on four pillars: commitment to process safety, understanding hazards and risks, risk managements, and learning and improvement. It is interesting to explore the relation between these pillars and the Bow-ties. The commitment to process safety is reached when workforce and management are involved in risk analysis, sharing risk information across the pyramidal hierarchy, promoting a positive culture and facilitating an effective communication. The graphical impact of Bow-tie simplifies the understanding of hazards and risks, thanks to a proper way in describing causes, unwanted events, and final scenarios, including their paths in a logical cause-and-effect relationship. Risk management is part of the Bow-tie method, since links to performance standards and procedures to barriers are provided in the diagram, clearly showing which barrier is critical, and using whichever taxonomy, also using user-defined classes. Furthermore, the possibility to map incidents to barriers and manage corrective actions to improve safety is the point of connection between the fourth pillar and the Bow-ties.

Table 4: Barrier conditions

Condition	Description
Effective	In place, available, and effective
Partially effective	In place, available, but operating below its intended functionality
Not effective	Not in place, not available
No data	No operational information is currently available
Deactivated	Not in place, turned-off, deactivated. Optional expansion of category “Not effective”. It can be used to distinguish a local barrier from a corporate standard

4. Conclusions

Process safety discipline should help in answering several questions about process risks:

- “Do we understand what can go wrong?”
- “Do we know what our systems are to prevent this happening?”
- “Do we have information to assure us they are working effectively?”

A general consideration that lies in the background of each risk assessment method is that any protective barrier is fully reliable. This is what the well-known “Swiss cheese model” by J. Reason intends to explain. In that model, the layers of protections are represented like some swiss cheese slices, placed in sequence.
The holes represent their being not reliable at 100%: some holes are due to latent conditions, others to active failures. Generally, barriers are put in place to have not an overlapping of the holes; this ensures that, even if each barrier is not completely effective, the whole system is still safe. But under certain conditions, it may happen that the holes, i.e. the barriers weaknesses, overlap causing the actual transformation of hazards into an unwanted event. According to this approach, a barrier-based thinking can be effective in measuring and managing risks, regardless of the typology of them. Center for Chemical Process Safety (CCPS) of American Institute of Chemical Engineers (AIChE) translated this approach in the very well-known Layers Of Protection Analysis method (LOPA) (CCPS, 2011, 2013, and 2015) where barriers are identified as Independent Protection Layers (IPL) characterized each one by a probability of failure on demand. In recent years “barrier-

based management" has become a fundamental element of process risk management and barrier quality and effectiveness judgement became an important issue to deal with considering their entire lifecycle.
Barriers are the "safety measures" or "controls". Barriers interrupt the scenario so that the threats do not result in the top event when control is lost over the hazard. Barriers can also ensure that the top event does not escalate into an actual impact (the consequences). Barriers can be categorized using any classification system desired. A common classification system is if the functioning of the barrier is dependent on human behavior or technology. Categorizing barriers very often creates a greater understanding of how risks are managed. You can build on this basic barrier structure further to deepen your understanding of where the weaknesses are. Barrier categorizing your barriers as a certain type, it is also advised to include information on barrier effectiveness. After that, you can look at the activities you have to implement and maintain your barriers. This essentially means mapping your management system on the barriers. Also determining who is responsible for a barrier and assessing the criticality of a barrier are things you can do to increase your understanding of the controls that are in place for the threats posed by a specific risk. Barrier based approach is the founding principle of two specific assessment methods: Bow-tie (BT), used for risk assessment and management, and Barrier Failure Analysis (BFA), used for near-accident, near-misses and accident or unwanted events investigation.
The BT diagram is the core of the BT method and one of the most used diagrams within barrier-based management. With the BT diagram you can visualize a risk scenario that would be very difficult to explain otherwise. A BT is a diagram that visualizes the risk you are dealing with in just one, easy to understand the picture. The diagram is shaped like a "bow-tie", creating a clear differentiation between proactive and reactive risk management. The BT method was first used in the oil & gas industry (BT is referenced in ISO 17776 standard), and later in other industries such as maritime, aviation, mining, chemicals, etc. The initial application of BTs was to create a visual risk assessment, often in the context of a 'safety case' (license to operate). Article presents the work done (almost completed) by AIChE CCPS to promote a guideline for the use of BT in process safety (Project 237). Guidelines intend to review the foundation of the method, provide instructions on how to draw the BT diagram correctly and how to avoid common errors. Some specific issues are covered: typical constructs for typical process threats – corrosion, impact, improper operation / human error, operational upsets, etc. would be demonstrated. The risk management information associated with every barrier has been explained, e.g. barrier owner, performance expectation, pending actions, related documents. The pay-off is tremendous: risk assessments come to life. Instead of being forgotten and archived, risk assessments are actually used because they are relevant in "day-to-day" operations. Furthermore, the aggregation of various data sources allows a level of understanding and insight into risks, which is unprecedented in risk management until now. In particular BT becomes a significant improvement to existing LOPA assessments. It incorporates human factor and process safety management system link described in four pillars (commitment, understanding, management, learning).

References

Bruce K. Vaughen, P.E., Kenneth Bloch. Use the Bow Tie Diagram to Help Reduce Process Safety Risks. CEP Magazine (An AIChE Publication); 2016.
CCPS. Guidelines for enabling conditions and conditional modifiers in layers of protection analysis. Wiley; 2013.
CCPS. Guidelines for initiating events and independent protection layers in layer of protection analysis. Wiley; 2015.
CCPS. Layer of Protection Analysis: Simplified Process Risk Assessment. New York: Wiley; 2011.
CCPS. Process Safety Glossary: Bow Tie Diagram. Available online at www.aiche.org/ccps/resources/glossary/process-safety-glossary/bow-tie-diagram; last access on April, 30th 2018.
CCPS. Project 237: Guidelines for Barrier Risk Management (Bow Tie Analysis), 2017 (in progress).
ISO 17776:2016. Petroleum and natural gas industries – Offshore production installations – Major accident hazard management during the design of new installations; 2016.
IEC 31010:2009. Risk management – Risk assessment techniques; 2009.
ISO 31000:2018. Risk management – Guidelines; 2018.
Luca Fiorentini, Luca Marmo. Principles of Forensic Engineering Applied to Industrial Accidents.
Wiley, Chichester UK; 2017.
Luca Marmo, Norberto Piccinini, Luca Fiorentini. Missing safety measures led to the jet fire and seven deaths at a steel plant in Turin. Dynamics and lessons learned. Journal of Loss Prevention in the Process Industries 26(1), pp. 215-224; 2013.
Luca Marmo, Norberto Piccinini, Luca Fiorentini .The Thyssen Krupp accident in Torino: Investigation methods, accident dynamics and lesson learned. Chemical Engineering Transactions 26, pp. 615-620; 2012.