Bow Tie Analysis

Albert C vd Vyver

A risk control effectiveness evaluation technique for managers

SheRisk - Business partner of: CGE Risk Management Solutions Making risk understandable

SheRisk Director: AC vd Vyver Mobile Contact 0798722978 E-MAIL: sherisk@telkomsa.net

Table of Contents

1 Strategic Context and Scope of the Technique

Introduction

Bow Tie Analysis (BTA) was developed during the early 1970s and has since developed into a well-defined threat control evaluation and management tool. Many a manager and risk specialist has seen this tool as either a risk assessment tool or a risk identification technique. In either case it is the wrong impression created by implementation pitfalls. Bow Tie Analysis is a risk management technique that was developed from the traditional fault tree analysis and event tree analysis, both with the same objective: making the right decisions through either qualitative or quantitative analysis.

Taking this technique back into the risk management framework to establish the correct application is fundamental to the process. Risk management is about coordinating activities and directing related controls concerning identified risks. Managing risk involves fundamental decisions based on sound risk evaluation, analysis and good corporate governance principles, which in turn produce the company's risk appetite.

Currently we have a vast amount of risk identification and analysis techniques that are used and misused interchangeably in the industry. The leading drawback comes with unifying the risk assessment and analysis practices to suit our own biased and prejudicial judgement, not following the tangible objectives of each of these techniques heralded in ISO 31010.

In *The Six Mistakes Executives Make in Risk Management,* Nassim N. Taleb, Danile G. Goldstein, and Mark W. Sptznagel identify six assumptions that are problematic in the risk management context:

- We think we can manage risk by predicting extreme events.
- We are convinced that studying the past will help us manage risk.
- We don't listen to advice about what we shouldn't do.
- We assume that risk can be measured by standard deviation.
- We don't appreciate that what's mathematically equivalent isn't psychologically so.
- We are taught that efficiency and maximizing shareholders value don't tolerate redundancy.

The authors explain that *"recommendations of the "don't" kind are usually more robust than "dos". For instance, telling someone not to smoke outweighs any other health-related advice you can provide. 'The harmful effects of smoking are roughly equivalent to the combined good ones of every medical intervention developed since World War II. Getting rid of smoking provides more benefit than being able to cure people of every possible type of cancer,' points out genetics researcher Druin Burch in* Taking the Medicine*.*

In the same vein, had banks in the U.S. heeded the advice not to accumulate large exposures to low-probability, high-impact events, they wouldn't be nearly insolvent today, although they would have made lower profits in the past.

Psychologists distinguish between acts of commission and those of omission. Although their impact is the same in economic terms, a dollar not lost is a dollar earned. Risk managers don't treat them equally. They place a greater emphasis on earning profits than they do on avoiding losses. However, a company can be successful by preventing losses while its rivals go bust and it can then take market share from them" (Taleb, Goldstein & Sptznagel)

An important aspect to deal with would be the context and objectives of relevant risk management techniques used widely in the industry. Consider that risk identification techniques has been developed over years and most of them during the early 1960s, all with the objective to minimize losses in respect of profitability and safety. This has changed during

the past decade where the emphasis shifted to control management.

In addition to the impact of changing objectives, the application of these techniques was applied to suit the partiality of the risk specialists, not the intended outcome. This has led to alternative techniques not suited to risk management objectives. Examples are the current misuse of Hazard and Operability Studies and Bow Tie Analysis. Other forms of risk identification were changed and branded with new names not mentioned in any risk management doctrines.

All of this calls for a formal approach concerning the “return to fundamental principles”. We have to acknowledge that risk management is not accident investigation and that accident investigation does not stop or prevent accidents. It is the management of risk that contract the anticipation, deterrence, prevention and mitigation of the impact of unacceptable risk. The latter entails taking risks on calculative pre-set criteria aligned with the risk appetite of the company.

The aforementioned convey the question as to where risk identification resides and where does risk analysis reside within the risk managing methodologies. The primary objective of this module is to establish the context in which Bow Tie Analysis is done and where it fits into the total risk management framework. Many companies have a formal risk management policy dealing with risk, qualitatively or quantitatively, at different levels of management. Some work from a corporate enterprise risk management system to a middle management level to a worker involvement level, and several work on a three tier process while others work on a four-tier process. The number of tiers does not brand it more effective. In reality, as will be shown in this module, its effectiveness is complementary to the interaction between the layers (tiers), regardless of the number, and the flow of information and risk based knowledge.

Lost between the tiered approach and risk assessment techniques are the subjects of “Behaviour” or “Human Error”. Both are characteristics of purely accident investigation jargon, developed from an old reactive era. As terms that are simultaneously illusive and official sounding, they are often the “scape goats” for all accidents purely due to the popularity of their use and reiteration in accident investigation reports. Their continued popularity among risk managers shows an outdated single-mindedness that should not be part of the Bow Tie Analysis, unless the focus changes to activity Bow Ties.

Similarly, one can ask where do “ill-discipline”, “poor supervision” and “lack of training or skills” fit into the risk management world. These control failures has swamped our rationale and has blindfolded us in the proper execution of the Bow Tie Analysis technique.

Framework of the Bow Tie Analysis

In layman’s terms, we conduct a baseline risk assessment using some form of risk identification technique, followed by a next set of risk assessment techniques called issue based risk assessments, task specific risk assessments and then individual risk assessments. Somewhere in-between is the project and change management risk assessment. This is a good system that is well thought through, and it does provide a structured format of managing risk; however, something is missing. The link between these activities and the way they affect each other is the essence of effective risk management.

With the aforementioned the objective is the identification of risk and positioning controls into place. Subjectively we change the risk evaluation numbers from a risk matrix to prove that the controls are effective enough to carry on with the work. This is apparent in the double evaluation practices we see in the industry. “Raw” risks are evaluated and then a final risk score developed from our perception of the effectiveness of the controls. No set criteria is used, just the perception of the risk assessment team members, which in most cases are the persons available rather than the most knowledgeable persons on the subject.

To some extent the subjectivity in risk management practices show that we still have an issue with “group think” during the analysis phase. Bow Tie Analysis was brought into the picture to solve this problem of subjectivity and knowledge. This is possible because Bow Tie Analysis relies on a set of acceptance criteria built into the system that the dominant parties cannot overrule.

We will set the terminology during this module, and, for the sake of understanding, we will base decisions on set rules during the Bow Tie Analysis, and not on the perception of biased individual opinions. It will be essential that the required criteria have been set before any risk analysis technique is used. In the case of the Bow Tie Analysis, it will be built into the software and will command proper thinking and evaluation undertakings.

Consider the following hitherto typical scenario in a risk assessment context: following a risk identification technique, a selection of “high” risk is identified. What do we do with them? How do we prove that the controls used during the evaluation or the suggested improvements will be effective to manage the risk? Where does “as low as reasonably practicable” fit into all of this? We have been doing risk assessments for the past few decades and will continue doing so for the next few decades. Only if it is to satisfy legislation, have we done what the regulator has asked us to do.

Take for instance if I have done all the risk assessments mentioned in paragraph one, still an accident happens. Guess what is the recommendation? Re-do the risk assessment and develop more procedures. This has been going on for many years in our industry, without anyone noticing we are chasing our own tails. The situation is not due to a lack of improved risk management techniques, but simply because most risk professionals have not been willing to make the necessary changes and incorporate the improved techniques that are at their exposal.

Bow Tie Analysis is also not a new technique; it was merely the objective that was ignored. This is one of the few techniques on the analysis side of risk management that was never in use, and was never regarded as a “factual” way of scrutinising the effectiveness of controls. Since its implementation we have started to recognise the chief advantage it provides for control and critical control management.

The industry will have to make this paradigm shift into managing controls instead of preventing accidents. Major modifications in thinking, which few risk professionals currently feel comfortable with, need to be implemented to prevent industry from getting stuck in investigation mode. Baseline and issue based risk assessments has become a traditional setting of history, very few has revealed any other than the norm. The so-called high risks have remained the same over decades, and only changed at irregular intervals to suit the flavour fictitiously affected by accidents within the industry. Simply put, what happened gets recorded, and the industry relies to a great extent on recorded events to determine what should be deemed “high risks”. Bow Tie, on the other hand, lends itself to scenario setting and has provided numerous new “events” never recorded before, revealing a suite of absent or misplaced controls in our structure.

This raises the next question, where does the Bow Tie Analysis actually fit into the layers or tiers of risk management? Following a baseline risk assessment, issue based risk assessment, project risk assessment or change management risk assessment, some risks are still produced which gives the impression that the controls cannot mitigate or deal with the consequences. This is where the Bow Tie Analysis should intervene and provide the necessary results. Hence, understanding the framework in which this is done becomes critical to the effectiveness of the outcome.

Terminology changes and one has to become attentive to the different language and philosophy. It is not risk assessment, it is not investigation and not problem solving. For the latter, we cannot use Bow Tie Analysis to weigh one risk against another, nor force a decision that one control is more effective than another. It is more about a suite of controls, managed according to pre-determined criteria that make the risk acceptable. It cannot "take away" risk, and we would not want it to as we use risk to do our work – a point that will be explained in section two.

Thus, risk identification produces a set of risks evaluated from a matrix to set priorities for the management of the risk. The "way" to manage these same risks comes from the Bow Tie Analysis. In more detail, which will be discussed later, one can accept that the Bow Tie Analysis will provide the specific suit of controls to manage a specific risk, produce those controls that is critical to the management of systems and physical activities or the monitoring thereof. How do we achieve this?

- Before any Bow Tie Analysis we have to conduct a risk assessment.
- Before any Bow Tie Analysis we have to set the rules and acceptance criteria, which involves the following:
  - Risk appetite of the company,
  - Hierarchy of control criteria,
  - Preventive control acceptance criteria,
  - Mitigating control acceptance criteria,
  - Control effectiveness criteria,
  - Escalating factor control acceptance criteria,
  - Authoritative persons responsible to manage controls,
  - Control framework (layers of controls),
  - Level of competence to management controls,
  - Critical control selection criteria and selection process,
  - Monitoring control criteria,
  - Risk assessment matrix criteria for each risk category,
  - Basic risk factor criteria for control selection,
  - Document link criteria,
  - Auditing criteria questions for control effectiveness management,
  - Level of monitoring criteria, and
  - Activity criteria to allocate activities supporting controls
- Competent persons have to be involved.

Each of the terms listed above will be discussed in detail during the next module. By following the guidelines we will cultivate a decision framework vested with the expertise, capability, ownership, responsibility and authority for risk analysis.

The Bow Tie Analysis outcome will set the "strategies" for the next and lower layer (tier) of risk management.

- Critical controls will be identified, which can be linked to specific activities and tasks.
- Critical control management will be allocated to task related risk assessments.
- Critical controls will be made specific to physical or conditional inspection regimes and individual risk assessments.
- Critical controls will be made available to system control management and auditing protocols for leading indicators.
- Trigger action control points will be identified to produce trigger action response plans.
- Trigger action response plans (TARP) will be used for specific critical control training.
- Critical control dashboards can be developed, identified at lower echelons and managed from a higher tier in risk management.
- Control strategies become dynamic.

1 Three Simple Questions

Answering 3 simple questions:

- “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?”

Where do these questions come from?

The Buncefield Incident occurred on 11 December 2005 at the Hertfordshire Oil Storage Terminal, an oil storage facility located near the M1 motorway by Hemel Hempstead in Hertfordshire, England. The terminal was the fifth largest oil-products storage depot in the United Kingdom, with a capacity of about 60,000,000 gallons of fuel. A simple tank overfill event that escalated into catastrophic explosion and fire, causing significant damage to the terminal and surrounding business and residential neighbours.

The UK Health and Safety Executive (HSE) prosecuted the 5 operators of the terminal. At the end of the trial in June 2010, Gordon MacDonald, the then Director of Hazardous Installations Directorate (HID) for HSE, issued a challenge to high hazard industries on behalf of all the United Kingdom Competent Authorities to answer the above mentioned three questions from the boardroom down: 1) 'Do we understand what can go wrong?', 2) 'Do we know what system are in place to prevent this happening?' and 3) 'Do we have assurance that these systems will work?'

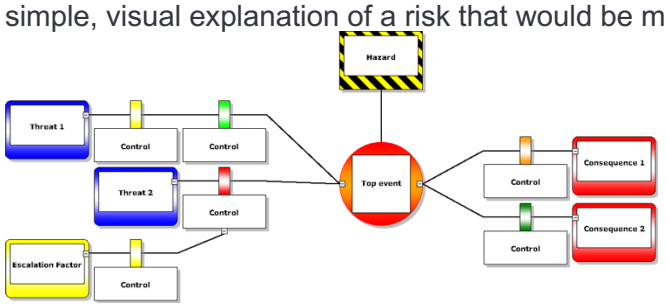
The challenge that HSE gave to the UK High Hazard Industry is applicable across the globe as these questions strip down the complex subject of process safety into a simple concept that is easy to understand. An organisation can test itself internally, can it answer these three questions in structured and clear way?

The challenge is to answer all three questions at the same time.

These questions are not limited to thinking about people and the environment but can equally be applied to commercial risk management too.

2 The Bowtie Method

A BowTie is a diagram that visualises the risk you are dealing with in just one, easy to understand picture. The diagram is shaped like a bow-tie, creating a clear differentiation between proactive and reactive risk management. The power of a BowTieXP diagram is that it gives you an overview of multiple plausible scenarios, in a single picture. In short, it provides a simple, visual explanation of a risk that would be much more difficult to explain otherwise.



Hazard

The word “hazard” suggests that it is unwanted, but in fact it is the opposite: it is exactly what a business wants or even needs to succeed. Hazards are similar to the negative side of a “risk source”. Although this course will focus mainly on the negative influences of a risk source we should be able to use any risk source as a starting point for a Bow Tie Anlaysis.

It is an entity with the **potential** to cause harm – but without it there is no business. An example is driving a car on the highway. We need to get to wherever we are going, but driving cars can be dangerous. Or oil is a dangerous substance – it can cause a lot of harm when treated without care. At the same time, it is the one thing that keeps the oil industry in business. It needs to be managed because as long as it is under control, it is of no harm.

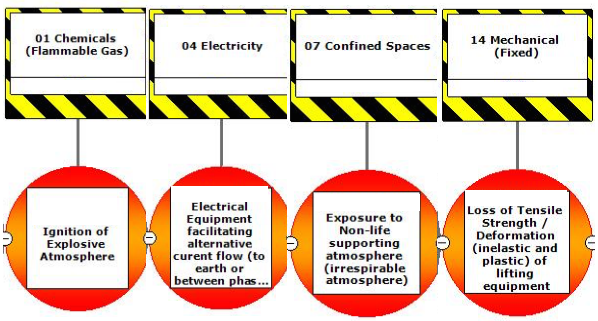
Hazards may also be seen as a source of risk deriving from the use of an energy source during business activities or functions. It continues to be similar to environmental aspects. In fact, anything that has the potential to cause a negative impact on business objectives can be considered a hazard.

Although enterprise risk management also focuses on opportunities the description of a hazard is negative and will not include the positive influence on business objectives. It may however be an outcome of a Bow Tie Analysis. It does not keep us from conducting a Bow Tie Analysis to evaluate the effectiveness of controls dealing with opportunities. At least one should be able to turn threats into opportunities and benefit from it. We should manage this method with caution and not dilute our approach to avoid losses.

Top event

It follows that as long as a hazard is controlled it is in its wanted state, for example: oil in a pipe on its way to underground workings or from the storage facility to the delivery system. But certain events can cause the hazard to be released. In bow tie methodology such an event is called the top event. The top event is not a catastrophe yet, but the dangerous characteristics of the hazard are now in the open. An example of this would be if the oil is outside of the pipeline (loss of containment). This in itself is not a major disaster, but if not mitigated correctly it can result in more unwanted events (consequences).

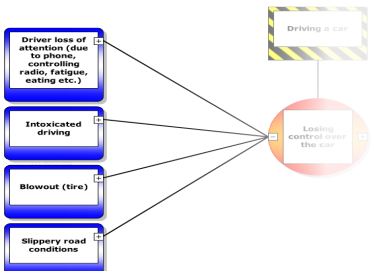
We can also use an energy release timeline to determine the top event. Draw a line from the hazard to the unwanted event, normally the fixtures in the event timeline. Fill in-between how the energy is released, transferred, transformed, changed in magnitude, released, etc. The top event is the release mechanism at the stage before you reach the “point of non-return”.



Threats

Often there are several factors that could cause the top event. In bow tie methodology these are called threats. These threats need to be sufficient or necessary: every threat itself should have the ability to cause the top event. For example, corrosion of the pipeline can lead to the loss of containment.

Threats cannot represent a control failure, such as the failure to comply with lockout. Threats are tangible and non-tangible causes and will directly lead to the top event. In few instances it might combine with other threats to produce the top event. An event such as Fires and explosions, as an example, will have combined threats before the top events become evident.



Consequences

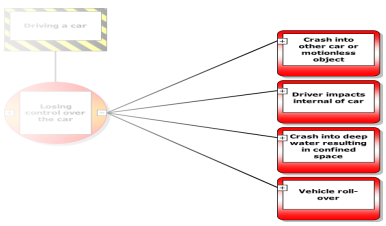
When a top event has occurred it can lead to certain consequences. A consequence is a potential event resulting from the release of the hazard, which results directly in loss or damage. Consequences in bow tie methodology are unwanted events that an organisation wants to avoid by all means, for example: oil leaking into the environment.

Consequences provide the opportunity for scenario setting; one will become responsive to this during the execution and evaluation of control effectiveness, where “generic” controls are used instead of the scenario specific controls required. A complex risk will force this way of thinking. As an example, one may have a Code of Practice for emergency response, but it deals with the general recovery of a person from a vehicle once an accident has occurred. It will however lack the specific control to release or demobilise the airbags before starting to cut the vehicle to recover the person.

The effectiveness of controls should be determined in the context of a specific scenario, and not in general. For that reason it would be fundamental to the process to be specific in the description of these consequences.

The picture so far

At this stage we have a clear understanding of the risk and what needs to be controlled. The Hazard, Top Event, Threats and Consequences give us an overview about everything we don’t want around a certain Hazard. Every line through the Bowtie represents a different potential incident. Besides containing incident scenarios that might already have occurred, part of the strength of the Bowtie is that there is also room for scenarios that have not occurred yet. This makes it a very proactive approach.



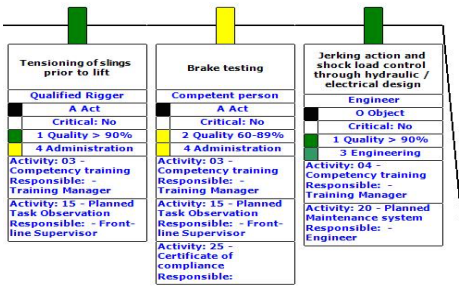
Barriers: controlling unwanted scenarios

Risk management is about controlling risks. Placing barriers to prevent certain events form happing makes this possible. A barrier (or control) can be any measure taken that acts against some undesirable force or intention, in order to maintain a desired state.

In bow tie methodology there are proactive barriers (on the left side of the top event) that prevent the top event from happening, for example: regular corrosion-inspections of the pipelines. There are also reactive barriers (on the right side of the top event) that prevent the top event resulting into unwanted consequences. An example of a reactive barrier is leak detection equipment or a concrete floor around the oil tank platform.

We should, however, pay attention to the control framework or explore the opportunity of improvement of these controls when populating these controls. The control framework will be explained during the next module.

Note the terms “barrier” and “control” are the same construct and depending on industry and company, one or the other is used. In this manual we will use the term barrier.



Escalation factors & Escalation factor barriers

In an ideal situation a barrier will stop a threat from causing the top event. However, many barriers are not 100% effective. There are certain conditions that can make a barrier fail. In bow tie methodology these are called escalation factors.

An escalation factor is a condition that leads to increased risk by defeating or reducing the effectiveness of a barrier, for example: an earthquake leading to cracks in the concrete floor around a pipeline.

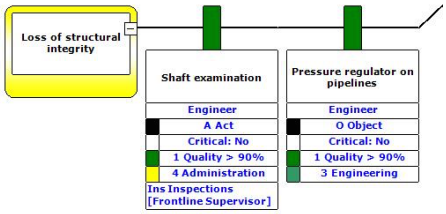
Escalation factors are also known as defeating factors or barrier decay mechanisms – which term is used is dependent on industry and company. In this document we will use the term escalation factor.

We should, however, be careful as not to take “control failure” or “human error” as escalating factors. The reason why the control is ineffective cannot be an escalating factor if it can be removed by an action. This means that the effectiveness can improve or the aspect resulting into the ineffective control be removed by implementing systems. Escalating factors should stay in a bow tie, and cannot be removed unless illuminated by retrieving the threat. For that reason we develop controls to manage these escalating factors and in most cases will be known as mitigating the impact of escalating factors.

An example would be a rain event for open pit mining operations linked to the control of fail-safe breaks which do not take into account skidding on wet surfaces. One may have the best braking system yet on the type of material used to build the road surface and wet conditions, the controls become ineffective. For that reason we will provide for additional controls dealing

with this escalation factor.

Escalating factors are among the strong points of a bow tie and provide chief opportunities for dealing with factors outside our normal control, mainly natural perils, pre-conditions to the threats and post consequences.



Warning: be careful with escalation factors. You do not describe all the potential failure modes. Only describe the real weaknesses of your control framework and how you want to manage that. These factors are classified into four major categories that will be described later. A key principle would be that you list only those factors that will remain permanently in the Bow-Tie. Meaning that it cannot be removed by a logic action of improvement.

Critical Controls

Critical controls are those which if compromised will lead to the development of the top event or significantly increase the consequences and will include:

- Those controls that if compromised to any extent will render all other controls in the same pathway or multiple pathways ineffective realising the top event.
- Those controls that independently will prevent the top event to realise, even on failure of other controls in the same or multiple pathways.

Example for the selection process of Critical Controls

Step 1: Complete the full BTA without any reference to Critical Controls.
Step 2: Identify High Contributor Threats.

- Threats directly leading to the top event without any consideration of controls in the same pathway.
- It will have a “daily” frequency of exposure:
  - No consideration of past incident history.
  - Under normal operating conditions.
  - Exposure to the Threat, not exposure to the top event or consequence.
- Significance / Dominance in relationship to other Threats.

Step 3: Identify Vulnerable Pathways.

- Apply the acceptance criteria for each Threat and Consequence.

Step 4: Identify Critical Controls

- Pathways identified as being both High Contributors and Vulnerable will have at least one Critical Control.
- All high contributor pathways will have at least one Critical Control.
- All Vulnerable pathways should be considered for Critical Control selection.
- Engineering and higher order controls will ideally be considered to be selected as Critical Controls. However, engineering controls that have an automated monitoring system will be selected as a Critical Control.
- Administrative controls that appear on multiple pathways will be considered as Critical Controls.
- Controls, backed by other layers of protection, which independently manage the release of the

Threat will be considered as Critical Controls.

- Controls closest to the mechanism of release should be considered as a Critical Controls.
- Controls that prevent or mitigate the risk source, alone or in combination, has the intrinsic potential to give decline to the consequence should be considered as Critical Controls.
- Filter controls with caution to the following:
  - Controls dealing with more than one hazard
  - Controls directed at sub / secondary consequences
  - Controls subordinate to escalating factor controls:
    - Rather pinpoint the escalating factor control,
    - Start with one per pathway.
  - Allow the selection of one Critical Control per pathway.
  - Challenge threat control versus mechanism of release control – discard those not directly contributing towards the energy flow line.
  - Re-Visit Hazard Inventory for Major Hazard and ensure it is updated and aligned with the BTA results:
    - Have the release mechanisms all been part of the Critical Controls?
    - Have the uncertainties been covered by the Critical Controls?
    - Have the risk source (pre-condition of the Threat) been addressed?

3 The history of Bowtie

The Bowtie method is a risk evaluation method that can be used to analyse and demonstrate causal relationships in high-risk scenarios. The method takes its name from the shape of the diagram that you create, which looks like a men's bowtie. A Bowtie diagram does two things. First of all, a Bowtie gives a visual summary of all plausible accident scenarios that could exist around a certain Hazard. Second, by identifying control measures the Bowtie displays what a company does to control those scenarios.

However, this is just the beginning. Once the control measures are identified, the Bowtie method takes it one step further and identifies the ways in which control measures fail. These factors or conditions are called Escalation factors. There are possible control measures for Escalation factors as well, which is why there is also a special type of control called an Escalation factor control, which has an indirect but crucial effect on the main Hazard. By visualising the interaction between Controls and their Escalation factors one can see how the overall system weakens when Controls have Escalation factors.

Besides the basic Bowtie diagram, management systems should also be considered and integrated with the Bowtie to give an overview of what activities keep a Control working and who is responsible for a Control. Integrating the management system in a Bowtie demonstrates how a company manages Hazards. The Bowtie can also be used effectively to assure that Hazards are managed to an acceptable level (ALARP)

By combining the strengths of several safety techniques and the contribution of human and organisational factors, Bowtie diagrams facilitate workforce understanding of Hazard management and their own role in it. It is a method that can be understood by all layers of the organisation due to its highly visual and intuitive nature, while it also provides new insights to the Risk professional.

It is said that the first 'real' Bowtie diagrams appeared in the (Imperial Chemistry Industry) course notes of a lecture on HAZAN (Hazard Analysis) given at The University of Queensland, Australia (in 1979), but how and when the method found its exact origin is not completely clear.

The catastrophic incident on the Piper Alpha platform in 1988 awoke the oil & gas industry. After the report of Lord Cullen, who concluded that there was far too little understanding of Hazards and their accompanying risks that are part of operations, the urge rose to gain more insight in the causality of seemingly independent events and conditions and to develop a systematic/systemic way of assuring control over these Hazards.
In the early nineties the Royal Dutch / Shell Group adopted the Bowtie method as company standard for analysing and managing risks. Shell facilitated extensive research in the application of the Bowtie method and developed a strict rule set for the definition of all parts, based on their ideas of best practice. The primary motivation of Shell was the necessity of assurance that appropriate risk controls are consistently in place throughout all worldwide operations.

Following Shell, the Bowtie method rapidly gained support throughout the industry, as Bowtie diagrams appeared to be a suitable visual tool to keep overview of risk management practices, rather than replacing any of the commonly used systems.

In the last decade the Bowtie method also spread outside of the oil & gas industry to include aviation, mining, maritime, chemical and health care to name a few.

Methodological parents of Bowtie

While the origin of the Bowtie method itself is unclear, there were other methods which were either at the root of Bowtie thinking, or which came later but can be used to explain the type of thinking. So we do have some idea about what logically preceded the Bowtie.

As already mentioned, there are two things that the Bowtie does. First, the Bowtie analyses chains of events, or possible accident scenarios. The way it does that was inspired by three different methods. The first method is the fault tree, which covers the left side of the Bowtie in a different form. Second, the event tree that can be seen on the right side of the Bowtie, but also in a different form than the original event tree. Lastly, causal factors charting, which is most likely the origin of Escalation factors. The following pages will be used to explain exactly what the differences are between the original methods and how the Bowtie uses them.

The second thing the Bowtie does is to identify control measures that an organisation has in place. This type of thinking is more easily explained with the famous Swiss Cheese model by James Reason, which originated in the early nineties.

Fault tree analysis

The fault tree method was created in 1962 and quickly became popular in the nuclear and aviation industry. A fault tree uses Boolean AND/OR gates to model causal relationships between events (the method is mostly used to model the causality of unwanted events, but it is possible to model any kind of causal relationship). The original fault tree was often quantified with failure probabilities, and calculate derived probabilities.

The left side of the Bowtie diagram consists of a simplified Fault Tree.

Although the Boolean logic gates in Fault Tree Analysis allow the model to be filled with actual numbers about failure probabilities, and calculate derived probabilities, this information is seldom available due to the costs of testing and human influence on the system.

To prevent the focus of the analysis to be diluted by this level of detail, the Bowtie method simplifies the fault trees by removing this possibility, leading to overall better readability of the analysis.

One of the most distinctive Bowtie method items is the Escalation Factor which is used to identify and demonstrate the weaknesses in Controls and hence the system as a whole. These potential failure modes are neglected in Fault Tree Analysis.

Fault trees paint a very detailed picture, which is a strength or a weakness depending on the goal and context of an analysis. If the goal is to exhaustively analyse all possible interactions between forces in an organisation, the fault tree will do that.

Positive:
- High level of detail
- Theoretically possible to quantify

Negative:
- Hard to communicate
- In practice hard to reliably quantify

Event tree analysis

The right side of a Bowtie diagram resembles an Event Tree. However the Bowtie method is not looking for probability or frequency information but rather aiming at how to make sure that the controls ARE working properly and asking the question: “Are we doing enough or should we implement more safety measures?”

The Bowtie method is most often used for the analysis Major Hazard Scenarios in which the consequence spectrum is so bad that the keeping control over these Hazards is of major importance, regardless of the actual probability of the consequences. Fortunately there is little accurate information available about the frequency of these worst-case-scenario consequences.

Causal factors charting

In the Bowtie method causality mapping (similar as in Causal Factors Charting) is found in the relationship between Threats and the Top Event and the Top Event and its Consequences.

Another causal path in a Bowtie diagram is between a Control and its Escalation Factor(s).

Causal Factors Charting is mainly used for the analysis of incidents whereas the Bowtie method is more appropriate for proactive risk analysis / process hazard analysis. The Bowtie method does not look at one causal factors chain but to all possible causal paths that are associated with a certain Hazard.

Control thinking

In 1990 psychologist James T. Reason proposed the Swiss Cheese metaphor as an accident causation model. Reason hypothesized that hazards are prevented from causing losses by a series of controls, known as controls in the bowtie method.

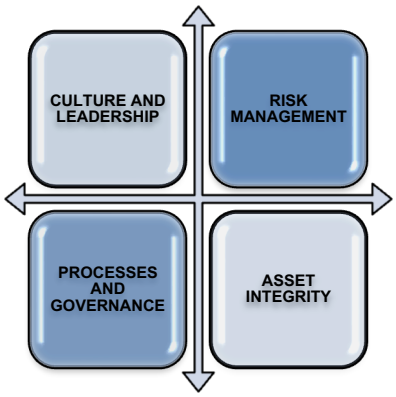
He states that these controls however are never 100% effective. Each control has unintended (inconstant) weaknesses and when these so called ‘holes’ line up a hazard can be released.

According to Reason the common causes of the weaknesses in controls can often be found in the organisation (latent failures). E.g. cost & time cutting on maintenance management can eventually lead to the deterioration of the integrity of many hardware controls within a system. In the Bowtie method these weaknesses are defined as Escalation Factors and are important features to fight the illusion of control that organisations sometime tend to have.

4 The Risk Management Context

Risk Assessments are used in many different industries, of which Oil & Gas is a clear example. But also in industries like Mining, Natural Resources, Transport, Energy, Chemicals, Healthcare, IT, Pharmaceuticals, Production, Aviation, Financial Institutions and Commercial Business assessing risks and managing risks are practiced on a daily basis.

What is not so clear, is how risk assessments and risk management interact with the Control Framework, Culture, Processes, Governance and the basic design/set-up of assets and/or processes. We believe that these areas are strongly interconnected and that on a basic level this interaction is applicable for any given industry. And we believe that a 'qualitative' method of assessing risk improves the insight and quality of any operation. Some risks simply cannot be calculated and dealt with 'in itself', but are very important to be assessed, communicated and dealt with in the overall context of Threats, Risks, Controls and possible Consequences. Whether the core business process is drilling for oil, treating patients, running an airline business or managing financial processes.



In the field of Assurance, Quality, Health, Safety and Environment, some of our clients have 12 focus areas, some clients 8. Being consultants by nature, we like the 2x2 representation of what most of our partners and clients deal with on a daily basis; see the illustration on the left. This 'risk management context' gives a comprehensive overview and context of the competencies of our partners – as well as the software solutions we represent in the areas of Risk Management (Risk Assessment, Incident Management, Incident Analysis) and Processes and Governance (Enterprise Risk Management, Compliance, Assurance).

We focus on providing software solutions for Risk Management and Processes and Governance. Our partners deliver the services that are required to make our solutions work for our clients. We restrict ourselves to a limited number of business development projects with industry leaders, in order to test new concepts and techniques. We do not deliver solutions for Asset Integrity and Culture & Leadership.

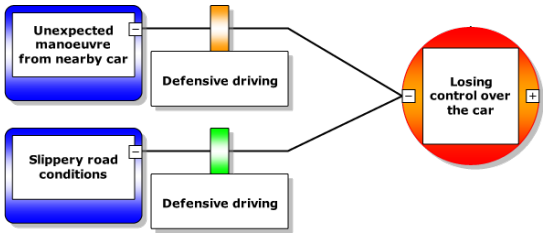
Being 'qualitative' risk management experts with a background in psychology we are pleased to inform our prospects and clients to ask advice from some of our partners on this.

5 Barrier effectiveness

Barriers are not created equal. Some are better than others. Barrier effectiveness is a way to assess how well a barrier performs. Effectiveness is often used as a single property of a Barrier. However, in this article we'll break effectiveness down into two main elements. Adequacy and reliability.

Adequacy

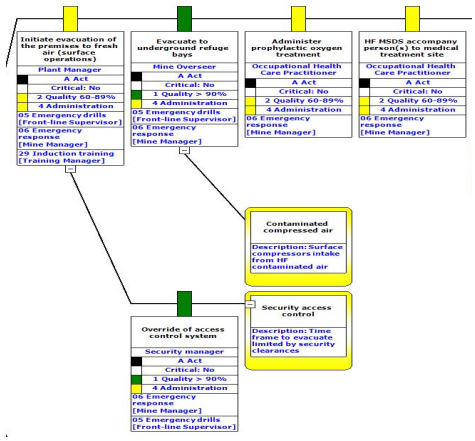
If you look at defensive driving as a barrier, it actually features on multiple Threats. However, defensive driving is not equally effective for those Threats. That's because the adequacy is different. Adequacy tells you to what extent a properly functioning Barrier will interrupt a particular scenario. It's important to understand that adequacy is not an absolute measure. The adequacy of a barrier can be different depending on the scenario that it is controlling. This is also the main reason why you shouldn't copy paste Barriers with an effectiveness rating. It could be that the effectiveness is different, because the adequacy is different.



Reliability

Having a perfectly adequate barrier is not enough, it needs to actually work when needed. That's what reliability is about. Will my barrier do what it's supposed to do, when I need it? Assessing the reliability is done by looking at the Escalation factors (although not all Escalation factors necessarily impact the reliability), incidents in which the barrier failed or was missing, audit results and other sources.

For example, under release of hydrofluoric acid the barrier "Evacuation to refuge chambers" has an Escalation factor, which reduces the reliability, so we need to adjust the effectiveness because the fresh air used to ventilate the refuge chamber will be contaminated with the same toxic gas from the intake of the compressors (indicated by the yellow colour).



6 Barrier Types

One of the lesser-used functionalities in BowTieXP is Barrier type. These allow you to categorise barriers and assess the mix of different types of barriers. Generally, having different types of barriers is good for two reasons.

- Different barrier types decrease the chance of common mode failure.
- Different barrier types can compensate for each other's weaknesses.

There are different categorisations possible, but they generally describe either barrier functions or barrier systems.

Barrier function

A barrier function is a function planned to prevent, control, or mitigate undesired events or accidents´.

This definition by Sklet gives a good summary of barrier function. Instead of describing what is there in an organisation, the barrier function should describe why it's there. One of the first systems to describe the differences in barrier function was developed in the early 70's. Haddon described 10 strategies for countering energy damage of any form in a classic article. This was one of the first categorizations of barrier functions and it would have a lot of influence on later categorizations. The ten strategies (taken from the original article) are:

- The first strategy is to prevent the marshalling of the form of energy in the first place
- The second strategy is to reduce the amount of energy marshalled
- The third strategy is to prevent the release of the energy
- The fourth strategy is to modify the rate of spatial distribution of release of the energy from its source
- The fifth strategy is to separate, in space or time, the energy being released from the susceptible structure, whether living or inanimate
- The very important sixth strategy uses not separation in time and space but separation by interposition of a material 'barrier'
- The seventh strategy, into which the sixth blends, is also very important - to modify appropriately the contact surface, subsurface, or basic structure, as in eliminating, rounding, and softening corners, edges, and points with which people can, and therefore sooner or later do, come in contact.
- The eighth strategy in reducing losses in people and property is to strengthen the structure, living or non-living that might otherwise be damaged by the entry transfer.
- The ninth strategy in loss reduction applies to the damage not prevented by measures under the eight preceding - to move rapidly in detection and evaluation of damage that has occurred or is occurring, and to counter its continuation and extension.
- The tenth strategy encompasses all the measures between the emergency period following the damaging energy exchange and the final stabilization of the process after appropriate intermediate and long-term reparative and rehabilitative measures.

Later systems tried to describe barrier functions on a higher level. Prevent, control and mitigate/protect are the three high-level barrier functions that in some form or another, ended up in most classification systems. It is important to understand that all of these functions are relative to the progression of an incident. A barrier (such as a wall) might have a preventive function in one incident, while it has a mitigation function in another incident. Barrier functions are not an absolute property of any barrier, but describe a relationship within an incident sequence.

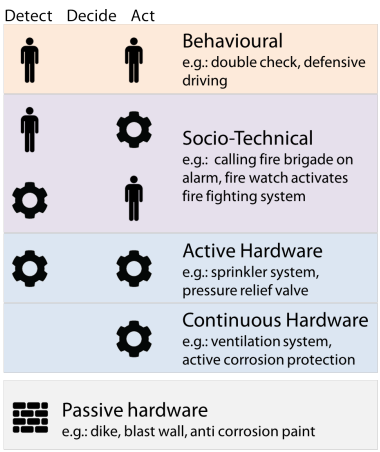
Barrier system

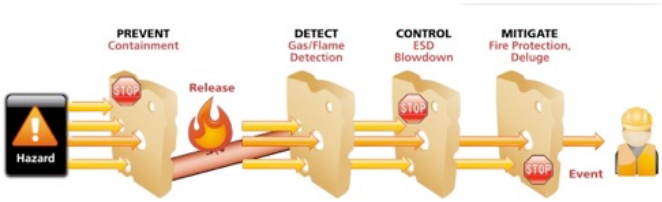
A barrier system is a system that has been designed and implemented to perform one or more barrier functions´

This definition by Sklet, defines barrier systems as the means to implement a barrier function. For example: A fire extinguisher is a barrier system that is there to implement a mitigation function. The type of barrier system is inherent to the barrier itself, unlike the barrier function, which is a relative property. There are different ways to categorise barrier systems as well.

A barrier system can first be divided into active or passive. A passive barrier is for instance a fence or dyke. Active hardware can be further divided using the Detect-Decide-Act (DDA) principle. A complete active barrier system includes all three. Depending on whether people perform these three elements or technology determines what kind of active hardware it is.

If the DDA system is completely represented by people, we call it a Behavioural Barrier. If the whole cycle is hardware based, we call it Active hardware. If the DDA cycle is a mix between people and hardware, we call it a Socio-Technical (or Man-Machine) barrier system. The last type is one where there is no detection, but a continuous action (like for instance a ventilation system). This is called Continuous hardware.





Conclusion

Barriers can be categorised in different ways. The lists and models presented here are not definitive by any means. Looking at barrier functions and barrier systems both has its benefits, but you have to decide for yourself how you want to use barrier types to aid decision-making.

References

Guldenmund, F., Hale, A., Goossens, L., Betten, J., & Duijm, N. J. (2006). The development of an audit technique to assess the quality of safety barrier management. Journal of hazardous materials, 130(3), 234-41.

Haddon, W. (1995). Energy damage and the 10 countermeasure strategies. 1973. Injury prevention : journal of the International Society for Child and Adolescent Injury Prevention, 1(1), 40-4.

Hollnagel, E. (2004). Barriers and Accident Prevention. Ashgate Publishing, Ltd.

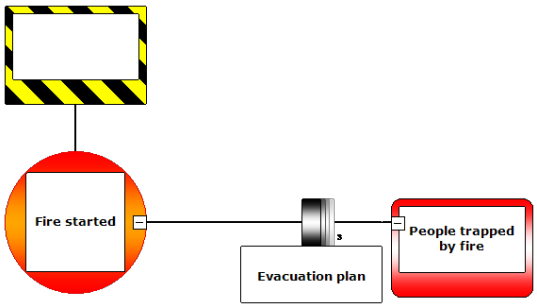
Sklet, S. (2006). Safety barriers: Definition, classification, and performance. Journal of Loss Prevention in the Process Industries, 19(5), 494-506

7 Barrier Families

Many organizations struggle with the level of detail when defining barriers. For example: should barriers be fully independent and therefore be more generically defined? Or does that make the barriers less useful, because fewer details are presented and assessed?

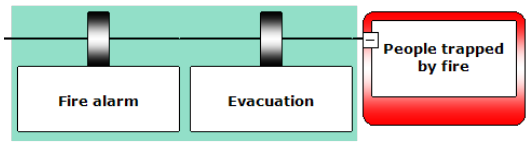
Often organizations need more than just one level of detail. It all depends on your goal. For example: quantification of the bowtie diagram can only be done with independent, high level barriers. Communication of safety critical tasks (SCTs) can only be done when showing specific detailed barriers, including detailed responsibilities, etc.

Example: 'Evacuation plan'

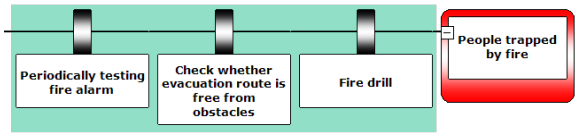


Barrier families allow you to toggle between multiple levels of specificity and grouping. With a single click, you can open the barrier family and show the family members. Below are some highlighted examples.

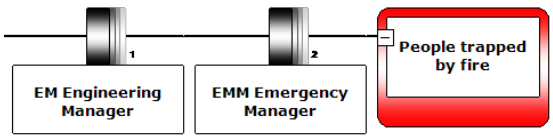
Detect-(decide)-act



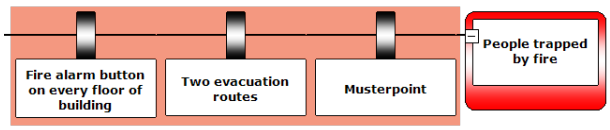
Safety critical tasks



Lookup tables (e.g. Accountability)



Safety critical 'elements'



8 How to use Escalation Factors

Escalation Factors are a valuable aspect of BowTie Risk Assessments. They allow you to dig deeper into your organisation and really assess the weaknesses of your safety Barriers. However a lot of people struggle to apply Escalation Factors in a useful and meaningful way.

The Theory

Escalation Factors are “conditions that lead to increased risk by defeating or reducing the effectiveness of barriers”, also called Defeating Factor or Barrier Decay Mechanism. In other words, Escalation Factors create the holes in the Swiss Cheese Model of James Reason.

Historical use & misuse

When people apply Escalation Factors in BowTies they often take them too far. As a result, some BowTies contain large amounts of Escalation Factors. Sometimes exceeding more than ten per Barrier. When you picture an average BowTie with ten Threats on the left, five Consequences on the right and per line (scenario) three or four Barriers, you already have hundreds of Escalation Factors. The end result is an enormous BowTie that is unreadable and has lost the real power of a BowTie; visualisation and communication of the risk.

Causes for misuse

BowTies can have too many escalation factors because of two main reasons:

Being too specific leads to an exhaustive list of very small factors that might have an impact. This is probably more common if you're used to building fault trees, because those go into much more detail than BowTies. If the objective is to include all those factors and create a really detailed assessment this is not a problem. But if you want to manage your risks and use BowTie as a risk assessment to realise this, it is probably not the best approach

Being too generic: including things like "poor maintenance", "human error" or even "poor safety culture" will not get you anywhere. These factors apply to a lot of barriers and will result in the same escalation factors appearing over and over. Also, generic escalation factors cause you to think of equally generic Barriers to control them, like Competence management, Maintenance management, Auditing, Supervision, etc. These should also be avoided, as they’re not describing specific Barriers, but instead whole management systems that support a whole range of Barriers.

Best practice approach

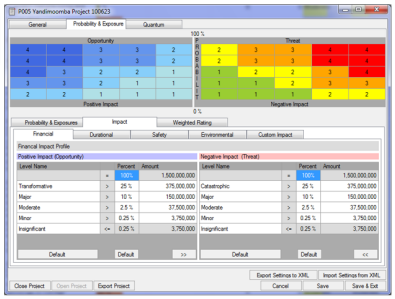
Based on our experience we’ve found that escalation factors work best when they’re used to identify and highlight a limited number of real problems or weaknesses in the organisation. This approach leads to BowTies, which do not exhaustively describe all the potential ways in which barriers can fail, but instead highlight key areas that need extra attention. Sometimes less is more, and this is certainly true for escalation factors. Use escalation factors as exclamation marks instead of exhaustive lists, and the communicative value of the BowTie will be increased tremendously. A key rule: If you can remove the Escalation factor with an activity or action, do not apply as escalation. Something that will remain permanently an escalation on the barrier; e.g colour blindness for electrical operator or artisans, body mechanics for certain jobs, mental fatigue during repetitive work, etc.

9 Risk Matrices

Risk matrices are probably one of the most widespread tools for risk evaluation. They are mainly used to determine the size of a risk and whether or not the risk is sufficiently controlled. There is still confusion about how they are supposed to be used. This article will explain their use in the context of the bowtie diagram.

There are two dimensions to a risk matrix. It looks at how severe and likely an unwanted event is. These two dimensions create a matrix. The combination of probability and severity will give any event a place on a risk matrix (there are some events that are more difficult, but we'll come to that later).

LIKELIHOOD \ CONSEQUENCE	1 MINOR	2 LOW	3 MEDIUM	4 HIGH	5 MAJOR
5 ALMOST CERTAIN	MEDIUM (11)	HIGH (16)	HIGH (20)	EXTREMELY HIGH (23)	EXTREMELY HIGH (25)
4 LIKELY	MEDIUM (7)	MEDIUM (12)	HIGH (17)	EXTREMELY HIGH (21)	EXTREMELY HIGH (24)
3 POSSIBLE	LOW (4)	MEDIUM (8)	HIGH (13)	HIGH (18)	EXTREMELY HIGH (22)
2 UNLIKELY	LOW (2)	LOW (5)	MEDIUM (9)	HIGH (14)	HIGH (19)
1 RARE	LOW (1)	LOW (3)	MEDIUM (6)	MEDIUM (10)	HIGH (15)



Most risk matrices have at least three areas.

- The low probability, low severity area (usually green) that indicates the risk of an event is not high enough, or that it is sufficiently controlled. No action is usually taken with this. If we talk about risk matrices in a bowtie however, usually bowties are done for major hazards, so most events are high risk and don't fall into this category.
- The high probability, high severity (usually red), which indicates an event, needs a lot or more control measures to bring the probability or severity down. Bowties will have a lot of events that fall into this category.
- The medium category (usually yellow) is in between these two areas. Any event that falls in this area is usually judged to be an area that needs to be monitored, but is controlled as low as reasonably practicable (ALARP). Essentially it means if we keep the risk at that level, we accept it.

It's important to understand that a risk matrix by itself makes for a poor decision making tool. It is best suited for ranking events. There is not enough granularity in a risk matrix to use it for anything other than saying that some events are really bad, and others are less so. Decisions need to be based on an underlying analysis (like a bowtie diagram) that will tell you what will cause the unwanted event and what an organisation is already doing to control it. This information will make an informed decision possible.

Another misconception is that a risk matrix is a quantitative tool. In theory, it can be, but in practice, it is not. The risk matrix is made up of two ordinal rating scales, with mostly qualitative descriptions along its axes. This makes it very difficult to assign any real numbers to a matrix and thus to do calculations with it. It can only give a qualitative score that indicates in which category an event falls. It won't allow for any sophisticated calculations.

Severity / Consequence

There are different ways of looking at severity. Something can be very severe from the perspective of human life, or from the perspective of damage to a facility. Usually four perspectives are used (although more or less is also possible) that form the acronym PEAR. This stands for People, Environment, Assets and Reputation. Any event can be judged against these four categories. For instance: a car crash will have an impact on people, but also on assets. An oil spill might have an impact on the environment and reputation, and also some asset and people impact.

These different perspectives do make it very difficult to compare two events with each other. If we have two events, one that scores high on people, and another that scores high on environment, which one is more severe? This is why aggregating risk matrix scores are difficult, if not impossible to do. The best way to compare the severity of events is to make a qualitative judgement.

	Consequence Level (consider the maximum reasonable potential consequence of the event)				
Impact Type (Additional 'Impact Types' may exist for an event; identify & rate accordingly)	**1** **Minor**	**2** **Low**	**3** **Medium**	**4** **High**	**5** **Major**
(S) **Harm to People-Safety**	First aid	Medical treatment	Lost time	Permanent disability or single fatality	Numerous permanent disabilities or multiple fatalities
(H) **Harm to People- Occupational Health**	Exposure to health hazard resulting in minor discomfort.	Exposure to health hazard resulting in symptoms requiring medical intervention and full recovery (no lost time).	Exposure to health hazards/ agents (over the OEL) resulting in reversible impact on health (with lost time) or permanent change with no disability or loss of quality of life.	Exposure to health hazards/ agents (significantly over the OEL) resulting in irreversible impact on health with loss of quality of life (permanent disability) or single fatality.	Exposure to health hazards/ agents (significantly over the OEL) resulting in irreversible impact on health with loss of quality of life of a numerous group/ population or multiple fatalities.
(E) **Environmental Impact**	Lasting days or less; limited to small area (metres); receptor of low significance/ sensitivity (industrial area).	Lasting weeks; reduced area (hundreds of metres); no environmentally sensitive species/ habitat).	Lasting months; impact on an extended area (kilometres); area with some environmental sensitivity (scarce/ valuable environment).	Lasting years; impact on sub-basin; environmentally sensitive environment/ receptor (endangerous species/ habitats).	Permanent impact; affects a whole basin or region; highly sensitive environment (endangerous species, wetlands, protected habitats).
(C) **Social / Community Impact**	Minor disturbance of culture/ social structures	Some impacts on local population, mostly repairable. Single stakeholder complaint in reporting period	On going social issues. Isolated complaints from community members/ stakeholders	Significant social impacts. Organized community protests threatening continuity of operations	Major widespread social impacts. Community reaction affecting business continuity. "License to operate" under jeopardy
(L&R) **Legal & Regulatory**	Technical non-compliance. No warning received; no regulatory reporting required	Breach of regulatory requirements; report/involvement of authority. Attracts administrative fine	Minor breach of law; report/investigation by authority. Attracts compensation/ penalties/ enforcement action	Breach of the law; may attract criminal prosecution of Operating Co. and/or of Directors/ Mgrs. And penalties/ enforcement action. Individual licence temporarily revoked	Significant breach of the law. Individual or Class action law suits, criminal prosecution of Co., Directors/ Mgrs. Suits against parent Co.; permit to operate substantially modified or withdrawn
(M) **Material Losses/ Damage/ Business Interruption**	< 0.01 % of Annual Revenue/ Total Assets	0.01 - 0.1 % of Annual Revenue/ Total Assets	0.1 – 1.0 % of Annual Revenue/ Total Assets	1 - 5 % of Annual Revenue/ Total Assets	> 5 % of Annual Revenue/ Total Assets
(R) **Impact on Reputation**	Minor impact; awareness/ concern from specific individuals	Limited impact; concern/ complaints from certain groups/ organizations (e.g. NGOs)	Local impact; public concern/ adverse publicity localised within neighbouring	Suspected reputational damage; local/ regional public concern and reactions	Noticeable reputational damage; national/ international public attention and

Probability and Likelihood

Up till now, only probability has been discussed. But there are different possibilities. If we drive to work, and there's a probability of 0,05 that we'll crash, we expect for every car that in 100 workdays, there are 5 crashes. The probability will be the same every time we drive to work.

Instead of focusing on a single event, we can also say: how often can I drive to work before I crash? The frequency of a crash will be 1 in 20. This is essentially the same, just written down differently.

The last category looks at the past and scores higher if the event has occurred more. The main difference is that probability and frequency tell us something about the future, while historical scales will only tell us something about the past. If something has not occurred yet, a historical scale will not allow you to make a prediction about how often it might happen in the future. This is why most risk matrices now use probability or frequency scales.

It should however be noted that likelihood used widely in qualitative risk assessments has its own set of definitions and because it is used to determine priority of improvement actions to meet objectives set during risk apatite statements.

	Description
Likelihood	Considering the presence and magnitude of the hazard and the exposure to that hazard (number of people and frequency of the tasks exposing those people), as also the status of existing controls,...
5 **Almost Certain**	the unwanted event is almost certain to happen within the LOM (Life of Mine). In the case of repetitive/ frequent tasks the unwanted event has or will occur in order of one or more times per year. In terms of major events, as also in the case of long term health, environmental or social impacts, it may happen only once in the LOM.
4 **Likely**	there is a high probability that the unwanted event will occur within the LOM. In the case of repetitive/ frequent tasks the unwanted event has occurred or is likely to occur in order of less than once per year. In terms of major events, as also in the case of long term health, environmental or social impacts, it might happen once in the LOM.
3 **Possible**	it is possible that the unwanted event can occur within the LOM. In the case of repetitive/ frequent tasks the unwanted event has occurred or is likely to occur in order of once every 5-10 years. In terms of major events, as also in the case of long term health, environmental or social impacts, it may possibly happen once in the LOM.
2 **Unlikely**	there is a low probability for the unwanted event to occur within the LOM. In the case of repetitive/ frequent tasks the unwanted event has occurred some time or is likely to occur not more than once every 10-20 years. In terms of major events, as also in the case of long term health, environmental or social impacts, there is a low probability for the event to happen in the LOM.
1 **Rare**	there is a very low probability for the unwanted event to occur within the LOM. In the case of repetitive/ frequent tasks there are no records of the event occurring or it is highly unlikely that it will occur within the next 20 years. In terms of major events, as also in the case of long term health, environmental or social impacts, there is a very low probability for the event to ever happen.

Low probability, high severity

There is a problem with events that have a very low frequency, but a catastrophic severity. If the risk matrix categories are not set up correctly, these types of events tend to 'fall off' the grid and get less attention than they deserve. This is especially a problem with historical frequency scales, where an event will get the lowest possible score just because it has never occurred. A possible solution is to make the worst severity category the highest priority category, regardless of the probability.

Strategies for giving scores

Ranking an event on a risk matrix can be done in three ways:

- Worst-case scenario. This is done by taking the worst that could happen. For instance in the case of a car crash, there will be multiple fatalities and it might be likely to occur. Essentially when looking at the worst-case scenario, all Barriers are ignored and only the Hazard, Top event and Consequences are considered. These types of incidents might occur in reality, but they will most likely be the exception, not the rule.
- Current situation. The second strategy tries to evaluate the severity and probability of the average event. So the average severity for a car crash might be a single fatality, and it's unlikely to happen. This strategy takes into account all the barriers that are currently implemented.
- Future situation. The last strategy tries to make an estimate of how the risk might go down after improvements to barriers, or implementation of new barriers. It aims to estimate the future average of incidents.

Even though the risk matrix has a lot of drawbacks, it has endured the criticism and is still one of the standard tools used in most risk assessments. If the risk matrix is used in the correct way, it can add some understanding, although probably the greatest challenge today is for people to understand its limitations.

Risk heuristics (Slovic et. al., 1979)

The heuristic paradigm offers some explanation as to the variation in public risk perception. Several factors have been identified that can influence public risk perception. Below a summary of factors that have an influence of risk perception (why do some persons rate a risk higher than others, either on consequence or on likelihood).

- The familiarity heuristic suggests that the more familiar a person is with a hazard, the lower the level of perceived risk that will be associated with it.
- A person exposed to a hazard in the present perceives the associated risk as being greater than the same risk posed in the future.
- The voluntary vs. involuntary exposure comparison refers to the choice that a person has in incurring the risk. It has been shown that a risk is perceived as less dangerous and more acceptable if it is voluntary accepted, than that to which a person is involuntary exposed.
- The natural vs. technological risks heuristic concept deals with the phenomena that risks imposed by natural causes tend to be far more readily accepted and tolerated than man-made risks. This could be due to the fact that there are fewer alternatives to accepting natural risks and that there is usually no person or group to blame for the occurrence of a natural disaster. The impressions that with age most technological systems fail and must be replaced, increase that level of concern towards technological risks.
- Catastrophic consequences, often referred to as the severity heuristic, suggests that people tend to have a much greater tolerance of risks which results in low fatalities than those which result in high number of fatalities.
- The dread outcome heuristic suggests that hazards feared to produce death due to dreaded outcomes (i.e. slow and painful deaths) are perceived to be riskier than those, which present a more likely chance of death due to a less dreaded means.
- People appear to accept a much greater risk when they feel that the hazard is well controlled and even more when they feel that they themselves have some control over the situation. This

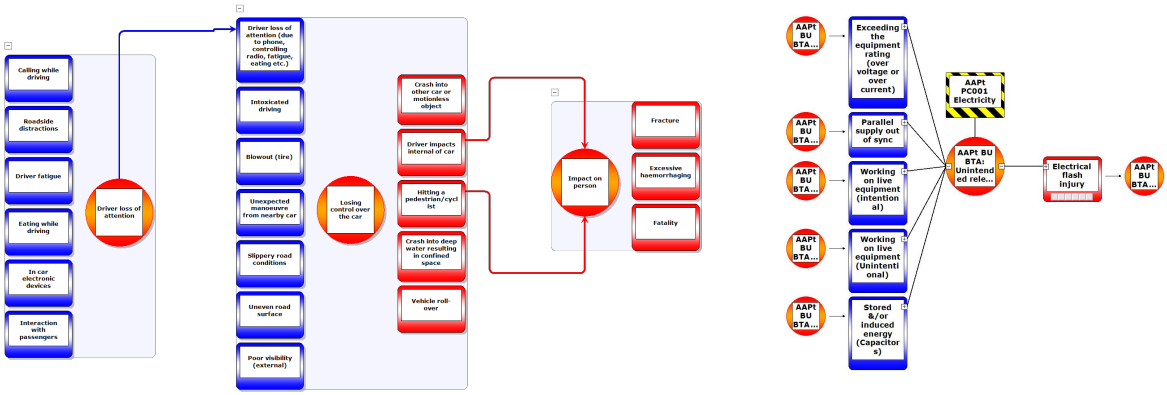
phenomenon has been described as the controllability of outcome.

- Consequences, be they delayed or immediate have a profound affect on lay risk perception. People tend to perceive a hazard as less risky when the consequences of exposure are delayed. An example of this is the acceptance of cancer risks as a result of smoking cigarettes.

10 Chaining Bowties

A BowTie diagram analyses a specific section of a longer causal chain. The diagram focuses on the crucial phase that leads to an accident. Although the diagram is usually enough to capture all important factors that need to be considered, sometimes an issue is so complex and far reaching that we need to look further back.

In BowTieXP, we've built the ability to chain BowTie diagrams together, so the reach of the BowTie can be extended when the need arises.



To get started this article provides some guidance on how best to chain BowTies together. First, start with building normal BowTies. Chaining BowTies is a solution if you need more detail, but should not be the default. Mainly because there's a trade-off between gaining complexity while losing how easy the diagram is to communicate.

Once you've identified Threats or Consequences in a normal BowTie that require additional investigation, create a new BowTie that has as it's Top Event that Threat or Consequence. Any Threat that you want to create a separate BowTie for should only contain previous Threats (essentially creating a left-sided BowTie). A BowTie to elaborate on a Consequence should only have further Consequences (creating a right-sided BowTie). That will most likely be sufficient for most purposes.

After the BowTies have been extended, we also need to look at the Barriers. Some Barriers in the original BowTie will be focused on eliminating the Threat. Logically, these barriers take effect before the Threat to stop it, but in BowTie we place them to the right to create a single diagram. But since we're creating extra diagrams before, we can take all the elimination barriers out of the original BowTie, and place them on the correct lines in the previous BowTie.

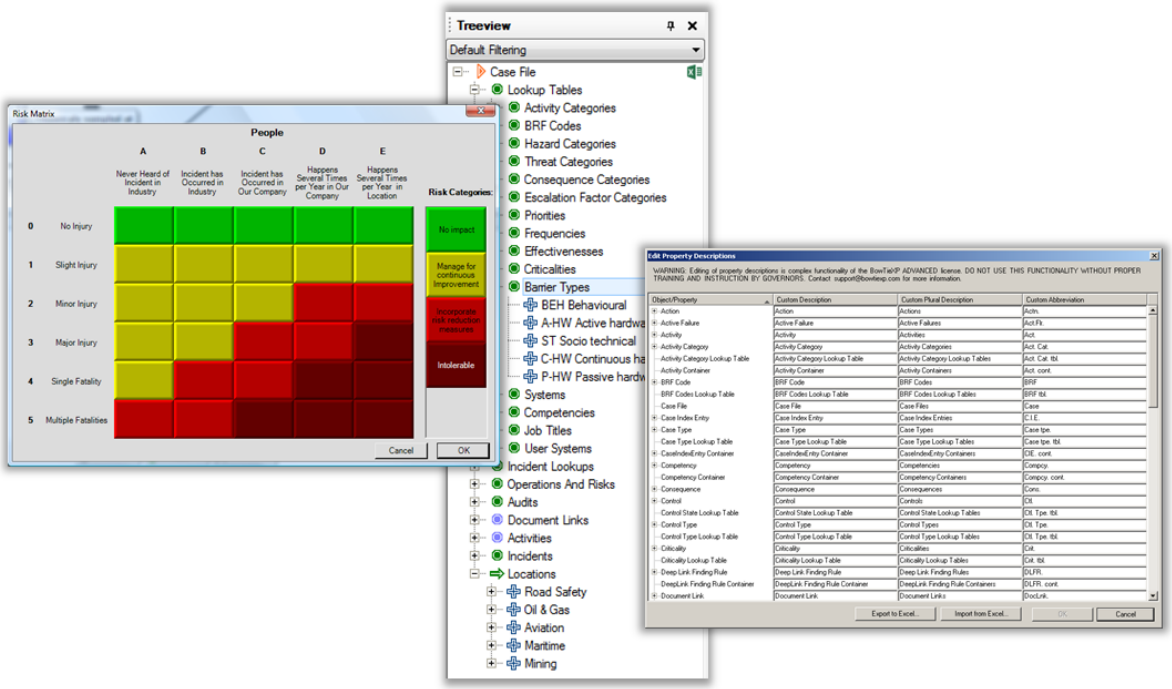
The same is true for Barriers on the right hand side. Some Barriers focus on mitigating the Consequences, which means they logically take their effect after the Consequence has occurred to minimise further Consequences. If we're creating an extension of the BowTie, we can place these mitigation Barriers in the next diagram.

In summary, chaining BowTies can greatly increase the level of detail, but always at a cost of more complexity, so you need to make sure the situation you're trying to model is sufficiently complex to warrant this kind of diagram.

11 Bowtie Template

Speak the same Bowtie language

Most organizations use their own risk matrices, have their own terminology and use specific job titles. It is important to speak the same language and modify all default BowTieXP settings to your organizational standards and needs. By using the Template functionality you are able to save all these modified settings and make sure you -and all other BowTieXP users in your company- always use these settings when making a new Bowtie file.



5 Steps - How to use the Bowtie Template

Step 1: Create Template settings

Customize all the settings to meet your company standards. Especially the lookup table lists, terminology and risk matrices are important. However, there are also other elements to consider. For an overview of these elements.

Step 2: Send the Bowtie file (.btf) to other BowTieXP users

Save all your settings as Bowtie file ("File – Save as…") and send this file to other bowtie users. The size of the Bowtie file is very small, so it can be easily sent by e-mail.

Please note: The Bowtie file doesn't have to contain bowtie diagrams.

Step 3: Save Bowtie file (.btf) as template

Open the Bowtie file in the BowTieXP software and save this file as a BowTieXP Template ("File – Save a copy as Template…").

Please note: Save the .btf template in the default folder. Do not change the folder / location where to save the .btf template.

Step 4: Select template when starting up a new file in BowTieXP software

A window will appear when starting up the software, which allows the user to make a decision which template to use.

Please note: When starting up the BowTieXP software by double clicking on a Bowtie file (.btf), the software will use the template in which the selected Bowtie file is created.

Step 5: Manage Template(s) - Templates Directory

You are able to remove templates in the Template Directory ("Help – Go to Templates Directory…").
Please note: To modify the template, just open the template, modify the settings and save the file again as template (step 3).

Bowtie Template content

Bowtie Template content overview

Highly recommended customizations:

- Terminology: barriers/controls etc.
- Risk matrices: 4x4, 5x5 4x5, colouring etc.
- Barrier effectiveness
- Barrier types
- Job titles
- Priorities (for Actions)

Functionally dependent customizations:

- Actual activities
- Actual document links
- Any AuditXP functionality
- Any IncidentXP functionality

Interesting optional customizations:

- Scrap Book
- Sample BowTies
- Locations: List per region, rig, site etc.
- Acceptance criteria
- File properties
- Display profiles
- Barrier criticalities
- Systems
- Threat categories
- Frequencies (for activities or threats)
- Revision info box

Other optional customizations:

- Treeview filters
- Hazard categories
- Consequence categories
- Escalation factor categories
- User systems
- Activity categories
- Competency (for activities)

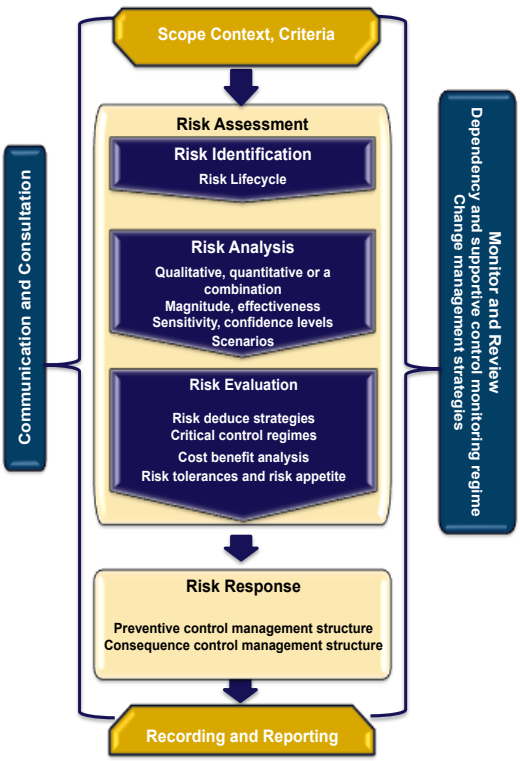
12 Hazard Identification and Bowtie

What is a Hazard Identification study?

Hazard Identification stands for Hazard Identification. Legislation for high-risk industries often requires that all hazards with the potential to cause a major accident be identified. Hazard Identification is one of the best-known methodologies to identify potential hazards because it provides a structured approach to identify hazards, potential undesirable consequences and evaluate the severity and likelihood of what is identified.

ISO 31000:20018

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies. The main task of ISO is to prepare International Standards. ISO 31000 provides principles and generic guidelines on risk management. This International Standard can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.



Principle 6.4.2 Risk identification

"The purpose of risk identification is to find, recognize and describe risks that might help or prevent an organization achieving its objectives. Relevant, appropriate and up-to-date information is important in identifying risks.

The organization can use a range of techniques for identifying uncertainties that may affect one or more objectives. The following factors, and the relationship between these factors, should be considered:

- tangible and intangible sources of risk;
- causes and events;
- threats and opportunities;
- vulnerabilities and capabilities;
- changes in the external and internal context;
- indicators of emerging risks;
- the nature and value of assets and resources;
- consequences and their impact on objectives;
- limitations of knowledge / reliability of information;
- time-related factors;
- biases, assumptions and beliefs of those involved.

The organization should identify risks, whether or not their sources are under its control. Consideration should be given that there may be more than one type of outcome, which may result in a variety of tangible or intangible consequences."

Principle 6.4.3 Risk analysis

"The purpose of risk analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk. Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness. An event can have multiple causes and consequences and can affect multiple objectives.

Risk analysis can be undertaken with varying degrees of detail and complexity, depending on the purpose of the analysis, the availability and reliability of information, and the resources available. Analysis techniques can be qualitative, quantitative or a combination of these, depending on the circumstances and intended use.
Risk analysis should consider factors such as:

- the likelihood of events and consequences;
- the nature and magnitude of consequences;
- complexity and connectivity;
- time-related factors and volatility;
- the effectiveness of existing controls;
- sensitivity and confidence levels.

The risk analysis may be influenced by any divergence of opinions, biases, perceptions of risk and judgements. Additional influences are the quality of the information used, the assumptions and exclusions made, any limitations of the techniques and how they are executed. These influences should be considered, documented and communicated to decision makers.

Highly uncertain events can be difficult to quantify. This can be an issue when analysing events with severe consequences. In such cases, using a combination of techniques generally provides greater insight.

Risk analysis provides an input to risk evaluation, to decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment strategy and methods. The results provide insight for decisions, where choices are being made, and the options involve different types and levels of risk."

Bowtie diagrams for high-risk hazards

It is not possible to make bowtie diagrams for all existing hazards. There are simply too many hazards, and it will take too much time to make as many bowtie diagrams. Moreover, it is less beneficial to create bowtie diagrams for simple or low impact hazards, because structuring these hazard (by making bowtie diagrams) will not provide a much better understanding of the hazard (assuming these hazards will have a relatively simple structure). Therefor a separation should be made between high priority hazards that require bowtie analysis and low priority hazards for which only a Hazard Identification analysis is sufficient. The Hazard Identifications inherent risk assessment levels can be used to assess which hazards require closer examination by creating bowtie diagrams.

Hazard Identification module in BowTieServer

In BowTieServer we created a Hazard Identification module, which allows you to group your Hazard Identifications by location, perform your Hazard Identifications, and use the output to create bowtie diagrams for the high-risk hazard.

Overview

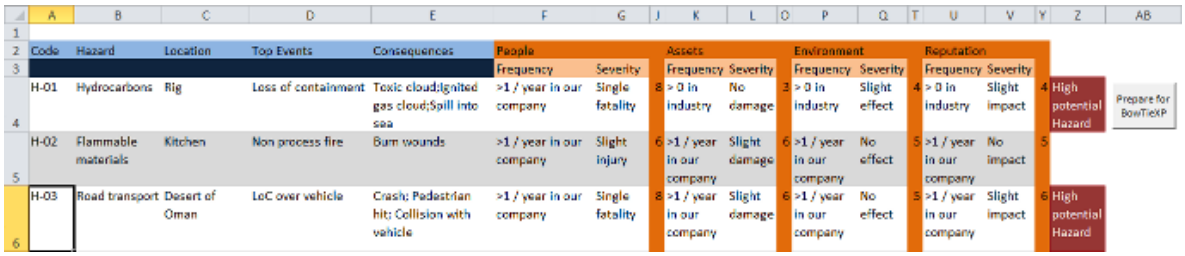
The Excel template workbook allows you to do your Hazard Identifications in Excel, and import the output into a BowTieXP case file.

The Hazard Identification workbook

The workbook consists of two Excel sheets: the Hazard Identification sheet and the risk matrices sheet. The Hazard Identification sheet is the place to put all your risk assessments. The risk matrices sheet allows you to configure risk matrices, which determine the hazard potentials.

Doing the Hazard Identification analysis

The image below shows the hazard sheet:

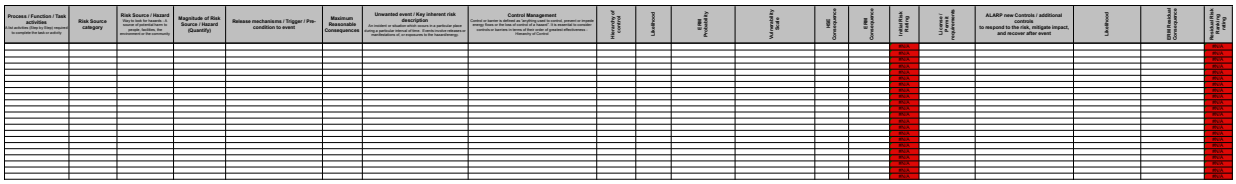


Code	Hazard	Location	Top Events	Consequences	People			Assets			Environment			Reputation				
					Frequency	Severity		Frequency	Severity		Frequency	Severity		Frequency	Severity			
H-01	Hydrocarbons	Rig	Loss of containment	Toxic cloud;Ignited gas cloud;Spill into sea	>1 / year in our company	Single fatality	8	> 0 in industry	No damage	3	> 0 in industry	Slight effect	4	> 0 in industry	Slight impact	4	High potential Hazard	Prepare for BowTieXP
H-02	Flammable materials	Kitchen	Non process fire	Burn wounds	>1 / year in our company	Slight injury	6	>1 / year in our company	Slight damage	6	>1 / year in our company	No effect	5	>1 / year in our company	No impact	5		
H-03	Road transport	Desert of Oman	LoC over vehicle	Crash; Pedestrian hit; Collision with vehicle	>1 / year in our company	Single fatality	8	>1 / year in our company	Slight damage	6	>1 / year in our company	No effect	5	>1 / year in our company	Slight impact	6	High potential Hazard	

The table below shows the columns on the Hazard Identification sheet:

Column	Description
Code	The hazard code
Hazard	The hazard title
Location	The location where the hazard occurs
Top Events	The top events related to the hazard
Consequences	The consequences related to the hazard
Frequency	For each of the risk matrices, the frequency indicates how often the top events lead to the consequences in this category
Severity	For each of the risk matrices, the severity is the worst that can happen when the top events occur, for each of the categories

The image below indicate an Enterprise Risk analysis spread sheet in Excel



Risk matrices

On the risk matrices sheet, you can customize the risk matrices used to determine the hazard potentials. Also, you can set the cut-off for which hazards are added to the BowtieXP case file (under settings).

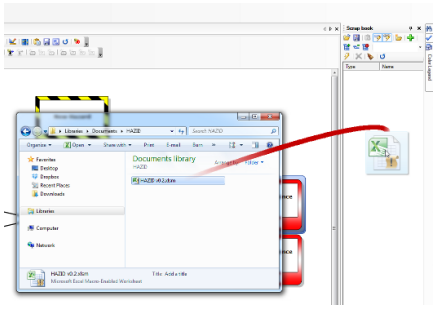
The hazard sheets contain four risk matrices: people, environment, assets and reputation. The software does have the option to change the categories and add up to 8 categories of consequence impacts. Each of the categories has a severity and a frequency. The severity indicates the possible extent of damage; the frequency indicates how often this happens. In the matrix, a hazard potential rating is assigned to each of the combinations of frequency and severity. Different hazard potentials have different colours.

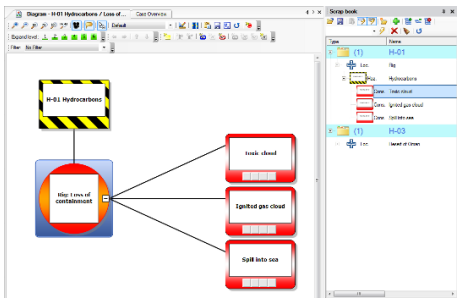
The risk matrix can be use in various risk analysis, but should serve the purpose of indication the level of effectiveness of the controls that has improved the original risk assessment that was done. Example: A major hazard from a Lifecycle risk assessment was used to do the risk analysis through the use of the Bow Tie Analysis, the original risk rating was 24 on a 5X5 risk matrix. After the BTA a number of improvement actions were allocated to the effectiveness of controls, Escalation factors were identified and reliable mitigating controls assigned. Tus the residual risk should be less, either by likelihood or by consequence, subject to the level of control that was employed.

Importing in BowTieXP

To import the Hazard Identification information into BowTieXP, follow these steps:

- On the Hazard Identification sheet, press the "Prepare for BowTieXP" button. For each of the hazards, a Spreadsheet will be generated.
- Save the file.
- Open BowTieXP, and open the Scrapbook through the menu (View - Windows - Scrap book).
- Locate the Excel file in Windows Explorer and drag it onto the Scrapbook.





You can now drag elements from the scrapbook onto your BowTie diagram. Below you see a BowTie diagram, which was dragged in from the scrapbook.

Obtaining the Hazard Identification workbook

You can obtain the Hazard Identification Excel Template workbook by contacting support.

Notes

Importing the Hazard Identification sheet into Excel works via the Scrapbook, and thus requires that you have BowTieXP Advanced installed. To check if you have the Advanced features, follow these steps:

- Open BowTieXP
- In the menu, click "Help" and select "About...". A dialog pops up.
- Under "Enabled Features", you should see "Advanced" as shown here:

BowTieXP Software Copyright © IP Bank B.V. 2003-2012

Release Version: 5.2.0.0
Enabled Features: Advanced, Black, SharePoint, Spreadsheet

Windows may automatically block specific Excel functionality for security reasons. Because of this, you have to unblock this functionality the first time you open the file in Excel. You may see the following warnings:

- Protected View. This file originated from an Internet location and might be unsafe. To resolve, click "Enable Editing".

- Security Warning. Macros have been disabled. To resolve, click "Enable Content".

13 Risk Based Auditing

Abstract

Barriers that are defined in the Safety Management Systems are the means to manage safety. Information on the quality of the barrier is therefore of vital importance. A common way of assessing the quality of your safety management system is to perform audits. A Dutch study (Zemering & Swuste, 2005) suggests that we should move away from traditional categorical audits and move on to scenario (risk) based audits.

Assessing safety management systems

Safety Management Systems (SMS) can be represented using the bowtie methodology. The method structures the SMS by identifying barriers that should prevent incident scenarios from becoming reality. Managing the effectiveness of these barriers thus ensures process safety. It can therefore be said that the quality of the SMS is defined by the quality its barriers.

In order to adequately manage your barriers, it is important to know the quality of your barriers. For example, it can be dangerous to rely on barriers that are defined in the SMS but are in reality inadequate. Good ways to gain insight into barrier quality are: Incident analysis and auditing. This article will take a closer look into the auditing part.

Traditional auditing

A traditional audit is often directed to assess a specific part of a process. It focuses on a predetermined category selected from a list of categories. For example, in order to comply with OSHA legislation, companies have to be subjected to Process Safety Management (PSM) audits. The audits provided by PSM identify 14 elements that cover a broad spectrum of process safety issues (i.e. employee participation, operating procedures, mechanical integrity etc.). These elements and audit formats have been heavily standardized. The results can therefore be easily compared between companies or sites.

Risk based auditing

However, a study has argued that traditional categorical audits may not be as effective as once thought. It has exposed three main shortcoming of categorical auditing: Poor hazard identification (1), they are not scenario based (2) and they neglect human factor related issues (3). First, it is argued that most audits do not take hazard identification as the starting point.

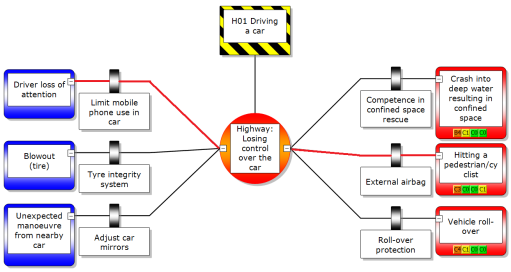
Hazard identification is the first step of designing a SMS. If this stage is poorly executed, the SMS will not deal with the actual hazards. Audits should take the hazard as a starting point to ensure that the SMS that is being assessed is capable of handling the actual hazards.

Secondly, the traditional category approach is not scenario based. It looks at individual elements, often neglecting the way they need to work together in case of an incident. By auditing from the perspective of a possible incident scenario, the system is tested as the sum of its parts. This is a better reflection of realistic situations.

Thirdly, human factors are often mentioned in traditional audits as being relevant, but do not specify which types of human factors are encountered. This makes it difficult to generate adequate solutions that effectively improve the human factor issues.

Human factor issues can be difficult to identify from abstract categories and are better described with real-life examples. Because scenario audits take a more lifelike approach, human factor issues are more likely to come to light.

Once identified properly, they can be adequately addressed.

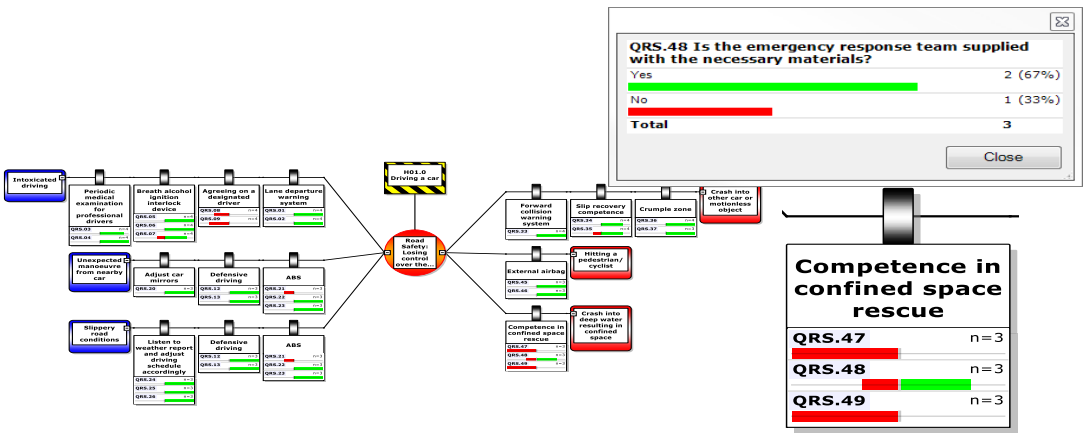


The red line represents an incident scenario. The driver loses attention, thus losing control over the car and hits a pedestrian.

BowTie diagram and Risk Based auditing

Risk based audits can be based on BowTie diagrams. They graphically represent the various incident scenarios and the barriers that should prevent them from evolving. Creating a pathway from a threat, through a top event to a consequence is a possible scenario.

The audit should assess whether the barriers in between are adequate in such a scenario. The hazards represented in these scenarios are used to set the criteria, which the barriers should meet. This allows criteria to be defined more specific and risk based. Such an approach will generate relevant feedback that directly applies to the barriers defined in the SMS.



Conclusion

Risk based audits are a more risk based approach to auditing. Instead of focusing on abstract categories, the scenario focuses on the barriers that reduce the unique risks of an organization. The direct link to scenarios and barriers makes it easier to make concrete recommendations for improvement. This means that resources invested in scenario auditing return more valuable feedback that improves the safety of and organization.

Bowtie for risk-based inspection

The Bowtie methodology is a risk evaluation method that can be used to analyse and demonstrate causal relationships in high-risk scenarios. The method takes its name from the shape of the diagram that you create, which looks like a men's bowtie.

Bowtie takes out the complexity of methodologies like Fault trees and Event trees and uses barriers instead, making it an excellent tool for risk communication and risk-based inspections.

An assisting tool for Compliance Control

An Inspection Authority is not able to inspect all existing safety measures. Compliance Control often focuses on a selection of critical safety aspects. Bowtie risk assessment can be used to identify which safety measures should be considered as critical, and thus can be used to develop inspection programs. Some examples have been given below.

The Dutch State Supervision of Mines (SSM) has developed inspection programs for the next five years by looking at the risks shown in the bowties. The frequently used barriers in the bowties will be supervised in separate inspection projects of the programs. Bowtie could be also a helpful tool to identify whether the right data is inspected during Compliance Control. For example, while creating Bowtie diagrams, the UK Civil

Aviation Authority (CAA) found that they did not inspect certain data which is helpful for the assessment of barrier effectiveness[4]. The bowtie methodology hence can be used to identify the right questions that should be asked by inspectors during compliance control.

Further, Bowtie diagrams provide a direct link between risk scenarios and inspection results. Therefore, Bowtie gives an indication of the severity of the non-compliance in the inspection results. For example, multiple non-compliances in one single possible scenario should be rated as more severe than various non-compliances in different scenarios.

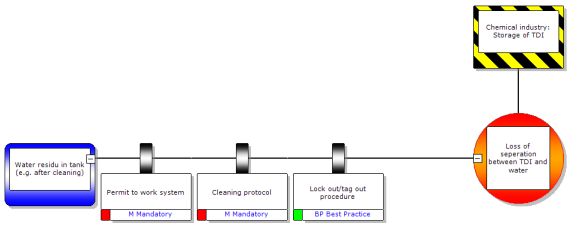
During 2013, the Petroleum Safety Authorities Norway (PSA) will clarify relationships between risk assessments, barrier strategies and barrier performance, and they will ensure that barrier performance is being monitored throughout the producing life of installations.

ARAMIS recommends using the Bowtie methodology to demonstrate that hazards are identified and risks are properly managed and to indicate what kind of safety barriers could (best practices) or must (compliancy) be implemented.

A communication tool for Compliance Promotion

The bowtie diagram is perfectly suitable for communication. The diagram is easily understandable and 'the picture paints a thousand words'. Inspectorates can use the diagram to communicate information to the industry. For example, in case of non-compliance, the inspectorate can use Bowtie diagrams to show the non-compliant organization which (mandatory) barriers have to be implemented or should be adjusted to achieve the level of compliance.

Also, when new legislation comes into force, Bowtie diagrams can be used to communicate and 'promote' the new legislation, by visualizing the new mandatory safety measures.



A tool for sharing Best Practices

As a suggested extension of Compliance Promotion, Bowtie diagrams can be used for "Best Practice Promotion". Sharing best practices between Inspectorate and industry is evaluated as very useful by most organizations since this communication is more focused on collaboration between Inspectorate and industry, instead of giving or getting penalty due to non-compliance.

The Dutch State Supervision of Mines (SSM) is a good example of an inspectorate collaborating with the industry. In 2012, SSM has started the development of bowties around the distribution of gas, working closely together with the industry. The SSM tries to help the gas network to get a better understanding on how to manage the major hazards relating to the distribution of gas. The insights from the bowtie diagrams have been very helpful for assisting the gas network operators with their safety programs.

Civil Aviation Authority (CAA), UK's specialist aviation regulator, is another example of sharing best practices with the industry using bowties[4]. The CAA is developing Bowtie diagrams covering each of the CAA's 'significant seven' safety issues. The shared goal of CAA and the industry is a balanced risk overview for the whole aviation system.

A tool for Structuring Assessment Feedback

The information derived from Compliance Control, Compliance Promotion and Enforcement need to be assessed. This information will need to be considered when improving the appropriate elements of the Regulatory Cycle. The Bowtie diagrams will provide an indication of industry-wide safety measurement performance when plotting all inspection results in the bowtie diagrams. Some elements of the cycle such as Regulations and Compliance Control can be improved based on the result of this safety measurement performance indication.

References

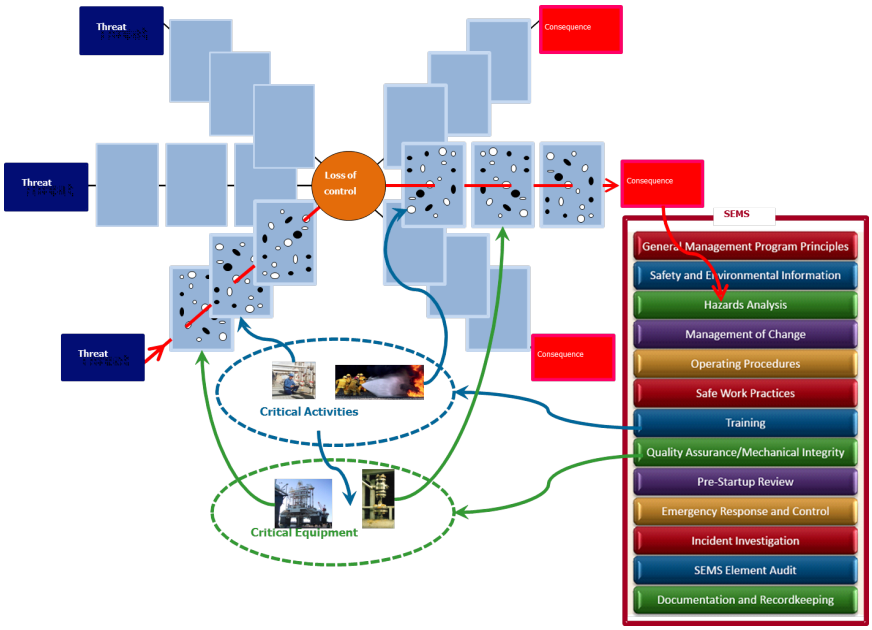
Putte, I. van der (2006). Chemicals In Our Environment. Practical implementation of risk-management strategies. AWE International June 2006.
Directive 2010/75/EU of the European Parliament and of the Council. On industrial emissions (integrated pollution prevention and control) (2010).
CGE Risk Management Solution (2013). BowTieXP Methodology Manual. Revision 13. Not published.
CGE Risk Management Solutions (2012). Civil Aviation Authority develops BowTies for 'Significant Seven' Safety Issues. Not published.
CGE Risk Management Solutions (2012). Analyzing barriers at the Dutch State Supervision of Mines. Not published.
H.Andersen, J.Casal, A.Dandrieuxet, et. Al. (2004). ARAMIS: User guide. The European Commission. Community Research.
Delvosalle, C., Fiévez, C., Pipart, A., Londiche, H., and Debray, B. (2004). ARAMIS Project: Effect of safety Systems on the Definition of Reference Accident Scenarios in SEVESO Establishments. The European Commission. Community Research..

14 Bowtie: Closing the loop between risk assessment and the management system

Sheryl Hurst (Warrington) - Risktec

Companies in major hazard industries have long been accustomed to carrying out hazard identification and risk assessment. They are also expected to have in place a structured safety management system. In recent years, moves have been made to link the two visibly – to demonstrate that the management system is indeed able to control the actual hazards present, rather than being a separate system produced in isolation.

The latest such development has occurred in the US, where operators are required to develop and implement a Safety and Environmental Management System (SEMS) for oil and gas operations in the Outer Continental Shelf. A key requirement is for SEMS to demonstrate that safety critical equipment is being maintained and that safety critical jobs are undertaken by competent people – in other words a joined up SEMS.



Linking barriers to the SEMS

Bowtie analysis is an established risk assessment technique that allows detailed analysis of prevention and mitigation measures for specific hazards. This is achieved by constructing a bowtie diagram, which illustrates potential causes of the hazardous event and ultimate consequences. However, one aspect of the technique that is not always exploited to its full potential is to verify the link between the barriers in the bowtie and the SEMS.

Each prevention barrier on the left side and each mitigation barrier on the right side can be linked to critical tasks which keep the barrier working and are in turn linked to job descriptions, training and competence assessments, i.e. the competence assurance part of the company's SEMS.

Barriers that make a claim on a piece of equipment can also be linked to computerised maintenance management systems which specify the equipment's criticality and inspection/test regime, as well as to performance standards, performance assurance activities and verification schemes, i.e. the asset integrity part of the company's SEMS.

Managing what matters

Exploring these direct links between risk assessment and the SEMS highlights any weaknesses in arrangements and establishes objectively whether effective systems are in place to sustain those measures essential for controlling hazards.

Not only does this provide assurance that hazards are effectively managed, it also ensures that the SEMS is designed to focus on the real-life threats to the organisation's safe operation it manages what matters.

Having conducted the risk assessment and confirmed the links between hazards and the SEMS, a third 'layer' of bowtie analysis allows for the audit of the arrangements on the ground. The bowtie diagrams and supporting critical activities and equipment reports can act as checklists to verify that the hazards continue to be controlled as intended.

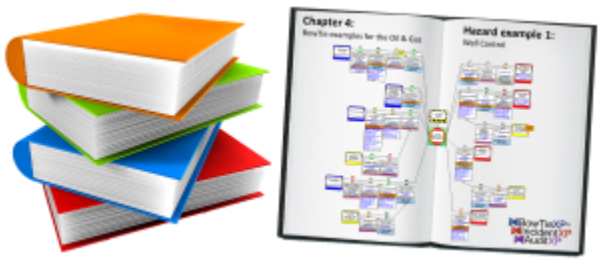
Living safety cases

Safety cases can use bowties to map the link between major hazard barriers and the SEMS. Operators or regulators inspecting the facilities can easily check for evidence of the supporting competence assurance and asset integrity activities, providing proof that the safety case is based on reality and that hazard management is truly owned by the workforce.

Conclusion

Making full use of the bowtie methodology helps organisations develop a joined up SEMS, which is targeted at major hazards. Thereafter, using bowties to audit competence and asset integrity closes the loop between the SEMS and risk assessment.

The BowTie Examples Library



CGE has initiated a Joint Industries Project, called "The BowTie Examples Library".
Our ambition is that the BowTie Examples Library will make a valuable contribution to safety and operational excellence, by assisting both new and expert users of BowTieXP.

15 BowTies in the Heart of your Company

Bowties are easy, but it takes brains and effort to get them in the heart of your company. A successful adoption of barrier based risk management throughout the enterprise requires a number of prerequisites. How do you combine the tangible and less tangible, but equally important, elements?
During the implementation of barrier based enterprise risk management, all aspects of the matrix shown below are equally important.

The introduction of barrier based risk management throughout the enterprise should involve all aspects of the matrix. For instance:

- Excellent software tools
- Integration with existing systems
- Thorough introduction to and training
  - Risk management
  - Incident management methods
- Implementation and project management skills
- Awareness and leadership
- Increasing Corporate Performance with BowTies

Organizations throughout the world rely on Barrier Based Risk Management to ensure their risks are monitored and controlled. However, the same method can also be used to increase the Corporate Performance.

BowTies are recognized to be perfectly suitable not only for assessing risks, but also to be at the centre of your risk management efforts as a company. Therefore, the model has been adopted by more and more companies for its granularity and outstanding capabilities to define both the black swans leading to catastrophes and the best ways to prevent them from happening.

Improving risk management will have an impact in many layers of your organization. By realizing which barriers need to be implemented to prevent unwanted situations, the core processes in your organization will improve.

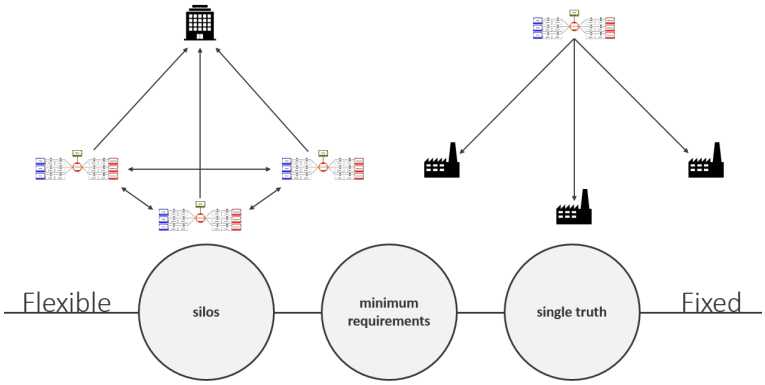
This will increase the quality and lower the costs of your operation. In short, it will improve your operational excellence.

16 Global vs Local

BowTieServer: Global vs Local

There are multiple ways to structure data in BowTieServer to suit different types of organisations. It is possible to create a “top-down” approach, which usually means there is a corporate standard that is rolled out to multiple sites. This is useful if the knowledge on how to manage risk is present on a corporate level. On the other hand, if sites have more knowledge on managing their specific risks, it might be better to go for a bottom up approach, where each site determines their own ways to manage risks. Obviously, a lot of organisations will be a mix between these two extremes, which can also be done.

The next paragraphs explain these three types of organisations in more detail.



Top-down approach: "single truth"

A top-down approach is suitable for organisations that have operations on multiple sites with a high level of similarity and a corporate department that has enough knowledge to determine what should be done on these sites. For instance, a fast food chain with restaurants throughout the world. Although the physical locations may differ, the processes within each restaurant should be almost identical. Because of this, the corporate office can create standards that every restaurant should adhere to. The individual sites only have to make sure that the barriers indicated on the corporate BowTies are implemented correctly. Having a single BowTie standard makes it much easier to monitor sites through audits and compare them because the audits will be based on the barriers from the same BowTie diagrams.

Bottom Up approach: "silos"

Where the Top Down approach is mostly useful for organisations with a high level of similarity between sites, the Bottom Up approach is a better option for organisations where sites all have different processes. These individual differences between sites make it difficult to create a single generic BowTie that all sites should adhere to (like the Top Down approach).

The generic BowTie will not adequately represent individual sites. Instead, it may be better if sites create their own BowTies to ensure a close fit. In order to share knowledge between sites, read-only access can be granted between sites, so they can view each other’s BowTies. When selecting this approach, the role of the corporate office is different compared to the Top Down approach. Instead of using BowTies to dictate which barriers should be in place at each location, the BowTies are now used by the individual sites to show they are adequately in control of their risks.

The advantages of creating Bottom Up is that the diagrams will be very specific and will have a close fit with reality. The disadvantage is that it is more difficult to compare sites and it will take more resources to create all the BowTies.

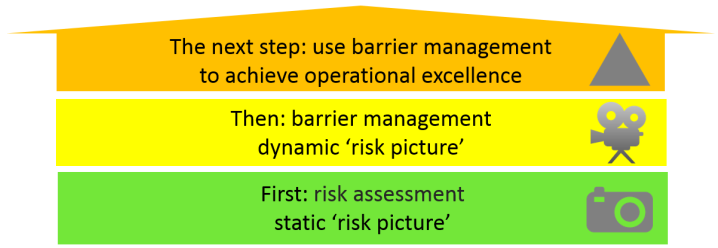
Hybrid approach: "minimum requirements"

Of course, not all companies will fit exactly in a Bottom Up or Top Down profile. There are hybrid forms that try to bridge the gap between the rigid Top Down approach and Bottom Up approach. The hybrid approach is suitable for companies that run operations that share a lot of common ground, but also have slight differences per location. For example, an airline company may operate in different countries. Although the main operation is flying an aircraft, differences in legislation or airport facilities may result in some barriers or threats being present in one place but absent in another. So, even though there are some differences, a large proportion of the BowTie content will be the same for all locations. In that case, a hybrid approach might be most suitable.

In a typical hybrid approach, the corporate office creates a set of template BowTies on a generic level. The barriers, threats and consequences that are identified on those should be seen as minimum requirements. Every individual site will then make a copy of the template BowTies and add/remove content so it fits their particular reality. This way, the general structure of the BowTies will remain consistent, but there is still room to make small adjustments to make them fit for the location. The corporate office can then audit against the minimum requirements, and individual sites can show where and why they deviated or added extra barriers.

17 Advanced Barrier Management

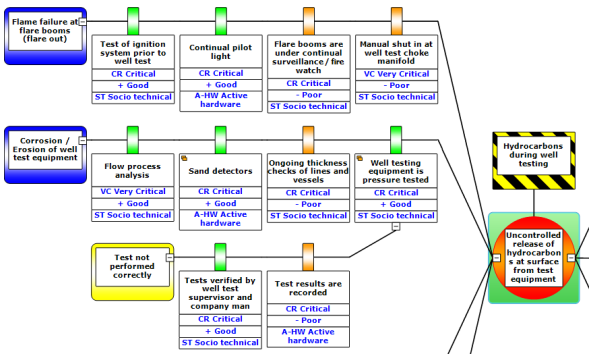
Before we can talk about Advanced Barrier Management, we need to be specify first what Barrier Management Risk Management is: Barrier Based Risk Management is all about your primary business processes; to know what your critical controls are (the 'barriers') and what the status of these barriers is, and then to understand how to manage the barriers. Advanced Barrier Management is to aim to monitor the status of these barriers on a daily basis. The BowTie method is used as a means to get this 'picture', and as a structure to monitor the status of the barriers.



How does Advanced Barrier Management work?

Identifying what control measures a company has in place can be an illuminating experience. But once those barriers have been identified, how can you know that the controls are actually performing well? The process of going from having identified the controls, to assessing the performance based on actual data, is a project we have called Advanced Barrier Management. It is advanced in two ways.

- Companies need to have an excellent understanding of what their controls are and have them identified with sufficient confidence in a risk assessment such as BowTie.
- Performance is tested using a range of different data sources such as incidents, audits and maintenance systems. Those data need to be aggregated. So it is advanced in the sense of both data collection and analysis.



Advantages:

- Risk assessments come to life. Instead of being forgotten and archived, risk assessments are actually used because they are relevant in the day-to-day operations.
- The aggregation of various data sources allows a level of understanding and insight into risks, which is unprecedented in risk management until now.

18 Process Deviation management

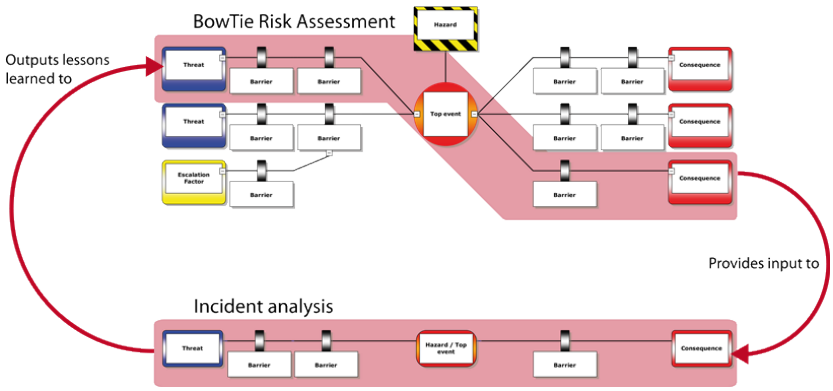
Learning from incidents

Analysing incidents using a barrier-based philosophy is a common occurrence. Learning from individual incidents is becoming more ubiquitous, we know roughly how to do it. The challenge is to learn from many incidents.

In the area of risk assessment, the same barrier philosophy can be applied. The BowTie method is the most advanced barrier-based methodology for risk assessment.

Both of these methods, incident analysis and risk assessments are used in their respective areas; one is reactive, the other is proactive. Both follow the same barrier-based philosophy, which makes the two compatible to exchange information. Merging the information from these two approaches can have tremendous benefits. Using the findings from incidents to update a risk assessment can help in aggregating and seeing patterns emerge across incidents.

Some of the advantages are; combining several near misses to see the potential for looming future incidents; extrapolating the failed controls from one scenario to another; uncovering and updating the risk assessments with information from incidents; using the risk assessments as a final quality check on the incident analysis.



Process Deviation Management

Analysing and understanding incidents is nothing different than analysing and understanding process disruptions from an operation point of view. The same methods, the same tools and the same applications can be used for this purpose.

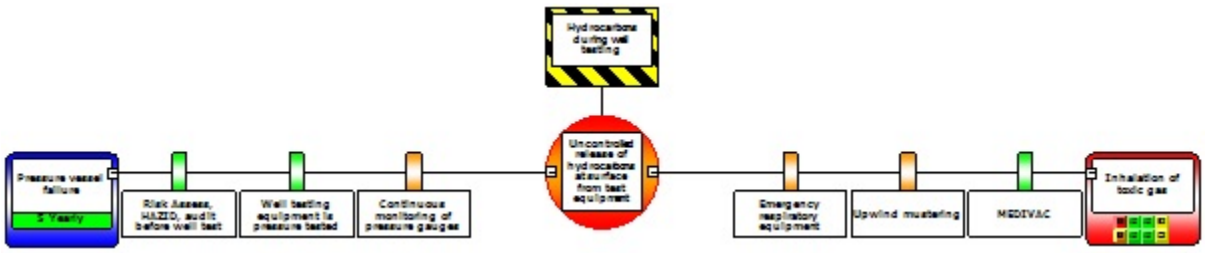
Process Deviation Management is about capturing, analysing and managing data and improvement actions related to process deviations "from a barrier perspective|. Process deviations can be about operations, HSE and quality.

The essence is to understand which controls or barriers have failed or proven to be reliable - and why (5x) this is the case. Furthermore the barriers are linked to your management systems, so you know who is responsible, which procedures are applicable and what the (status of the) improvement actions are.

19 Focusing on Safety Barriers

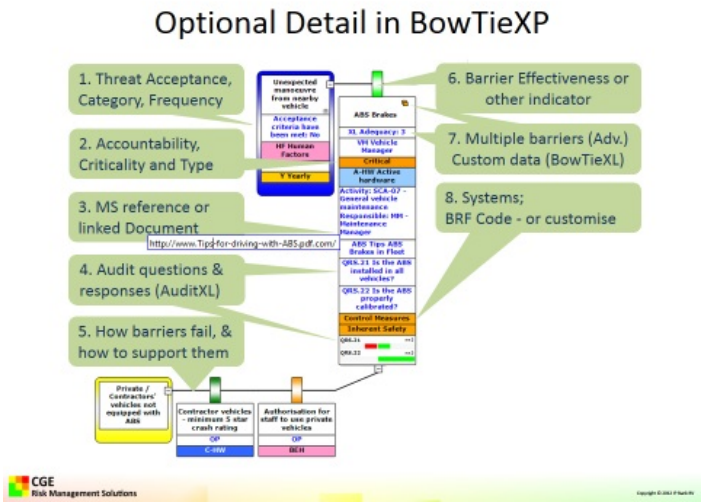
CGE Risk Management Solutions' BowTieXP software product is the leading qualitative risk analysis tool, with a high take-up in all industries.

- Bowties are primarily barrier based analysis diagrams, with strong involvement and input from workshop participants. Unlike many traditional hazard registers, risk assessment teams using Bowties are visually informed by the one-to-one links between Threats (or Consequences) and the specific barriers that prevent or mitigate the events.



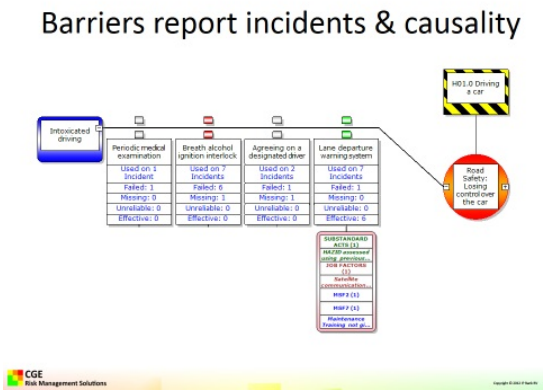
- As the focus of efforts to manage risks, barrier analysis requires some level of detail. BowTieXP and its modules have an infinite capacity to store optional detail on barriers. With the ability to selectively display all, none or any level of detail in between, BowTieXP assists the risk professional to comprehend the efficacy and performance expectations of each SCE via a range of attributes some of which are listed here and shown in the diagram below:
  - Type
  - Independent protection layer, or system
  - Criticality
  - Responsibility for the barrier and supporting activities from the Management System
  - Effectiveness (can be a product of defined factors such as reliability, availability, etc.)
  - Strengths and weaknesses (how the barrier might be compromised)
  - Supporting systems (escalation factor barriers and activities, documents, etc.)
  - Historical and current reliability (especially via the Audits and Incidents recorded on each barrier)
  - Customizable user-fields

The diagram below shows some of the detail that can be recorded and displayed.

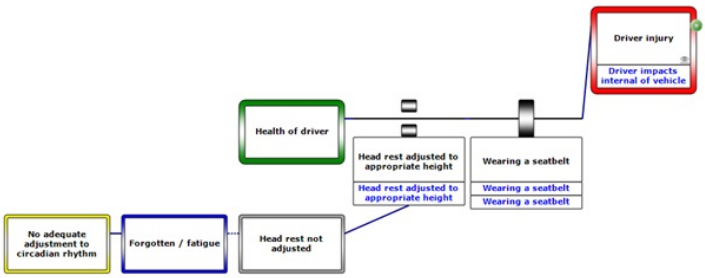


- We all know barriers can fail, but the analysis and recording of this reality is rarely done. BowTieXP's escalation factors (as shown in the diagram as the yellow element) and compensating barriers provide the risk analysts to prepare for foreseen weakness and impairment in barriers.
- Digesting barrier performance is enhanced by the two latest functions available in the software.

- Allowing audit results and trends to be clearly displayed on the diagram or reported in detail in documents. A range of questions can be built in the AuditXP module, assigned to barriers. Custom surveys can be distributed and inputs recorded and displayed on each barrier.
- With the BowTieXP integratable IncidentXP, a timeline or storyboard is generated and events recorded, borrowing elements from the BowTie diagrams where applicable. Being able to match incidents on your BowTie barriers provides a powerful tool to prove to your stakeholders and regulator that you are managing and monitoring barriers for improvement. Although four different incident methods can be used, the following shows BSCAT (as per DNV's design) and Tripod Beta methods:



The Tripod Beta extract below has been drawn in BowTieXP, linking Consequences and Barriers, the performance of which can be included on the BowTie as above.



20 ALARP thinking

Prescriptive safety: Have we gone too far? (Risktec)

ALARP thinking

The principle of reducing risks ALARP (As Low As Reasonably Practicable) adds in to the mix a legal imperative for continuous improvement. In a nutshell, for new equipment the ALARP principle requires compliance with relevant codes and standards and adoption of good practice elsewhere as a minimum, together with consideration of options for improvement, which can only be discounted if the time, trouble and cost are grossly disproportionate to the benefit. If these improvements are subsequently enshrined in updated standards or deemed to be relevant good practice, this becomes the new baseline.

The problem is compounded when more and more preferential requirements are added into standards by well-intentioned technical authorities – something that is quite common in large operators with their own engineering standards. The standards can be come complex, difficult to comply with and may even lead to design solutions where the associated safety risk is actually higher than a simpler, cheaper design based on inherent safety thinking. Moreover, it is difficult to see how raising standards ad infinitum is sustainable, economically speaking.

Quite clearly, the solution to this conundrum is to think hard about the potential applicability of

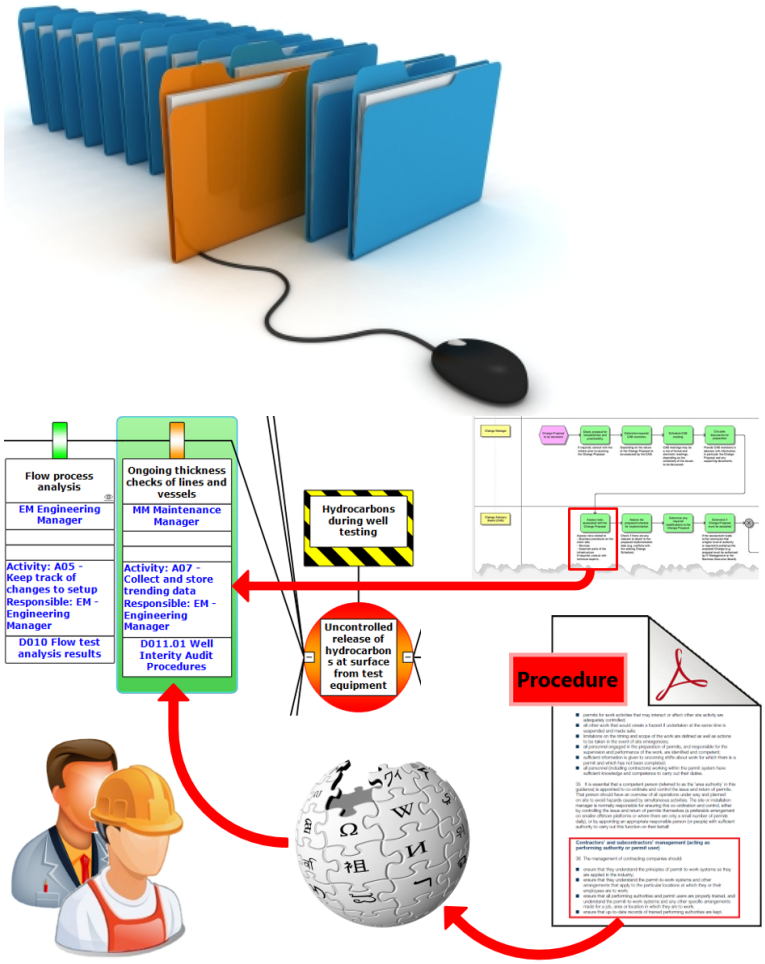
standards and make clear the distinction between essential and nice-to-have requirements in varying circumstances. At a high level this could take the form of specifying when certain standards as a whole apply (and when they don't). At a more detailed level, with in standards themselves, there is plenty of scope for spelling out any relaxations or offering alternative risk-based avenues of compliance.

Conclusion

In a world where spiralling costs in the name of safety are a recipe for project cancellations, the clear message to operators and professional bodies is to build risk-based flexibility into otherwise black and white standards.

21 Contextual Information Management

Linking the "paper" compliance world to "real" barrier based risk management



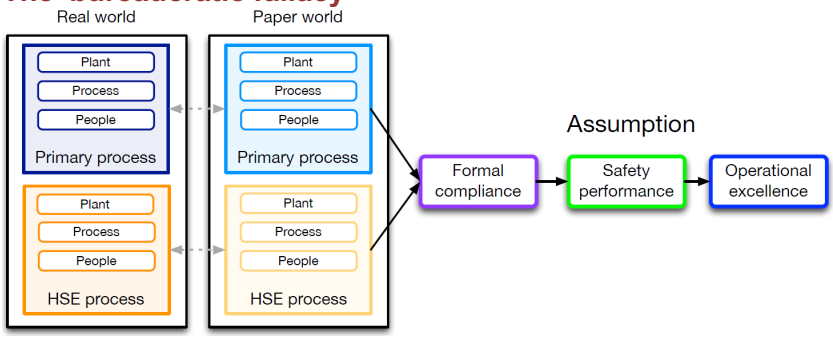
The release of BowTieServer includes a contextual 'wiki based' information management system, as an integral part of BowTieServer. The BowTieServer Wiki allows documentation to be integrated into risk management.

Instead of having separate documents floating around, the documentation can be part of the bowties and linked to specific sections or even paragraphs.

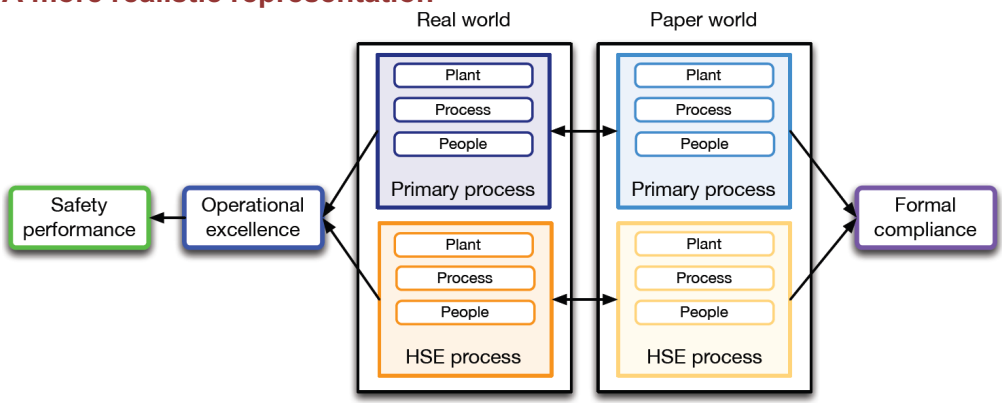
This approach means that the "paper" risk compliance world and the "real" barrier based risk management world is connected in such a way that all people that deal with risks in organisation understand how processes are related to barriers, threats, hazards,

consequences, responsible people, relevant activities and procedures. This approach creates the ideal situation, see below.

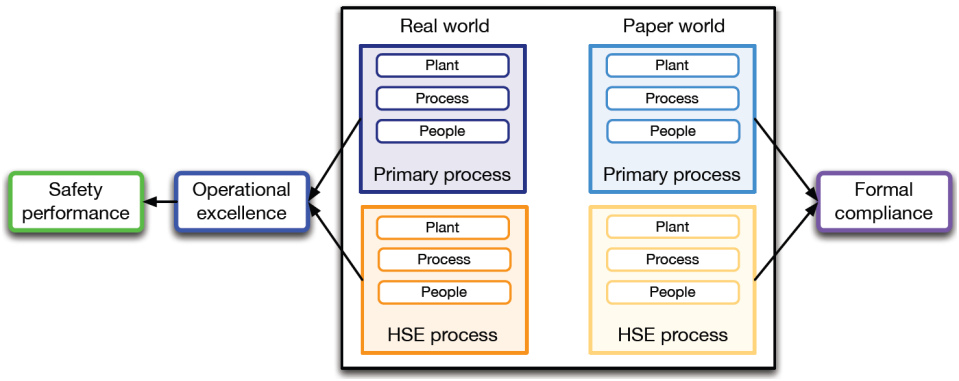
The 'bureaucratic fallacy'



A more realistic representation



The ideal situation



22 Making risk data useful for all layers in your organisation

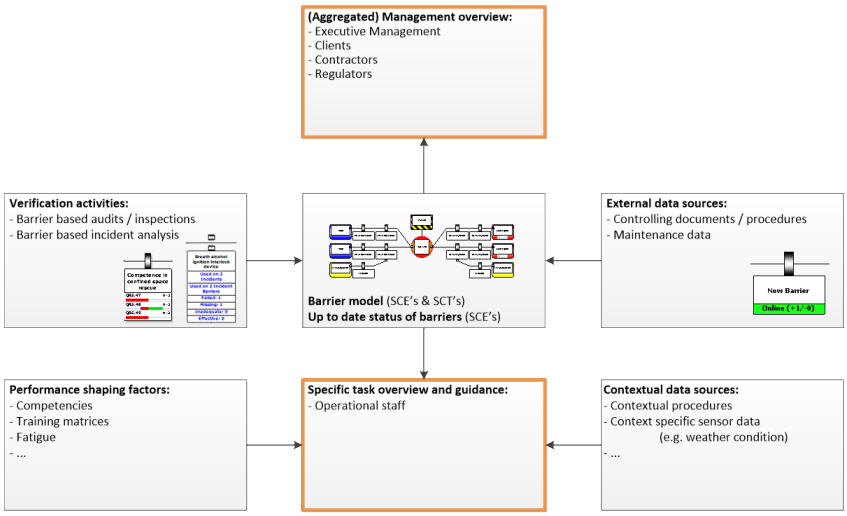
People with different positions need different risk information. Senior Management shouldn't be bothered looking at nitty gritty details, while on the other hand these are the details that operational personnel actually needs to be able to execute their job. This is one of the challenges that will be resolved by BowtieServer: making the same risk data useful for different type of users.

Barrier Management

For many years already the 'BowTie' method has been acknowledged as the only method that provides real insight in risks. Risks that can affect performance and assets as a whole. Risk Management is a way to assess risks and act on these assessments on a day-to-day basis to get better insight, provide assurance, avoid incidents, improve efficiency and deliver better quality. Central in this approach are 'barriers'. Barriers can be seen as critical controls to make

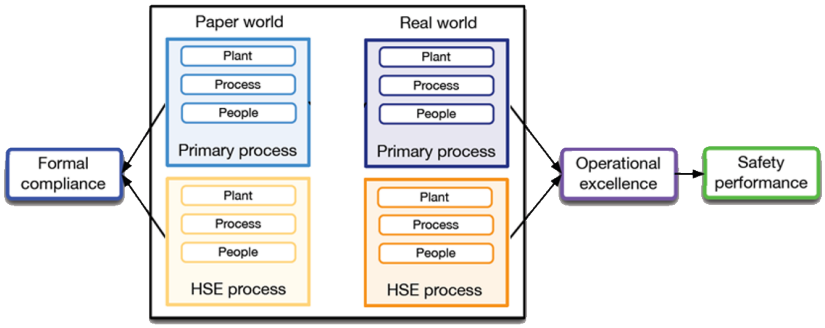
sure that processes go as intended, or as a safeguard to mitigate consequences and regain control if a process is compromised.

This approach is commonly referred to as 'Barrier Management'. Nowadays this approach is not only applicable for subject matter experts, but also for operations, frontline people and everyone who is responsible and accountable for the operations from a management perspective. Understanding what critical barriers are, and what the status is of these barriers, is the only way to make informed decisions. Decisions if it is safe to operate, decisions what needs to be done to improve the management system, decisions how to conduct daily tasks and decisions to work more efficient in the SJA/tool box meetings.

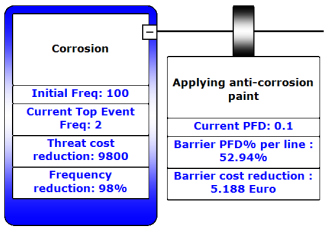


Integrate Barrier Management with Compliance

Barrier Managements also allows for reducing instructions, guidelines and procedures (controlling documents), providing the workforce with only those procedures and work instructions that matter for working in a safe and efficient manner. It enables you to utilize incident analysis to improve normal operations, conduct smarter audits and inspections, and to integrate compliance (safety cases) with 'real' operations.



Barrier Benefit Analysis



Some of the most asked questions about risk management are “how do we know whether we save money by controlling and mitigating our risks?” and “does adding more barriers still add significant value to our risk reduction?“.

The bowtie cost-benefit analysis automatically calculates how much money you are expected to save by implementing a barrier. The calculation is based on initial threat frequencies, probability of barrier failures on demand (PFD’s) and incident (consequence) costs per occurrence.

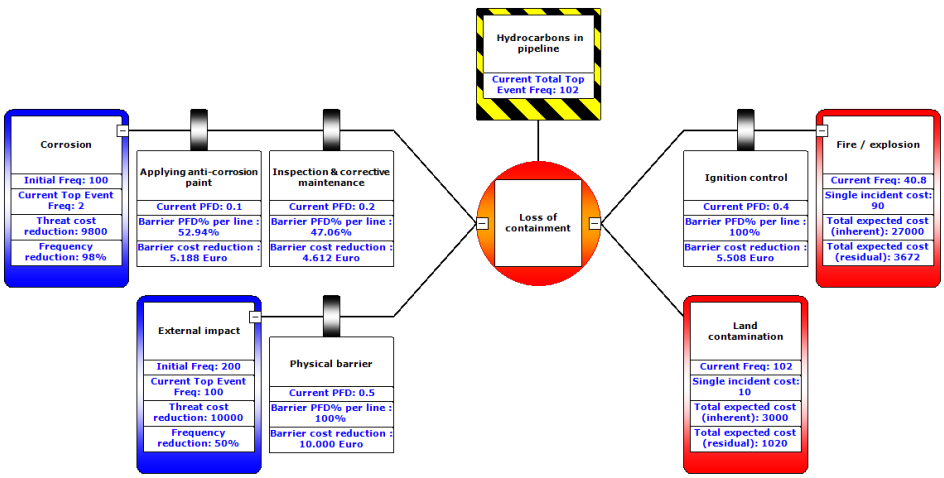
When barriers are added or values (e.g. initial frequencies) are changed, all outcomes will be recalculated and updated automatically. This creates new insights, e.g.: it becomes clear that certain threats need more attention, or some earlier implemented barriers can suddenly become not profitable anymore.

Additional interesting variables

- Barrier cost reduction
- Inherent expected incident costs (without barriers)
- Residual expected incident costs (including barriers)
- % risk reduction per threat
- % influence barriers per threat line

Possible future extension variables

- Barrier costs (design / implementation / maintenance / re-activation)
- Future calculation (in line with LOPA plugin)
-



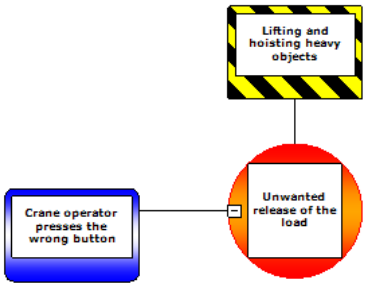
23 Human Error in BowTies

How human factors & human error can be taken into account in the bowtie method

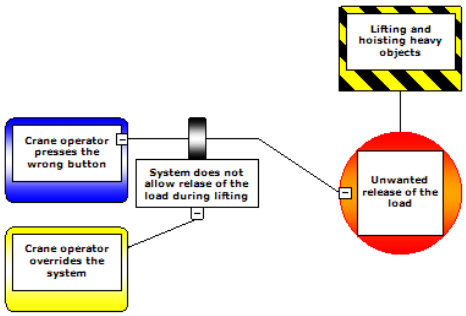
Human factors & human error can negatively influence safety in complex industries, activities and processes. This means that human factors & human error need to be considered in bowtie risk assessment; otherwise you are lacking and ignoring crucial information. In this section, a common pitfall with the inclusion of human factors & human error into the bowtie method is discussed and useful guidelines are proposed in how human factors & human error can be effectively included in bowties.

In bowtie risk assessments, human factors & human error can be found in two places:

- Threats: human factors or human error appear as a threat in a bowtie when the human act or condition is able to directly cause a top event.
- Escalation factors: human factors or human error can appear as an escalation factor in a bowtie when the human act or condition can defeat or reduce the effectiveness of a barrier.



Relation of human factors & human error with threats

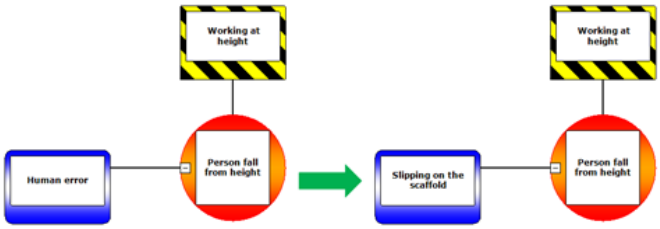


Relation of human factors & human error with escalation factors

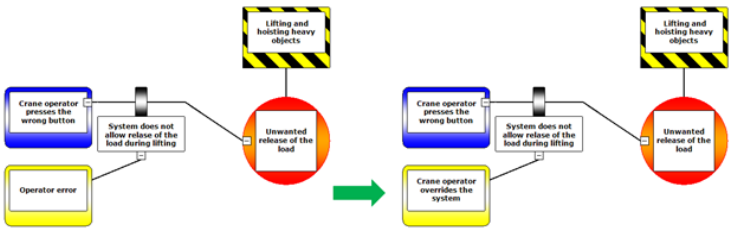
There is a common pitfall for including human factors & human error into bowties for both the threat and escalation factor element. The common pitfall is that human factors or human error is described in generic terms, such as ‘Human factors’, ‘Human error’ or ‘Operator error’. Ultimately they might be true, but it does not add a lot of context or extra information to the bowtie. Moreover, the generic terms for describing human factors & human error often results in the identification of generic barriers and recommendations such as ‘Training’ and ‘Procedures’. Therefore it is useful to define which specific human act or condition can impact

the bowtie scenario to add value to the bowtie. This pitfall can be circumvented by describing the human act or condition that could cause the top event or by describing the human act or condition that defeat or reduces the effectiveness of the barrier.

Including and describing more specific human factors & human error with the guidelines outlined in this section, will help to identify specific barriers and recommendations to improve safety. Also, this approach facilitates risk communication since the information is more explicit which makes it easier to comprehend.



Improving the bowtie risk assessment by describing the human act or condition that could cause the top event instead of a generic term



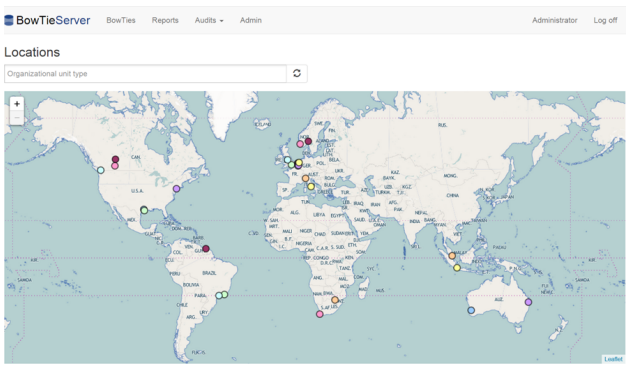
Improving the bowtie risk assessment by describing the human act or condition that could defeat or reduce the effectiveness of a barrier instead of a generic term

The impact of using the guidelines in this section (making it easier to identify specific safety measures & the diagram is easier to understand)

BowTieServer

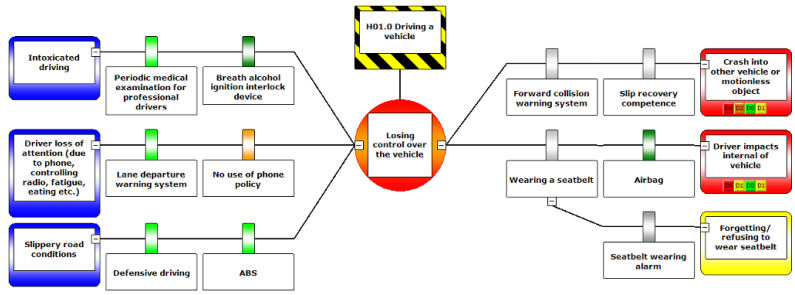
Bringing BowTies to the Enterprise

BowTieServer brings BowTie related information together. For the first time, company-wide information is combined to gain a higher level of insight into barrier-based risk management.



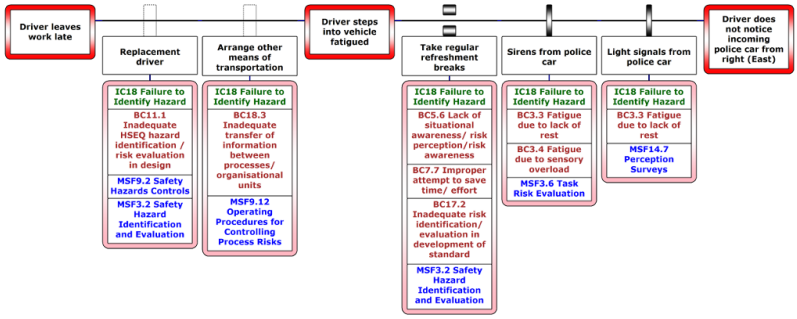
BowTieXP

Visual Risk Assessment



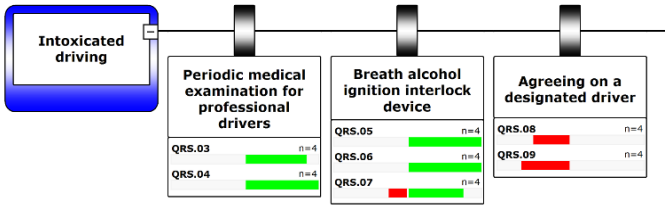
IncidentXP

Analyse incidents with BSCAT, Tripod Beta, Barrier Failure Analysis or RCA



AuditXP

Use your BowTies for Audits



Incident analysis by Kelvin TOP-SET

i³Investigator 3

BlackBox

Two primary types of barrier: hardware barriers and human barriers.

Hardware and human barriers are put in place to prevent a specific threat or cause of a hazard release event, or to reduce the potential consequences if barriers have failed and an event has occurred.

Both hardware and human barriers are supported by the processes and procedures contained within the Management System Elements, such as those in the Operating Management System in Report 510 [2].

24 Incident Analysis Methods

This article gives an overview of the 'best practice' incident analysis methods used in different industries. These methods are:

- Root Cause Analysis (TOP-SET)
- The "5 Why" Method 3. BlackBox Analysis Diagram 4. Tripod Beta
- 5. Incident BowTie 6. Fault tree
- 7. Event tree
- 8. Systematic Cause Analysis Technique (DNV SCAT)

What are incidents?

An incident is an unplanned event or chain of events that results in losses such as fatalities or injuries, damage to assets, equipment, the environment, business performance or company reputation. A near miss is an event that could have potentially resulted in the abovementioned losses, but the chain of events stopped in time to prevent this. These incidents can be classified in all kinds of severities and types, and thus into categories. Investigation and cause analysis should take these different categories into consideration.

TOP-SET® Root Cause Analysis

Root Cause Analysis is the drawing of a diagram in which the relationships between the causes of an event are displayed. The method is aimed at finding the Root Causes of the event. By solving the problems described in the Root Causes the probability of the incident (and other events that have the same Root Causes) reoccurring is lowered. This will prevent the incident from happening again. The Root Causes Analysis diagram makes a distinction between three types of causes: Immediate Causes, Underlying Causes and Root Causes. The investigator moves through these causes by asking 'Why?' until the level of the 'Root Causes' is reached. The answer to the 'Why?' question is the next item in the diagram. This creates a Cause-Consequence tree that can resemble an Event tree.

The TOP-SET® method is based on the Root Cause Analysis method. This incident investigation methodology, in which the Root Cause Analysis method is part of TOP-SET® incident investigation methodology, was developed in 1988. The method entails a best-practice way of doing incident investigation based on years of experience in incident investigation for companies worldwide. It incorporates both incident investigation and the analysis of components to form a complete investigation process that takes the investigator from developing a team, gathering data, and investigating to generate evidence, to interviewing witnesses, analyzing evidence, preparing recommendations and actions, and reporting. The method is used in over 30 countries in many industrial sectors, including oil and gas production, explosives, and the rail transport and maritime industries.

The "5 Why" method

The 5 Why method is a way of conducting incident analysis which is originally developed in the 70's by Sakichi Toyoda and was later used within Toyota Motor Corporation during the evolution of their manufacturing methodologies. It is a simple but effective method to find the cause of incidents.

The 5 Why method is a question-asking method that is used to understand the cause/consequence relationships that underlie a particular problem. The ultimate goal of applying the 5 Whys method, is to determine a root cause of an event or problem. The idea is

to ask the question why the event happened and to ask why for that answer as well until you reach the root cause of the event.

Originally the method prescribes that five iterations of asking why is generally sufficient to get to a root cause. But nowadays a sixth, seventh or even greater level is used as well. The purpose remains to find the root cause to the original event through any amount of levels of abstraction and to encourage the user to avoid assumptions and logic traps. The answer to the last question, or the root cause should always be an organizational factor on a systemic process level. To reach this level it is advisable to ask the question 'Why did the process fail?' instead of asking the question 'Why?' when the fifth level is reached. The background thought in the 5 why method is: "People do not fail, processes do!". This method is closely related to the Cause & Effect (Fishbone) diagram.

BlackBox Analysis Diagram

The Root Cause Analysis method that is used in the TOP-SET method (See 3.1 Root Cause Analysis (TOP-SET®)) is changed and simplified for the use in the BlackBox tool. BlackBox is a software tool that guides you through all phases of incident analysis. The tool is used for reporting smaller, low risks incidents or near misses and to analyze the underlying causes. The program consists of a fixed workflow which leads you through all these steps to make a complete incident report. It is designed in a way that makes sure all fields are filled in to get standardized reports that contain the same sections. This gives more guidance and makes it easier to make quick but accurate analyses.

TOP-SET incident investigation BlackBox is based on the TOP-SET® incident investigation and analysis methodology. This method threats the incident as a system that the organization has lost control over. Something needs to be different or changed from the situation before to get the system out of balance. The dynamics of a system can be expressed in different components. TOP-SET has identified six elements to investigate what has caused the incident: Technology, Organization, People, Similar Events, and Environment that are displayed against Time (the acronym of the word TOP-SET). The cause of the incident can be found in at least one of the five elements but most likely in an interaction of more than one element. The Time element can be a check on the causality of the facts found in the other five elements. In BlackBox the Time element is used in the 'Sequence of Events' step in which Events and their time before incident can be identified. The elements Technology, People, Organization and Environment are used in the Incident Analysis. At least one of these elements should be worked out in order to find the underlying causes. The element 'People' is in red in the Figure below because this element always plays a role in every incident.

In the BlackBox Analysis investigation diagram you analyze at least one of the four elements of the TOP-SET method that you feel played a role during the incident: Technology, Environment, Organization and People. For each of the chosen elements an analysis is made. This analysis per element consists of minimal 3 maximal 5 items containing Immediate Causes, Missing Barriers and Underlying Causes.

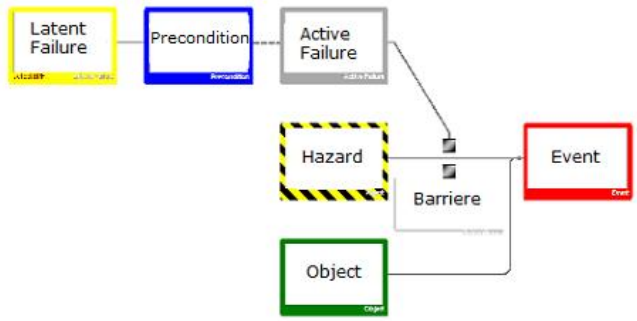
The analysis starts with a single Immediate Cause that triggered the incident directly. The reason for the Immediate Cause to occur is the next item; the Missing Barrier. After the Missing Barrier has been identified the reason for this barrier to fail is explained by the Underlying Causes. You need to analyze at least one with a maximum of three Underlying Causes. All the causes in the diagram should be linked with a generic cause from a predefined list. The four elements and the Immediate Causes and Underlying Causes all have their own generic cause's lists, making eight different lists. Therefor the analysis will contain a specific description of the user and a linked generic cause. The generic causes of different incidents can be compared with each other because they are all picked from the same list in BlackBox. The different generic causes can be counted to make a trend analysis.

Tripod Beta

The Tripod Beta method was developed on the bases of research done in the late 80's and early 90's into human behavioural factors in incidents. The research was commissioned by Shell International and executed by the University of Leiden and Victoria University in Manchester. The research question was: 'Why do people make mistakes?' The answer to that question was because organizations expose them to an imperfect working environment. This does not mean people will not make mistakes when they work in a 'perfect' working environment, but it is the aspect were organizations have control over and therefor can make changes for improvement.

The Tripod Beta method analyses which barriers have broken during an incident, the error or mistake made, the working environmental aspect that encouraged this and finally the latent failure in the organization that caused that mechanism. A Tripod Beta analysis process follows three steps:

- Identify the chain of events preceding the consequences
- Identify the barriers that should have stopped this chain of events
- Identify the reason of failure for each broken barrier. This should be broken down in the human failure (Active Failure), the working environmental aspects (Preconditions) and the Latent Failure in the organization.



For the identification of the reason why the barriers broke the Human Error theory is kept in mind. It is investigated what error was made, what failure in the working environment caused this and what latent failure caused this to be present. The core of a Tripod analysis is a 'tree' diagram representation of the incident mechanism which describes the events and their relationships.

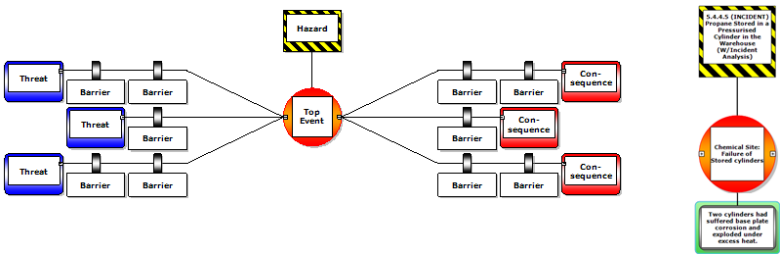
Incident BowTie

The 'Incident BowTie' method was developed because there was a demand for doing incident analysis within the BowTie diagram. The BowTie diagram contains a lot of information about the ways incidents can happen and how to prevent them. Therefore to add information about actual incidents has a lot of added value. This information can 'prove' the effectiveness of barriers and the prevalence of Threats, TopEvents and Consequences. Incidents can also point out if there are any holes in the risk analysis; if all the scenarios are covered. In the Incident BowTie method all this information is displayed in one diagram.

The 'Incident BowTie' analysis method combines two analysis methods; BowTie risk analysis and Tripod incident analysis. The method brings the advantages of both worlds together. The information from the BowTie analysis can be used as input for the incident analysis, viewing it from a broader perspective and making sure all the possible scenarios are taken into account. The input from the Tripod incident analysis can be used to make the BowTie analysis more realistic and up to date, using real-life data. It creates an extra layer in the BowTie diagram, making it possible to add more specific information to the risk analysis. The two methods have

an important similarity in the analysis technique; the barriers. For both methods barriers are used to show what is done to prevent incidents or events (BowTie) or to show where the failures lie (Tripod). To build an 'Incident BowTie' diagram the items from both methods are connected on the level of the barriers, making it possible to collect information about those barriers from two viewpoints.

An incident can be mapped on an existing or developed BowTie risk analysis diagram. BowTie risk analysis is a proactive method that maps different risk scenario's making a visual representation of a hazard and how you can lose control over the hazard. The diagram contains a left side which represent all the scenarios (the Threats) that can lead to the TopEvent, which is the moment control is lost over the Hazard. The right side of the diagram represents all the scenarios that can lead from the TopEvent (the Consequences). For each scenario barriers are used to show how loss of control is prevented. Control measures show how Threats can be prevented and recovery barriers show how Consequences can be prevented.



The BowTie method is mentioned in the guidelines of the International Association of Drilling Contractors (IADC) as a preferred way of doing risk analysis and is therefore used in a lot of oil and gas companies. These companies make use of their pre-defined BowTie risk assessments to map incidents on. This is possible when the BowTies are virtually complete which allows for barriers from the incident analysis to translate to the barriers mentioned in the BowTie. For companies that do not have such risk assessments predefined when an incident happens, the Incident BowTie method is more difficult to apply. Making a BowTie risk analysis after an incident has happened narrows down the free thought process that is necessary to point out all the possible scenarios in a BowTie diagram.

SCAT

The SCAT analysis method is developed by DNV risk consultancy about 20 years ago as part of the ISRS (International Safety Rating System) guidelines. The SCAT version that corresponds with the 6th version of the ISRS is discussed below. This version addresses a full range of loss control events, however it focuses explicitly on occupational health and safety incidents. The newest version of the SCAT method following ISRS 8 will be discussed in the next section.

SCAT (Systematic Cause Analysis Technique) is a widely used methodology for structured analysis of incidents. It is a vertical root cause analysis approach that incorporates the DNV 'Loss of Causation Model'. The analysis is based on predefined categories of loss events, their potential direct and basic causes and guidance towards a management system structure for actions for improvement. The SCAT method guides the user systematically to work backwards from the loss to identify where the organization lacks control over deficiencies that led to the occurrence of the incident.

A good preparation before building the SCAT diagram is to make a timeline of the incident. This will help getting a good overview of the events that occurred during the incident. The timeline is then broken down in different sections; choosing the key events that will be analyzed in the SCAT diagram. When the Events are chosen a cause path is foll owed that explains why the incident happened. The cause path consists of five items: the Loss, Event,

Direct Cause, Basic Cause and Lack of Control. A Loss is the main consequence of the incident. It represents an unintended harm or damage, for example damaged equipment, a broken arm, loss of production, etc.

A SCAT analysis can only have one Loss. When the user wants to analyze more Losses, multiple SCAT diagrams need to be made. A Loss can be the result of one or more Events. An Event is a happening or a moment in which the state of the incident changes. Each Event is analyzed with a cause chain of three cause types. The Direct Cause is a substandard act or substandard conditions that triggered the Event. Examples are:

- Inspection not performed by new employee
- Failure to secure lift
- Safety valve is broken
- The Basic Causes include personal and job or system factors that together made it possible for the Direct Cause to occur. Examples are:
- Maintenance department understaffed
- High workload
- Wear and Tear

A Lack of Control factor can be inadequate program standards or compliance to standards that cause the Basic Causes to occur. These factors always act on an organizational latent level. They will influence a range of unsafe conditions and can therefore cause different incidents. Examples are:

- Inadequate leadership
- No task or risk assessments
- Lack of training

These causes can be defined specifically in one's own words or with use of the DNV SCAT chart. This chart gives a list of generic descriptions for each of the causes. Picking the descriptions from the SCAT chart can be very useful when comparing different incidents. Every user will pick from the same list for every incident. For each cause level there can be multiple items per incident explaining the event. Actions for improvement can be made on every cause level, but will be most effective on the Lack of Control causes because these will address the latent failures in the organization.

For more information on any topic in this document contact:

Albert C vd Vyver
Specialist Member IRM:UK
Mobile Contact: (+27) 798722978,
E-MAIL: sherisk@telkomsa.net
Fax: +27 867517119

OR

CGE
Risk Management Solutions
Vlietweg 17 V
2266 KA Leidschendam
The Netherlands
Tel: +31 (0)88 100 1350
Fax: +31 (0)88 100 1349
www.cgerisk.com

Rabobank / IBAN: NL42RABO0106273760
KvK no: 27379386
VAT no: NL822367026B01
BIC: RABONL2U

CGE Contact person: Pierre Eijkelboom

Phone: +31 (0) 88 1001 350
Email: p.eijkelboom@cgerisk.com