BowTieXP

The next generation BowTie methodology tool

Bowtie Methodology Manual

Revision 15 (27-Mar-2015)

Please note that this documentation is preliminary and subject to change without notice. The latest version of this document can be obtained via CGE (e-mail support@cgerisk.com).

Comments

Please direct any comments, questions and other feedback to Arjan Zipp (a.zipp@cgerisk.com).

Copyright

Terms and conditions for using this document

The copyright of this software manual and training guide (the document) belongs to IP Bank B.V. who has empowered CGE Risk Management Solutions B.V. to provide this document to the market.

This document and/or any part of the document may only be used for training in the BowTieXP software tool and methodology. It may not be used for methodology-only training or training with respect to any other tool or methodology.

This document and/or any part of the document must always be accompanied by these terms and conditions. Without them, any possession and/or use of this material is illegal.

This document may not be published on a public download location; Value Added Resellers (VARs) may provide this document in print and/or in PDF format only and at no cost. Only VARs may distribute this document and only to their leads and customers, none of whom may be a competitor of CGE and/or IP Bank.

This document may only be provided by official VARs of the BowTieXP software tool. Check the list of VARs on the www.bowtiexp.com website before using this document. If this document has not been provided to you by an official VAR, please report this to us immediately by e-mail on support@bowtiexp.com.

“All models are false, but some are useful.”

- George Box -

Table of Contents

List of Figures

1
Introduction

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.

1.1. Purpose and structure of this document

This document aims to educate the reader on the bowtie method as it is used in the industry at the moment. It is both a practical reference for everyday users of the method and a theory guide. This means that theoretical concepts are elaborated with practical tips and examples on how to use the method.

Chapter 1 (this chapter) contains a quick overview of the elements in a bowtie diagram. The rest of the manual will go into more detail on each concept. Since some subjects interrelate, a quick introduction allows you to read this manual in order without getting confused. However, it is advised to revisit chapter two and three after you have become intimately familiar with all the details of the method.

Part one – High level discussion

Chapter 1 - Introduction (page 7) gives an overview of this document and quick introduction to the bowtie terminology. You are reading this chapter now.

Chapter 2 - Discussion of related methods (page 12) explores similarities and differences with related methods, and lists advantages and disadvantages of the method compared to these other methods.

Chapter 3 - The application of bowties, today and tomorrow (page 16) discusses current use of bowtie diagrams and explores future opportunities for improving safety.

Chapter 4 - Before getting started, this chapter (page 17) gives tips on determining the scope of a bowtie project and things to do before doing a bowtie workshop.

Part two – Building bowties

Chapter 5 - Building a Bowtie (page 20) contains an in-depth discussion of all elements, how they interrelate, examples of each, tips and pitfalls. This section is the main body of this document.

Part three – After building bowties

Chapter 6- Risk evaluation (page 56) is about demonstrating ALARP and making an improvement plan once the bowties are finished.

Chapter 7 - Bowtie implementation (page 60) gives some tips on ways to implement the bowtie once the project is done.

1.2. General

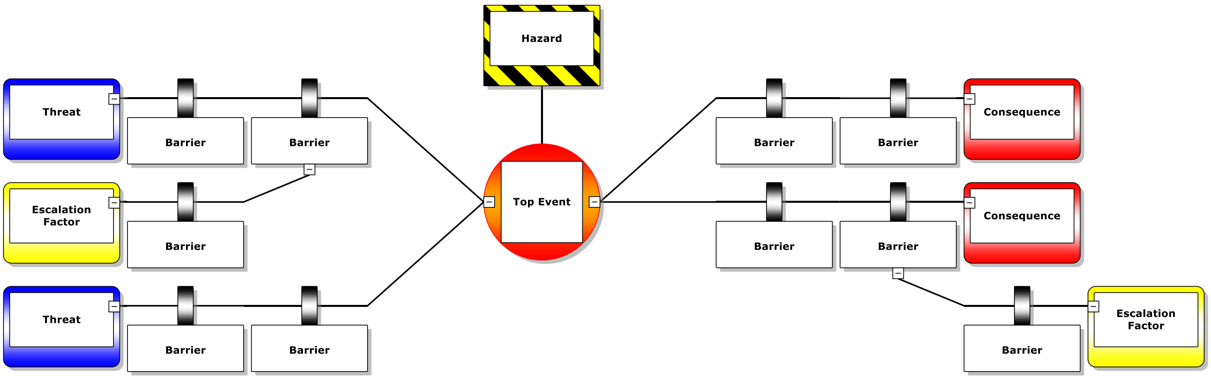


Figure 1 - A bowtie diagram showing all elements

The bowtie method is a risk assessment method that can be used to analyse and communicate how high risk scenarios develop. The essence of the bowtie consists of plausible risk scenarios around a certain hazard, and ways in which the organisation stops those scenarios from happening. The method takes its name from the shape of the diagram that you create, which looks like a men's bowtie.

The bowtie method has several goals:

- Provide a structure to systematically analyse a hazard.
- Help make a decision whether the current level of control is sufficient (or, for those who are familiar with the concept, whether risks are As Low As Reasonably Practicable or ALARP).
- Help identify where and how investing resources would have the greatest impact.
- Increase risk communication and awareness.

The next section will introduce the elements that make up a bowtie diagram. Building a bowtie happens in the same order.

Example - lion in a cage: An example will also be worked out to illustrate the elements. Say you are the general director of a zoo. Your zoo is an organization that earns its existence by exhibiting animals to the public. Like every organisation, your zoo is subject to certain risks that originate from your business.

1.3. Step one - Identify hazards

A bowtie starts with a hazard we want to analyse. The word ‘hazard’ has a negative connotation in daily life. In the bowtie method however, hazards are part of normal business and are often also necessary to run a business. What makes a hazard special is that this part of the business introduces the possibility for harm to occur. Most hazards are introduced into an organisation for good reasons, otherwise they could simply be eliminated and no harm would be possible. Hazards can be operations/activities (operating rotating machinery, driving a car), substances (chemicals, hot fluids, etc.) or situations (a load suspended at height) we deal with in the normal processes of our business. As long as these hazards are under control, they will not cause harm, but they introduce the potential for harm.

Example - lion in a cage: One of the obvious sources of risk is that we have dangerous wild animals in our zoo. They are a part of normal business, without them we would not have a zoo, and as long as they are controlled, we are fine. Let us take a lion as an example.

1.4. Step two – identify top events

When control over a hazard is lost, it is usually possible to identify the moment when a normal situation changes to an abnormal situation. That point is called the top event in bowtie and is also the centre event of the diagram. The top event is not a catastrophe yet, but the company is now exposed to the potential harm of the hazard. It should be possible for the organisation to bring the situation under control again. If control is regained after the top event has occurred it will be thought of as a close call that could have led to more serious unwanted events.

Example - lion in a cage: We could lose control over these animals – they might get out the cage. If our lion escapes, we can face potential consequences.

1.5. Step three – identify threats

There are often several factors that could cause the top event. These are called threats in the bowtie. Threats lead directly to the top event and should be able to cause the top event independently.

Example - lion in a cage: How could our lion escape? On the one hand, the cage itself might fail – allowing the lion to escape. But maybe a mistake was made and the cage was left open/unlocked.

1.6. Step four – identify consequences

When a top event has occurred it can lead to certain consequences. Consequences are unwanted scenarios that could be caused by the top event. They should be realistic and specific. Consequences are mainly unwanted because they will lead to loss or damage.

Example - lion in a cage: If the lion gets out, we can face a multitude of consequences – the lion might attack and injure the public. At the very least we will get a lot of negative press, leading to a bad reputation and loss of revenue; we might even need to close.

After these four steps, our diagram looks like this:

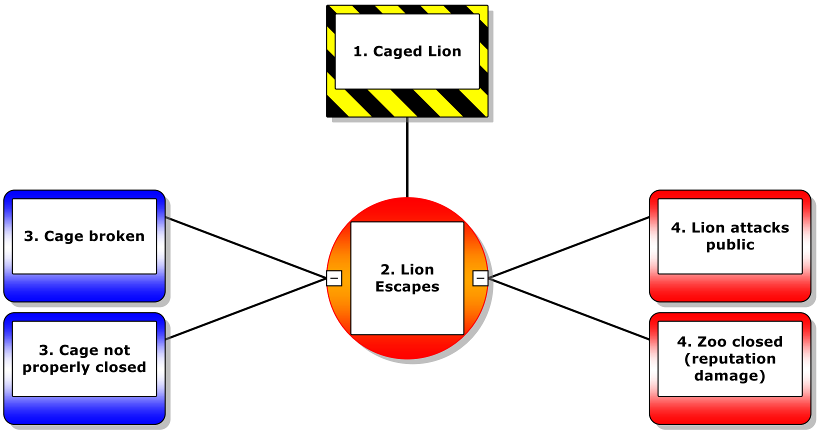


Figure 2 - Scenarios around a hazard and top event

1.7. Step five and six – identify preventive and recovery barriers

Risk management is about controlling risks. This is done by implementing barriers to prevent certain events form happening. A barrier (sometimes also called a control) can be any measure taken that acts against some undesirable force or intention, in order to maintain a desired state. Barriers can be hardware systems, design aspects, human behaviour and so on. Barriers are placed on both sides of the top event. Preventive barriers on the left side of the bowtie prevent the top event from happening. Recovery barriers on the right side of the bowtie can either prevent the top event from resulting in unwanted consequences or mitigate further consequences.

Example - lion in a cage:
There are two threats in our example and we can think of barriers for both. The first threat is a broken cage. To prevent this we can make sure the initial design is correct to ensure a minimum level of quality. If the initial design is up to our standards, we also have periodic maintenance and inspection and a testing schedule. The second threat is not properly closing the cage door. To prevent the cage being improperly closed, we ensure we have competent zoo keepers, and we have self-closing gates.

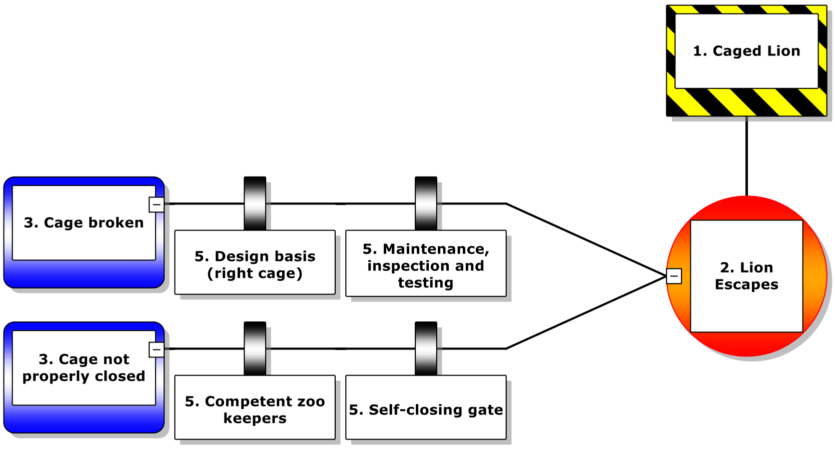

1. Caged Lion
3. Cage broken
5. Design basis (right cage)
5. Maintenance, inspection and testing
2. Lion Escapes
3. Cage not properly closed
5. Competent zoo keepers
5. Self-closing gate

Figure 3 - preventive barriers

There are also two consequences in our example that should have barriers. First, we want to know how to prevent or mitigate the lion attacking the public after it has escaped. To do that we have camera surveillance and escape alarms. We also have a search plan and dart gun to find the lion as soon as possible and get it back into the cage. To prevent reputation damage possibly leading to closing of the zoo, we have a prepared spokesperson to address the press along with a prepared press release. We also have insurance to cover any losses (up to a point).

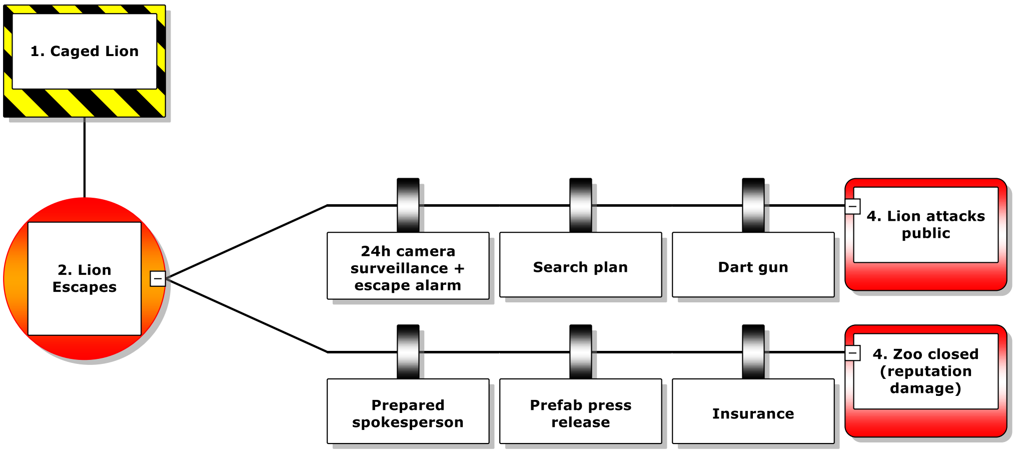


Figure 4 - Recovery barriers

1.8. Step seven and eight – identify escalation factors and escalation factor barriers

Once the control measures are identified, the bowtie method takes it one step further and identifies specific conditions or actions that make it more likely that a barrier will fail. These are called escalation factors. There are barriers for escalation factors as well. These barriers protect the main barrier from an escalation factor.

Example - lion in a cage: Our self-closing gate is reliant on mains power – if the power fails, our self-closing gate will not work. But then, if the power does fail, we have an emergency generator to ensure our safety systems keep working.

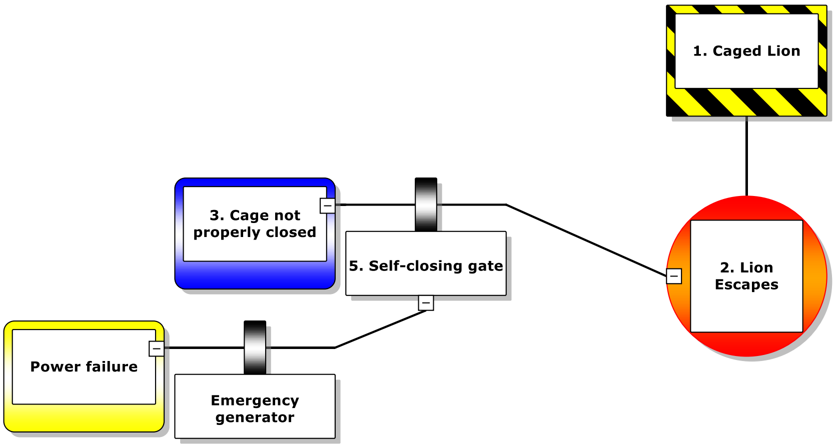


Figure 5 - An escalation factor and escalation factor barrier

And the complete bowtie diagram is now as follows:

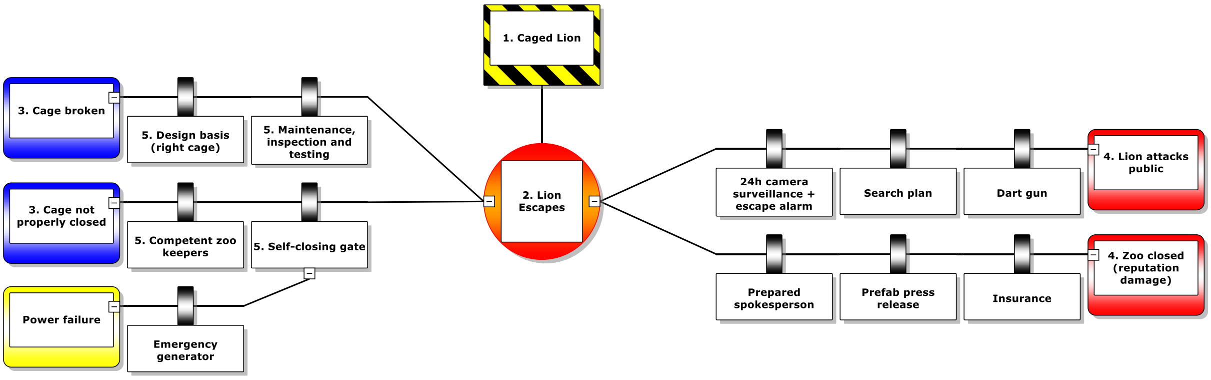


Figure 6 - Complete bowtie diagram

1.9. Next step after the basic bowtie

After creating the basic bowtie diagram, there are several ways to work out the barriers in more detail. One good way is to identify and link the underlying management system activities to the barriers. This will tell you what should be done to keep the barriers working, like maintenance activities on hardware barriers. Mapping the management system onto a bowtie also demonstrates in more detail how barriers are managed by a company. Furthermore, responsibilities could be attached to barriers, as well as a rating of their effectiveness and what type of barrier it is. We could also indicate which barriers are critical, so we can do our best to ensure they are always available.

2
Discussion of related methods

What relations do bowties have with other well-known analysis techniques? What is similar? What is different?

2.1. History and rise to popularity

It is said that the first ‘real’ bowtie diagrams appeared in the Imperial Chemistry Industry (ICI) course notes of a lecture on Hazard Analysis (HAZAN), given at the University of Queensland, Australia in 1979, but how and when the method found its exact origin is not completely clear. ICI was a British chemical company which has introduced major changes in process safety, a number of which were adopted by many companies (such as HAZOP and HAZAN). The company was later acquired by Akzo Nobel and Huntsman Corporation.

The catastrophic incident on the Piper Alpha platform in 1988 shook the oil & gas industry. After the report of Lord Cullen, who concluded that there was far too little understanding of hazards and their accompanying operational risks, the urge rose to gain more insight in the causality of seemingly independent events and conditions and to develop a systematic way of assuring control over these hazards.

In the early nineties the Royal Dutch / Shell Group adopted the bowtie method as part of the companies’ HEMP standard for analysing and managing risks (Zuijderduijn, 1999). Shell facilitated extensive research in the application of the bowtie method and developed a strict rule set for the definition of all items, based on their ideas of best practice. The primary motivation of Shell was the need for assurance that appropriate risk controls are consistently in place throughout all worldwide operations.

Following Shell, the bowtie method rapidly gained support throughout the industry because bowtie diagrams appeared to be a suitable visual tool to keep an overview of risk management practices, rather than replacing any of the commonly used systems. In the last decade the bowtie method also spread to industries outside of the oil & gas industry: aviation, mining, maritime, chemical, financial, judicial and health care to name a few.

2.2. Related methods

While the origin of the bowtie method itself is unclear, there were other methods and ideas at the root of bowtie thinking. So we do have some idea about what logically preceded the bowtie. There are three main methods which have relations to the bowtie methodology:

1. The first method is fault tree analysis which, in simplified form, corresponds to the left side of the bowtie. It shows how different scenarios can cause a company to lose control over its processes or hazards.

2. The second method is event tree analysis which, again in simplified form, corresponds to the right side of the bowtie. This side of the diagram shows what the consequences can be once control over a process or hazard is lost.

3. Barrier-based thinking. The fault and event trees have been simplified largely by adding the barrier concept. The best way to explain this concept is perhaps with the famous Swiss cheese model by James Reason, which originated in the early nineties. This metaphor of thinking about safety systems is not new – it has existed for a long time since before the bowtie model, such as for example in the nuclear industry’s defence in depth philosophy or Haddon’s 10 strategies for controlling energy.

The following pages will briefly explain these methods, what the differences are between these methods and how the bowtie relates to them.

2.2.1. Fault tree analysis

The fault tree method was created in 1962 at Bell Laboratories for failure modelling of ICBM launch control systems and quickly became a popular method for reliability and safety analysis, for example 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 with unwanted events, but it is possible to model any kind of causal relationship.

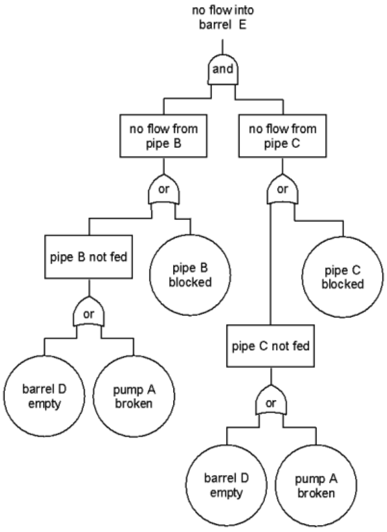


Figure 7 - A fault tree

Fault trees are often quantified with event probabilities and then used to calculate derived event probabilities.

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

The left side of the bowtie diagram corresponds with a simplified fault tree. The simplification lies in the AND/OR gates that are abstracted away, leading to a much simpler diagram with overall better readability and much higher communicative value. In bowtie the gates are replaced by independent barriers. Because of this change, it is more difficult to calculate probabilities in a bowtie. Also, the areas where bowtie diagrams are used most often tend to be more abstract and more focused on human behaviour. In this more abstract environment the information and statistics to reliably calculate is seldom available, due to the complexity and costs of testing and human influence on the system. This makes it very difficult to calculate reliable probabilities, even if one would do it with for instance a fault tree.

2.2.2. Event tree analysis

The event tree method is used to analyse event sequences following an initiating event. The method is widely used in many fields such as finance, economics, reliability, risk assessment and numerous other probabilistic types of analysis. Event tree analysis and fault tree analysis are closely related. Fault trees describe the necessary failures in order to reach a top event, whereas event trees model the potential outcomes. If quantified, it will also model the frequency of the outcomes.

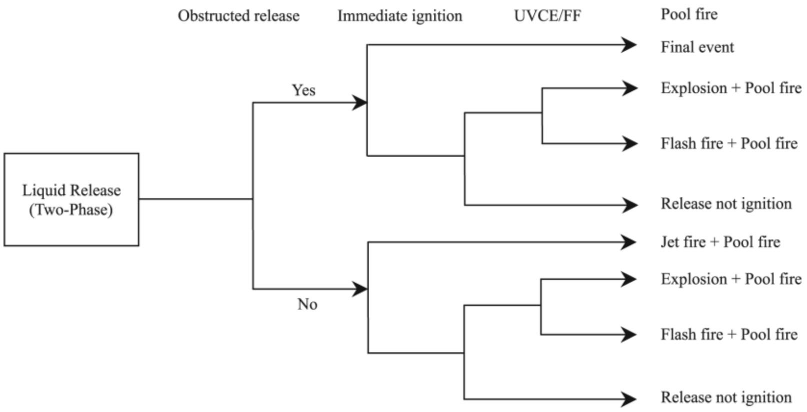


Figure 8 - An event tree

The right side of a bowtie diagram resembles a simplified event tree. Just like in the fault tree / left hand side of the bowtie diagram, the level of detail to represent the interdependencies between parts of a system have been removed, leading to a much more readable diagram. This information is not needed, as the bowtie method is not looking for probability or frequency information but rather aiming at risk awareness and operational barrier management.

2.2.3. Barrier thinking

Barrier thinking can be traced back to at least the 60’s when the nuclear industry started using the ‘defence in depth’ philosophy – multi-layered, redundant protection systems. This is essentially the same as the barrier concept. Haddon and Gibson were two other pioneers who firmly introduced the concept of controlling energy transfer in 1973.

However the most famous barrier metaphor is without question the Swiss cheese model of psychologist James T. Reason, who in 1990 proposed the Swiss cheese metaphor as an accident causation model. Reason hypothesized that hazards are prevented from leading to losses by a series of barriers. According to him these barriers are never 100% effective. Each barrier has unintended intermittent weaknesses and, when they line up, a hazard can lead to losses. This explains the reason for having multiple barriers, instead of one that is 100% effective.

To help explain the barrier concept, he compared the barriers to slices of Swiss cheese with holes. The holes in the barriers are dynamic and continuously change in size and location. When holes in all the slices line up, the hazard (the arrow) can pass through these deficient barriers, leading to an accident (losses).

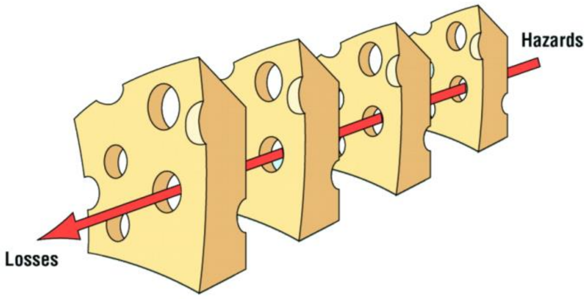


Figure 9 - The Swiss cheese barrier model

Identifying the barriers is central to the bowtie method. It takes what might seem like a large collection of disconnected safety measures and relates it to specific risk scenarios in manageable barrier chunks. This is very useful to allow more focused and detailed analysis on each part of safety in an organisation.

2.2.4. Escalation factors

The reasons why barriers have ‘holes’ can often be found in the organisation. For example cost & time cutting on maintenance management can eventually lead to the deterioration of the integrity of many hardware barriers within a system. In the bowtie method these weaknesses can be modelled as escalation factors. They are important tools, enabling organizations to gain insights to the specific conditions under which barriers are degraded or defeated. Escalation factors are another distinctive characteristic of the bowtie method that allows the analysis of barriers to go beyond just identification. It adds a failure analysis to a barrier.

This kind of subsystem failure analysis is also present in fault trees, but they are not explicitly isolated in the same way. Being able to concentrate on a single barrier failure allows problems to be divided into distinct manageable components.

2.3. Quantification vs. Communication

The previous sections introduced several methods that preceded the bowtie diagram, most notable fault tree analysis (FTA) and event tree analysis (ETA). It's important to understand these methods and the bowtie have different goals. Fault trees and event trees were created to quantify risk. The bowtie diagram on the other hand is meant to communicate the risk. These two goals influence so many decisions around how risks are analysed, that they automatically lead to different approaches and methods.

Obviously both goals are valuable in different areas. The quantitative FTA and ETA are typically used in detailed, technical systems oriented settings, where they work very well. Especially in design phases we need to know for example how thick a fire wall needs to be or how much time it takes for equipment or machinery to wear. The more specific and more isolated a system, the better we can calculate.

However, in more open operational settings with human and organisational influences, these methods are of limited value for two major reasons. First, FTA and ETA both become large and complex which makes them difficult to understand and use by people who did not initially create the analysis. Second, there are too many variables, interactions and unknowns to realistically run a FTA or ETA in an operational context. For example, we can place the exact same installation in different parts of the world, in different companies and have widely varying failure rates. How we treat our installations and processes, how our work-force and management make decisions cannot be quantified. The only way to manage these risks is qualitative.

The bowtie is on a higher level in order to work well in an operational context. It simplifies the complexity to a manageable size without losing the context. A bowtie is well suited to create an overview of the organisation's risks and how they are managed. To conclude, the primary goal of the bowtie is not quantification, but risk communication and awareness on all levels of the operational phase.

A last nuance is that both goals lead to an assessment whether the remaining risks are tolerable. They just go about it in different ways.

Note: Some quantification is possible as long as the limitations of the bowtie model are taken into account.

3
The application of bowties, today and tomorrow

3.1. Today

Bowties today are mainly used to make a decision whether the current level of control is sufficient. This can be done to satisfy an organisation internally or an external regulator or customer. There are many methods that do this, so what are some additional reasons why bowties are used? First, the bowtie has a helpful structure to brainstorm with a team on risks. Second, it contains operational hardware barriers, behavioural barriers and organisational management systems, which makes it an ideal place to holistically look at where investing resources would have the greatest impact. But perhaps the best reason for choosing the bowtie method is that it creates an easy picture to understand and communicate on multiple levels of the organisation. A complete bowtie diagram, linked to the management system, is like a graphical table of contents – a map, showing everything an organization does to controls its major risks.

To summarise, these are the main reasons to create a bowtie:

- Provides a structure to systematically analyse a hazard.
- Helps make a decision whether the current level of control is sufficient (or, for those who are familiar with the concept, whether risks are As Low As Reasonably Practicable or ALARP).
- Helps identify where and how investing resources would have the greatest impact.
- Increases risk communication and awareness.

3.2. Tomorrow

Even though the bowtie is used a lot for risk communication, it still remains a static piece of information which might get reviewed only once every couple of years. This is a waste because it contains a lot of useful information. A trend we see is that an increasing number of regulators and companies are expanding their attention to include monitoring of barrier performance.

There are already a lot of ways in which barriers are monitored implicitly. The challenge is to collect the available information from these sources and relate them to the barriers. This information can come from a number of sources like audits, inspections, permit to work systems, maintenance backlogs incident- and near-miss investigations.

The future will first see an increase in relating these data sources to barriers. After that, these data sources will be combined to create a regularly updated bowtie diagram which visualizes the current status of barriers. With regularly we mean fairly short term, compared to traditional risk assessment. As short as is feasible – updates can vary from monthly down to hourly. It enables more dynamic risk assessment that is embedded in the daily operations instead of begin a printed document that collects dust on a shelf.

4

Before getting started

4.1. Deciding if you need bowtie

Do you need bowtie? That should be the first question to answer before getting started with bowties. Bowties are risk assessment diagrams that provide a qualitative visual diagram to increase understanding of a risk. If you're looking for a quick scan of all your risks, a HAZID might be more suitable. If you're looking for a purely quantitative model, QRA might be more suited. Bowtie is really useful in most other risk assessment areas. It's meant to structure a brainstorm session with multiple disciplines and get a result that everyone can understand without going through a thick report. If this sounds like something you're looking for, keep reading.

4.2. Determining scope

Like any project, doing bowtie risk assessment requires some preparation to make the actual assessment run smoothly. A lot of the experience you may have with similar types of projects will also be relevant for a bowtie project.

4.2.1. Goal

At the outset, it should be pretty clear what goal the bowtie is supposed to achieve, or which problem it is supposed to solve. Obviously it is possible to have several goals. But make sure goals do not conflict, as this makes for a muddy project. The goal will also determine who the intended audience of the bowties is. This will help make decisions about how to build the bowtie later on. Some examples of goals are:

- To demonstrate the level of control on risks to a regulatory body.
- To find areas for improvement.
- To improve the quality and clarity of risk communication.

It is also good to think about what will be done with the bowtie once it's completed. Will it be integrated in a training program, will there be posters, will it be included in a printed report, and will it be included in audit and incident processes? This is very much linked to the goal and should be considered together.

4.2.2. Resources

The organization should allocate appropriate resources for the bowtie project. Some examples of things to consider are:

- Which locations can/should we include?
- How much time is available?
- Is there sufficient budget?
- Do attendees require training?
- Who will be responsible for the bowties once the project is done?
- Who will facilitate the sessions?
- Do we have the necessary documentation to prepare?

The quality of a bowtie is normally determined partially by the facilitator, and largely by having the right people attend. It might significantly change from organisation to organisation, but generally one should try to have cross disciplinary teams. A lot of the value of bowties is created by having different department brainstorming on issues that have never been questioned before. These are examples of people that might be involved in different phases of bowtie development.

Hazards & Top event	Threats & Consequences	Preventive barriers	Recovery barriers	Escalation factors & barriers
• Operational management • Safety professionals • Process experts • (Regulators)	• Process Safety • Operators • Operations Management	• Operations • Maintenance • Process Safety	• Operations • Maintenance • Process Safety • Emergency Response Organisation	• Maintenance • Operations • Safety Department

4.3. Setting the context for bowtie

Once the above decisions are made, we essentially have the context in which the bowties need to work. Before discussing the specifics of building a bowtie, here are two questions that will come back during the bowtie process and help determine the scope of everything in the bowtie. First, which abstraction level is appropriate and second, what moment in the causal chain is the top event.

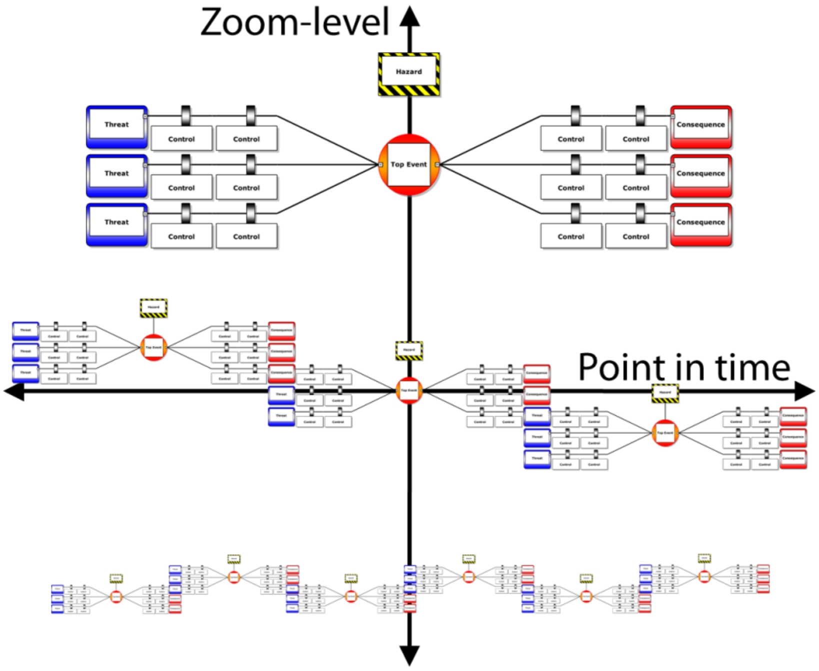


Figure 10 - Bowtie zoom level and causal chain explained

4.3.1. Level of abstraction

The zoom level, or level of abstraction at which the bowtie will be built is an important decision to make. In practice they should not be too specific because the bowtie diagram will become too large if all bits of information are included. But the bowtie should also not be too generic, since relevant information that is necessary to put the analysis into practice might be lost. People tend to be too generic – being generic is easier, because specific means actually knowing the specifics. It is critical to involve people who know the specifics about scenarios you are assessing.

Depending on the zoom level / abstraction level, there will be either more diagrams which are more detailed, or fewer diagrams which are more abstract. Which one is fit for purpose is a choice to be made.

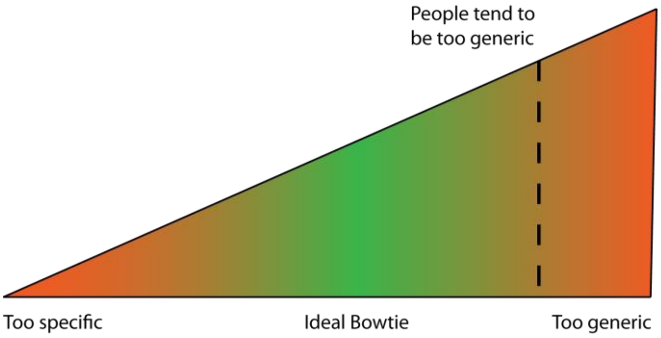


Figure 11 - The ideal zoom level for bowties

4.3.2. Choosing a top event

Events are usually part of a longer chain of events: drinking and driving can lead to a loss of control over a vehicle, which can lead to crashing into open water, which can lead to occupants becoming entrapped in an enclosed space, which can lead to fatalities. Which one is made into a top event is important, because this choice dictates how the diagram will turn out. It is important to realise that the top event is not an absolute event. It is very much a subjective choice that depends on the perspective you take. For example, an explosion can be a consequence for an organisation, and a top event for a fire fighter.

Sometimes a generic bowtie is created where the threats and consequences are specified in other bowties. In this case a threat or consequence can become a new top event in another bowtie. In this manner several bowties will be linked, creating a chain of events. This is called chaining bowties.

5
Building a Bowtie

In this chapter we discuss the various bowtie elements in-depth – what are best practices for them, what are the pitfalls – all explained with examples.

5.1. A Bowtie Diagram in 8 Steps

The next pages discuss the eight steps in greater detail. We will also examine completing the bowtie with barrier types, responsible persons, how to link your bowties to the management system and how to assess effectiveness.

Remember that everything here is meant to help build bowties and provide guidance. It is not intended to be strictly applicable or reliable in every situation. These are not absolute rules because the safety reality is much too complex for absolute rules – a pragmatic approach is advisable.

The purpose of the bowtie diagram is to gain insight in complex processes through oversight. This objective is always leading and can therefore overrule the guidelines if necessary. The intention to be analytically correct almost never outweighs the objective to keep an understandable diagram.

As seen in the introduction, there are eight basic steps in building a bowtie diagram. They are as follows:

Step	Description
1. Identify hazard	The first step in managing risks is to identify what their sources are.
2. Identify top event	When we know what is potentially hazardous, we need to know how we could lose control over it.
3. Identify threats	Next we need to consider the scenarios or events which could directly cause the occurrence of the top event.
4. Evaluate consequences	After the top event occurs, subsequent scenarios or events are now possible. These consequences can lead to losses and damage.
5. Identify preventive barriers	The next step is to identify the barriers which should prevent the threats from reaching or causing the top event. These are preventative barriers.
6. Identify recovery barriers	Barriers on the right side try to recover from the occurrence of the top event. These barriers should prevent or mitigate the consequences and/or the resulting losses and damage.
7. Identify escalation factors	The next step is to identify the specific situations or conditions under which the barriers are less or not effective.
8. Identify escalation factor barriers	The last step is to look at what barriers you have to prevent or manage these escalation factors.

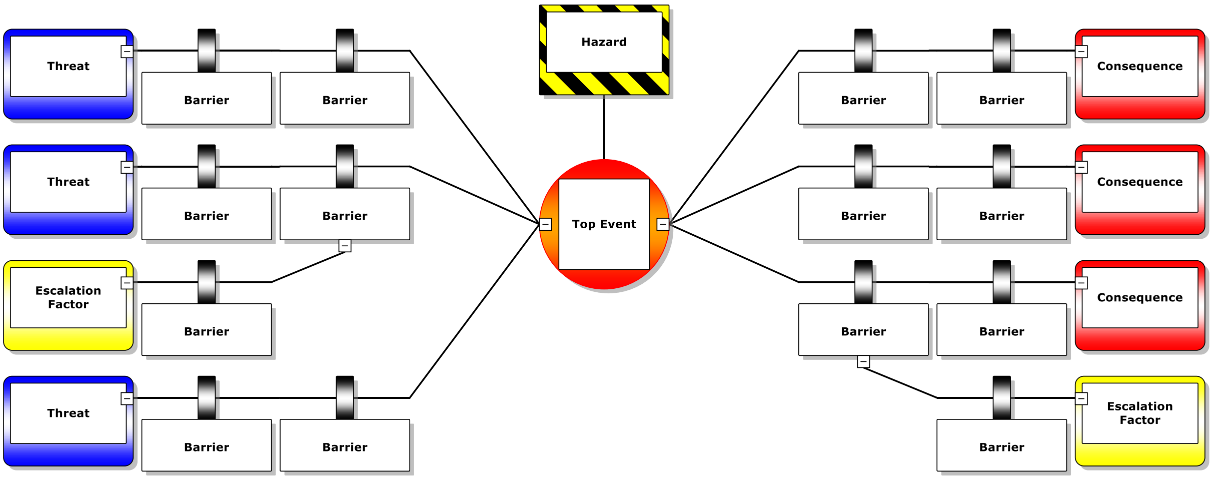


Figure 12 - Complete bowtie diagram

5.2. Hazards

The first step in managing risks is to identify what their sources are. In the bowtie method these sources are called hazards.

Figure 13 - Driving a car has the potential to cause harm (e.g. if we lose control over it)

From the perspective of an organisation, there are certain things that have more potential for harm than others. Typing a document on a computer has a very low potential to cause harm. Transporting fuel in a truck is potentially much more harmful. Assessing the organisation and identifying what operations, activities, situations etc. are potentially dangerous is the first step in creating a bowtie. Think about dangerous operations, situations, processes but also substances.

5.2.1. Hazard identification

The bowtie itself is not a specialized hazard identification method, so you need to use another technique that will identify hazards. Choose the technique that is appropriate for the organisation and management systems. Most commonly used techniques are: HAZID, What-if, PHA, GHA, HAZOP, and HAZAN. For a broad overview of existing techniques please consult ISO 31010.

Most organisations already have a complete hazard register. This can be used as the starting point of a bowtie risk analysis. The bowtie method is particularly suited to analyse major hazard scenarios. These are scenarios of which the possible consequences are rated as intolerable or high. However, other workplace hazards can also be analysed using the bowtie method - this depends on the preference of an organisation.

After all the possible sources of harm are identified in a complete hazard register the top major hazards are selected for further analysis in a bowtie diagram. This selection is based on the probability and severity of the potential consequences that are introduced by the hazards. This is usually displayed by means of a risk assessment matrix. How many of the hazards in the register are analysed using bowties varies depending on scope, time and available resources.

See section 5.5.1, Risk matrices on page 33 for a discussion of risk assessment matrices.

5.2.2. Formulating hazards

Formulating hazards can be challenging. It is often a trade-off between being specific (which will generate a lot of small hazards) and being generic (which will not capture the level of detail you want). This is why it is very important to have a clear scope. The scope helps determine the level of detail that is required.

Also remember that everyone in the organisation needs to interpret the meaning of the hazard in the same way. There are 4 things to keep in mind when formulating hazards to achieve that:

1. **Describe the hazard in the desired (controlled) state.** One of the most difficult things about hazards is that they should be formulated in a controlled state. So a hazard description should be “transporting fuel in a truck from a to b” and not “fuel truck explosion”. A hazard describes a potentially harmful situation and not the actual harm that can lead from that situation (this is stated in the consequences). Hazards are part of normal business and are in fact often the sources that are also responsible for creating the business opportunity.
2. **Use commonly accepted names.** People need to interpret the description of the hazard in a similar way. Keep organisational terminology in mind, but also whether a department’s particular terminology is used and understood in other parts of the organisation.
3. **Provide situational context.** Situational information can be essential to comprehend the type of hazard. Presence of snow or sub-zero conditions can make a bowtie look completely different from a desert location with heat and dust.
4. **Give an indication of scale.** The scale that is involved can also provide important information. How much fuel is there in the truck? Under how much pressure is the chemical substance?

5.2.3. Guidelines

- Hazards are part of normal business
- Hazards exist, they do not ‘happen’
- Describe and define the hazard carefully

5.2.4. Workshop questions

- What can be dangerous at this location?
- What are the things we need to be careful with during day-to-day operations?
- What are potential sources of risk that can lead to loss or damage?

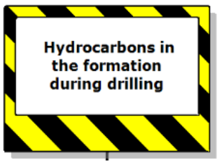
5.2.5. Samples

***Hazard:** Lion in a cage*

The lion is a part of the normal zoo business – no lion, no visitors. The lion can cause damage/loss, but only if we lose control over it – i.e. the lion is no longer in the cage.

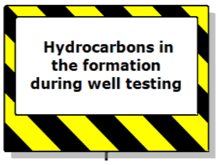
***Hazard**: Driving a car*

Driving a car is a normal requirement for many businesses – we have to get from A to B. This in itself is not a problem, but does have the potential to cause harm. We can lose control over the vehicle and crash into objects or people.



***Hazard**: Hydrocarbons in the formation during drilling*

Hydrocarbons in the rock formations we are drilling towards are absolutely necessary. Without those hydrocarbons there is no need to drill. But they do have the potential to cause harm – blowouts for example do happen.



***Hazard**: Hydrocarbons in the formation during well testing*

Like the previous example, the hydrocarbons are a part of normal business. The reason to create separate bowtie diagrams for hydrocarbons in different operational phases is because the threats and barriers are different.

Here are some more samples of hazards:

***Hazard**: H2S gas in formation*
***Hazard**: Flammable substances present on the installation*
***Hazard**: Working at height*
***Hazard**: Helicopter transporting people to and from the rig*

5.2.6. Exercises

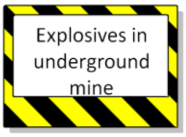
Exercise #1 - which of these three examples is not a hazard:

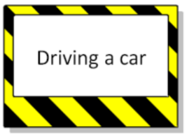
Uncontrolled Fire

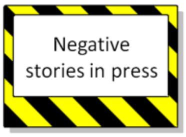
Birds around aerodrome

The answer is 'Uncontrolled fire' – this is neither a loss of control nor a part of normal business. This is a consequence. 'Birds around aerodrome' is a proper hazard. In all airfields birds can be present and therefore they are a part of normal business. They do contain the potential for harm – for example if they fly in an engine. 'H2S' is also a proper hazard. H2S can be a part of normal business and most definitely has the potential to cause harm - it can burn and is toxic.

Exercise #2 - which of these three examples is not a hazard:







‘Explosives in underground mine’ is a good hazard. It is part of normal business; it has potential to cause harm and is formulated specifically. ‘Driving a car’ is also a good hazard. It is a part of normal business and has the potential to cause harm. A 1500 kg piece of steel moving at high speed can cause a lot of damage, both to occupants and environment. ‘Negative stories in press’ is not a good hazard, it represents a consequence.

Exercise #3 - which of these three examples is not a hazard:

Hydrocarbons

Derailment

Landing
aircraft

‘Hydrocarbons’ is a good hazard In the oil and gas it is an essential part of normal business, and has many different ways in which it can cause trouble. However its definition is very broad – what kind of hydrocarbons? Where? What are we doing with them? ‘Derailment’ is not a good description of a hazard, because it is not a part of normal business. ‘Landing aircraft’ is a good example of a hazard, because it is a part of regular business and can cause harm.

5.3. Top Events

The next step in the bowtie method is to define the top event in the centre of the diagram. The top event is the first moment control over a hazard is truly lost, releasing its harmful potential. The organization is now in a recovery state – trying to regain control, before the loss of control causes any damage. It can be tricky to find the right top event, but you can always just start with 'Loss of control' and refine it later on, once the context has become clearer.

To make it even more difficult, what is considered a top event can change depending on the department or circumstances. For instance, a maintenance department might have "release of unairworthy aircraft to service" as a top event, while for the pilot of that aircraft, it is a threat to losing control over the aircraft.

The top event is a crucial point in time which usually has multiple causes and consequences. If the top event has only a single cause and consequence, there is no real distinctive characteristic which makes it a bowtie above a generic linear barrier diagram. So the bowtie works best if the top event has multiple causes or consequences.

The top event is usually not yet a catastrophe, disaster or actual damage; it is still possible to recover from it, at least to some extent. Catastrophes and disasters are typically consequences in the bowtie method, and not top events. Check if the consequences of a top event can still be mitigated. If not, the chosen top event might actually be a consequence of another top event that needs to be identified.

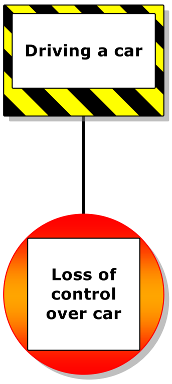


Figure 14 - Driving a car has the potential to cause harm (e.g. if we lose control over it)

Note: it can be helpful to use disasters to come up with the right top events: to think about the first event that initiated the final phase of this disaster.

One hazard can result in multiple top events – the potential harm can be released in different ways. Therefore one hazard can result in multiple bowtie diagrams. For example, the hazard 'working at height' can result in two top events 'dropped object' or 'person falls from height'.

Tip: If you cannot agree on the exact definition of the top event choose one of the following generic terms:

- Loss of containment
- Loss of separation
- Loss of stability
- Loss of control

You can return to this step later in the process to refine the definition of the top event.

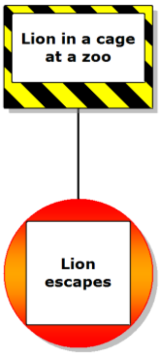
5.3.1. Guidelines

- Top events are usually not disasters (disasters are often consequences)
- Hazards can have multiple top events
- Usually involves a change of 'state'
- Describe how control is lost
- Give an indication of scale if possible

5.3.2. Workshop questions

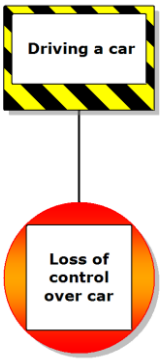
- When do we lose control over this hazard?
- What change of state of the hazard makes us lose control?
- What is the moment that normal business changes into abnormal business?

5.3.3. Examples



Hazard: *Lion in a cage at a zoo*
Top Event: *Lion escapes*

The lion escaping from the cage is the moment we lose control. Before this moment normal business operations were performed. After this moment the operations to recover from the top event are executed. –The lion attacking the visitors is not a correct top event –control is lost before that consequence occurs.



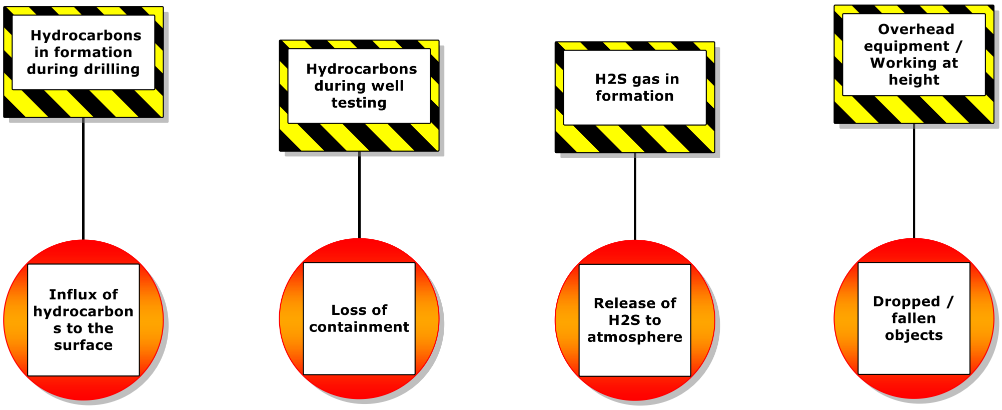
Hazard: *Driving a car on the highway*
Top event: *Loss of control over the car*

In this case loss of control is very literal – losing control over the vehicle is the top event. Crashing into something is not a top event – we don't suddenly crash into things, we have lost control before that occurs.

Here are some more samples:

H: *Hydrocarbons in the formation during drilling*
H: *Hydrocarbons during well testing*
H: *H2S Gas in formation*
H: *Overhead equipment / Working at height*

TE: *Influx of hydrocarbons to the surface*
TE: *Loss of Containment*
TE: *Release of H2S gas to atmosphere*
TE: *Dropped / fallen objects*


Hydrocarbons in formation during drilling
Influx of hydrocarbon s to the surface
Hydrocarbons during well testing
Loss of containment
H2S gas in formation
Release of H2S to atmosphere
Overhead equipment / Working at height
Dropped / fallen objects

5.4. Threats

After a hazard and top event are known, the threats should be identified. Threats are potential causes of the top event. They are located on the left hand side of the top event. There can be multiple threats for one top event and each threat represents a single scenario that could directly and independently lead to the top event.

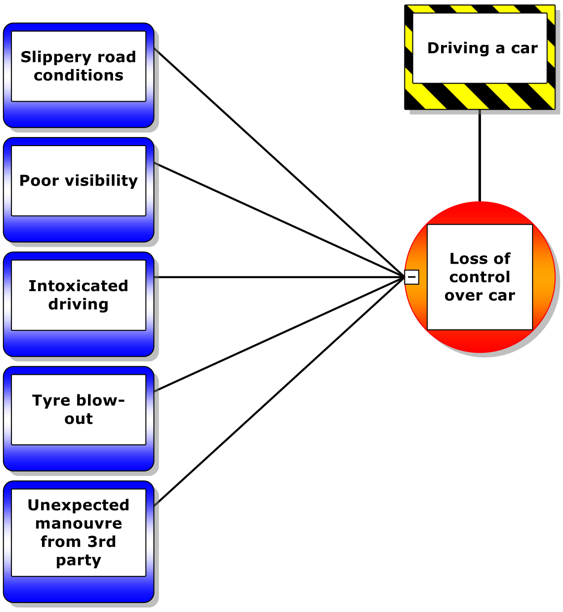


Figure 15 - Threats leading to loss of control when driving a car

For example, the loss of control over a car can be caused in several ways. A few of the threats are Slippery road conditions, Poor visibility, Intoxicated driving, Tyre blow-out and Unexpected manoeuvre from 3rd party.

Many of the above mentioned possible threats will rarely lead to the top event because there are many preventive measures (barriers). But the reason that these measures were ever implemented is that these possible threats threaten us. It is all about visualizing the potential scenarios and making sure you control them sufficiently.

Tip: It is often helpful to ask the question why a certain procedure or protocol exists - there is usually a very good reason. Probably it is meant to control something (e.g. a possible threat in a high risk scenario).

Tip: When brainstorming about hazards and their threats in a group, you might hear that many of the proposed scenarios will never happen because of specific procedures, fences or gates: that's when you know that you are on the right track – that is the reason why these procedures, fences, and gates were implemented; to avoid or reduce these threats.

5.4.1. Direct threats

Threats should be able to directly cause the top event. This does not mean that they should occur just before the top event in time; a threat can occur years before the actual top event occurs. Direct in this context means causally direct. Bad weather conditions can indirectly cause someone to lose control over their car, the direct effect however is that the road gets slippery (or visibility reduces, but that is a different threat). The reason to define a direct threat is because it helps in making the different threat scenarios more specific.

Specific scenarios, in turn, help to identify more specific barriers. With the risk of skipping ahead, first try to think of barriers for bad weather conditions and after that for slippery road conditions and poor visibility. The brainstorm that results from these related issues is completely different. In general, abstract threats lead to abstract barriers, whereas specific threats lead to specific barriers. Specific barriers give more practical information leading to a better understanding of what should be done to actually implement a functional barrier.

There is always a balance to be struck. It could be said that slippery road conditions also do not directly cause the loss of control over a vehicle; instead it is the wheels losing grip on the road that directly cause it. Be pragmatic and chose a direct threat without losing oneself in nitty-gritty discussions on causality. The goal is to create a bowtie that is specific instead of abstract, which will increase the quality and value, without going overboard in the causality discussion.

5.4.2. Sufficient and independent threats

Each threat itself should, in theory, be sufficient to directly cause the top event. This means that if two threats **need** to occur together in order for them to cause the top event, those threats need to be reformulated into one independent threat.

The reverse is not true. It doesn't mean that a potential incident always has to occur because of a single threat. Many threats acting simultaneously could have contributed to an incident.

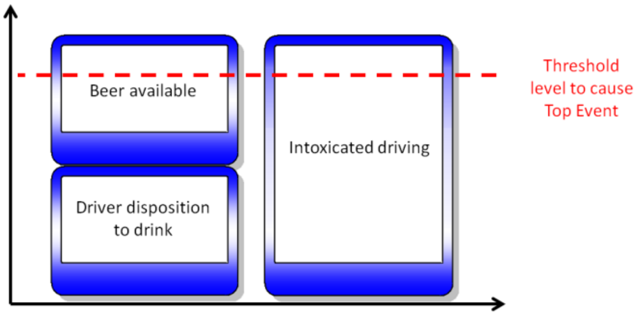

Beer available
Driver disposition to drink
Intoxicated driving
Threshold level to cause Top Event

Figure 16 - Sufficient / independent threats visualized

5.4.3. No barrier failures

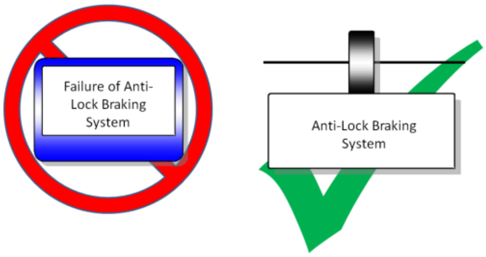
> This section requires some knowledge of barriers but it is most relevant in relation to threats. If it is not entirely clear, read the section on barriers first before reading this section.

One of the most frequent mistakes is to formulate a threat as the failure of a barrier. Barrier failures can be spotted by certain words such as:

- Lack of <……>
- Failure of <……>
- Absence of <……>
- Etc.

There is one type of threat that is also described with these failure words, while still being correct and those are primary process failures. If a piece of equipment that is part of the primary process fails (such as an engine failure in a helicopter, or a pipeline integrity failure in an installation), those are actual threats. But when the function of a piece of equipment is safety related, its failure can never occur as a threat. Every safety measure should be thought of as a barrier, and not as a threat described as a failed barrier.

Another way to look at the same thing is this: a threat should be a force or condition that pushes an unwanted chain of events further. A primary process failure will do that. For instance an engine failure can lead to a loss of control of a helicopter. A barrier failure is the absence of a good thing. It doesn't push the unwanted chain of events forwards, but it just sits by and does nothing, while a threat leads to a top event.



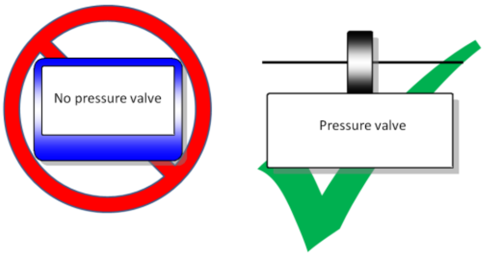


Figure 17 - Barrier failures are not threats

For example, the failure of anti-lock braking systems: anti-lock braking systems do not cause loss of control over a vehicle; they are a safety device which allows the driver to remain in control over the vehicle during hard braking and slippery conditions. The threat is actually a failed barrier that is intended to prevent another (possibly more underlying) threat.

The same goes for a pressure relief valve exists to make sure that overpressure does not lead to loss of containment. The incorrect handling of the valve is therefore not a threat but a broken barrier or an escalation factor of a barrier. The threat in this example is: ‘Overpressure’.

5.4.4. Prevalence of a threat

Only include those threats that are likely to actually happen or exist – you need to consider the prevalence (or size) of the threats you are discussing. If a certain threat is very unlikely to occur in the bowtie scenario you can choose to exclude it from the analysis. It’s also wise to list your threats in order of prevalence: those that are most likely to cause the top event are placed on top.

5.4.5. Guidelines

- Threats should be direct
- Each threat should be sufficient and independent
- Consider the prevalence (size) of a threat
- Barrier failures are not threats

5.4.6. Workshop questions

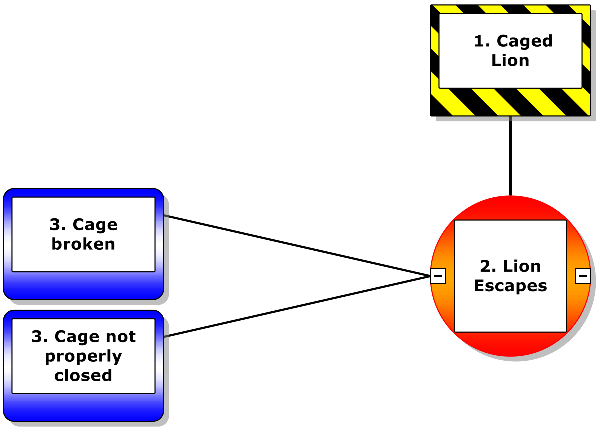
- What can cause this top event to happen?
- What caused this top event to happen in the past?

5.4.7. Samples

***Hazard**: Lion in a cage at a zoo*
***Top event**: Lion escapes*

Brainstorm: In our sample zoo, there is a dangerous lion in a cage, which can escape. This can be caused by the cage failing or the cage not being properly closed and locked.

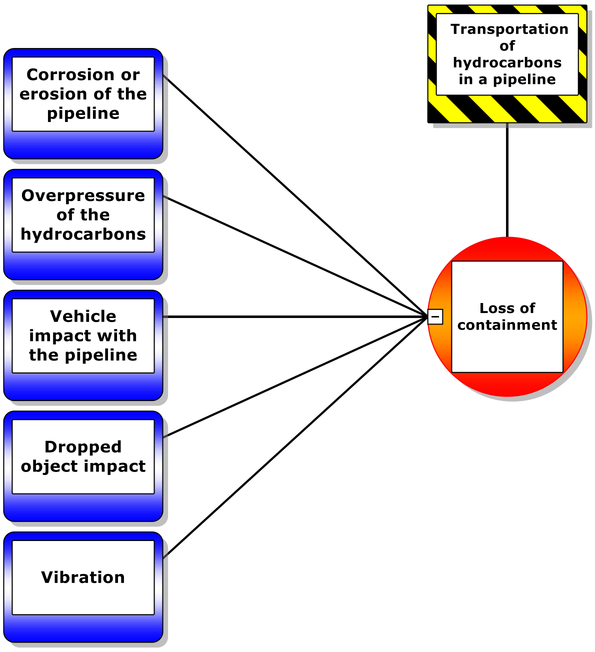
Both scenarios are plausible threats and some might have happened in the past already.



***Hazard**: Transportation of hydrocarbons in pipeline*
***Top event**: Loss of containment.*

Brainstorm: If hydrocarbons (gas, oil) are pumped through a pipeline, the contents of the pipe might spill out. Reasons for this include threats such as:

- Corrosion or erosion of the pipeline
- Overpressure of the hydrocarbons
- Vehicle impact with the pipeline
- Dropped object impact
- Vibration leading to metal fatigue

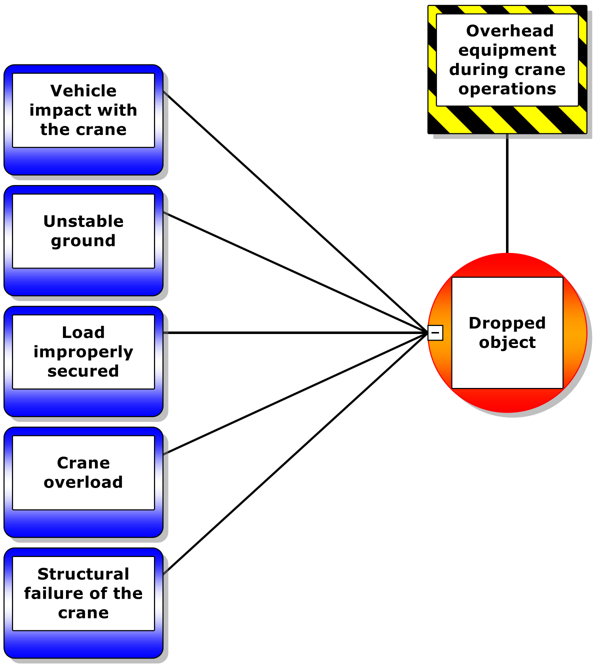

Transportation of hydrocarbons in a pipeline
Corrosion or erosion of the pipeline
Overpressure of the hydrocarbons
Vehicle impact with the pipeline
Dropped object impact
Vibration
Loss of containment

***Hazard**: Overhead equipment during crane ops*
***Top Event**: Dropped / fallen objects*

Brainstorm: One of the hazards related to working at height is the presence of overhead equipment. Losing control of overhead equipment during crane operations could lead to objects falling down. This could be caused by various threats such as:

- Vehicle impact with the crane,
- Unstable ground on which the crane is placed,
- Improperly secured load,
- Overloading of the crane or even
- Structural failure of the crane.

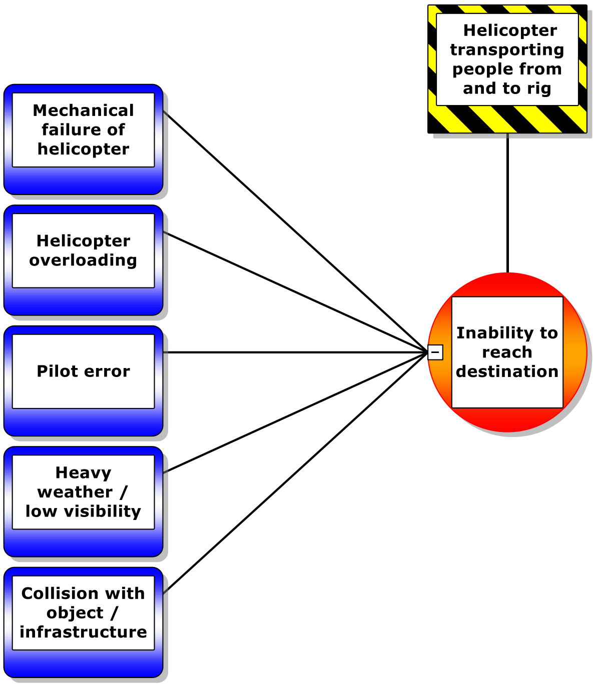
All these potential causes for losing control of overhead equipment are plausible threats in this accident scenario.


Overhead equipment during crane operations
Vehicle impact with the crane
Unstable ground
Load improperly secured
Crane overload
Structural failure of the crane
Dropped object

***Hazard**: Helicopter transporting people to/from rig*
***Top Event**: Inability to reach destination*

Brainstorm: The loss of control of helicopter operations can be phrased in various ways: crash or simply loss of control. Another option is: 'Inability to reach destination'. Possible threats for this top event are those events that interrupt the process of transporting people to and from the rig. For example:

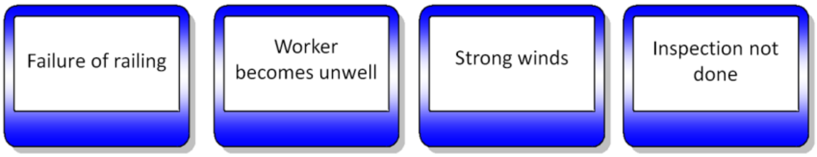
- Mechanical failure of the helicopter
- Overloading of the helicopter,
- The pilot making an error
- Heavy weather or low visibility
- Collision with an object (e.g. with a crane on board of the platform)


Helicopter transporting people from and to rig
Mechanical failure of helicopter
Helicopter overloading
Pilot error
Heavy weather / low visibility
Collision with object / infrastructure
Inability to reach destination

5.4.8. Exercises

For these exercises it might be wise to read the section on barriers first.

Exercise #1 – is this a threat or barrier failure?



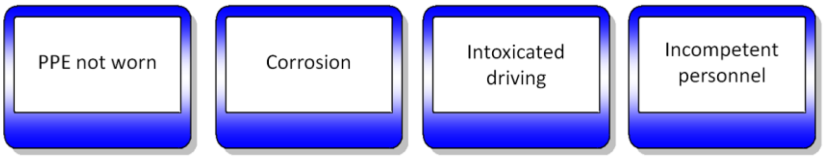
Failure of railing This is not a threat but a barrier failure. The barrier 'railing' exists to prevent people from falling. It is also not a part of the primary process which can fail, such as engine failure in a car.

Worker becomes unwell This is a threat and can cause top events to happen. If e.g. the driver of a truck becomes unwell, the control over the vehicle can be lost.

Strong winds This is a threat as well which can cause top events to happen.

Inspection not done This is a barrier failure. Inspections are barriers that prevent threat from leading to a top event. Unless we are building a very specific bowtie, such as a human-error bowtie, or a bowtie where we examine what procedural violations can cause, this is not a threat

Exercise #2 – is this a threat or barrier failure?



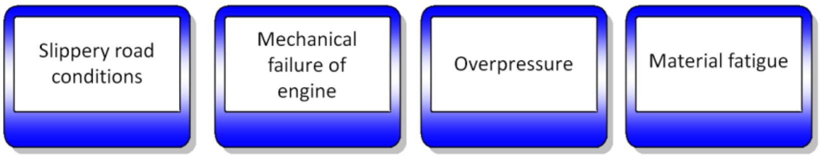
PPE not worn Barrier failure. PPE is a barrier to prevent a worker from harm. Also, not wearing PPE will not cause top events to happen. Not wearing PPE will make some top events (and consequences) more likely – but that is due to the absence of PPE as a barrier.

Corrosion A threat. It is something we protect ourselves against with barriers such as coatings.

Intoxicated driving This can also be a threat.

Incompetent personnel This is probably a failed barrier. The barrier which failed could be ‘competency standards’.

Exercise #3 – is this a threat or barrier failure?



Slippery road conditions A threat. It can cause loss of control over a vehicle.

Mechanical failure of engine This can be a threat or barrier failure, depending on what the engine does. If the engine is part of the primary process which fails, it can cause all kinds of trouble and would be regarded as a threat. The exception would be if the engine was actually part of a safety device (like a backup generator for instance). In those cases it would actually be a barrier failure.

Overpressure A threat. Overpressure happens and we have barriers like a pressure relief valve to stop it from leading to a loss of containment.

Material fatigue This will be a threat. It is something we protect ourselves against with barriers.

5.5. Consequences

Consequences are events that are caused by the top event. They are the reason why we decided to make a bowtie analysis on a hazard in the first place. Consequences are what we ultimately want to prevent, not threats or top events. Those are only a problem because they can lead to a consequence.

One top event can have multiple consequences. After defining consequences an overview of possible scenarios is reached. Different threats and combinations of threats can lead to the top event, from which it can lead to different consequences or combinations of consequences.

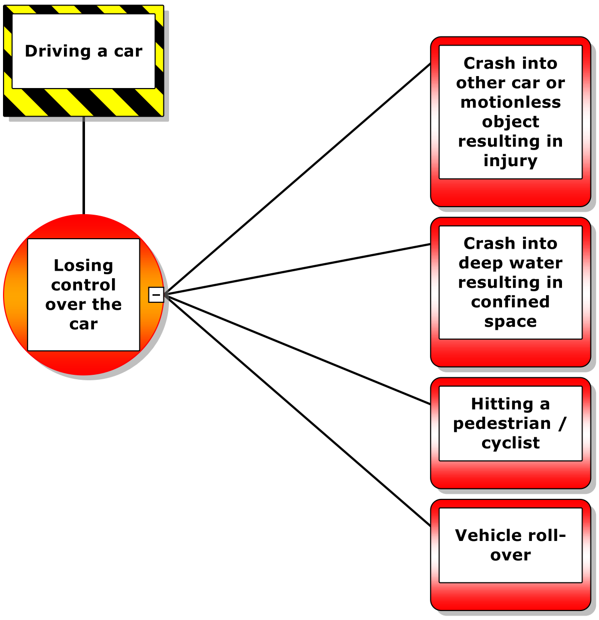

Driving a car
Losing control over the car
Crash into other car or motionless object resulting in injury
Crash into deep water resulting in confined space
Hitting a pedestrian / cyclist
Vehicle roll-over

Figure 18 - Consequences when losing control over a car

Consequences are events that can directly result in loss or damage, but are not the loss or damage themselves. A large scale fire can result in fatalities, asset and environmental damage. The consequence is the fire, which leads to loss or damage. But when defining consequences, one often made “mistake” is to create generic consequences which describe loss or damage directly, such as: injuries/fatalities, asset damage, environmental damage, reputation loss. Those are ultimately true, but what is their added value? Most likely all hazards involve the above four in some way and one could simply copy and paste them into every bowtie without adding a lot of understanding about its subject. Instead we want to know how we got to that generic loss or damage.

This is done by making consequences specific for a top event. Think about the event that leads to injuries/fatalities. Is it for instance due to smoke inhalation or blunt impact? These events will lead to more specific barriers later on, and help to get more out of the bowtie. Obviously one needs to be careful about being too specific with these events, but it is better to start with being specific and decide later on to group several consequences than the other way around.

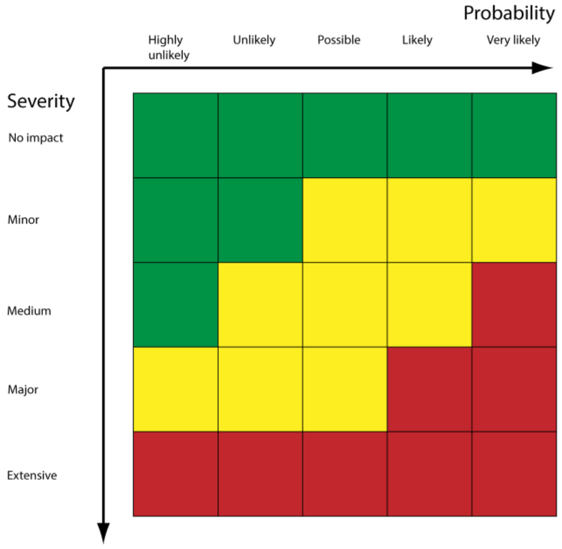
> If you still want to include a generic loss or damage description such as ‘fatality’ in a consequence, you can describe a specific event like ‘crash into an object’ and add ‘leading to fatality’. That way you group the end result together with a specific event. The downside is that assessing that consequence from multiple perspectives using risk matrices will not work as well because you’ve focused it on one specific type of loss or damage.

5.5.1. Risk matrices

Risk matrices are used in the bowtie to assess the possible loss or damage that a consequence might cause. This is where the generic categories such as people, assets, environment and reputation come in. These aspects are used to assess each consequence on their frequency and severity.

Risk matrices are 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 section will explain their use in the context of the bowtie diagram.

A risk matrix has two dimensions. Severity and probability of an unwanted event. These two dimensions create a matrix. The combination of probability and severity will give any event a place on a risk matrix.



Severity	Highly unlikely	Unlikely	Possible	Likely	Very likely
No impact	🟩	🟩	🟩	🟩	🟩
Minor	🟩	🟩	🟨	🟨	🟨
Medium	🟩	🟨	🟨	🟨	🟥
Major	🟨	🟨	🟨	🟥	🟥
Extensive	🟥	🟥	🟥	🟥	🟥

Figure 19 - A risk assessment matrix

Most risk matrices have at least three areas.

- Green - the low probability, low severity area that indicates the risk of an event is low enough, or that it is sufficiently controlled. No additional action is usually taken here. 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.

- Red - the high probability, high severity area which indicates an event is unacceptable and needs a lot of control measures to bring the probability or severity down. Bowties will have a lot of events that fall into this category.

- Yellow - the medium category 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 for possible improvements and to make sure the risk does not become worse.

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 (such as 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.

5.5.2. Severity

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 (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, 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 is difficult, if not impossible, to do. The best way to compare the severity of events is to make a qualitative judgement.

What is severe is also a relative concept. A car crash has a much bigger impact to a small taxi company than a multi billion oil & gas multinational. The severity scale needs to reflect this. As an organisation grows, the risk matrix scales should grow with it.

5.5.3. Probability

Up until now, probability has been discussed in general terms. But there are different possibilities for interpreting what probability means. 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 on the way to work. 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 frequency will only tell us something about the past. If something has not yet occurred, 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.

5.5.3.1. 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 give the worst severity the highest priority category, regardless of the probability.

5.5.4. Strategies for giving scores

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

- **Worst case/credible 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. This can be hard to define if, due to the nature of the processes and installations, a situation without barriers simply cannot exist. These types of incidents might occur in reality, but they will most likely be the exception, not the rule. A variation on this looks at worst credible scenario. Which does the same, only looks at what would be an average incident given a simultaneous failure of barriers which is realistic (or credible). This will lead to a more optimistic, but also more realistic assessment.

- **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 an event.

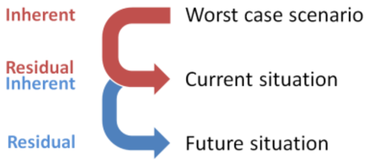


Figure 20 - Different definitions for inherent and residual risk

The differences between these three levels of risk create two possible comparisons that are used depending on the scope and goal of the bowtie. First, the difference between the worst case/credible scenario (inherent) and the current situation (residual) is used to indicate that the current barriers have brought the risk of a consequence down to an acceptable level. This is mostly used for regulatory purposes. Second, the difference between the current situation (inherent) and the future situation (residual) is used to indicate where an additional investment would have the highest risk reduction. This is mostly used as support when presenting an improvement plan.

Risk matrices are an important piece of the puzzle. They help judge the level of risk in consequences. It's also an important factor when we talk about risk evaluation in chapter 6.

5.5.5. Guidelines

- Consequences are events

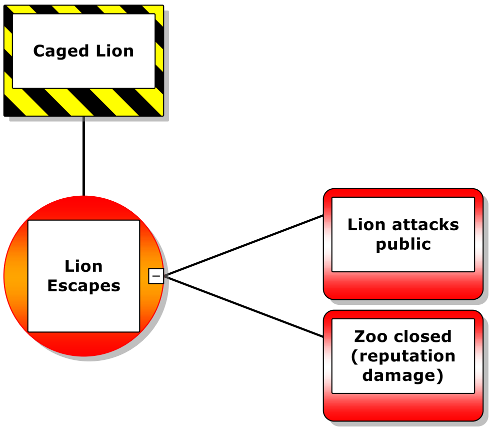
- Not the actual loss or damage (yet)
- Consequences are the actual risks

5.5.6. Workshop questions

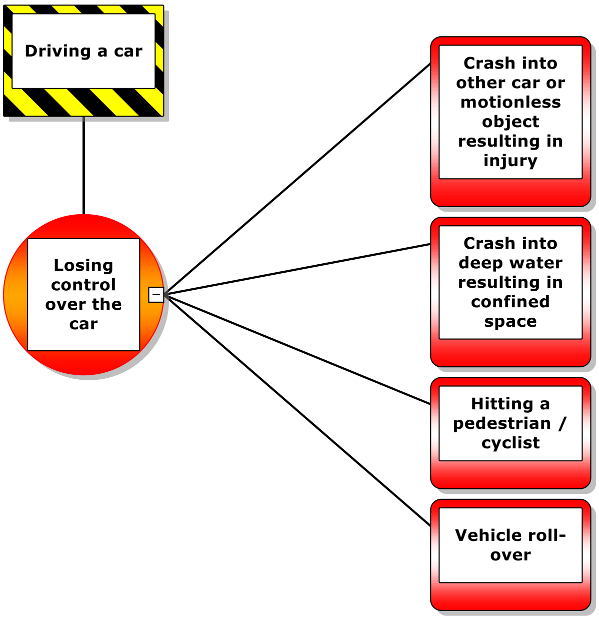
- How could the top event evolve?
- What could happen after we lost control?

5.5.7. Examples

Hazard: *Lion in a cage at a zoo*
Top event: *Lion escapes*
Brainstorm:
Our zoo is an organization that earns its existence by exhibiting dangerous animals to the public. These carry certain risks. One of the animals we have on display is a lion. It might however get out of its cage. If the lion gets out, we can face a multitude of consequences – the lion might attack and injure the public. At the very least we will get a lot of negative press, leading to a bad reputation and loss of revenue, we might even need to close.

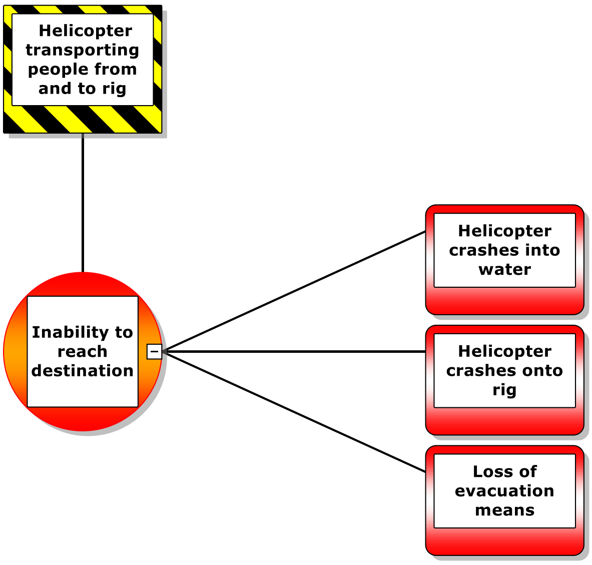


Hazard: *Driving a car on the highway*
Top event: *Loss of control over the car*
Brainstorm:
Losing control over the car can have various consequences. We could crash into another vehicle or roadside object, injuring the driver. We could crash into water, leaving the driver trapped inside. We could hit a pedestrian or bicyclist, resulting in injury. Our vehicle might roll over.


Driving a car
Losing control over the car
Crash into other car or motionless object resulting in injury
Crash into deep water resulting in confined space
Hitting a pedestrian / cyclist
Vehicle roll-over

Hazard: *Helicopter transporting people to and from the rig*
Top Event: *Inability to reach destination*

Brainstorm: If a helicopter is not able to reach its planned destination there are two (main) events possible: the helicopter crashing into the water or the helicopter crashing onto the rig. Both are undesirable and will definitely lead to loss and damage for the organization. If the helicopter crashes into the water, people will be in the water (injury / fatality to your personnel, business interruption), and the helicopter gets severely damaged (loss of assets for the helicopter company). If the helicopter crashes on the rig, even larger problems can occur; (structural) damage to the platform or helideck, the onset of an explosion / fire on the rig or the impact causing loss of containments of hydrocarbons. Another consequence of this top event is the loss of emergency evacuation means. This could be part of this diagram (as an extra consequence) or as an escalation factor on a recovery barrier (e.g. escape by helicopter) in another scenario. The losses that will be the result of a crash into the water or onto the rig will be assessed in a later phase.


Helicopter transporting people from and to rig
Inability to reach destination
Helicopter crashes into water
Helicopter crashes onto rig
Loss of evacuation means

5.6. Barriers

Once all the unwanted scenarios are identified, we can focus on how we stop those scenarios from occurring. The bowtie method uses the concept of barriers to think about this in a structured way. According to (Sklet, 2006), “Safety barriers are physical and/or non-physical means planned to prevent, control, or mitigate undesired events or accidents”

> Please note that the terms barrier and control refer to the same concept and depending on industry and company, one or the other is used. In this manual we will use the term barrier.

In the bowtie method there are three different places for barriers: between a threat and the top event (preventive barriers – also known as proactive barriers), between the top event and a consequence (recovery barriers, also known as reactive or defence barriers) and between a barrier and an escalation factor (escalation factor barriers).

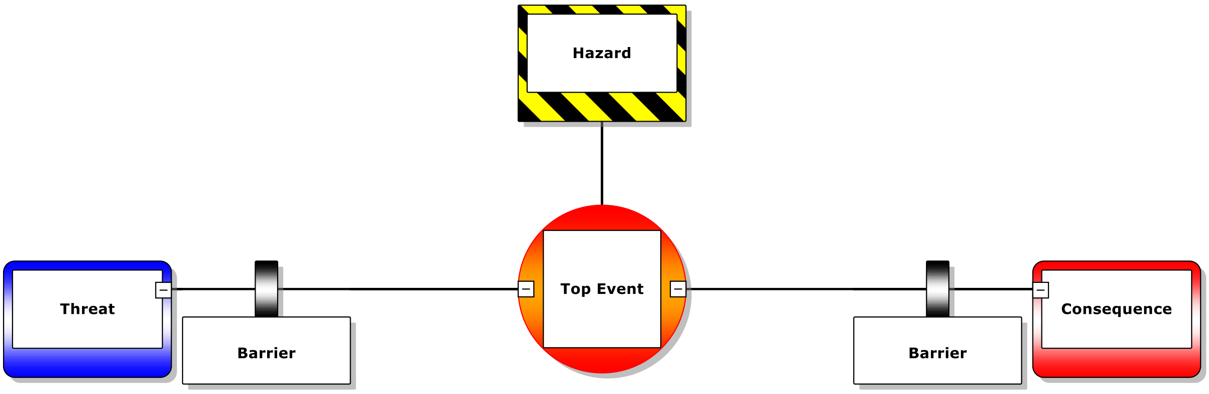


Figure 21 - Bowtie showing barriers on both sides of the top event

A barrier is placed at the moment it delivers its effect. For instance, the barrier ‘Fire fighting system’ is effective after the top event ‘Loss of containment’ and is therefore visible on the right side of the bowtie diagram. Sometimes people get confused and argue that the Fire fighting system is proactive because it was implemented years ago, before any incident ever took place. The fact that the implementation was done years before does not make it a preventive/proactive barrier. The moment when that barrier takes effect is what determines whether it is a preventive, recovery or escalation factor barrier. A good question to ask is whether the Fire fighting system will prevent the top event ‘Loss of containment’. If the answer is no, then the barrier can be placed on the right side.

Preventive and recovery barriers will be elaborated on below. Escalation factor barriers will be discussed in depth after we have discussed escalation factors.

5.6.1. Preventive barriers

A preventive barrier is a barrier that acts against a threat or top event. The effect of preventive barriers is before the top event has happened and is therefore always present on the left side of the bowtie diagram.

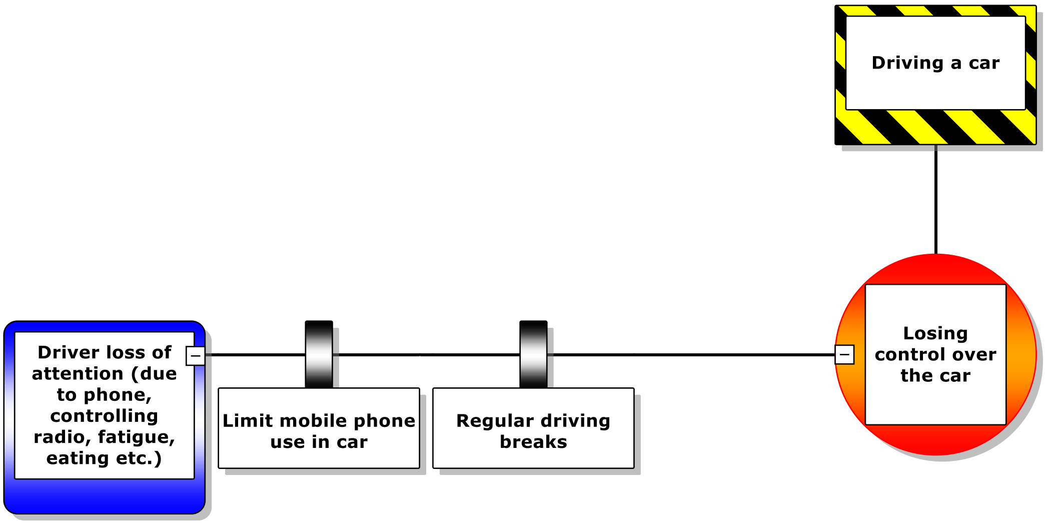

Driving a car
Driver loss of attention (due to phone, controlling radio, fatigue, eating etc.)
Limit mobile phone use in car
Regular driving breaks
Losing control over the car

Figure 22 - Barriers to prevent attention loss when driving a car

There are two main ways in which a preventive barrier has its effect. This is known as the barrier function.

1. **Elimination.** These barriers eliminate the threat and make sure that there is nothing (or less) to cause the top event. Logically these take their effect before the threat, but to keep the diagram simple, these barriers are included between the threat and top event.
2. **Prevention.** These barriers don't do anything about the threat but make sure to stop the threat from becoming a top event, either by blocking the causal effect of the threat or directly stopping the top event from happening.

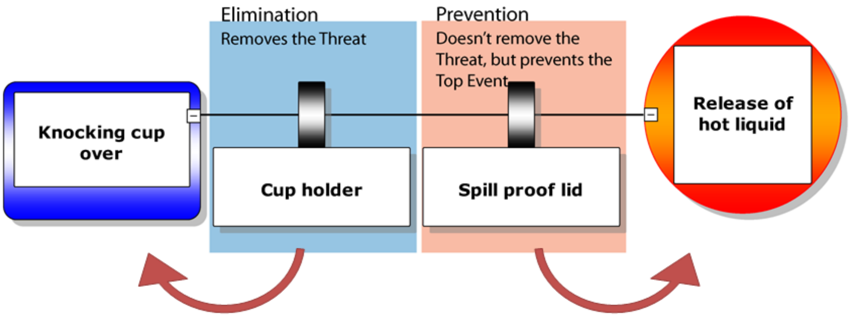


Figure 23 - Preventive barriers and their moments of effect

5.6.2. Recovery barriers

We should always try to avoid top events first, but unfortunately things sometimes do go wrong. Experience teaches us that our top events do occur even if we are managing our potential threats properly. Therefore we should be prepared to regain control once it is lost. This is why we implement recovery barriers that act on the likelihood or severity of a potential consequence.

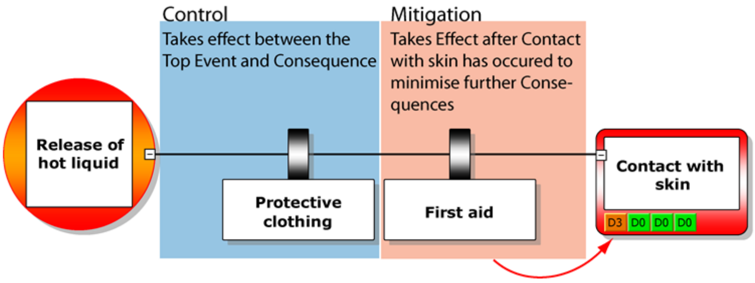

Control
Takes effect between the Top Event and Consequence
Mitigation
Takes Effect after Contact with skin has occured to minimise further Conse-quences
Release of hot liquid
Protective clothing
First aid
Contact with skin
D3 D0 D0 D0

Figure 24 - Recovery barriers and their moment of effect

> Tip: Try to target the barriers onto specific risks. Barriers that have an effect on a potential gas cloud will probably not work in case of a fire. It is a choice however how far you will take this principle. This depends on the level of detail you are aiming at, but also on the scope of the analysis (e.g. the financial burden of loss of assets is not always part of safety related analysis).

Recovery barriers have a function just like preventive barriers. See the example in Figure 24. Recovery barriers function through either:

1. **Control**. Prevents the consequence from happening. In the example, the barrier 'protective clothing' will actually prevent the contact with skin itself.
2. **Mitigation**. Does not prevent the consequence from happening, but lessens the severity of the consequence. The barrier 'first aid' won't prevent the consequence 'contact with skin', but it will minimize the effects after the contact. At some point barriers take effect too long after the initial consequence but there is no strict rule about where to stop. In this example a control such as 'reconstructive plastic surgery' is probably too far removed from the contact with skin to be meaningful, but even that is a subjective judgment.

These recovery barriers and their function have impact on the risk assessment. The control barriers lessen the frequency of the consequence, and the mitigation barriers lessen the severity of the consequence.

5.6.3. Splitting of threats and consequences

If during barrier identification, you notice that some barriers are only applicable in a special case of the threat or top event, you should consider splitting the threat or consequence into multiple more specific items.

Let us demonstrate with a sample: Flammable gas can be released, leading to a fire. We identified the following barriers:

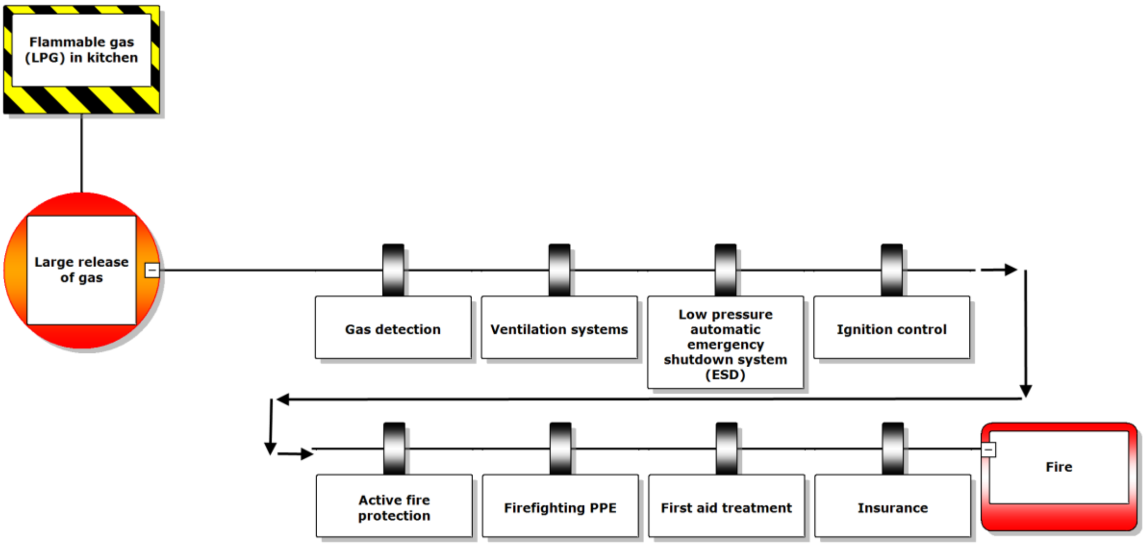


Figure 25 - A long barrier chain

There are a lot of barriers, and not all of them are immediately applicable to a fire. It is better to split this consequence up as follows:

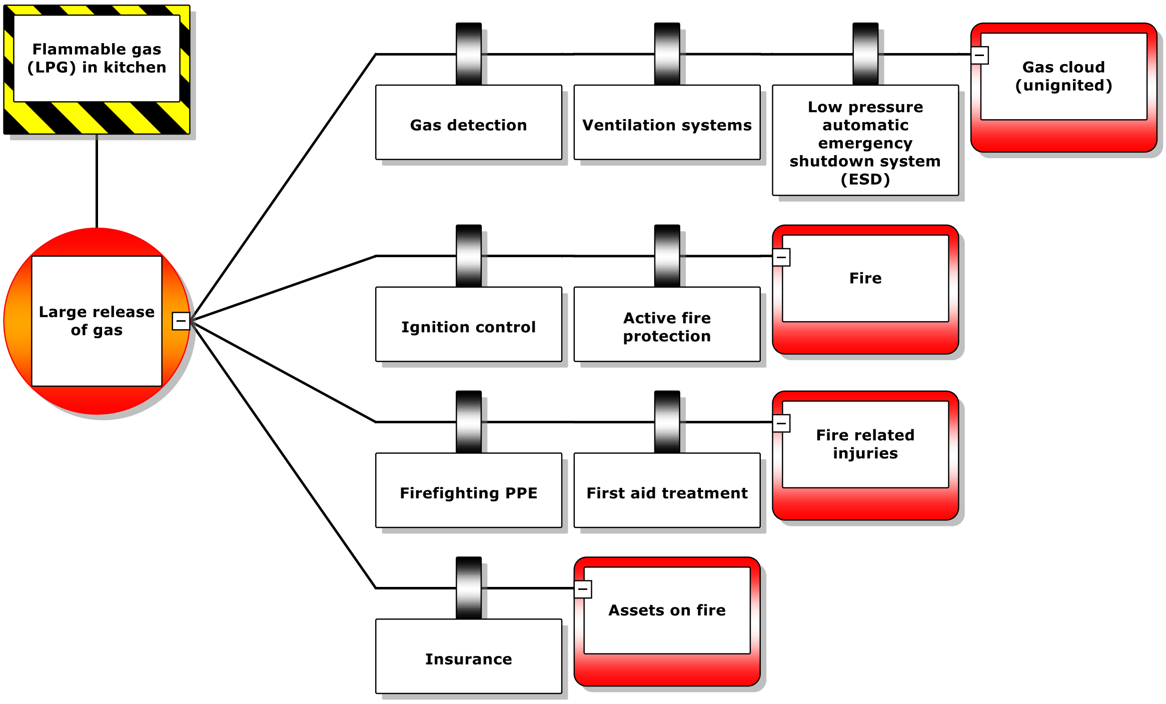


Figure 26 - More specific consequences lead to shorter barrier chains

Even though some consequences logically appear after another, in bowtie we can have these events underneath each other to avoid splitting the bowtie into multiple diagrams. Getting this right is an iterative process. It is difficult to make the right choice immediately, so be prepared to change things that you did earlier in light of the barriers that you identify.

5.6.4. The barriers you control

When a bowtie is developed, the analysis displays how well an organization is able to manage the risks that are evolving from their business operations. Because the integrity and effectiveness of barriers can only be assured by the party that is responsible for them, the focus should be on the barriers that are implemented and can be controlled by the organization itself. Adding external barriers, which are outside the direct influence of the organization, is something which has to be decided upon. It has to be a conscious decision to include such barriers, and in how much detail. It is important the bowtie will not give you a false sense of security by including barriers of which the effectiveness cannot be guaranteed by you.

5.6.5. Guidelines

Preventive barriers:

- The focus is on eliminating the threat
- Then prevent or reduce the top event
- Effect delivered before the top event

Recovery barriers:

- Has no effect upon the top event – has already happened
- Works on likelihood and scale of risks
- Effect delivered after the top event
- Effect (possibly) also delivered after the consequence

5.6.6. Workshop questions

Preventive barriers:

- Can we eliminate this threat? / What do we do to eliminate this threat?
- What do we do to prevent that this threat does not lead to the top event?

Recovery barriers:

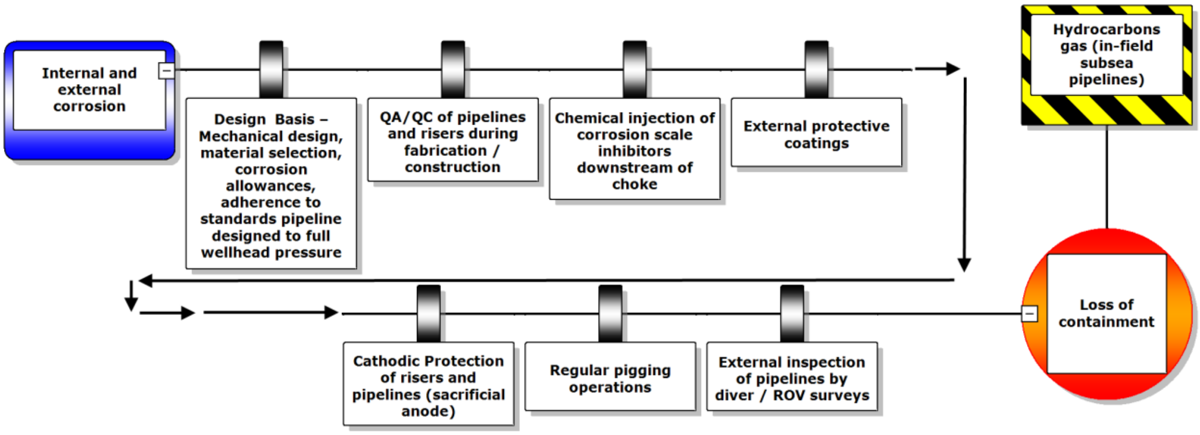
- What do we do to prevent top event from leading to this consequence?
- What do we do to reduce / limit the scale and severity of this unwanted event?
- What do we do to mitigate the significance or damage caused by this unwanted event?

5.6.7. Preventive barrier examples

TODO: Add samples for lion in a cage and driving a car

Hazard: *Hydrocarbons gas (in-field subsea pipelines)*
Top event: *Loss of containment*
Threat: *Internal and external corrosion*

Brainstorm: Corrosion of in-field subsea pipelines through which hydrocarbon gas is transported could eventually cause a loss of containment, a leak or a larger rupture. This corrosion of the pipelines could be internal as well as external and is one of the most common causes in loss of containment scenarios. Since we are well aware of the possibility of this threat, there is extensive industry knowledge on how to control it. The bowtie diagram fragment displays several preventive barriers on how to minimize the chance that corrosion causes the loss of containment of hydrocarbon gas.

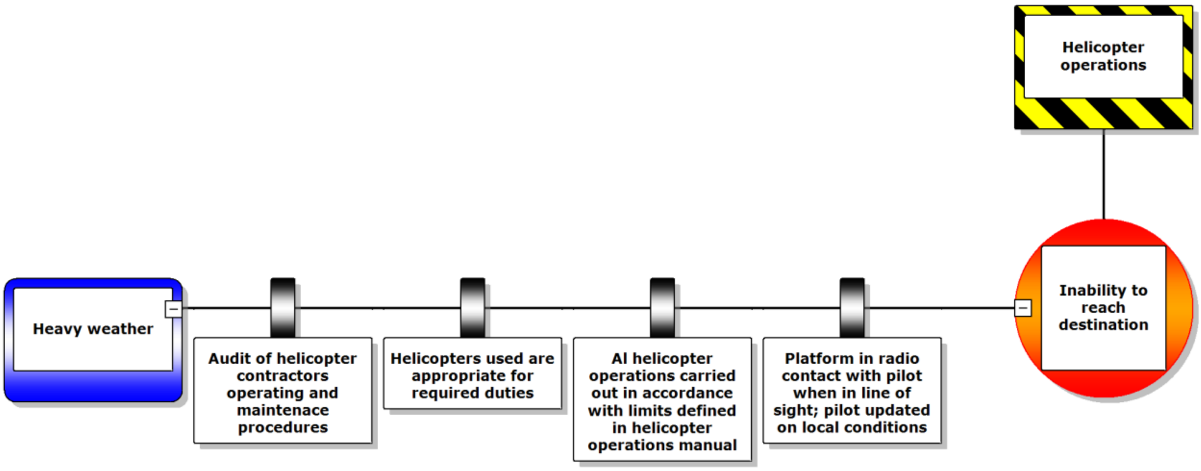

Internal and external corrosion
Design Basis – Mechanical design, material selection, corrosion allowances, adherence to standards pipeline designed to full wellhead pressure
QA/QC of pipelines and risers during fabrication / construction
Chemical injection of corrosion scale inhibitors downstream of choke
External protective coatings
Hydrocarbons gas (in-field subsea pipelines)
Cathodic Protection of risers and pipelines (sacrificial anode)
Regular pigging operations
External inspection of pipelines by diver / ROV surveys
Loss of containment

The first questions to ask are: Can we (or did we) design away the problem, and are there ways to avoid this threat? The answer in this case is the design basis barrier – mechanical design, material selection, corrosion allowances, adherence to standards pipeline designed to full wellhead pressure. The next step is to assure that the construction of the selected materials is done properly – the QA/QC of pipelines and risers during fabrication / construction.

Note: this is part of the design / construction phase of the facility and is therefore not always included in a safety case of a platform that is already operating.

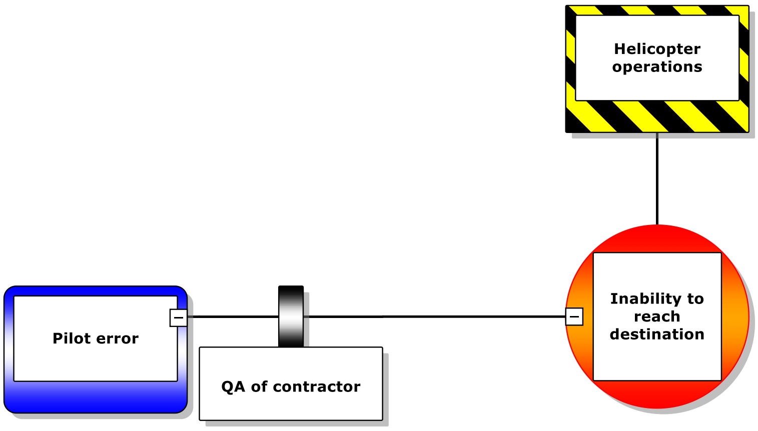
Preventive barriers that are specifically aimed at internal corrosion are the chemical injection of corrosion scale inhibitors and the regular pigging operations. Preventive barriers that are specifically aimed at external corrosion are external protective coatings, cathodic protection of risers and pipelines and external inspection of pipelines by diver / ROV surveys. Note that it is not the inspection itself that serves as a barrier but the actions taken following the results of the inspection.

Hazard: *Helicopter operations*
Top event: *Inability to reach destination*
Threat: *Heavy weather*


Helicopter operations
Heavy weather
Audit of helicopter contractors operating and maintenace procedures
Helicopters used are appropriate for required duties
AI helicopter operations carried out in accordance with limits defined in helicopter operations manual
Platform in radio contact with pilot when in line of sight; pilot updated on local conditions
Inability to reach destination

Brainstorm: We have identified that heavy weather can cause the loss of control over helicopter operations. Now we start asking ourselves: Can we eliminate this cause? Can we prevent heavy weather or helicopter transportation during heavy weather? How do we decide whether to proceed or abort this operation or not? How do we communicate about this? Is our helideck appropriate for helicopter operations (during heavy weather)? Do we have signs and/or procedures that increase the visibility during heavy weather? The answers to these questions give you the information that you need to define your preventive barriers.

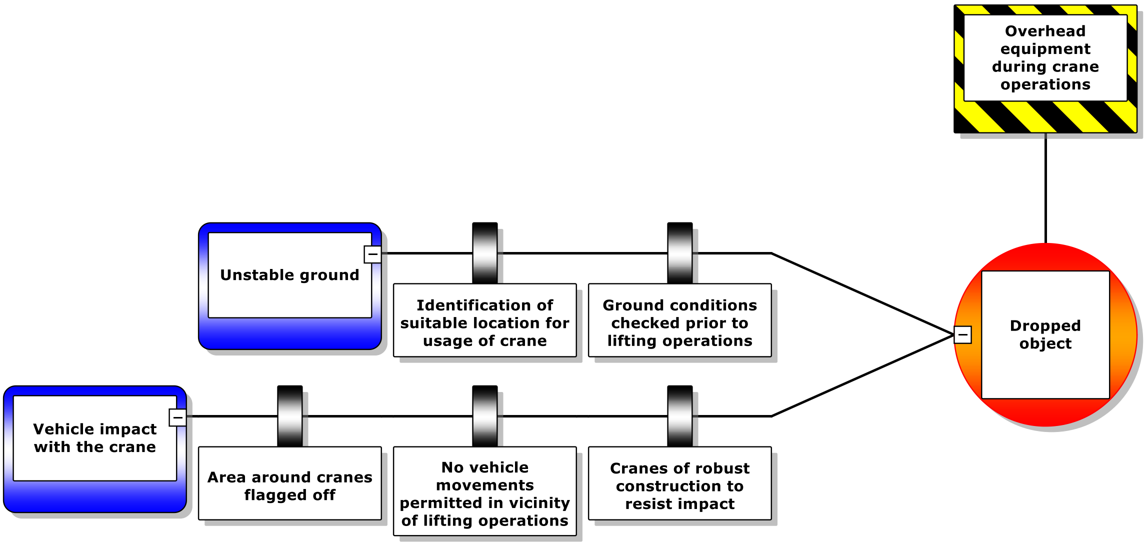
Hazard: *Helicopter operations*
Top event: *Inability to reach destination*
Threat: *Pilot error*



Brainstorm: An oil company needs to rely on the risk management procedures of you as a drilling contractor - one of the reasons why you are making a safety case. But you are also using contractors for some of your operations, for example a helicopter company. We identified earlier that a pilot making a major error could cause a helicopter filled with your people to crash onto the rig. This leads us to ask the question: what do we do to prevent that this threat leads to the top event?

The answer to that question is short: the only real thing you can do about your contractors' potential faults is to conduct a proper QA study before (and during) the contract period to assure that the contractor is managing these risks properly themselves.

Hazard: *Overhead equipment during crane operations*
Top event: *Dropped object*
Threats: *Unstable Ground & Vehicle impact*


Overhead equipment during crane operations
Unstable ground
Identification of suitable location for usage of crane
Ground conditions checked prior to lifting operations
Dropped object
Vehicle impact with the crane
Area around cranes flagged off
No vehicle movements permitted in vicinity of lifting operations
Cranes of robust construction to resist impact

During crane operations we are lifting equipment and some (or all) of the lifted load could fall down. We identified that unstable ground and a vehicle impact with the crane can be causes for a load to be dropped.

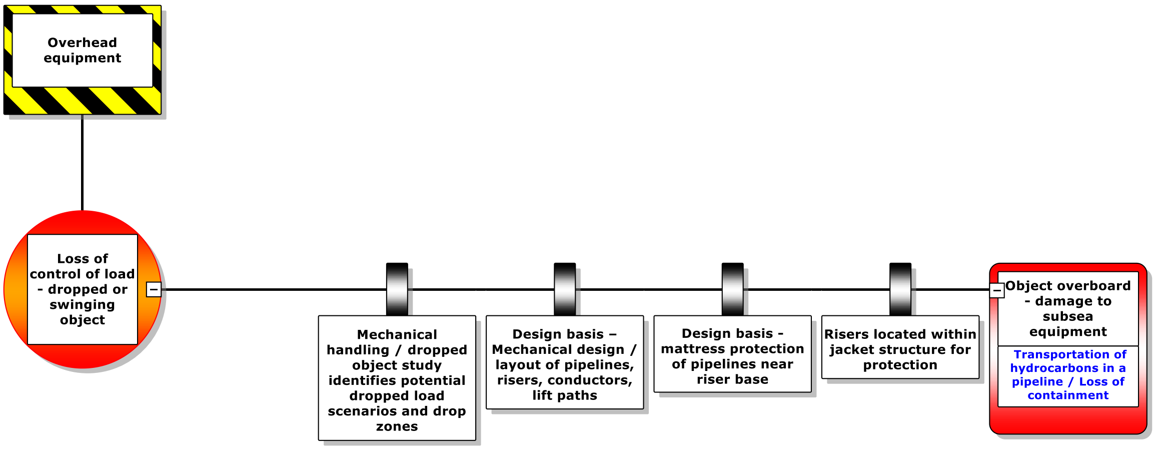
To prevent unstable ground from leading to a dropped object, we identify suitable locations for the crane (eliminate the threat), and once placed, we check the ground when commencing operations to ensure conditions have not changed.

To prevent vehicle impact with the crane, we flag off the area surrounding the crane as an indication to drivers to steer clear. We also procedurally forbid vehicle movements around the operation. These two barriers are two sides of the same coin, but are listed separately as they might have different effectiveness and responsible people. We might want to highlight that the procedural prohibition of vehicles needs to be indicated to drivers, and someone is responsible for flagging off the area. Also, we ensure our cranes are robust enough so that an impact might be withstood.

5.6.8. Recovery barrier examples

TODO: Add samples for lion in a cage and driving a car

Hazard: *Overhead equipment*
Top event: *Loss of control of load – dropped / swinging object*
Consequence: *Object overboard (damage to riser / conductors / pipelines)*

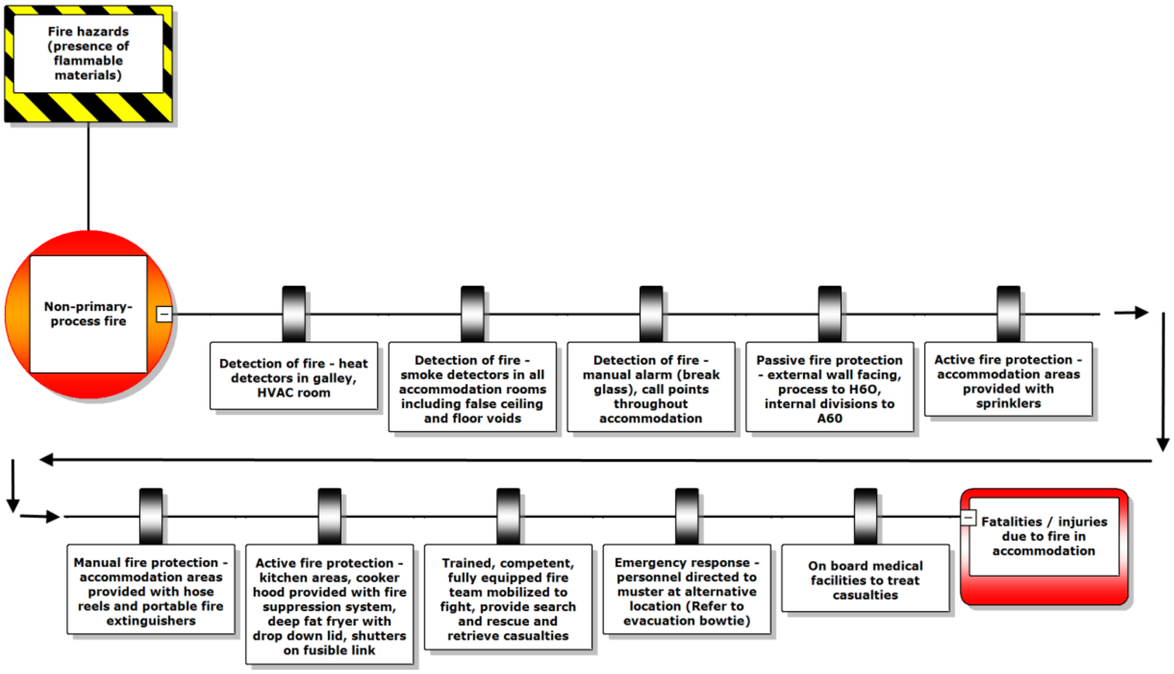

Overhead equipment
Loss of control of load - dropped or swinging object
Mechanical handling / dropped object study identifies potential dropped load scenarios and drop zones
Design basis – Mechanical design / layout of pipelines, risers, conductors, lift paths
Design basis - mattress protection of pipelines near riser base
Risers located within jacket structure for protection
Object overboard - damage to subsea equipment
Transportation of hydrocarbons in a pipeline / Loss of containment

Brainstorm: Loss of control of overhead equipment could lead to objects falling down at several locations on board but also overboard. An object falling overboard could cause severe damage to underwater equipment such as risers, conductors and pipelines. To minimize this risk there should be various recovery barriers in place. Questions to ask are:

- What is the potential drop zone of this overhead equipment and can (or did) we design out this problem? Did we take this dropping-object risk into account when determining the layout of the pipelines, risers, conductors and life paths? These are reflected in barriers 1, 2 & 4.
- Is there anything we can do to reduce the impact of potential objects falling down on subsea equipment? Answer: the design basis – mattress protection of pipelines near the riser base.

If certain subsea equipment (such as a pipeline) would be struck by a falling object, this could lead to loss of containment of hydrocarbons. For the analysis on that scenario a link is added (the blue text on the consequence).

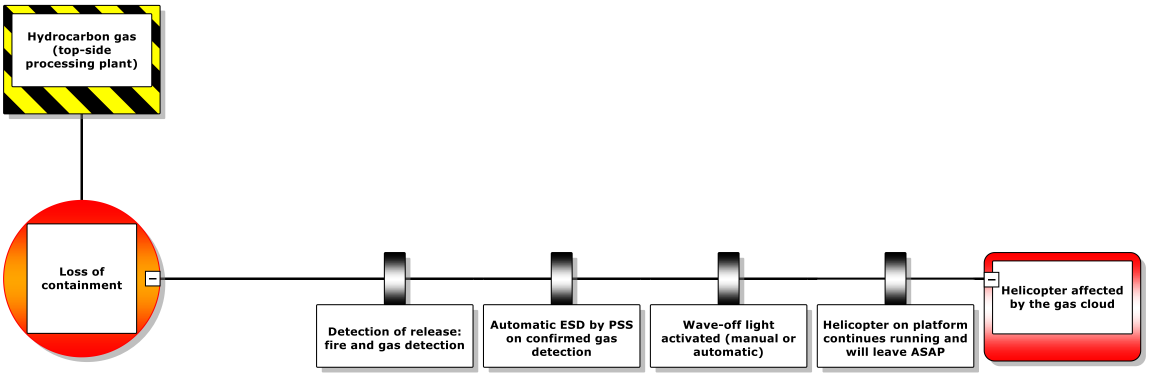
Hazard: *Fire hazards (presence of flammable materials)*
Top Event: *Non-primary-process fire*
Consequence: *Fatalities / injuries due to fire in accommodation*


Fire hazards (presence of flammable materials)
Non-primary-process fire
Detection of fire - heat detectors in galley, HVAC room
Detection of fire - smoke detectors in all accommodation rooms including false ceiling and floor voids
Detection of fire - manual alarm (break glass), call points throughout accommodation
Passive fire protection - external wall facing, - process to H60, internal divisions to A60
Active fire protection - accommodation areas provided with sprinklers
Manual fire protection - accommodation areas provided with hose reels and portable fire extinguishers
Active fire protection - kitchen areas, cooker hood provided with fire suppression system, deep fat fryer with drop down lid, shutters on fusible link
Trained, competent, fully equipped fire team mobilized to fight, provide search and rescue and retrieve casualties
Emergency response - personnel directed to muster at alternative location (Refer to evacuation bowtie)
On board medical facilities to treat casualties
Fatalities / injuries due to fire in accommodation

Brainstorm: Hydrocarbons are not the only fire hazards present on an oil & gas platform. There are also other flammable materials present which could lead to a non-primary-process fire. This hazard could be applicable to various locations but this sample we'll examine a fire in the accommodation area. One of the possible consequences of this top event could be: 'Fatalities/injuries due to fire in accommodation'. In this case the analyst chose to include the potential losses of the consequence in the description.

The recovery barriers are present to minimize the chance of this consequence occurring and to mitigate the potential losses are firstly aimed at the detection of the fire: heat detectors in galley and HVAC room, smoke detectors in all accommodation rooms and manual alarms and call points. Secondly the barriers are aimed at passive fire protection and thirdly at active fire protection: sprinklers, hose reels, portable extinguishers and suppression systems. Next to that there is a trained, competent, fully equipped fire team ready to mobilize to fight fire, provide search and rescue and retrieve casualties and there are on-board medical facilities to treat casualties. Also all the present personnel are directed to muster at an alternative (safe) location. This is part of the evacuation process and is covered in another analysis (therefore the referral).

Hazard:	*Hydrocarbon gas (topsides process plant)*
Top event:	*Loss of containment*
Consequence:	*Helicopter affected by gas cloud*


Hydrocarbon gas (top-side processing plant)
Loss of containment
Detection of release: fire and gas detection
Automatic ESD by PSS on confirmed gas detection
Wave-off light activated (manual or automatic)
Helicopter on platform continues running and will leave ASAP
Helicopter affected by the gas cloud

Brainstorm: Loss of containment of hydrocarbon gas could evolve into several unwanted events, such as a fire/explosion at the installation, injuries/fatalities on the attendant vessel and an environmental spill to sea. Another possible consequence of this top event is that an approaching or leaving helicopter is affected by the gas cloud, potentially leading to loss of control of the helicopter.

The recovery barriers to minimize the chance of this consequence occurring and to mitigate its potential losses are firstly the detection of the release and then the automatic emergency shutdown. The wave-off light is activated to alarm approaching helicopters. Any helicopter on the platform does not shut down its engine, so in a situation like this one it can leave as soon as possible.

5.7. Escalation factors and escalation factor barriers

Barriers are seldom one hundred percent effective and history teaches us that they do fail. Therefore we need to understand the factors that cause this to happen. An escalation factor is a condition that reduces the effectiveness of a barrier. An escalation factor cannot directly cause an event but increases the chance that a certain threat or top event will, by taking out a barrier.

Escalation factors can be things that are not part of usual business such as: abnormally strong winds, the loss of power or operating outside the design envelope. To help identify escalation factors, the following three escalation factor categories can be used to spark discussion:

1. **Human factors** – anything a person does to make a barrier less effective
2. **Abnormal conditions** – anything in the environment that causes a barrier to be put under strain
3. **Loss of critical services** – if a barrier relies on an outside service, losing that service might cause it to lose effectiveness

Once we have identified the escalation factors that reduce the effectiveness of our barriers the last step is to look at what barriers we have in place to manage these escalation factors. Escalation factor barriers are the same concept as all the previously discussed barriers, but now they do not prevent/mitigate a top event or consequence from happening, but they prevent a barrier from failing.

For example, the weighing of passengers is a proper (preventive) barrier to avoid helicopter overloading. The effect of this barrier can however be defeated if the used scale is inaccurate (escalation factor). To reduce the chance that the scale is inaccurate it is calibrated every year (escalation factor barrier). Next to that the weight data are always compared to previous similar flights (escalation factor barrier).

> Tip: Escalation factor barriers only work on escalation factors. Escalation factor barriers do not control threats, top events or consequences.

Escalation factor barriers can be divided into the following categories, depending on the escalation factor category:

Human factors

- Training and induction
- Supervision and mentoring
- Qualifications and certifications
- Auditing and verification

Abnormal conditions

- Prediction and proper preparation (e.g. weather forecasts)
- Maintenance and repairs
- Inspection and testing
- Redundancy and spares
- Design and specifications

Loss of critical services

- Backup systems (backup power),
- Clean shutdown systems (design / trip systems)

5.7.1. Guidelines

Escalation factors:

- Escalation factors need to be credible
- Learn from other incidents
- Focus effort on the critical barriers
- They should not cause a top event or consequence

Escalation factor barriers:

- Focus on the escalation factors
- They don't control threats or consequences
- Avoid repetition and duplication

5.7.2. Workshop questions

Escalation factors:

- Are there any circumstances under which this barrier will not work?
- How can we “destroy” this barrier?
- Has this barrier failed in the past (i.e. implicated in incidents or near misses?)

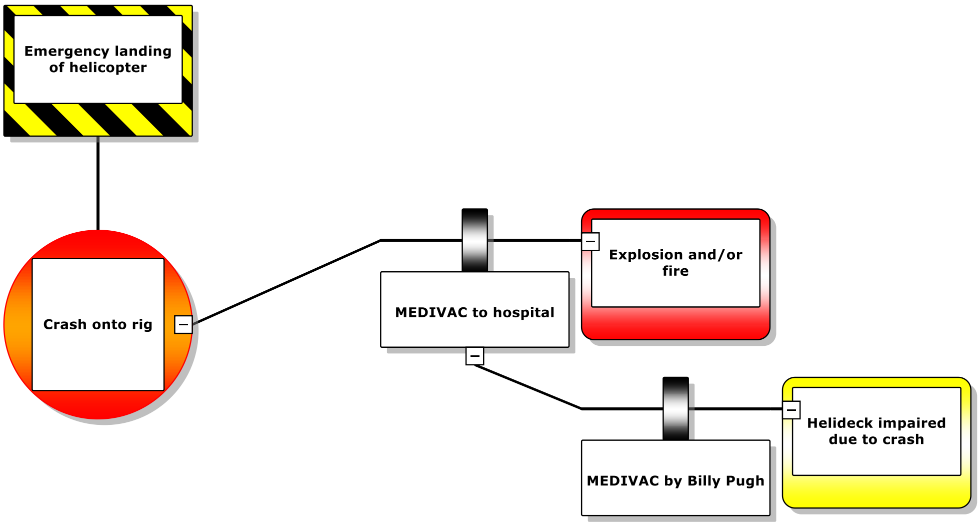
Escalation factor barriers:

- What do we do to control the condition that reduces the effectiveness of this barrier?
- Will this escalation factor automatically lead to the breaking of its barrier or do we have means to avoid this?
- Did we account for this escalation factor to exist?

5.7.3. Escalation factor examples

***Hazard**:* *Emergency landing of helicopter*
***Top event**:* *Crash onto rig*
***Consequence**:* *Explosion and/or fire*
Recovery *barrier*: *MEDIVAC to hospital*

Brainstorm: After identifying the MEDIVAC barrier we can think about why the MEDIVAC to hospital wouldn’t work. Say the pilot of a helicopter heading towards the rig and has lost control over the machine and needs to make an emergency landing. An emergency landing most often leads to or a crash into the water or a crash onto the rig. Both scenarios could cause severe loss for your organization but the latter one could also result in damage to the rig.



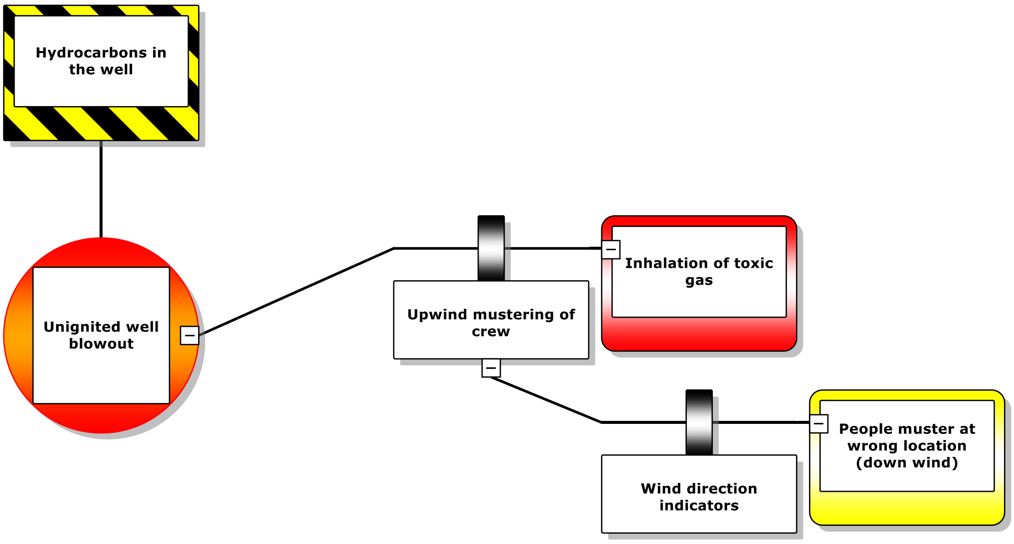
The barrier MEDIVAC to hospital exists to assure that injured people get medical attention as soon as possible, if necessary at a medical facility onshore transported by helicopter. But if the helideck is impaired, due to a crash onto the rig, the effectiveness of this barrier cannot be assured.

Fortunately MEDIVAC can also be done by Billy Pugh (a basket which can be lowered from the chopper), which serves as an alternative mean to evacuate severely injured persons.

***Hazard**:* *Hydrocarbons in the well*
***Top event**:* *Unignited well blowout*
***Consequence**:* *Inhalation of toxic gas*
***Recovery barrier**:* *Upwind mustering of crew*

Brainstorm: An unignited well blowout could lead to the inhalation of toxic gas by personnel. To make sure that this consequence is reduced / mitigated as much as possible there are several measures we have in place. One of these is the upwind mustering of the crew. However, this recovery barrier will not work if people are unaware of the wind direction to decide what is up- or downwind.

It has occurred that people accidently muster downwind instead of upwind and end up standing directly in the toxic gas flow.



This risk especially exists with low wind velocities since people their ability to sense the correct direction is limited. Wind direction indicators are in place to help determine where to muster.

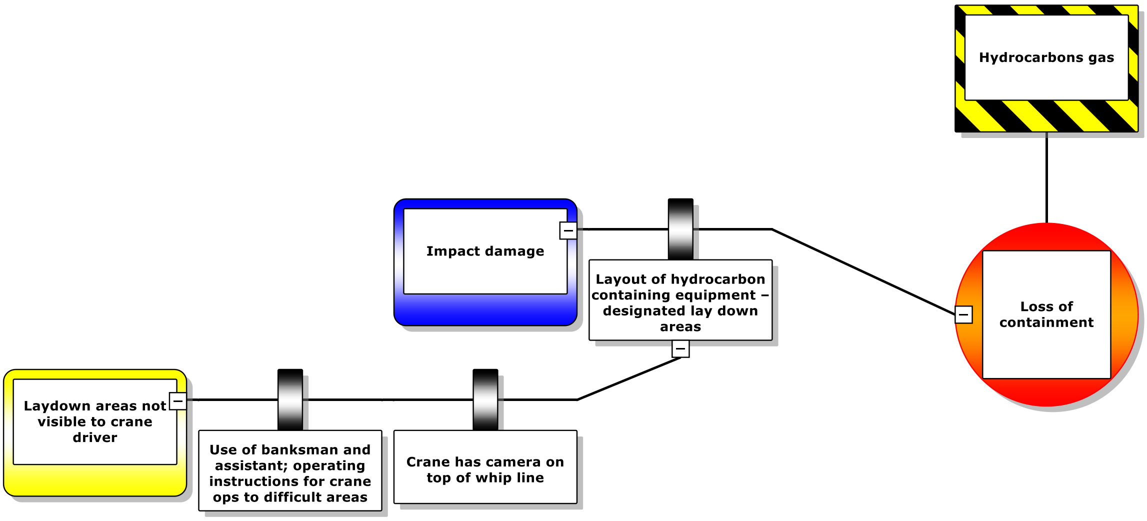
Hazard: *Flammable substances*
Top event: *Non process fire*
Consequence: *Fatalities / injuries due to fire*
Recovery barrier: *On board medical facilities*

Brainstorm: A non-process fire could lead to injuries or even fatalities in the accommodation. To avoid or reduce this consequence we have medical facilities on board to treat casualties. This barrier can be defeated when the medical facilities are impaired by the fire but also when the casualties exceed the on-board capabilities.

TODO: Add picture

Hazard: *Hydrocarbons gas*
Top event: *Loss of containment*
Threat: *Impact damage*
Recovery barrier: *Layout of hydrocarbon containing equipment – designated lay down areas*

The design basis of a facility takes into account the layout of any hydrocarbon containing equipment. Lifting and hoisting and working with heavy equipment around here is dangerous – therefore we have designated laydown areas where loose items of equipment can be laid down safely – far away from the equipment carrying hydrocarbons to ensure we cannot accidentally damage it with e.g. an impact or a dropped object.


Hydrocarbons gas
Impact damage
Layout of hydrocarbon containing equipment – designated lay down areas
Loss of containment
Laydown areas not visible to crane driver
Use of banksman and assistant; operating instructions for crane ops to difficult areas
Crane has camera on top of whip line

This preventive barrier is pretty effective in controlling the threat. However this is only the case if the designated lay down areas are visible to all people on site. If the lay down area is not properly visible this will impact the effectiveness of the barrier.

To make sure that this escalation factor does not lead to a situation with increased risk during crane operations, we have implemented two escalation factor barriers: the first one is the use of a banksman and an assistant who gives operating instructions to the crane operator in difficult areas, and the second one is the addition of a camera on top of the whip line on every crane – so the operator can also see exactly where the load is going.

5.8. Linking management system activities to barriers

To ensure that barriers will work as they're supposed to, a company has a management system. An (HSE) management system is a collection of all documentation that exists to ensure safe operations. Most often the whole system is divided into several manuals and handbooks which again refer to more specific documents and systems, such as policies, activities, procedures and standards.

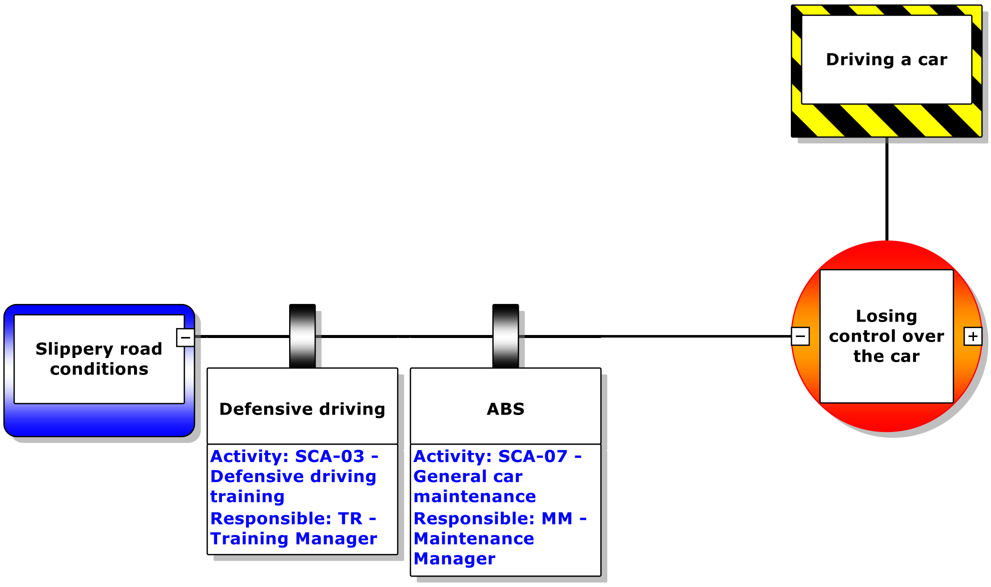

Driving a car
Slippery road conditions
Defensive driving
Activity: SCA-03 - Defensive driving training
Responsible: TR - Training Manager
ABS
Activity: SCA-07 - General car maintenance
Responsible: MM - Maintenance Manager
Losing control over the car

Figure 27 - An example of using training and maintenance activities

The safety critical activities that need to be carried out to ensure the integrity of risk reduction measures can include (but are not limited to):

- Equipment maintenance
- Equipment specification and standards
- Equipment inspection
- Employee training
- JSAs/TRAs
- Provide work procedures and checklists
- Management of change procedures / procedure review protocols

By linking the relevant parts of our management system onto the barriers, we create insight into how we as a company are supporting our barriers – what do we do to ensure their adequate operation and availability.

This information is very important to bring onto the bowtie:

- It allows us to gauge barrier effectiveness by taking into account how effective the barrier is managed.
- It helps to understand the management system – it decomposes the entire management system into safety critical elements and groups them to each barrier being supported
- It allows us to test/audit our management system from a risk based perspective

Tip: Some example activity hierarchies can be found in Appendix 1 on page 61.

5.9. Escalation factor guidelines

Now that we know about activities, let's revisit escalation factors, because there is an interesting interaction between the two. As you may have noticed, extensive use of escalation factors can make the size of the diagram explode. This reduces its readability and practical use. However, with proper use of activities, the number of actual escalation factors on the diagram will remain low, and the diagram will remain readable. In this section we'll discuss some pitfalls that should be avoided to keep the diagram readable and to the point.

The general message here: try to avoid redundancy. The strength of the bowtie method lies in its visual communicative value. Bowtie diagrams large enough to wallpaper a room will miss this purpose.

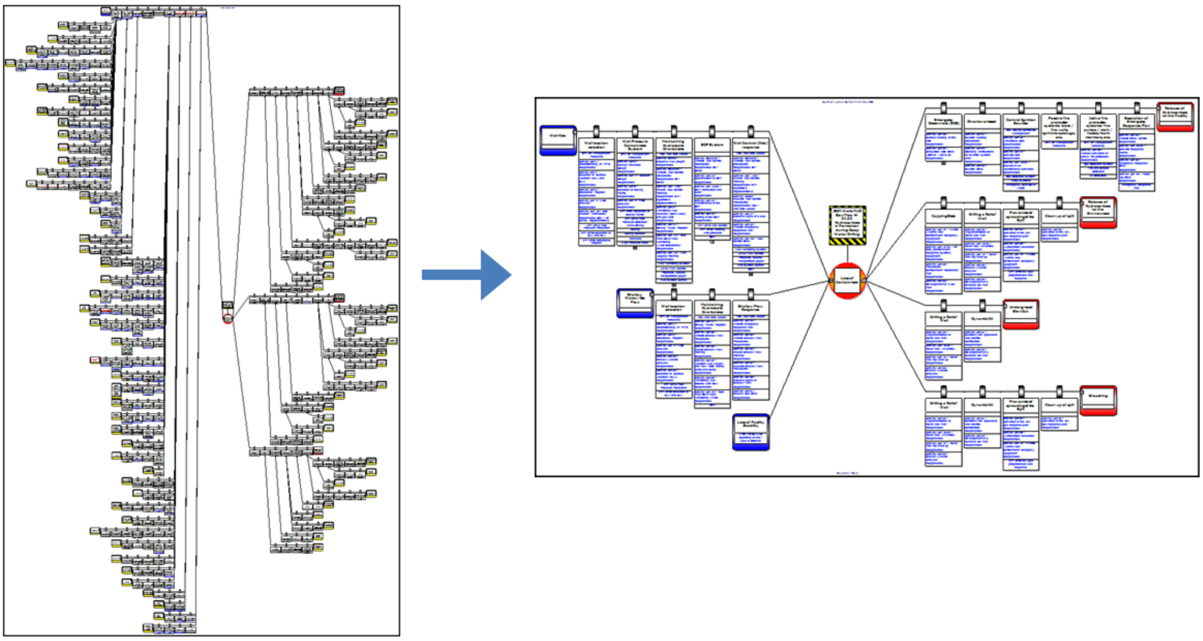


Figure 28 - Proper use of escalation factors and activities leads to readable diagrams

5.9.1. Guideline #1: activity escalation factor

Most organizations have a safety management system which implements and maintains barriers. If an activity such as maintenance is important to keep a barrier working, omitting that activity will reduce the integrity of the barrier. We could identity an escalation factor such as "maintenance not done" to communicate this, and the barrier would be to do the maintenance.

It is possible to do this, but only to highlight a real problem in your organisation. It should be avoided if it is only a possible problem. For instance, if the maintenance manager says that he's not doing the required maintenance because he does not have enough personnel available, it is possible to highlight this problem using an escalation factor. But if he's confident the maintenance is being done, still putting an escalation factor in will lead to an explosion of similar escalation factors (because you're not focusing on the critical issues, but on every possible issue).

If it is only a possible problem, but not deemed critical, we leave out the escalation factor and instead show the information by linking an activity:

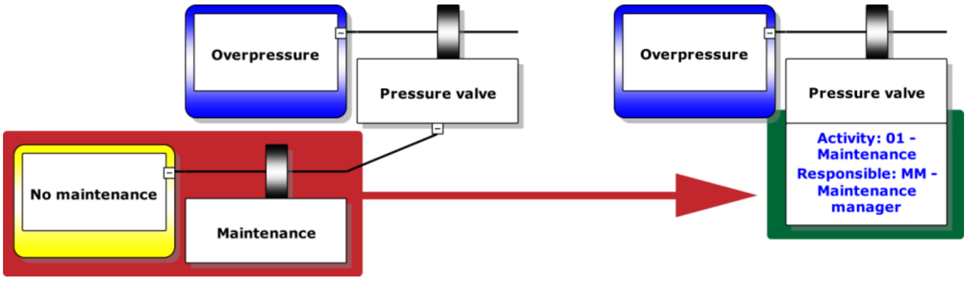


Figure 29 - Activities instead of escalation factors

It is important to understand that no real information is lost by doing this. Both communicate the need to do maintenance. One just highlights that need as a problem.

5.9.2. Guideline #2: barrier negation

Escalation factors should add extra information about barrier failure scenarios. Sometimes we see that the absence of the barrier is put into the bowtie as an escalation factor (see the example below). This does not add any additional information and so should be left out.

The barriers on this type of escalation factor often describe the activities to implement and maintain the main barrier. This makes it easy to convert those barriers into activities on the main barrier.

If an escalation factor adds a piece of information about how a barrier can fail, it’s of course justified to put it in as an escalation factor. For instance, in the example below we would like to know why there is no pressure valve, instead of just saying there is no pressure valve.

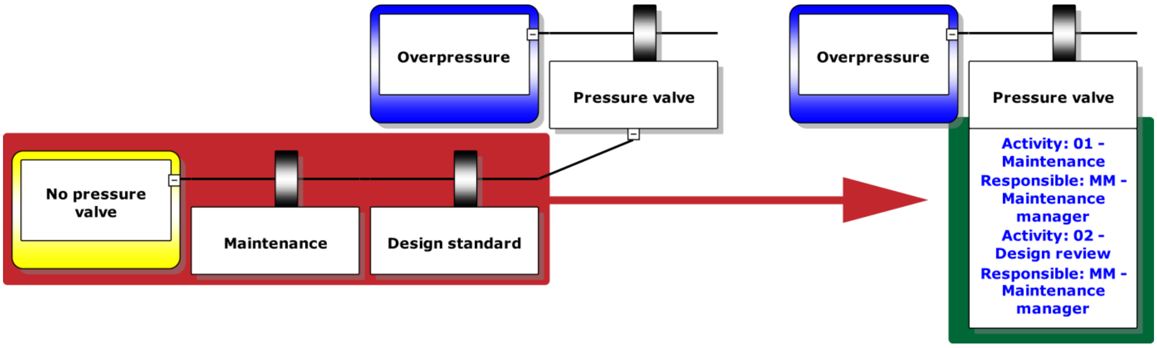

Overpressure
Pressure valve
No pressure valve
Maintenance
Design standard
Overpressure
Pressure valve
Activity: 01 - Maintenance
Responsible: MM - Maintenance manager
Activity: 02 - Design review
Responsible: MM - Maintenance manager

Figure 30 - Don't use absence of the barrier as an escalation factor

5.9.3. Guideline #3: high level escalation factors

Sometimes escalation factors in a bowtie are on a more fundamental level of the organisation. These issues, such as human error, communication failure, poor safety culture etc. run the risk of being repeated because they have an impact on so many things. This should be avoided. Obviously a poor safety culture will impact everything you do, but it is not part of the scope when you’re making a bowtie on working at height or loss of containment specifically. These subjects should contain things that are specific to that subject. Fundamental issues should be treated separately from a specific bowtie because mixing them will cause your diagram to grow larger. Instead, make a separate bowtie on human error. That way, you cover the issue, but it does not dilute the specific focus of other bowties.

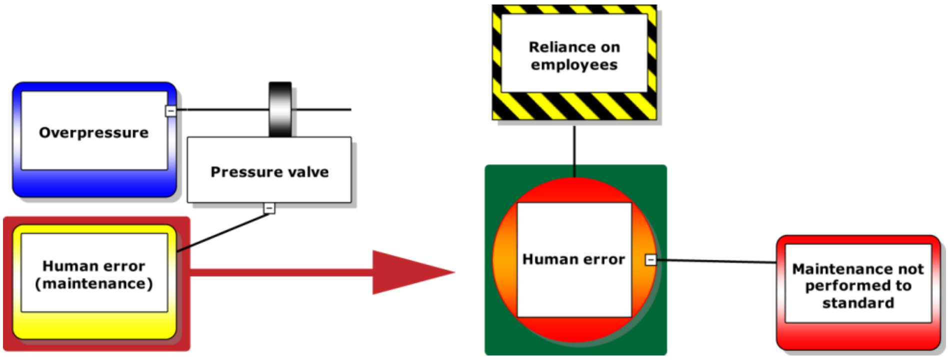

Reliance on employees
Overpressure
Pressure valve
Human error (maintenance)
Human error
Maintenance not performed to standard

Figure 31 - don't add generic escalation factors - do a separate bowtie if analysis is needed

5.9.4. Guideline #4: Barrier failure bowties

Sometimes an important barrier occurs multiple times in a bowtie. If this barrier also has multiple escalation factors attached to it, the bowtie will quickly grow larger as the same escalation factors are repeated on each barrier. To solve this issue, you can make a separate bowtie on this barrier. The hazard in such a bowtie becomes the barrier itself, the top event becomes the barrier failure, and all the escalation factors and barriers can be put in as threat lines. This bowtie will only have a left side, because once the barrier fails, you go back to the main diagram, where the next event in that bowtie is now more likely to occur.

5.10. Completing barrier information

5.10.1. Barrier types

Once we've identified our barriers, it is time to look a little closer at how we can characterize or classify those barriers. There are several ways to go about this. In this case, we'll discuss two complementary ways of classification. First, barrier function, which describes the purpose of a barrier. Second we'll discuss different types of barrier systems that can fulfil a function. There are other ways of classifying barriers (like the Hierarchy of control idea), but we'll describe this approach. Before deciding on a barrier type set, please review the alternatives in the literature.

> Note: The following barrier types are meant to be guiding, as are all guidelines in this publication. Perhaps your organisation has other rules to define barrier types and functions.

Before we dive into barrier functions and systems, we should ask ourselves why we want to classify barriers in the first place. There are two main reasons. The first reason is to prompt us to think outside of what is currently there. For instance to consider implementing a different function, or add a different type of system. It gives us an idea of what else we can do. Second, it allows some heuristics and aggregations to be done using those classifications. For instance, we could analyse how a whole group of barriers is doing by looking at a single function or type of system.

5.10.1.1. Barrier function

Barrier function is a relative property that describes why a barrier exists. It's relative because it relates to the scenario that it is on. Because of this, a barrier can have a different function, depending on where it appears in a bowtie. We split up barrier function in five types.

1. **Eliminate or substitute the hazard:** This type of function doesn't come back in the bowtie diagram, but eliminating or substituting a piece of the organisation because it is hazardous is always the ultimate barrier. However it will no longer be necessary to create a bowtie on hazards that are eliminated or substituted. Therefore, this type of barrier function cannot be displayed on the bowtie. When we decide a hazard cannot be eliminated or substituted, we should have some justification for it (usually it's needed for business and there are no harmless substitutes). Also list the reasons for not eliminating the remaining hazards. This will lead us to think about the possibility of eliminating our hazards instead of thoughtlessly accepting them.
2. **Eliminate the threat:** Any barrier that tries to remove the possibility of a threat in its entirety has an elimination function.
3. **Prevent the top event:** If the threat can't be eliminated, there are still barriers that try to prevent the top-event from occurring.
4. **Separate the consequence:** Once the top event has occurred, barriers can be put in place to stop a top event from leading to a consequence. Even though the term is different, it is logically equivalent to a prevent barrier, only it is one step further in the causal chain.
5. **Mitigate the consequence:** Any barrier that helps limit the knock-on effects of a consequence can be considered mitigation barriers.

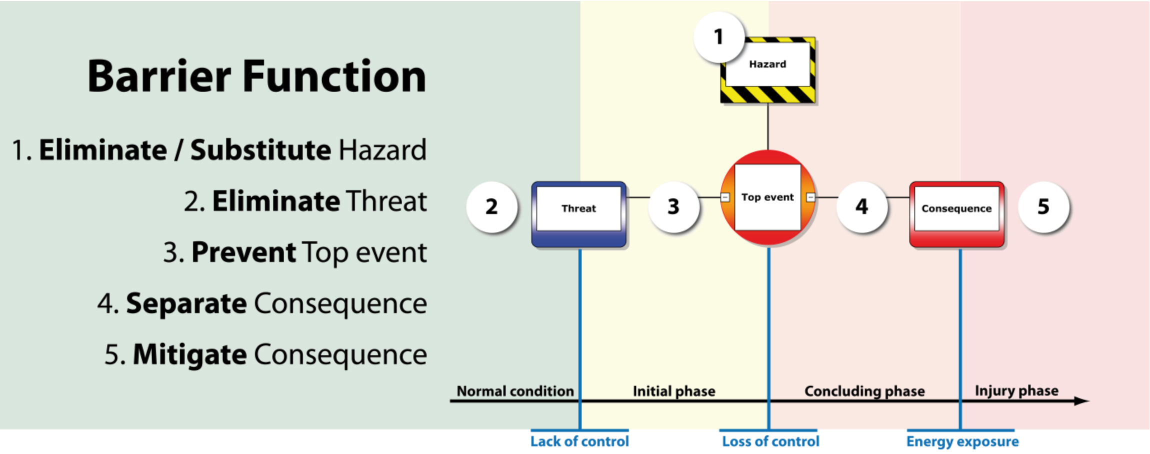


Figure 32 - Barrier functions

5.10.1.2. Barrier system

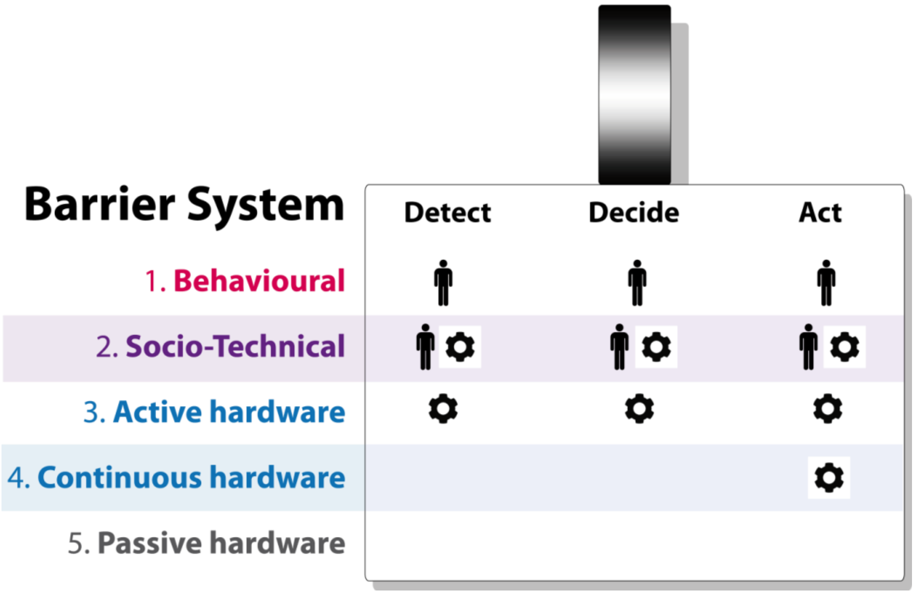
Besides identifying what type of function a barrier has, one can also identify the different types of systems that can implement a function. These systems usually consist of either some type of hardware, behaviour or a combination of both.

There are different ways to classify these systems. In this example we use five different categories: Behavioural, Socio-Technical, Active hardware, Continuous hardware and Passive hardware.

Depending on the category, a barrier can contain three distinct parts. A detection mechanism, a decision based on what's detected, and an action that follows the decision. When analysing a barrier, one needs to identify its parts, and whether those parts are behavioural or technical in nature. The different combinations determine the system type.

For instance, a double check is a purely behavioural barrier because the detection, decision and action are all behavioural. Another example could be a sprinkler system that is activated by pressing a fire alarm button. The detection and decision are behavioural, whereas the action is technical, which makes it a socio-technical barrier. A fence or dyke does not detect, decide or act. Its existence alone is enough to have an effect (we're leaving maintenance out of the discussion, as that is on a different level and not part of the barrier itself), which makes it passive hardware.

1. **Behavioural barrier:** the detect decide act parts of the barrier are completely represented by people
2. **Socio-technical:** the detect decide acts parts of the barrier are a mix between people and hardware
3. **Active hardware:** the detect decide act parts of the barrier are completely hardware based
4. **Continuous hardware:** a barrier with no detection, but a continuous action (like for instance a ventilation system)
5. **Passive hardware:** is effective by just existing without any need for explicit action. Does not have detect decide or act parts.



Barrier System	Detect	Decide	Act
1. Behavioural	🧍	🧍	🧍
2. Socio-Technical	🧍⚙	🧍⚙	🧍⚙
3. Active hardware	⚙	⚙	⚙
4. Continuous hardware			⚙
5. Passive hardware			

Figure 33 - Barrier systems

The added advantage of categorising barrier systems is understanding the diversity of barriers. More diversity in the type of barriers you have is generally better. Having only behavioural barriers or only hardware barriers makes a system vulnerable, not only because barriers of one type can compensate for the weaknesses of other types, but also because barriers of the same type are more vulnerable to common mode failure.

5.10.2. Barrier responsible persons

For all identified barriers we need to define who is responsible for its current and future state. Usually a job title / position title is linked to a barrier but it could also be a person's actual name. Depending on the purpose of the bowtie (for operational use or for risk assessment) one of the two is chosen.

The advantage of assigning responsibility is three-fold:

1. Everyone in the organization can see his or her responsibilities in the context of risk scenarios, making it visible what might happen when a barrier is not properly maintained.
2. By going through the barriers and assigning responsibilities, the chance of having a barrier that no one is responsible for is reduced.
3. The organization can analyse where a single person is responsible for all barriers on a scenario line, and spread the responsibility for more resilience.

Responsibility for barriers can be divided into two layers: responsibility for the integrity of the whole barrier and responsibility for the execution and quality of management system activities that are linked to that barrier.

5.10.3. 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, to gain some more insight into what effectiveness is, we'll break it down into two main elements: adequacy and reliability.

5.10.3.1. Adequacy

If you look at defensive driving as a barrier, it actually features on multiple Threats. However, defensive driving is not equally effective for each of 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 differ depending on the scenario that it is controlling. This is also the main reason why you should not copy paste Barriers with an effectiveness rating: It could be that the effectiveness is different, because the adequacy is different.

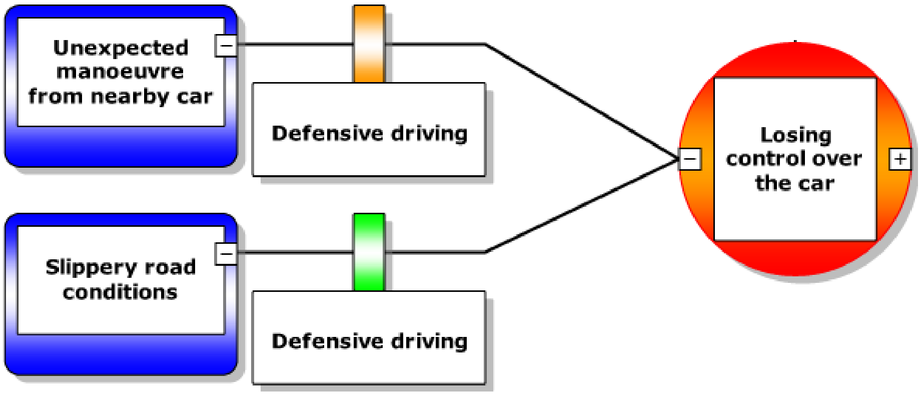

Unexpected manoeuvre from nearby car
Defensive driving
Slippery road conditions
Defensive driving
Losing control over the car

Figure 34 - An example of adequacy being different across scenarios

5.10.3.2. 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, the barrier "Wearing a seatbelt" has an Escalation factor, which reduces the reliability, so we need to adjust the effectiveness of wearing a seatbelt to medium (indicated by the yellow color). An airbag (if properly installed) will almost always expand during a crash situation and is therefore highly reliable. However, the seatbelt may not be worn at the time at the incident. In that case it will not respond when challenged and has thus a lower reliability.

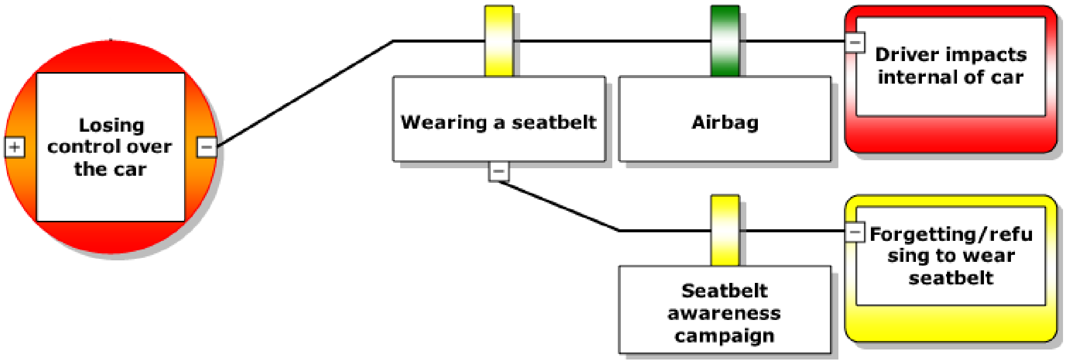

Losing control over the car
Wearing a seatbelt
Airbag
Driver impacts internal of car
Seatbelt awareness campaign
Forgetting/refusing to wear seatbelt

Figure 35 - An example of an escalation factor impacting the reliability of a barrier

5.10.3.3. Other aspects of effectiveness

Threats, top events and consequences are not the only things that need to be taken into account when assessing effectiveness of a barrier in relation to a scenario. The management system activities are also part of the scenario. The effectiveness of a barrier cannot be determined without taking into account how well the attached management system activities are executed. For more information on other dimensions of effectiveness which are not discussed here, read the excellent article about barriers, definition, classification and performance by Snorre Sklet (Sklet, 2006).

6
Risk evaluation

The main question we want to answer in this chapter is whether the current level of control is sufficient or whether we need additional barriers to control the risk further. We need to discuss the concept of ALARP (As Low As Reasonably Practicable) before we show how ALARP is used in bowtie to answer this main question.

6.1. Overview of ALARP

The amount of risk can always be reduced further, up to a point where a company goes bankrupt to avoid risk. This is why the amount of risk is always a trade-off between what is practicable given the available resources, the risk reduction and the original risk. The HSE UK says: "In essence, making sure a risk has been reduced ALARP is about weighing the risk against the sacrifice needed to further reduce it." In order to do this, there are three things that need to be looked at.

- The inherent risk level
- The risk reduction gained by introducing a new barrier for that risk
- The sacrifice in time, money and trouble needed to implement that new barrier

		Sacrifice (time, money, trouble)								
		Low			Med			High		
Risk reduction	High	High risk	Med risk	Low risk	High risk	Med risk	Low risk	High risk	Med risk	Low risk
		Go	Go	Go	Go	Go	Go	Go	Go	Stop
	Med	High risk	Med risk	Low risk	High risk	Med risk	Low risk	High risk	Med risk	Low risk
		Go	Go	Go	Go	Go	Stop	Go	Stop	Stop
	Low	High risk	Med risk	Low risk	High risk	Med risk	Low risk	High risk	Med risk	Low risk
		Go	Go	Stop	Go	Stop	Stop	Stop	Stop	Stop

Table 1: ALARP concepts

These three things can vary, and depending on all three, we might decide that a risk is already ALARP, or needs an additional barrier to reach ALARP. Table 1 lists an example of how these dimensions interact. We see that if the sacrifice is low, most additional barriers would be implemented. The only category where we are already ALARP is if the risk reduction of the barrier is low, and the inherent risk is also low. If the sacrifice is medium, more categories can be marked as ALARP, because they do not justify the additional investment. For instance, a low risk reduction on a medium risk is not justified if the sacrifice is medium. A high sacrifice marks even more categories as ALARP. In general, we're not going to bother with barriers that have a low risk reduction and high sacrifice, no matter how large the inherent risk is. But we see that even a high risk reduction does not justify the high sacrifice if the inherent risk is low, meaning we are As Low As Reasonably Practicable in those situations. This is obviously an abstract example, but hopefully it communicates how these three dimensions interact.

6.2. ALARP in Bowtie

Now that we have an idea on what ALARP means, we can see how this high level concept is used in bowtie. The process can be broken down into five steps.

Current risk

1. Determine the inherent risk present in the bowtie. This will be the baseline.
2. Identify the risk reduction achieved by existing barriers. This will determine how much the inherent risk is currently reduced.
3. Determine the residual risk by adjusting the inherent risk with the risk reduction of the barriers.

ALARP evaluation

4. Investigate additional barriers to reduce the risk further and estimate the sacrifice necessary to implement them.
5. Weigh the residual risk against the risk reduction and sacrifice of additional barriers to determine whether the residual risk is already ALARP or requires you to implement additional barriers.

We'll describe each step in detail below.

6.2.1. Inherent risk

There are two sides to a bowtie. We'll start at the left hand side and work our way to the consequences on the right to determine the inherent risk.

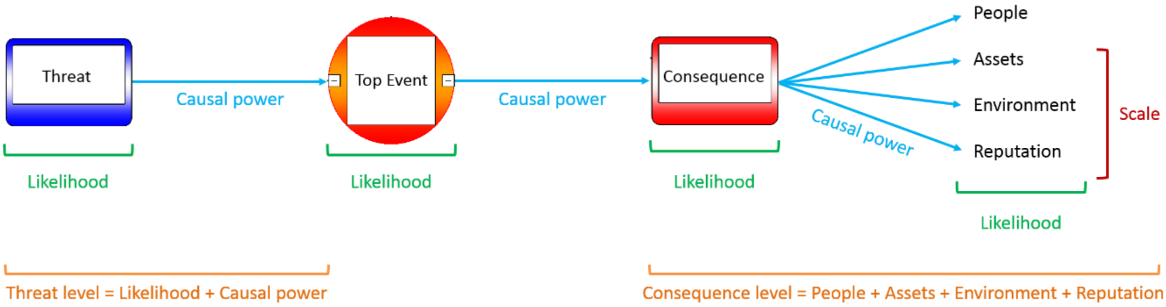


Figure 36: Diagram explaining the causality in the bowtie

6.2.1.1. Proactive side assessment

Assessing the left side of the bowtie focuses mostly on the likelihood of the top event. To do that, we first estimate each threat. Most people focus on the frequency or likelihood of a threat. Here we go one step further and introduce two variables on each threat: causal power and likelihood (also see Figure 36). We need these two aspects because a threat can occur without leading to the top event.

For instance, loss of attention does not always lead to loss of control over car, whereas a tyre blowout will almost always lead to loss of control. So besides the likelihood of the threat occurring, we also score its causal force, which gives us an indication of how likely it is that the next event will take place if the threat occurs. The likelihood and causal force combine to give us an idea of how serious we should take a particular threat. To estimate the likelihood of the top event, we sum the scores for all threats together.

Of course it’s not always necessary to split them out explicitly. But it can be useful in the discussion to break the assessment apart into these two aspects, to be able to come to a final judgement for each threat.

6.2.1.2. Reactive side assessment

The right hand assessment is similar but slightly different. For every consequence, the top event has the same likelihood, but a different causal power. The logic on the left side of the bowtie also applies to the right side. The occurrence of a top event does not necessarily lead to a consequence. After control over the car is lost, it is more likely to lead to a crash into another vehicle than it is to drive into the water. These differences in causal power lead to different likelihood scores on each consequence.

Up until now the right hand side is pretty similar to the left. We just use likelihood and causal power to tell us what the likelihood of the next event is. The last step also uses causal power and likelihood, but introduces the concept of scale on top of that.

A consequence appears to be the last step in the bowtie, but we still need to look at the damage that can be caused by this consequence. There are generally four categories of damage: People, Assets, Environment and Reputation (or a variation on those). These different kinds of damage are visually incorporated into the consequence, so a consequence is grouped together with the kinds of damage it causes. The likelihood and causal power of the consequence together lead to the likelihood of each type of damage. This is the same as before because the damage that a consequence causes is just another event (for example, a consequence fire can lead to an event fatality).

There is one difference: we look at the scale of the damage instead of its causal power. Looking at a risk matrix, the two axes are likelihood and severity (aka, scale). These dimensions are what we want to use for damage. Once we've assessed the likelihood and a credible scale for the damage, we have our inherent risk. This risk is not a single number. It is spread across many damage categories on each consequence. Now that we have an idea of the inherent risk, let's discuss how the risk reduction of barriers is integrated.

> The likelihood of the damage is often equated to the likelihood of the consequence. Although this is not necessarily true (the likelihood of a fire is not the same as the likelihood that a fire will cause a fatality), in some cases it might not matter. It can actually save a lot of time to assume that the likelihood of the consequence and the damage that the consequence causes are the same. However, be aware that even a consequence has a different causal power for certain kinds of damage, which influence the likelihood of that damage.

6.2.2. Barrier risk reduction

Determining the risk reduction of a barrier is very tricky and often a subjective judgement. We'll start by discussing the risk reduction of a single barrier, and after that the combined risk reduction of multiple barriers.

The impact of a barrier is largely determined by its effectiveness (which has been discussed in chapter 5.10.3). Note that effectiveness is only relevant in relation to the threat or consequence that it is on. On its own it does not tell us anything about the overall risk reduction. Think of it like this: barrier effectiveness describes the risk reduction for one scenario only, so two barriers with equal effectiveness in different scenarios do not have the same risk reduction, if the scenarios are different in likelihood or scale. Once we have the effectiveness of a barrier and understand its scope, it is time to take the next step and look at how multiple barriers work together to increase risk reduction.

One of the primary ideas behind the bowtie and barrier thinking in general is having multiple barriers that can compensate for each other, such that if one fails, there is still some other barrier that takes effect. The idea that more barriers will increase the risk reduction is one we will discuss in more detail.

In theory it does not matter if we have one very good barrier or multiple medium ones. However in practice it is very difficult to get a very good barrier that we accept as completely reliable and adequate, so we need multiple flawed barriers, because the perfect barrier does not exist.

When deciding how many barriers are necessary, it is also important that the barriers are as independent as possible to decrease the likelihood that all barriers fail simultaneously. There are a number of ways to assess this level of dependency.

- First, see if a single person is responsible for multiple barriers in a scenario.
- Second, see which barriers rely on the same underlying management system activity (like a maintenance activity) or system (like power).
- Third, look at any common escalation factors.
- A fourth high level dependency assessment can be done by looking at barriers with the same barrier type. For instance, if all barriers are hardware, it is more likely for them to fail simultaneously, although looking at barrier types does not tell you how that will happen exactly.

All of these things make it more likely that there is a shared vulnerability. Perhaps the easiest way to take into account the dependencies between barriers is to start by summing the effectiveness values of individual barriers, and then correct that sum with the level of dependency between the barriers on a line. We won't go into further details. This might seem like dodging the subject, but it is more important to be aware of the ideas, and decide on how to implement the details yourself.

6.2.3. Residual risk

Assessing the impact of a barrier on the risk is done differently on both sides of the diagram. A barrier that is added to the left lowers the likelihood of a top event or threat, and indirectly lowers the likelihood of all the consequences. A barrier that is added to the right of the diagram has a direct influence on the consequence line it is on. If the barrier stops the consequence from occurring, it has an effect on the likelihood. If it doesn't stop the consequence, but mitigates the damage (and logically takes its effect after the consequence), it has an effect on the likelihood or scale of the damage. Because of this, the assessment is done in three different ways: the left hand assessment, the right hand assessment, and the mitigation assessment.

6.2.3.1. Proactive side assessment

On a high level, what we do is take the threat, and correct it with the impact that the barriers have. This will result in a residual score that indicates how often the top event is caused by that threat. All threat scores are summed to give a final likelihood for the top event.

6.2.3.2. Reactive side assessment

The effect of the barriers on the right side of the bowtie is split into either preventing the consequence from occurring, or mitigating the damage. For those that prevent the consequence, the process will be very similar to the left hand side. The likelihood of the consequence is corrected by the overall effectiveness score of the barriers on that line.

6.2.3.3. Mitigation assessment

There are barriers that try to minimize the damage. We call them mitigation barriers. First-aid is a typical example of a mitigation barrier. These have an impact on the scale or likelihood of the damage. The assessment of these barriers is done by correcting the scale or likelihood of the damage by the impact of the barrier.

6.2.3.4. Bringing it together

Don't forget that all of the barriers in the end have an impact on the damage. You should make sure that your assessment reflects this. For example, the risk reduction of a barrier on the left side of the bowtie should have an impact on the likelihood of damage on the right hand side, via the top event and consequence.

6.2.4. Additional barriers

Once the residual risk is known, it is time to investigate options to reduce the risk further. Start by brainstorming ideas for new barriers, and estimate how much risk reduction you would get and the level of sacrifice necessary to implement them.

6.2.5. ALARP

The last step is to take these three outcomes: the residual risk in the bowtie, the estimated risk reduction gained by a new barrier, and the sacrifice to implement it. Then weigh them similarly to the high level example that we started this chapter with. There are two possible outcomes: the risk is already ALARP, because the risk or risk reduction is too low, or the sacrifice is too high. The other possibility is that the risk is not ALARP yet, because either the risk is still too high, the risk reduction is high enough to make it worthwhile, or the sacrifice is low enough to justify implementing the barrier. Obviously, there is a large grey area where these three variables interact. All actions that can be taken to make the risk ALARP, can be made into an action plan.

This concludes the basic bowtie process. The next phase of the project will be to first make sure the remedial actions really get implemented, and second to communicate the content of the bowties in the organisation. This will be the subject of the next chapter.

7
Bowtie implementation

In some ways, the most crucial phase of a bowtie project comes after the bowtie diagrams have been built. It is the most crucial because this is where projects tend to fail. Because of this, it is important to spend some time to plan what will be done once the bowties are finished. Just keep the original goal in mind, which is never to just build bowties. There is always a follow-up to actually achieve the goal of the bowties.

7.1. Implementation

Here are some areas to think about when implementing bowties:

- One easy win to implement the bowties is to communicate and distribute the bowties, for instance with posters or reports, to the intended audience (whether it's the workforce, management or a regulator).
- Another area to look at is integration with training or induction programs. Use the bowties to train new people, and stir discussion among existing employees.
- Using the bowties for a safety case to demonstrate ALARP to a regulator is probably the most common type of implementation. An important note to understand is that the audience for a safety case is the regulator. Often, a safety case is not perceived as useful by operations, because it was not written with them in mind. It is likely to contain a lot of information that is not relevant to them, so it is likely they ignore everything, including the relevant pieces.
- Often the bowties contain valuable information to update the management system
- And we can't say this enough: track the actions that come out of the bowties and make sure something actually changes.

7.2. Monitoring

Once the bowties are identified and implemented, it is easy to consider the job done and close the bowtie project. This is probably not a bad idea when first starting with bowties to keep the scope small and not bite off more than you can chew. However, the next step with bowties is to use them as a monitoring tool. The bowties give you an excellent risk based control framework which can be used in auditing, referenced in incidents, and applied within operational decision making. An organisation is not a static thing, and monitoring that everything stays ALARP using the bowties is a good idea.

7.3. Revisions and change management

Because an organisation is not static, you also need to plan when the bowties will be revised and updated. Whereas monitoring is checking to see how things change within the organisational structure, change management needs to be done to ensure the changes to an organisational structure itself do not unacceptably increase the risk.

There are two main approaches to do this. One is a periodic revision, regardless of any real world changes. The second is event driven revisions, where a structural change can trigger a revision of the bowties. Ideally both approaches are combined. Periodical revisions are necessary because not all structural changes trigger a revision. Event driven revisions are necessary because big changes between periodical revisions can leave us unprepared while we wait for the next review.

Appendix 1

Sample SMS outlines

In this appendix we show some ways in which management systems are organized, as seen in various companies across industries.

Company A

1. Manage Operations
    - Process Operations
    - Export Operations
    - Manage Process Changes
2. Logistics Operations
    - Marine Logistics Operations
    - Aviation Logistics Operations
    - Lifting and Load Management Operations
    - Materials Management
3. Maintenance Activities
    - Wellhead System Maintenance
    - Safety System Maintenance
    - Lifting Equipment Maintenance
4. HSE Management
    - Safe Systems of Work
    - HSE Inspection and Audit
    - HSE Communication
5. Emergency Response
    - Emergency Response Planning
    - Emergency Response Arrangements
6. Integrated management system
    - Policy
    - Planning
    - Implementation
    - Monitoring
    - Review
7. Operating Instructions

Company B

1. Company management system
    - Maintenance Management System
    - Environmental Management System
    - Quality Management System
    - Safety Management System
    - Training Manual
    - Human Resources Manual
    - Emergency Response Plan
    - Well Control Manual
    - Auditing and Monitoring Manual
    - Medical Protocols Manual
    - Job Safety Analysis Register
2. External management systems
    - Bridging Document References

Company C

1. Design
    - Prepare Specification
    - Prepare Designs
    - Purchase / Construct Plant
    - Commission New Plant
2. Operate
    - Process Units
    - Storage Facilities
    - Export Facilities
    - Lifting Operations
3. Maintain
4. Manage
    - Emergency Preparedness
    - Security
    - Emergency Response
    - Training
    - Supervision
    - Safe Systems of Work
    - Audit and Inspection
    - Contract Management

Appendix 2
A sample bowtie

We have already seen one small sample bowtie in the introduction. We'll now show another one. Note this sample is limited in size – we do not attempt to show all threats and consequences, we only discuss a subset to illustrate the concepts.

You are the safety manager for a package delivery service. A lot of the employees drive cars to deliver the packages.

Let's start with the first four steps:

1. Identify hazards - What could be a potential source of risk?

Driving a car is something so must do for your business, but has the potential to cause harm. You might be involved in an accident. The driving of a car is a source of risk, a hazard in bowtie terms. For this sample, we will focus on the driving of the car on the highway. This allows us to be more specific.

2. Identify top events - When do we lose control over this hazard?

When driving a car, the moment where we lose control is the moment we lose control over the vehicle. That is the point in time where the process (of driving) is no longer controlled, and consequences might happen. Note that they do not have to happen, we can still recover.

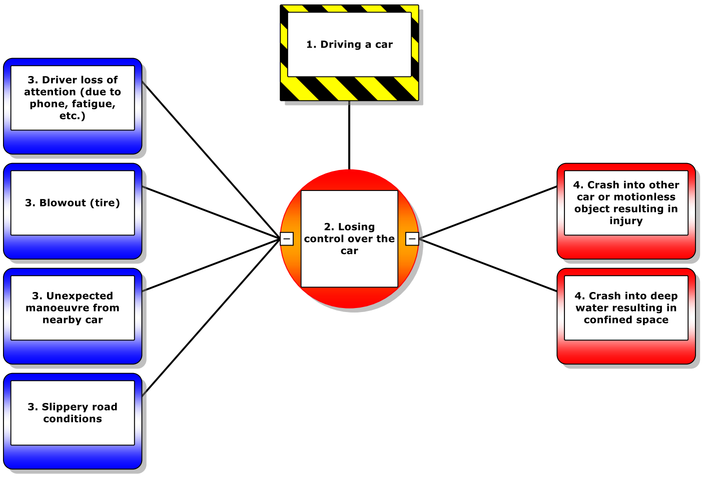
3. Identify threats - How could we lose control over this hazard?

So how can we lose control over the vehicle? This might happen because the driver loses attention – because the driver is tired, or on the phone. A tire might fail. Another vehicle might make an unexpected manoeuvre for which we cannot compensate. Perhaps the condition of the road is bad – it could be slippery because of various reasons.

4. Identify consequences - What could be consequences of this loss of control?

Once control over the vehicle is lost, numerous consequences might happen. We could crash into another vehicle or roadside object, injuring the driver. We could crash into water, leaving the driver trapped inside.

After these four steps, our bowtie diagram is as follows:


1. Driving a car
3. Driver loss of attention (due to phone, fatigue, etc.)
3. Blowout (tire)
3. Unexpected manoeuvre from nearby car
3. Slippery road conditions
2. Losing control over the car
4. Crash into other car or motionless object resulting in injury
4. Crash into deep water resulting in confined space

5. Identify preventive barriers - What should we do to prevent the top event?

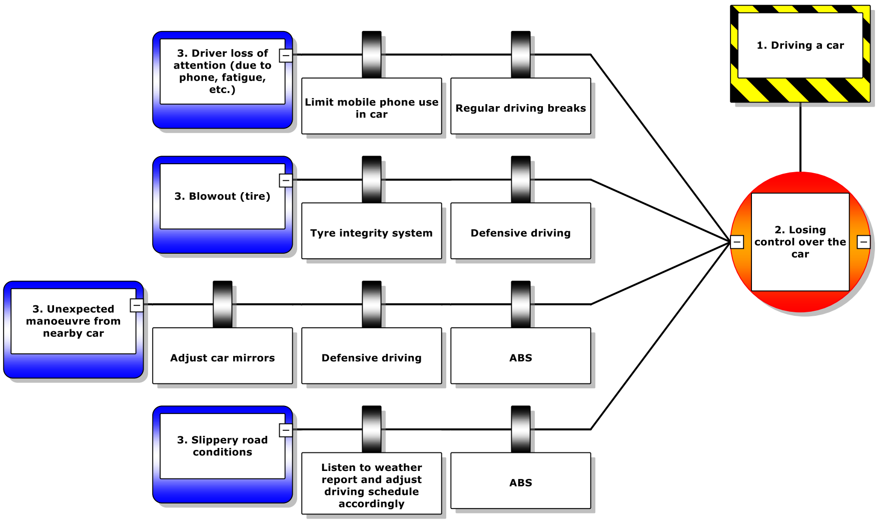
To prevent driver loss of attention, we limit the use of mobile phones in cars. We also ensure regular driving breaks are taken.

Tire blowouts do occur, but less if the tires are in good condition and have the correct tire pressure. So we ensure they are in good order by means of our tire integrity system – regular checks and replacement if worn. Defensive driving techniques also help in prevention – ensure no curbs are driven over, and areas with debris which could cause tire damage are avoided.

To prevent an unexpected manoeuvre by another car causing us to lose control over the vehicle, we ensure we can see the other vehicles on the road as good as possible by adjusting the car mirrors correctly. Again defensive driving techniques are valuable too – ensure appropriate speed and distance from other vehicles, expect the unexpected and make sure our drivers are trained in avoidance manoeuvres. We also ensure our vehicles are fitted with anti-lock brakes so the vehicle will remains controllable during hard braking.

Slippery roads can be a big threat – things such as snow and ice can unexpectedly turn a normal road into a dangerous driving environment. To mitigate, we do proper pre-journey planning where we examine the weather report and adjust our schedule as needed. If we get into slippery road conditions unexpectedly, we have anti-lock braking to assist.

The left side of our diagram is now as follows:



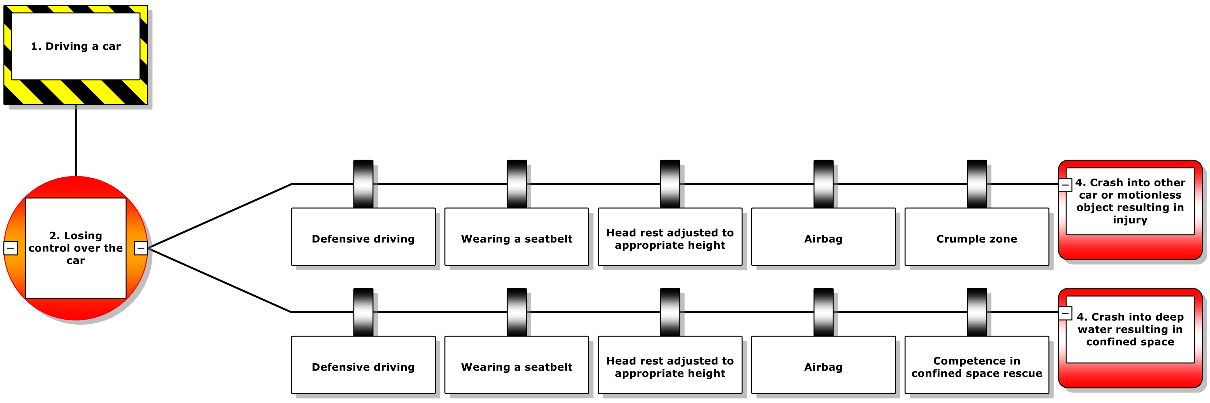
1. Driving a car
2. Losing control over the car
3. Driver loss of attention (due to phone, fatigue, etc.)
Limit mobile phone use in car
Regular driving breaks
3. Blowout (tire)
Tyre integrity system
Defensive driving
3. Unexpected manoeuvre from nearby car
Adjust car mirrors
Defensive driving
ABS
3. Slippery road conditions
Listen to weather report and adjust driving schedule accordingly
ABS

6. Identify recovery barriers - What should we do to avoid/mitigate the consequences and regain control?

Once we have lost control over the vehicle, there are a number of things which might happen – we either regain control over the vehicle, or we are well on our way towards the consequences.

To regain control, we again have our defensive driving techniques – our drivers are trained in how to respond in order to regain control over the vehicle. If this fails, we could crash. To mitigate the effects, we wear seatbelts and ensure the headrest is set to the correct height. We also have airbags, and the car body is designed with crumple zones to dissipate the energy to lessen the impact on the driver.

Crumple zones are not that useful when crashing into deep water, and we will have an additional problem – the car will sink and the driver will have to escape. To improve chances of success, our drivers are trained in confined space rescue.



1. Driving a car
2. Losing control over the car
Defensive driving
Wearing a seatbelt
Head rest adjusted to appropriate height
Airbag
Crumple zone
4. Crash into other car or motionless object resulting in injury
Defensive driving
Wearing a seatbelt
Head rest adjusted to appropriate height
Airbag
Competence in confined space rescue
4. Crash into deep water resulting in confined space

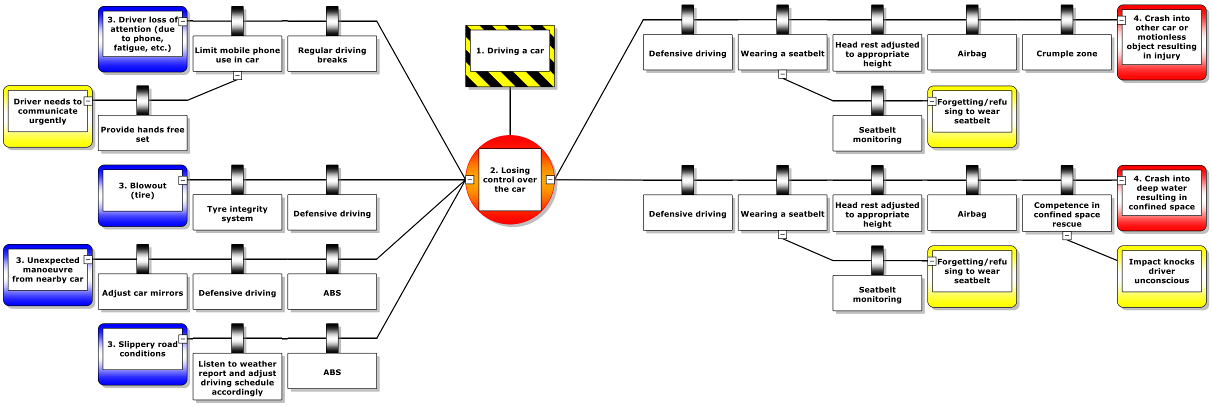
7. Identify escalation factors- what factors or conditions could defeat the effectiveness of the barriers?

Our barriers might fail – how could that happen? Perhaps drivers will use their mobile phone anyways, even though the company does not allow this. Also, people might forget or refuse to wear their seatbelts. Perhaps escaping from the vehicle under water is impossible because the driver has been knocked unconscious.

8. Identify escalation factor barriers - what should we do to control these escalation factors?

These escalation factors we again try to control. We outfit our cars with hands-free phone sets. We monitor to ensure drivers are wearing the seatbelts. We cannot control for the driver being unconscious.

Now with the escalation factors in place, our complete diagram is as follows:


3. Driver loss of attention (due to phone, fatigue, etc.)
Limit mobile phone use in car
Regular driving breaks
1. Driving a car
Defensive driving
Wearing a seatbelt
Head rest adjusted to appropriate height
Airbag
Crumple zone
4. Crash into other car or motionless object resulting in injury
Driver needs to communicate urgently
Provide hands free set
Seatbelt monitoring
Forgetting/refusing to wear seatbelt
2. Losing control over the car
3. Blowout (tire)
Tyre integrity system
Defensive driving
Defensive driving
Wearing a seatbelt
Head rest adjusted to appropriate height
Airbag
Competence in confined space rescue
4. Crash into deep water resulting in confined space
3. Unexpected manoeuvre from nearby car
Adjust car mirrors
Defensive driving
ABS
Seatbelt monitoring
Forgetting/refusing to wear seatbelt
Impact knocks driver unconscious
3. Slippery road conditions
Listen to weather report and adjust driving schedule accordingly
ABS

Now the diagram can be completed with more information over each barrier:

- Determining the barrier type.
- Which parts of the management system support the barrier, such as procedures, policies, standards, etc?
- Who is responsible for the correct functioning of each barrier?
- Assessing barrier effectiveness.

But those are beyond the scope of this sample.