The modern, fast and easy to use risk analysis tool

The Bowtie Methodology

BowTie Pro™
Enterprise Business Centre
Admiral Court
Poynernook Road
Aberdeen, AB11 5QX, UK

Tel: +44 (0) 1224 51 50 94

enquiries@BowTiePro.com
www.BowTiePro.com

Introduction

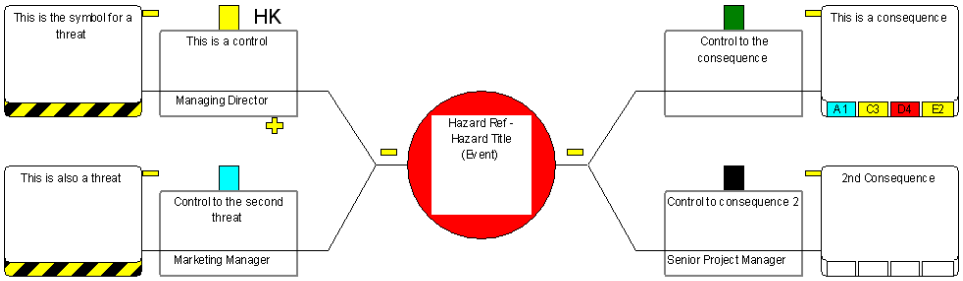
This bowtie method of analysis is a qualitative analysis incorporating management system techniques.

The bowtie has become popular as a structured method to assess risk where a quantitive approach is not possible or desirable. The success of the diagram is that it is simple and easy for the non- specialist to understand. The idea is a simple one of combining the cause (fault tree) and the consequence (event tree). When the fault tree is drawn on the left hand side and the event tree is drawn on the right hand side with the hazard drawn as a "knot" in the middle the diagram looks a bit like a bowtie as shown

This method of analysis uses the risk matrix to categorise the various scenarios, and then carries out more detailed analysis (in the form of fault and event trees) on those with the highest risks. The essence is to establish how many safety barriers there are available to prevent, control or mitigate the identified scenarios, and the quality of those barriers.

When managing major hazards there are four key objectives of using bowties

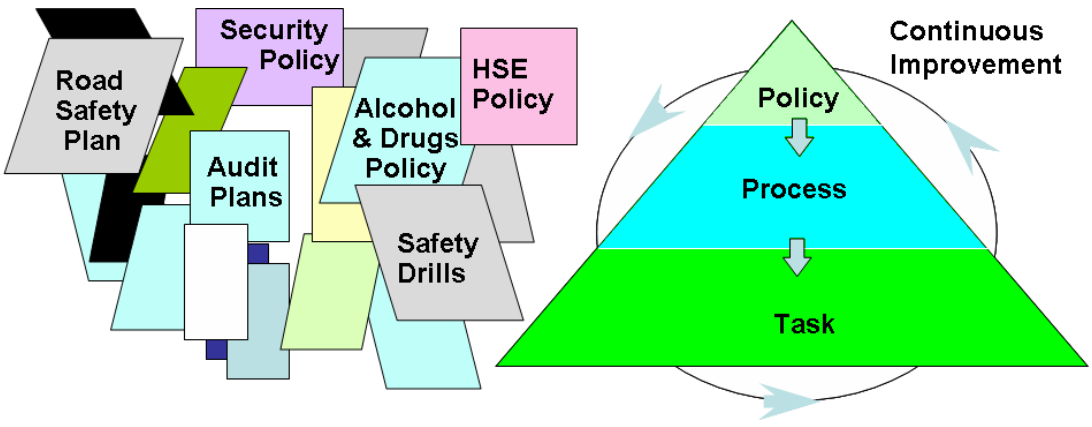
1. To give an overview of the framework relating to managing major accident hazards
2. To illustrate the interdependencies between the various stages in the framework
3. To show how the process needs to be applied to any analysis
4. To ensure we all have a common understanding of what we're doing, why and how we're doing it



Fault Tree **Event Tree**

Management Systems

A Management System can be defined as a structured set of controls for managing the business; to ensure and to demonstrate that business objectives are met. It brings a structure to the policies of the business.



No Structure **Structure**

The management system is a systematic and 'fit for purpose' way of managing risks through personnel, resources and procedures. It is not documentation alone.

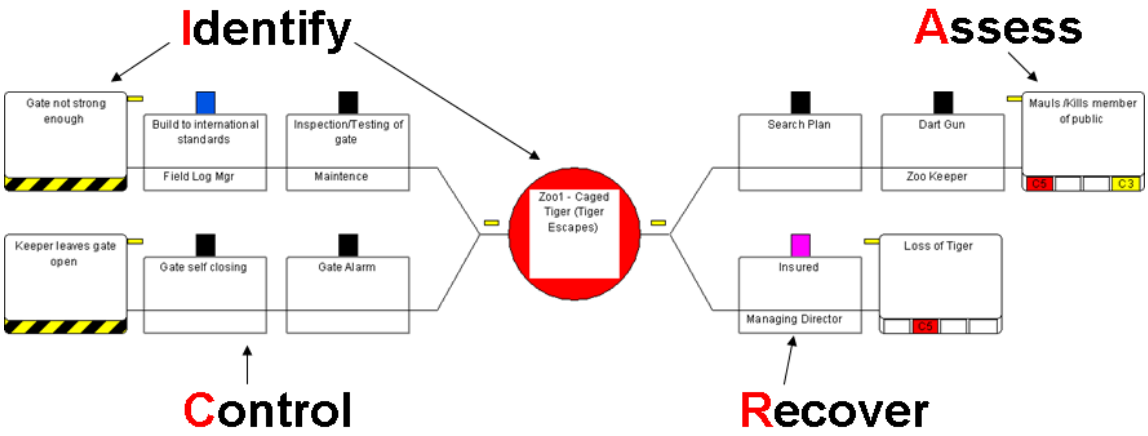
A successful management system requires the full participation & commitment of everyone involved in facility or operation and a safety culture developed over years not months.

Risk Management Process

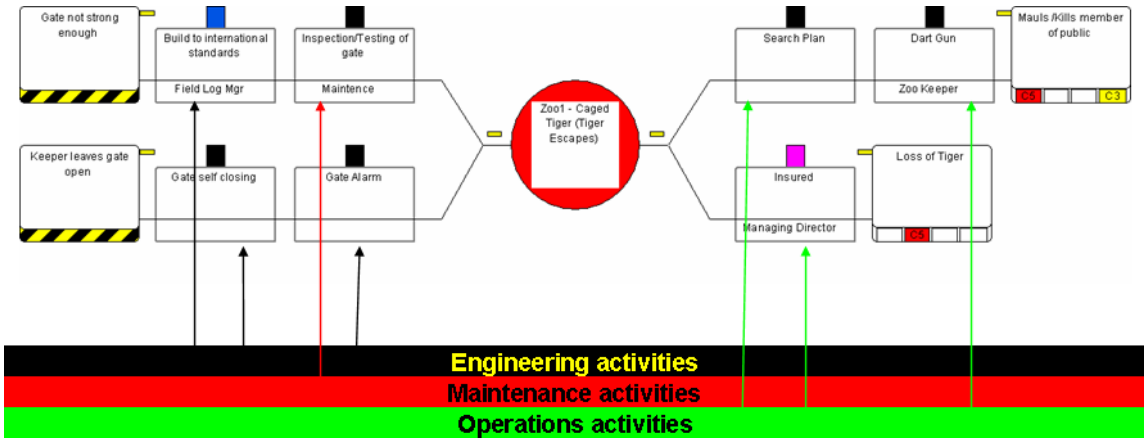
The key to any management system is the risk management process. This process can be simplified to

Identify	Are people, environment or assets exposed to potential harm?
Assess	What are the causes and consequences? How likely is loss of control? What is the risk and is it ALARP?
Control	Can the causes be eliminated? What controls are needed? How effective are the controls?
Recover	Can the potential consequences or effects be mitigated? What recovery measures are needed? Are recovery capabilities suitable and sufficient?

This appears in the bowtie diagram



Where does this fit in the management process



BowTie Pro's sophisticated yet easy to use approach makes the identification of the posts and further analysis very possible

Which risks have to be managed?

Any risk that has the "potential to cause harm" need to be managed. This includes ill health, injury, and damage to property, products or the environment, production losses or increased liabilities.
Examples of HSE risks include:

- Health, Safety and Environmental incidents, e.g.
  - acute intoxication,
  - large fires and explosions,
  - major spills on land or water
- Long term exposure of staff
  - workplace exposure (e.g. to chemicals, noise, heat)
  - infections (e.g. food, water, parasites)
  - ergonomic conditions
  - psychological conditions (e.g. stress)
- Long term exposure of the environment
  - discharges to air, water and soil (waste)
  - use of resources (ground water, sand, wood)
  - use of space
  - socio-economic impact

Risk is defined as the Combination of PROBABILITY x CONSEQUENCE. An excellent way of estimating the risk is to use a risk matrix

SEVERITY	CONSEQUENCES				LIKELIHOOD				
	People	Asset	Environment	Reputation	1	2	3	4	5
					Very Unlikely	Unlikely	Possible	Likely	Very Likely
1	No/ Slight Injury	No/ Slight damage	No/ Slight effect	No/ Slight Impact	Low	Low	Low	Low	Low
2	Minor Injury	Minor damage	Minor effect	Limited Impact	Low	Low	Low	Medium	Medium
3	Major Injury	Local damage	Local effect	Major Impact	Low	Low	Medium	Medium	High
4	Fatality	Major damage	Major effect	Nat. Impact	Low	Medium	Medium	High	High
5	Multiple fatalities	Extensive damage	Massive effect	Internat. Impact	Medium	Medium	High	High	High

Risk matrixes come in a wide variety of both sizes and types.

- The matrix above is known as a 6 x 5 and is one of the most commonly used, though matrices may be encountered ranging from 2 x 2 to 10 x 10.
- The colours in the matrix can be altered but most are in line with the "traffic light" identification (as shown) but options such as the "black swan" options can also be implemented
- The example matrix shown is a 'reactive' matrix which uses historical evidence to provide guidance on the frequency term. The other most frequently encountered type is a predictive matrix, where the frequency terms could be e.g. '1 in 10,000 chance of occurring' to 'will occur ten times per year'.

The basis of the risk matrix is always, however, the same - matching the frequency and consequence terms. As such it is important that the scoring mechanism used is decided in advance and applied consistently.

Where does all this information come from?

Although you may not have the information organised, it is very rare that you will not have any information to create your bowties. The information can come from a range of sources.

Possible sources of information are shown below:

Identify	Assess	Control	Recover
Hazards • HAZID • Checklists • Incidents • Experience • Job Hazard Analysis **Threats** • HAZOP • SAFOP • FEMA • Tripod-D E L T A • Process Hazard Review **Consequences** • FirePran • Explosion Protection Review • Process Hazard Review	• Codes and practices • Job Hazard Analysis • Physical effects modelling • Environmental Dispersion Modelling • Oil Spill Trajectory Modelling • Qualitative Risk Assessment • Quantitative Risk Assessment • Human Exposure to Soil Pollutants (HESP)	• Codes and practices • Procedures • Human Factors Engineering • Waste management	• Codes and practices • Tripod-B E T A • Drills and Exercises

It should be emphasised that when moving forward with the bowtie methodology use what you have got, DO NOT start again from scratch

When managing major risks the bowtie methodology gives real advantages as it gives a single integrated overview of issues and solutions providing transparency, connectivity (traceability) and Interactions between cause, effect and control

The Bowtie process

The process involves the systematic identification of hazards and effects, assessment of the associated risks and the specification of the control and recovery measures which must be in place and maintained in place. The bowtie process is iterative and is often carried out by a team.

The steps are:

- **Step 1** - *Identify* the bowtie hazard
  - Are people, environment, assets, continued operation or company reputation exposed to potential harm?
- **Step 2** - *Assess* the Threats
  - What are the causes?
- **Step 3** - *Assess* the Consequences
  - How likely is loss of control?
  - What is the risk and is it ALARP?
- **Step4** - *Control*
  - Can the causes be eliminated?
  - What controls are needed?
  - How effective are the controls?
- **Step 5** - *Recover*
  - Can the potential consequences or threats be mitigated?
  - What recovery measures are needed?
  - Are recovery capabilities suitable and sufficient?
- **Step6.** *Identify* threats to the controls
  - Are the controls or recovery controls at risk?
- **Step7.** *Identify* the controls for the threats to the controls
  - How do we prevent the controls from failing?

Step1. *Identify* the bowtie hazard

A bowtie hazard consists of two items, the hazard and the event that will occur.

Hazard

The hazard has the potential to cause harm, including ill health and injury, damage to property, products or the environment, production losses or increased liabilities.

Examples of hazards include:

- Hydrocarbons
- Elevated Objects
- Toxic Substances
- Electrical Energy
- Noise
- Working at Heights
- Hazardous Equipment
- Temperature Extremes
- Radiation
- light, vibrations

Event

The event is the undesired event at the end of the fault tree and at the beginning of an event tree. The “release” of the hazard.

Example Events include:

- Loss of Containment
- Structural Failure
- Dropped Objects
- Loss of Control
- Electrical Shock
- Falls to Same Level
- Falls to Lower Level
- Oxygen Deficiency
- Loss of Separation
- Explosion

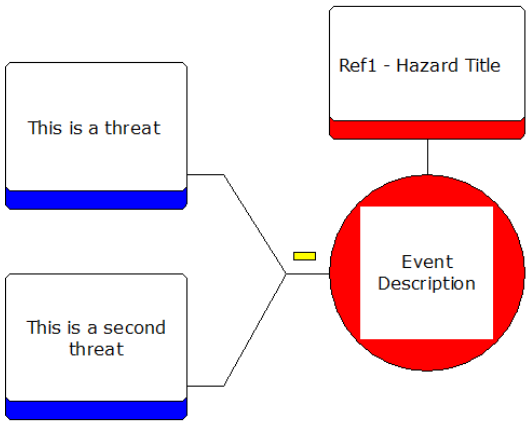
Step2. *Assess* the Threats

The threats are at the far left hand side of the diagram. A Threat is something that will potentially cause the releases of the identified hazard.

Example Threats may include:

- Thermal
  - high temperature
- Chemical
  - corrosion

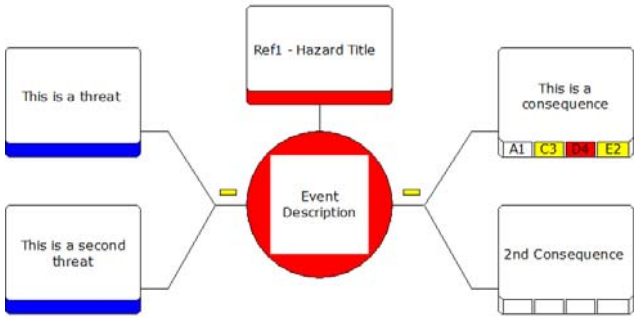
- Biological
  - bacteria
  - marine growth
- Radiation
  - ultraviolet
- Kinetic
  - fatigue
- Electrical
  - high voltage
- Environmental Condition
  - poor visibility
  - flooding
  - severe storm
  - earthquake
- Uncertainty
  - design unknowns
- Human Factor
  - incompetence



Step3. *Assess* the Consequences

The consequences are at the far right hand side of the diagram. A Consequence is an event or chain of events that result from the release of a hazard

The consequence can have a range of results which are determined by a customisable risk matrix within BowTie Pro™. The BowTie Pro™ diagram displays the square reference and the colour below the consequence text if a risk assessment has been made.

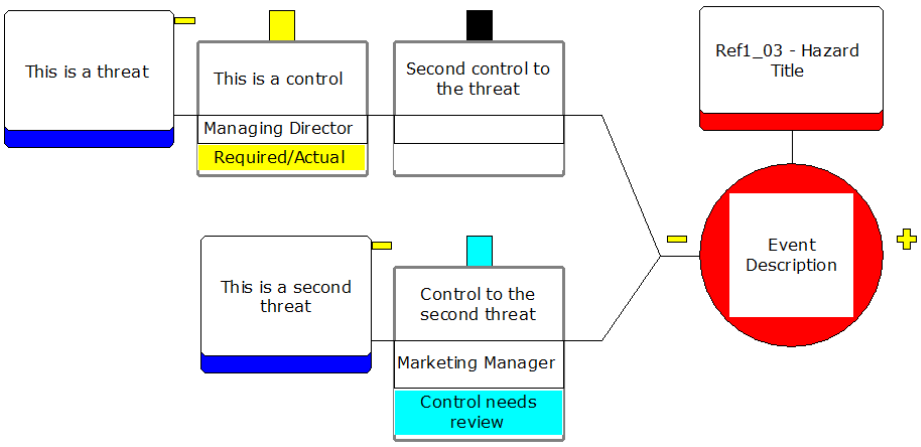


Example consequences include:

- Fire and explosion
- Environmental Pollution
- People injured
- Fatalities
- Financial penalties

Step4. *Control*

The control is the protective measure put in place to prevent threats from releasing a hazard. On the bowtie diagram they sit between the threat and the hazard.



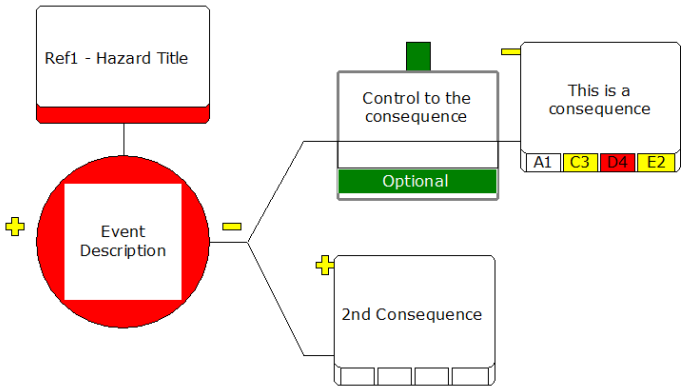
All controls be them preventing threats, consequences or threats to the control each hazard and to reduce the risk to a level As Low As Reasonably Practicable (ALARP).

Examples of Controls could be

- Guards or Shields
  - Coatings
  - Inhibitors
  - shutdowns
- Separation
  - time and/or space
- Reduction in Inventory
- Control of Energy Release
  - safety valves
  - lower speeds
  - different fuel source
  - Administration
  - warnings, training, drills
- Procedural
- Preventative measures
  - alternative resources
  - re-cycling
  - process integrated solutions
  - improved ergonomic conditions
  - health surveillance
- Repressive measures
  - end-of-pipe measures
  - ventilation
  - dust filtration

Step5. *Recover*

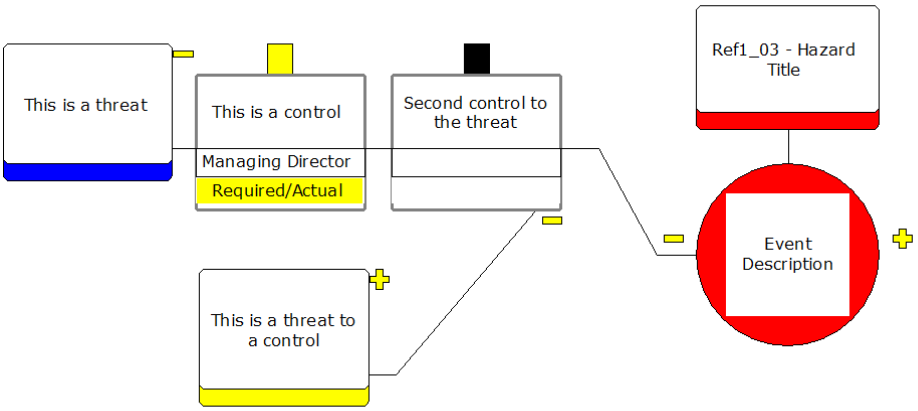
The recovery controls sit between the Hazard and the Consequence. Recovery Controls are technical, operational, and organisational measures that limit the chain of consequences arising from an Event.



Examples of recovery controls are:

- Systems to Detect and Abate Incidents
  - gas, fire & smoke alarms, ESD, deluge
- Systems Intended to Protect the Safeguards
  - fire & blast walls, protective coatings, drain systems
- Operational Systems Intended for Emergency Management
  - contingency plans, training, drills
- Curative measures
  - clean up, restoration, landscaping, first aid, hospital treatment
- Compensative measures
  - re-stock fish, financial or nature compensation

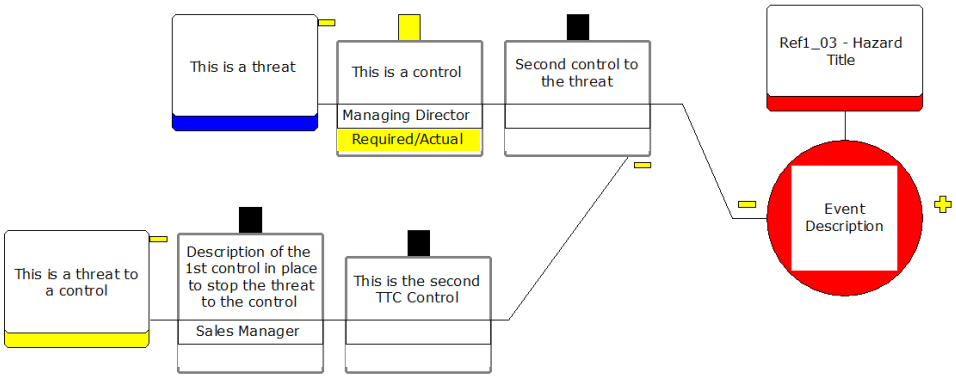
Step6. *Identify* threats to the controls
Threats to the Control are conditions that lead to increased risk by defeating or overriding a control. On the diagram these are displayed under and off to the side of the control.



Example Threats to the Control are:
- Abnormal Operating Conditions
  - maintenance mode, testing of equipment
- Operating Outside Design Envelope
  - corrosion
  - flow velocities
- Environmental Variations
  - extreme weather & tidal conditions
- Human Error
  - Lapses, rule violations (ask yourself: “why do lapses or rule violations take place?”)

Step7. *Identify* the controls for the threats to the controls

Controls for the threat to the control should be put in place to ensure that the threat to the control does not cause the control to fail.

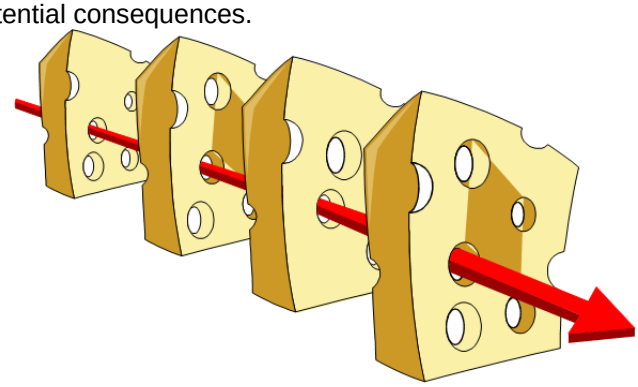


Note: If there are lots of threats to the control ask yourself is the original control safe and sound? The key purpose is to manage the threats and consequences through the controls not to try to fix bad controls

Combined Control Effectiveness

The threats and consequences are managed by the combination of the controls. Each control is a barrier where the combination of the controls should eliminate the hazard or reduce its frequency of occurrence, or mitigate its potential consequences.

It is only when ALL the controls fail that the hazard or consequence will occur depending on which side of the bowtie you are working. This is described by James Reason as the "Swiss cheese model".



The controls can include physical or operational systems and procedures that may be in place.

In many cases it is better to use a more pragmatic approach with rigorous peer review.

How do we know if we have enough controls?

There is a rule that the system should be ALARP. "ALARP" is short for "as low as reasonably practicable". At the core is the concept of "reasonably practicable"; this involves weighing a risk against the trouble, time and money needed to control it. Thus, ALARP describes the level to which we expect to see workplace risks controlled.

Reasonably practicable is defined as:

> "'Reasonably practicable' is a narrower term than 'physically possible' … a computation must be made by the owner in which the quantum of risk is placed on one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time or trouble) is placed in the other, and that, if it be shown that there is a gross disproportion between them – the risk being insignificant in relation to the sacrifice – the defendants discharge the onus on them."

The Objective of ALARP is

- To reduce a risk to a level which is as low as reasonably practicable involves balancing reduction in risk against the time, trouble, difficulty and cost of achieving it.

- This level represents the point, objectively assessed, at which the time, trouble, difficulty and cost of further reduction measures become unreasonably disproportionate to the additional risk reduction obtained.

Determining that risk has been reduced ALARP

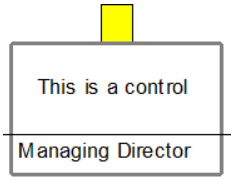
This process can involve varying degrees of rigour which will depend on the nature of the hazard, the extent of the risk and the control measures to be adopted. The more systematic the approach, the more rigorous and more transparent it is to the regulator and other interested parties. However, duty-holders (and the regulator) should not be overburdened if such rigour is not warranted. The greater the initial level of risk under consideration, the greater the degree of rigour HSE requires of the arguments purporting to show that those risks have been reduced ALARP.

Management of Controls

The bowtie can be developed without BowTie Pro™ however without the software the analysis would stop here and management of the controls would need to be done through other means.

Categorise Controls by Type

The control type changes the colour of the box above the control. As many types can be defined as required and each can have its own colour user defined. When a diagram is printed out there is an option to add a legend to the diagram with its description next to the colour.



There are many options on how to use control types but one favoured by a major oil company is to use it for "Physical types" e.g. hardware, procedural etc remembering that for each threat or consequence different kinds of controls should be in place where ever possible.

Categorise Controls by Effect

The control effect allows the classification of the controls by both a colour and a short code to be placed at the top left hand side of the control. Again these are user defined and customised.

Categorise Controls by Code

The control code allows a classification by a short descriptor to be placed at the top right hand side of the control. Again these are user defined and customised and can be have many uses.

Cost

As discussed the control can have the cost taken into account as part of the ALARP comparison

Safety Equipment

The equipment that is associated with the control

Tasks

In order to make sure your controls are kept in place, BowTie Pro™ let's you add the tasks to the controls. This is done through BowTie Pro's easy to use innovative technology allowing tasks to be typed in or selected from a list of previous tasks as required.

Responsible Parties

Along with a control task a responsibility for maintaining the task and the control is vital for the control to be effectively managed. The concept of a responsible party is not bound to specific individuals but to the role/ job function within the organisation.

BowTie Pro™ allows you to define the roles and then select the appropriate item from a list. This means there is consistency and clarity between the organisations functions and the BowTie Pro™ file.

Documents

Any type of document can be entered against a control e.g. procedures, logs that need to be maintained. Documents can have a URL which can be opened directly from BowTie Pro™.

Task Verification

The verification is a description of how a task will be ensured. This is important when auditing that the threat or consequence to ensure the risk is managed and diagnoses of the critical tasks.

By entering this information, it allows BowTie Pro™ to be used in providing vital information in the analysis and audit of the risks

Target Dates

Tasks can have optional target start and finish dates which can be identified as complete.

How BowTie Pro™ analyses the bowtie data

BowTie Pro™ has numerous analysis tools to ensure that data is complete and controls are ALARP. Some of the modules include:

- **Risk Registers**
- **Document Analysis**
- **Date Completion Activities.**
- **Quality Assurance**
- **Deficiency tracking**

BowTie Pro™ goes beyond the bowtie

The bowtie is a great method and leads onto many other techniques. These include:

- **Layers of Protection (LOPA)** – where a quantitative analysis is performed on each branch.
- **Permitted Operations** – This is a record of the items that can and cannot be done simultaneously. By eliminating conflicting operations environments can be made safer.
- **People and Competence**
- **Incidents** – This is a rapidly developing module in BowTie Pro™ and the data feeds back into the lessons learned for a bowtie.

Review Checklist

For each hazard have you taken account of…

Threats

- Are there any further threats that should be considered?

Consequences

- Are there any further consequences that should be considered?
- Have all relevant risks been assessed for each of the categories against all of the consequences

Control chains

- Is each of the controls from a threat or consequence “independent”?
- Are any of the controls in the chain reworded versions of another control?
- Are all the controls in the chain full and clear?
- Are there any further controls that should be added into the chain?

Controls

- Has a Task been allocated against each control?
- Has a Post been allocated to each control?
- Is there any threats that will cause the control to fail that should be added to the “Threat to the Control”
    - If so should another better control be put in place?
- Is each control full and clear?