Chicken or egg?: Safety Critical Task Analysis and bowties

Jodie Lewis, Andrew Bradbeer, Ian Hamilton, Tamara Maynard, Human Factors, Environmental Resources Management.

Human error is a significant contributor to incidents and accidents in high hazard industries. The barriers, or control measures, that are put in place to mitigate the risks associated with Major Accident Hazards (MAH) are reliant on human performance. Humans have a role in assuring that the barriers are effective; whether this is through the application and operation of the barriers, or through maintenance of the barriers.

Safety Critical Task Analysis (SCTA) and the bowtie methodology can be used in combination to assess the human error potential around a MAH event and identify the control measures that can be implemented to mitigate risk.

This paper describes how the findings from SCTA and bowties can feed into one another to support the control of human reliability in barrier performance. It discusses how the results from both these studies can provide an in-depth understanding of the human role in assuring barrier effectiveness and, from this, how leading indicators can be developed to monitor human interaction with barriers.

Keywords: Safety Critical Task Analysis, Bowties, Human Error, Human Factors

Introduction

It is widely recognised that human error is a significant contributor to incidents and accidents in high hazard industries. Some would argue this contribution equates to up to 90% of incidents (e.g. Dhillon, 2007, Khandpur, 2000, Shappell & Weigmann, 1996) and indeed when the role of humans in the design, operation and maintenance of equipment, systems and processes is considered it could be further argued that *all* incidents have a human or organisational factor as a direct cause or contribution. However, as Trevor Kletz pointed out, "People say most accidents are due to human error, which is true in a sense, but not very helpful; a bit like saying that falls are due to gravity" (CSB, 2013). What is helpful, however, is understanding how human performance failings can lead to accidents and how these can be managed to reduce risk.

The UK's Health and Safety Executive (HSE) has highlighted the need for companies to manage human error "as robustly as technical and engineering measures". The Control of Major Accident Hazards (COMAH) Regulations (2015) also stipulate that businesses must "take all necessary measures to prevent major accidents" and "limit the consequences to people and the environment of any major accidents which do occur" (COMAH, 2015). Regulatory bodies such as the HSE check that businesses are managing *all* hazards on their facilities, for example: primary containment, moving machinery, falling objects and electricity, to name but a few.

The human role in barrier management

Humans have a role in assuring that the barriers put in place to mitigate the risks associated with Major Accident Hazards (MAHs) are effective. These control measures, or barriers, typically fit into three categories: physical, procedural or behavioural. Examples of physical barriers might include correctly specified process pipework and equipment, control system interlocks, fire and gas detectors etc. Examples of procedural barriers include Permit to Work systems and operating and maintenance procedures. Behavioural barriers include a good safety culture with strong safety leadership, shared values and safety as a primary motive for behaviour.

Peoples' responsibilities in relation to these barriers are to apply, operate, test, inspect and maintain the barriers to ensure they are working as intended, to manage the risks around MAHs. Recognising this, industry regulators are focusing their attention on human reliability and Operating Companies are becoming increasingly proactive in demonstrating how they are controlling the risk that human error presents to safe operation.

It is not only important that Operating Companies are able to demonstrate this during facilities' operational phases, but also during the earlier design and construction phases. The most effective way to ensure risks are controlled in the operational phase is to identify and assess human error potential early on in the design, so that plans can be made to mitigate the error potential and designs can be adapted to suit (OGP, 2011). The best engineering solution may not always be the best human factors solution, so it is important to assess this as early in the design process as possible.

Demonstrating control of human error risk: The methodologies

There are a number of tools and methods in a Human Factors practitioner's toolkit that can be used to assess human reliability and the potential for human error within a given task. Using human factors methods to identify the sources of human error enhances technical risk studies by providing detail on the human element of process safety management.

The two methods selected as the focus of this paper are Safety Critical Task Analysis (SCTA) and bowties. Bowties can be used to identify barriers and SCTA to assess the human interaction with these barriers. In combination, these methods can be used to conduct a thorough risk assessment and improve barrier effectiveness.

Safety Critical Task Analysis

SCTA is a method used to identify the potential for human error within a given task and assess the measures in place to mitigate the error (HSE, 1999). Several regulatory bodies and organisations have published guidance on SCTA, including the HSE 7-step process (HSE, 2016) and the Energy Institutes guidance on human factors safety critical task analysis (Energy Institute, 2011).

Whilst the guidance varies slightly among these, the SCTA method broadly consists of:

- Identifying hazards.
- Identifying safety critical tasks. The identification of Safety Critical Tasks (SCTs) is a core element of the UK HSE's Safety Case regulations (APOSC Principle 8) and a core topic within the COMAH Human Factors toolkit. By identifying SCTs a business is identifying the tasks that are key to ensuring the controls they have in place are operated and maintained appropriately to manage the hazards on their site.
- Analysing the tasks to identify each step involved in carrying out the task.
- Carrying out human error assessment of the task.
- Identifying factors that may influence the likelihood of an error. These are Performance Influencing Factors (PIFs); examples include job factors such as inadequate procedures, person factors such as fatigue and organisational factors such as levels of supervision (HSE, 2005)
- Identifying the consequences of these errors and the means of error recovery.
- Identifying the measures in place to prevent or mitigate the consequences of the error. Measures put in place should consider the hierarchy of control. Where possible the error should be eliminated through 'designing-out' the need for human interaction. If this is not possible other measures such as engineered controls that reduce the need for human interaction may be implemented. The very last measure of control is to rely on measures that simply to protect workers after an error and subsequent incident occurs (i.e. personal protective equipment), compared to those aimed at *preventing* the incident in the first place.

Bowties

A bowtie diagram is a way of describing the relationship between a major hazardous event (referred to as the 'top event'), its potential causes (threats) and potential consequences. A bowtie diagram is typically developed in a workshop setting with various subject matter experts and those involved in carrying out tasks related to the control of the MAH event.

The aim of the Bowtie workshop is to identify and assess the safeguards (referred to as 'controls' or 'barriers') that are in place to:

- Prevent the threats from leading to the top event,
- Mitigate the extent of the top event, or,
- Prevent or mitigate the consequences of the top event.

During the Bowtie workshop the strength and reliability of the barriers are also assessed to identify how effective they are as safeguards and how reliably they are operated and maintained. The strength of the barrier refers to how robust the barrier is in preventing or mitigating the top event, if it is always applied. The reliability of the barrier refers to how consistently the barrier is applied and how well the barrier is maintained.

Once these barriers have been assessed, the high strength critical barriers are then further analysed in a barrier management plan to identify weaknesses in the barriers. An example of this process is described in more detail in the following sections.

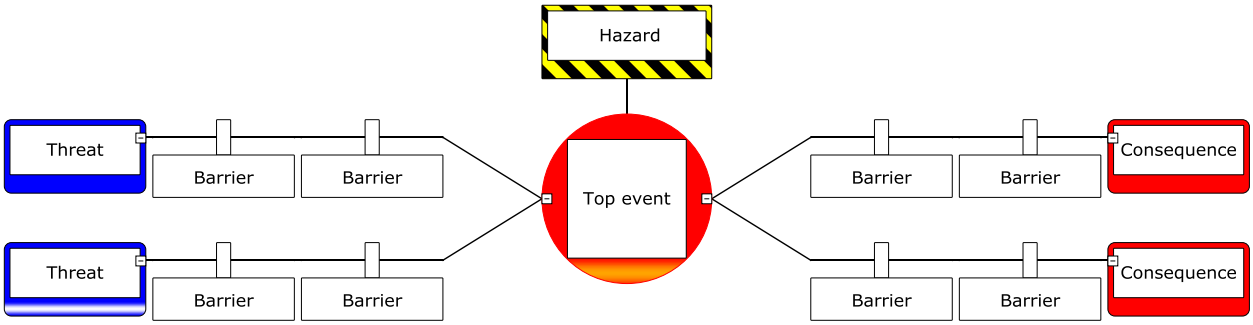


***Figure 1**. Screenshot taken from BowTieXP software, CGE Risk Management Solutions*

Combining methodologies for effective barrier management

The relationship between SCTA and the Bowtie methodology is bi-directional. Each can be used independently as part of risk management activities and human factors is integral to both methods. They can also be used in combination and the information gleaned from one can be used to inform the other. Hence the chicken and egg analogy in the title of this paper.

An example of this is illustrated in Figure 2 below. The example concerns the task of filling a storage tank with gasoline from a delivery tanker. In this scenario a SCTA is carried out for the task. In order to start filling the storage tank, the tanker delivering the gasoline needs to be connected to the storage tank. This step is identified during the SCTA and then assessed for human error potential. It is noted that connecting and lining up the tanker to the correct storage tank is a manual operation and a possible error associated with this is that the tanker is lined-up incorrectly, i.e. valves are opened in an incorrect sequence, directing flow to the wrong storage tank. This could result in the gasoline being sent to a storage tank that contains a substance other than gasoline, resulting in product contamination, or the gasoline being sent to a storage tank that may already be full, resulting in overfilling of the storage tank.

The information from the SCTA can be translated onto a bowtie; as shown in Figure 2 below. If the bowtie diagram considers the *hazard* "Gasoline" and the *top event* "Tank overfill", the error identified through the SCTA (incorrect line-up during import) can be included on the bowtie diagram as a *threat.*

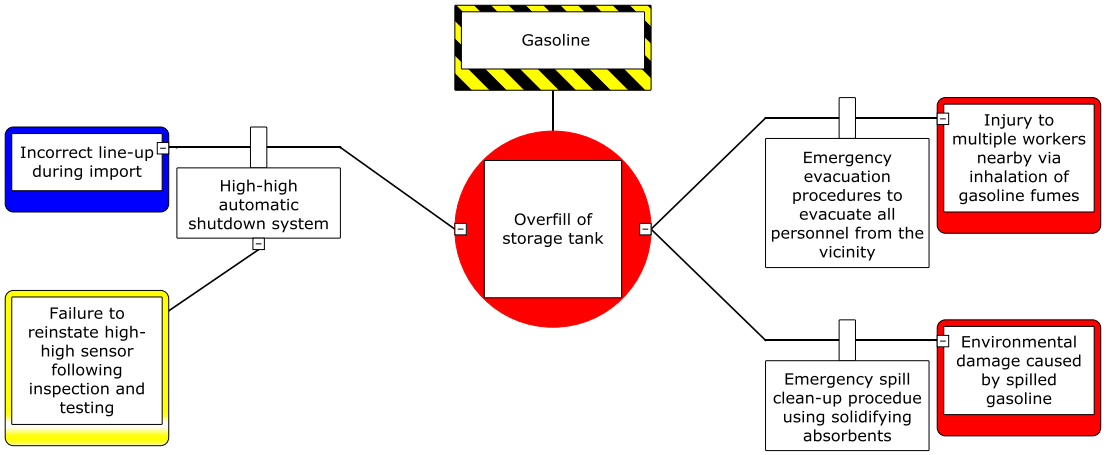


***Figure 2**. Bowtie diagram, example scenario*

Now considering the same bowtie diagram, one of the barriers identified to prevent this threat from leading to the top event is the high-high shutdown system. The system comprises a sensor that detects a high-high level of material in the tank and a logic controller that initiates a signal to shut down the tank-side valves, closing off the transfer of gasoline into the tank . This is a high strength control because correct operation of this barrier will prevent the tank from overfilling. In this example, the barrier is also the only barrier in place to prevent incorrect line-up from leading to tank overfill.

It is generally the case that strong barriers are considered 'critical' because their function is vital in controlling the risk presented by the threat. Single barriers along a threat line may also be considered critical because they act as the only barrier preventing a threat from resulting in a MAH event. These two aspects therefore define the barrier in this example as 'critical'. Tasks relating to the operation and maintenance of this barrier are therefore considered Safety Critical Tasks (SCTs) because these tasks ensure that the barrier remains effective i.e. it does its job of mitigating the risk.

One of the benefits of using a bowtie diagram is that it provides a clear visual illustration of the barriers in place around a specific hazard. SCTs are therefore relatively simple to identify and can be assessed in greater depth using SCTA. The bowtie may also prove useful in helping a business to prioritise SCTs for deeper analysis. However, understanding and managing human reliability and its role in assuring barrier effectiveness is not a trivial activity. Sites may have numerous hazards with numerous barriers and numerous SCTs. It is therefore necessary that businesses first prioritise the most important SCTs for assessment. SCTs relating to a single critical barrier may be prioritised over SCTs that relate to a critical barrier on a threat line with many other high-strength barriers, particularly if these barriers are considered to be highly reliable.

A SCT linked to the high-high shutdown system barrier is inspection and testing of the high-high level sensor. To do this the sensor needs to be taken out of use, inspected, tested and then reinstated. By carrying out a SCTA on this task it is identified that a simple error in reinstating the sensor following testing would result in the sensor not operating correctly and this would render the entire barrier ineffective. This is a 'threat' linked to the barrier and so can be included on the bowtie as an escalation factor (also referred to as a sub-threat) on this barrier, as shown on the example bowtie diagram in Figure 2.

The SCTA methodology can identify discrete threats and escalation factors that may not have been identified during the bowtie development process. Conversely, the bowtie may identify SCTs that should be further analysed using SCTA, or highlight critical steps in a task that demand particular attention.

Barrier reliability and developing leading indicators

The reliability of the barrier can be thought of as how effectively the barrier is applied, operated and maintained.

A barrier high in reliability will be:

- well designed and resilient against failure
- used on every occasion where it is necessary to mitigate risk, and
- regularly inspected, tested and maintained

Reliability is independent of strength; even a high-strength barrier can be made ineffective (i.e. unreliable) if it is not operated and maintained to its design specifications. At the same time, a barrier can be considered high in reliability but low in strength. This means that the barrier may always be applied and maintained but will not necessarily entirely prevent a threat from leading to a top event. An example of this is the use of traffic cones to prevent unauthorised access into roadwork lanes. The cones are a physical control however, even if they are always in place, they cannot solely prevent a vehicle from crossing into the work lane.

The high-high shutdown system described in the example scenario in Figure 2 is a high strength barrier. Its reliability depends on two main aspects: operation and maintenance. Regular testing, inspection and maintenance are necessary to ensure it operates effectively, but its effectiveness also relies on the barrier being operated correctly. For example, in the

example scenario, if the high-high sensor is routinely switched off due to previous incidences of spurious activation, the sensor will not work when required, the shutdown system cannot be automatically activated and therefore the barrier is essentially inactive. This would mean that incorrect line-up to the storage tank would go undetected and eventually lead to the over-fill of the tank.

Developing leading indicators

Humans are integral to assuring the reliability of barriers and therefore it is important that businesses recognise this role and develop measures to monitor human interaction with barriers. One way of monitoring this interaction is through leading indicators of barrier management. Examples of these include test measurements, manpower levels, training records and maintenance logs (Hamilton & Turner, 2014).

Leading indicators allow a company to monitor the performance of barriers and identify the potential for an incident before it occurs. This is in contrast to lagging indicators, such as incident reports or equipment failures, which provide information about when a barrier has not performed in the way that it should, to mitigate risk.

Consider the example of the vibration hazard posed by the use of certain tools such as pneumatic hammers or hand held drills. Prolonged use of these tools can result in hand-arm vibration injuries that can cause irreversible damage. One way of monitoring this risk is to establish a leading indicator by monitoring the time spent using such equipment. This could be achieved using engineered equipment that records the time in minutes that a tool is operated (i.e. exposure time). Maximum exposure limits can be monitored and companies could even set targets for lowering the exposure over a set time frame to demonstrate to the regulators their commitment to managing risk.

A way of identifying and developing leading indicators is through development of a management plan for critical barriers which focuses on the human and organisational factors that influence the operation and reliability of the barrier (Hamilton & Turner, 2014). Critical barriers can be identified from bowtie diagrams and recorded in a barrier management plan for further analysis. Hamilton and Turner (2014) define a set of criteria for the barrier management plan, provided in Table 1 below.

Table 1. *Barrier Management Plan criteria*

Operation	
Critical barrier	Identify the specific barrier measure
Barrier objectives	What is the objective of the barrier that prevents or mitigates the major hazard and makes it critical?
Safety critical tasks	What are the tasks that people must perform to operate or maintain the barrier? What is the required performance quality of the tasks (what error mode must be controlled) What additional control measures are needed to manage the risk of error?
Control responsibility	Who (what role) will perform these tasks? Who (what role) will check their performance?
Training and competence requirements	What specialist knowledge and skills are required to perform the tasks? How will this be provided and assured?
Reliability	
Criteria to meet barrier objectives	What is the target performance of the barrier (e.g. sensitivity)? What are the availability and reliability criteria?
Assessment process	How are the sensitivity, availability and reliability to be assessed?
Critical measures	Are special measurement processes to be applied? What are the requirement measurement tolerances?
Test frequency	How often are the assessments required to be performed?
Assurance measure	What is the evidence that the assessments are completed satisfactorily?
Concerns	What weaknesses have been identified for this barrier?
Remedial actions	What improvement actions must be applied to address the concerns? Who will be responsible for their completion? What is the due date for completion?

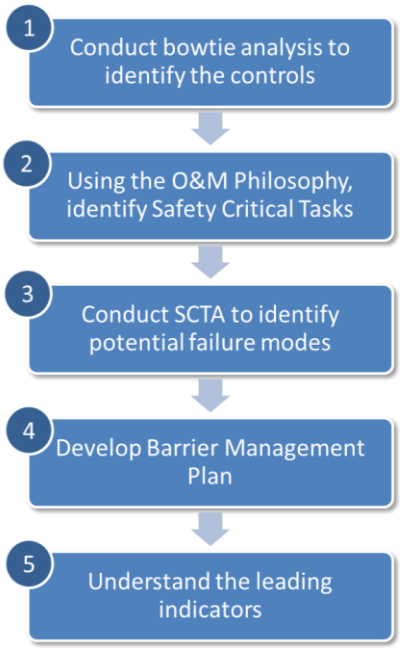
The plan's criteria assess the various human and organisational performance elements that impact on the operation and reliability of the barrier. The criteria lay out:

- the specific requirements of the barrier in relation to its intended function,
- the relevant competency and training required to operate, maintain and monitor the barrier, and
- the necessary measures to ensure the reliability of the barrier e.g. checking and monitoring.

Leading indicators can be derived directly from the criteria and targets can be set against these indicators so that a company can demonstrate it is monitoring the performance of its barriers and managing them effectively.

How the process fits together

Using the example of a manufacturing process involving the use of acid, this section demonstrates the link between SCTA, bowties and leading indicators.



The Scenario – A chemical facility has several separate manufacturing processes. One of the manufacturing processes involves the use of hydrochloric acid, whilst the other involves sodium hypochlorite. If combined this mixture results in the production of chlorine gas.

The site uses bowties and SCTA to understand the failure modes that could result in the mixing of hydrochloric acid and sodium hypochlorite, and the barriers in place to prevent this.

Step 1 – Develop bowtie diagrams

In a bowtie workshop the MAH event (top event) is identified: inadvertent mixing of hydrochloric acid and sodium hypochlorite, resulting in the production of chlorine gas.

A potential cause of this event is the erroneous transfer of acid from Tank A to Tank C which contains sodium hypochlorite, instead of the transfer of another material from Tank B to Tank C. A critical, high-strength barrier is identified that will prevent the threat from leading to the top event, namely; an in-line pH sensor connected to an auto-shutoff system that will automatically close the connection to Tank C on detection of acid.

Figure 3. *The link between SCTA, Bowties and leading indicators*

Step 2 – Identify the Safety Critical Tasks

Behind each barrier is an operations and maintenance philosophy. The operations and maintenance philosophy of the pH sensor control includes regular testing and maintenance of the pH sensor and shutdown system to ensure it functions as required. These are Safety Critical Tasks and are subsequently analysed further using SCTA.

Step 3 - SCTA

The SCTA identifies a number of failure modes of the tasks. These include failure to carry out maintenance on the pH sensor or failure to carry out accurate testing of the pH sensor and shut-down system. The information obtained from both the bowtie assessment and SCTA feeds into the development of a Barrier Management Plan.

Step 4 – Barrier Management Plan

Working through the Barrier Management Plan the site confirms the particular requirements for effective operation and maintenance of the barrier, such as monthly testing of the sensor as per manufacturer's guidelines. The test checks the calibration of the sensor to ensure it functions at the necessary pH range of the solution. Using this information, leading indicators can be developed to monitor the performance of the pH sensor control and shut-down system.

Step 5 – Leading Indicators

Table 2 gives two examples of the operation and maintenance criteria defined in the barrier management plan. For each criterion a leading indicator can be developed and monitored over time. Any deviation away from the set criteria can be easily detected and appropriate action taken to ensure the barrier remains operational and reliable.

Table 2. *Examples of leading indicators*

Operation and maintenance criteria (as defined in the barrier management plan)	Leading indicator	Warning signs detected through monitoring leading indicators
Test frequency: Monthly testing of the sensor as indicated by manufacturer's guidelines	Record of maintenance schedule and test completion	Testing/maintenance missed or delayed, especially when several are missed in a row.
Reliability criteria: Monitoring of spurious trips to ensure the system is always operational	Record of the number of spurious trips	The number of spurious trips increases above a defined 'acceptable' level. There is a risk that this will result in distrust in the system leading to the system being overridden without checking.

In summary:

- The bowtie and SCTA identify the failure modes and controls around a particular MAH event
- This feeds into development of the Barrier Management Plan to define a set of criteria for barrier assurance
- Leading indicators are developed based on the criteria defined in the Barrier Management Plan
- Leading indicators are monitored to detect any changes to the reliability of the barrier and the potential for failure.

Conclusions

Both SCTA and the bowtie method can be effective tools in identifying the potential for human error and evaluating human reliability in relation to critical controls, with the aim of improving overall barrier management. One of the advantages of both is that they can be used throughout the various stages of a facility's lifecycle (from design through to decommissioning). They can also be used in combination to provide both a broad picture of the barriers in place around a specific hazard and also a more detailed picture of the role of people in assuring barrier reliability.

The methods are discussed in this paper in the context of MAH events, however, these methods can also be applied to other areas, such as environmental hazards that may not necessarily prove hazardous to people or equipment on site. It is often the case that bowties are developed with consideration for multiple potential consequences, including injury to people, damage to equipment, damage to the environment, reputational damage and financial loss to a company. The SCTA process can also be used to assess environmentally critical tasks, although safety critical tasks and environmentally critical tasks are often two sides of the same coin.

Human reliability is a major component to the effective and safe functioning of a facility and it is vital that the role of human performance and the potential for human error is identified and managed appropriately. SCTA and bowties provide solutions to not only identifying and assessing this risk but also to understanding how humans fit into effective barrier management. They show how these activities can be monitored through use of leading indicators and careful consideration of human factors within the design of a barrier management system, and how the risks from human error can be mitigated.

References

Dhillon, B.S. 2007. Human Reliability and Error in Transportation Systems. U.S. Springer

Energy Institute. 2011. Human factors guidance on safety critical task analysis. ISBN 978 0 85293 603 0, 1st Edition.

Hamilton, W. I. and Turner, C. 2014. Building a Culture of Effective Process Safety Management. SPE-172323-MS. Society of Petroleum Engineers (SPE) Annual Caspian Technical Conference and Exhibition held in Astana, Kazakhstan, 12-14 November 2014

Health and Safety Executive (HSE). 1999. Human factors assessment of safety critical tasks. Offshore technology report, OTO 1999 092.

Health and Safety Executive (HSE). 2016. Core topic 3: Identifying human failures. http://www.hse.gov.uk/humanfactors/topics/core3.pdf Accessed 18/01/2016.

Health and Safety Executive (HSE). Human factors: managing human failures. http://www.hse.gov.uk/humanfactors/topics/humanfail.htm Accessed 18/01/2016.

International Association of Oil and Gas Producers 2011. Human factors engineering in projects. Report no. 454. OGP Publications.

Khandpur, R. 2000. Human Factors in Ship Design, Technical Report, Ship Technical Operations Committee, Panel O-38, Human Factors (HF) and Manning, http://www.sname.org/technical committees/tech_ops/panel038_reports.htm

Shappell, S. And Weigmann, D. 1996. U.S. Naval aviation mishaps 1977-1992: Differences between single and piloted aircraft. Aviation, Space, and Environmental Medicine, 67, 65-69

The Control of Major Accident Hazards Regulations (COMAH) 2015.