Engineering safety into the design

Peter Scantlebury P.Eng
Technical Safety Manager
Amec Foster Wheeler, Oil & Gas Canada

Abstract

Safety by design is Amec Foster Wheeler's systematic approach to engineering safety into the design. It is a five step approach to engineering design which results in the ability to demonstrate that hazards to people, environment, assets and reputation have been systematically and comprehensively identified and eliminated or controlled during the design phase of a facility/system or equipment.

As a result of the safety by design process, the overall risks of a design are minimised by eliminating hazards or applying the right hazards controls to minimise the right hazards. Furthermore, the design elements to control or eliminate the hazards are identified and designed early in the design process when the implementation cost is at a minimum.

Introduction

Safety by design is Amec Foster Wheeler's systematic approach to managing plant risk during engineering design. It consists of five steps as illustrated in Figure 1.

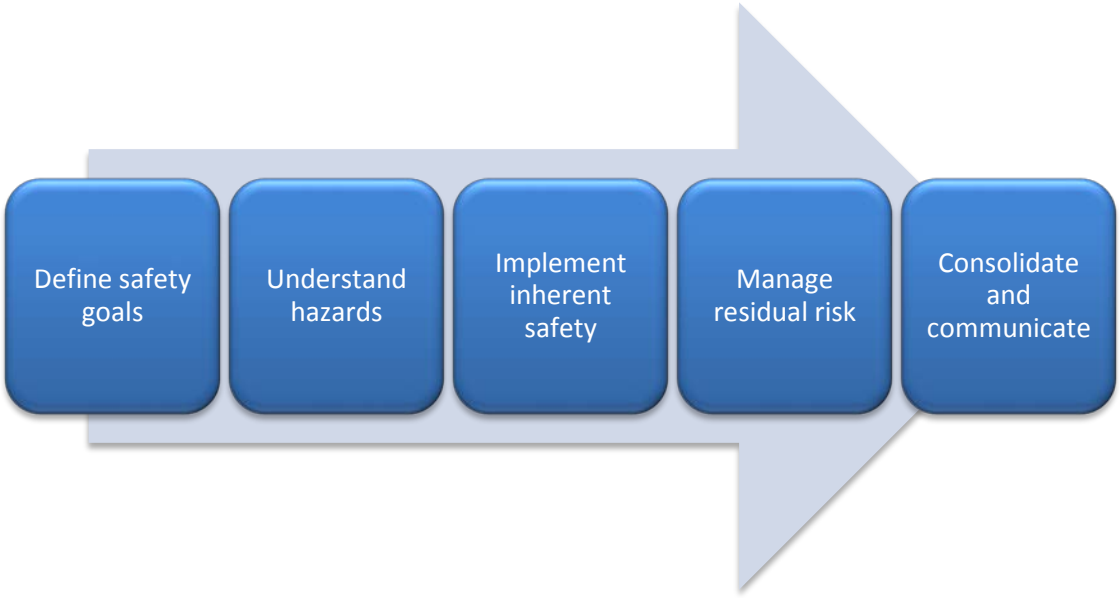

Figure 1: Amec Foster Wheeler's Safety by Design Process

By following the five steps of safety by design, Amec Foster Wheeler is able to demonstrate that hazards to people, environment, assets and reputation have

been systematically and comprehensively identified and assessed during the design phase of a facility/system or equipment.

A key feature of the safety by design process is that before hazards are managed with safeguards, it is examined whether these hazards can be entirely avoided, or their magnitude can be reduced by design. The result of this is that fewer safeguards are required and the performance requirement of these safeguards is reduced.

Safety by Design

Amec Foster Wheeler's safety by design process is a five step approach to engineering design which results in the ability to demonstrate that hazards to people, environment, assets and reputation have been systematically and comprehensively identified and assessed during the design phase of a facility/system or equipment.

The five steps, as illustrated in Figure 1, are:

- Define safety goals
- Understand hazards
- Implement inherent safety
- Manage residual risk
- Consolidate and communicate

Define safety goals

Defining the safety goals maintains focus throughout the safety by design process. The safety goals typically include the regulatory requirements, project specific requirements, risk criteria and as low as reasonably practicable (ALARP) criteria.

Understand hazards

Understanding the hazards identifies the hazards to people, environment, assets and reputation. The hazards could occur in the development phases (e.g. construction, fabrication, testing) and operational phases (e.g. operations, upgrade, decommissioning).

Implement inherent safety

Implementing inherent safety is a process that seeks to eliminate a hazard completely or reduce its magnitude sufficiently by means that is inherent in the process and thus permanent and inseparable from it. The result of this process is that the need for safeguards is eliminated or the required effectiveness of the safeguards is reduced.

Amec Foster Wheeler's approach to implementing inherent safety is based on the principles of inherently safer design, as defined by Amyotte and Kletz (2010) and the Center for Chemical Process Safety (CCPS) (2008). These principles are:

Eliminate – Remove hazardous materials, processes and activities;
Minimise – Use smaller quantities of hazardous substances,
– Minimise the number of hazardous activities;
Substitute – Replace a hazardous material with one that is less hazardous,
– Substitute a hazardous activity for one that is less hazardous;
Moderate – Minimise the impact of a release of hazardous material or energy, by changing the layout/configuration, adopting less hazardous operating conditions or a less hazardous form of a material, facilities,
– Minimising the number of people exposed, and;
Simplify – Design facilities in order to eliminate unnecessary complexity, thus minimising the possibility of human errors.

Manage residual risk

Managing residual risk determines the magnitude of risk associated with the hazards and adds controls or safeguards to reduce the risk to meet the risk criteria. Safeguards can categorised by type and sequence that they act on reducing the magnitude of risk.

The types of safeguards can be defined as follows and are presented in order of preference:

Passively engineered – Reduce the consequence or likelihood of an incident arising from a hazard through devices which do not require detection of an incident or action by any person or device.

Actively engineered – Reduce the consequence or likelihood of an incident arising from a hazard by detection of an incipient incident and activation of devices which interrupt the sequence of events resulting in the incident or mitigate the consequences of the incident.

Administrative – Reduce the consequence or likelihood of an incident arising from a hazard by detection of an incipient incident followed by implementation of procedures or human activated devices to interrupt the sequence of events resulting in the incident or mitigate the consequences of an incident.

The sequence that the safeguards act upon risk can be defined as follows and are presented in order of preference:

Prevention – Minimise likelihood of a hazard materialising
Detection and control – Limit severity of hazard before effects take place
Mitigation – Limit impact and prevent escalation
Emergency response – Evacuate and recover personnel

Combining the safeguard type and sequence order of preferences results in the overall order of preference shown in Figure 2.

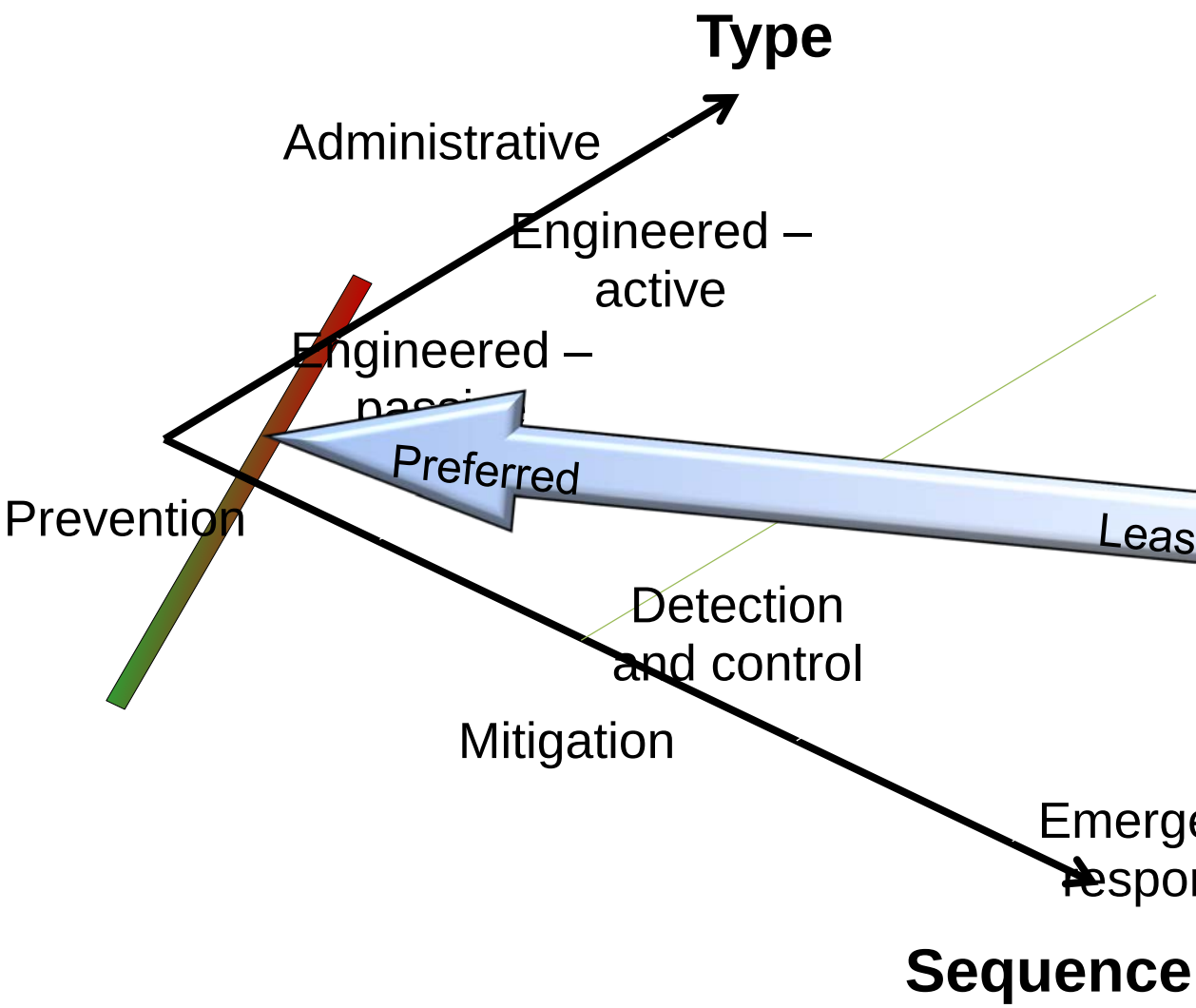

Figure 2: Safeguard Preference

Safety instrumented functions, such as high pressure trips, are considered active engineered safeguards and typically prevent a hazard from materialising. While safety instrumented functions, such as fire and gas trips, detect and control, or mitigate a hazard.

Consolidate and communicate

Consolidating and communicating demonstrates that the safety by design process has been completed as intended, meeting the goals defined at the beginning of the project. This is done by consolidating the results of the safety by design process and communicating these results to the relevant stakeholders.

Impacts of Applying Safety by Design

A systematic approach to engineering safety into the design is widely applied to managing major hazards. However, the systematic approach also reduces

other hazard types such as occupational health and safety, environmental, and asset.

Research by the Australian Safety and Compensation Council into the role of design in occupational health and safety incidents in Australia found design contributed to a significant portion of occupational health and safety incidents. In the Australian Safety and Compensation Council (2006) guideline it is reported that

- *Design-related issues were definitely or probably involved in at least 50% of the incidents in the agriculture, trade and mining industries with between 40-50% of the incidents in construction, manufacturing and transport/storage industries.*
- *Solutions already exist for most of the identified design problems…*(pg. 6)

By implementing a systematic approach to engineering safety into the design early in a facility's design lifecycle, the facility's risk can be minimised for the least cost.

To illustrate this, consider the location of occupied buildings in a facility with explosion hazards. By identifying the explosion hazards early in the facility's design lifecycle, before the layout has been fixed, the impacts of rearranging the layout of the plant to minimise the consequences of an explosion are minimised. There are no schedule impacts or engineering rework required in changing the layout. Thus, the layout will be optimised based on technical, operational and ALARP factors.

Once the layout has been fixed in the design lifecycle, the schedule impacts and/ or engineering rework becomes a constraint in optimising the layout. Additionally, the further the design lifecycle progresses the greater the schedule impacts and/or engineering rework. Once the plant is build the implementation costs become an additional factor.

Safety by Design Applied

An ethylene oxide explosion which was investigated by the US Chemical Safety Board (2006) will be used to illustrate the safety by design process.

Background

The following is a brief background to the incident. A complete background of the incident and subsequent investigation can be found on the US Chemical Safety Board (2006) website.

Ethylene oxide is a toxic and explosive gas used to sterilize products such as medical products. The product to be sterilized is placed into a large chamber and ethylene oxide is introduced into the chamber. Once the sterilization cycle has completed a gas wash occurs to purge the ethylene oxide through a scrubber and then the chamber is ventilated with air through a catalytic oxidizer. The catalytic oxidizer has an open flame.

The accident sequence started when the operator experienced alarms indicating a sequence failure in a sterilization chamber. In investigating the cause of sequence failure, a maintenance worker bypassed the gas wash. As a result of this a flammable mixture was sent to the catalytic oxidizer which subsequently ignited the mixture causing an explosion in the sterilisation chamber.

The explosion caused significant damage to the facility and shattered glass windows in the control room. Fortunately there were no fatalities but the shattered glass caused minor injuries to four people.

In this incident it is easy to focus on the maintenance worker who bypassed the gas wash. However, a different focus is achieved if the question is asked: What could the designers of the facility have done to prevent this incident?

To answer this question the five steps of safety by design can be followed.

Define safety goals

At a high level the safety goals defined would typically be:

- Fulfill applicable regulatory requirements relating to safety and environment.
- Implement inherent safer design principles.
- Meet risk tolerability criteria and/or as low as reasonably practicable (ALARP) criteria.

Understand hazards

Having defined the safety goals, a hazard identification (HAZID) study would be conducted to identify and understand the hazards of the facility. A key point at this stage is that the likelihood of a hazard is not considered. The focus is solely to identify hazards and understand their severity.
In this example, the HAZID would have identified that ethylene oxide is toxic and flammable, and the potential for an explosion.

Implement inherent safety

The inherent safer design principles are now applied to eliminate or reduce the hazards.

The first question that is explored is: Can the ethylene oxide be eliminated? There are other methods of sterilization which do not use ethylene oxide but if the other methods are not suitable for the products ethylene oxide is intended to sterilise then ethylene oxide is an integral component of the process and cannot be eliminated.

The second question that is explored is can ethylene oxide be minimised? How small of a volume of ethylene oxide can be used and stored, and still fulfil the

facility's process requirements? In this example the sterilization chamber could be reduced in size. This would reduce the size of the explosion.

The third question that is explored is can a different material that is less hazardous be used? In this example there is no option to substitute the material with a less hazardous material.

The fourth question is can we moderate the hazard? In this example, moderate can relate to modifying the layout to reduce the severity of the hazard. The layout of the facility could be optimised to minimise the severity of the hazard by moving the sterilization chamber away from occupied areas such that an explosion or toxic release would not impact the occupied areas.

Another way to moderate the hazard is to use a technology other than a catalytic converter with an open flame to remove the ethylene oxide in the final ventilation step.

The final question is can we simplify the design? How can we design this so that an operator or maintenance personnel will be less likely to make an error or an error will less likely release a hazard? In this example we would look at the actions operators and maintenance personnel would do and modify the design to simplify these actions.

Manage residual risk

Having applied the inherently safer design principles, the next step of the safety by design process is to manage the residual risk. It is at this stage that a hazard and operability (HAZOP) study is typically conducted to identify the scenarios that lead to consequences of interest.

It should be highlighted that due to the inherently safer design principles being applied in the previous step of the safety by design process, the HAZOP may not identify all of the scenarios identified during the HAZID as these scenarios have been designed out prior to the HAZOP. Additionally, the consequence severity of many of the scenarios would be significantly reduced.

Having identified the scenarios, each scenario's risk is assessed and evaluated against the risk and ALARP criteria defined in the safety goals. If a given scenario's risk does not meet these criteria then safeguards are evaluated in order of preference.

To illustrate this process, consider that none of the opportunities to implement inherently safer design identified above were implemented. The HAZOP would identify sequence control failure leading to ignition of ethylene oxide resulting in an explosion in the sterilization chamber.

The safeguards typically considered for this scenario would be:

- Sequence shutdown to safe state on detection of high gas concentration to catalytic converter (active engineered prevention)

- Install a flame arrestor (passive engineering prevention)
- Design of sterilisation chamber to withstand explosion and direct to safe location (passive engineered mitigation)
- Design of occupied areas such as the control room to withstand explosion(passive engineered mitigation)

The assessment of the safeguards would start at the most preferred safeguard where the safeguard's risk reduction and cost would be assessed to determine if the scenario meets the risk and ALARP criteria.

Consolidate and communicate

Finally, the documentation from the process is consolidated together. The documentation may include performance standards for the safeguards. The performance standards would then become the basis for the facility's safety management system.

As a result of following the safety by design process, it can be seen that the designers had ample opportunity to either prevent this ethylene oxide explosion from occurring or mitigating the risk to ALARP.

Conclusion

By applying a systematic to engineering design such as Amec Foster Wheeler's safety by design process it can be demonstrated that hazards to people, environment, assets and reputation have been systematically and comprehensively identified and assessed, and eliminated or mitigated as ALARP.

Furthermore, the application of the systematic process during the design cycle maximises the risk reduction to cost ratio as the costs of reducing risk is at a minimum.

References

Amyotte, P.; Kletz, T., 2010 'Process Plants: A Handbook for Inherently Safer Design', CRC Press, Boca Raton, Florida

Australian Safety and Compensation Council, 2006 'Guidance on the Principles of Safe Design for Work', Commonwealth of Australia, Canberra, Australian Capital Territory.

Center for Chemical Process Safety (CCPS), 2008, 'Inherently Safer Chemical Processes: A Life Cycle Approach' American Institute of Chemical Engineers, New York, New York

US Chemical Safety Board, 2006 'Sterigenics Ethylene Oxide Explosion - Investigations', http://www.csb.gov/sterigenics-ethylene-oxide-explosion/ accessed 29th October, 2015

