Evolving the hierarchy of risk control from blunt instrument to precision tool for cutting risk

Andy Brazier, AB Risk Limited, www.abrisk.co.uk

The process safety toolkit (e.g. HAZOP, LOPA, bow ties) introduces different terminology to describe the way risks are managed (e.g. safeguards, layers of protection, barriers). Although this sometimes leads to distracting discussions around definitions there is no real problem because each tool is quite clear. However, no single method can cover the complex nature of process safety risk and a broader perspective is required to form an overall judgement of how risks are and should be managed.

The hierarchy of risks controls [NIOSH 2023] is well regarded as a valuable concept that that helps with selecting the most appropriate strategies for managing risks. It encourages options to eliminate and reduce hazards are considered before engineering and administrative controls. However, its application to process safety risks is not entirely clear. PPE is normally presented as the bottom layer of the hierarchy, implying more relevance to personal safety. Also, the layers presented in the hierarchy are very broad and imply differentiation between types of control that may not exist in practice.

Inherent safety is another well regarded concept and is entirely consistent with the higher levels of the hierarchy of risk control, saying that hazard elimination and reduction is the most effective approach. Although it was introduced in the 1980's, application of inherent safety in practice has been quite limited. The challenge is that many undertakings in the process industry are inherently hazardous and in some circumstance an inherently safer solution may not actually create the lowest overall risk [Brazier et al 2021].

The hierarchy of risk controls reinforces a perception that engineering controls are better than controls that rely on human actions. However, humans can perform better than machines in many types of activity [Fitts 1951]. Also, there are very few engineered controls that can function reliably without human interventions at some point in their lifecycle.

The aims of this paper are to:

- Present a more detailed hierarchy of risk controls incorporating inherent safety;
- Highlight how different types of control rely on a combination of physical items (hardware), defined instructions or algorithms (software) and human actions (wetware);
- Encourage the acceptance of human actions as effective risk controls where appropriate;
- Illustrate how simplifying the way reasonably practicable controls are identified can lead to reduced overall risks.

Looking at engineered controls (currently one level in the hierarch) in more detail shows that they can be divided into multiple types. Engineered controls that are passive, permanent and preventative can be assumed to be available and effective at all times. They will appear higher on the hierarchy than engineered controls that are active, temporary and/or mitigative because there are more scenarios where the control may not be effective. However, there are potential issues to be considered with all types of control and the ultimate requirement of demonstrating that risks are As Low As Reasonably Practicable (ALARP) requires judgement to ensure positive and negative aspects of all risk controls are properly considered.

As an example, a fully welded pipeline carrying a hazardous substance is not an inherently safe solution because a leak may be unlikely but not impossible. It is a passive, permanent, preventative engineered control and so should appear relatively high on the hierarchy of risk controls . A pipeline made up of shorter sections of pipe connected by bolted joints is still a passive engineered control but its reliability depends on human actions when making the joints. It seems reasonable to place a pipeline with bolted joints lower that a fully welded one on the hierarch of control. However, it has some advantages that should be considered. No pipeline is 'fit and forget' and will require inspection or replacement at some time. Bolted joints make this far easier. If the associated human actions can be performed reliably it should be possible to overcome the apparently negative aspect of including joints in the design. There is no right or wrong answer and so judgement is required to decide which option creates risks that are ALARP.

The paper will present the expanded hierarchy of risk controls and use examples to illustrate how it may be used in practice. The aim is to create a more productive discussion of inherent safety, human factors and ALARP demonstration.

Key words: Human Factors, Human Factors Integration Plan, HFIP, Simultaneous Operations, SIMOPS, major project, temporary project, project lifecycle, construction and commissioning, rental equipment, contractors

Introduction

The hierarchy of risk control suggests that different approaches are more effective than others for controlling risk. For example, eliminating a hazard is better than adding engineered or administrative controls. It is a useful concept but practical application is not so clear. This paper describes how a more detailed hierarchy could be developed that may lend itself to developing a useful, practical tool.

Process safety toolkit

We have a number of tools available to support identifying process safety hazards and evaluating risks. No single tool addresses everything and so meaningful and comprehensive analysis requires use of several. Examples of tools in the toolkit include:

- Hazard and Operability (HAZOP) – examines plant, process or operation to identify credible deviations from design intent. Safeguards are identified that are intended to control risks of causes and consequences;
- Layers of Protection Analysis (LOPA) – a semi-quantitative assessment of hazardous scenarios. Layers of protection are identified and evaluated to confirm that, overall, the risk of the hazardous scenario achieves a specified target;
- Bow tie – a graphical representation of threats, hazards, consequences and escalation factors. Barriers are identified that are intended to stop threats leading to hazardous events, and hazardous events leading to consequences.

The terminology related to risk controls (e.g. safeguard, layer of protection, barrier) is defined within each tool but often used interchangeably. This can cause some issues because criteria for taking credit for a control varies between the tools, but in practice this is not really a problem as long as the source of information is known (i.e. which tool had been used). Most important is that the most appropriate tools are used, correct methods are followed and the focus is in the right areas. This should create a realistic evaluation of overall risk and control.

Hierarchy of risk controls – current form

The hierarchy of risk controls is a concept to be used when identifying and ranking risk controls to protect people from hazards [NIOSH 2023]. Following it should provide a robust and defensible risk control strategy.

The hierarchy is usually presented as an inverted triangle, as shown in Figure 1, to illustrate how controls vary in effectiveness from the top to the bottom.

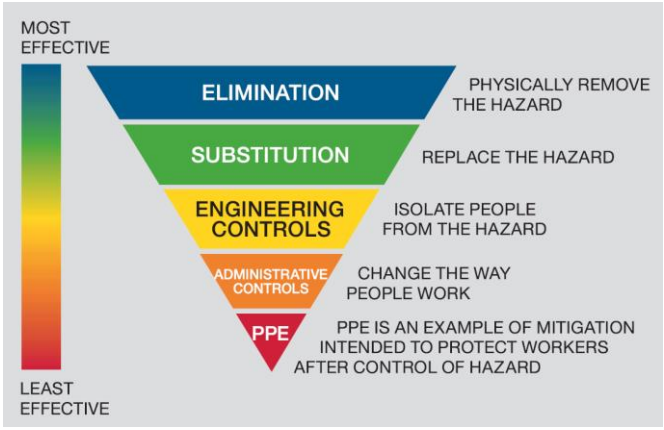

Figure 1 - Typical illustration of the hierarchy of risk control [Brazier and Wise 2021]

This concept is well regarded and has stood up to a degree of scrutiny. The validity of the triangle representation is questionable because there appears to be only one variable (effectiveness). Also, its application to process safety is unclear, reinforced by the inclusion of Personal Protective Equipment (PPE), which is far more concerned with personal safety.

The control types on the current hierarchy are very broad and create an overly simplistic view of how risks can and should be controlled in practice. It can lead to a view that engineering controls are purely technical and any human action falls into the administrative controls. In practice there are some very significant overlaps. For example, all engineered controls require some degree of maintenance, inspection and/or testing, which is inevitably carried out by people.

Inherent safety

Inherent safety proposes that controlling risks at source is more effective than adding safety systems. This is entirely consistent with the top levels of the hierarchy of risk control (i.e. elimination and substitution). Although originally promoted in 1980s by Trevor Kletz and others, practical application of inherent safety has been quite limited. Several organisations including the US Center for Chemical Process Safety (CCPS) and Energy Institute (EI) have developed definitions and some guidance [Brazier et al 2021]. However, over recent decades there has been an expansion in the use of engineering risks controls, particularly safety instrumented systems (SIS), which is entirely the opposite to inherent safety.

Trevor Kletz had a neat way of describing inherent safety as follows [Kletz 1991]:

- What you don't have can't leak;
- People who are not there can't be killed;
- The more complicated a system becomes, the more opportunities there are for equipment failure and human error.

One challenge is that inherent safety is often viewed as a binary outcome, either fully achieved or not at all. For an industry where hazards are integral to the process, it may appear that inherent safety cannot be applied. This is not the case and at all stages of plant's lifecycle there are opportunities to select inherently safer solutions, which reduce reliance on add-on risk controls.

ALARP

The ultimate requirement for any hazardous undertaking is to reduce risks to As Low As Reasonably Practicable (ALARP). This may be a legal requirement in some countries, including the UK, but should be seen as a moral obligation by any professional who influences the way risks are managed, especially where there is the potential for major accidents.

Although ALARP may be seen as another high level concept that can be difficult to apply it can be handled in a simple way. The UK HSE [HSE 2019] suggest that answering the following questions can demonstrate that risks are ALARP:

Question 1 – What more can I do to reduce risks?

Question 2 – Why have I not done it?

You should note that HSE uses the pronoun "I" in these questions. It implies that deciding if risks are ALARP relies on assessments made by individuals on behalf of a company. It does not matter what role you have in a company. If you are working with major accident hazards you need to make sure you can answer these questions [Brazier 2021].

Evolving the hierarchy of risk control

The principles of the hierarchy of risk control appear to be sound but a lack of precision seems to limit its practical application. Creating a more detailed hierarchy with additional guidance about benefits and potential downsides of each risk control type may improve understanding of how risks can be managed in practice.

Taking credit for inherent safety

One of the challenges with applying inherent safety is that removing or substituting a hazard fundamentally changes an activity. The original hazard that has been eliminated is unlikely to feature on the risk assessment for the new activity and so it is difficult to take credit for selecting the inherently safer solution. This can perversely result in safety features being added to demonstrate something has been done.

Perhaps expanding the ubiquitous risk matrix to include an 'inherently safe' region would help?

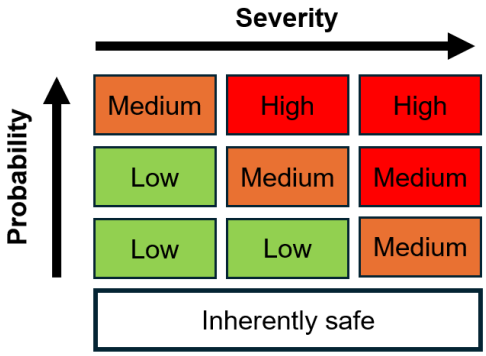

Figure 2 - Risk assessment matrix including inherent safety

Even if a fully inherently safe solution is not available, being able to take credit for selecting the inherently safer solution should be beneficial. Explaining why a hazard cannot be avoided should be part of the ALARP demonstration.

Taking credit for controls considered to be weaker

There is general view that engineered risk controls are better than controls that rely on human actions. The argument is that people are error prone and unreliable. However, the concept of allocation of function [Fitts 1951] tells a different story. It identifies that machines are good at speed, repeatability and simultaneous operation. However, people are usually better at detecting, perception, using judgement and improvisation.

Another issue with favouring engineered risk controls is that very few can function reliably without human interventions at some point in their lifecycle. The irony is that people using the hierarchy of risk control are satisfied if an engineered control is identified because they believe human factors do not need to be considered.

Explaining why a control is not selected

The second question when demonstrating ALARP requires you to say why a risk control is not being used. Cost benefit analysis may be used to make that argument, but it is complex and relies on data that is often hard to source and justify.

All types of risk control have potential downsides. Even inherent safety through hazard elimination can result in risk being transferred elsewhere. Whether that is your concern may be a moral dilemma, but being aware of the issues of each type of risk control can support a thorough ALARP demonstration.

Control components

Risk controls can have a range of components, consisting of:

- Physical items, tools and equipment (hardware);
- Logic and programmes used by electronic systems. Also, rules and procedures used by people (software);
- Actions perform by people (wetware).

Recognising this is particularly important when considering engineered controls. For example, it is easy to focus on the hardware (e.g. sensors, logic solver, final elements, cables etc) and software (e.g. conditional rules or logical constructs handled by relays, processors) of a SIS. However, the wetware element is also critical, for at least its maintenance, inspection and testing, which are performed by humans.

Identifying all the components required for a risk control to function (i.e. hardware, software and wetware) may encourage a more a balanced view when deciding what combination of control is required to achieve risks that are ALARP.

The only exception to this is inherently safe controls, which should be intrinsic to the system. If hardware, software or wetware are required for a control to function it should not be considered as an inherently safe.

Proposed hierarchy

The figure below proposes an evolved hierarchy. Features include:

- Hazard elimination and substitution have been replaced by inherent safety;
- Inherent safety has been expanded to allow credit for simplicity and keeping people away from hazards;
- The hierarchy shows that mitigation can make a valuable contribution to risk management (not just PPE);
- Inherently safe controls may be either prevention or mitigation; whilst engineered and administrative controls can be applied to both.

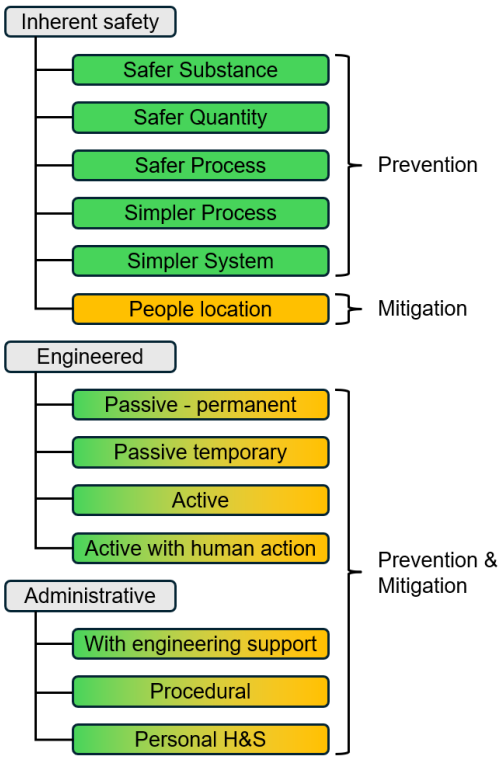

Figure 3 - Expanded hierarchy combing prevention and mitigation

The figure only shows the high level set of control types. Within each there are multiple examples that can be arranged into a more detailed hierarchy. See Appendix A below.

Some of the interesting developments from creating this hierarchy are discussed below.

Inherent safety - substance and quantity

Addressing ‘what you don’t have can’t leak’ can be achieved by either elimination or using a low hazard substance. This should always be the first consideration but even this option has potential downsides if risks are simply transferred elsewhere. This fact may be used as part of an ALARP demonstration (i.e. why a hazard has been retained and not eliminated).

Using a source of material that has a naturally low concentration of the hazard may be inherently safe if it is below the level when harm can occur. Doing so is likely to result in handling of greater volumes of material and may be vulnerable to natural variability. If the low concentration is achieved by processing a natural product, or it undergoes a process on site to increase its concentration a judgement needs to be made about how close the solution is to being inherently safe.

Substances in a stable form (i.e. solid instead of gas) can be inherently safer. Also, a substance that is naturally conspicuous to humans due to odour, colour etc. may be safer than an odourless, colourless alternative.

Inherent safety - simplicity

Trevor Kletz included simplicity in his principles of inherent safety, and the benefit it quite clear. However, credit is rarely given to simplicity and the proliferation of control and safety systems has generally resulted in more complexity.

A simpler process would create fewer parameter changes and have more predictable outcomes. A simpler system would have fewer add-on control and safety systems. They may result in less efficient processes or create a higher reliance on human monitoring and control. However, including simplicity in the hierarchy should prompt a discussion about whether arrangements are as simple as they can be and a justification for complexity where it is deemed unavoidable.

As an example, propane road tankers are routinely filled by operators or drivers, with minimal instrumentation or overfill protection devices. An ‘ullage’ valve is opened, which starts to release liquid when the fill level has been reached. This is a simple solution and proven to be effective. More complex systems could be introduced (e.g. instrumented level control and overfill protection), but add complexity with associated issues. Being able to take credit for simplicity should remove incentives to add on safety features that increase complexity.

Inherent safety – human location in relation to hazards

This aspect of inherent safety is covered by Trevor Kletz’s principle that people who are not there can’t be killed. It can be viewed as a mitigation control. Features that result in people being physically separated from a potential hazard are most effective. Locating sites away from housing and company offices away from hazardous plant may not protect everyone, but can reduce the likelihood of harm to many people. Natural ventilation can prevent hazardous atmospheres forming without any equipment. Also, modern technology gives us the opportunity to deploy drones and remotely operated vehicles into potentially hazardous areas, so that people can remain safe.

There are potential downsides to each option. For example the technology required to operate remote facilities may add complexity. This does not mean this is not a valid option but highlights how judgement is required whenever risk controls are being selected. Whilst it is most effective during the design phase when deciding plant layout it can still apply during operations, including the use of exclusion zones when hazardous tasks are being carried out.

Passive engineered controls

Passive controls are designed to function without requiring any external input, action, or power to achieve their function. The most reliable are passive engineered controls that are permanently in place. In a preventative role they include the pressure envelope created by permanently installed pipework, vessels and other plant. In a mitigation role they include permanent obstacles that keep people away from potentially hazardous areas, secondary containment and passive fire protection.

Some passive engineered controls may not always be available and should appear lower on the hierarchy than permanent ones. For example flexible piping or hoses used to form the pressure envelope, blank flanges and valves used as isolation. Also, a secondary containment that includes drain valves should appear lower on the hierarchy than those without valves.

Pipework provides an illustration of how the hierarchy may work in practice. It is tempting to consider fully welded pipework as an inherently safe solution because it does not have any joints, which are usually considered as a potential leak point. But the hazardous material is still present and solid pipe does fail. The effectiveness of the control depends on the physical design (hardware) and quality of maintenance, inspection and testing performed by people. It should be identified as a permanent, passive engineered control (i.e. not inherently safe) that requires human factors to be considered.

Pipework with joints is also a passive engineered control, but should appear lower on the hierarchy because the joints are a potential leak point and require more human intervention (e.g. make the joints, leak testing etc). However, there are advantages in having joints, especially when performing maintenance, inspection and testing. Although the order on the hierarchy is probably correct (i.e. fully welded above pipework with joints), they should appear very close to each other.

Flexible pipework is also a passive engineered control but should be considered as temporary. This puts it lower on the hierarchy than fully welded or pipework with joints. This makes sense because there are more opportunities to fail, even if hoses are fully rated for the service.

Active engineered controls

Active controls involve a reaction to an input that triggers a function. They usually involve moving parts (hardware) and some method of interpreting the input and triggering the function (software). They have a high reliance on maintenance, inspection and testing (wetware). Preventative controls include safety valves, bursting discs, SIS and other trip systems. Powered devices that activate to control a known hazard such as local exhaust ventilation or a waste gas afterburner may also appear in this part of the hierarchy, although their position in comparison to safety valves and SIS is difficult to decide. Examples of mitigation controls include Emergency Shutdown (ESD) initiated by Fire and Gas (F&G) detection, emergency venting or blowdown and automated active fire fighting (e.g. deluge).

The main challenges with active engineered controls is ensuring they activate reliably when required. Human factors often receive insufficient attention when designing active engineered systems including the means of informing people that the control is unavailable or has failed to activate on demand. Maintenance, inspection and testing can be complex and can introduce failures, leaving the controls unavailable.

Active engineered controls with human action / administrative controls with engineered support

The current hierarchy of risk control shows a clear divide between engineered and administrative controls. In developing a more detailed hierarchy it became apparent that there is really a continuum between these with a subtle difference between controls that may be considered as engineered but require a human intervention to operate (this is in addition to maintenance, inspection and testing which applies to all engineered controls) and controls that are largely achieved by human actions but supported by engineering.

Response to process system alarms is an interesting example of a preventative control. It is easy to focus on the hardware and software that result in alarm annunciation and conclude that it is an engineered device. But control only occurs when a person takes action. On this basis most alarms are best considered as an administrative control supported by engineering (i.e. lower on the hierarchy). One class that may be viewed slightly differently is a Highly Managed Alarm (HMA). Where these are used the standards [IEC 2022] require much greater consideration to the reliability of the human operator, who may be considered as an integral part of the alarm system. HMA should appear higher in the hierarchy than normal process alarms, and may be identified as engineered controls with human action.

Other preventative administrative controls with engineered support include a control system that keeps a process away from potentially hazardous state, valve minimum stop, slow acting valves and automated sequences achieved by a control system but triggered by the operator.

Another example that is often viewed as an engineered control but may not be as reliable as it seems is a key trap interlock. Again the focus is often on the hardware but it is the operator action of opening or closing the valve that can result in a hazard. If interlocks can be proven to be highly reliable and impossible to defeat, they may be located higher on the hierarchy but in practice the operation of the valve should be seen as an administrative control and the interlock as an engineered support (i.e. lower on the hierarchy).

There are quite a number of mitigation controls where hardware and / or software are provided, but rely on people to operate. We often rely on humans to make a judgement of when and how to react to hazardous situations, which is consistent with the allocation of function mentioned above. Sounding evacuation alarms, active fire fighting and reactor quench or kill are examples.

Administrative controls

The role of procedures, signage and competence are well understood as administrative controls. Hardware rarely features (although physical design of a sign may be an exception) and software is limited to documented rules and systems (i.e. not electronic).

Other administrative controls include high performance Human Machine Interfaces (HMI) that support situational awareness, dilution of hazardous substances to make them safer and use of additives to make them more conspicuous (e.g. colour, odour). Also, hazard segregation, defined operating limits (including managed inventory) and reduced occupancy of buildings. The reliance on human behaviour and performance, including compliance are clear. However, one of the aims of developing the hierarchy is to allow credit to be taken for all types of control.

Personal health and safety control

The current hierarchy of risk controls usually shows PPE at the bottom, and that is a valid as a type of mitigation control from a personal health and safety perspective. Even here there is a hierarchy because collective PPE is viewed as more effective than individual devices (e.g. a safety net protects everyone whilst a harness and line only protects an individual, and only if they are using it correctly).

For prevention, examples that may contribute to personal health and safety include ergonomic design, mechanical aids to reduce manual handling, personal monitors with alarms and health screening. It makes sense to include these on an enhanced hierarchy, although their relevance to MAH is minimal.

Conclusion

The aim of this paper was to illustrate how the hierarchy of risk controls could be expanded. It is proposed that it could be divided into three main types (inherent safety, engineering and administrative), with all applying to both prevention and

mitigation. Further sub-division is possible, with the transition between each being a continuum rather than distinct. And within each sub-division it appears to be possible to arrange specific examples in hierarchical order. Overall, it appears to be possible and potentially beneficial to do this.

Ultimately the true benefit will be achieved by developing a tool that uses the expanded hierarchy of control to ensure an appropriate range of controls is used. This should allow judgement to ensure the overall outcome achieves risks that are ALARP. For each item on the expanded hierarchy it has been possible to highlight what each control needs to function (hardware, software and wetware); and the issues that need to be considered when deciding if a control should be implemented or demonstrating that it is not required because an alternative will achieve ALARP. The expanded hierarchy should support this by ensuring all options are considered and sensible decisions are made about which controls should and should not be used.

An overview is shown in Attachment A of this paper. Also, a spreadsheet showing the components of each control type and issues to consider can be downloaded at https://abrisk.co.uk/wp-content/uploads/2024/09/ABRisk-Expanded-Hierarchy-of-Risk-Control.xlsx

References

Brazier, A. Risks: Tools of the Trade. The Chemical Engineer (2021)

Brazier, A. Edwards, D. Macleod, F. Skinner, C. Vince, I. Trevor Kletz Compendium. Elsevier (2021)

Brazier, A. Wise, N. Making sure risks are ALARP. The Chemical Engineer (2021)

Fitts, P. M. Human engineering for an effective air-navigation and traffic-control system. Washington, DC: National Research Council (1951).

Health and Safety Executive (HSE). Health and Safety Executive HID CI5A, Guidance, SPC/Permissioning/37, Version 3 (2019)

International Electrotechnical Commission (IEC). 62682 Management of alarm systems for the process industries, edition 2.0 (2022).

Kletz, T. Plant Design for Safety - A User Friendly Approach, Hemisphere Publishing (1991)

National Institute for Occupational Safety and Health (NIOSH). Hierarchy of Controls. https://www.cdc.gov/niosh/topics/hierarchy (2023)

Attachment A – Proposed hierarchy with examples in hierarchical order

Type	Examples – prevention	Examples – mitigation
Inherently safer substance	• Low hazard substances • Naturally low concentration of hazardous substance. • Stable form (e.g. solid not gas) • Naturally conspicuous hazard (odour, visible, detectable)	Not applicable
Inherently safer quantity	• Small fixed volume of hazard. Tanks, vessels, pipework (length/diameter)	Not applicable
Inherently safer process	• Process sub-steps eliminated • Pressure / temperature near ambient at source (i.e. not achieved by a control system)	Not applicable
Inherently simple process	• Parameter changes have few and predictable outcomes	Not applicable
Inherently simple system	• Minimum of add on control /safety devices	Not applicable
Inherently safer location for people	Not applicable	• People located outside of the hazardous zone • Natural, permanent obstacle between hazard and people. • Natural ventilation prevents hazardous concentrations forming • Remotely operated or autonomous mechanised devices (robots in hazardous area)
Passive engineered item - permanent	• Pressure envelope rated for the full range of operating conditions possible - without joints. • Pressure envelope rated for the full range of operating conditions possible - with joints. • Bridge over road or rail track	• Created permanent obstacle between hazard and people. • Secondary containment with no breaches (double walled tanks) • Tertiary containment with no breaches (bunds, dykes) • Permanently installed passive fire protection
Passive engineered item - temporary	• Pressure envelope rated for the full range of operating conditions possible - using temporary connections (hose, loading arm) • Positive isolation (blank flange, spade) • Valve isolation • Physical obstacles that could be removed (machine guards, dust hoods, road barriers)	• Secondary containment with breaches (double walled tanks with drain valve) • Tertiary containment with breaches (bunds, dykes with drain valves)
Active engineered	• Physical obstacles deployed automatically (train level crossing) • Pressure safety valve / bursting disc • Hazard removal (local exhaust ventilation, after burner) • SIL rated safety instrumented function • Non SIL rated trip	• Automated blowdown • Automated active firefighting (deluge, water mist, water curtain) • Shutdown initiated automatically by fire and gas detection
Active engineered with human action	• Highly managed alarm	• Protective system alarms (fire, gas spill). • Manually operated active fire fighting • Decontamination devices (safety shower)
Administrative control with engineered support	• Tightly controlled process keeping hazard within boundaries (minimum gassing off, no over-spray) • Fixed physical device forcing an action (valve minimum stop, slow acting valve) • Active physical device forcing an action (Valve sequence fixed by key trap interlock) • Automated actions initiated by a human (Automated sequence via BPCS) • Automatic process control • Process alarm • Beacons, light-up signs triggered by a condition.	• Shutdown initiated manually • Exclusion zones around hazardous areas • Reaction quench / kill
Administrative control	• High performance HMI for operator situational awareness • Created low concentration of hazardous substance. • Created conspicuous hazard (odour, visible, noise) • Hazard segregation • Defined operating limits (tank level, operating temperature / pressure). • Control of work procedure (permit to work) • Safety critical operating / maintenance procedure • Plant patrol with effective checklist • Competence management system • Operating / maintenance procedure • Signs and labelling • Communication supported by a relevant tool (shift handover with formal log, permit to work)	• Emergency response procedures • Emergency response practice (emergency exercises, desk top scenarios) • Emergency response training (class room) • Reduced occupancy
Personal health and safety control	• Ergonomic design • Mechanical aids (avoid manual handling) • Personal monitors with alarms • Health screening • Hazard exposure surveillance	• Collective PPE (safety net) • PPE used routinely (safety glasses) • PPE used during emergency (escape BA)