# Making Sure Risks are ALARP

*Andy Brazier and Nick Wise explain why it's so important to consider real-world situations in risk assessment*

**IN THE previous two articles[1,2] we have highlighted that the various safety study methods available are the tools in your toolkit, and you should expect to use them wisely to allow you to decide whether risks are as low as reasonably practicable (ALARP). This final article in the series illustrates how even the fundamental safety principles that we are all familiar with (including inherent safety, hierarchy of risk controls, continuous improvement and being cautious) have to be applied sensibly when deciding whether overall risks are ALARP; and why it is so important to consider real-world situations.**

## INHERENT SAFETY

We have, as an industry, been aware of inherent safety since the 1970s, thanks to a great extent to the late Trevor Kletz. Although he says that he did not develop the original idea, it is very clear that he did a great deal to advance and promote it to the point today where it is widely accepted as a fundamental safety concept[3].

When we look back at the intervening decades, there has been an expansion in the use of engineering risks controls, particularly safety instrumented systems (SIS). This appears to be at odds with the principles of inherent safety, which Kletz summarised with the following concepts[4]:

- "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."

The best time to consider inherent safety is very early in a new project (typically, the concept phase). This may give you the impression that after this stage, and particularly once a system is operational, the opportunity has been missed. There may be fewer options available but it should still be considered as part of safety studies performed later in projects, when planning modifications, revalidation of safety reports/cases and when identifying actions following an incident investigation[3]. Also, the principles can be applied for routine work, for example by reducing stored inventories and when preparing plant for maintenance.

Inherent safety can often be viewed as a binary outcome – either fully achieved or not at all. Certain hazards may be integral to your process, so there is no viable option to eliminate them, and you may assume that inherent safety does not apply unless you are prepared to completely change business. This is not the case.

CERTAIN HAZARDS MAY BE INTEGRAL TO YOUR PROCESS, SO THERE IS NO VIABLE OPTION TO ELIMINATE THEM, AND YOU MAY ASSUME THAT INHERENT SAFETY DOES NOT APPLY UNLESS YOU ARE PREPARED TO COMPLETELY CHANGE BUSINESS. THIS IS NOT THE CASE

Understanding the 'gap' between current arrangements and the inherently safe solution can be particularly useful, especially when deciding what additional risk controls should be in place. If the gap is large, there will be a high reliance on add-on risk controls. In many cases, the gap may be quite small or only exist for certain modes of operation (eg plant startup).

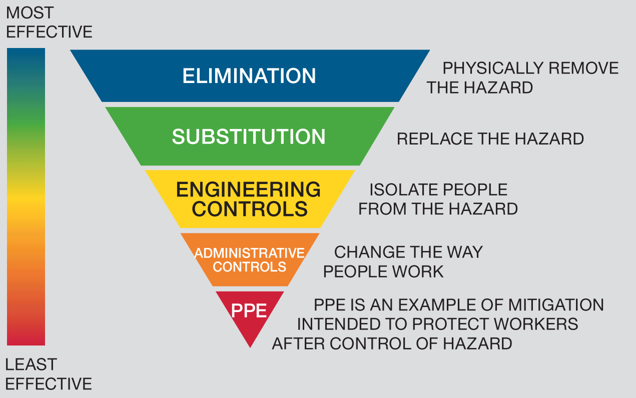
Whilst you should be looking for opportunities to apply inherent safety at all times, eliminating or reducing your immediate risks may only mean that they are transferred elsewhere. For example, choosing to not make a product, to eliminate a hazard, may simply mean that production is moved to another site, possibly in another country[3]. The alternative may apply lower safety standards. Also, risks from transport will have increased. This does raise some complex societal risk conundrums, which you may think are not your responsibility. You may be able to argue that continuing local manufacturing is the inherently safer option because you have better control of the risks. This highlights why inherent safety cannot be seen as a simple, binary decision.

## HIERARCHY OF RISK CONTROL

The hierarchy of risk control (*see Figure 1*) is another fundamental safety concept. Controls at the top of the hierarchy are generally more reliable. Controls at the bottom of the hierarchy are generally easier to implement once a system has been designed or is in operation, but are less effective.

There are clear overlaps at the top of the hierarchy (elimination and substitution) with inherent safety. This is a useful reminder that you have multiple approaches when evaluating risks and making clear-cut distinctions between them is neither necessary nor helpful[3]. One important difference is that inherent safety can reduce risk by reducing potential consequences and likelihood. Other controls are mostly concerned with reducing likelihood.

**FIGURE 1:** HIERARCHY OF CONTROLS


MOST EFFECTIVE
ELIMINATION
PHYSICALLY REMOVE THE HAZARD
SUBSTITUTION
REPLACE THE HAZARD
ENGINEERING CONTROLS
ISOLATE PEOPLE FROM THE HAZARD
ADMINISTRATIVE CONTROLS
CHANGE THE WAY PEOPLE WORK
PPE
PPE IS AN EXAMPLE OF MITIGATION INTENDED TO PROTECT WORKERS AFTER CONTROL OF HAZARD
LEAST EFFECTIVE

The principles behind the hierarchy of risk control are very sound, but may give you the impression that you only need to consider administrative controls and mitigation if you cannot implement effective engineered controls. In reality, all engineered controls have their limitations. You should be considering risk controls from all parts of the hierarchy when deciding if risks are ALARP.

One of the arguments for discounting operational controls and mitigation is that they are vulnerable to human error. Hardware controls appear to be more reliable, but can only be relied on for the situations they are designed for. Human performance can vary dramatically and so people can appear to be less reliable. However, this is also a benefit because it allows people to deal with the variability of the real world, including non-routine, unplanned and unexpected situations.

## CONTINUOUS IMPROVEMENT

The Plan-Do-Check-Act (PDCA) cycle is standard in many management systems. It can imply that you should always be doing something to improve safety. This may encourage you to keep adding more risk controls, especially if your organisation has not defined a level of risk that is considered to be broadly acceptable.

It is difficult to argue with the underlying principle of continuous improvement but it has limits. If effective controls are already in place, the risk reduction achieved by adding more will be negligible, and knock-on effects and unintended consequences may actually result in increased overall risk.

As an example, the introduction of digital control systems allowed more alarms to be added at minimal cost. The result was that operators became overloaded with nuisance alarms, which detracted them from proactively operating the system and identifying and dealing with problems early.

The answer has to be to have the right controls in place, recognising their strengths and weaknesses. You should continuously review your risks to confirm they are still ALARP, but do not feel pressurised into adding or changing controls just to prove you are applying continuous improvement.

## BEING CAUTIOUS IN ASSESSMENTS

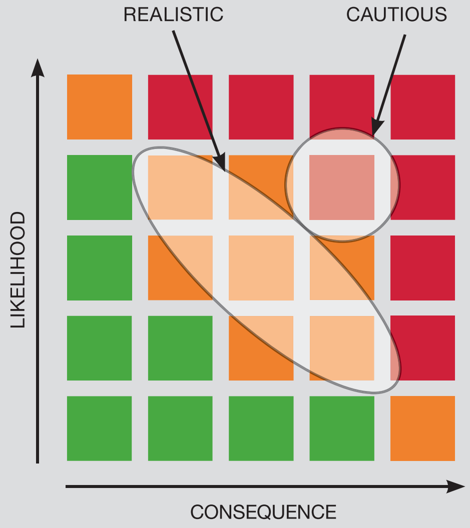
No one wants to be considered reckless where safety is a concern. Surely it is much better to be cautious and have a system that is safer than it needs to be? This may lead you to take the worst cases for both consequence and likelihood when using a risk assessment matrix, inputting a greater hazardous event frequency when performing LOPA or taking a pessimistic view of the reliability of every risk control measure applied. However, this can force you into adding controls that are not really required in order to satisfy perceived risk targets.

> CAUTION CAN RESULT IN RISK AVERSION WHERE THE OBJECTIVE BECOMES THE AVOIDANCE OF ALL KNOWN RISKS

Caution can result in risk aversion where the objective becomes the avoidance of all known risks (*see Figure 2*). This can have immediate and significant impacts on business because the cost of safety will quickly spiral. However, risk aversion can lead to poor management of risks in practice. People may feel compelled to circumvent systems to get the job done or they lose the ability to deal with risks effectively.

There is no harm in taking a cautious approach as long as you acknowledge and record it as such, and the outcome is a sensible set of risk controls. However, be prepared to challenge additional controls resulting from overly-cautious assessments if these appear unreasonable based on your engineering judgement and experience.

**FIGURE 2:** BEING CAUTIOUS CAN LEAD TO BAD DECISIONS



## FAILING TO RECOGNISE REAL-WORLD ISSUES

Safety studies can only consider a fairly limited snapshot of a system and its operation. The real world throws up a lot of challenges. These can mean that your nicely-designed controls are not as effective as you assume. This is important when making sure overall risks are ALARP.

Steady-state production may be the most common mode of operation but is usually lower risk than others (ie a disproportionate number of process accidents occur during startup and shutdown[5]). Controls set up for steady state can often be problematic for other modes. For example, plant startup may require SIS to be overridden and cause a high number of process alarms. These reduce the effectiveness of the controls and increase operator workload.

You need to consider the real world when deciding if risks are ALARP. When you factor in requirements for engineered controls to be maintained, inspected and tested, and the effect they can have on your operation when they fail, you can understand why inherent safety is so important; but also why you need good operational controls and mitigation as a backup.

## PUTTING THIS INTO PRACTICE

*Table 1* gives you an idea of how you can use the findings from safety studies and other inputs including operational experience to make your judgement about whether risks are ALARP. You may want to use it at key stages in projects and routinely for an operating plant (possibly every five years when revalidating a safety report/case). The example from the first article in this series is used to illustrate – a heater fired by natural gas with three coils operating in parallel, handling process gas.

## CONCLUSIONS

The aim of this series of three articles was to remind you that you have a responsibility to make sure risks are ALARP. Carrying out safety studies and following fundamental safety principles in isolation will not do this for you. Ultimately you should make your own judgement about whether risks are ALARP, and be prepared to defend it.

Over the last couple of decades we have seen a proliferation of add-on engineered controls (particularly SIS). This is partly due to developments in technology; but often they have been installed as a result of actions from safety studies. Unfortunately, we have not seen the same developments in the application of inherent safety. Also, the increased availability of engineered controls may have removed incentives to improve operational controls and mitigation, even though we instinctively know they make a great contribution to the control of risks.

For overall risks to be ALARP, the controls in place have to cover all modes of operation and every eventuality. Your judgement needs

**TABLE 1:** EXAMPLE OF HOW TO USE FINDINGS FROM SAFETY STUDIES

| PROMPT | EVALUATION | EXAMPLE REFERENCES |
|---|---|---|
| *Scenario* | No flow through coil leading to coil failure and release of process gas. | PHR report. |
| *Inherent safety* | Coil design temperature = 220°C.  Heater maximum temperature = 250°C. | Manufacturer's specification. |
| *Engineered controls (passive)* | During operation the process gas flow removes sufficient heat to maintain the maximum operating temperature at 190°C.<br>The coil will withstand some heat input and would not fail instantaneously. | Operational experience. |
| *Engineered controls (active)* | SIL 1 rated SIS activated by coil high temperature.<br>Non-rated trip activated by low combined process flow (does not protect against single coil being blocked). | LOPA report.<br>Bow tie diagram. |
| *Operational controls* | Low process flow and high coil temperature handled by the control system.<br>Alarm responses are defined. Control room operators are trained and assessed on their ability to respond to alarms.<br>Return to service procedure for the heater includes checks to confirm coil isolation valves are open. There is no operational requirement to operate these valves.<br>Heater startup procedure ensures process gas through the coils is achieved before ignition. | Alarm rationalisation report.<br>Safety critical task analysis report. |
| *Mitigation* | Gas from failed coil would enter the heater firebox and be ignited instantaneously. A jet fire is possible. The heater is in a low occupancy area so the likelihood of immediate harm to people is low.<br>Fire detection automatically shuts down the heater and stops the process gas flow. The site evacuation alarm is sounded automatically if multiple fire detectors are activated or will be sounded manually by the control room operator. | PHR report.<br>LOPA reference report.<br>Bow tie diagram.<br>Fire & gas mapping report. |
| *What more could be done to reduce the risks?* | Coils could be fully rated for maximum temperature.<br>Coil isolation valves could be removed.<br>Upgrade process gas low flow trip to a SIL1 SIS.<br>Upgrade the process gas trip to activate on low flow through any coil. | ALARP review workshop. |
| *Are these actions required to achieve ALARP?* | Coil design is already close to maximum temperature possible. There is no situation where coils are isolated individually. The risk reduction of this measure would be negligible.<br>Valves are required to balance flows. Removal would affect furnace efficiency and environmental performance.<br>High temperature SIS provides full and reliable protection. Incremental improvement of this action would be very small.<br>Being able to monitor flows through individual coils may not have a significant safety improvement but may have operational benefits. | ALARP review workshop. |
| *ALARP summary* | The gap between current design and inherently safe design is small. There is no experience of blocked coils whilst the heater is online. Coil isolation valves would only be operated very infrequently and status checks are covered clearly in procedures. The SIL1 for the high temperature SIS is based on a cautious assessment of hazardous event frequency. | ALARP review workshop. |
| *Action* | Investigate options for providing individual flow transmitters on each coil. If reasonably achievable, display flow data on the heater control system graphics. Also, consider any benefits of providing alarms and/or a trip activated by the new transmitters | ALARP review workshop. |

to take into account information from many different sources including safety studies and operational experience (yours and others). You need to accept that risks exist and continually review how you control them. Having more controls does not necessarily mean lower risk. Ultimately you have to become skilled at understanding risk and how it is controlled in practice. ■

*Andy Brazier AMIChemE is Consultant at AB Risk; Nick Wise CEng FIChemE is Business Support Manager at SSE Thermal*

## REFERENCES

1. Brazier, A, and Wise, N, *What Safety Studies Have You Got on Your Menu?*, TCE 958, April 2021, https://bit.ly/3vJUapM.
2. Brazier, A, *Risk: Tools of the Trade*, TCE 959, May 2021, https://bit.ly/2SxshmA.
3. Brazier, A *et al*, 2021, *Trevor Kletz Compendium*, Elsevier.
4. Kletz, T, 1991, *Plant Design for Safety - A User Friendly Approach*, Hemisphere Publishing.
5. BP Process Safety Series 2006, *Safe Ups and Downs for Process Plants*, IChemE.