

## Safety practice

# Flixborough and inherent safety – inspired by Trevor Kletz

Andy Brazier, UK

## Overview

The official inquiry into the Flixborough disaster<sup>1</sup> identified shortcomings in integrity of plant, management of change and plant management as specific learnings. Trevor Kletz, on the other hand, was prompted to consider why the plant had been so hazardous in the first place and whether a better chemical process design could have allowed a smaller inventory, which would have been inherently safer. A paper presented by N.A.R. Bell at a symposium three years before the accident ultimately led him to develop his ideas about inherent safety, leading to his first paper on the subject being published in 1978. Of course, Kletz is not the only person to have thought about inherent safety in the 50 years since Flixborough, but he was one of the most prolific. In the Trevor Kletz Compendium<sup>2</sup> we dedicated a full chapter (40 pages) to summarising the historical and current views on the subject and its place in the hierarchy of risk controls. This paper is a shortened version.

**Keywords:** Inherent safety, Flixborough, Kletz

## What is inherent safety?

It is probably fair to say that inherent safety is a concept rather than a clearly defined method or approach. This may explain why the development of a universally agreed definition has not been straightforward.

Whilst Kletz wrote a lot about the subject, he does not appear to have used a specific definition. One of the closest attempts appears in his autobiography<sup>3</sup> where he says the main concept is that "it is better to remove a hazard than to keep it under control."

Organisations including US Center for Chemical Process Safety (CCPS), UK Health and Safety Executive (HSE) and the Energy Institute have actively explored the subject with the following common themes:

- risk reduction is an intrinsic part of the process and not an added layer;
- it is permanent and inseparable from the process;
- it should be balanced with other decision-making criteria, especially where there is significant cost or technical risk.

## Relevance to Flixborough

Kletz wrote<sup>4</sup> "Flixborough in 1974 occurred in a plant for the oxidation of cyclohexane with air, at about 150°C and

a gauge pressure of about 10 bar (150 psi), to a mixture of cyclohexanone and cyclohexanol, usually known as KA (ketone/ alcohol) mixture. It is a stage in the manufacture of nylon. The inventory in the plant was large (200 to 500 tonnes has been quoted) because the reaction was slow and the conversion low, the latter being about 6 percent per pass! Much of the inventory was held in six large continuous reactors operated in series, and the rest was held in the equipment for recovering the product and recycling the unconverted raw material."

Based on this explanation, Kletz believed that a more efficient reaction process would have significantly reduced the inventory of hazardous material present on site. Even if a mechanical failure of plant had occurred the consequences would have been much less.

## An alternative description of inherent safety

One of Kletz's skills was his ability to reduce seemingly complicated issues to the simple fundamentals. For inherent safety he proposed the following very simple but effective statements<sup>5</sup>:

- "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 way of preventing a leak of hazardous material is to use so little that it does not matter if it all leaks out, or to use a safer material instead. We cannot always find ways of doing this but once we start looking for them, we find a surprisingly large number.

Whilst hazard elimination will always be the most effective measure, Kletz was very well aware that this was not always possible or desirable. With this in mind, keeping people away from hazardous areas can be very effective at reducing the consequences of accidents that occur.

There is a view that complication is inevitable today. Sometimes it may be, but not always. There are many ways in which plants have been made simpler, and thus cheaper and safer. As with the reduction of stocks, the constraints are often procedural rather than technical. We cannot simplify a design if we wait until it is far advanced; we have to consider alternatives in a structured and systematic way during the early stages of design.

With regards to cost, Kletz was adamant that an inherently safer plant is also cheaper to build, operate and maintain because it can be smaller and use less protective equipment.

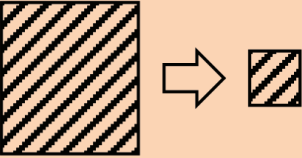
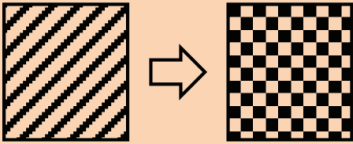
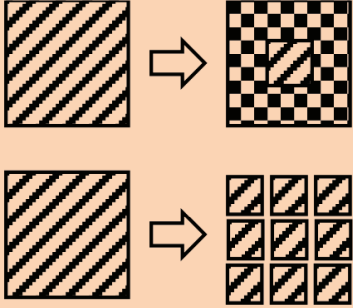
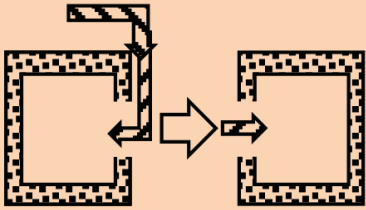
<p><b>Intensification or minimisation</b></p> 	<p>The aim here is to perform the same activity with smaller quantities of hazardous material or performing an activity less often. This can be achieved by selecting different equipment and processes that are more efficient or require smaller hazardous inventories. Switching from batch to flow reactors can significantly reduce inventories.</p>
<p><b>Substitution</b></p> 	<p>The aim here is to reduce the hazard severity by replacing a hazardous substance or a processing route with a less hazardous alternative. Another option is to replace a procedure with one that presents a lesser hazard. Using safer solvents or choosing processes that require less hazardous conditions.</p>
<p><b>Attenuation or moderation</b></p> 	<p>The aim here is to use a substance in a way that reduces its hazardous properties or to use less severe processing conditions. Another way is to store or transport material in a less hazardous form. It can be achieved by controlling operating temperature to below where a runaway reaction can occur and storing materials in less hazardous forms (e.g. paste instead of powder).</p>
<p><b>Simplification</b></p> 	<p>The aim here is to reduce the likelihood of an accident through inherent features of the design. This can involve designing processes, equipment and procedures to eliminate opportunities for failure, including human error; also, designing equipment that cannot be exposed to extreme process conditions by the worst-case processing conditions.</p>

Table 1: A series of images Kletz presented to illustrate the principles of inherent safety<sup>6</sup>.

## Principles of inherent safety

In his workshop notes published by IChemE in 1978, Kletz references Edward de Bono as saying simple pictures can be very powerful at conveying ideas. Images do not have to be accurate or descriptive, but simple enough to lodge in the memory. Above is a series of images Kletz presented to illustrate the principles of inherent safety<sup>6</sup>.

Elimination may be considered the most fundamental principle of inherent safety but did not appear on Kletz's list because he generally saw it as a result of applying inherent safety rather than a principle in itself<sup>2</sup>.

## Applying inherent safety through design

The concept and principles of inherent safety can be applied at all stages of a system's lifecycle. However, the greatest opportunities for risk reduction are found at the earlier stages of development because there are more options to eliminate or significantly reduce hazards by changing the chemical process, fundamental engineering design or plant location. Also, making

these changes earlier is likely to be cheaper and cause fewer knock-on issues.

In the very early stages of a project decisions are made about what to make, by what route and where the facility will be located. Adopting and mandating formal conceptual stage studies can ensure sensible discussions take place so that optimal decisions can be made. Researching all available chemical processes, including low-inventory flow reactions and semi-batch methods, and conducting laboratory and pilot plant experiments should be considered to ensure the safest chemical process is selected. Also, it sets the scene for the remainder of the project.

During Front End Engineering Design (FEED) or Define phase, when a flowsheet that identifies the main sub-systems has been developed, the following can be used as a prompt<sup>7</sup>:

- materials — develop an inventory, identify their hazards and consider options to remove or reduce;
- reaction — size of reactors and opportunities to reduce; process conditions and opportunities to make less severe;

and any potential for runaway reaction;

- separation — inventory of material in separators and opportunities to reduce;
- heat transfer — inventory of material in exchangers and opportunities to reduce; use of less hazardous heat transfer medium; ensuring the most hazardous material is in the safest part of the exchanger (e.g. in tubes not shell);
- storage — factors defining storage requirements and options that would reduce these; storage process conditions and options to make less hazardous;
- equipment types — options to use simpler alternatives;
- human error — options to reduce susceptibility that do not involve additional safety systems.

Although it may become more difficult, it is still important to continue looking for options to increase inherent safety as the detailed design is developed. Examples include eliminating or minimising the stored inventory of hazardous materials, substituting a more corrosion resistant material of construction for equipment, minimising potential hazardous impact by locating access routes and roads away from potentially hazardous areas, locating emergency equipment such as fire water pumps and switch gear for emergency equipment away from the main plant which it is designed to protect, and designing the equipment arrangement in well vented and open process areas to prevent accumulation of hydrocarbon if released.

## Applying inherent safety during operations and maintenance

Whilst inherent safety is a critical design issue there can be many opportunities to use the same principles during the operational stage of a system. Whilst it should be a continual goal, there will be specific times when it should be considered formally including identifying actions following an incident investigation or when evaluating a plant or process change.

Although options to follow an inherently safer approach should always be considered, application to a system that has already been designed and built is not straight forward and can often lead to unintended consequences.

Managing inventories is one option. Just because a tank or vessel can hold a quantity of material, it does not always need to be filled to capacity. Reducing inventories to only what is needed will reduce the potential consequences of failure. On the other hand, reduced inventories will inevitably mean that materials need to be handled more often (e.g. smaller deliveries carried out more often). The risk of additional handling needs to be considered against the reduction of risk through reduced inventory.

It is standard practice to isolate, drain, clean and purge process equipment before maintenance. But decisions can be made about how much plant needs to be prepared in this way. The inherently safer approach is to shut down and prepare the whole facility because this will minimise the inventory of material present whilst the maintenance is being carried out and also reduces the potential consequence of maintenance errors (e.g. someone breaking the wrong pipework joint). However, it can have significant impact on production. Also, preparing plant and equipment for maintenance; and returning it to service after

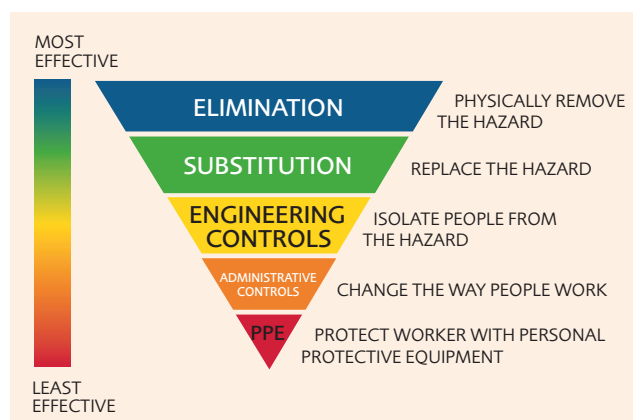


Figure 1 - Hierarchy of Risk Controls

maintenance carries its own risk and so a balanced approach has to be taken.

Another decision to make when carrying out maintenance is the type of isolation to be used. The inherently safer option is to use positive isolation, with removal of spool pieces being the most robust option because the alternative methods (e.g. spades, blind flanges) are easier to defeat. However, all forms of positive isolation involve breaking joints and so introduce their own risks.

Whilst hazard is present there is always some risk. But certain operations such as plant start-up and shutdown are known to be more hazardous. In these cases, the concept of "people who are not there can't be killed" can be applied by clearing sites during the most hazardous operations, or at least limiting them to essential personnel only. Other hazardous operations where this applies include tanker deliveries of hazardous material, opening pig receivers/launchers, sampling and any activity involving a break of containment, such as filter changing.

## Hierarchy of risk controls

The goal of inherent safety is to avoid reliance on added safety systems as it is recognised that these can never be fully effective. The hierarchy of risk controls highlights that the options available to control residual risks are not all equally effective or reliable<sup>8</sup>.

It is possible to argue that inherent safety results in hazard avoidance and so it not technically a control. However, pragmatically it is clear that it is part of the overall management of risks and excluding it in order to make clear-cut distinctions is neither necessary nor helpful.

The concept of the hierarchy of risk control illustrates that the effectiveness of controls depends on their characteristics. As a general philosophy controls at the top of the hierarchy should always be considered first because they are most reliable. But the overall solution is likely to involve controls at all levels of the hierarchy.

## ALARP

The acronym ALARP is now widely used and stands for "As Low As Reasonably Practicable." In a safety context it is used when discussing whether a risk is ALARP or further action is required to reduce it.

ALARP is generally applicable in 'goal-setting' regulatory

systems where it is the duty holder's responsibility to demonstrate that they are managing their risks rather than prescriptive 'rule-setting' systems where the regulator has a greater role in saying how risks shall be managed. Other countries including the US have avoided adoption of the ALARP principle. One of the reasons is that it is difficult to define what is considered as reasonably practicable for a given circumstance.

The UK's HSE provides guidance on how to apply ALARP in practice. Cost benefit analysis may be one approach but can be complicated and relies on quantified data that may not be readily available in any useful form<sup>2</sup>.

Guidance for permissioning within the Control of Major Accident Hazards (COMAH) regulations states that "ALARP demonstration for individual risks is essentially a simple concept which can be satisfied by the operator answering the following fundamental questions"<sup>9</sup>.

1. What more can I do to reduce the risks?
2. Why have I not done it?

Answers to the first question are qualitative in nature and involve looking systematically at the risks and drawing up, in a proportionate way, a list of measures which could be implemented to reduce those risks.

The answer to the second question may be qualitative or quantitative in nature depending on the predicted level of risk prior to the implementation of those identified further measures. The guidance states that if "it cannot be shown that the cost of the measure is grossly disproportionate to the benefit to be gained, then the operator is duty bound to implement that measure"<sup>9</sup>. However, there are often reasons to not implement additional measures that are not purely due to financial cost. Risk transferral is very often a factor where a measure to reduce one risk increases another.

In some cases, ALARP can mean that an inherently safer solution is not safer overall. 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. The alternative may apply lower safety standards. Also, risks of transport will have increased. In this case the issue may be moral rather than economic, and there may be an argument to say that such global issues are not necessarily the responsibility of commercial organisations. However, with increased scrutiny from customers of the supply chains of their suppliers it is possible that keeping production local may be the best solution from all perspectives.

## Conclusion

There have been many publications since the Flixborough disaster encouraging us to adopt inherent safety, with very little (if any) dissent. Similarly, the hierarchy of risk controls is well established and accepted. However, Safety Instrumented Systems (SIS) have proliferated, which are clearly an add-on safety device rather than an inherently safe solution. Instead of eliminating hazards they can be used to allow more hazardous processes to take place, whilst also increasing overall complexity.

There have been plenty of accidents since Flixborough that would have been avoided or far less serious if inherent safety had been adopted more widely. At Bhopal the methyl isocyanate that leaked was only an intermediate that was stored

for convenience rather than necessity (what you don't have can't leak). At BP Texas City, most of the 15 people who died were in a temporary building that could have been located in a far safer place on the site (people who are not there can't be killed). At Esso Longford the heat exchanger that failed had not been designed to withstand the low temperatures possible under abnormal or fault conditions (the more complicated a system becomes, the more opportunities there are for equipment failure and human error).

Controlling risk is not simple. Opportunities for reduction should always be looked for, whilst being aware of unintended consequences. Whilst it may be easier at the early stages of a design project, the principles of inherent safety can be applied at any time. When contemplating a task everyone involved should be asking themselves whether all reasonably practicable steps have been taken to remove hazards, if people who do not need to be present have been kept away and if arrangements are as simple as they could be.

An inherently safer solution may not actually create the lowest overall risk. Applying the hierarchy of risk controls is not a case of selecting which control to apply but can provide a structured way of evaluating the potential strengths and weaknesses of different options. Ultimately the aim is to achieve risks that are ALARP, which requires you to continually consider what more can be done to reduce risk and demonstrate that doing more is not beneficial.

All this is taking place in a global context. We may feel that our responsibility is to the safety of our colleagues, neighbours and local environment; and that decisions we make that may affect risk in another part of the world are not our concern. But morally we all have to be aware of how the decisions we make affect others. The message for industry is that it should "export inherent safety not risk."<sup>10</sup>

## References

1. *The Flixborough Disaster. Report of the Court of Inquiry. Department of Employment (1975)*
2. Brazier, A. Edwards, D. Macleod, F. Skinner, C. Vince, I. *Trevor Kletz Compendium. Elsevier (2021)*
3. T. Kletz, *By accident ... a life preventing them in industry*, PFV Publications (2000).
4. T. Kletz, *Plant Design for Safety - a user friendly approach*, Hemisphere Publishing Corporation (1991)
5. T. Kletz, *Lessons from Disaster*, Institute of Chemical Engineers (2003).
6. T. Kletz, *Cheaper, Safer Plants or Wealth and Safety at Work (Notes on Inherently Safety and Simpler Plants)*, The Institution of Chemical Engineers (1984)
7. T. Kletz, P. Amyotte, *Process Plant, A Handbook for Inherently Safer Design*, 2<sup>nd</sup> Edition, Taylor & Francis (2010).
8. A. Brazier, N. Wise. *Making Sure Risks are ALARP. The Chemical Engineer (2021)*
9. *Health and Safety Executive HID C15A. Guidance on ALARP Decisions in COMAH. SPC/Permissioning/37. Version 3*, [http://www.hse.gov.uk/foi/internalops/hid\\_circs/permissioning/spc\\_perm\\_37/](http://www.hse.gov.uk/foi/internalops/hid_circs/permissioning/spc_perm_37/) (Accessed March 2024)
10. D. Edwards, *Export inherent safety - not risk*, Loss Prevention Bulletin 240 (2014).