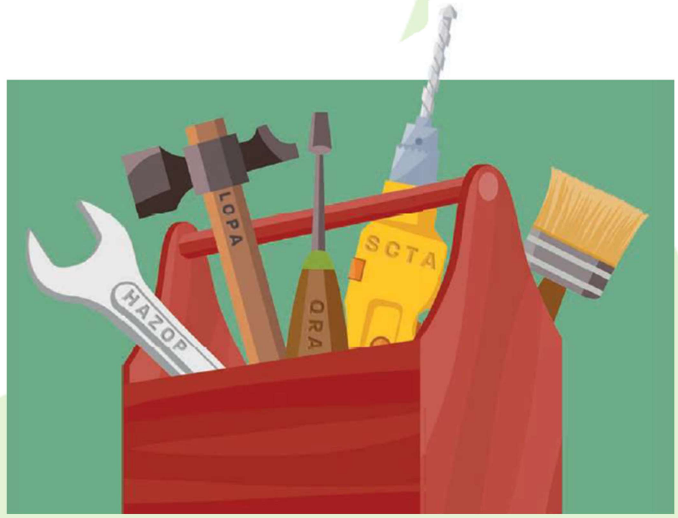
Having spent 30 years in the process safety industry I have realized that we are generally very good at using tools. We also say we like some of the higher level concepts, but generally fail to apply them. I think most people agree with the underlying message behind the hierarchy of control but I see fairly patchy application in practice. I wondered if developing a more detailed hierarchy could lead to a useful tool.

- Safeguards
- Layers of protection
- Barriers



AB Risk
Limited

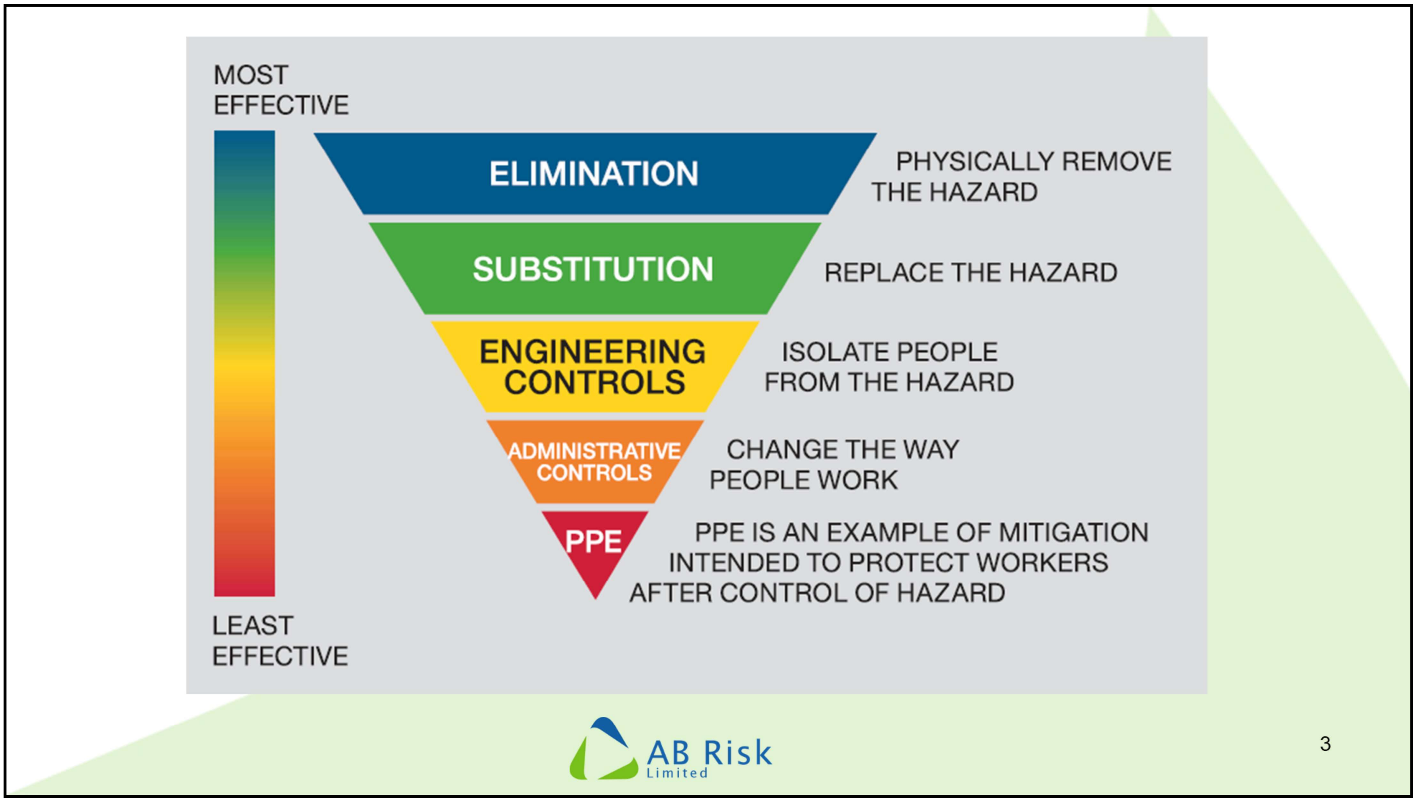
We have a range of tools available. This is useful because it allows us to look at issues from different perspectives. It can be a bit tricky because each tool uses its own terminology.

HAZOP refers to safeguards

LOPA refers to layers of protection

Bow ties refer to barriers.

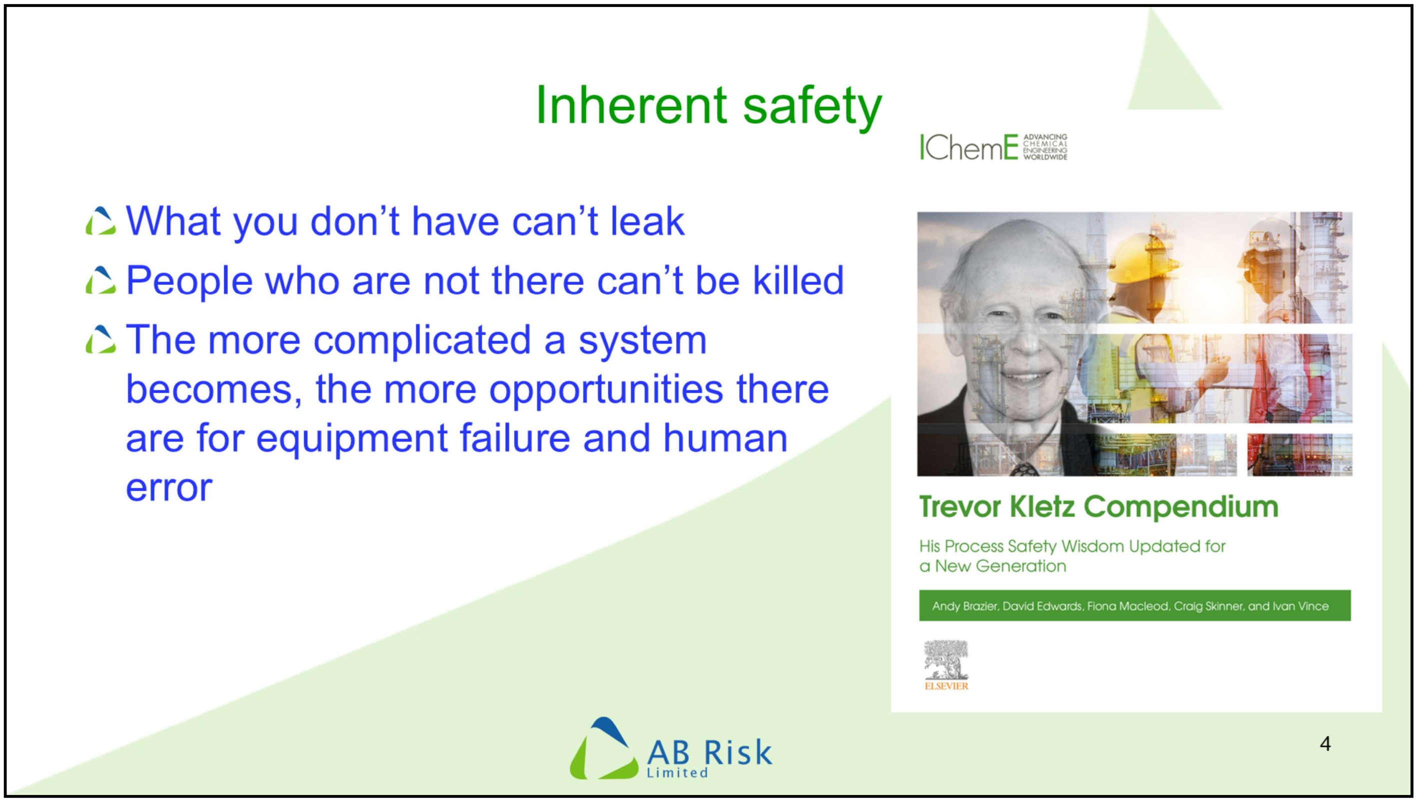
In general terms these are all risk controls and we probably use some of the terminology interchangeably. But each tool has its own rules about what can be counted as a control and ultimately we need a way of creating an overall view.



Here is an example of a typical representation of the hierarchy of risk control. I think we all buy into the general idea but closer scrutiny suggest a few problems. The triangle implies there are two dimensions to the relationship when in fact there is only one, effectiveness.

It implies that selecting a higher control means we don't need any lower ones. But all controls have positive and negative aspects, and we usually need several controls.

The inclusion of PPE at the bottom suggests the main concern is personal safety. It could be used as an example of mitigation, but in that case there are a number of different mitigation controls that can be used, including engineered and administrative.



Another concept that we have all accepted but has failed to have the impact I think it should have is inherent safety. I am not aware of any tools that deal with it directly and attempts to define it have tended to cause more confusion.

Of course Trevor Kletz was an early proponent and in his typical style he had a very neat way of explaining the principles.

The first one is used fairly frequently.

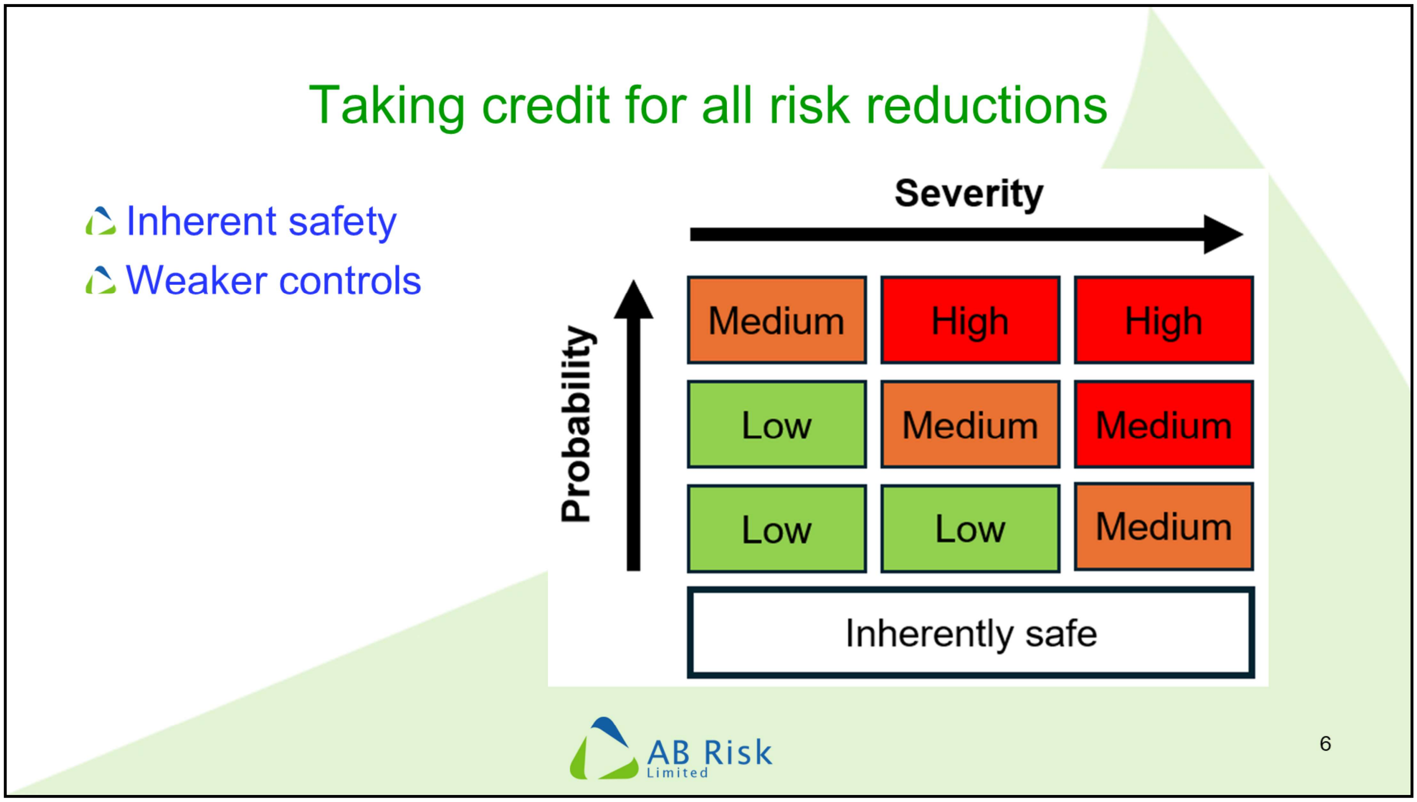
The other two maybe less so. I certainly see a need for simplicity to be an aim in managing risks, and add-on safety features add a lot of complecxity.

ALARP is simple

- Question 1 – What more can I do to reduce risks?
- Question 2 – Why have I not done it?

AB Risk Limited

Although ALARP is another concept, the requirement to reduce risks to as low as reasonably practicable is a legal requirement in some countries and a moral requirement for anything that has the potential to cause a major accident. Unfortunately some guidance regarding ALARP makes it seem complicated whereas in fact it really is simple. You just have to ask yourself what more you can do to reduce risks and then be prepared to explain why you have not done those things. Note the use of ‘I’ in these questions, directly from HSE guidance. I believe this was done to highlight how risk management is a personal judgement and not the result of some calculation or other evaluation.



So to demonstrate risks are ALARP we need to be able to demonstrate what we have done. I think one of the reasons that inherent safety does not always get the attention it should is that once applied the need to control risk has been drastically reduced. In many ways it is easier to appear good by taking an inherently hazardous system and then shown how effective add on controls can be. I wonder if adding a new region to the ubiquitous risk assessment matrix could help.

Similarly, there is a tendency to exclude the influence of weaker controls, particularly administrative, because they do not move the risk to a new region. But I feel that many of them make more of a contribution in the real world than some of the supposedly stronger engineered controls and the underlying issue is the availability of reliability data.

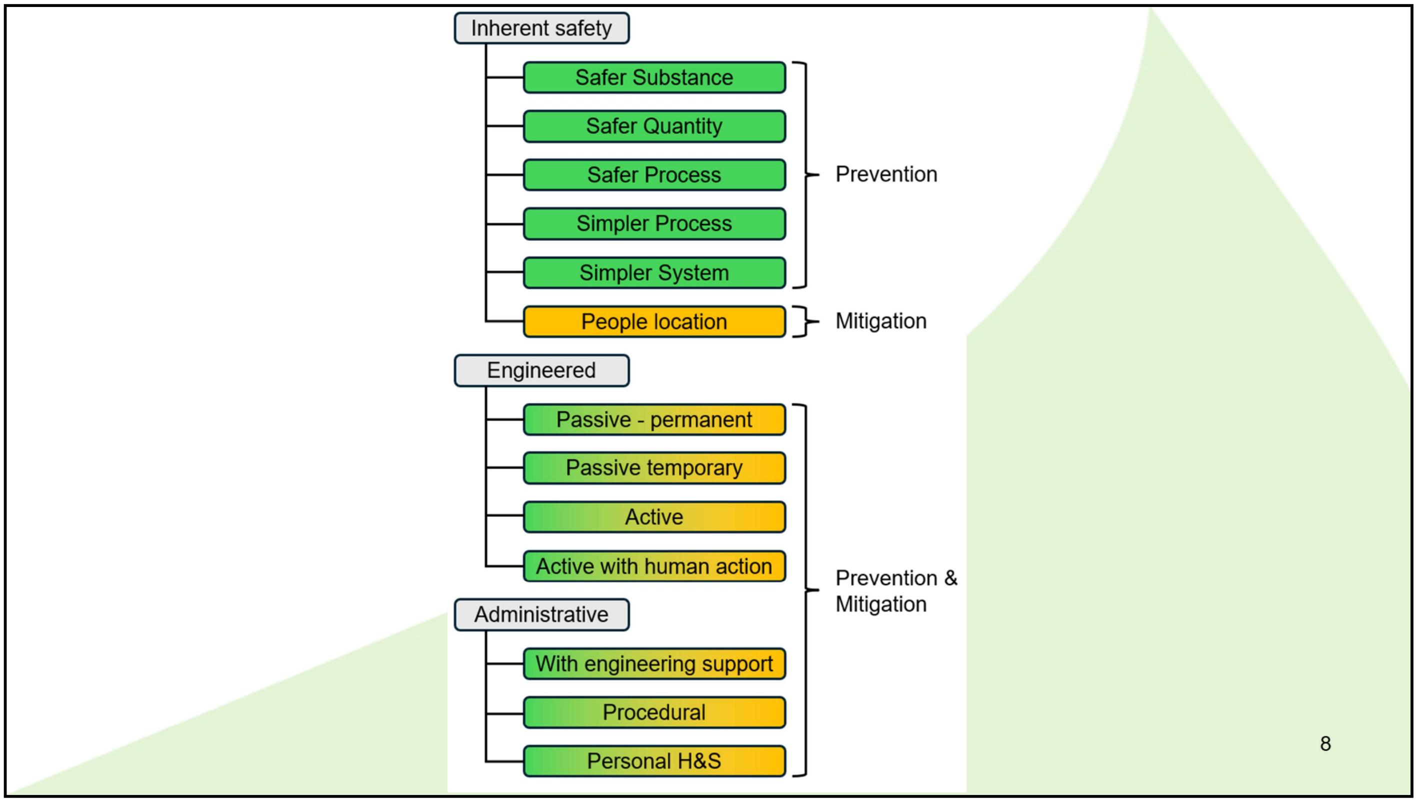
Control components

- Fitts list (1951)
  - Machines are good at speed, repeatability & simultaneous operation.
  - People are better at detecting, perception, using judgement & improvisation
- Physical items - hardware
- Logic and programmes - software
- Actions of people – wetware

AB Risk Limited

Another issue I observe regularly is the view that engineered controls are better than controls that rely on human actions. The explanation seems to be that people make mistakes and so are unreliable. But this seems unfair to me because human reliability is being measured using metrics suitable for machines. Paul Fitts pointed out in 1951 that this is not the case, and there are plenty of things where human excel and as far as I can see this is still the case now despite significant developments in technology.

And this is where the current blunt instrument style hierarchy of control falls down. If we breakdown each control type into hardware, software and wetware we immediately see that engineered controls inevitably rely on human actions for at least maintenance, inspection and testing. The engineered is good and human is bad approach hides this fact.



So here is what I have come up with so far. These are headings and I have been able to list examples under each, and I am comfortable that at all levels the hierarchy stacks up fairly well.

The colour code here is that green is a prevention control and orange mitigation. I concluded that there are engineered and administrative controls for both. However, the top fine inherent safety controls related to substance and simplicity are preventative and the sixth related to people location is mitigation.

Type	Examples - preventative	Hardware Control	Software Control	Wetware Control	Be aware of
Inherently safer substance	Low hazard substances	None	None	None	Risk transferred to suppliers.
	Naturally low concentration of hazardous substance.	None	None	None	May require greater volume. Natural variation in concentration affecting hazard and process stability.
	Stable form (e.g. solid not gas)	None	None	None	Risks of state changes.
	Naturally conspicuous hazard (odour, visible, detectable)	None	None	None	People or equipment need to be present to detect.
Inherently safer quantity	Small fixed volume of hazard. Tanks, vessels, pipework (length/diameter)	None	None	None	Excludes managed inventory (administrative control). May require higher concentration or greater pressure process.
Inherently safer process	Process sub-steps eliminated	None	None	None	Risk transferred to suppliers. Transport risks.
	Pressure / temperature near ambient at source (i.e. not achieved by a control system)	None	None	None	May require greater volume. Reduced conspicuousy of releases. Difficult to cross check instrumentation when at ambient.
Inherently simple process	Parameter changes have few and predictable outcomes	None	None	None	Less efficient process may require additional plant.

AB Risk Limited

As an example of the more detailed view here are the preventative inherent safety controls. You will see that hardware, software and wetware do not apply because the function is intrinsic to the system and not an add on. Also, you will see that even inherent safety can create issues. Identifying them here will be an important part of an ALARP demonstration when explaining why those options have not been selected.

Type	Examples - mitigation	Hardware Control	Software Control	Wetware Control	Be aware of
Inherently safer location for people	People located outside of the hazardous zone	None	None	None	Unlikely to apply to all people at all times. Will restrict operations.
	Natural, permanent obstacle between hazard and people.	None	None	None	Rarely a realistic option
	Natural ventilation prevents hazardous concentrations forming	None	None	None	Affected by weather conditions
	Remotely operated or autonomous mechanised devices (robots in hazardous area)	None	None	None	Need to be installed and removed for MIT. Will restrict operations.
Passive engineered item - permanently in place	Created permanent obstacle between hazard and people.	Structural materials	None	MIT	Unlikely to apply to all people at all times. Will restrict operations.
	Secondary containment with no breaches (double walled tanks)	Containment device	None	MIT	Failure of primary containment creates hazard to be removed from secondary. May restrict access to primary containment for MIT.
	Tertiary containment with no breaches (bunds, dykes)	Containment device	None	MIT	Failure of primary / secondary containment creates hazard invicinity of teriary and has to be removed. May restrict operations.
	Permanently installed passive fire protection	PFP	None	MIT	Restricts access to structure for MIT

AB Risk Limited

Similarly here is the inherent safety and passive engineered controls for mitigation. You will see that engineered controls all have a hardware and wetware component. As I mention earlier Maintenance, Inspection and Testing or MIT is a critical requirements. Again, you can see how I have captured potential issues with each example.

	Propane Storage - prevention						
Type	**Status**	Implemented - fully	Implemented - partially	Not possible / required	Rejected - risk based	Rejected - other (cost)	**Explanation**
Inherently safer substance	Rejected - other (cost)						Diesel could be used as fuel on site but cost is greater. Propane has better environmental performance.
Inherently safer quantity	Rejected - risk based						Smaller storage vessel would require more frequent deliveries.
Inherently safer process	Not possible / required						Storage conditions dictated by the substance.
Inherently simpler process	Not possible / required						Storage conditions dictated by the substance.
Inherently simpler system	Implemented - fully						Design philosophy to minimise reliance on add-on safety systems
Passive engineered item - permanent	Implemented - fully						Vessel and components fully rated for full pressure / temperature range
Passive engineered item - temporary	Not possible / required						Eclipsed by permanent arrangements

AB Risk Limited

11

The way I see this working is to determine the status for each of the controls on the hierarchy. In this example for a propane storage vessel the prevention controls may be arranged like this.

A safer substance could be used like diesel but rejected due to cost or environmental impact. This would create a higher reliance on controls further down the hierarchy and require justification.

Reducing the size of the vessel would reduce the potential consequences of a release but a risk based argument may be made that the additional deliveries required would create a higher risk.

We may conclude that the chosen design is as simple as it could be and we would want to take credit for that. Also, we would want to be able to say that the passive engineered aspects are as good as they could be because the vessel and components are rated for all potential conditions.

The final item on the list is temporary passive items like hoses. This is not an issue here but in other cases, including the propane delivery facility it may be necessary to demonstrate an appropriate solution has been selected. In this case it has been eclipsed because the storage facility uses permanent components only.

Type	Examples - preventative	Hardware Control	Software Control	Wetware Control	Be aware of
Inherently simpler system	Minimum of add on control /safety devices	None	None	None	May create higher reliance on human monitoring and response.
Passive engineered item - permanent	Pressure envelope rated for the full range of operating conditions possible - without joints.	Plant materials	None	MIT	Reduced options for positive isolation. Higher risks for maintenance and inspection.
	Pressure envelope rated for the full range of operating conditions possible - with joints.	Plant materials Joint design	Joint specifications	MIT Make / break joints	Joints considered to be potential leak points. Potential for material changes (pipework, gasket).

Whilst making an evaluation we would be referring to the detailed table. Looking at the passive engineered controls I realised that fully welded pipework is often viewed as safer than jointed, but it actually introduces some potentially significant issues of the like time of the plant. I concluded that fully welded should appear higher on the hierarchy, but that jointed would be adjacent. One thing I was clear about was that fully welded pipework cannot be considered as inherent safe because it relies on hardware and wetware.

Where we have made a claim that a control has been fully or partially implemented we would have to be sure that the hardware, software and wetware elements are properly managed.

Type	Status	Implemented - fully	Implemented - partially	Not possible / required	Rejected - risk based	Rejected - other (cost)	Explanation
Propane Storage - prevention							
Active engineered	Rejected - risk based				■		SIS has been rejected to avoid complexity. Risk reduction was not sufficient to justify.
Active engineered with human action	Not possible / required			■			None identified.
Administrative control with engineered support	Implemented - partially		■				Ullage valve provided to allow operator to determine when vessel is full. Indication only - does not prevent overfill.
Administrative control	Implemented - fully	■					Full set of operating and maintenance procedures in place for propane storage. SCTA carried out for most critical.
Personal health and safety control	Not possible / required			■			None applicable to prevention.

AB Risk Limited

Looking at the remainder of the prevention controls you can see that active engineered controls have been rejected due to risk based decision. In this case the simplicity is considered more effective, baked up by it being near the top of the hierarchy.

The administrative control with engineered support refers to an ullage valve. This is a very small vent at the maximum fill point that is opened to check when liquid reaches that point. It is only a partial control because it helps the operator to prevent overfill but does not prevent it necessarily.

Propane Storage - mitigation

Type	Status	Implemented - fully	Implemented - partially	Not possible / required	Rejected - risk based	Rejected - other (cost)	Explanation
Inherently safer location for people	Implemented - fully						Storage tank in remote part of site
Passive engineered item - permanently in place	Not possible / required						No options for secondary containment for propane
Passive engineered item - temporary	Not possible / required						No options for secondary containment for propane
Active engineered item	Implemented - fully						Automated water deluge activated by fire / gas detection
Active engineered item with human action	Not possible / required						Eclipsed by automated deluge
Administrative control with engineered support	Implemented - fully						Evacuation alarm activated manually will direct people to a safe location
Administrative control	Implemented - partially						General site emergency procedures in place. Propane storage scenarios need to be developed further.
Personal health and safety control	Implemented - fully						Personnel issued with PPE suitable for Propane contact / exposure

AB Risk Limited

If we look at the mitigation controls the profile here seems to be well balanced and no options rejected. I have identified under administrative controls that there may be further work to do with emergency procedures for specific propane storage scenario.

- https://abrisk.co.uk/wp-content/uploads/2024/09/ABRisk-Expanded-Hierarchy-of-Risk-Control.xlsx

AB Risk Limited

If you are interested I have added an Excel spreadsheet with the full hierarchy for download on my website at this address.

Looking back at how the hierarchy of risk control is commonly presented scale is usually effectiveness. This may be appropriate when presented at such a high level, but as I said earlier I do not believe that engineered controls are always better than administrative.

If you look at the more detailed level there is a hierarchy within engineered controls with passive above active. But take this simple example. It is law in the UK to supply bikes with a rear reflector. This is a passive device. But in most regards an active device as simple as an old school battery and bulb will be more visible. And modern LED devices with flash modes are even more visible. I don't think it is positions on the hierarchy that are wrong but I suggest the scale could be availability instead of effectiveness. An inherently safe solution is always available because it is integral in its design. Passive engineered devices should be available most of the time because they don’t need power or control, but they do degrade and need maintenance. Active devices have more failure modes and need more maintenance.

My final observation is the illustration on the right. Why are cyclists not all using the very sophisticated laser displays that are readily available? They are expensive, but they also add some considerable complexity where a simpler solution of an LED light is probably good enough.

- If you would like any more information you can contact me as follows:
  - Email – andy@abrisk.co.uk
  - Phone – +44 7984 284642

AB Risk Limited

I hope you have found this useful and thank you for your interest. If you have any questions do not hesitate to contact me.

Type	Examples - preventative	Hardware Control	Software Control	Wetware Control	Be aware of
Administrative control	High performance HMI for operator situational awareness	Control system design	HMI design	Situation detection, diagnosis and response	Relies on equipment and human reliability.
	Created low concentration of hazardous substance.	None	Operating limits	Quality control	Human error creates hazard.
	Created conspicuous hazard (odour, visible, noise)	None	Operating limits	Quality control	Human error creates hazard.
	Hazard segregation	None	Segregtion rules	Establish and maintain segregation	Human error creates hazard. May restrict operations.
	Defined operating limits (tank level, operating temperature / pressure).	None	Operating limits	Monitor and respond to keep in limits	Human error creates hazard. May restrict operations.
	Control of work procedure (permit to work)	None	Control of work rules	Review, approve and implement work.	Relies on human compliance. May restrict operations.
	Safety critical operating / maintenance procedure	None	Procedure use rules. Procedure template	Develop and implement procedure	Relies on human compliance. May restrict operations.
	Plant patol with effective checklist	None	Checklist content	Frequency of patrol and quality of checking	It is not the checking but the ability to detect, diagnose and respond to what is found.
	Competence management system	None	Competence management system	Define, implement and confirm competence requirements	Competence levels vary and degrade. Relies on human compliance.

Type	Examples - mitigation	Hardware Control	Software Control	Wetware Control	Be aware of
Administrative control	Emergency response procedures	None	None	Procedures	Relies on human compliance.
	Emergency response practice (emergency exercises, desk top scenarios)	None	None	Procedures	Relies on human compliance.
	Emergency response training (class room)	None	None	Procedures	Relies on human compliance.
	Reduced occupancy	None	Occupancy rules	Implement occupancy rules	Relies on human compliance.
Personal health and safety control	Collective PPE (safety net)	PPE design	Selection methods	MIT	May not cover all scenarios. May restrict operations.
	PPE used routinely (safety glasses)	PPE design	Site rules. Control of work.	Site rules. Control of work procedures	Relies on human compliance.
	PPE used during emergency (escape BA)	PPE design	Emergency response.	Emergency response procedures	Relies on human compliance.

AB Risk
Limited