Safety practice

Buncefield failures aligned to the hierarchy of risk control

Andy Brazier, AB Risk Ltd, UK

Summary

This paper analyses the Buncefield explosion through an expanded hierarchy of risk control, emphasising that major accidents result from multiple failures rather than isolated errors. It categorises prevention and mitigation measures, highlighting inherent safety principles, engineered controls, and administrative practices. The study identifies deficiencies in design, maintenance, communication, and emergency planning that contributed to the incident, offering lessons for improving reliability, reducing complexity, and ensuring risks remain as low as reasonably practicable (ALARP).

Keywords: Buncefield, risk control, inherent safety, prevention, mitigation

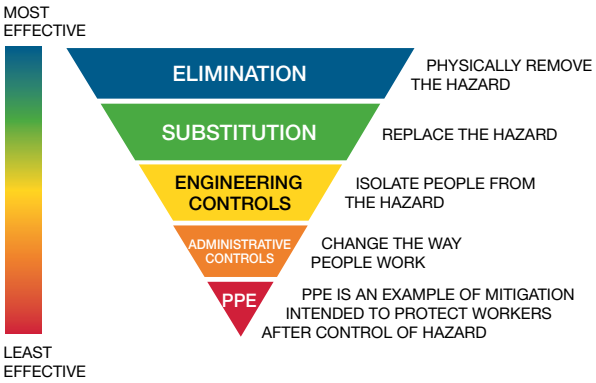

Figure 1 - Typical illustration of the hierarchy of risk control[2]

Introduction

The Buncefield explosion, like all major accidents, was not the result of a single failure. A combination of circumstances came together, leading to storage Tank 912 being overfilled with gasoline. A significant loss of containment created a flammable vapour cloud that found an ignition source beyond the depot boundary.

It is easy to focus on individual failures in the chain of events leading to an accident. At Buncefield, for instance, a faulty level switch meant an alarm did not sound and the automated pipeline shutdown did not function when the tank was overfilled. However, this does not explain why the tank was allowed to reach an overfilled state in the first place. Also, no risk control is ever completely reliable, so occasional failures must be anticipated.

The basis of safety for any hazardous operation should include multiple features that work together to reduce the risk to as low as reasonably practicable (ALARP). The hierarchy of risk controls as shown in Figure 1, identifies different options for controlling risk and indicates that some may be more effective than others[1].

The underlying principles of the hierarchy are well regarded but, in this form, the broad categories defined do not lend themselves to any detailed explanation of how features of a system work together to ensure safety or how failure results in accidents. However, developing it into a more detailed set of risk control types may make it a useful tool[3].

An example of an expanded hierarchy is shown in Attachment 1. It was developed by subdividing the existing categories and integrating concepts of inherent safety and identifying that some controls can be effective for both prevention and mitigation[3].

Prevention controls applicable to the Buncefield accident

Prevention risk controls should ensure a process stays within its safe limits and hazardous scenarios are avoided. For Buncefield, if Tank 912 had not been overfilled there would have been no release of gasoline and the accident would not have occurred.

This section summarises the prevention controls identified in the expanded hierarchy of risk control (see attachment A) when applied to Buncefield depot operations. In some cases, the control was in place and effective. However, in other cases there were deficiencies that allowed the accident to occur. This hindsight view of a past event may provide some foresight to allow others to avoid similar occurrences.

Inherently safer substance – without a hazard there is no risk. The sole purpose of the Buncefield depot was to store hydrocarbon fuels (gasoline, diesel and aviation fuel). Changing the substances would fundamentally change the business and would require customers to find alternative sources. Flammability was the main hazard of the substances being handled. It was beneficial that the Buncefield terminal was not handling substances with other hazards (e.g. toxic, corrosive, reactive).

Inherently safer quantities – a reduced hazard creates less risk. This would have required reducing the number and/or reducing the size of tanks at Buncefield. Managing

0260-9576/25/$17.63 + 0.00

Figure 2 – Pipeline network connecting Buncefield to refineries[4]

inventories without changing the tanks would be viewed as an administrative control, which appears lower in the hierarchy because the inherent storage capacity is not affected. Whilst the total inventory of the depot affected the duration of the subsequent fire and associated environmental impacts, the original release was determined by the flow rate from the pipeline and not the capacity of Tank 912. There is an argument to say that fewer and smaller tanks would increase the likelihood of overfill.

Inherently safer process – operating at ambient conditions minimises the energy to drive hazardous events. The Buncefield depot processes may be considered inherently safer than a system operated at high pressure or temperature, because the substances were stored at ambient conditions. However, the pipelines were at elevated pressures to create required flow rates. It may have been possible to reduce the pressures by adding intermediate pumping stations along the length of the pipeline. For risks to be ALARP the risk reduction from reducing pressure would have to be greater than the risk increased from introducing these extra pumping stations.

Inherently simple process – having few interconnected parts makes it easier to understand and predict how a process will perform. Buncefield was connected to three refineries by two pipelines (see Figure 2). The Finaline pipeline was a direct connection to the Lindsey and may have been considered inherently simple. However, the Thames-Mersey pipeline had several branches, connecting different sites and so was more complex.

The depot was divided into six sites based on ownership (see Figure 3). This introduced complexity for the human operators, which should have been recognised as a contributor to risk.

Using direct pipelines (like the Finaline) and operating the depot as a single site would have reduced complexity but may not have been commercially viable.

Inherently simple system – having few control and safety devices makes it easier to understand how it will react to situations. At the Buncefield depot the main control and safety concerns were tank level. The system may have been considered inherently simple.

Passive engineering (permanent) – suitability of the plant and equipment to contain the hazard. The leak at Buncefield was not the result of any plant or equipment, which was all fully rated for the full range of operating conditions. However, there was an inherent risk because the capacity of the tanks receiving product was limited whilst the pipelines supplying was essentially unlimited. Larger tanks may have reduced, but not eliminated, the potential for overfill. Supplying the depot from road or rail tankers would significantly reduce the likelihood and size of any potential spill but would introduce additional risks of transportation. Also, it would have had a significant environmental impact that had to be considered as part of the cost of changing arrangements when deciding if the risk is ALARP.

Passive engineering (temporary) – physical devices used to physically contain the hazard that are not always present. Valves were used to direct products to the correct tanks. On the day of the accident the quantity of product being delivered required the receiving tanks to be swapped by changing valve configuration. There were no technical failures of the valves and the overfill occurred because valve operations did not take place when required.

Active engineered controls – devices that operate automatically to prevent a hazard from creating a significant consequence. At Buncefield each tank had a high-level trip

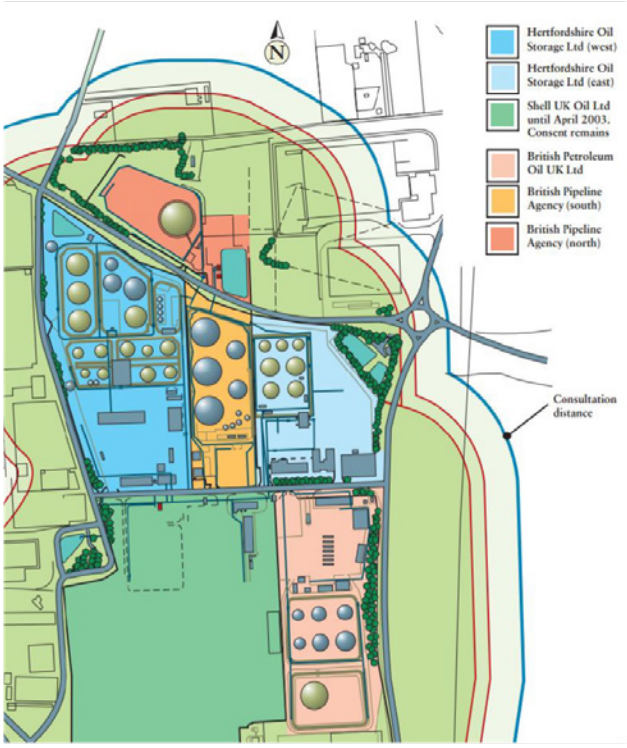

Figure 3 – Buncefield depot divided into multiple sites[4]

0260-9576/25/$17.63 + 0.00

installed that would stop flow from pipelines when activated. Errors made during the maintenance of the associated level switch on Tank 912 meant the trip was not initiated. Flow from the pipeline continued until gasoline was released from the tank's overflow.

Active engineered with human action – an engineered control that relies on human actions. Highly Managed Alarms (HMA) may have been identified as an option at Buncefield. They are differentiated from 'normal' alarms and other administrative controls because they require a much more detailed assessment of system reliability taking into account the role of the human operator[3]. No HMA were present at Buncefield because the existing controls were considered sufficient. This is consistent with standards and guidance[5] that specify that HMA should be avoided wherever possible because automating critical actions with reliable systems is preferred to relying on a human response.

Administrative control with engineered support – humans keeping processes within safe parameters using data and controls provided by engineered systems. Flow and pressure of pipelines feeding Buncefield were controlled, but there was no feedback of tank level to the control system. Depot operators were required to monitor tank levels and react when required. However, there were many tanks but, whilst the control system graphics allowed all to be viewed, it did not provide an easy way of seeing them all at the same time. Operators had to select tanks to monitor. At the time of the accident, they were not aware that Tank 912 was being filled and so were not looking at the graphic that showed its level. The tank had a level gauge, but this was known to stick. Also, a high-level alarm that would have notified them of the overfill, but the error made when maintaining its level switch (see above) meant that this did not activate.

Administrative control – competent people performing tasks to keep the process within safe parameters. Operating procedures at the depot defined operating limits, including tank maximum fill levels, and configurations for import and export of product. These were well known and understood by the operators and the overfill was not the result of any deliberate deviation from safe working practices. However, procedures were focussed on individual operations and did not account for multiple operations being performed in parallel or make allowances for inherent complexities in arrangements (see above). Communication failures at shift handover meant the duty operators were confused about which tanks were being filled and meant that they were not monitoring Tank 912. Communication with the refinery and pipeline operators supplying the depot did not address these issues.

Personal health and safety control – minimising harm to personnel. The health and wellbeing of personnel working at Buncefield made no direct contribution to the accident.

Mitigation controls applicable to the Buncefield accident

Mitigation risk controls take effect after a hazardous scenario has occurred and are intended to minimise the consequences. For Buncefield, mitigation should have occurred immediately after Tank 912 was overfilled and escalated as soon as it started to overflow. The aim would have been to minimise the size of release and contain spilt product in a safe form.

This section summarises the mitigation controls identified in the expanded hierarchy of risk control (see attachment A) when applied to Buncefield depot operations.

Inherently safer location for people – knowing the hazardous extent of potential scenarios when deciding where people may work or live safely. The occupancy of the depot was normally low. However, the accident caused significant offsite damage to buildings that would have been occupied had it been a working day. Because tanks and pipework were located in open air it may have been assumed that an explosion like the one occurred was not possible. One learning was that features such as walls and hedges can influence the spread and overpressure a flame front, significantly increasing blast pressure.

Passive engineered item (permanent) – physical items that contain a hazard after initial control has been lost. All tanks at Buncefield were bunded to prevent spilt liquid from spreading. They were effective before the explosion, although subsequent damage contributed to the fire and associated environmental impact. However, another passive element of design was the roof vent on Tank 912. This was point where containment was lost. The arrangement of the vent led to the gasoline being vaporised and mixed with air to form a large, flammable cloud that was able to find an ignition source a significant distance from the tank.

Passive engineered item (temporary) – physical items that are not always present or have features that mean they are not always effective. None of these were relevant for the Buncefield accident.

Active engineered item – systems that act automatically when a hazard occurs to mitigate the consequences. There was no effective leak detection at Buncefield, so it was not possible to automate any shutdown or other mitigation when gasoline was released.

Active engineered item with human action – systems that prompt people to act when a hazard occurs. Because there was no leak detection the depot operators were not aware of the release until members of the public phoned to say there was a visible vapour cloud. However, even if they had known about the leak earlier they could not have stopped the supply to site directly because they did not have control of pipeline. They were reliant on the pipeline operators, who did not have visibility of the site. Stopping the flow quickly would have prevented the formation of the cloud or significantly reduced its size. This should have been considered into the arrangements for operating the depot and pipeline.

Administrative control with engineered support – action taken by a person that is initiated or supported by an engineered system. The Buncefield operators could have quickly and easily requested the pipeline to be shutdown at any time. They may have done this as soon as they realised the tank had been overfilled, before any product had been released. However, they were not aware of any problems until the hazardous vapour cloud had been formed.

Administrative control – emergency response procedures and practices enacted after a hazardous event to mitigate

0260-9576/25/$17.63 + 0.00

consequences. Once the vapour cloud had ignited, the main safety hazard had occurred and passed. The subsequent fire had significant environmental impacts but the risk to people was much less. An incident of this scale and nature had not been properly considered in emergency planning. This meant that issues, particularly fire water run-off, had not been properly considered in advance.

Personal health and safety control – protecting people from hazards. Given the scale of the accident the number of injuries experienced was relatively modest. There are very few options to protect people from an explosion like the one that occurred. However, there were many opportunities for people to be harmed during the subsequent firefighting operation. The products handled were non-toxic, and fire-fighting equipment, including breathing apparatus, was sufficient to protect personnel.

Conclusion

Applying an expanded version of the hierarchy of risk control has highlighted a number of factors related to the Buncefield accident that may be applicable more widely. The table below summarises some of the main ones.

References

1. *National Institute for Occupational Safety and Health (NIOSH). Hierarchy of Controls. https://www.cdc.gov/niosh/topics/hierarchy (2023)*
2. *Brazier, A. Wise, N. Making sure risks are ALARP. The Chemical Engineer (2021)*
3. *Brazier, A. Evolving the hierarchy of risk control from blunt instrument to precision tool for cutting risk. IChemE Hazards 34 conference (2024).*
4. *Buncefield Major Incident Investigation Board. The Buncefield incident 11 December 2005 – the final report Volume 1 (2008)*
5. *Engineering Equipment and Materials Users Association (EEMUA). Alarm systems – a guide to design, management and procurement. Publication 191 Edition 4 (2024)*

Potential learning	Buncefield relevance
Even when a business fundamentally relies on handling hazardous substances, it is important to ensure hazards are properly risk assessed. Also, to avoid introduction of and any supplementary or unnecessary substances.	The depot handled flammable fuels. There were no substances with other hazards (e.g. toxic, corrosive, reactive).
Complexity is often the result of commercial factors. Simplification is inherently safer, but if it is not possible, complexity has to be recognised as a risk that must be controlled.	Branching of the Thames-Mersey pipeline and division of the depot into multiple sites added complexity for the depot operators. The risks were not adequately addressed in the design of control system graphics or operating procedures.
Transferring products from a source with a large capacity into a receiver with smaller capacity introduces a significant risk of overfill.	The tanks at the depot had a fixed volume whilst the supply via pipelines was much greater. Overfill controls had to be much more reliable than may be required for other supply routes (e.g. road or rail tanker).
Reliability of active engineered controls relies on effective maintenance, inspection and testing.	The high-level switch on Tank 912 was left inoperable due to errors during maintenance. This meant the associated alarm and trip were unable to operate. The reason it was inoperable was that it was unreliable, which was unacceptable given its criticality for safety.
Control systems should have feedback loops from all critical plant parameters.	Pipelines had flow and pressure control, but no direct feedback from tank levels. The depot operators were responsible for managing tank levels.
Control system graphics should present data in a way that it is useful to the operator. It is not good enough to just make the data available.	There were graphic displays for each tank that showed level, but no overview display. Because the operators were not aware that Tank 912 was being filled, they were not actively looking at the data and it was hidden from view by other displays being monitored at the time.
A procedure describing a single task is less effective if multiple tasks are performed in parallel.	Procedures described how to conduct individual transfers from pipeline to tank, but operators were responsible for multiple transfers at any time.
Communication is an error prone activity. Shift handover is a particularly critical activity.	Depot operators were confused after shift handover and did not realise that Tank 912 was being filled. This meant they were not monitoring it. The poor control system interface and high-level alarm failure meant they were not aware until after the release occurred.
Low occupancy and open-air layouts may mean most releases do not result in significant harm but barriers like walls, off site features and populations can dominate the risk to people.	Industrial buildings near to the Buncefield site were very badly damaged. On another day many people were likely to have been serious injured or killed.
The route of a liquid from tank overflow to secondary containment bund can have a significant effect on hazard.	Gasoline being released from the overflow on Tank 912 was physically disturbed in a way that increased vaporisation and mixing with air. This had not been recognised in the design of the overflow.
Effective leak detection can allow interventions that may not prevent a release but can significantly reduce the consequences.	There was no leak detection. This meant there was no way of automating pipeline shutdown and no indications to the operators that a spill had occurred. The depot operators only knew that Tank 912 had been overfilled and gasoline was being released when members of the public phoned the control room.

0260-9576/25/$17.63 + 0.00

Attachment A – Proposed hierarchy with examples in hierarchical order[3]

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

0260-9576/25/$17.63 + 0.00

Type	Examples – prevention	Examples – mitigation
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 (classroom) • 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)

0260-9576/25/$17.63 + 0.00