A Strategy for Chemotoxic Safety on a Nuclear Licensed Site

Timothy P Boland, Design Capability Lead, Sellafield Ltd, Hinton House, Birchwood Park Avenue, Risley, Warrington, WA3 6GR

Keith A Johnson, Design Capability Lead, Sellafield Ltd, Hinton House, Birchwood Park Avenue, Risley, Warrington, WA3 6GR

Joanne Griffin, Safety in Engineering Lead, Sellafield Ltd, Hinton House, Birchwood Park Avenue, Risley, Warrington, WA3 6GR

1 Summary

This paper describes how Sellafield Ltd has absorbed and used learning from wider industry to develop an alternative strategy for chemotoxic hazards (that is the non-nuclear and non-radiological hazards). It uses the well recorded approach to basis of safety through good design (typical of nuclear safety cases) supplemented by pragmatic, proportionate, assessment techniques adopted by other high hazard high reliability industries. Using the most appropriate learning from both the UK nuclear industry and the wider chemical & process industry leads to chemotoxic hazard management that is implementable, is recognizable to supply chain partners, is consistent and integrated with the nuclear and radiological safety cases and most importantly does not hinder the progress towards the greater goal of high hazard reduction at Sellafield.

2 Introduction

The “Safety Case” – a simple term with many nuances. In Sellafield Ltd there are five identified aspects:

1) Nuclear and radiological safety
The two key definitions here are:

   i) Nuclear Safety
   The effective control and containment of nuclear material.

   ii) Radiological Safety
   The protection of people from the biological effects of radiation from nuclear material.

2) Chemotoxic safety

   i) This is an expression seldom found outside of the nuclear industry. An Internet search for the expression “chemotoxic” yields a number of definitions all associated with medical treatments and most commonly the side effects of cancer chemotherapy drugs or radiotherapy side effects.

   ii) In the context of a nuclear licensed site it means:

   “Hazards to people from materials present in the workplace that can cause harm as a result of their physical, chemical and biological properties in both use and storage.”

3) Conventional Safety
Best described as the traditional occupational health and safety.
They are the hazards due to the configuration of plant.

4) Environmental Safety
This Hazards that impact non-human biota or reduce human utility.

5) Security
It is a fact of modern life that the hazards arising from deliberate malicious damage to a facility must be considered.

Table **1** provides examples of the type of hazards covered by each of these five safety aspects.

The nuclear “dread factor”, the requirements of the Nuclear Installations Act 1965; the Nuclear Site Licence Conditions and the chronic effects of nuclear and radiological accidents tends to drive an emphasis on the nuclear and radiological aspects and security.

Furthermore, the regulatory regime reinforces the emphasis on nuclear and radiological safety. The regime is one of Permission rather than Forgiveness. Permission requires adherence to all detailed Regulator rules and the Regulator must give prior approval to certain changes to plants or procedures, which may affect the design intent or safety operating envelope of the facility which may affect the design intent or safety operating envelope of the facility. This is different to the modus operandi in other parts of the HSE who monitor and only become involved in depth when Forgiveness is sought when matters go wrong. (Kletz 2001)

A consequence of these factors is that the term “the Safety Case” has come to mean the nuclear and radiological aspects of safety.

This emphasis was reinforced at the January 1995 "Winter Seminar" between the regulator (the Nuclear Installations Inspectorate (NNI) now Office of Nuclear Regulation (ONR) and site licensee (BNFL now Sellafield Ltd). This meeting had a number of outputs:

- a review, which took several years, concerning the basis of Safety Cases;
- "understandings" between BNFL and NII on a number of generic issues affecting safety cases;
- the understandings are *binding* on both sides (with an update process);
- the concept of a Design Basis Accident Analysis (DBAA):
  - a methodology of analysis that gave rise to a Basket of Safety Measures, the "Basket methodology";
  - the methodology drives greater Safety Mechanisms;
- integrated input from engineers, safety assessors & operators;
- a 'slim' safety report summarising the wider safety case;
- an emphasis on ALARP not just probabilistic targets.

The DBBA Basket of Measures methodology evolved from the 1992 Safety Assessment Principles that required at least two independent safety measures. This was based on power reactor concepts. The concept considers the potential dose received by a worker or the public offsite and the frequency of the event. The philosophy is illustrated in Figure 1. The measures are designated as Safety Mechanisms; these should act to terminate the event causing the hazard.

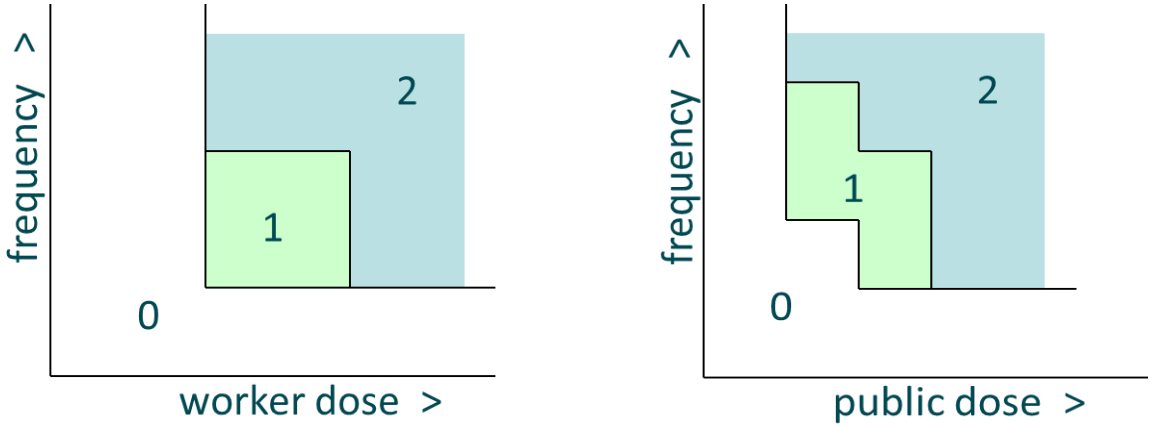
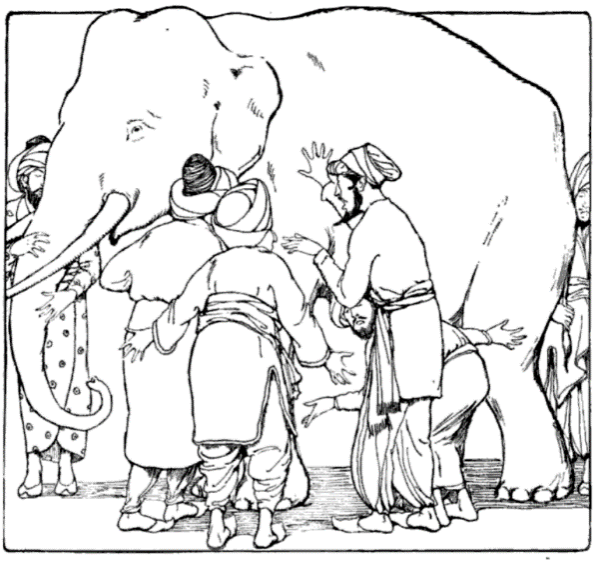


Figure 1 – Illustration of Design Basis Accident Analysis

DBBA methodology also embraced further features including:

- a conscious move to deterministic safety measures;
- avoidance of mathematical sleight of hand (such as salami slicing: the breaking down of a problem into smaller parts and demonstrating the parts to be "safe" without looking at the hazard holistically).

Winter seminar principles were aimed at evolving a more flexible approach, still using the dose and frequency criteria, but using a range of measures that will protect workers and the public and should terminate the event. The Basket of Measures should also be ALARP – "as low as reasonably practicable". This is a laudable aspiration. However, there is a problem with the interpretation of the ALARP principle There is no right or wrong answer only good or bad answers, it is, simplistically, what Horst Rittel, defines as a "Wicked Problem". The definition of which is: a problem that is difficult or impossible to solve because of incomplete, contradictory and changing requirements that are often difficult to recognize. An entertaining illustration of this is the allegory of the blind men and the elephant.



A group of blind men heard that a strange animal, called an elephant, had been brought to the town, but none of them were aware of its shape and form. Out of curiosity, they said: "We must inspect and know it by touch, of which we are capable". So, they sought it out, and when they found it they groped about it. In the case of the first person, whose hand landed on the trunk, said "This being is like a thick snake". For another one whose hand reached its ear, it seemed like a kind of fan. As for another person, whose hand was upon its leg, said, the elephant is a pillar like a tree-trunk. The blind man who placed his hand upon its side said, "elephant is a wall". Another who felt its tail, described it as a rope. The last felt its tusk, stating the elephant is that which is hard, smooth and like a spear.

The Winter Seminar output has been effective when applied to the rigours of nuclear and radiological safety. On face value, if the nuclear and radiological hazards are addressed by the Nuclear Safety Case then the chemotoxic hazards will be automatically addressed; this is a myth that has been promulgated through the nuclear industry for a number of years.

Operationally, plant managers like consistency in approach to hazards management; as a consequence, nuclear facilities with large chemical hazards within the, then BNFL estate, applied DBAA to the chemical hazards. However, there are inherent problems that are not immediately apparent when applying DBAA to other facets of safety. Fundamentally good safe design starts with Relevant Good Practice (RGP). There is limited RGP for complex, bespoke nuclear chemical processing plant hence the need for thorough safety assessment. However, there is considerable RGP for chemical hazards. Failing to use the plethora of RGP available and applying DBAA methodologies leads to routine challenges having bespoke, complex and difficult to implement on plant solutions. These solutions place an over emphasis on two independent safety measures.

Take as an example routing a service gas pipeline from a site supply into a process building. The supply is through a 50mm nominal bore pipe at a normal pressure of 37mbar. The basket of measures could include providing a fully welded pipeline and gas monitoring instrumentation that acts to shut off the supply if the building ventilation fails. To achieve the reliability two independent instruments and control loops are required with independent power supplies. This may be required if the consequences are severe. However, at 37 mbar the pipeline is not challenged by the pressure and hence best practices would suggest twin ferrule fittings and joints would be adequate. Is the control loop on building ventilation failure appropriate?

Another limitation of the Winter Seminar output was the ‘slim’ safety report summarising the wider safety case. The Health and Safety at Work Act and its subordinate Regulations require recording of the management of hazards in a “suitable and sufficient” manner. Where there are interactions and compromises between safety requirements a slim summary report is not the vehicle to address the decision making and the balance of potentially conflicting requirements.

A facet of “Winter Seminar is the need to substantiate that equipment delivers the safety requirements and functions that are claimed. This focus overlooks the why structures, systems and equipment must deliver any given function; how that “why” was derived and how that why fits into a bigger picture. This tends to drive the substantiation of the safety case into a back end activity particularly the chemical engineering aspects where the decisions on how the strategic approach to manage and assess hazards are made as a front end activity. This mismatch in timing causes scope drift and inefficiencies on nuclear design projects that are already typically lengthy.

Applying the “Winter Seminar” philosophy to the exigencies of nuclear and radiological safety is, arguably, proportionate; it is not proportionate to apply it to the other aspects of safety.

These consequences of the Winter Seminar directed the development of an alternative, design led approach to managing the chemotoxic hazards. The aim of the development was to apply learning from others whilst retaining the best of the nuclear safety case philosophy to provide a clear line of sight to decision making and the use of best practices from wider industry and not inventing bespoke solutions that are routinely addressed in other industries. This records the “golden thread” that is hazard identification, management strategy, the tactics and the implementation from cradle to grave.

3 The Approach (Basis of Process Safety)

The vehicle for the explicitly recording of the decision making process starts with the Basis of Process Safety supplemented by argument mapping tools such as Claims, Arguments and Evidence.

Process Engineering is predominantly a front-end discipline. It selects the most appropriate process within the constraints given by the business. Process selection fundamentally affects the Basis of Design, establishing design intent and subsequently the strategy of the Safety Case production. This is reflected by the difference in substantiating Process design compared to other disciplines. The Basis of Process Safety helps to document the rationale. Or to put it another way it is to explicitly show how inherent safety thinking (Kletz 1978, Kletz 1984) influences the design, considers all the hazards and articulates to others what the designer believed the balance between hazards and solutions to be.

The hazards fall into three categories:

- Intrinsic hazards
  These are the hazards with the feed .
  They express urgency of dealing with the issue.
- Introduced hazards
  These hazards are a consequence of the process or the management of an intrinsic hazard. Examples include: reagents, utilities, heating, cooling, moving etc.
- Deferred hazards are those left for others: decommissioning, demolition, effluents etc.

3.1 Purpose

The Basis of Process Safety shall:

- Describe the intrinsic Process hazards;
- Explain the rationale behind Process Selection, showing any compromises and why it is considered ALARP and BAT;
- Demonstrate the application of appropriate Hazard Management Hierarchy Principles (such as Inherent Safety);
- Outline the selected Hazard Management Strategies.

The BoPS is a live record and should be updated as the design progress from a study into concept, preliminary and detail design and ultimately into an as built plant record. As such it becomes that "golden thread" running through the lifetime of the facility.

At the outset of a project, the Study stage, the intrinsic Process hazards will be identified and differences in Hazard Management Strategies will be understood in order to differentiate between them and to select an option with the best chance of success.

At the concept stage of a project (when a single fit-for-purpose, cost effective scheme is confirmed as delivering the business benefits before commencing preliminary design) the intrinsic hazards will be understood and the main hazard management strategies outlined.

As design progresses, the hazard management strategies are understood and the functional and performance requirements clearly defined. (Functional requirement – what a system must do; performance requirement - how well a system must do it). The link between these design performance requirements and the nuclear safety case is through a separate document, an Engineering Schedule. The primary function of the engineering schedule is to present and communicate all safety important structures, systems and components with their associated safety functions and performance requirements.

The Basis of Process Safety shall be controlled through Design Change Control procedures, once the Hazard Management Strategies are frozen (typically prior to detailed HAZOP). The Site Licence for Nuclear Licensed sites makes Design Change Control mandatory.

During the development of the BoPS, multidiscipline or specialist input may be required, particularly in the later project stages. The amount of input will vary depending on the scope of the project.

3.2 Content of Basis of Process Safety

The typical content of a Basis of Process Safety document includes:

- Explanation of why the chemical and physical processes selected are appropriate for the consequences and how the safety risks are balanced to demonstrate ALARP and an optimised solution across all hazard types and legal obligations.
- Acknowledging that in order to address the primary hazard, secondary risks may need to be introduced.
- The appropriateness of any compromises between hazards and that the risk appetite is suitable. When initiated during the Study phase it will show Programme or even Portfolio strategic decisions and context. It shall justify the Programme's adopted Hazard Management Strategy. Later, as a Project document, it will need to refer back to those higher level decisions to articulate the constraints and assumptions which bound or influence the solution.
- All Process hazards including chemotoxic are considered not just Nuclear Safety hazards.
- Table 1 illustrates this feature.
- Description and justification of:
  - existing intrinsic hazards;
  - hazards that are incurred due to the processing chosen;
  - deferred hazards;
- A hazard tree showing how lesser hazards are incurred due to dealing with larger hazards. An example of such is shown in Figure 4;
- Explanation of the uncertainty associated with feeds. Feed basis may require some explanation; why some hazards are thought to be present and what hazards will not be addressed by engineered means. That is some

hazards associated with the feed may be considered to be of such low likelihood that operational or reactive measures would be more appropriate than providing a design solution;

- Demonstration of how 'inherent safety' has been considered in the design;
- An outline of the hazard management strategy for each identified process hazard. The science (or why) of the hazard should be explained. Each hazard is considered even if the consequences are relatively minor in order to demonstrate ALARP and BAT. Compromises in the use of hazard management hierarchy (Eliminate, Reduce, Isolate, Control) shall be justified;
- Process parameters (temperatures, pressures, concentrations etc) that are essential to the hazard management strategies are identified in the Basis of Process Safety. They also may constitute or inform performance requirements for the Engineering Schedule which in turn may influence control measures or mitigation identified/designed by other engineering disciplines. The Engineering schedule functional and performance requirements are discussed later;
- The conclusions from the Claims, Arguments, Evidence approach that demonstrates the clarity of argument and 'golden thread' which may then be used within a safety case;
- Referral to any relevant substantiation;
- Conclusions and work still to do should be listed.

Note Bene: the BoPS concentrates on "why" decisions have been made; it is not a process description (the "what" has been concluded). When describing the designer's rationale statements of adequacy are inappropriate; this is the realm of safety assessment and should be left to others.

In summary: the Basis of Process Safety articulates key decisions and moves the substantiation to much earlier in the design and safety assessment process and captures the rationale of the safety of the facility.

The BoPS provides a number of other advantages including:

- a foundation for the analysis of the hazards starting with Relevant Good Practice rather than starting with a blank sheet. This avoids reinventing the wheel by starting with unmitigated consequences and then work out what barriers are required. Enables the building in of decades of external learning from across industries.
- underpins applying semi quantitative techniques such as Layer of Protection Analysis (LOPA) to the chemotoxic hazards rather than the demands of addressing the nuclear dimension. One assessment technique does not fit all and is not appropriate for all. The BoPS enables the clear visibilities of all constraints and hazards to enable the proportionate application of RGP and assessment to identify appropriate control measures commensurate with the level of consequence.

4 Learning from the Experience of others

The recognition that chemical hazard management could "reinvent the wheel" led to exploring tools developed in other industries that could be used directly or adapted to support the BoPS production. Key amongst these is the argument mapping tool approach Claims, Arguments and Evidence (CAE); this is used in the aviation and defence arenas (amongst others). Through research and development this approach has been adapted to recognise the uncertainty in front end design that is typically managed by chemical engineers. How the CAE approach has been adapted and applied in detail during all phases of the design process is better described in a future paper.

Other tools include Bow Ties and Layer of Protection Analysis (LOPA). These are understood and recognisable by suppliers and partner organisations and more importantly are appropriate for assessing and understanding the management of commonplace chemical hazards rather than the DBAA approach taken for Nuclear hazards.

5 Summary of Overall Strategy

The objective of the work was to deliver business assets with the hazards from the five facets of safety managed in a practical and proportionate manner with the underpinning recorded and communicated to stakeholders in a suitable and sufficient manner. The focus of the paper has been on the chemotoxic arena and its relationship to the nuclear and radiological safety case development. Examining the definition of chemotoxic hazards proffered above, nuclear and radiological hazards are merely a specialist subset of chemotoxic hazards rather than a separate entity. However, this is a rather heretical view because there is a tacit assumption that nuclear safety is different and much harder.

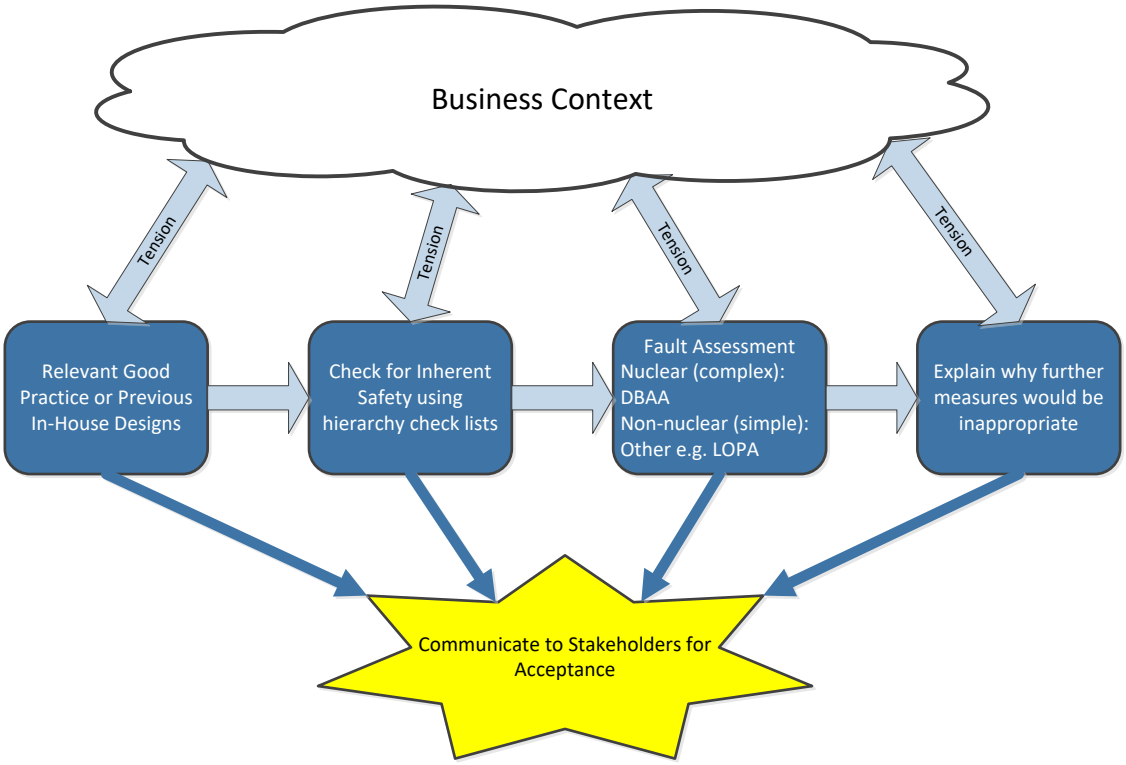
The strategy in summary:

- uses the Basis of Process Safety as:
  - the vehicle to inform and record the decisions and "whys" of all hazards and their management
  - making safety related decisions clearly front-end activities and therefore within the sphere of design influence
  - to provide the "golden thread" from cradle to grave giving a clear line of sight to all about decisions, reasons and underpinning
  - the justification for the approach taken to assessment whether it be LOPA, DBAA, Bow-tie etc.
- explicit consideration of inherent safety
- clearly adopts and records the use of Learning from Experience to the management of hazards

- adapted and developed the Claims Arguments and Evidence tool to address the uncertainties in the early stages of design
- applies the CAE tool to underpin and communicate safety related decisions
- delivers safety management solutions that are proportionate and appropriate to the hazard and the consequences
- markedly improves communication with stakeholders.

Figure 2 is a high level illustration of how the elements discussed come together.

Figure 2 Safety case development and communication high level strategy



6 Case Study 1 – Carbon Dioxide Asphyxiation Hazard

This illustration of the application of the strategy is from a project delivering an effluent treatment system. The process requires control of the pH to maximise the efficiency and longevity of a naturally occurring zeolite ion exchange medium: clinoptilolite. The pH control is by dosing with carbon dioxide; this presents asphyxiation and toxicity hazards

6.1 Asphyxiation Hazards

Carbon dioxide is used to neutralise the pH of the filtered effluent ahead of passing through ion exchange medium via a Carbonation Tower. Carbon dioxide presents an asphyxiation and work place exposure hazard (i.e. presents a toxic effect).

Remove: Not Applicable – Carbon dioxide is used to neutralise the filtered effluent based on prior experience.

Reduce: High integrity storage tanks and pipework, fully welded pipework within building by locating valves, fittings and instruments outside the building. Minimising pipe length by locating carbon dioxide tanks as close to the point of use as possible. System designs will comply with regulations and recommended best practice.

Control: Limited flow, good ventilation, thermal and pressure relief systems.

Mitigate: Pressure and temperature monitoring (alarms/ trip), EIM&T (Examination, Inspection Maintenance and Testing) by SQEP (Suitably Qualified and Experienced Personnel) operators, PPE during maintenance activity as identified on the Safe System of Work (SSoW).

6.2 Normal Operations

Carbon dioxide is used to neutralise the filtered effluent from pH 11-12 to ~7 (pH 6 - 8) to improve the:

- performance and prevent degradation of the ion exchange bed;
- ensure treated effluent pH suitable for sea discharge.

A study confirmed that the best available technologies available, given the time constraints, were to use carbon dioxide pH control. Therefore, neutralisation with carbon dioxide is adopted and no other neutralisation methods are explored.

The Chemotoxic Report reviewed the hazardous scenarios against the design to demonstrate that the identified potential consequences are eliminated, prevented or mitigated by engineered and operational safeguards. The report also identifies additional design and/or operational features which can act to further reduce the risk.

Below are the engineered and operational safeguards in place to support the sub-claims to minimise the asphyxiation and work place exposure hazards caused by the carbon dioxide system. A précise of the CAE is included below:

Sub-claim C1S1: The carbon dioxide system design will minimise the potential for operator exposure.

Argument C1S1A: High-integrity storage tank and pipework to ensure primary containment. Fully welded pipework within SCP building and locating all valves, fittings and instruments outside the building. Supply line will be routed to minimise length, avoid clashes and away from operator.

Evidence: SCP Chemotoxic Assessment.

Under normal operations, the following generic measures will be taken to minimise the risk of asphyxiation and exposure to toxic levels of carbon dioxide:

- The vendor package (tanks, pipework and instruments) will be supplied by approved contractor with significant carbon dioxide experience. The cryogenic storage tanks and delivery pipework will be designed and installed in accordance with Safe Storage, Handling and Use of Special Gases (BCGA COP18). Equipment design, manufacturing and maintenance will meet the requirements of the Pressure Equipment Regulations 2016 (SI 2016 No 1105) and the Pressure Systems Safety Regulations (SI 2000 No 128).
- The pipework is specified to meet the maximum design process environment. (RGP Piping Standards).
- The storage tanks and pipework will be subjected to a rigorous inspection regime, during construction, commissioning and throughout their operational life.
- The pipework within the building will be fully welded.
- Pipe lines will be routed to avoid clashes and away from the operators (e.g. away from access pathways).
- The storage tanks will be located in a relatively remote area and the carbon dioxide storage layouts have been undertaken in accordance with safe distance recommended by British Compressed Gases Association (BCGA COP 36).
- All valves, fittings and instruments (e.g. pressure, temperature and flow) are located outside the building to minimise leak paths inside the building and any leakage from flanges or connections can be safely dissipated.
- Actuated valves and instruments (e.g. pressure, temperature and flow) within the carbon dioxide compound outside the building will be relayed to the Supervisory control and data acquisition (SCADA) system to allow monitoring and operation of actuated valves without accessing the compound.
- The carbon dioxide storage compound is locked closed during normal operation and access only available under management control.
- The building ventilation system to provide good ventilation within the building. The ventilation ductwork is design in accordance with all relevant standards and legislation. Ductwork will be tested and inspected during construction and commissioning.

Sub-claim C1S2: Delivery of carbon dioxide liquid and EIM&T of tanks, valves, relief valves, fittings and instruments can be undertaken safely.

Argument C1S2A: The carbon dioxide system can be safely shutdown and isolated. Local and control room alarms will alert operators not to enter the compound.

Evidence: Facility Chemotoxic Assessment.

The carbon dioxide compound will be locked closed during normal operation and access only available for any routine loading and EIM&T requirements. The following safeguards will be in place to ensure safe loading and maintenance operations:

- The carbon dioxide system can be shut down and supply line can be suitably isolated and vented prior to maintenance
- Local audible alarms are in place to warn operators in the event of faults and potential unsafe working conditions.
- Carryout risk assessment out to ensure no significant hazards have been identified prior to entering into the compound (RGP).
- An appropriate SSoW will be in place to access the area and carryout works within the compound.
- The carbon dioxide storage facility will be operated by SQEP operators knowledgeable in the precautions required and aware of the risks (RGP).
- carbon dioxide tanker offloading will be undertaken by an agent of the supply company, specifically trained in tanker offloading and following industry standard instructions for the delivery of cryogenic liquids (RGP).

6.3 Foreseeable fault scenarios

Sub-claim C1S3: Lost of containment of carbon dioxide can be detected, controlled and recovered.

Argument C1S3A: Alarms/trips (pressure and temperature) and relief systems within the carbon dioxide package will alert operators to faults and prevent low pressure and overpressures of the system. The flowrate will be restricted so that any leakage in the facility building can be minimised.

Evidence: Chemotoxic assessment.

The potential for loss of containment of carbon dioxide may be a result of manual handling error, overpressure of the system, failure of the storage tank, pin-hole leak or potential release from equipment such as flanges, valve/instrument connections or welded joints. The loss of containment could result in a release of carbon dioxide into areas where operators are present. The high-integrity and through-life inspection and maintenance of all equipment conducted in line with relevant design standards and procedures will reduce the probability of failure. High and Low alarms/trips will reduce the likelihood of tank and pipework failure (e.g. low pressure/ temperature alarms will minimise the likelihood of carbon dioxide solidification potentially impacting on tank and pipework integrity). The barrier surrounding the carbon dioxide compound will reduce the likelihood of an external mechanical or vehicle impact on the carbon dioxide storage tanks, hence, reducing the risk of large loss of containment. In an unlikely event the following measures are in place to manage the hazard under these fault conditions:

- Instrument alarms (pressure and temperature) will alert of faults within the control room and locally (audible). Remote telemetry system will alert maintenance and operations of alarm and hence prompt to investigate the fault.
- Thermal and pressure relief valves will prevent overpressure of the system if the alarms are not acted on. The thermal and pressure relief valves will be tested and maintained on a routine basis in accordance with the PSSR.
- The carbon dioxide storage compound is locked and access only available under management control. This reduces the likelihood of personnel being present in the area should a fault occur.
- Emergency procedures will be in place to stop the continuous loss of carbon dioxide, to prevent the gas reaching a toxic concentration.
- The storage tanks will be located away from building and operators, in accordance with BCGA recommendations, which ensure that escape routes are not impeded [RGP].
- All valves, fittings and instruments (pressure, temperature and flow) are located outside the building, any leakage from flanges or connections can be safely dissipated.
- The carbon dioxide supply pipe is routed directly to its point of use within the facility and so avoids being routed through man accessible areas within the building which would otherwise have had to be classed as a confined space.

6.4 Additional hazards introduced

No additional hazards are introduced as a result of managing the asphyxiation and workplace exposure hazard.

7 Case Study 2

This is an example of using Claims Arguments and Evidence Mapping tool to support the demonstration that an oxygen monitor does what it is required to do, that is the substantiation.

The approach is captured in a logic diagram reproduced here as Figure 3. This illustrates the value of the CAE approach:

- when used in safety case environment.
- how it can inform risk and development plans.
- provides explicit recognition of assumptions and has the ability to inform decision-makers of the consequence of changing their mind!

Figure 3 - Use of CAE to support substantiation of an oxygen monitor

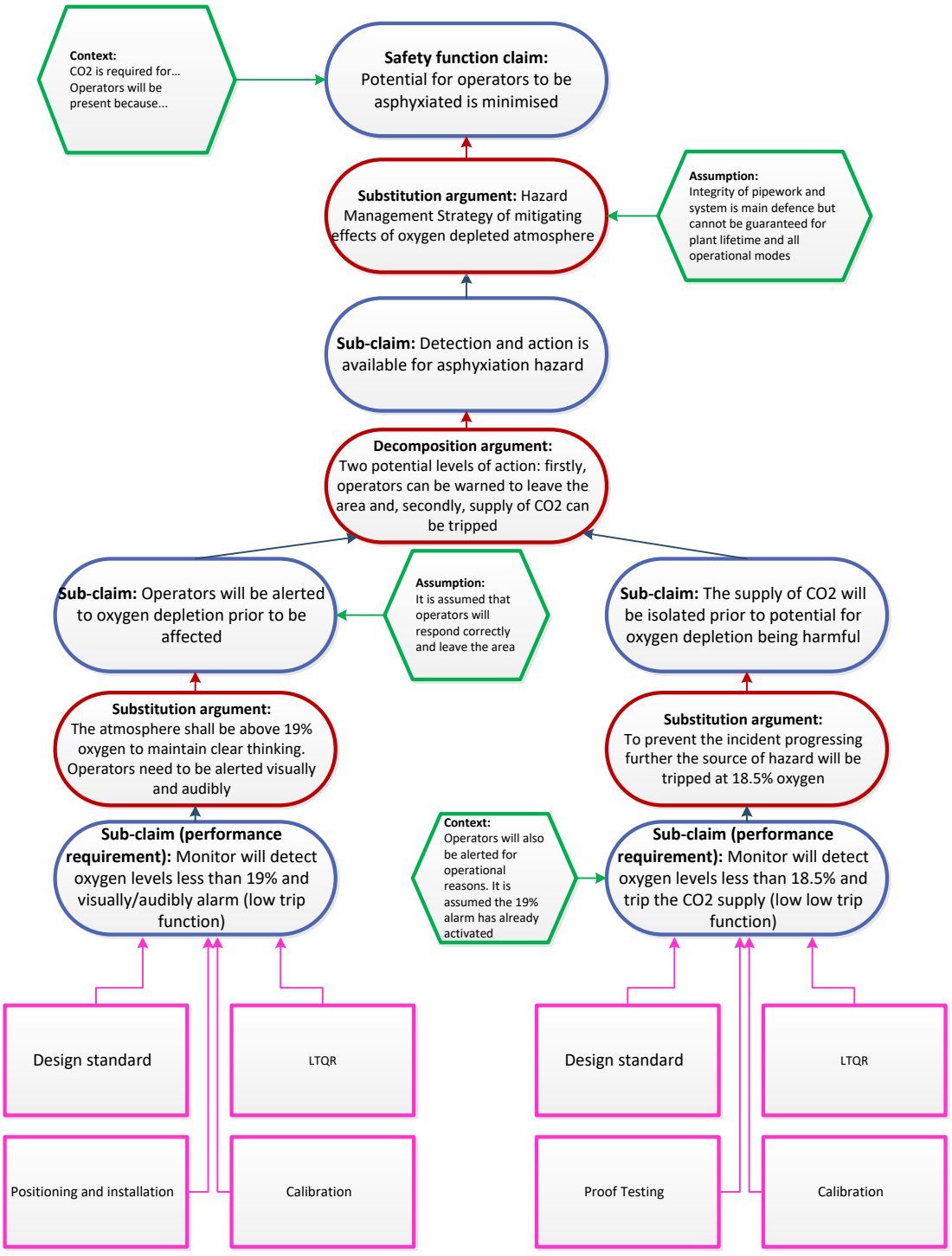
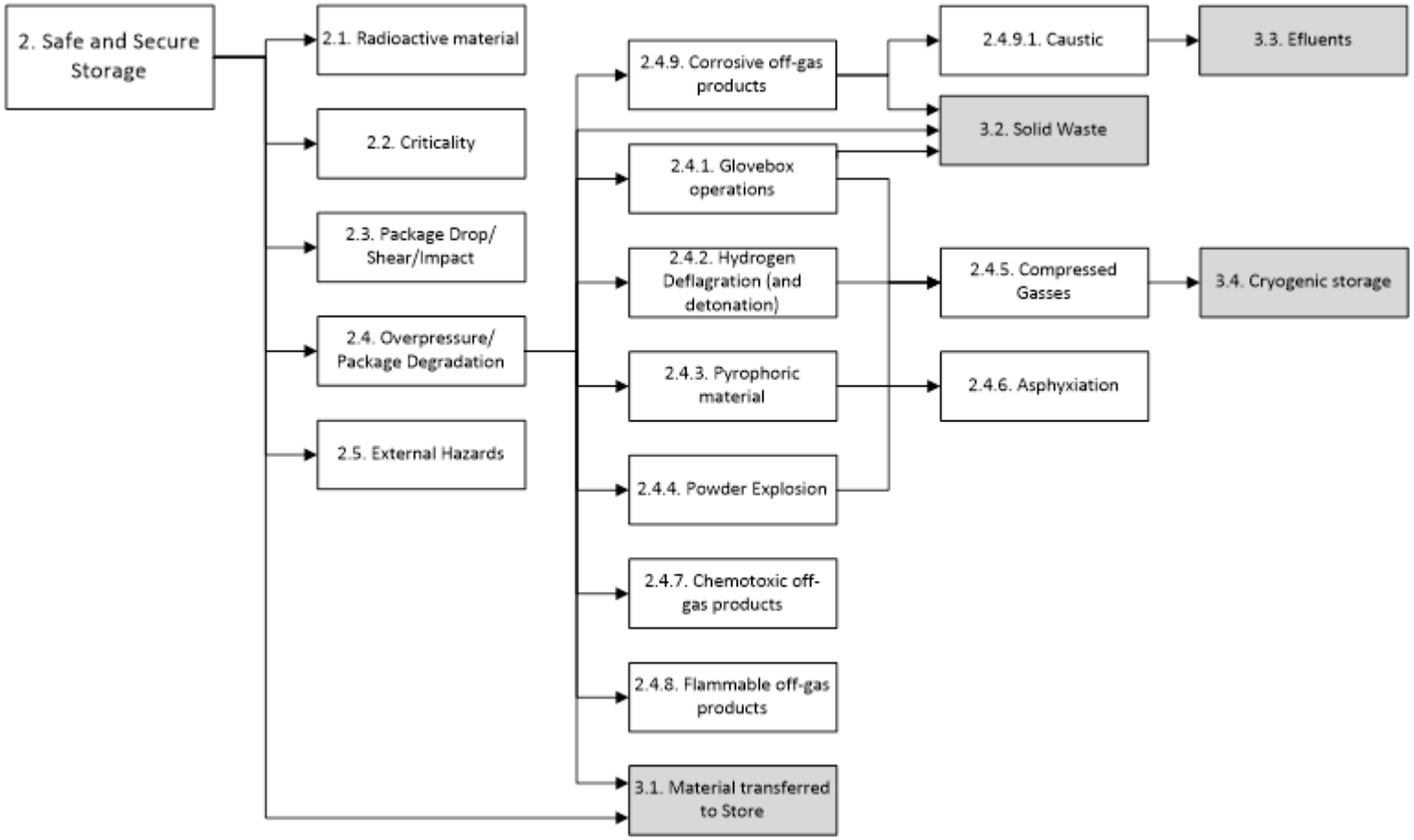


Table 1 – Examples of the Five Aspects of Safety

Nuclear and Radiological Hazards	**Chemotoxic Hazards**	**Conventional Hazards**	**Environmental Hazards**	**Security Hazards**
Hazards due to radiation	*Hazards due to the properties, conditions and behaviours of materials (other than radiation).*	*Hazards due to the configuration of plant.*	*Hazards that impact non-human biota or reduce human utility (enjoyment)*	*Hazards that are malicious*
Examples: • Internal dose • External dose • Criticality	Examples: • Explosive hazards • Flammable hazards • Oxidizing agents • Corrosive chemical hazards • Pressure related hazards • Acute and chronic health hazards • Asphyxiation • Reaction hazards • Biohazards (e.g. Legionella)	Examples: • Working at height • Slips, Trips and falls • Moving machinery • Stored energy • Suspended loads • Manual handling • Noise • Vibration • Fire • Electricity	Examples: • Radiological discharges (that are remote from humans, otherwise covered by Nuclear) • Non-radiological discharges (where biota are more sensitive than humans, otherwise covered by Chemotoxic) • Non-renewable resource use • Loss of biodiversity, habitats or cultural assets • Nuisances (traffic, dust, noise, visual etc)	Examples: • Impacts • Explosive devices • Isolation (resilience) • Cybersecurity • Accountancy

Figure 4 - Example Hazard Management Tree



Note: Shaded boxes are Deferred Hazards

Figure 5 Generic Bow Tie Diagram:

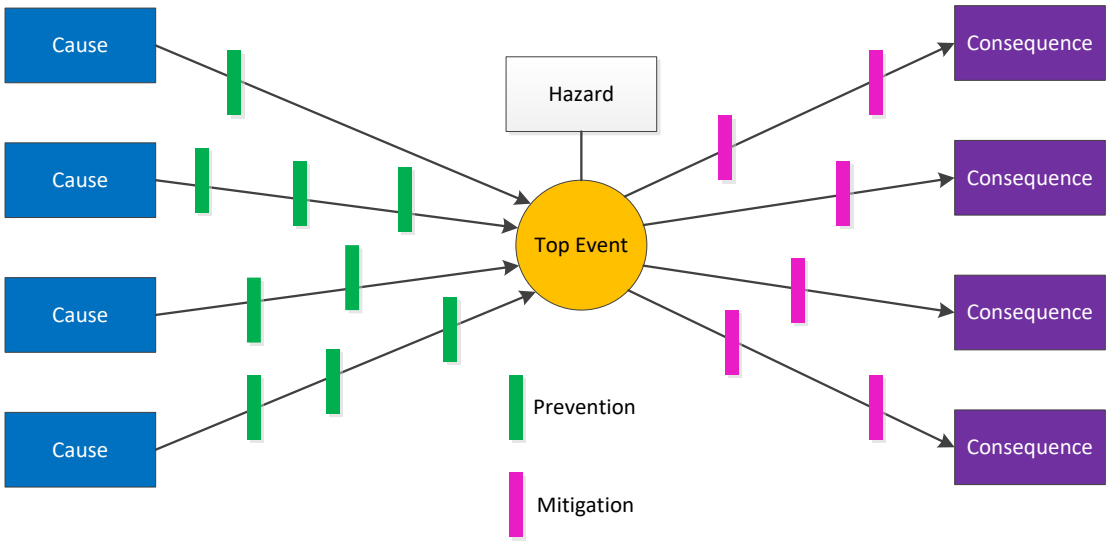
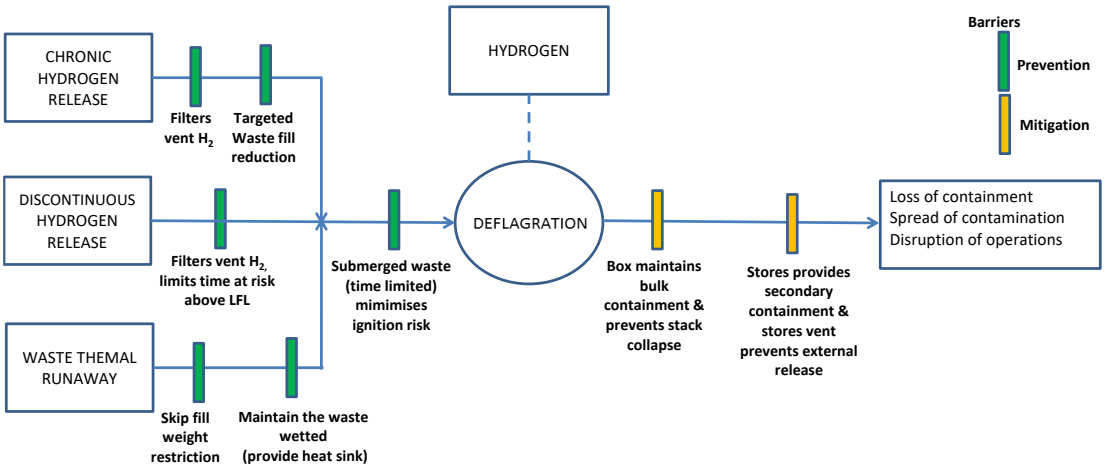


Figure 6 Example of Bow Tie from a Basis of Process Safety for a deflagration on a legacy facility



References

BCGA COP 18 Safe Storage, Handling and Use of Special Gases, British Compressed Gases Association (BCGA) Code of Practice 18

BCGA COP 36, 2013, Rev 2, Bulk Cryogenic Liquid storage at user premises. ISSN 0260-4809

Center of Chemical Process Safety 2015 Guidelines for Iniating Events and Independent Protection Layers in Layer of Protection Analysis AIChemE.

CLP 2008
REGULATION (EC) No 1272/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 December 2008 on classification, labelling and packaging of substances and mixtures, amending and repealing Directives 67/548/EEC and 1999/45/EC, and amending Regulation (EC) No 1907/2006

Cullen, W. D. 1990. The public inquiry into the Piper Alpha disaster. London: H.M. Stationery Office. ISBN 0101113102.

Kletz, T.A., 1978 *Chemistry and Industry* pp, 287–292 “What You Don’t Have, Can’t Leak”

Kletz, T.A., 1984 *Cheaper, Safer Plants or Wealth and Safety at Work –Notes on Inherently Safer and Simpler Plants* IChemE Rugby, UK

Kletz, T A. 2001, Learning From Accidents 3rd Edition

SI 2000 No. 128 The Pressure Systems Safety Regulations 2000

SI 2016 No. 1105 The Pressure Equipment (Safety) Regulations 2016