'LIFE CYCLE RISK ASSESSMENT AND IMPLEMENTATION ON AN EXPANSION PROJECT FOR A HAZARDOUS FACILITY'

R. P. Argent, P. Cook and P. Goldstone
Process Technology Group, Air Products PLC, Hersham, Surrey, KT12 4RZ

Air Products designs and operates potentially hazardous cryogenic processes and applies the theoretical and practical aspects of hazards analysis and risk quantification techniques. This paper describes a case history of an expansion to an operating facility.
A rigorous methodology identifies hazards throughout the design phase and includes a verification programme to monitor the implementation of protective measures. During normal plant operation, auditing and analysis of feedback data ensure that the design and safety philosophies are not compromised. Examples are given which emphasise the value of meticulous reviews and the need for effective maintenance of protective systems to meet quantified reliability and safety targets.

Key Words: Cryogenic, Hydrogen, HAZOP, Risk

INTRODUCTION

As both a designer and operator of potentially hazardous plants utilising cryogenic processes, Air Products has the advantage of a complete overview of all aspects of hazard appraisal and evaluation together with the specification of protective systems and subsequent retrieval of operating experience.

The achievement of 'Total Safety' through the application of Hazard Review and Risk Quantification techniques can only be realised by meticulous attention to detail during the design, commissioning and operating phases of a project and by implementing the recommendations of the Hazard Study using sound engineering and operating practices.

The paper describes a case history of a recent expansion to an operating facility as a means of illustrating the processes of hazard review, mitigation, verification and feedback required to meet established reliability and safety targets.

PROJECT SCOPE

The project consisted of a hydrogen purification/liquefaction, storage and road tanker loading facility as an extension to an operating site in Holland using an existing natural gas-steam reformer to provide hydrogen feedstock.

The hydrogen liquefier was a repeat of a unit previously designed and built in the USA. Full details of all aspects of the original technical design were available together with a HAZOP dossier. Considerable operating experience was available based on 20 years of supply and transport of liquid hydrogen to NASA. The storage envisaged a 70 tonne vacuum insulated sphere (1047m³ water volume) to which the top tier criteria for liquid hydrogen as laid down in the Council Directive 82/501/EEC "Major Accident Hazards of Certain Industrial Activities" were applicable.

Design work commenced in November 1985 and the facility extension was commissioned in January 1988.

MANAGEMENT OF HAZARD REVIEW

The Air Products safety philosophy is based on its declared policy that safety is a line management responsibility and that all accidents are preventable. The Corporate Procedure 'Project Hazard Review' was developed to reflect and implement these principles in practice. The main purpose of the procedure is to ensure that a hazard review team is formally appointed and charged with the responsibility to assess, quantify and reduce, wherever possible, the risks associated with any new project.

In approaching its task, the hazard review team will be required to compare the quantified risks with other risks involved in the industrial gas business and exercise good judgement in balancing risk reduction against cost.

However, the final decisions as to whether certain levels of risk are acceptable or not will be made only be the senior management of the Corporation. For this project, due account was taken of the third party risk criteria being developed at the time by the Dutch authorities which are encompassed by the Dutch National Environment Policy Plan 'Risk Limits in the context of the Environmental Policy' (1988-89) (see References).

The procedure identifies the Project Manager as responsible for all activities up to the hand over of the plant to the operating staff. The hazard review team is normally chaired by a qualified chemical engineer, trained and experienced in hazard assessment techniques. The team is supported by a task force of design and specialist engineers in the appropriate disciplines.

General outline of procedure:

- assessment of risk categories with divisional and corporate safety managers
- creation of the hazard review team
- implementation of preliminary hazard reviews to determine those areas requiring detailed review
- definition of design hazard reviews for various specific sections identified above. Such work to include a review of detailed quantified risk assessments carried out by appropriate specialists
- HAZOP studies of new/revised processes
- design verification reviews after detailed design
- preparation of comprehensive dossiers for transfer to the construction/commissioning and operating phases of the project.

GENERAL AREAS OF INTEREST DURING SAFETY REVIEWS

Since the design of individual equipment blocks already existed, safety reviews were telescoped into the front end of the design process with practically all internal information available.

For what was virtually a repeat project, there was a risk that project management would not be amenable to changes highlighted by specific safety reviews on a basis of unjustified additional cost.

This did not in fact occur due to the commitment by project management and the design task force to meet or exceed all the agreed targets with respect to cost, schedule, safety, operability, reliability and integration with existing operating equipment. There was significant involvement with Dutch local approval authorities over the perceived risk of liquid hydrogen. For the calculation of off-site risks it was agreed to use the SAFETI programmes developed by Technica for The Netherlands Organisation for Applied Scientific Research (TNO).

The SAFETI data for liquid hydrogen required a significant degree of collaboration with Technica to develop suitable models and data for hydrogen release phenomena.

With copious information available on the hydrogen liquefaction/purification process, project hazard reviews could focus on the implications and effects of a large liquid hydrogen storage installation, European trailer loading requirements, local authority licence requirements and a co-ordinated approach to facility layout (including a carbon monoxide tube trailer filling facility and garage facilities for distribution network) on offices and other processes already on-site.

Although the plant layout was subjected to repeated examination for optimisation and cost reduction, it was possible to establish criteria for separation distances between the major process units and other areas using the worst case releases and calculated consequences. The results showed the types of incidents which could be contained within the process units and those which had a general effect and needed to be subjected to third party risk quantification.

It proved necessary to insist on several changes to existing facility arrangements to avoid unnecessary risk to personnel and services not associated with the new operating units. Temporary offices had to be moved; permanent offices/workshops had their functions changed to reduce staff levels; plant systems and services had to be segregated or relocated for operability reasons; established contractor laydown and service areas had to be relocated.

Initial calculations for third party risk showed that a catastrophic failure of the liquid hydrogen sphere resulting in a vapour cloud drifting without premature ignition might cause fatalities several kilometres away from the source of the release. However, such third party consequences would be

much less severe if the vapour cloud encountered an ignition source close to the point of release. The effect on the site in this case would be worse due to the potential exposure of operating personnel and other process units.

As a result of the initial investigations the authorities laid down minimum licence requirements for the design and protection of the liquid hydrogen storage and provided criteria for external overpressure tolerances (from independent incidents) in line with the criteria developed for the on-site separation distances previously discussed.

Hazard study reports were required by the authorities for the liquid hydrogen storage tank, the liquefier process and the fire-fighting provisions. In addition, the liquid trailer loading arrangements and procedures, the hydrogen feed from the PSA system, the venting and flaring arrangements were all subjected to HAZOP and HAZAN studies. Design safety reviews were mostly completed by mid 1986, except for the trailer loading system which was not conducted until 1987.

SPECIFIC ITEMS RESULTING FROM DESIGN HAZARD REVIEWS

The liquefier process itself, although operating with pressures as high as 63 bar and with temperatures down to -253°C, did not constitute an offsite risk since the original design (in the USA) had paid particular attention to limiting the inventories of liquid (<20 kg) and vapour (<100 kg), and utilising the smallest possible line sizes. The method of construction of the 'cold-box', containing the exchangers and purifiers, using an internal stainless steel vacuum jacket was a significant factor in reducing the off-site risk.

The compression system was housed in an acoustic enclosure without a roof (for ventilation reasons). Because the enclosure obscured the line of sight, the internal equipment was protected with a fire detection system and fixed fire fighting equipment. However, as it turned out, the design of the compressor area created difficulties with the segregation and protection of operating and emergency electrical cabling systems. In addition, there were a large number of unnecessary permanent start-up vents and bleeds. The relatively small gas inventories, however, served to limit the effects of a fire on adjacent equipment.

While fire detectors were ultimately provided for the liquefier expanders (at the 'cold box'), the tanker loading area, the PSA valves and the compressor enclosure, it was decided that the detectors would provide alarms only and would not automatically actuate the fire water deluge systems.

This was to avoid spurious actuation of the water systems even though the reliability of the detectors were to be enhanced by means of voting systems. The detector system design allowed for the consequence of low manning of an automatic plant coupled with the high likelihood of ignition in the event of a pressurised hydrogen gas release.

For a sustained water deluge of equipment in the event of a fire, it proved necessary to have a water availability beyond the capacity of the existing facility cooling water system. An external supply from neighbouring customer facilities in the petrochemical complex was therefore provided.

In designing the liquid hydrogen storage tank, it was found necessary after a review of previous criteria to increase the size and number of inner vessel overpressure protection devices. This necessitated a major rework of the vent/flare arrangement for the tank to accommodate the possible flows safely. There were also unusual considerations (for liquid hydrogen storage) for the effects of loss of vacuum on the insulation space, where the ingress and condensation of air on the cold surfaces would promote rapid boiling of the stored liquid. The heat flux created by this event exceeded that for the fire engulfment case and determined the relief device sizing. A further hazard could be created by air condensing on vent or drain lines in the event of use or valve leakage; this would create a potential for the accumulation of oxygen enriched liquid in addition to the hazards of liquid hydrogen.

The mechanisms for overpressure of the liquid hydrogen tank are illustrated in the fault tree shown as Figure 1.

A major contribution to catastrophic failure of the storage tank was the improper selection or fitting of the overpressure bursting disc.
A special monitoring provision had to be developed to minimise such an event by ensuring that no other bursting discs of the same size were stored on the facility (for other cryogenic tanks) and by methodically preparing an auditable maintenance and replacement procedure for bursting disc changeover.

With the implementation of appropriate design, construction and testing methods for the liquid hydrogen tank, allied with the inbuilt safety features and the inherent properties of austenitic stainless steel in liquid hydrogen service, it was possible to conclude that a catastrophic failure of the storage tank with a release of its contents was so unlikely an event as to be non-credible.

This conclusion was accepted by the authorities in spite of their initial concerns about the theoretically significant worst case consequences that might result. The policy of accepting potentially large societal consequences, providing the risk is low enough, is now included in the Dutch Risk Management Premises referred to previously. (See also Figure 2)

Although the liquid hydrogen trailer design was standard, having originated in the USA following comprehensive transport safety studies, the rigorous HAZOP technique highlighted some concerns with regard to the loading procedures originally prepared from the American standards. Revised procedures were developed incorporating critical checks for leakage from coupled hoses, and for failure of the vacuum in the jackets of connecting hoses, to reduce the risks of release to an acceptable level. In the event of a release from a hose broken by mechanical failure or towaway of a connected trailer, it was found necessary to incorporate remotely actuated shut-off devices on the loading station and trailer side of the hose. To reduce the risk of a tanker towaway, an interlock system is provided which automatically applies the tanker brakes while the transfer hose is connected to the tanker.

DESIGN VERIFICATION AND TRANSFER OF INFORMATION TO INSPECTION AND START-UP PHASES

The design was complete and construction well advanced by May 1987, at which time consolidation and checking of all outstanding hazard review recommendations was conducted.

Although adequate files had been maintained by the Safety Engineer, no system of cross referencing existed and it was therefore necessary to produce a comprehensive bibliography of all internal and external correspondence for checking and review. The documentation sources

within the various design departments were identified and checked after which it was a simple matter for the hazard review team to check that recommendations had been carried forward through the chronology to completion or identified as outstanding items for the prestart-up auditing procedures. The review was time-consuming but yielded important results both in identifying major deviations from the original design safety philosophy and in finding those items still incomplete after 18 months of the design phase had elapsed.

In fact, the need to perform a HAZOP on the PSA unit was identified at this stage as there had been a change of vendor and cycle from that envisaged during the original design. The meetings also highlighted those items which were related primarily to the operating phase of the plant for which the plant management were solely responsible. Examples included updating and expanding the existing facility emergency plans, operator training, personnel protection (fire resistant overalls, were introduced at this time), maintenance frequencies and proof test intervals for critical circuits.

By August 1987, all items had been completed or recatalogued for inclusion in the site inspection procedures. The latest feedback from the operating American plants had also been obtained and collated (these affected the design of flame arresters on hydrogen vents which, from previous experience, have a high ignition probability) and the files updated for future reference.

SAFE TO OPERATE VERIFICATION

A comprehensive engineering and safety audit was conducted at the end of the construction phase to determine if the plant could be commissioned safely. The team for the audit activity included the core members of the HAZOP group. This was the first opportunity for the hazard review team to inspect the completed plant and to consider the practicalities of safety related improvements. The activities of the team included:

- A rigorous flowsheet check against the installed equipment.
- A detailed check of all operating areas for safe and easy access to equipment.
- A review of vent or purge locations to determine if localised accumulations of flammable liquids or gases were possible.
- Dummy runs on areas involving intensive operating activity e.g.the liquid hydrogen trailer fill system.

At the end of the audit a 'Safe to Operate' certificate was issued including a summary of outstanding remedial work, each item of which was categorised as either "essential before start up" or "complete by a specified date". On completion of the essential items the equipment was released for commissioning.

It is important that items in the "non essential" category are not forgotten and are reviewed about 3 months after commissioning to ensure that plant safety in the long term is not compromised.

A selection of defects discovered during the Engineering and Safety Audit on the facility is displayed in Table I.

POST-COMMISSIONING AUDIT

It is recommended that a post-commissioning audit be conducted within 2-3 years of commissioning with the object of ensuring that key recommendations made during the course of the hazard studies are still being followed and that any problems arising are identified and resolved.

The audit should cover the following:

- Review of any safety related incidents since start up.
- Review of premature failures or maloperation of protective equipment eg relief devices, trips, alarms etc.
- Inspection of critical process areas to check housekeeping, access, information displays, isolation and system integrity.
- Review of preventive maintenance schedules to ensure proof test periods are correct.
- Discussion with process and maintenance staff to confirm that proof testing is readily achievable without major risk of interruption.
- Checks on critical operating activities to review potential hazards and to determine if special procedures are fully operative.

The audit should be as detailed as possible to confirm that the key activities arising from the HAZOP design and verification stages are not compromised. It should be conducted in two stages:

- An early appraisal of the major hazards which provided the focus for third party risk assessment, fault tree quantification, special operating licence etc.

- An appraisal of lower level hazards listed in the review including items such as equipment maintenance activities.

On the facility in question, the following five examples demonstrate how the post-commissioning audit revealed weaknesses in the implementation of the hazard study recommendations:

Liquid Hydrogen Trailer Earthing

The loading procedure highlighted the need to earth the trailer using its built in earth reel and the earth strip common to the loading point. In order to verify that the earthing was correct, the facility was modified by the site management, subsequent to commissioning,
to add a zero potential check. This involved the attachment of a lead between a control box fitted at the loading point and the trailer via a clamp. The control box showed a 'GO' (Green) or 'NO GO' (Red) signal lamp. During the audit it was found that the detector showed green at all times whether the clamp was fitted to the trailer or not.

The operator did not realise the device had developed a fault as he only looked at the light after fitting the lead clamp. The device created a potential hazard as it was not fail safe.

All modifications to a potentially hazardous area must be referred back to the HAZOP review team even if such changes appear innocuous.

Remote Isolation of the Liquid Hydrogen Trailer

As part of the final fire safety review for the facility extension, a modification was proposed to enable remote isolation of the liquid hydrogen trailer should a leak occur on the loading hose. This was achieved by removing a spool piece from the trailer loading valve

instrument supply and installing a solenoid operated trip valve using quick release connections. This activity formed part of the trailer loading preparation and required that the spool piece be inserted into a location in the loading station liquid valve instrument supply line, thus enabling the valve to be opened as necessary. During the loading condition the trailer can therefore be remotely isolated in an emergency or, both fill point and trailer valves opened as required.
In the drive away condition the fill point valve cannot be opened without a trailer present.

During the audit it was found that the spool piece and connections were complete. However, the solenoid operated trip system had not been installed and a jumper line had been fitted in its place to permit normal operation without the remote trip facility.

This proved to be a classic example of a late project modification where final completion escaped the scheduled construction activity and pre-commissioning auditing. It was nevertheless identified by the post-commissioning checks.

Maintenance of Process Protective Systems

The company operates a computerised preventive maintenance system whereby each plant receives a monthly instruction detailing the tasks to be carried out. Each plant then makes a formal return on pre-printed cards, confirming that the tasks have been completed.

Examination of the monthly task sheets revealed that although the protective systems recommended by the HAZOP and risk quantification studies were included, the critical nature of their functions, and the degree of priority required for their maintenance, was not given sufficient emphasis. It was also found that while records of instrument failures were being maintained by the plant personnel, such information was not communicated to the central office on a regular basis using the task confirmation cards. These observations reflected no lack of diligence on the part of the maintenance department, but served to highlight the need for improved communication links between the hazard review team and the plant operator.

Anti-Tow Away Protection

To reduce the risk of a trailer 'tow-away' whilst still connected to the fill point via the loading and vapour return hoses, a flexible steel cable is connected between the trailer end of the fill hose and a manually operated three way valve on the instrument line to the fill valve. In the event of a trailer moving away from the loading station with the hoses connected, the three-way valve is actuated which closes the fill valve. Unforeseen lack of flexibility in the vacuum jacketed fill hose resulted in the system as designed proving difficult to operate and causing several trips of the fill valve during the process of connecting the hose for a normal filling operation. During the audit, the cable actuator was found to be inoperative due to an unsatisfactory mounting and leverage arrangement on the three way valve. The system was subsequently modified to ensure correct operation.

Trailer Stop Bar

A concrete block normally engages the wheels of a trailer and prevents reversal into the loading point when positioning before filling. It is normal practice to fill competitors' trailers at the site, as well as those operated by Air Products. The fact that different types of trailers were using the loading system rendered the original positioning of the block inoperative from a protection viewpoint and a modified location was proposed. During the audit the blocks were found to be unsecured, providing no permanent protection of the loading point against a reversing trailer. Correction of this problem is in progress.

The latter two items are good examples of design provisions which were later found to be only partially complete after the plant had been handed over for normal operation.

ANALYSIS OF OPERATING INCIDENTS SINCE COMMISSIONING

Hydrogen Compressor Purge Valve

A 2 inch purge valve on the discharge of the hydrogen liquefier recycle compressor suffered a yoke failure during normal operation

with the valve in the closed position and the system at a pressure of 63 bar. The sudden opening of the valve created a sonic pulse in the vent header downstream of the valve. The reactive force from the vent discharge tore the header from its supports and turned the pipe outlet downwards into the compressor area. The venting hydrogen gas ignited causing considerable fire damage.

Observations

- The valve failed due to stress corrosion cracking in the yoke bushing. The bushing had been supplied in a different material from that originally specified.
- The vent was modified late in the project following a recommendation from the safety audit team to increase the stack height to reduce radiation at ground level in the event of a vent ignition.
- The supports for the modified stack proved inadequate for the reactive force when venting occurred.
- The subsequent investigations recommended the installation of dual isolation valves and highlighted an inconsistency in the hazard review process. The hydrogen liquefier section of the process was a repeat of an existing design, previously subjected to a HAZOP study, whilst the purification, storage and trailer fill areas were covered by the new HAZOP study. The latter recommended dual isolation valves on high pressure (>40 bar) circuits which should have reduced the potential for the event.
- Subsequent hazard reviews on similar systems recommended single valves with blinds. The valves are only used for purging at low pressure, with the compressor off line, and the blinds are changed under work permit control.
- The resulting fire from the valve failure caused extensive damage to cables linking control and trip circuits. This highlighted the need to pay careful attention to the location, routing and fire protection of critical instrumentation and circuitry at the design stage of a project.

Lessons Learned From The Incident

- There is a risk of inconsistency where HAZOP studies are applied piece meal or where projects are repeated.

- Late design changes require special vigilance to ensure the recommendations of the HAZOP study are not compromised.

- A simple design change can often eliminate the hazard more effectively than adding more costly and complex protection.

General Plant Performance

A summary of all plant interruptions is given in Table II with safety related issues highlighted. It should be noted that the facility is subjected to energy management planning which introduces shutdowns during peak electrical demands for the area. This places higher demands on the protective systems than those experienced with the original liquefier in the USA. We believe that the low incidence of failures and operating problems reflects the diligence of the Hazard and Operability studies and subsequent monitoring.

CONCLUSION

It is recommended that the following actions are adopted after the initial start-up as an extension to the normal HAZOP functions:

A post-commissioning audit (as per Section 8).

Clear and positive identification of critical safety systems by:

- Highlighting of critical safety circuits and devices on flowsheets by colour printing, special symbols or other means.

- Highlighting appropriate sections on subordinate documentation such as instrument loop diagrams, analyser schedules, instruction manuals and preventive maintenance documentation.

- Formal transmission of preventive maintenance requirements from the hazard review team to the operator together with instruction that no changes are permitted without management approval.

- Positive feedback of defects and failures of components during operation, shutdown or proof test. Such information must be checked against fault tree quantification criteria or HAZOP recommendations.

- Field identification - Safety devices and equipment may be of distinctive colouring, tagged or sealed.

- Where critical maintenance activities of an infrequent nature are to be conducted (e.g. replacement of bursting discs on the liquid hydrogen storage tank) the use of notices, posted adjacent to the equipment, should be considered to remind personnel that special procedures must be observed..

As has been indicated in this paper the HAZOP activity does not cease after the commissioning phase. It is essential that the plant operator is continually aware of the significance of recommendations arising out of hazard studies which were devised to prevent or mitigate the consequences of potentially hazardous events. Only by constant vigilance with respect to the maintenance of safety systems and the interchange of information relating to incidents or failures can we feel confident that the facility hazard review will be meaningful during the operating life of the plant.

References

"Premises for Risk Management" - an annex to the Dutch National Environmental Policy Plan, 2nd Chamber of the States General, 1988 - 89 Session, 21137 Nos 1 - 2.

FIGURE 1
FAULT TREE FOR
LIQUID HYDROGEN STORAGE SPHERE
OVER PRESSURE RELIEF PROTECTION SYSTEM

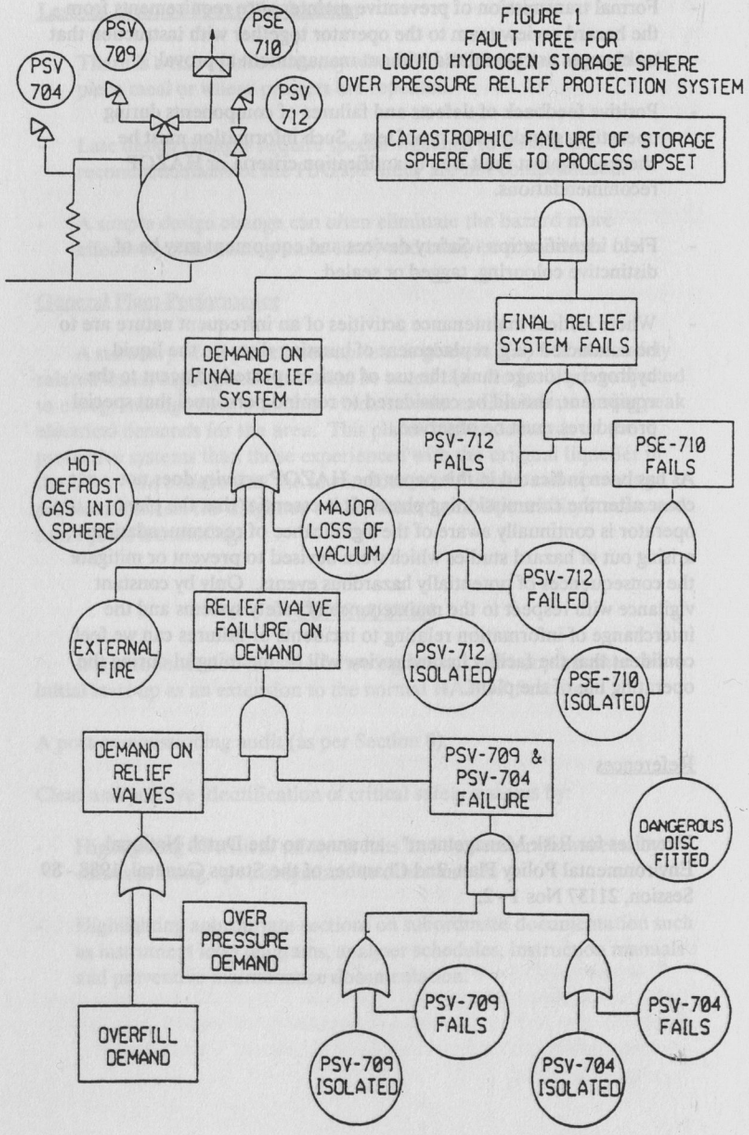

FIGURE 2
GROUP RISK LIMITS FOR MAJOR ACCIDENTS (1)

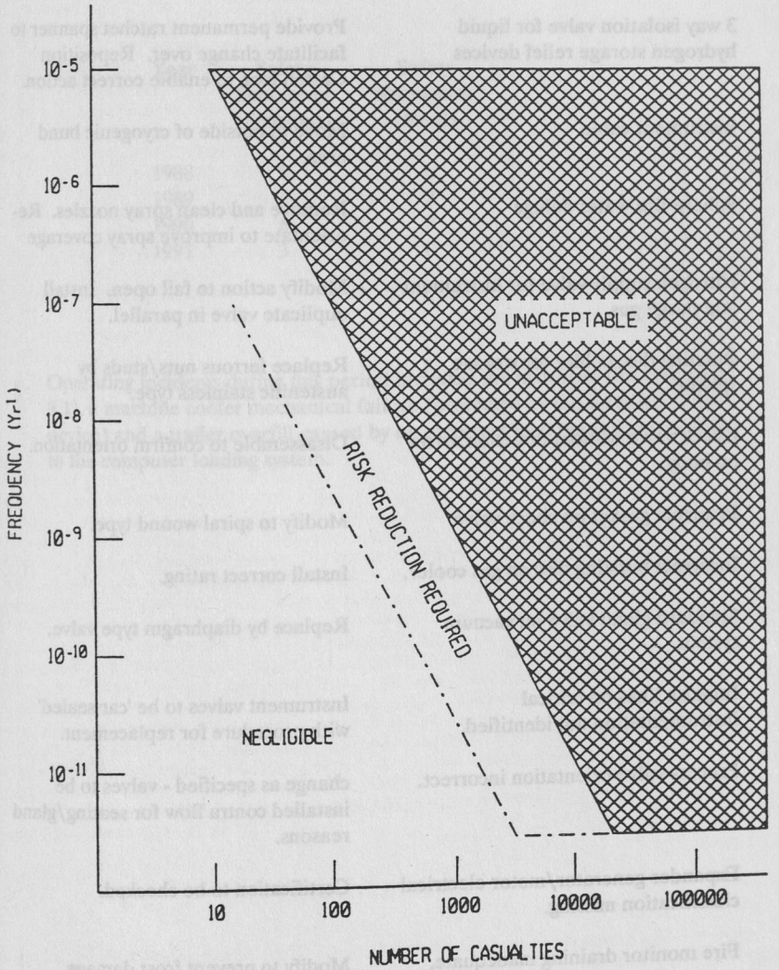

TABLE 1
SAFE TO OPERATE VERIFICATION
Examples of Key Items Found

COMPONENT	CORRECTION REQUIRED
3 way isolation valve for liquid hydrogen storage relief devices	Provide permanent ratchet spanner to facilitate change over. Reposition Castell lock to enable correct action.
Instrument cable	Move to outside of cryogenic bund area.
Sphere fire water deluge	Remove and clean spray nozzles. Re-orientate to improve spray coverage
Nitrogen supply valve for instrument and purge gas.	Modify action to fail open. Install duplicate valve in parallel.
Bursting disc holder for storage sphere	Replace ferrous nuts/studs by austenitic stainless type.
Check valve without direction arrow on body.	Disassemble to confirm orientation.
Incorrect gasket on check valve.	Modify to spiral wound type.
Incorrect bursting disc on gas cooler.	Install correct rating.
Standard gland valve on vacuum system.	Replace by diaphragm type valve.
Impulse lines on critical instrumentation not identified.	Instrument valves to be 'car sealed' with procedure for replacement.
Process valve orientation incorrect.	change as specified - valves to be installed contra flow for seating/gland reasons.
Expander generator/motor electrical classification missing.	Certification to be checked.
Fire monitor draining inadequate.	Modify to prevent frost damage.

TABLE II

SUMMARY OF OPERATING INTERRUPTIONS

Year	Safety Shutdowns (Spurious)	Safety Shutdowns (Real)
1988	0	0
1989	6	2
1990	6	3
1991	3	0

Operating incidents during this period included the hydrogen fire (see para 9.1), a machine cooler mechanical failure (protected by the installed relief device) and a trailer overfill caused by an incorrect load being input as data to the computer loading system.