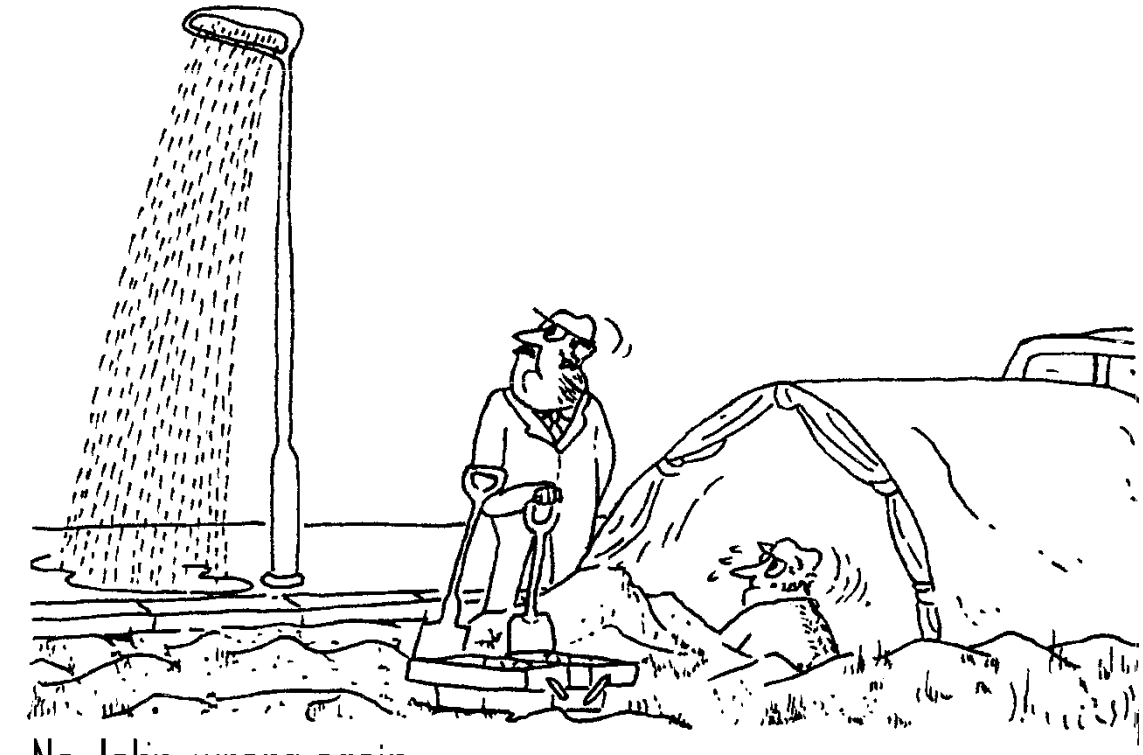
Part H

HISTORIC INCIDENTS THAT ILLUSTRATE THE BREACHES IN DEFENCE IN DEPTH

Incident Studies and Illustrated Safety Teaching Examples for ChemEngers



Safety is no more that the application of "O" and "A" level physics and chemistry. Most, if not all of it is known already but not applied in the right manner. (FKC)

Incident studies must not be used in isolation from the basic "safety fundamentals". They are, for the most part illustrative of "***management failures***" but the outcomes of these failures must be discussed and reference made to the "risk".

In some cases the problem may appear to be a risk to humans (for example a dripping pump seal) but if the drip is only water the risk is zero! In some cases it might be the risk to the environment.

All activities require an analysis of the potential risks (***Risk Assessment***) and then the residual risks and potential mitigations must be assessed properly! Many Risk Assessments will be "qualitative" (as in a permit to work) and not "quantitative" in nature asking:

"**How can we eliminate the "risk" and if we can not eliminate the risk how can we mitigate the risk**?"

The following set of "incident studies" for use in the Safety Courses in University Schools of Chemical Engineering do not describe the "risk", this MUST be assessed separately. The main features of the analysis should centre on the Corporate Management Systems.

As a generalisation most incidents are the result of:

1. Didn't think of that!
2. Poor understanding of the risks.
3. Poor risk assessment.
4. Not understanding the physics and chemistry!
5. It could not happen to me!

Is 2 to 5 a repeat of the first entry?

The tutor can use these incidents as teaching tools (and there are some cases which fall into this category) or to ask the class to be a part of the incident investigation with the tutor answering any questions raised.

The studies have a number of elements: the **word picture** of the incident, **possible questions and answers** that can be directed to the students, **background** which may be essential to the understanding of the issues – this can be given as part of the incident and finally the **teaching points** which are the main thrust of the studies and must be emphasised by the tutor.

Analysis of incidents can be used to teach simple engineering, the human factors and also the interaction between engineering disciplines.

All of these incident studies are as they occurred or with some **VERY** minor details changed to disguise the "guilty" party. These changes **DO NOT** affect the conclusions or the final messages.

Caveat with Videos

Some of the BBC videos and the CSB illustrations must be reviewed critically if used during a teaching course. It is necessary to ask "what are the teaching points?" And "is it true and relevant to the UK culture/regulatory system?"

In the case of the BBC "Disaster Series" some of the facts as displayed are in error, so much so that the real messages and conclusions may be erroneous if these errors are not recognised or corrected. Likewise the cultural and regulatory differences between USA and Europe as in the CSB animated videos must be recognised.

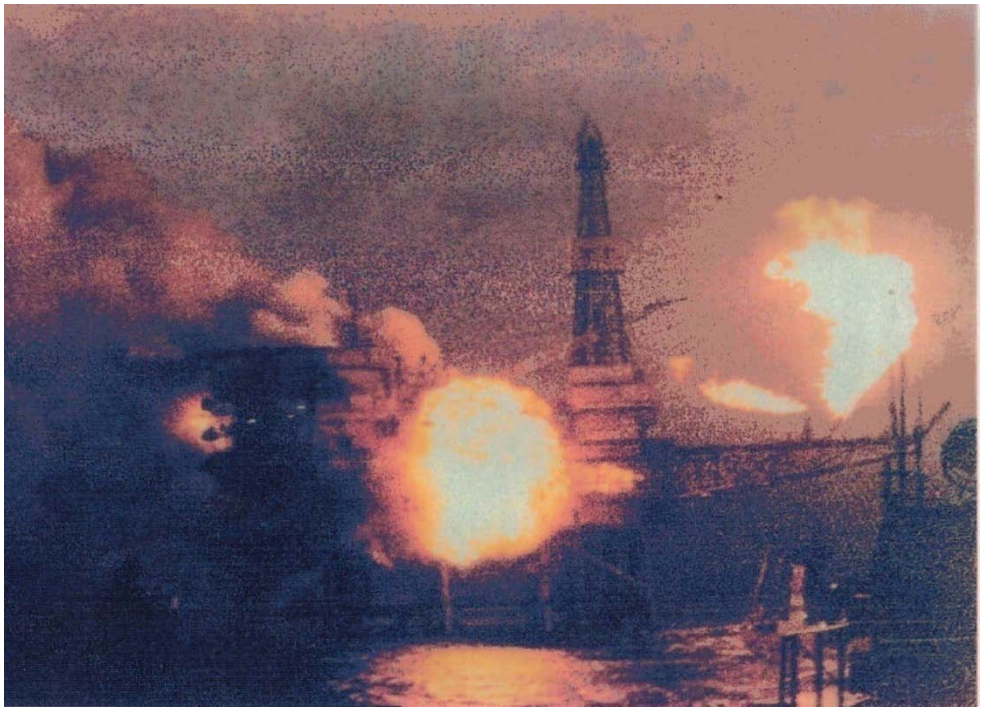
These issues are now highlighted:

Piper Alpha (BBC)

- The support jacket was designed against the Gulf of Mexico wind/wave profile. The N Sea is different and the jacket suffered from early fatigue failures (5 years against a life of 50). Some VERY elegant bracing was installed which over came the problem.
- The original design intent was that the production area would be naturally ventilated by it being open on 3 sides.
- Shortly after the fatigue analysis the then Regulator, D of E, issued a SI concerning the irrigation rate on equipment in a fire. This required more firewater pumps which would increase the fatigue loading or require fire zoning with fire walls. The latter approach was adopted but it violated the

design intent. (Caught between a rock and a hard place). NOTE fire walls NOT blast walls as said by T Barrell.

- The need to inhibit the fire pumps with divers in the water is a bit of a myth. In a HAZOP which I facilitated the "as well as fire water" answer was "a diver". So the inlet was fitted with a bell mouth with inlet velocity of 0.5 m/s and catcher bars.
- There **WAS** an Emergency Isolation on the Oil export riser! Did it work or was it damaged by the initial explosion?
- Oil in a pipeline is compressible and the pipe line expands under pressure. The result is a stored amount of oil called "line pack". The line pack was about 50 te, the liquid fire was equivalent to about 20 te/hr so even if Tartan was shut down the oil (if it was oil) would still ooze past a valve.
- There **was** an alternative source of liquid fuel in diesel oil (for the gas turbines) which was stored in the production module roof. The handling pumps were close to the compression/production module fire wall.
- There is at least one photo showing the BLEVE of what was probably a propane bottle, stored in the production module. Some of the BLEVE can be seen entering the well head module – that is the firewall between the production and well head modules was damaged. If that wall was damaged could not some of the diesel oil piping be damaged?
- There was some discussion on the need to have the injection pump on line "or else the power gas turbines (GTs) would shut down". The design of the fuel supply to the GTs is that there is a continuous change-over from gas to diesel and reverse – it has to be so!



Conclusion

Don't let the facts get in the way of a good story!

Texas City (CSB)

- There are cultural and regulatory differences between USA and UK. As an example the storage of Ammonium Nitrate in UK is covered by COMAH. It was not covered by OSHA Process Safety Management in USA. Hence the explosion in West, Texas. It is covered now but too late.
- The vent arrangements in TX City complied with American Petroleum Institute Recommended Practices (API RP). They would NOT be acceptable in UK.
- The position of the Pressure Relief Valves (PRVs) was at the BOTTOM of a "swan neck". This facilitated the removal of the PRVs but ensured that the imposed hydrostatic head following the internal roll-over in the fractionator would prevent the PRV closure.
- The best location for the PRVs would be exit the reflux drum which would then act as a liquid interceptor. The root causes were bad supervision, bad engineering and bad training or procedures. Quite a list!!!!
- There were many other features as described by CSB.

Conclusion

The TX City event does not readily transfer across the pond because of the engineering, cultural and regulatory differences.

It is an excellent incident for examining the plant design (more particularly the piping) in three dimensions, not normally analysed well in a HAZOP which treats it as two dimensions!

The following incidents are used to illustrate the role of Management (or lack of Management) and design faults in the build up to major incidents. Three incidents are used:

FLIXBOROUGH

PIPER ALPHA

CHERNOBYL

The Texaco Refinery Fires can be accessed through the LPB obtainable from the Institution of Chemical Engineers. It highlights the problems with training and information overload**.**

LPB 104 contains an analysis of the Sevesco incident which resulted in the production of Dioxane. It is possibly a bit too elegant for teaching purposes.

These case studies are not meant to be critical, in any way, of the asset owner. They are only there to illustrate that failures in the "***defence in depth***", that they occurred slowly and may not have become manifest for a number of years. For example some of the defences at Flixborough were eroded some years before the event but the erosion was not recognised. If there had been regular Audits it may well have been that these failures would have been rectified and that the explosion would not have occurred.

Try to project yourselves into the Flixborough environment where energy costs were rising rapidly and cost saving was essential for a viable future. Would you have been able to recognise the implications of the reduction in staff numbers and competence and could you have resisted it?

Flixborough 1974

Background

The precursor for the production of nylon is cyclohexanol/cyclohexanone which is produced in a series of continuously Back Stirred Reactors between 4 and 6 in number. The reaction is carried out by the reaction of Cyclohexane and Air in the presence of a cobalt catalyst at conditions of about 150^{o}C and about 900 kPa. Air is injected under the liquid and dispersed by an agitator moving at about two revolutions per second. The conversion is about 3 to 5% so about 97 to 95% of the cyclohexane per pass has to be distilled off and recycled to the feed point. The reaction produces acid by-products so the vessels are usually made in Stainless Steel or Stainless Steel Clad vessels. The reactants are also quite aggressive and attack the jointing materials.

The site layout is shown in Fig A before the event and in Fig B as an actual view after the event. The process is shown in Fig C, it will be noted that reactor 5 is bypassed. The area and the site were rural and there was the usual application of fertiliser and nitrate run off into the ground water and river. The nitrate run off was not fully appreciated by the work staff. This is a feature of the ground water which played a major role in the lead up to the final explosion.

The Incident

Cyclohexane is a solvent and dissolves the binding agent in the conventional gasketting agents. There was a general acceptance that leaks in the process were inevitable so the occurrence and the remedy were treated as ***'custom and practice***' and there was little investigation into the potential consequences. It was standard practice to spray water onto the joint with the intent of condensing / dispensing cyclohexane. (This was standard practice but a little analysis of the dispersing mechanisms would suggest that condensation of the vapours was probably not affected but that the bulk air movement induced by the sprays was beneficial, not to mention the explosion suppression benefits of the water mist.)

Unknown to the operating team the water contained Nitrates. The management systems at that time were not ideal and were evolving; "***Management of Change***" was definitely in its infancy. (Large companies such as ICI had a form of Management of Change, which relied on experience and professional ability.) The management structure on the site at Flixborough lacked a qualified mechanical engineer, the mechanical engineer had moved to a new job as part of the cost cutting exercise and there was no perceived need for one as the engineering was fairly "run of the mill" after a period of steady operation. By now there were at least six breaches in the defence.

A few weeks before the event, a leak was found in reactor 5 and after initial examination it was decided to remove the vessel for more detailed examination. (A photo, which does not print well in the final report, shows the reactor with a long vertical “coupon” about 25cm wide by 1 m long. The coupon was along the line of “hoop stress” starting at a stress raiser, a nozzle on the vessel, this is indicative of stress corrosion cracking). The process was considered to operate safely with only 5 of the 6 reactors but at reduced rate / conversion per pass. At least one successful start up with the new piping configuration had taken place prior to the final event.

The original piping between the reactors was bellows units - in a horizontal line as shown in Fig C.

Each step was about 1 to 2 feet vertical drop, which accounted for the hydraulic gradient (See Fig C). A simple - non-engineering analysis suggested a "***dogleg***" could be fitted with the bellows to account for differential thermal growth during start up. This was quickly engineered and scaffolding used to support

the bellows (See Fig D). No mechanical analysis was carried out but the forces/moments show an oblique off-centred bending movement (Fig D). (This can be illustrated by rolling a sheet of paper into a cylinder and then applying an axial load before applying an offset load or bending moment.) By now another two defences are breached. The plant had operated for a few weeks, but during a start up on the day in question, for whatever reason, (and many have been proposed with hind-sight), the bellows rotated, the scaffold collapsed and the bellows tore out. Cyclohexane now rushed out of two 20" holes at a rate of more than one tonne per second.

The wind was in such a direction that the cloud was driven back into the plant where it ignited - that actual source is open to debate but is believed to have been the Hydrogen Plant where there were fired furnaces.

The explosion that followed was estimated to be equivalent to 16 tonnes TNT. There is some good evidence that there were two explosions close together. The resultant fire reduced the site to a state requiring total demolition and rebuild. Off site there were no deaths but significant damage to local housing.

It is now worth looking at the breaches in the defence in depth and the timing of that breach given as [ ].

Breach 1

The plant layout was congested. The potential for a vapour cloud expression were not appreciated and the control room was located close to the process plant. [Design]

Breach 2

The specification of the joints was not ideal and joint failure (loss of containment) was quite common. Better joints were available but were not used due to poor specification and/or engineering application. [Design and operation]

Breach 3

Following leaks it was normal practice to spray water (water containing nitrates) onto the shell of the reactors this resulted in stress corrosion cracking of the shell. Following inspection reactor 5 was removed as the shell was cracked. The appreciation of the potential for stress corrosion cracking was not understood nor were the implications of cracking appreciated. [Start-up]

Breach 4

The process had not been subject to a formal HAZOP process during design so the potential for leakage/metallurgical damage was not recognised. [Design]

Breach 5

The management structure on the works did not contain a fully trained and experienced Mechanical Engineer. [Some time before the event due to cost cutting] (In fairness the HAZOP technique was still in its infancy)

Breach 6

There was no formal Management of Change Procedure was in place on the site. [Some time before the event but MoC was not a developed management system].

Breach 7

The bypass was engineered but with breach 4 and breach 5 the full implication of the modification were not appreciated. [Months before the event as there had been at least one successful start up with the bypass]

Breach 8

The bypass shown in Fig D was designed as a dogleg containing a pair of bellows to take up thermal expansion. The support of the bypass was not engineered properly and the forces on the support and the bypass were not analysed. Fig D shows the bending movement / shear force diagram. Fig F shows the remains of the plant close to reaction 4/6.

It can be seen that some of the breaches were on place from the design of the plant - Breach 1, 2 and 4. Others occurred later in the life of the plant - Breach 3 and 5. Breach 6 was organic and may have been in existence before the plant was designed. Breach 1 was also organic but also occurred before the plant was designed. Breach 7 and 8 occurred just before the incident.

Breach 9

The wind was in the adverse direct such that the vapour cloud was blown back onto the plant where it exploded.

Analysis

There were engineering, management, design, and supervision of workers, which lead to a systematic breach of defences in:

Procedure

Equipment

Training

Supervision

On the 1st July 1974 there was a massive explosion, which killed 28 persons.

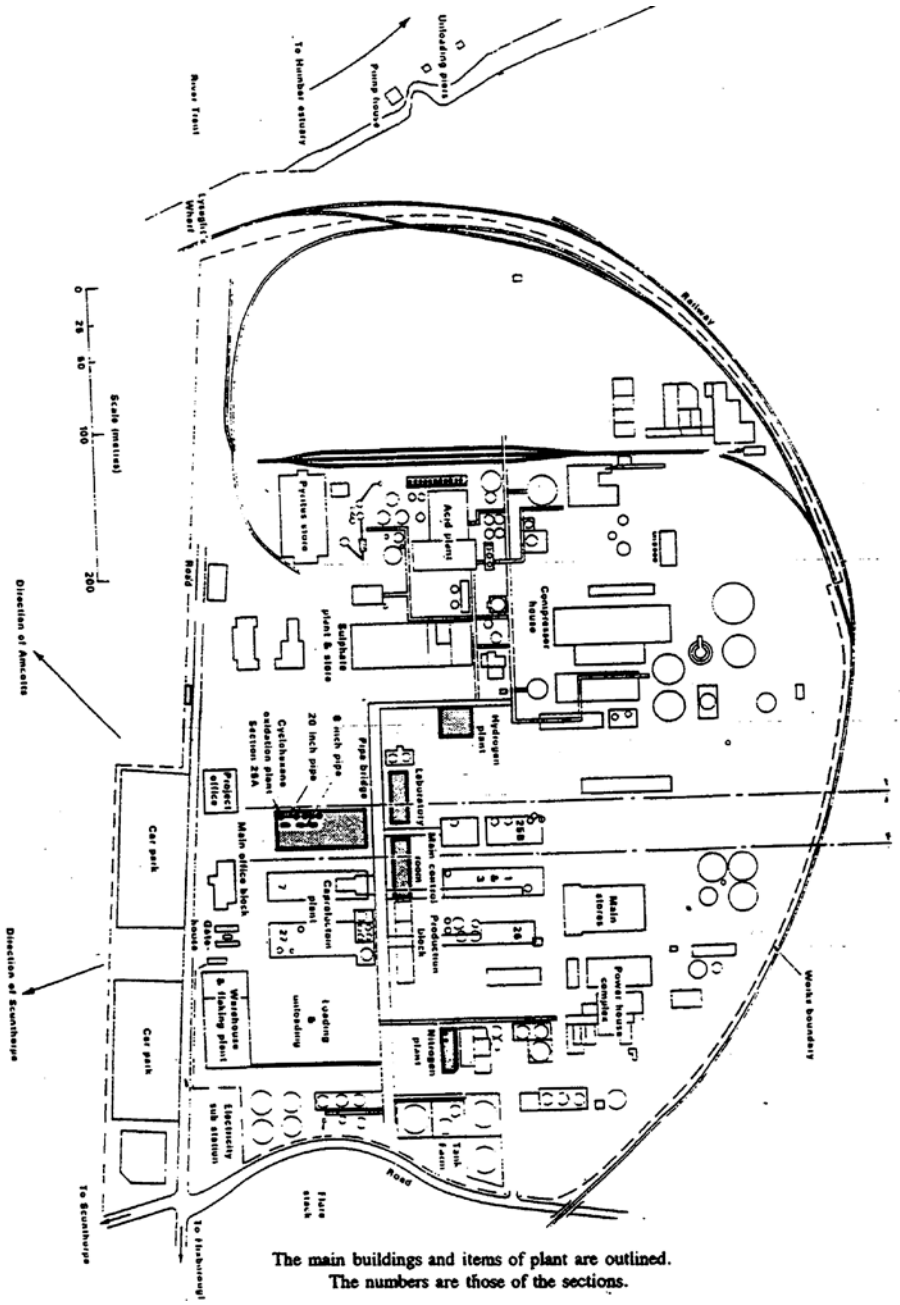


Figure A. Simplified site plan of the works of Nypro (UK) Ltd at Flixborough

Figure B Site after the fires were extinguished

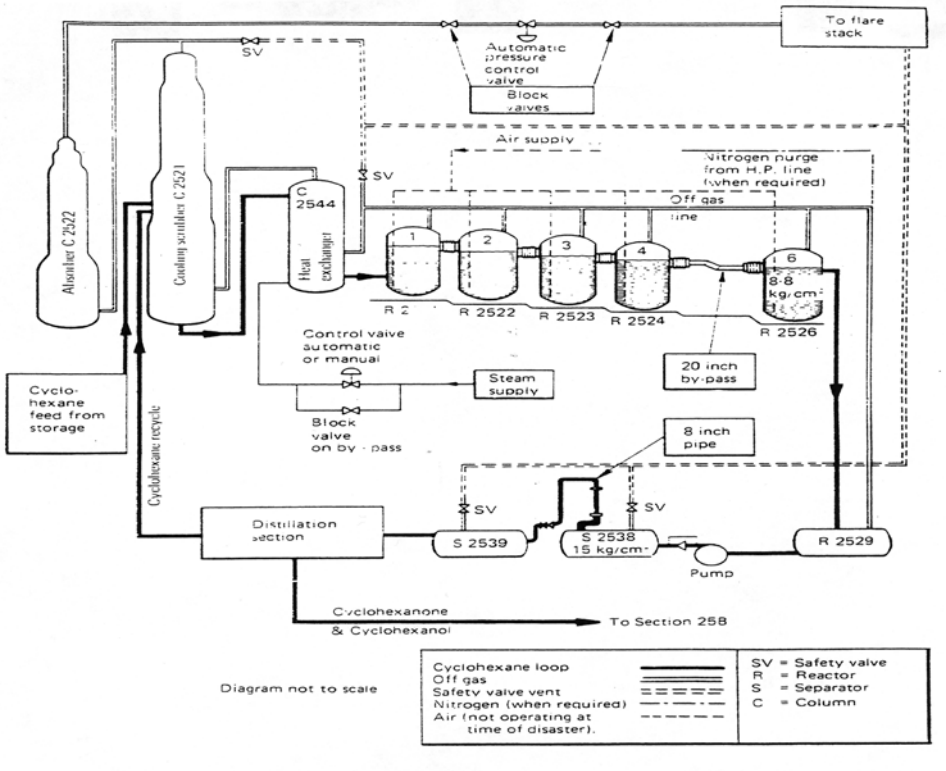


Figure C Simplified flow diagram (not to scale) of the cyclohexane oxidation plant at Flixborough

One photo, which does not copy well, shows the removed reactor with a vertical, thin metallurgical coupon taken from below a nozzle. This is indicative of a stress corrosion crack along the hoop stress line.

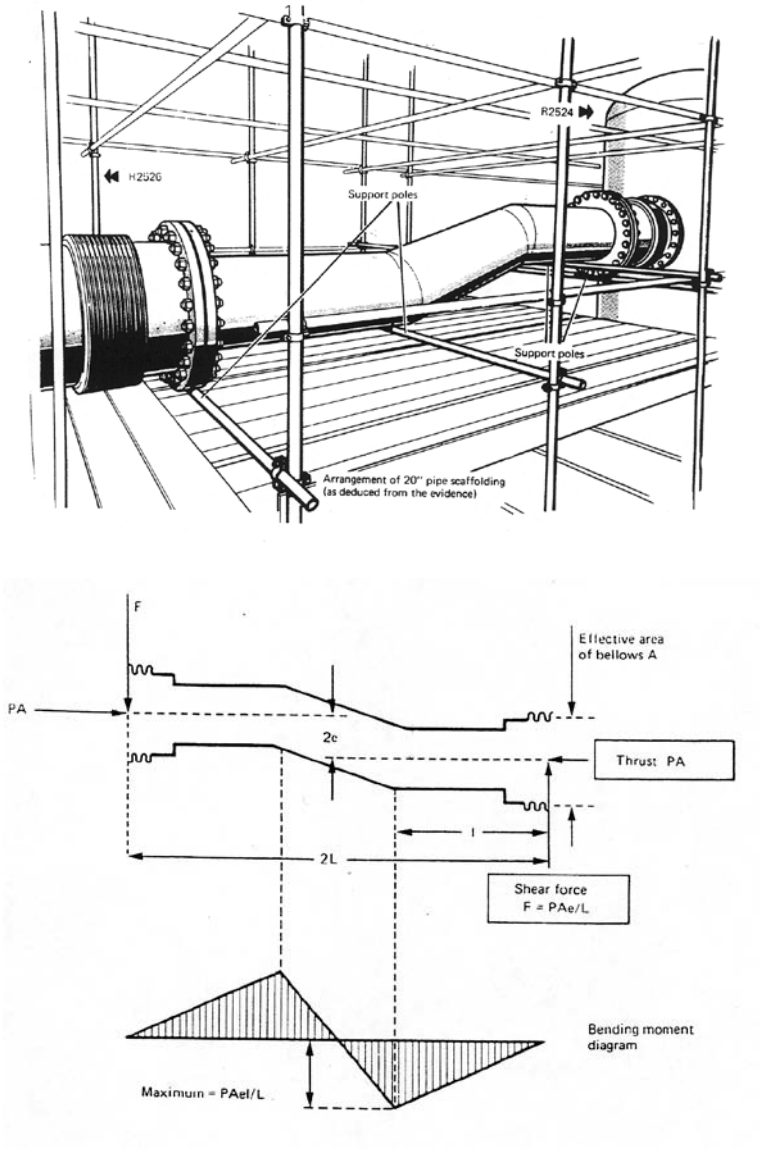


Figure D Sketch of pipe and bellows assembly at Flixborough showing shear forces on bellows and bending moments in pipe (due to internal pressure only)

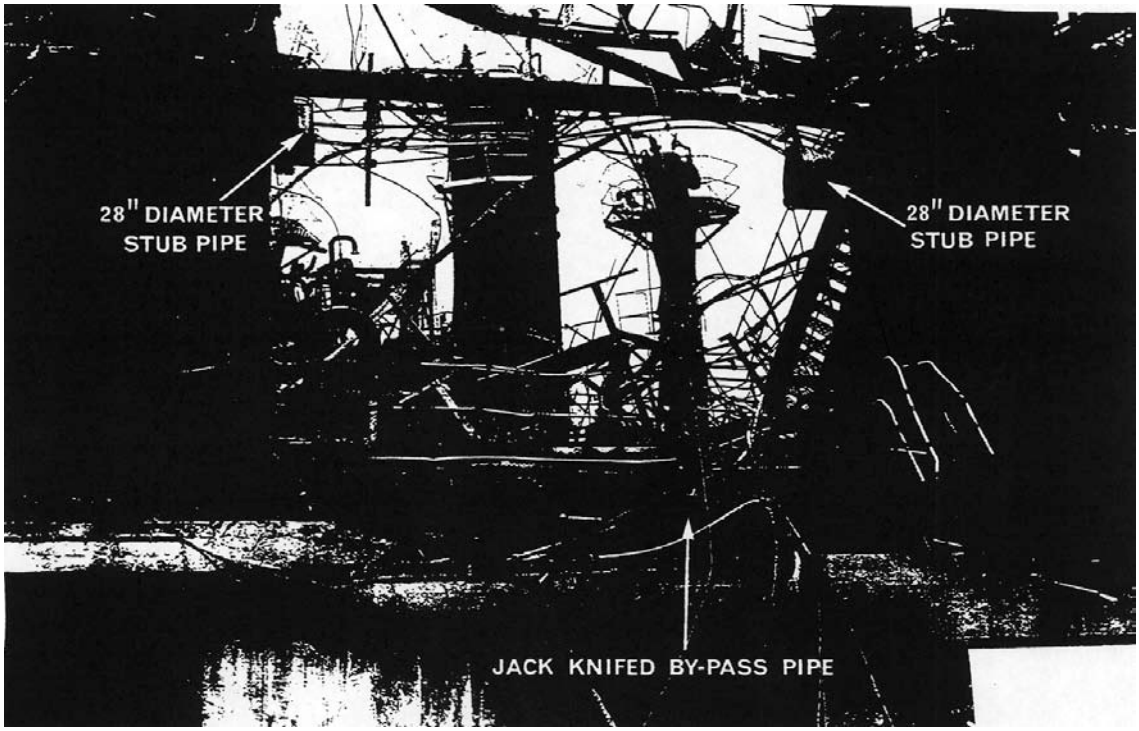


Figure E Reactors No 4 and 6 and the bypass assembly at Flixborough after the explosion

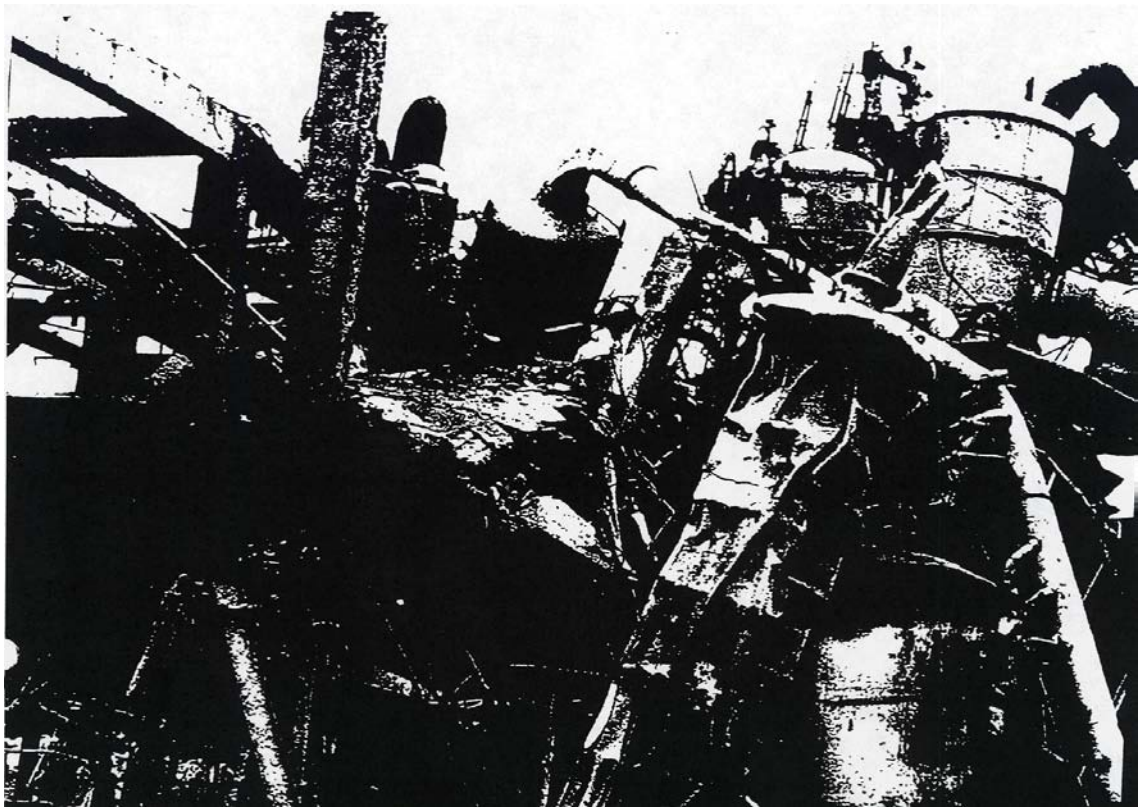


Figure F Area Damage. Note the internal collapse of a distillation column. Was this caused by the initial explosion?

Piper Alpha

Background

The offshore oil production is relatively simple. Oil in the reservoir is a mixture of hydrocarbons in the liquid phase under high pressure of at least 5M Pa. They contain Methane, Ethane, and Propane and extend to high molecular weight molecules with boiling points well over 300^{o}C. The oil is flowed into a separator at about 1M Pa where some of the lighter components come out of solution (degas). The liquid phase is let down into other lower pressure vessels where other gases are released. The gases from the various separators are compressed, cooled and any condensate is recycled into the separators. The main, primary product from the installation is oil with a vapour pressure of about 500 kPa; this is pumped by pipeline to the shore where it is further processed to produce oil, which can be transported by tanker. The secondary product from the installation is gas from the compression cycle above, which is further compressed and flowed into a pipeline to the shore where it is further processed to produce commercial domestic gas and LPG. In simple terms the offshore platform separates a mixture of hydrocarbons ranging from Methane to tars into a gas, which is mostly Methane and some Ethane, and a liquid, which contains Propane and heavier hydrocarbons plus some Ethane.

The process flow diagram for the High Pressure section is shown in Fig A. There are gas connections to Tartan, Claymore, export for gas to MCPO1 and hence to **Saint Fergus** and for oil to the **Flotta** terminal on the Orkneys (Fig B).

The design of the platform is somewhat congested and evolved as the legislation in the UK offshore processing industry evolved. The following is a personal view, which cannot be fully proved as some of the evidence is at the bottom of the North Sea. The analysis of the breaches is based on both Lord Cullins' enquiry and experience of the offshore industry plus the sister platform (Claymore). Some of the breaches are not fully proven but they are entirely probable.

Further information is given. At about 500^{o}C steel has very little strength and it becoming plastic. The products of combustion of oils in a poorly ventilated area produce about 5% v/v carbon monoxide and humans lose consciousness when they are exposed to a dose of about 50,000 ppm mins carbon monoxide. (10,000 ppm for 5 minutes, or 1000 for 50 mins).

The layout of the Piper Platform is shown in (Fig C_1/C_2). Module A contains the wells from which the hydrocarbon flows into module B where there are the separators. Module C contains the compressors and pumps, which handle "condensates", a mixture of Methane, Ethane and Propane. These condensates are injected by reciprocating pumps into the oil before it flows to the Flotta Oil Terminal on shore. The oil pipeline passed down under module B, the master oil isolation valve was located under module B. The pipeline then passed under Module C and the accommodation before passing down to the sea at the edge of the platform. The Master gas isolation valve on the gas pipeline is also under Module B and C. The gas pipeline passes under module B and down to the sea under the Accommodation Module.

Diesel Oil, which is used to fire the Gas Turbine power generators, is located in the roof area of Module B. [Fig C_1]

The accommodation block is in Module D and had been extended over the years.

The Incident

There were many breaches of defence before the incident. These range from procedure to training.

The original design intent was for an open platform, which would be naturally ventilated by the wind. This was changed into 3 compartments as a result of changes in legislation. Isolation standards were poor - normally valves are closed, locked and in some cases slip plates (line blinds) are fitted. On Piper some air operated valves were closed thereby giving a poor indication of status (open or closed).

Various extensions had been carried out on Piper Alpha over the years and the accommodation had been extended as well.

Above the Module B was a Diesel Oil tank just like car diesel fuel - which was used to fire gas turbines. The process modules were compact, if not congested. The pipelines to the shore **HAD** emergency isolation valves (see Fig D).

During the enquiry there was much discussion about the Fire Pumps being isolated due to diving operations. This is a potential red herring as the explosion would have probably damaged the fire water system, in any case it would probably have been of no benefit in mitigating this event.

The permit to work system and handover were not well administered and training for and handling of emergencies was poor.

During the morning shift of the day the event occurred, Pumps 2G-200A was handed to maintenance for an overhaul on its relief valve [Fig E & F]. (Note there is a labelling error on Fig E). A blank was loosely fitted at point X. The pump was isolated by two gas operated valves (GOV (1) and (2)). These were valves which were operated by a pneumatic cylinder and hence difficult to inhibit or lock in position. It would be easy to reopen the valves as no label or positive isolation was applied. At about shift change G.200 B shut down (tripped) and an operator was asked to re-start up the pump but this proved difficult. After a short time the permits on the A pump were signed off and the A pump started up. This is to be found almost true centre of Fig F. The pre-start up checks were omitted due to the urgency of the re-start. Either due to process pressure or a loosely fitting blank condensate sprayed out at about 2 kg/sec. Due to the poor ventilation a large flammable cloud was formed - many gas detectors recorded this. After about one minute there was an explosion - the ignition was probably static but it could have been electrical. About 100 kg of fuel were burned in a fraction of a second. The fire wall between Modules C and B and B and A was breached - the fragments becoming missiles which individually or with dynamic drag loads damaged instruments on smaller piping. One small line 2 P 517.4" -F15- second down from the top left hand side in (Fig G) is of note - it carried condensate to the oil line and was particularly vulnerable and could have been damaged when the fire wall blew out.

Emergency valves may have closed, may not have closed, and may have been damaged - this is not really important, as they were probably located in the wrong place anyway. The resultant fire consumed fuel at a rate of about 8 kg/sec. Some fuel ran down below module B and heated up the pipelines (see Fig C). Eventually the Tartan Gas Riser ruptured due to fire assault and a fireball about 50 to 75 m diameter enveloped the platform. The initial gas overflow from the ruptured line was many tonnes per second but rapidly fell to about 100 kg per sec over half a minute. This fire lead to the collapse of the platform and/or rupture of the other pipe lines.

The following is an analysis of the significant breaches in the ***Defences in Depth*** with the approximate timing of the breach shown as [ ].

Breach 1

The original design intent was that the whole of the Module A, B and C would be open and ventilated by the air/wind but in the late 1970s new regulations required that the fire water rates would be about 10

litres per minute per m^2 of area within a specific fire area. The fire area was defined by the limits of fire walls. On investigation the available fire water did not match the new requirements so two strategies were possible:-

1. Install new firewater pumps.

2. Install new firewalls.

The latter option was adopted, as new firewater pumps would have adversely affected the fatigue life of the structure which was already challenged. These walls affected the air movement and violated the original design ventilation philosophy for the modules such that gas build up was more likely. [10 years before the event]

Breach 2

There was a door into the accommodation block with access from Module C, this door was normally closed but if left open it would allow fumes to enter the accommodation block if there was a fire in Module C. [Installed some years before the event, but left open on the day of the event]

Breach 3

The permit to work system (safe systems of work – HASWA) was poorly administered. The standard of isolation was poor and it was possible to start up a pump while under maintenance. [Systematic over many years]

Breach 4

The hand over at shift changes was poor and the status of equipment was not clearly described and outlined to the on-coming shift. [Systematic over many years]

Breach 5

The line of command in an emergency was poor. The line for ultimate decision-making in an emergency was not clearly defined. It lay somewhere between the Offshore Manager and the Onshore Emergency Team. [Many years]

Breach 6

The practice of emergencies was poor and only involved small emergencies, further evacuation drills were carried out under non-stressful conditions. [Many years]

Breach 7

The supervision of work was poor and the operations staff had a fairly broad scope for decision-making, (the Standing Instructions were poor). [Some years]

Breach 8

Coupled with Breach 7 there was a general acceptance of lax operating practices and an acceptance that hydrocarbon leaks were a norm and to be tolerated. [Some years]

Breach 9

There were design weaknesses, which predisposed the installation to failure such as piping routing, the location of the diesel oil and others. [Design]

It is of debate that evacuation was theoretically possible up till the point where the Tartan Riser ruptured - this is not proven nor can it be proven. There was some futile discussion about whether other platforms pumping oil into pipelines connected to Piper Alpha should have closed in. In theory the answer is "yes" but in practice it made no difference as it was the gas line, which ruptured.

There was also some futile discussion about the role of the emergency support vessel Tharos. The Captain, by the law of the sea, is responsible for his crew and vessel. Should he jeopardise the lives of his crew? The author has his opinions but will not say more.

Breach 10

The wind direction was in the adverse wind direction such as to hinder escape and drive products of combustion into the accommodation block.

Analysis

There were weaknesses in the design Breach 9. There were weaknesses in the Management Systems Breach 3, 4, 5, 6, and Breach 7 and 8. There was poor management of change procedures Breach 1 and 2.

169 persons lost their life.

A long discussion on the ability to run the power generation in the BBC film is a distraction as in reality the generators are multi-fuelled (gas and diesel oil) with a continuous and seamless change-over between the two. This is not always 100% successful but it is the design intent.

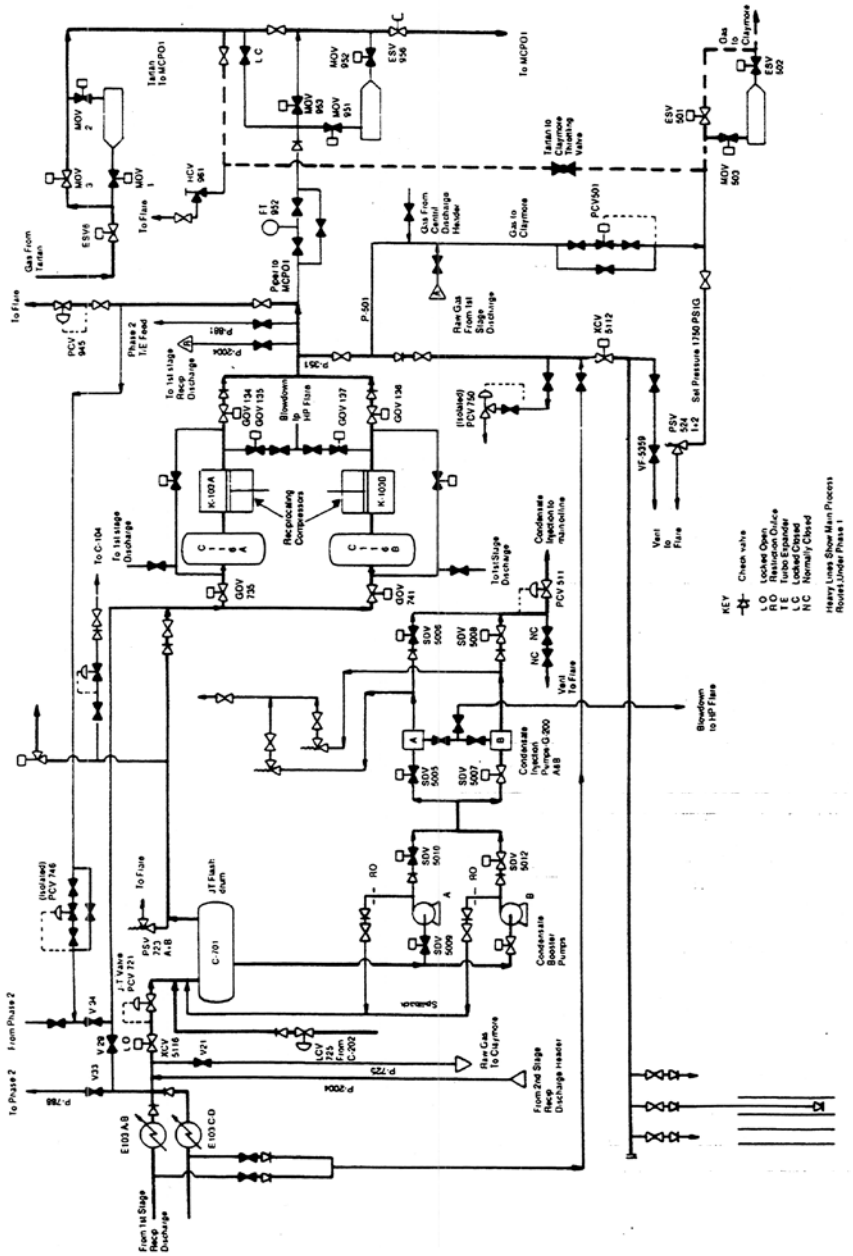


Figure A Simplified flow diagram of the second stage reciprocating compressors and export and gas lift lines.

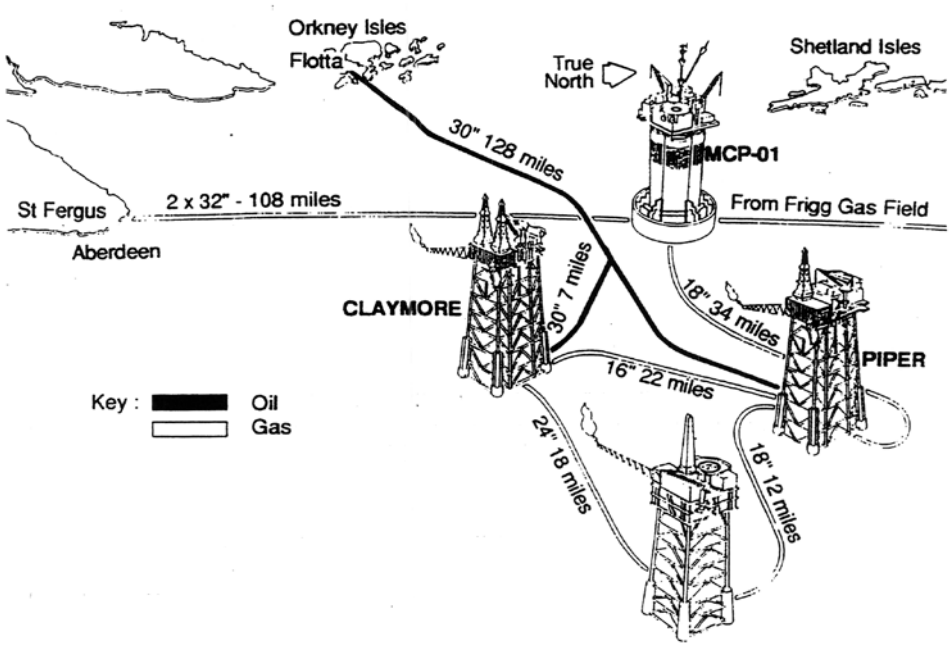


Figure B Pipeline connections of the Piper field

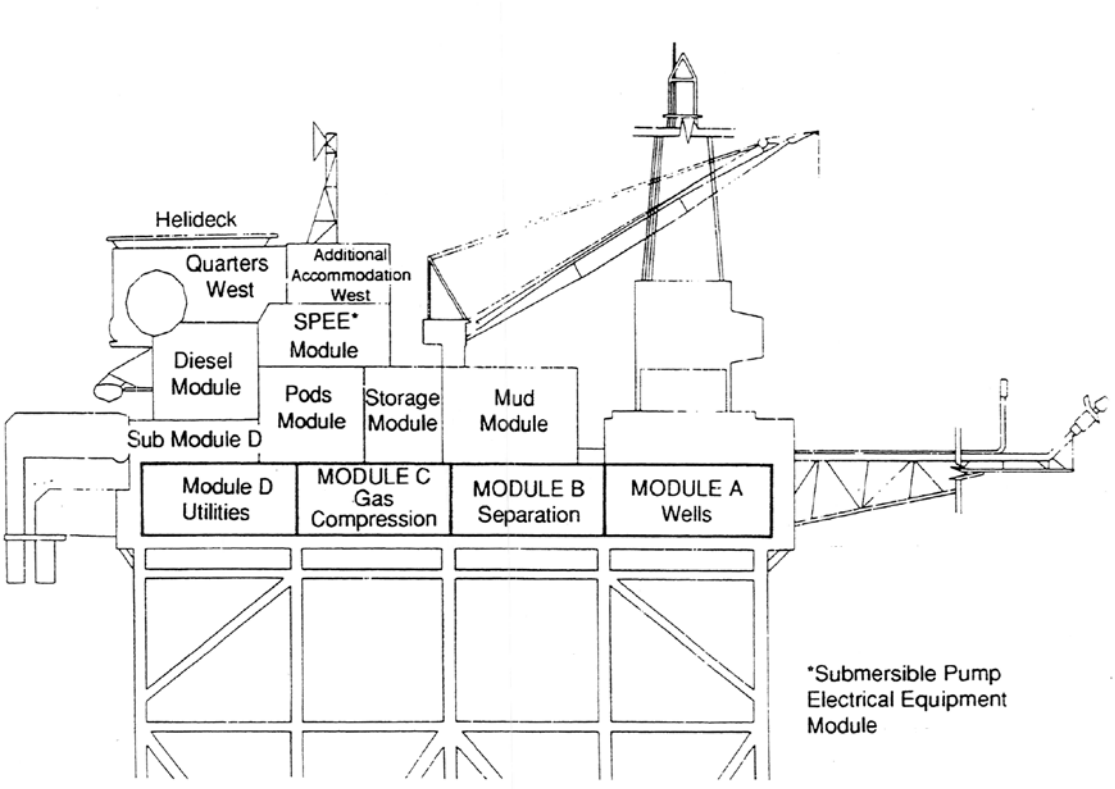


Figure C_1 The Piper Alpha platform: west elevation (simplified)

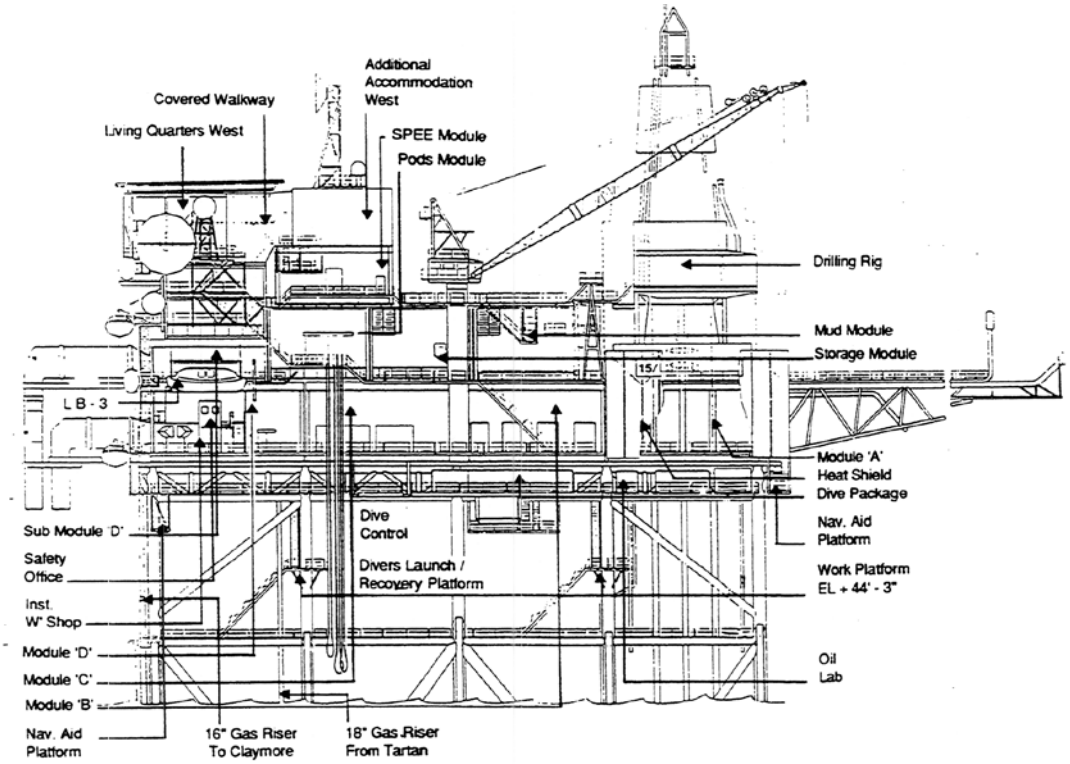


Figure C_2 Piper 'A' Platform West Elevation

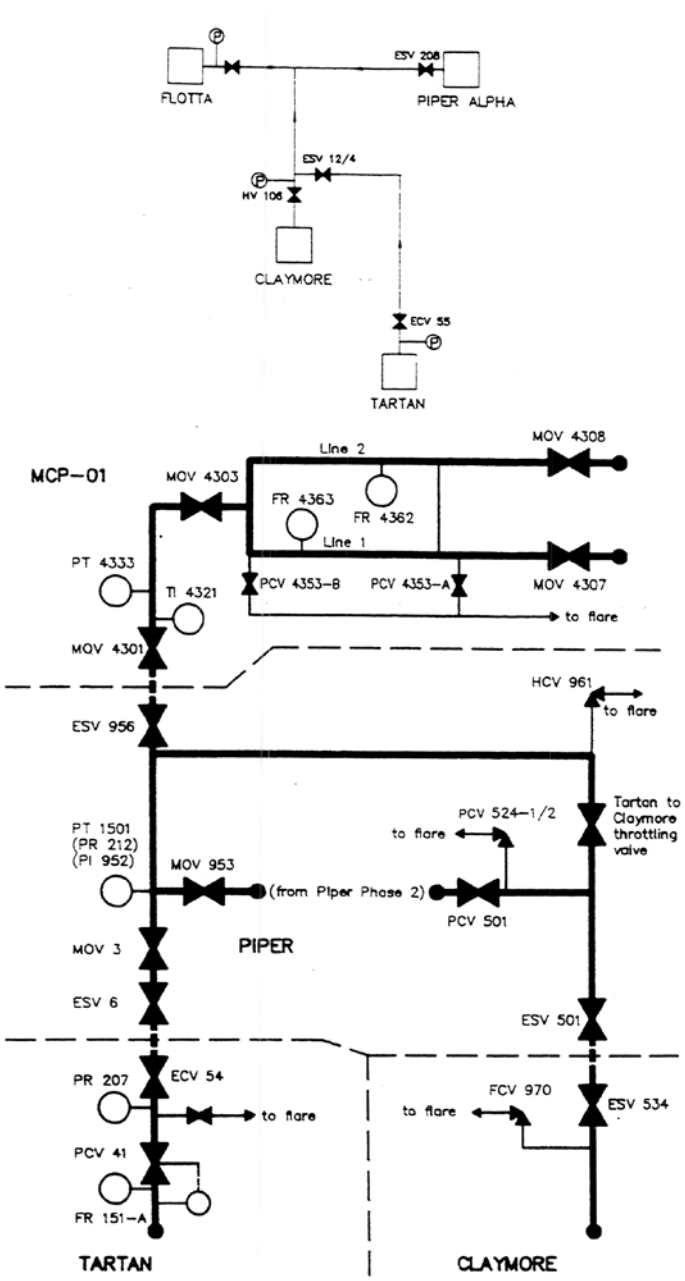


Figure D Simplified flow diagram of the emergency shutdown of the oil and gas pipelines.

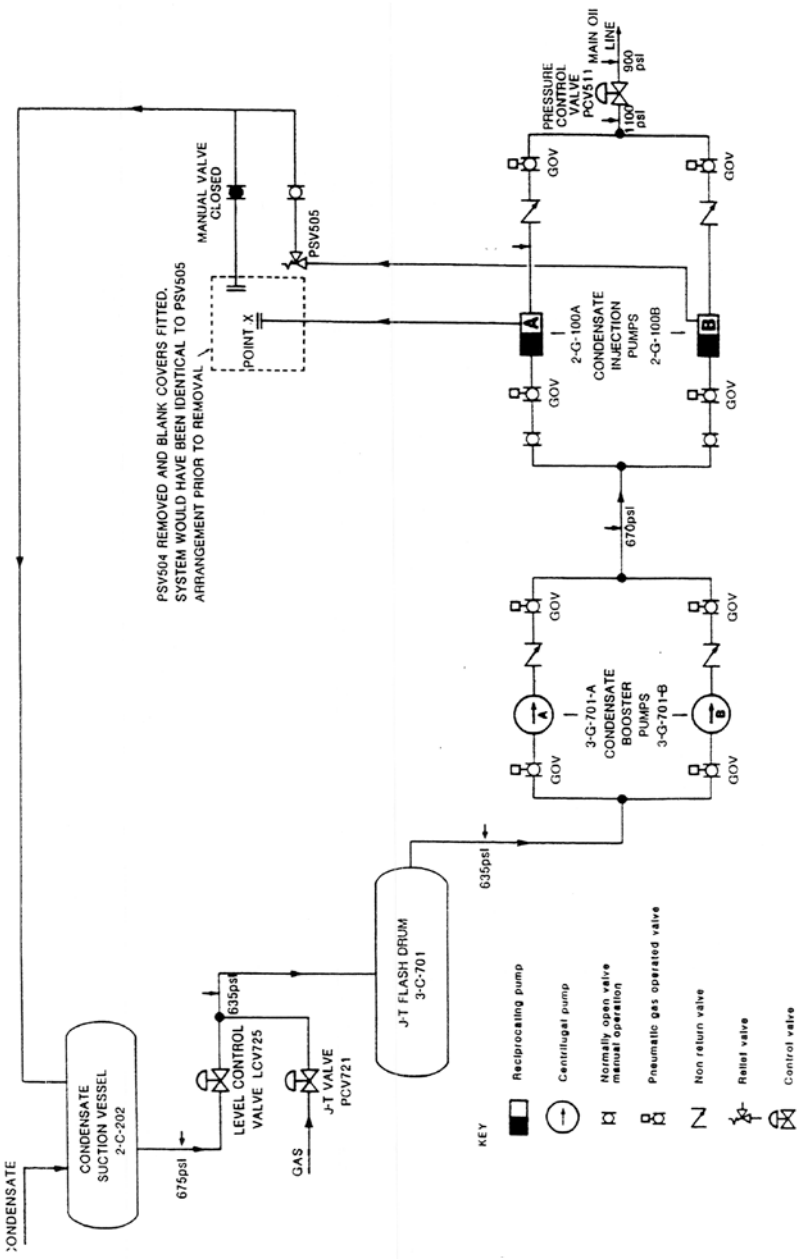


Figure E Simplified flow diagram of the condensate injection pumps

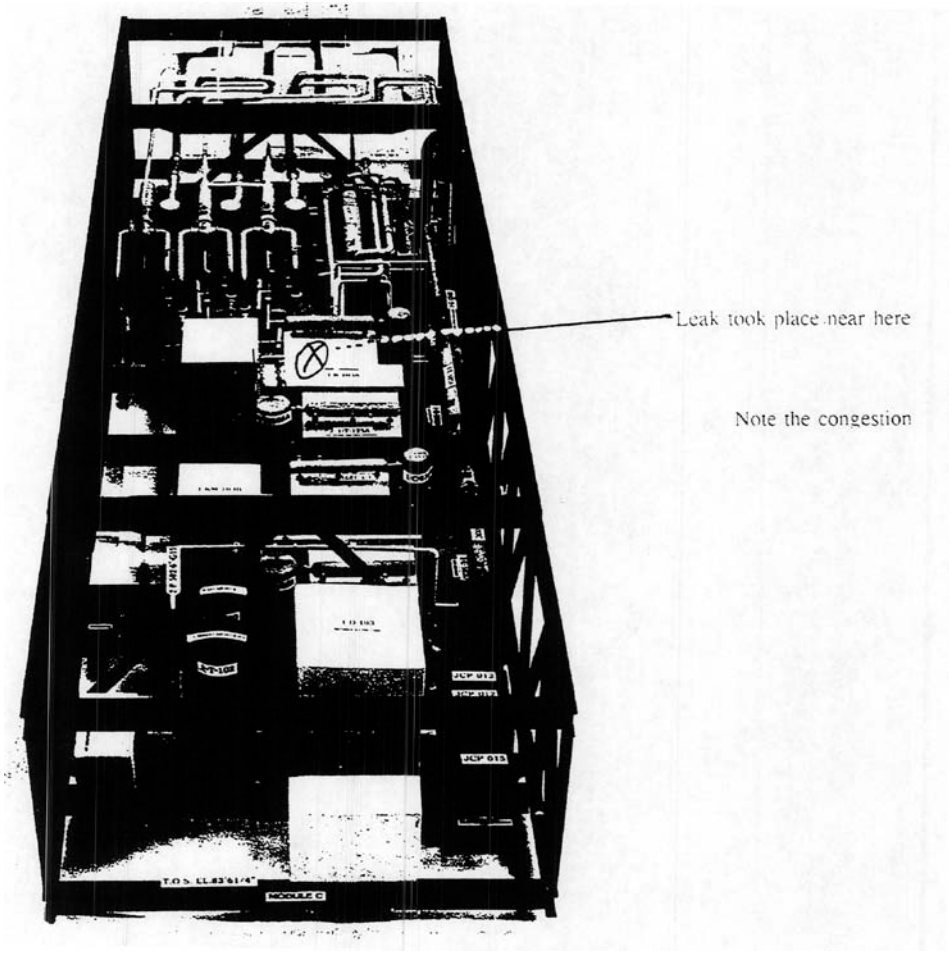


Figure F Layout of compressors and leak side

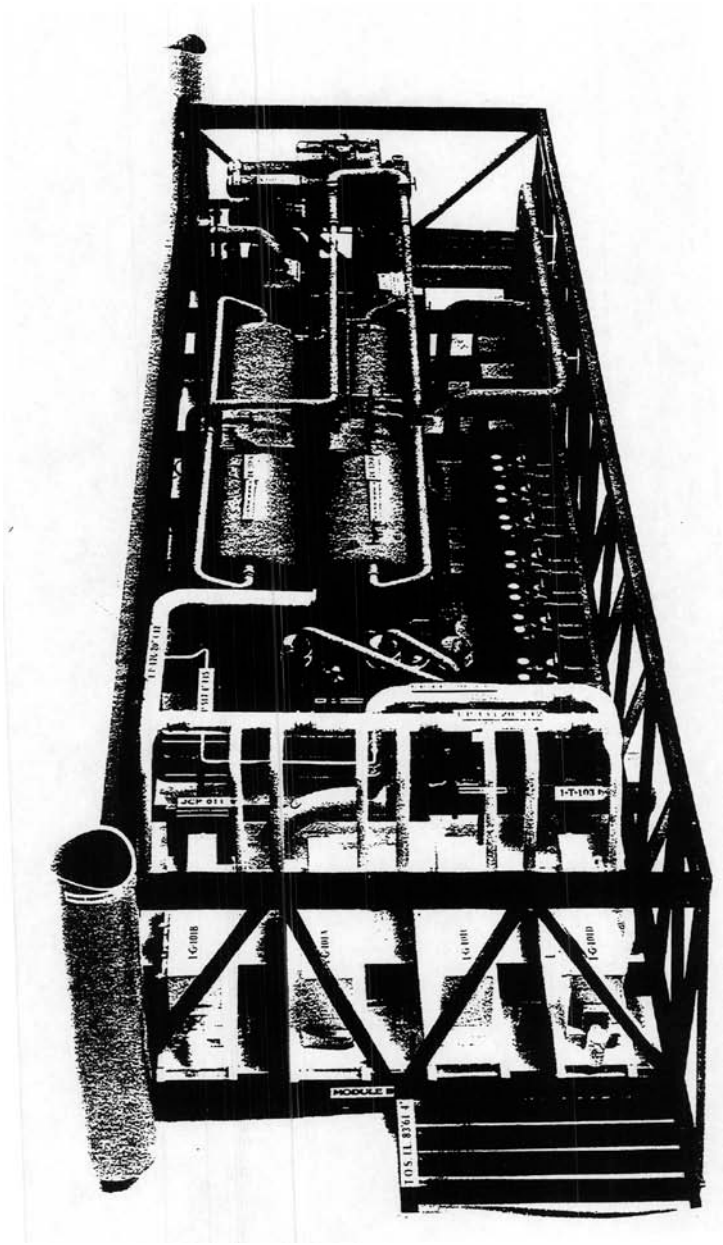


Figure G

Chernobyl

Introduction

This is a collation of written and verbal (unofficial) reports of the Chernobyl incident on 26th April 1986. The analysis is given in good faith - the accuracy of the analysis is not guaranteed but is believed to be accurate from the evidence presented - history may prove some of the points to be inaccurate in fine detail but still basically correct.

It must be noted that the PWR of the RBMK type is not used elsewhere in the world. The design of the RBMK is designed to squeeze the last drop of thermal efficiency from the Reactor and is potentially unstable and difficult to control below 20% load. Other PWRs are less efficient but they are "Inherently Safer".

Summary

Between 01.24 and 01.24 and 30 seconds on 26 April 1986 a massive steam explosion occurred in the number 4 reactor of the Chernobyl Power Station in the then Russia. (Times local). In the immediate aftermath 31 persons were killed - 29 by radiation, over 100,000 persons were evacuated locally and thousands of square miles of land were declared unfit for agriculture. The cost of rehabilitation, decontamination and encasing the reactor cost the order of £50 Billion (1996 value). The subsequent deaths were estimated to be up to 10,000 over 40 years (but in practice the ongoing evidence is that it will be slightly less than this) while it is a large number it represents only 5% of those who would have died due to the effects of background (*natural*) radiation in the then Russia.

The incident occurred because of a gross break down of procedures while testing a safety improvement (yes, a safety improvement).

Background

The RBMK 1000 is relatively primitive and would not be permitted in UK (or elsewhere in the world). The reactor was potentially unstable in some operating conditions; the shutdown was slow in operation and not fully automatic.

The electrical grid system in Russia was (and still is) "unreliable". It was essential that the reactor cooling was maintained and there was a 15 second delay following loss of electrical power before the stand-by (Diesel Driven) emergency power generations ran up to speed and synchronised. This delay was considered to be significant but it was believed that the rotational energy in the turbines/alternators could be converted into electricity and gives a short power back up for 30 to 45 seconds - bridging the 15 second gap mentioned earlier.

The reactor was controlled by Boron rods and moderated by <u>both</u> Graphite and the water flow through the reactor tubes. In the RBMK 1000 reactor most of the moderation was provided by graphite but if it has a full equilibrium content of Plutonium it had a small positive void coefficient, that is, if the steam ratio in the tubes increased the local reactivity increased, this created the need for a sophisticated local control system, the time constant was some seconds. The daughter products - particularly Xenon-135 and Samarium - depended upon the power history of the reactor. At high power the concentration of the daughter products was reduced therefore local neutron fluxes and power could increase intensifying any perturbations - this had a much greater time constant.

When shut down the reactor had a heat output of about 7% of its pre-shut down rate due to the nuclear decay in the core itself. The products are mixed so there is no true half life - the decay curve falls from 7% at time 0 to 0.4% after one day and 0.12% after a month, 7% represents about 200 MW of full load so cooling is essential for some time after shut down. (But remember the heat to electricity conversion is of the order of 32% so the heat output of a 1000 MW power station is about 3200 MW).

This residual energy was significant in the final clean up of the reactor.

The Incident

It must be re-emphasised that the incident occurred because there was an attempt to improve the safety of the Reactor! Unfortunately it was poorly controlled!!

The build up to the incident will be described as a series of breaches of the "defences on depth". These will be given as a code with the timing in brackets or the lead times before the event thus [ ].

Loads as quoted are Thermal loads unless explicitly stated.

The reactor was Inherently Unstable - that is not Inherently Safe [20 years lead - Breach 1]. The reactor had to be operated within closely controlled bands with a slow but sophisticated control. These parameters were cleared defined and the envelope defined by a computer program. (The operators were given a loaded gun with a hair trigger).

A test programme for the tests on the emergency power system had not been drawn up, analysed and agreed in the proper manner. [A change was proposed some months before the incident, but the implication had not been fully analysed, the complications assessed, the guidance notes prepared and approved by an independent authority - Breach 2 but within this there were probably at least 3 breaches].

The operations were given a narrow time window within which to carry out the experimental program of testing the conversion of rotational energy (kinetic energy) into power. This put the operators under some stress. In preparation 24 hours before the incident the thermal load was reduced from 3200 MW to 1600 MW over 12 hours. This lead to a growth of Xenon –135 in the core. This affected the reactivity of the core and the neutron flux distribution. The reactor was moving towards a potentially unstable zone.

At 14.00 on 25th April the emergency cooling system was disconnected from the forced circulation loop. However, on request from the grid controller the reactor was not taken out of service [- 11½ hours - This was a violation of regulations - Breach 3]. The emergency cooling system was not put back into operation.

At 23.10 on 25th April the power could not be reduced further. The reactor was very unstable and difficult to control. [-2 hours - The reactor was operating in a dangerous regime and should have been shut down. - Breach 4].

At 01.00 on 26th April the reactor was stabilised at 200 MW (about 6% output) The operational reactivity margins were very low and below those specified by regulation [-25 mins - the reactor was operating in a prohibited regime and by regulation should have been shut down - Breach 5]. The reactor was also "poisoned" by daughter products due to the prolonged period of operating at low power and this made the control very difficult.

It was decided to carry with the tests (This is not considered to be an additional breach as there had already been at least one violation of procedure).

At 01.07, two reserve circulation pumps were started so that power could be restored after the tests. The flow of coolant through the reactor was 8000 m^3/hr per pump [-15 mins - this flow was outside regulations and was forbidden due to cavitation and piping vibration. This led to a change in the reactor parameters - this was not a new violation, but it led to a worsening of the situation, which catalysed the end result - Breach 6].

The actions above led to water levels below the emergency levels [-15 to -10 mins - Breach 7]. The operation over-rode the emergency protective signals [-15 to -10 mins Breach 8].

At 1.22 and 30 seconds the operator realised that the reactivity conditions and availability of control rods were unacceptable and immediate shut down was called for as the reaction was far away from its operating envelope (30 control rods should have been in the reactor but were virtually none) however the team decided to carry on with the tests [- 1½ mins - a total violation of procedure - Breach 9].

As a result of all of the violations of procedure/instruction the reactor is now in a very unstable condition and it is worth reviewing the situation. At 01.19 on 26th April the operator increased boiler water feed make up to restore levels. This produced a reduction of steam voidage in the reactor resulting in the control moving up automatically. (The reduction in voidage results in a reduction in the reactivity). Within 30 seconds the rods were fully withdrawn and the operator withdrew the manual control rods so reducing the operational reactivity margin. This lead to the final outcome. At 1.22 and 30 seconds the reactivity margin was less than half the maximum permitted level. Due to the breaches, the reactor was in an irregular condition.

At 1.22 the operator had reduced the feed water flow to the reactor significantly.

At 1.23 and 4 seconds the operator closed the stop valve on the turbine steam drive to the generator.

When the turbine was shut down, the steam pressure started to rise but the water flow through the reactor started to fall as the circulating pumps were powered by the shut down alternator. (Remember the emergency cooling pumps had been isolated nearly 12 hours earlier). At this very moment any change in steam voidage increases the reactivity of the reactor. This leads to an increase in power output. The Emergency Shut Down was initiated at 01.23 and 4 seconds and the control rods were inserted. (It will be remembered that some of the mechanical rods had already been drawn, this resulted in a reduction of the performance of the shut down system). The rods did not fall fast enough and the “freefall mode” was initiated - but too late.

Finale

Within 3 seconds the power output exceeded 530 MW (originally 200 MW) doubling every 20 seconds. This increased the steam voidage and the reactivity. The effects were that the boiling film changed from nucleate boiling to film boiling - or in other words the reactor cooling fell off rapidly. The reactor temperature rose rapidly and the pressure tubes ruptured due to thermal weakening, water was injected into the hot core producing a violent steam generation which blew off the containment cap, steam reacted with the zirconium tubes to produce hydrogen which then also exploded.

Aftermath

It will be realised that the heat output from a nuclear reactor decays - the heat generation continued until the nuclear reaction of fission products falls off. The hot mass produced a cloud of radioactive particulates which entered the atmosphere and fell over a larger area of North Europe and also Scotland. Most of the cloud missed Britain but oddly one of the first indications of the disasters outside Russia was a rise of detected radioactivity on air filters of an offshore oil platform. The news finally broke some days later.

The first attempts to kill the source of particulates were to dump sand and clay on to the reactor from helicopters so as to act as a filter and to cool the burden with liquid nitrogen. The helicopter pilots who dumped sand and clay received excessive radiation doses.

The rest is history.

Within Britain statistically about 4 persons will die from the nuclear doses over the next 40 years. In the same period over 10,000 will die from breathing, eating or being exposed to natural background radiation. No one will be able to identify those 4 unfortunate persons nor the other 10,000 for that matter!

Postscript

I leave you to decide where the source of errors lays which are:

Compliance?

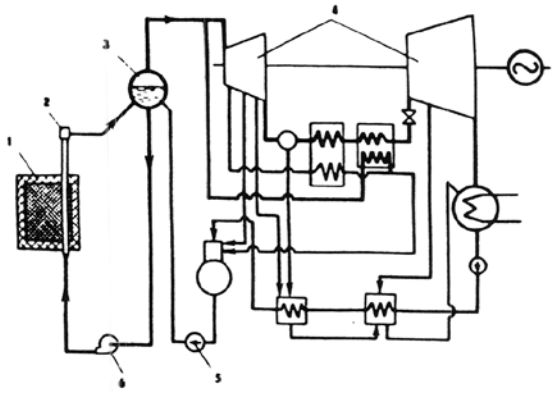
Judgement (training/experience/procedure)?

Procedural?

Design?

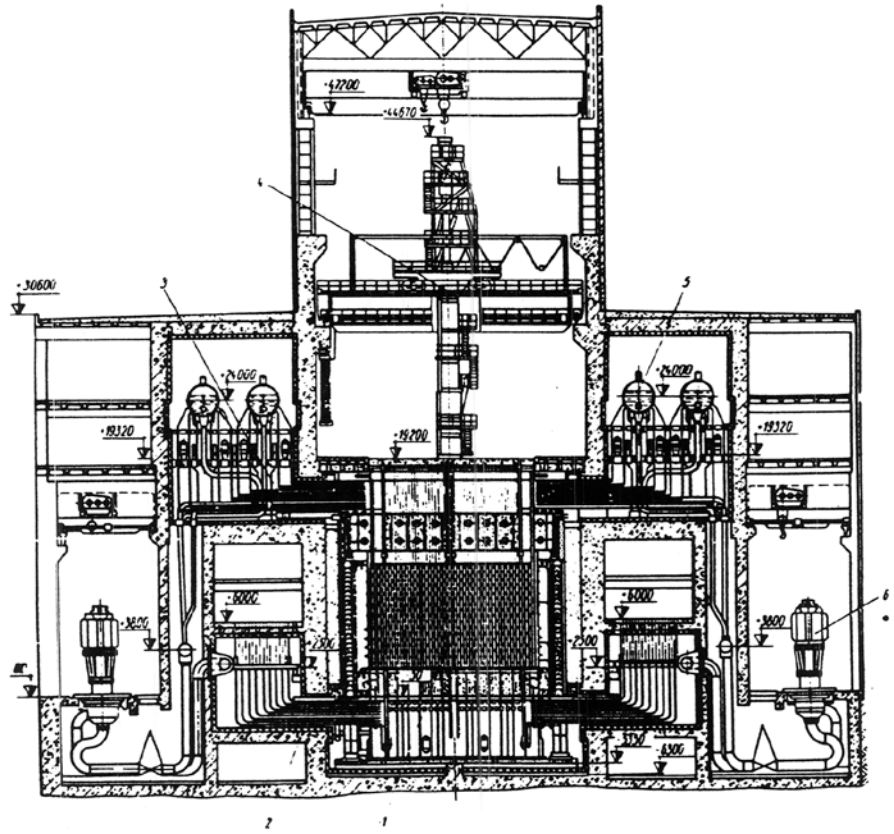
Thermal block — diagram:

1 — reactor; *2* — process channel; *3* — separator-drum; *4* — steam turbine; *5* — feed pump; *6* — main circulation pump



The reactor and main equipment of forced circulation circuit:

1 — reactor; *2* — water pipelines; *3* — steam-water pipelines; *4* — loading machine; *5* — separator-drum; *6* — main circulation pump



SPECIFICATIONS

Electric power, MW	1000	Fuel element parameters, mm:	
Thermal power, MW	3140	diameter	13.6
Coolant flow rate, t/h	$37.5 \cdot 10^3$	length	3500
Steam capacity, t/h	$5.4 \cdot 10^3$	Reactor charge (UO_2), t	204
Saturated steam temperature, °C	284	Initial enrichment, %	1.8
Reactor inlet water temperature, °C	270	Burn-up, MW·d/kg U	18.5
Pressure in the separator, kgf/cm²	70	Parameters of the reactor concrete well, m:	
Average steam content at process channel outlet, %	14.5	cross-section	21.6×21.6
Number of process channels	1693	height	25.5
Number of channels of the reactor control and safety system	179	Circulation pump capacity, m³/h	8000
Lattice pitch, mm	250×250	Circulation pump head, kgf/cm²	≈13

Chernobyl

Texaco Refinery – Milford Haven July 1994

The Explosion and Fires at the Texaco Refinery – Milford Haven 24 July 1994 HSE Books 1997 is also a useful study summarised in LPB.

Amongst the recommendations are references to the use of simple mass balances!!!

H 2 Historic Events which are easier to analyse

So as to re-enforce the message on learning from history, look at the photo above. It looks like a photo of a rising mist cloud in a valley at dawn. Do not assume anything. It is the photo of a release of liquid ammonia. If you were in this cloud – well to put it simply - you are dead!!!

What were the causes and who was responsible?

Was it a civil engineering issue where there was differential settlement resulting in a break in the pipe? Should the Civil Engineer have specified the support?

Was it a piping issue where the pipe was over pressured? Did the Mechanical Engineer specify the pipe thickness for the maximum credible pressure?

Was it a corrosion issue? Did the Corrosion Engineer specify the correct corrosion protection?

Was it sabotage? Why was the pipe not patrolled or better still trenched and marked.

Was it dug up by a plough? Why was it not trenched properly and marked such that the farmer knew where it was located. (The farmer should know all about it and the limits imposed on his operations. He is paid ("*Way Leave*") for the use of his land!

All these are simple issues but vital Management issues!

Thanks are due to JR Taylor for this photo

Incident Studies

Incident studies are useful in highlighting human factors, management issues; inter engineering disciplinary issues and basic engineering.

IT IS OF FUNDAMENTAL IMPORTANCE THAT THE CORRECT MESSAGES OF THE INCIDENTS ARE TRANSMITTED. DO NOT LINGER ON THE EVENT ITSELF

One of the richest sources of incidents is during maintenance or upset conditions. Entry to enclosed spaces and welding are obviously another source of rich pickings but upset conditions are one of those conditions where there is a stressful situation and action has to be taken quickly and correctly. This requires "*thinking on the feet*".

The sections are divided into five "home":

Entry

Fires and Explosions

Maintenance

Upset

Others

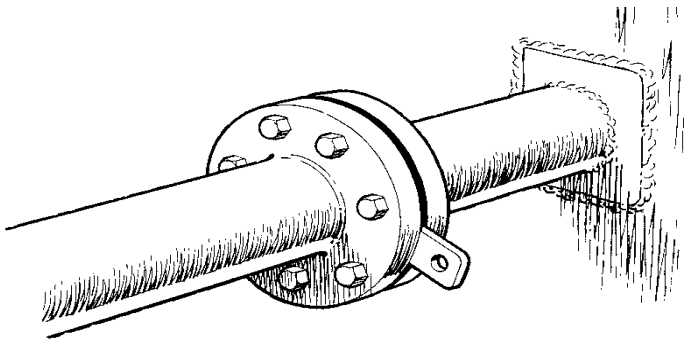
Some could be considered to straddle two possible "homes".

The studies include some background as well as the safety teaching points. The background could be suppressed if the student is trying to solve the problem and then reintroduced at the conclusion. The teaching points and answers to questions can also be suppressed and used as a check against the detail of the investigation.

Preparation.

Slip Plates

In a number of incidents reference will be made to the use of a slip plate as shown below. Essentially it is a blank sheet of metal inserted and held by tight bolts between two flanges. It is also called a "positive isolation" as NOTHING can flow down the line into the workplace. It has to leak to atmosphere.



Preparation of equipment for maintenance which may have contained hydrocarbons

It is a standard practice to steam out equipment (including vessels) to remove the "more volatile" hydrocarbon components or to displace toxics.

The elevation in temperature and the steam flow is usually sufficient to remove **MOST** flammable materials **BUT** it does **NOT** guarantee that there are no traces of low volatility materials to be found later, particularly when the system is disturbed or heated (see incident 1.4 and the HSE report - Fires and Explosions at BP Grangemouth - HSE Investigation.)

Some simple flash calculations on a multi component mix will illustrate this. It is only simple equilibrium!!!

In effect lighter (low molecular weight hydrocarbons) will be boiled off. However in the case of heavy films and also thick deposits there is a mass and heat transfer issue which will limit the efficacy of the steaming process. The heat flow through the deposit may be poor and then there has to be mass transfer such that high molecular weight materials are still left within the film/deposit. In crannies there is also a limiting diffusion process so "cleanliness" is not necessary assured and deeper in the layer there may still be harmful materials. Superficial tests may pass the acceptance criteria but the environment may change with time.

In effect the "*flash point*" of the material may be 100^{o}C BUT it does not guarantee that it will be non-flammable if heated to well above 100^{o}C. (The flash point is that temperature at which the vapour pressure of the material is such as to JUST produce a flammable atmosphere at the lower flammable limit).

Air Tests

Air in confined spaces COULD be oxygen deficient and contain "potentially harmful" agents. **Is the sample representative of the whole**? Do you know what might be in the air? How do you test for these? Can the conditions change with time and human activity???????

1 ENTRY

Incident 1.1 – Vessel entry at a major shut down

The incident

The figure 1 shows the simplified line diagram of a gas contactor – the plant is no longer there!

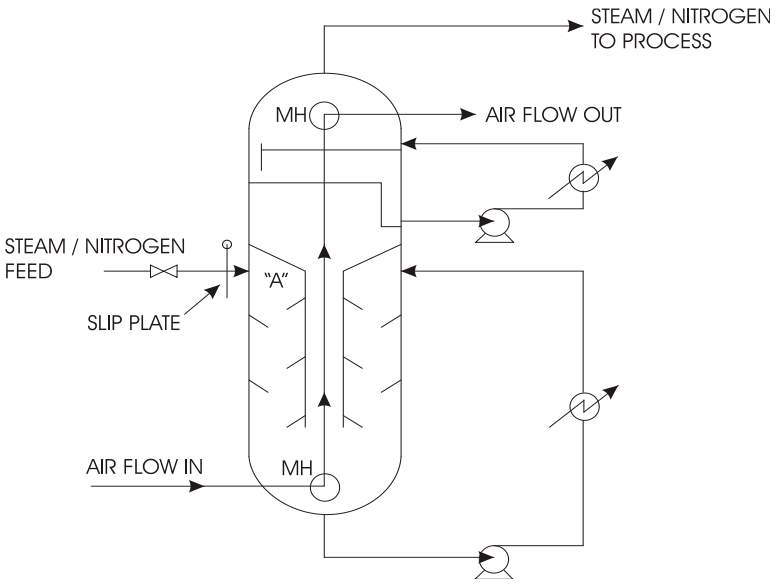


Figure 1.1 Gas Contactor – simple P & ID

Two oil recirculations, the lower one by hot oil at 150°C and the top one by oil at 50°C contact hot gasses. The lower section is co-current over "disc and doughnut" plates and the top by counter-current over standard trays.

The plant was to be inspected during a major overhaul and as part of the preparation the internals of the contactor was "steamed" by passing hot steam at 150°C for 6 hours at point "A" and then displacing the steam by nitrogen at the end of the 6 hours. The nitrogen was displaced by "the chimney effect" through air entering at the lower manhole (MH) and leaving at the top manhole (MH).

All process lines were sealed after the system had cooled by metal plates known as "*slip plates*" (as above) on the contactor side of every valve flange as shown. Air tests for oxygen and flammables were taken at the man holes top and bottom as shown. The oxygen samples at the manholes were 20.8% v/v and the flammables were not detectable (N/D).

Question 1.1.1

Can a safe entry be made to every part of this contactor – you have to issue the entry permit?

Answer 1.1.1

NO! The air flow between the two manholes only displaces nitrogen in the vertical section of the contactor. The section from the inlet, mid way up the column, to "A" is potentially a "dead pocket" which could still contain nitrogen. The author of this document made that entry and suddenly realised the error of his own judgement as he looked at the slip plate at the top of the dead pocket at "A" and asked "*what*

was the last fluid in here?" *NITROGEN*! That was the fastest exit ever made! In reality the nitrogen HAD been displaced during the fitting of the slip plate. This was confirmed by repeat air tests done under the correct controls.

Question 1.1.2

Why displace the steam with nitrogen - both are inert?

Answer 1.1.2

1. Steam will condense and the vacuum so produced could collapse the vessels, steam has to be displaced by a "non condensable". It is important to understand the physical properties of the fluids being handled.
2. Entry into a wet space is very unpleasant!!

Key Safety teaching points

1. Entry into confined spaces is hazardous at the best of times. It was one task that I treated VERY seriously. It could be my last task on this earth!!!
2. Has a full risk assessment been carried out? (A Risk Assessment had been carried out in this case but it was incomplete.)
3. Has the atmosphere in the confined space where persons might be been checked very carefully for, oxygen levels, flammability and toxics and increasingly nuclear debris. This will mean at least a multiple point sampling. (The atmosphere had been tested but not at the place where the inspection took place.)
4. Could the environment change over time as a result of the work carried out?
5. Are there any "dead pockets" (as above)?
6. Agitators or other mixing devices must be made safe. That is mechanically and or electrically isolated. Humans do not "mix" well! Sorry for the pun.
7. There may be sharp edges in the enclosed areas such as vortex breakers and weirs.
8. The route in and means of emergency exit should be reviewed. Should there be a harness and rope through a pulley plus "stand-by-man"? How does the person make an exit if there is trailing line for breathing air? It could get tangled on fixed internals.
9. The internals should be physically isolated to prevent harmful materials entering the confined space either from leaking valves or just atmospheric movement (from spills). Valve isolation is not acceptable, "physical disconnection" is, but better still with slip plates.
10. Conditions may not be as expected or may change with time/operation in the space – contingency plans must be in place. For example how is dirt in hidden pockets or behind weirs addressed?
11. The air flow regime in a vessel has to be fully comprehended.
12. It is important to understand the physical properties of the fluids being handled.
13. Pockets behind weirs can be traps for hazardous gas/fumes – see 4 & 10 above.
14. How does the inspector get out in an emergency – on site, on plant or in the enclosed space?
15. Plan! Plan! Plan! It may be your life that is lost!!!!

Incident 1.2 Asphyxiation

The incident

This is a true story that seems to occur more frequently that it should.

A vessel had been purged with nitrogen and then opened up in readiness for inspection by opening a manhole on top of the vessel. At that point there were no or gas tests taken or entry permit issued. The vessel "looked clean" from inspection through the manhole so a **very** experienced Supervisor and Engineer decided to check the vessel for evidence of corrosion. The Engineer entered the vessel while the Supervisor stayed outside. After about 5 minutes it was decided to inspect the seats of two large valves at the base of the vessel to ensure that there was no wear. The Supervisor, who was outside, opened one of the valves and the engineer lost consciousness within seconds. The Supervisor raised the alarm and entered the vessel where he too lost consciousness.

Question 1.2.1

Why might this have occurred?

Answer 1.2.2

There was an unauthorised and uncontrolled entry into a vessel. No tests had been carried out and no permit issued.

There was a trap of nitrogen behind the valve. The oxygen level in the vessel fell below 10% and the Engineer lost consciousness.

Question 1.2.2

Why did this occur?

Answer 1.2.2

The Engineer had broken a "golden rule". **Do not enter a confined space without a permit**.

There was a breach of discipline which could have been fatal.

Outcome 1.2

The Supervisor was reduced to "the ranks" and the Engineer was dismissed on the spot!

Question 1.2.3

Would you have dismissed the Engineer?

Answer 1.2.3

This is a difficult call but breach of safety discipline can not be tolerated.

> Sadly to relate I knew one excellent supervisor (Willy de B) who decided to do a "quick inspection" of a vessel purged with nitrogen by putting his head through a manhole. He collapsed inwards and died – that is why I typed "knew". Do not try it!

Key Safety teaching points

See the teaching points in 1,1

Incident 1.3 "It was done correctly".

The incident

A vessel had to be cleaned out on routine to remove heavy oil mixed with solid materials which might release hydrocarbons when disturbed. The vessel was "slip plated" and steamed out. Entry was carried out using breathing air and flame proof clothing. The tools used were "non-sparking" phosphor bronze. The work site was air tested every 15 minutes for traces of hydrocarbon which might have been released during the cleaning process. It was a **very** uncomfortable clean-out, hot and slow due to the nature of the entry conditions applied and tools used (soft phosphor bronze) - but it was safe.

Question 1.3.1

Was this excessive protection?

Answer 1.3.2

NO! It was carried out over 100 times and no-one was injured.

Key Safety teaching points

See the teaching points in 1,1

Incident 1.4 "It was not done correctly" (Same Company and 200 m from study 1.3)

The incident

A vessel was cleaned out on routine to remove traces of a latex rubber. The tank was "slip plated" and steamed out. The entry was made without breathing air and non-flam clothing and the tools were not "non-sparking". The site was not inspected on routine for traces of hydrocarbon which might be disturbed during the cleaning process.

There was a fire/explosion in the vessel, one person was killed and another seriously burned.

Question 1.4.1

How did this happen?

Answer 1.4.1

The latex was being disturbed by the digging/cleaning process. Any gas (butadiene in this case) trapped or dissolved in the latex would be released and a flammable cloud could have been generated. The ignition source was probably friction or impact from shovels but it is JUST possible that there was a cigarette involved. The ignition source was not identified with certainty.

Key Safety teaching points

See the teaching points in 1.1

Incident 1.5 Again and this time it was done correctly

A vessel was prepared for entry with slip plates and then by boiling water in the vessel using "live steam" (a steam lance put under the water). After two hours a flammable gas test was taken and traces of hydrocarbon (5% of the lower flammable limit) were detected at a "line of scum" on the vessel wall. (See the notes on diffusion/mass transfer earlier). Entry was carried out with full body and lung protection and the area where the gas was detected was scrubber down until gas could no longer be detected. Then the internal inspection was carried out safely without lung and body protection.

Incident 1.6 Trapped in a vessel.

"*The fire at Kinneil – Fires and Explosions at BP Grangemouth - HSE Investigation*". (HSE Books). The ignition source was a cigarette. This probably emphasises the need to monitor the work place against deviation from the stipulated precautions.

Incident 1.7 Asphyxiation in a scrap vessel

The Incident

This is a true story that seems to occur more frequently that it should.

An old, rusty, carbon steel vessel fitted with loose blanks on all branches and manholes was found on a dump. The vessel had not been operated for some years. It was decided to re-use the vessel, so, it was to be internally inspected by two engineers. Within 10 seconds of entry the two engineers lost consciousness.

Question 1.7.1

Why did this happen?

Answer 1.7.1

The clue is in the word "rusty". The vessel was in a "dump" so it was not considered that a full air test was required. It should have been – the message is "assume nothing". Air in the vessel had reacted with the wet steel to produce rust. The inspectors entered a vessel which was oxygen depleted and lost consciousness.

$$2Fe + 3O_2 = 2Fe_2O_3$$

Doh!!!!!!

Question 1.7.2

What would you do in these circumstances?

Answer 1.7.2

There is only one answer – carry out the risk assessment and air test any enclosed space system however simple it might be. How do you know that some heavy gasses have lodged in a "low point" and light gasses lodged in "high points"?

Key points for teaching with entry to confined spaces:

See the teaching points in 1.1

It is essential that the atmosphere into which any one might enter is tested for flammables, toxics and oxygen deficiency.

The zone must be free of moving parts and if possible sharp edges.

Where possible overhead debris should be removed – this might influence the order of entry "top – bottom" and not the other way round.

How does the inspector get out in an emergency?

In general entry to confined spaces is the most dangerous activity that most engineers will undertake. It has many potential unknowns which have to be analysed with care and a FULL RISK ASSESSMENT carried out. Remember the last fluid in the system was either a process fluid or an inert fluid, neither are life supporting!!!!

2 FIRES AND EXPLOSIONS

Study 2.1 An explosion in an "oil slops" storage tank.

The incident

Figure 2.1 shows a simplified diagram of the equipment. The tank collects thick oil spills and some traces of water. The tank is heated to about 50^{o}C by an electric heater bolted into the tank and is thermostatically controlled (on/off) by a circuit breaker, CB_2, by an integral thermocouple, TC_1. The oil and water is pumped to further storage by pump 1 under level controller, LC_1. The tank is inerted with nitrogen through a Pressure Controller, PC_1, which vents to atmosphere through a flame arrestor, FA. The electrical heater is independently shut off (CB_1) if 1) the pressure in the tank falls below a critical level by PA_L and 2) if the level falls below a critical level which might expose the heating elements by LA_L.

A flame arrestor is basically a spiral, corrugated coil of thin metal. The triangular gap between the corrugations is designed for the likely gases involved and is known as the "*quenching diameter*". The pressure drop is very low. It can be assumed that the arrestor was fit for purpose.

During the start-up phase nitrogen from the site inert gas generator was not be available so nitrogen bottles were used and then the inert gas generator was to be used once the plant was up and running.

About 1 year after the start-up there was a violent explosion in the tank. The electrical heater was ejected with such violence that it damaged structural steel on which it impacted. The likely over-pressure was

about 4 bar_g. (This was assessed from the UTS [ultimate tensile strength] of the steel and the root area of the bolt threads of the restraining bolts).

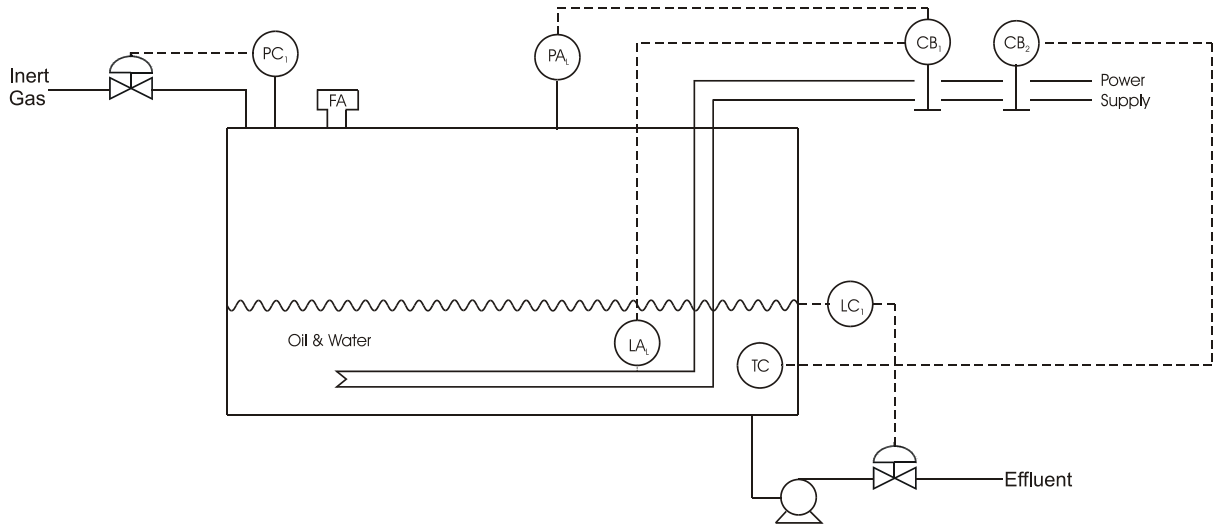


Figure 2.1

Question 2.1

You are the investigating team. What do you think might have been the causes of this event? You may ask your tutor for more information should you wish.

Clues to be offered by the tutor if asked:

1. On inspection of the nitrogen connection the paint was undisturbed. That is the nitrogen bottles had **not** been used and the site inert gas had **not** been connected.
2. A function test of the electrical shut off protection showed that it was by-passed.
3. The pressure differential across the flame arrestor was too low to allow the pressure controller to function correctly. Even at "full flow" of inerting medium the differential pressure would be low and register "low pressure" on PA_L.
4. The pressure differential across the flame arrestor was too low to "permit" the low level pressure cut off (that is the control system would be keeping the tank in the shutdown condition even if there was an inert gas flow. That is, the design was not "fit for purpose".) It was therefore permanently in the shut-off condition and had to be inhibited by the start-up crew who did not understand its function.

Answers 2.1 & possible Causes

1. There was a deviation from the design intent.
2. The actual design was flawed (the pressure differential could not be established to activate the pressure switch and allow the pressure controller to function correctly).

3. The process had not been subjected to a HAZOP. If it had been the "low pressure" question would have challenged the ability to establish of a pressure differential across a flame arrestor, which, by design intent has a low pressure differential. A small STEADY purge of nitrogen would have been enough to inert/blanket the tank.
4. The operations department carried out an unauthorised and unchecked change. There was no Management of Change inside the Company – there is now!
5. The tank had drained so exposing the electrical heater elements and the thermocouple. The oil over heated and an explosive atmosphere was established. This ignited on the hot heater element.

Background

1. "Fuel + air + ignition = Fire" or "Fuel + air + ignition = Bang"

Key points for teaching.

1. Change of design intent requires a rigorous analysis – a management of change procedure.
2. Had a HAZOP been carried out? (NO!)
3. Was the design intent valid/workable? (NO!)
4. Was the shut down system tested on routine? (NO!)
5. Did the start up crew understand the function of the various elements and have operating instructions? NO!

This was an accident waiting to happen

A hot water heater is an inherently safe heating medium.

See also – *Fires and Explosions at BP Grangemouth - HSE Investigation*". (HSE Books)

1. Here a shut down had been cut/bypassed so invalidating a low level cut off which eventually lead to a vessel rupture.

2. There was no function testing routine (or else the shut down bypass would have been identified).

3. Someone, somewhere made an unauthorised change to a protective system. It is quite possible that it was done with the best intentions but tell that to the widow of the person who was killed!!!!

4. The analysis of the FDT/PFD of the "protective system" suggested that the event should have occurred some years earlier. There was also one common cause or mode failure – wax in the oil!!!!

5. The performance of the protective system had not been formally assessed.

This is a useful study which shows how things can drift without strict Management controls

Study 2.2 An explosion in a tank

The incident

Dudgeons Wharf (1969) – synopsis of the Public Enquiry, HMSO

A redundant storage tank was being removed from the site. It had previously contained hydrocarbon oil, similar to turpentine, which could create a gummy material deposit. The chosen method for size reduction was by flame cutter (oxy-acetylene torch). The tank was prepared for size reduction by steaming out for 24 hours "to steam strip any hydrocarbons" from the internal surfaces. (See the notes on the limitations of the steaming process). Once the cutting process had started flames were seen at the cut site and the open manhole on the tank roof. The flames were put out with a water jet.

The internal cleanliness of the tank was not clear but the evidence of the flames strongly suggested that there was gummy material on the walls/roof. As a means to checking the internal cleanliness the bottom manhole in the tank was opened by flame cutting off the bolts. There was a violent explosion which blew off the roof, so killing 6 persons.

Question 2.2.1

Why did this happen?

Had a Hazards Study 7 been carried out? NO!

Answer 2.2.1 & Causes

1. The tank had been prepared in some manner but a full risk assessment of the extreme conditions had not been carried out. It is likely that the gas tests had not been taken at the walls (see 1.5)
2. The heat of the flame cutter on the bolts would have vaporised some hydrocarbon and probably created a localised flammable cloud in the tank around the hot manhole.
3. The cloud was probably ignited by the hot metal (auto-ignition) or by the flame itself.

.Note - flames had been seen previously when cutting the roof so it is a highly credible explanation but the demolition crew just did not have the experience to make the correct deductions.

As these tanks can only sustain a pressure equivalent to about 25cm of water before the roof blows off the hydrocarbon "explosive charge" may only be about a kilogram. A simple BOYLE's law calculation will prove this.

At best this could be classified as incompetence but it is not unlike any demolition site where the details of the tank conditions are vague, particularly if the previous owner has no longer any interest in it.

There is now a requirement to write a "safety case" for demolition. This may be more difficult than you think! However the previous owner still has a duty of care to ensure a safe hand-over to the demolition crew.

Question 2.2.2

Could this happen again?

Answer 2.2.2

It has! However for large scale demolition work there has to be a "*safety case*", the reverse of the safety case required before operation can commence. The case should explain how the size reduction is to take

place, the potential hazards, the precautions to be adopted and other safety procedures to be put in place. The case should also address the final disposal of materials. If materials have to be dumped the case will have to address topics such as ground water contamination and if steel is to be recycled the case should address the cleanliness requirements. This is not as difficult as it might seem, it is a case of recording the well established procedures and then following them!

Question 2.2.3

How could it be prevented?

Answer 2.2.3

Yes! This can be summarised below:

1. There is a duty of care by the previous owner to ensure that all relevant details on cleanliness and latent risks associated with redundant equipment is handed over to the demolition crew. (Safety Case for Demolition). Do not expect the demolition crew to understand or investigate the possible hazards of the equipment that they are due to demolish.
2. Steaming is not very effective for multi-component products but there are now nitrogen based foams which are very effective in inerting cutting sites. One cut on a major oil pipeline was carried out using these foams. The cut was done quickly and safely.
3. There is always the possibility of small traps of material behind weirs or even in down comers in distillation columns which may be ignited inadvertently. Physical inspection using the appropriate entry requirements (breathing air and flameproof clothing) may be required before any cutting is allowed.

<u>This type of incident is more common than might be expected. A review of Hazard Databases shows that it occurs with regularity more so in vessels with a weir. Weirs are common means of separating two liquid phases and flammable debris may still be found on the far side of the weir. Once a cut or weld is attempted the materials behind the weir ignite and a prompt exit is necessary!!!</u>

<u>Background</u>

There have been many fires and explosions in storage tanks which have contained hydrocarbons. The messages are still valid as fatalities occur from this cause even today.

<u>Key points for teaching</u>.

1. “Fuel + air + ignition = Bang”
2. Can you be sure that the **RISK ASSESSMENT** will cover **ALL** areas within the confined space? If not there may be a hidden tiger waiting to pounce on you!
3. Can the local conditions or requirement laid down in the Permit to Work (PtW) change with time?
4. The working environment must be monitored regularly
5. If the conditions change **ALL** work **MUST** stop at once!
6. Demolition is a dangerous event – possible more so than operation. It must be done under rigorous control and supervision.

Incident 2.3 29/7/12 in the press

On 29/7/12 someone decided to split a 45 gallon drum lengthwise to make a barbeque. The cutter was a rotary disc. The drum exploded and the person using the cutter was fatally injured. He will not do that again!

Incident 2.4 Unpredicted explosions in crude oil tankers (1970s)

The incident

Kong Haukkon after the explosion

Marpessa, Matra and Kong Haukkon

Oil tankers are usually cleaned out using high pressure water jets. This removes residual oil which is then separated elsewhere. The tank is also inerted using exhaust gases from diesel driven machinery as a flammable mix is more than likely within the tank during the cleaning process.

About 40 years ago the three super tankers, owned by the "same company" (house colours red and yellow), Marpessa, Matra and Kong Haukkon "blew-up" near to the equator over an interval of about 2 weeks. They had been carrying crude oil and were returning under ballast. Many rumours were generated – "*it was sabotage as they had delivered oil to South Africa during Apartheid*", "*it was bandits*" etc!

Background

1. The tanks were inerted using "waste gases" from the diesel generator exhausts.
   This is an "inconvenience" as the gases have to be scrubbed to remove sulphur oxides and particulates and must be monitored for carbon monoxide (a toxic) and residual oxygen which has to be less than about 5% v/v.
2. The inert gas generator is a piece of "process equipment" which is difficult to appreciate and not in the Tanker crew's Skills profile.
3. The generator is potentially a cost overhead which requires maintenance due to the corrosive SO_X in the exhaust gases.

Question 2.4.1

Why did this event occur on 3 tankers, owned by the same company, and in such a short time frame?

Answer 2.4.1

1. At the time it was far from clear what were the causes, but by reports from the crew it was neither sabotage nor bandits. However, it appeared that for economic reasons or possibly as the Company could not see the benefits, the inerting step had been removed from the storage tank cleaning cycle but it was not subject to a Management of Change procedure. Further the inerting equipment was bulky, required routine maintenance (a costly task) and the operation was not in the skills base of mariners. It can be seen that there was a persuasive argument to drop this part of the cycle.
2. Lightning is caused by static formation in the cloud as the droplets of water are re-circulated. It can result in major charge accumulation as is seen from the lightning strike. It was **"NOT THOUGHT"** that such a charge could accumulate in a tanker compartment as it was **THOUGHT** that the charge generated by the cleaning spray would be too low (charge is proportional to the droplet diameter) so as the droplets were small it was thought that the charge would be trivial.
3. A detailed study was carried out into static formation in sprays and it was found that smaller droplets coalesced to form larger droplets (as in clouds! Surprise! Surprise!) and these larger droplets COULD occasionally result in an incendive spark. So as to prove this point a rig was set up simulating the cleaning operation and a polythene roof fitted. There were explosions in the rig – case proved!
4. It is easy to be wise after the event but knowledge of the formation of lightning should have been enough to make the operators of the tankers think carefully before stopping the inerting process. The ***management of change*** had not been carried out.

Key points for teaching.

1. Changes can occur very easily if the rules for change (management of change) are not enforced rigorously
2. Out of sight = out of supervision (*or while the cat is away the mice will play*!)

Who did not learn their lessons 30 years later???

Incident 2.4 "Switch Filling"

The incident

Road and rail tankers are used to distribute diesel oil and petrol to distribution centres and filling stations round the country. Filling can be by "bottom fill", filling the material by a fitting on the base of the tank, this involves lifting a hose and it carries the risk of back injury and even worse the hose is "out of sight" and tankers can "move off station" without the hose being disconnected. However this filling technique prevents the formation of static electricity by "*splash filling*". Alternatively the filling can be by "top fill" using a lance which reaches almost to the bottom of the tank. This filling process has the potential to produce static electricity particularly with high resistivity fluids such as diesel oil. Therefor during the initial fill the flow rate is low (less than 1 m/s in the hose and lance) until the bottom of the lance is covered by the fluid, once the lance is covered the risk of static generation is negligible. The rate and time to cover the lance are programmed into the fill cycle and once sufficient fuel is added to cover the lance the fill rate is ramped up.

The tanker may have contained petrol or diesel prior to being filled. The cross contamination is insignificant as far as the fuel is concerned but the barrel may contain flammable vapours.

A new set of "jumbo tankers" was brought into operation. The diameter of the barrels was very slightly larger than the old ones and the length was about three times longer. The fill sequence as controlled by the same fill sequence which was locked into the logic control itself as described earlier so did not differential between the two types of tanker.

After 3 months there was a fire in one jumbo tanker.

Question 2.4.1

Why should that be when the fill process had been applied safely for 20 years involving about a million filling cycles?

Answer 2.4.1

The likely causes:

1. The records showed that tanker had contained petrol before it was filled. The vapour space would be "flammable" containing mostly butane. The traces of petrol would not affect the specification of the diesel.
2. The "fill process" was designed for the smaller tankers such that at the of the "low flow" part the fill lance was not drowned in the jumbo tanker and a static regime was formed once the controller went onto "high rate fill". The extension to the "low flow" part of the fill cycle may have only been a few minutes but that was enough.
3. It is likely that the operator did not understand the significance of low and high feed rates. (This was the outcome of a safety study carried out by the author).
4. Why was not a ***Management of Change*** study carried out? There was a change!!!!!

Key points for teaching

1. Bulk supplies of diesel oil and petrol are now distributed by rail. As the demand has increased the capacity of the rail tanks has trebled such that there are now "*standard*" and "*jumbo*" tanks.
2. Hoses and the tankers are always electrically earthed to avoid static electrical charges.
3. Splash filling is a powerful source of static ignition. There are **MANY** reports of fires in metal buckets used for sampling.
4. High velocity flow of high conductivity fluids (high resistivity fluids) results in charge separation leading to static ignition.
5. Wherever possible the tanks are re-filled with the previous material but occasionally it is necessary to fill a tanker which previously contained petrol with diesel oil. **Knowledge of the previous "contents" is important in risk avoidance planning.**
6. All changes, trivial or otherwise MUST be subject to a MoC study

Incident 2.5 Switch Filling

There is another example of an explosion created by a change in tanker body profile in LPB 209.

Incident 2.6 Static generated by transfer

A charge of volatile organic spirit was to be transferred from a storage tank into a "45 gallon drum". The drum sat on a trolley fitted with nylon wheels. There were some difficulties in starting the flow from transfer pump; it appeared to be "gas locked", that is there was vapour in the pump body. After a few minutes the flow was established and almost immediately there was an explosion in the drum, it split and the operator was showered with ignited spirit. He died from his injuries.

Question 2.6.1

Why might this have occurred?

Answer 2.6.1

1. The churning of the transfer pump, before the flow was established, would have heated the spirit and equally important it created an electrostatic charge in the fluid. The word "spirit" should have alerted to the possibility of a high resistivity fluid which has high static charge potential.
2. The drum was electrically insulated from earth by the nylon wheels. The filling hose was not bonded or earthed so as the spirit started to fill the drum there was a spark between the fill nozzle (similar to a nozzle in a petrol filling station) and drum which ignited the vapour created by the "hot, churned spirit". (The fill hoses in petrol stations are earthed).

This is a fairly common problem and there are many (too many?) stories of drums or pails of spirit catching fire when being filled.

Incident 2.7 - Displacement of air and compression ignition

Background

The flammable envelope for most flammable materials is fully defined. However is it necessary to displace all of the air when charging with a POTENTIALLY FLAMMABLE material such as diesel oil where the ignition temperature is about 200^{o}C? YES! If the closed end of the pipeline is not opened the line pressure will rise and at about 10 to 15 bar the temperature at the interface will reach auto-ignition temperatures – how else does the diesel engine run?

The incident

A pipeline, 50 km long and operating at 30 bars, was being charged with a high flash point (volatile) fluid with an auto-ignition temperature of 200^{o}C. The main isolation at the far end of the line was closed but there were facilities to vent the line and displace any air to a safe area when required. The operation of the valve and venting process was carried out on the second or receiving plant following instruction from the first or pumping plant. This operation had been carried out many times already. One day the pipeline ruptured following an internal explosion.

Question 2.7.1

Was the procedure inherently safe?

Answer 2.7.1

1. The procedure was NOT inherently safe. It was highly reliant on the communication between the two ends. See also the Buncefield Tank overflows.
2. Communication over a distance is at best poor. It can also be "forgotten" in the heat of the operations.
3. The vent valve had to be opened to vent the air and also to avoid a high pressure within the pipeline.
4. There had to be an established link between the two sites and a confirmed operation of the vent valve. This has many forms but in simple terms it is an "interplant permit" where the supervisors on both plants are signatories.

Question 2.7.2

What COULD go wrong and what might be the effect?

Answer 2.7.2

If the vent at the far end was left closed, as the pipeline was pressured the air plug would be compressed and the temperature would rise. As the pressure at the fluid/gas interface reached 10 bar the temperature, assuming, adiabatic compression, would exceed 200^{o}C, fluids could be vaporised at the interface and then ignited by auto-ignition. If the charge is large enough the pipeline would be split (as it was in this case). The pressure ratio in a confined explosion is about 8:1 so would almost certainly result in rupture of the piping.

There have been a number of such incidents. One was the destruction of a Coking Column when starting up, and other is to be found in *Frank Lees* book on Loss Prevention.

Key points for teaching

1. Communication between sites under common user is often at best awful, particularly with radio or telephone
2. Communication between two sites not under a common user is worse than awful
3. Work involving two sites requires a written and doubly signed inter-plant work permit.
4. Who has overall control of the procedure???????? Who issues it and who receives it?
5. Ignore compression ignition and inerting at your peril!

3 MAINTENANCE

Study 3.1 A toppled crane

Background:

1. The plant handled cryogenic hydrocarbons.
2. World wide experience showed that cryogenic hydrocarbon leaks had caused a number of serious incidents so a "Gas Barrier Wall" (GBW) was installed – Figure 3.1. This was 5 off 25 cm concrete slabs (1.25m in total). The height was not scientific but was called "*the psychological height of attempt*", that is, would you climb it in an emergency!? (The author of these studies ran over hurdles which were 1.05 m high). Behind the wall were sections of steam pipe drilled with vertical holes such that the upward momentum of the steam jets would entrain gas and air diluting the gas by "momentum transfer". In addition an array of Gas Detectors were installed at an elevation of 0.75 m - not good for the knees. (Figure 3.1)
3. There was a plant rule, Standing Instruction, that NO internal combustion vehicles were allowed inside the GBW.
4. There was a second, but unwritten plant rule that nothing was to be lifted over live, pressurised, equipment.
5. A materials handling study had been carried out on a plant model which showed that all equipment, control valves, pressure relief valves (PRVs) and pumps could be removed from the plant using bogies, tracks and block and tackle. (The author of these studies was on that study).

The incident

Sometime in the life of the plant a pressure relief valve (PRV) has to be removed for inspection, this is normal and is usually on a 2 yearly routine. There are two ways that it could be lifted down, the first is to use the davits, as supplied, which was the design intent – but this will involve riggers. The second is to remove the PRV by use of a crane.

In this case the plant handled cryogenic hydrocarbons and the global incidence of leaks made the management fit a "Gas Barrier Wall" (GBW) around the plant. Inside the wall are hydrocarbon gas detectors as shown in figure 3.1

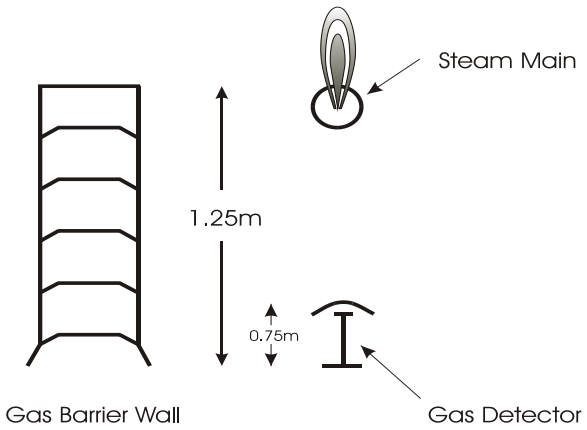


Figure 3.1 The basis of a "gas barrier wall" in the text

The plant in question was **not** shut down due to the general appearance (lack of scaffolding) and other maintenance effort. (The photo of the plant will be made available after the "inquiry".) You have to decide which of the two removal methods are to be used but it should be noted that there is a written Standing Instruction (SI, WGO, PI) that internal combustion engines are **NOT** allowed inside the GBW.

The choice is open to debate. A swinging or dropped load on a davit is potentially a hazard if not controlled/supervised properly as instruments could be damaged. In addition there will be riggers who do not necessarily understand the process operations of the plant. A crane might seem to be an easy solution but there was an historic, but unwritten rule that no lifts should be made over pressurised equipment.

Question 3.1.1

Which method would you choose?? You make the decision.

Answer 3.1.1

In reality the PRV was lifted off by a crane outside the GBW and as it did the crane toppled onto the plant, this required a shut down for the recovery (photo below)

Question 3.1.2

Why did the crane topple?

The essential information is as follows:

1. The crane had a MAXIMUM lift of 15 tonne
2. PRV weighted 150 kg (that is the load on the hook)
3. Extended jib 35m
4. Jib angle to the horizontal 30^{o}
5. Weight of jib 1.75 tonne treated as a uniformly distributed load
6. Crain weight 10 tonne
7. Outrigger spread 6 m
8. The outriggers were secure and did not sink into the ground
9. The crane was fitted with a *load on hook* alarm – not to exceed 1.5 tonne. Load on hook does not convert to toppling moments.

Check the maths or insert your own values.

Answer 3.1.2

Using simple moments about the outriggers the crane was not at the tipping point until the load from the PRV was on the hook. Photo 3.1 shows the outcome. The plant had to be shut down to affect a recovery of the crane!! Nothing was gained!!!!

Note that once the crane starts to topple the moment arms and centres of mass will change and the toppling rate will accelerate. The load on the hook has to be reduced immediately.

Key points for teaching.

1. Had a "statics" study been carried out – MOMENTS about a point – simple "A" level Physics. NO!

2. What made the new Manager deviate from the original intent? Lifting over live plant was a definite "***no-no***" on that Works but it was not recorded in writing! Ignorance? Bravado? "*I know best*!" Had a Risk assessment been carried out? Obviously NO! (See notes on Human Failure and Audits)
3. Was the crane driver fully briefed/trained/supervised? NO!
4. Had a full "risk assessment" been executed on the job to be carried out? NO!

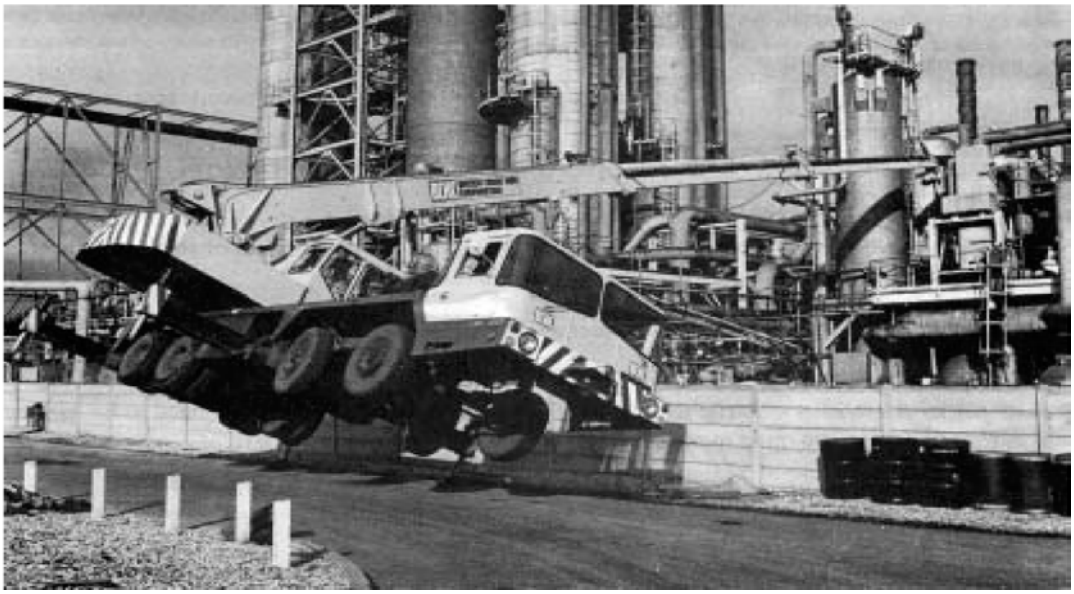


Photo 3.1 The "toppled crane" from ICI Safety Newsletter

Question 3.1.3

1. Why was a lift over live equipment allowed? (It was the "easier" of the two options).
2. It was a deviation from custom and practice. Why was a static analysis of an extended lift not carried out – risk assessment?
3. Could the crane be oriented differently to avaoid the toppling moment?
4. Was the driver/contractor competent to carry out such a lift? The maximum load usually applies to close in lifts not long reach lifts.

Answer 3.1.3

1. The new manager "knew best" and deviated from time established custom and practice! There had been a violation of the plant rules.
2. It is possible that the new manager had not been trained in "risk management" (or knew better!)
3. No one had carried out a simple moment analysis.
4. A cheap approach to the lift had been adopted and a detailed ***Management of Change*** had not been carried out.
5. A "*risk assessment*" had not been carried out.

Study 3.2 A Geyser

Background

Consider the mechanism driving a geyser. The water leaks from an aquifer and is heated, underground, by the hot rocks. Provided the flow is reasonably high the rate at which the water is heated is less that the rate of suppression of the water boiling point by the imposed hydrostatic head. At some point that column becomes unstable and starts to boil at the base, this displaces some of the column upwards so reducing the hydrostatic head and accelerates the depressuring (boiling off) of the superheated water at the base of the column. This is a geyser. The flow into and rate of heating are such that the geyser, such as "Old Faithful" in Yellowstone NP USA, is quite predictable.

This might seem a bit odd to be included under maintenance – but read on.

The incident

Figure 3.2.1 shows a typical steam pressure relief valve (PRV) arrangement. The PRV has a vertical tail pipe, to avoid any steam burns to bystanders should it lift, which is fitted with a "weep hole" of about 5mm diameter at the bottom. (See fig 3.2.1) The design intent of this hole is to drain any steam which had leaked passed the PRV metal seats and condensed on the cold vent pipe (or rain water that may have accumulated in the pipe.) This steam condensate, if not drained, would impose a back pressure on the PRV, increasing the lift pressure, and it would create corrosion of the elements in the PRV causing it to stick shut, hence the drain hole is a **key safety feature**.

One day there was a violent eruption of hot condensed steam from the tail pipe!

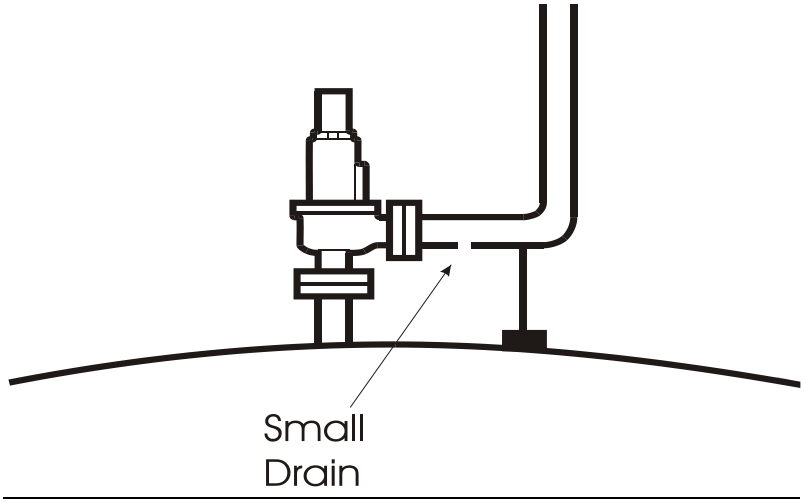


Figure 3.2.1 Typical steam relief line

Question 3.2.1

Why did this happen? This has been witnessed by this engineer!

Answer 3.2.1

1. If the drain hole is choked any slight steam leakage generates condensate which builds up as a column of water, the column is heated by conduction from the PRV internals or the leakage of steam. There must be a balance point of heat gain against suppression of the boiling point of the condensate
2. More importantly the drain hole is actually a safety system – who checks it? In many cases the answer is "no-one".
3. Figure 3.2.2 (below) shows what happens when the line is not properly supported against jet reaction.

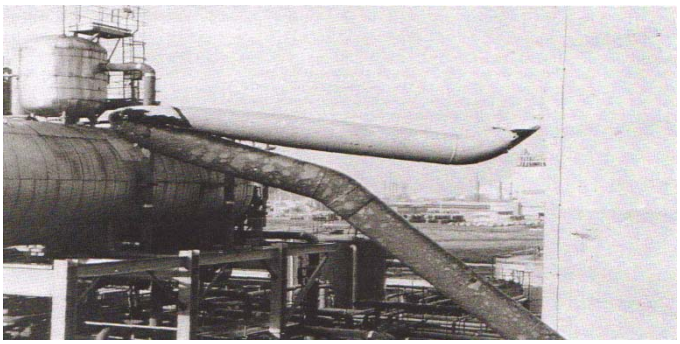


Photo 3.2.2 A bent steam vent line taken from ICI Safety Newsletter.

Key points for teaching.

1. The drain hole in the tail pipe of a steam pressure relief valve (PRV) may appear to be trivial but it is a safety feature. The function is to remove (drain) any condensed steam passing the metal to metal seats. This avoids a back pressure and prevents corrosion of the PRV internals.
   The weep hole is an essential safety feature which must be cleaned/maintained on routine.
2. Did the operations team know of this?
3. Who was responsible for checking the integrity of the valve and drain hole – (function testing it)?
4. What was the secondary effect of spraying boiling water? People could get scalded!!
5. If a system is "*out of sight*" it is also likely to be "*out of mind*" and not come under the control of anyone!!!

Problems with steam.

1. Steam is treated as a benign fluid. It is anything but benign. I have seen many variations of this problem and as the steam system is "only steam" it is not treated seriously.
2. Steam mains can be split by what is called a "steam hammer". This can only occur when the pipe is being heated up from cold. The usual approach is to open all of the drains on the main (NOT steam traps). The condensate is driven out of the main and the steam main can then be pressurised slowly over about one hour. During an initial plant start up some years ago the drains from a 50cm diameter, 60bar steam main were, in reality too small to drain the condensed steam being generated during the warm-up, as a result there were three hammers of increasing ferocity before the steam flow into the main could be isolated. The last caused the piping to move about 10 cm – a quite disturbing sight! It is surprising how fast you can run when the devil drives you!!!
3. Some years ago a steam main in a site 30 miles east of Glasgow split due to a steam hammer resulting from inadequate condensate drainage during a "cold start up" following a site shut down.

Roll-over

There is a variation of the "geyser" called a "*roll-over*" in cryogenic storage tanks (and Texas City Refinery). In this there is incomplete mixing of layers of cryogenic liquids or hydrocarbons of almost identical composition. In the layering one, denser, layer may have a slightly higher boiling point (fraction of a degree C) with a less dense and lower boiling point material over-layering it. However, heat is still gained from the atmosphere, the soil or heaters installed to prevent frost heave and due to the differential density it does not mix. The boiling point of the lower, denser layer is suppressed by the hydrostatic head of added material and due to the slight density differentials it does not mix. Eventually the lower layer reaches its new boiling point or the density fall due to the warming allows the hotter lower layer to mix with the colder upper layer. This results in a rapid boiling pool (which induces a new mixing process resulting in a steady boiling of the tank contents.) This has been known to go on for some hours.

Incident 3.3 A major fire

The Incident

The sequence of events can be put down simply as follows:

1. A pump was under maintenance
2. The isolation standards were poor
3. There was a major fuel spill from the pump
4. The fuel ignited
5. An emergency isolation valve did not close
6. Persons were trapped
7. There were fatalities
8. The structure had to be demolished by explosive charges due to the fire damage

Question 3.3.1

Where did this fire occur?

Answer 3.3.1

Most people respond "Piper Alpha". NO IT WAS NOT. It occurred in 1967 in a refinery in Teesside but it has been lost to the memory. If the memory was still alive some 167 persons would not have been killed on Piper Alpha!!!

The incident

The full story is as follows, most of the above was correct but some minor points were omitted.

1. A crude oil distillation column had a side-stream stripper which produced diesel oil. The auto ignition temperature for diesel oil is about 200^{o}C (how else could the compression ignition occur!)
2. The temperature of the off-take was about 200^{o}C.
3. The off-take pump was running "rough" and a damaged bearing was suspected. The spare pump was put on-line.
4. The pump was scheduled for an inspection first thing next morning.
5. It was "tradition" that the spare pump (in this case the damaged one) was left with the suction valve open and the discharge valve closed in case the on-line pump failed or shut down.
6. A permit to work for the inspection was issued.

7. The inspection revealed a seriously damaged bearing and it was decided to remove the pump for maintenance.
8. The Supervisor noted that there was already a permit to work on the pump so the pump was removed using this (**the inspection**) permit.
9. The fitter was asked to break the joint at the body to assist in removal.
10. The fitter reported after the event that he had to "*hang a chain operator over an extended valve spindle as it got in my way*". (The suction valve for the pump was above head height and it was necessary to fit a chain over a pulley to operate the valve. This is a poor design but can a necessity with large equipment.)
11. Diesel oil blew out of joint on the pump as it was broken because the suction valve was not fully closed (see 9 above).
12. The diesel oil ignited spontaneously.
13. The emergency isolation was activated but did not close (it is possible that the fire damaged the shut-in mechanism).
14. Three persons were trapped and died.
15. The damage was such that the only safe means of demolition was by severing ligaments with shaped charges. The only success was that the structure and column fell within 25 cm of the desired line.

Question 3.3.2

How did this sorry sequence occur?

Answer 3.3.2

1. The slow drift in standards is sometimes difficult to detect
2. The culture had also drifted. A permit has to specify the task. It can not be used for two tasks. See also Part D.
3. In this case the site had moved from "slip plate" isolation to an in-house form of valve isolation as the plates were heavy and difficult to fit. (A cultural drift)
4. In addition the approach to "site inspection" prior to maintenance had drifted.

Question 3.3.3

Would this drift have been detected by an Audit?

Answer 3.3.3

YES it would! As a result it can be concluded that there had also been a drift in the Management of Safety!!!

Key points for teaching.

1. The site condition may change over a short period of time. The site should be inspected before any work is started and if necessary at regular intervals to ensure the conditions have not changed. (See incident 3.4 below)
2. A permit to work is specific to the task described. If the task changes a new permit MUST be issued and a site review carried out as a result.
3. The quality of isolation was poor. Reliance of human intervention is not really acceptable (See also Piper Alpha) and a positive isolation using a lock-off system is better and positive isolation using blinds is even better.

4. Changes in working practice should be considered under the Management of Change system

Post script

At the inquest it was reported that the permit was drafted by the previous shift and that the pump was fully isolated at that time. The on-coming Foreman who had returned to the job after a week break was busy "catching up" on the last week's events so signed the permit without carrying out a site inspection. (Information or work overload). It is just credible that the pump was isolated when the permit was drafted BUT then someone put it into a "ready-to-start" configuration. The lack of site inspection due to the work overload at this hand-over was a key driver in this event as was the use of a permit to work for a use for which it was not issued (the inspection only).

As a minimum standard the valves should have been locked in a closed position with some form of "tag" or warning notice.

Incident 3.4 A change in conditions

The incident

During an Audit of the Safety Systems on one site the Production Supervisor received a radio message to the effect that the limits for flammable gas concentrations in a work area involving some welding had exceeded the limit specified in the work permit (10% LFL). The reply was "*carry on and I will alter the permit*"; the site was NOT inspected.

Questions 3.4.

1. What would you have done
2. Is this acceptable
3. If not what should have been done?

Answers 3.4.

1. It is **NOT ACCEPTABLE** to change a Permit to Work without a review of the causes of the change in condition.
2. The work **MUST** stop; the PTW **MUST** be cancelled.
3. The site must be inspected to ascertain the cause of the change in conditions.
4. A new risk assessment (as in the PtW) should be carried out.
5. Once proven to be acceptable, and only then, can the Permit to Work be reissued and the work allowed to proceed.

This conversation was made in front of an Auditor - myself! I was speechless!!

Incident 3.5 Isolation standards

Background

Occasionally isolation valves “leak”. The typical valve has a metal to metal contact and debris in the contact zone can result in leakage. (Some valves have soft, PTFE, seats and they are subject to wear [and tear]).

The valve integrity, tightness of the closure, is critical to the safe removal of equipment for maintenance. Various strategies have been evolved. One is to carry out a “risk assessment”, this results in a steady increase in the integrity or quality of the isolation with the fluid pressure and its hazardous properties. (See part B Design) Each case is company specific but typically water will only have a single isolation between the water main and the equipment to be removed. At about 40 bar the requirement is for “*double block and bleed*” for flammable materials. This arrangement has TWO valves in series with a vent (bleed) for leakage to a safe area. The thinking is that if the UPSTREAM valve is tight shut there will be no leakage but if the UPSTREAM valve is leaking the leakage can be lead to a safe area and that the pressure in the interface between the two valves will be low and any leakage passing the second, DOWNSTREAM, valve will be trivial. In general this arrangement has served the industry well. 40 bars is a convenient pressure as it is also a transition pressure between two pipeline pressure ratings (ANSI 300 and ANSI 600). ANSI is the **A**merican **N**ational **S**tandards **I**nstitute and the pressure ratings, in pounds per square inch, are the maximum allowable pressure at fixed conditions. By coincidence the maximum pressure is about 2 times the rating at 40^{o}C).

It is possible to fit an ICE PLUG in a line to form a good standard of isolation in an emergency. It is formed by fitting a bath round the pipe and then freezing a plug of ice using liquid nitrogen in the bath. It is not quite as simple as it sounds as there has to be careful analysis of the metallurgy (low temperature embrittlement of steel) and the bath orientation. A vertical bath is better than horizontal as in the vertical orientation there can be no gas pockets. Even better is to have a bend downstream of the plug into which the plug can lodge.

The incident and plan

Figure 3.5.1 shows an isolation arrangement.

The upstream valve “Z” is passing and the downstream valve has a small by-pass to allow the slow pressurising of the system. A large valve is difficult to control and the forces on the valve, due to the differential pressure, can be so large that is difficult to open the valve. The smaller valve is easier to us and can be used to reduce the pressure differential across the larger valve.

(There is a subtle teaching point that in this specific case the by-pass valve was fitted at the bottom of the line (180^{o}) where fluids might accumulate and cause *interface corrosion*. Ideally the valve should have been fitted horizontally at the 90^{o} position; it can not be fitted at the 0^{o} position due to the master valve fittings.)

The by-pass valve piping was corroded due to interface corrosion and the small section of piping had to be replaced this involved removing one of the double block valves plus the bypass valve. As the upstream valve “Z” was leaking it was decided that an ice plug isolation would be formed in the vertical section of piping, at the hatched section of piping, by water injected through valve “Y”. The combination would be integrity tested by pressurising the interface between the ice plug and an expandable stopper or bung fitted inside the pipe as shown. In effect this was to become a new “*double block and bleed*”. The first isolation was the ice plug and the second was the expandable plug.

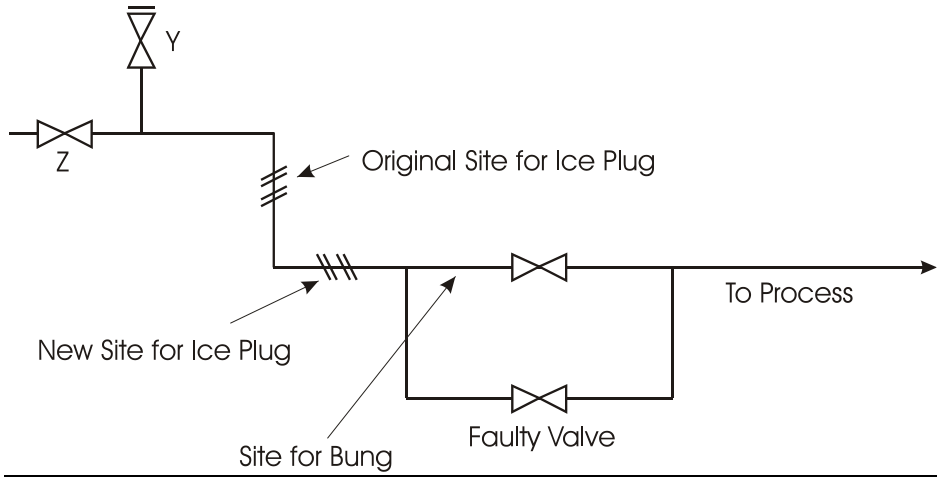


Figure 3.5.1 Simplified P & ID of work site

For various reasons the bung could not be proven to be pressure tight.

In addition the level measurement in the nitrogen flask failed but the contents could be assessed by weight.

For various reasons the ice plug could not be fixed in a vertical section but it was fitted in the horizontal orientation – as shown.

Finally the nitrogen flask went empty but the reserve could not be fitted due to thread damage.

The ice plug blew out!

Question 3.5.1

You have to carry out a risk assessment of this method knowing that it has been used successfully many times. What might go wrong and how can you mitigate this?

Answers 3.5.1

1. The supply of nitrogen is critical to the integrity of the ice plug. In risk terms the on-site, proven and available, supply of nitrogen **MUST** be significantly more than that which might be required as delays occur with even the best run plans. This would include "function testing" the hose threads to ensure that they are not damaged.
2. The ice plug **MUST** only be installed by a competent team and after a full metallurgical assessment.
3. The ice plug **MUST** be proven to be tight.
4. Once started the work **MUST** not be delayed.
5. The replacement section **MUST** be pre-prepared and readily available.
6. If there is a failure of any item 1 – 5 the work must not start.
7. What has been missed????

Question 3.5.2

Why did it occur??

Answers 3.5.2

This can be presented as a question or it can be fed as a number of defaults in the plan.

1. At which point MUST the work be aborted?

   Stop as soon as the first domino falls. The original plan had a number of defences in place (defence in depth) but once one defence was damaged safety was compromised.
2. Is there a spare nitrogen flask?

   There is one but are the hose threads damaged and can the connection be made within 5 minute?. The fittings on the spare flask were damaged and it could not be fitted. It is now too late as the plug will now melt and there is the inevitability of a leak. Note the word PROVEN in requirement

   The connections on the spare flask should have been checked BEFORE the work started – it is too late when it is found damaged when required. There is a parallel here to function testing protective systems.
3. The plug was set in a horizontal piece of pipe (due to access) and not the in the planned vertical section as intended. Is this acceptable?

   Probably not, as the bonding between the plug and the wall will be different particularly if there are any gas occlusions.

   There has been a deviation from the intent so the work should stop and a new risk assessment must be carried out.
4. If the expandable plug can not be fitted how can the plug be "pressure tested"?
5. The failure of the level measurement is not safety critical as the flask could be weighed and an approximate level assessed with sufficient accuracy. However it should have set the warning bells ringing!!
6. The difference between the horizontal and vertical arrangement is not a critical issue but the lack of a down-stream bend is potentially significant.

Key points for teaching

1. All changes have to be subject to a "***management of change***" process including changes to the change!!!!
2. This process should include a full risk assessment.
3. Changes from the plan **MUST** be risk assessed and if necessary work stopped. That is any changes in the plan **MUST** but examined carefully as it is a change in the intent!!!
4. Changes in the local environment are a potential violation of the intent.

Incident 3.6 A flare system modification

This incident is a mix of "Accident Investigation" and a genuine learning experience.

The incident

A new line was to be fitted in a flare system on a hydrocarbon production plant. A section of pipe inlet to the flare knock-out drum with flanges at each end (called a spool) was identified. The plant was shut down and during the shutdown some light, volatile, liquids entered the flare knock-out drum. (This satisfied the design intent of preventing liquids entering the flare tip). The flare pilots were NOT extinguished (Elgin

Franklin again). The spool was removed for modification. About 15 minutes later there was a loud “bang” heard “somewhere”. This was repeated 15 minutes later and again after 15 minutes!

Question 3.6.1

Why had this occurred?

Answer 3.6.1

1. A full risk assessment had not been carried out.
2. There is usually a small pressure differential in a flare. This can be due to the relative density differential of air and gases, or it can be due to the hot tip of the flare itself or it can be due to the eductive effect of the air flow across the flare tip. In this case the open end of the spool (inlet the flare knock-out drum) was the source of air ingress, the light, volatile, fluids in the knock-out drum evaporated so forming a flammable system. It would take about 15 minutes for the flammable mix to reach the pilot flame where it would ignite. The mix would then burn back to the knock-out and out of the open end at the spool where the flame from would be extinguished.
3. The pressure differential would re-start the air movement into the flare at the spool and the whole cycle would be repeated.

Question 3.6.2

What would you have done differently?

Answer 3.6.2

1. The pilots should have been extinguished. (However they are difficult to re-light!)
2. The open ends at the spool should have been “blanked off”.
3. The flare knock-out drum should have been inerted.
4. The flare drum should have been drained.

Are there any others? You decide!!!!!!

Alternative Question 3.6.3

What was the outcome? This is a more difficult question as it requires some more detailed process knowledge.

Answers 3.6.3

1. Panic and confusion! It took some time to identify the source of the “explosion”.
2. The flare main was over heated by the repeated flame front and expanded slightly beyond the design limit.
3. A MAJOR INQUIRY was initiated as to what had happened and why!

Key points for teaching

1. Any open end in piping or equipment has the potential for hazardous materials to flow out **OR** contamination (in this case air) to flow in.
2. It is important that there is a mental model of the operation and what happens inside the equipment so that the potential for an upset can be visualised and analysed.
3. A Risk Assessment MUST be carried out when **ANY** line or joint is broken.

4. Open ends in equipment have been the source of many fatal accidents (see incident 3.3)
5. Any break such as this MUST be positively isolated with a blank or locked closed valve.

Incident 3.7 – A crude oil tanker explodes while being off-loaded

Background

Sea going tankers are effectively a long rectangular tube. Loading (and unloading) has to be carried out in a predetermined sequence to avoid bending loads in the shell. This sequence is planned and may be confirmed by strain gauges within the tanked shell. Uneven loading such as the full loading the central compartments may result in a high downwards force at the centre of the "tube" and two resultant upward forces at the bow and stern. The bending moment created by poorly configured loading may be such as to overload (yield) the steel in the structure.

The incident

This is a true story of the explosion of the tanker Betelgeuse in Bantry Bay, Ireland.

The tanker had been in service for many years and was coming towards the end of its useful life. It was carrying a parcel of crude oil which it was offloading at the oil terminal. The transfer had stopped at the time of the incident and a significant quantity had already been discharged. A small fire was noted on the deck itself (a place of high stress during loading operations) and over a few minutes the fire spread slowly down the deck. Shortly after this the tanker exploded and large fragments weighting up to 1000 tonnes flew through the air.

Question 3.7.1

Why did this occur???

Answer 3.7.1

The answers may not be clear to a student but there are some serious teaching points:

1. Corrosion of tanker walls and also bulk carrier walls is a major problem. In the case of bulk carriers it is compounded by the impact and wear by the trucks used to clear the last remaining solids. Coal in particular is also potentially corrosive.
2. The bending moment created by uneven loading may be such as to overload (yield) the steel in the structure more particularly if it is corroded and thinned, as it was. See also background.
3. If the tanker shell and the internals are thinned and then the tanker put under an extreme bending load it will tear and the tear can (and has done) ignite the fuel vapours. Eventually the flame could reach a large container of air and flammable gases and as they say the rest will be history.
4. There is usually a corrosion allowance built into the original design but equipment ages at different rates. The real rate of corrosion may be higher or lower than the designer specified.
5. **As the equipment reaches its life expiry it becomes more and more important to carry out non-destructive monitoring for material losses and to adopt a more critical approach to the maintenance and monitoring strategy**.
6.

This is now called "Risk Based Maintenance"

7. It is not clear if the tanker was being inerted during the offloading cycle. However if the tanker shell was damaged air could still enter the tanks themselves.
8. The monitoring strategy should also examine if it has been operated outside the original design envelope or if it has been abused.

Key points for teaching

1. Equipment, like humans, ages and becomes more vulnerable with age
2. Inspection of aging equipment is now **risk based** and is one of the points that the HSE look at ***very carefully***
3. Once a crack appears in steel there is a stress intensification which can generate a running tear – it just runs and runs

4 UPSET CONDITIONS

Background

It is worth a reprise of the earlier notes on "the brain". There are five main mental states:

1. Information overload where the operator has too much information and can not differentiate the key, essential, factors that are relevant to the situation.
2. Cognitive dissonance where the operator reads the information being transmitted in warnings but works the warnings into a different but less hazardous scenario thinking that there is not a problem.
3. Mind set where the operator has a fixed idea as to what is happening and can not or will not change
4. Lack of knowledge (ignorance) where the information is not in that person's knowledge base.
5. Panic where the operator is so confused that he/she is unable to make a logical assessment of the situation and as a result does nothing or makes a dangerous action.

These conditions are usually catalysed by an event which requires prompt action.

In one event involving the electrolysis of brine to produce chlorine the hierarchy of the alarms was so configured that the "high oxygen" was the top alarm and stopped the transmission of other alarms and warning signals which were essential to the diagnosis of the problem. The operator was overloaded with the repeated oxygen alarms and could not make a reasoned diagnosis of the problem, the cell exploded.

Incident 4.1 Pollution of the Rhine at Basle or pressure to make decisions

The incident

A warehouse on the banks of the River Rhine at Basle contained a number of products one of which was a mercurial insecticide. During the night there was a fire, the suggestion was that it started on a shrink

wrapped container; the fire spread to the rest of the warehouse and enveloped the mercury based insecticides.

The smoke from the fire drifted across houses and the Fire Chief, not knowing what chemicals were in the warehouse, had to decide if the fire should be allowed to burn out or if it should be attacked. He adopted the latter plan not knowing that there was a mercurial compound in the warehouse. The firewater dissolved the mercury based compounds which ran off into the Rhine so resulting in the deaths of a number of fish.

Question 4.1.1

What was the fundamental error in the emergency planning for the warehouse and how has this now been addressed by legislation.

Answer 4.1.1

There was NO emergency plan and the Fire Chief did not know of the contents of the warehouse or the impact of fire water on the contents. The lines of communication were very dubious or flawed. Is this a repeat of Buncefield? The Fire Chief was put under pressures to kill the fire by the impact of fume/smoke on the neighbours but those requiring this did not comprehend the potential impact of this action. That is there was NO emergency plan which might reflect the materials stored in the warehouse!!!!

Question 4.1.2

Could this happen now? What has happened in the intervening years?

Answer 4.1.2

The Seveso II Directive now applies to Warehouses and the impact of any event on process plant or a warehouse on the environment. The safety case will include an assessment of the composition of the water run-off and the dispersion and nature of the reaction by-products formed in a fire.

Key points for teaching

1. An emergency plan must reflect the nature of the materials stored on the site
2. The emergency plan must develop with **any** new materials stored and could require a safety case
3. The emergency services must be involved in the development of the plan.
4. The emergency plan must involve the "neighbours".
5. Any changes to the storage may invalidate the plan.

See also Allied Colloids LPB 132.

See also Salford LPB 132

Incident 4.2 You have only 30 seconds to make a decision and act on it!

Background

The section of a centrifugal compressor is shown below. The lighter coloured (yellow) section is the body and stationary elements. The darker coloured sections (green) are the rotating elements, shaft, step up gear box and impellor. Within the impellor (and the volute or the section where the kinetic energy is converted to pressure energy) are vanes which are designed on vector analysis to avoid shock flow. The

pressure rise is roughly 50% in the impellor and 50% in the volute. The pressure differential between the inlet and volute (where kinetic energy is converted to pressure) could result in internal recycles so internal seals called “labyrinths” are fitted. The name “labyrinth” is very descriptive of the shape and function of this seal – it is a tortuous path creating the maximum turbulence and so limits the gas flows. The gaps between the stationary and rotating elements are about 1mm.

The impellor is (usually) manufactured from two pieces of steel, one has the vanes and the other is plain. The fitting of shaft and impellor is metal to metal and not welded. The impellor is “shrunk fitted” on the shaft and sits against a collar with a key between shaft and impellor to stop rotation (as shown).This requires heating the impellor such that it expands and then sliding it onto the shaft against a collar (shown) or stop while it cools and shrinks onto the shaft.. (Some smaller units can be fabricated out of a single casting or from riveted vanes in the impellor.) Compressors can ingest light liquid mists of up to 2% by weight for short periods of time. Slugs of liquid can result in the torsional failure of the shaft OR they can create such high pressures inside the impellors so as to bend the two (rotating) parts of the impellor away from each other so as to make them rub against the stationary fittings. (Treat the impellor as a flexible system – the ρv^2 [pressure head and hence resultant force] for liquid is up to a thousand times higher than that of a gas). Alternatively the forces can physically move one or both parts of the impellor away from each other by a few mm such that it rubs on the stationary fittings (the tip speeds can be over 250m/s). Whatever occurs, twisting or rubbing, the damage will be severe!!!!

The incident

The Plant Manager arrived on the plant at 16.00 to carry out the end of day checks. The Supervisor was in the compressor house looking at the alarm panel which showed that the suction vessel to a large centrifugal compressor (10MW) had the high level and high-high level shut down activated but the compressor was still running!! The shut down system, including the alarms, had been tested 20 times already without any detected failures (failure rate less than 0.01 per annum) and it had been tested only 3 days earlier. As both the high and high-high level alarms were activated the situation appeared to be real but the probability of failure of the whole shutdown system was mathematically less than 0.001. Put another way if the machine was left running for a minute more there was a 0.001 probability of a major wreck-up resulting and 2 months lost production, on other hand if it was shut down there would be 12 hours of lost production AND the unknown but mathematically credible risk that there might be a serious upset during the shutdown and restart cycle.

What should be done under these circumstances?

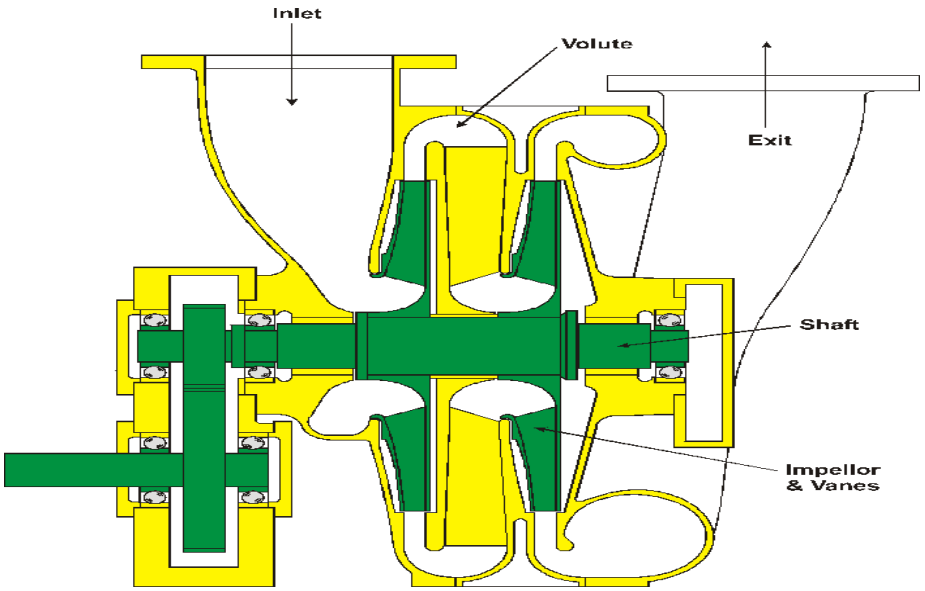


Figure 4.2 Section of a *simple* centrifugal compressor

Question 4.2.1

What is your decision??? You have 30 seconds to make up your mind, doing nothing is not a choice – get it wrong and you could be looking for a new job!

Answer 4.2.1

There is no "perfect answer" - see the introductory comments on the mental stresses.

In reality the Plant Manger told the Supervisor to delay the manual shutdown for 30 (and no more than 30) seconds while he gathered more information. It took 20 seconds (and it seemed like 20 hours) to verify that there was not a high-high level in the vessel so the Supervisor was asked to "stand down". How the verification was carried out is outside the scope of this incident study BUT the whole system was function tested (trip tested) properly and an electronic fault in the visual display was identified, this was quickly rectified.

The Plant Manger went home at 17.30.

Question 4.2.2

Was this the correct action?

Answer 4.2.2

It was in this case BUT .....How lucky can you get???????

The Supervisor challenged the wisdom of such an action, and he was right to do so. The Manager then wrote a Standing Instruction (SI) to the effect that only the Manager could take such a decision and that if the Manager was not present there was only one action –

SHUT DOWN.

Key safety teaching points

6. It is important that there is a mental model of the operation and what happens inside the equipment so that the damage potential can be visualised and analysed.
7. Sometimes it is necessary to carry out a risk assessment with very little time or room for error.
8. Equipment has a nasty way of fooling you! (Murphy's Law)
9. It would be nice if a comment could be made about the imperative of "trip testing" or function tests on shut down systems. The shutdown system performed correctly, it was an electronic card that failed to perform correctly! Maybe the message is that following so many tests the reliability had been shown to be very high which was instrumental in the decision making process.

Study 4.3 Collapsing vessels

The incident

A large vessel located 10m above the ground level with a design pressure of 400kPa was used to contact two fluids in a continuous extraction process. The vessel was full and the two fluids flowed counter-current. During maintenance the fluids in the vessel were displaced from the bottom with clean water. The operator then opened the drain located at ground level so as to drain the water. Initially he was a little surprised that the flow was very low until he heard the vessel groan and crumple inwards.

Question 4.3.1

Why did this happen and how could it be prevented?

Answer 4.3.1

The hydraulic head in the drain (barometric leg) was sufficient to create a full vacuum inside the vessel and so it collapsed inwards. The simple solution is to supply a vacuum breaker either procedural or mechanical. A simple vacuum breaker, depending on the nature of the fluids, could be no more than a non-return valve. Unfortunately the procedural approach is the least reliable.

Consider the relative strength of a coke can under internal pressure and external pressure. The can is strong in tension (internal pressure) but buckles when crushed inwards by external pressure. This also affects the strength of "*box girder bridges*".

There are variations on the basic theme; one being the draining of the tall vessel after a "*hydro test*". (Integrity test using water and a pressurising pump.)

Key points for teaching

1. Equipment may be strong against internal pressure but it might be weak against a vacuum – external pressure. This is evidenced by the "cola can" and the buckling of piping and structures such as box girder bridges.
2. Many pieces of equipment are located in structures many metres above ground level.
3. If the equipment is drained without a form of vacuum breaker it may collapse inwards.

4. You have to understand the changes in the static and dynamic pressure regimes when maintaining equipment.

Incident 4.4 Like Topsy it just grew!

This incident was taken from an article written by Bernard Hancock titled:

Human factors and systems failure: Case study of the fire and explosion at Chemstar

A fuller description, with drawings should be available through IChemE – if not the author has a copy.

The incident

This is a rewrite, with variations, of a true case history which has occurred more than once.

When a processes plant is demolished, some of the equipment is still in excellent operating condition and is sold on to another company who use it in a slightly different manner to produce new materials. The previous owner can only value the equipment at scrap metal value but the demolition team may value it as a usable item. In general the new processes are simple and do not require a "hi-tech" approach.

A process plant was to be demolished and the equipment was offered for sale in professional journals. The equipment fitted into the plans of a small entrepreneurial company who saw the opportunity to recover contaminated solvents using some of the distillation columns. Size and number of trays in the column was not an issue so it was operated fairly inefficiently from a thermal basis but as the cash flow was high it was not an issue. The initial operation was carried out by the "owner/manager" and a friend on an 8 hour per day basis.

The equipment was installed in an old warehouse. The process was quite simple. Solvents were fed into the distillation column on a batch basis, the heat to the re-boiler was supplied by a small steam boiler and the condenser was cooled by water from a stream which had been dammed off. Condensed solvents were received into a "reflux drum" and a small pump supplied the reflux to the distillation column. The process was controlled manually so as to produce the product of the correct quality. As the system could be over-pressured by steam there was a single pressure relief valve fitted to the condenser. Like any whisky distillery the relief valve discharged inside the building.

The cash flow was so good that it was decided to change the day work to shift work. This involved training shift workers and the original management team had to relinquish responsibility for the day-to-day operations. The rates increased over about 2 to 3 years. At the end of this period of increase there were a number of complaints from the local populous, particularly during hot summer days, about odours emanating from the plant. These were not actioned and production carried on.

One summer day there was a major explosion in the warehouse.

Question 4.4.1

Why do you think this happened?

Answers 4.4.1

The whole plant had evolved by two persons who, assumedly, knew what they were doing, worked on a one to one basis and had a minimum of operating instructions. As the throughput increased those who "had the knowledge" became more remote and was operated by the shift operators who did not have a training program for the process or operating instructions and also did not fully understanding what was happening. As a result the activities became more haphazard.

Equipment was not fully inspected and the evidence from the odours suggests that the condenser was either becoming fouled (three years without cleaning a heat exchanger is a long time!) or either the water supply flow was insufficient for the duty or the water temperature too high.

The venting into an enclosed space is dangerous and of course the boiler was a very powerful ignition source.

Like Topsy it just grew. There were no procedures, there was no management of change, and there was no maintenance in place. While the original intent may have been acceptable – just – once the operational controls are passed down to less competent personnel there has to be a training program, a monitoring program and more detailed procedures of what to do and why.

Question 4.4.2

Why was there an explosion?

Answer 4.4.2

The whole operation was done by word of mouth with little or no training, operating instructions or management!

The day to day maintenance was poor and there was no response to the "alarm signals" of odours in summer.

The heat exchanger had become fouled with debris from the stream; the Pressure Relief Valve lifted and vented flammable materials into n enclosed space. The vapours ignited at the boiler. (There are some parallels to Piper Alpha!)

Key points for teaching

1. The life of a plant is dynamic – nothing is steady and it changes with time.
2. The life of equipment changes with time – it can corrode and it can foul. This is particularly important with heat exchangers.
3. The production rates and spectra can change with time.
4. The management hierarchy can change with time.
5. The responsibilities can change with time.
6. Equipment performance has to be monitored and changes investigated.
7. There should be routine inspection procedures for key process items – planned maintenance.
8. **All of these changes have to be subject to a management of change procedure**.

Incident 4.5 High levels are a hazard

Background

1. Instruments can fail in a number of manners. Some fail danger and some fail safe
2. Loss of data can be a hazard in itself but is the data correct?
3. Traditionally when starting up a distillation column the reboil (heat at the base) is only started once a level is detected in the base of the column
4. Logically the reflux can only be started once the reflux drum contains fluids
5. If in doubt analyse all of the data available

The incident

The following are the facts:

1. The plant was being started up for the very first time (the initial start up)
2. A distillation column was being fed with cryogenic material
3. The response of the column – rate of level rise was unknown as some of the heat in the steel had to be removed by boiling off some of the feed material
4. There was both a level alarm and level measurement at the column base
5. After 30 minutes the temperature profile in the column appeared near to expectations indicating that some fractionation was occurring and that the metal was cooled to the operational level expected
6. There was no indication of a level in the base after feeding the column at half of the design rate for 30 minutes

This sounds like a variation on Texas City!

What should you do!

Question 4.5.1

What actions should be taken?

Answer 4.5.1

There is no point in carrying on with unknown levels in the distillation column. The column could be full, it can not be empty. Operating with unknown parameters is a serious hazard. Feed **must** be stopped and an investigation initiated.

A mass balance was carried out and with some allowance for boil off when chilling the column there should have been about 20 m of liquid in the base of the column!

(***If this had been carried out at Texas City the whole sorry story would not have occurred***.)

The level measurement was checked and appeared to indicate that there was NO LEVEL in the base for both the alarm and the controller level measurement. Odd!!!

The situation was made more confusing as the reboiler did not seem to operate so as to heat the base fluids! Very odd!

The investigation showed that there was a common cause failure of both the alarm and level measurement.

Question 4.5.2

Why do you think that the reboiler failed to heat the base fluids?

Answer 4.5.2

The hydrostatic head of liquid in the column (about 1.4 bars) was sufficient to raise the bubble point of the base fluid above the condensation temperature of the heating medium. The temperature differential across the reboiler during normal operation was only 7^{o}C.

(When it goes wrong, it really goes wrong!)

Compare the fact that the exit temperature in the Texas City heater was outside the operating band and nothing appeared to be happening

Key points for teaching

1 Simple mass balances would have prevented the explosions at Buncefield, Texas City and Texaco Milford Haven
2 Diagnostics are the key to analysing an unusual situation
3 It is important that there is a mental model of the operation so that the damage potential can be visualised and analysed

Incident 4.6

The incident

A distillation column is being fed with 40 te/hr feed at 250K. The top product was 35 te/hr and the base product was 5 te/hr.

Over an interval of 2 hours the pressure differential, bottom to top, rose steadily from 75 kPa to 150 kPa. (There were 120 trays in the column!)

There was no reason to suspect that the differential pressure measurement was faulty as it had been recording a value consistent with good operation for some days.

Question 4.6.1

What do you do?

Answer 4.6.1

Carry out a mass balance! Feed in = 120 te product out = 100 te at the top and 15 te at the base. There is a 5 te mass balance discrepancy.

Note: Normally the level of accuracy for a mass balance would be within norms of +/- 1 or 2% but in this particular case there was an accumulation of knowledge such that the real mass balance error was trivial.

Question 4.6.2

Where is the extra 5 te? Is it "holding up" in the "flooded" trays?

Question 4.6.3

What do you do now?

Answer 4.6.2 & 3

1. There probably is flooding of the trays.
2. Stop the feed to the distillation column as it appears to be flooded and spec will be lost quite rapidly.
3. The feed is stopped and the pressure differential does not fall! "*Instrument fault*" is the cry!
4. But wait! The base level is boiled off, the level falls to zero, nothing appears to be descending in the column (velocity time lag for changes in the reflux rate reaching the base = 10 minutes) and still the pressure differential is high. Is it a faulty instrument but where is the unaccounted 5 te?
5. One hour later the pressure differential fell to a reasonable value and the base level filled in!!! There was the 5 te of material!!!!!!

Diagnosis? The column had become fouled with an unknown material. For the chemists the previous part of the process involved hydrogenation of some impurities. The hydrogen stream contained traces of carbon monoxide. The following is the classic "methanation reaction".

$$CO + 3H_2 = CH_4 + H_2O$$

Doh! Water freezes at 273K

<u>Key points for teaching</u>.

1. It is important that there is a mental model of the operation so that the damage potential can be visualised and analysed
2. The rules that are applied in Chemical Engineering are correct and must be understood in an upset situation!

5 OTHERS

Background

The English language is complex and the same word could have different meanings in different contexts, Further Industries develop their own "jargon" and sometimes it is confusing to a new-comer. The problem is exacerbated by local dialect words. Some words that were acceptable in Dorset were considered to be rude in the N of England!

Study 5.1 Confusion in messages

Real Incidents

Question 5.1.1

- What is the difference between INFLAMMABLE and FLAMMABLE?

Answer 5.1.1

None! However in the English language **IN** is a form of negative. In this case the **IN** is a potential confusion. Does it mean not flammable? The correct word which has no ambiguity is ***FLAMMABLE***.

Question 5.1.2

What is the meaning of this sign hung on a manhole of a vessel under maintenance?

No Entry.

Permit Required

Is this statement logical? Does it mean ENTRY REQUIRED or NO ENTRY PERMIT REQUIRED?

Answer 5.1.2

No! The full stop is easily missed! Can entry be made without an entry permit? (As a generality the answer must be NO!)

Question 5.1.3

Is the following an acceptable instruction?

Open the Valve.

Answer 5.1.3

- Which valve? Give it a unique reference number.
- At what rate should it be opened? If too fast the control system may be unable to follow the ramp up rate. If too fast there may be a water hammer.

Question 5.1.4

Is the following statement acceptable?

Add 100 kg of material xxx

Answer 5.1.4

No! At what rate over a day or a year? – Define the interval correctly. This may be a safety critical operation with exothermic reactions. Are there any other pre-addition conditions which have to be satisfied?

Question 5.1.5

Is the following statement acceptable? This may appear to be a trivial case but it is not so! An instruction read:

"**Add a carboy of acid X**."

Answer 5.1.5

Yes! You are right! The acid and carboy were added to the reactor without opening the carboy! When this was told as a story in a meeting someone said:

"**That happened to us as well**!"

If it is garbage, do not blame the Operator – it is the Manager who is to blame.

Key points for teaching.

1. If it is garbage, do not blame the Operator – it is the Manager who is to blame.
2. Keep the message concise and do not use technical gobbledygook.
3. It is important that there is a mental model of the operation so that the damage potential can be visualised and analysed.

Study 5.2 Exploding pumps

Background

Centrifugal pumps are a demonstration of the classic ***Joule*** experiment on "*the mechanical equivalent of heat*." There are a number of potential recycle paths in a pump, one being the recycle round the wear-rings, there are also inefficiencies which result in the generation of heat. The classic pump characteristic (below) shows the head, flow and efficiency curves. At flows below about 10% maximum flow the efficiency falls rapidly and the fluids in the pump heat up. For this reason it is normal to include a "minimum flow recycle" (see the start up instructions in an earlier Part). However if a pump is run within closed isolations about 30 to 50% of the full load power is absorbed as heat by the "churning process" and the contents will heat up rapidly – the pump characteristic below Figure 5.2 is more applicable to large well designed pumps. As they heat the vapour pressure will rise accordingly and it is now a question of whether the boiling fluids can be vented fast enough to prevent an explosive rupture of the casing.

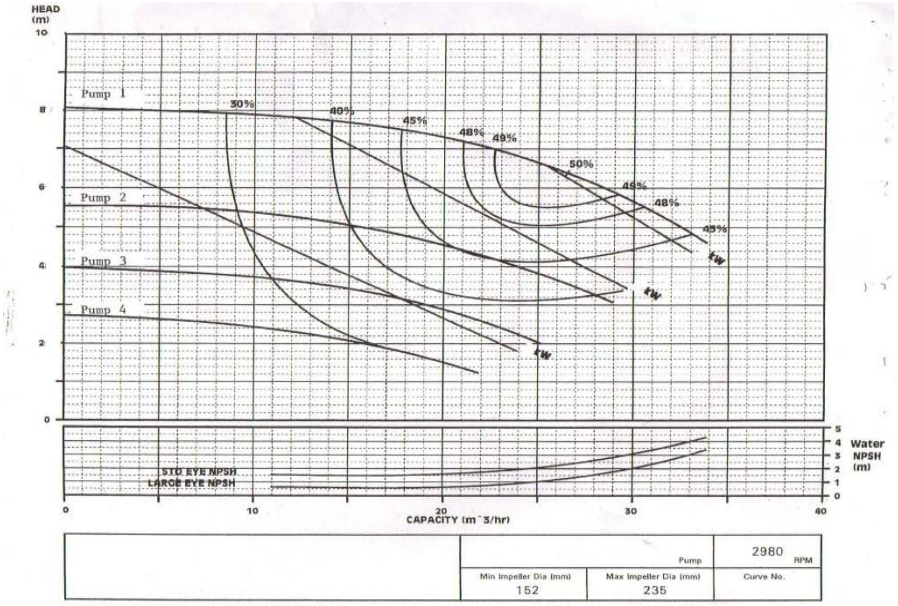


Figure 5.2 Family of pump curves

The power consumptions (diagonal upper left to lower right) are not given. As the flow approaches zero the efficiency approaches 0 but there is still a power consumption of about 30 to 50% full load.

Joule was a bright cookie.

It is sometimes appropriate to fit an "auto-start" on a pump which is activated by the shutdown of the on line pump – BUT in this case the suction and discharge valves must be automated to open on start up or the pump left with suction and discharge isolations open and the reverse flow arrested by a non-return valve.

The incident

A milk pump in creamery exploded without warning and fragments of the pump hit an operator.

Question 5.21

Why might this have happened?

Answer 5.2.1

The pump may have been started with closed isolations inadvertently by someone pushing the start button or it may have been started by an auto start. It is also possible that the pump was started deliberately but someone forgot to open the appropriate valves.

This occurrence happens with monotonous regularity.

In another example a pump was found running when the paint on the pump began to blister. The pump was removed and opened up. The contents had started to decompose leaving a coke type material. As the material was thermally sensitive it is a miracle that it did not result in a chemical explosion.

Key points for teaching

1. Joule was right!
2. Pumps should have some form of "minimum flow recycle"
3. Pumps must not be run within closed isolations – the start should be inhibited electrically or by procedure.

Study 5.3 Jet Reactions

The incident

Photo 5.3 shows the the tail pipe from a Pressure Relief Valve some 12" diameter which has been bent double. VERY FORTUNATELY the PRV reseated within a second or two as in the state shown in the photo the outflow would have been cut off and at best the PRV would not have protected the system and at worst the piping might have ruptured!

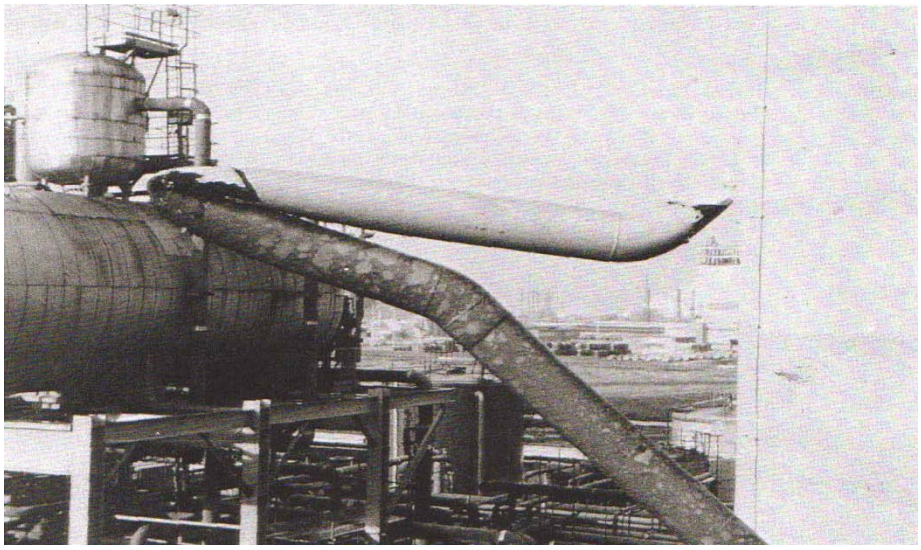


Photo 5.3 A bent vent line from ICI Safety Newsletter

Cause

The piping designer had a total lack of appreciation of the reactive forces produced by vents (and changes of fluid flow direction). The author missed his lunch that day!!!!

Background

Most tail pipes from pressure relief valves have robust supports to resist the jet reaction forces.

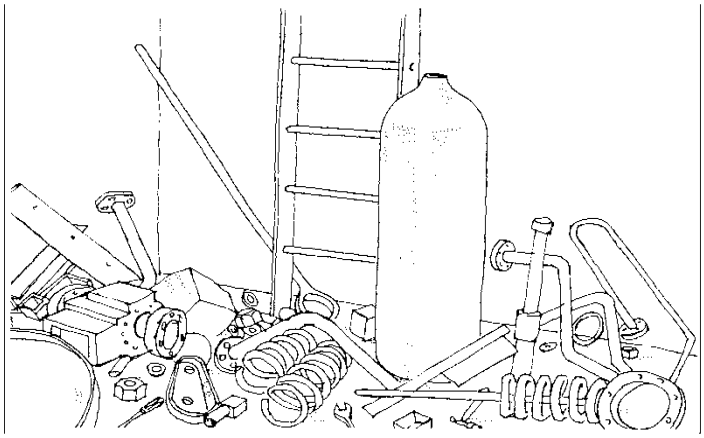
Key point for teaching:

Reaction forces can be enormous and piping has to be properly supported so as to resist reaction forces.

Incident 5.4 Cleanliness is next to godliness

Question 5.4.1

What is wrong with the following picture?



Sketch 5.4 Clutter (taken from ICI Safety Newsletter)

Answer 5.4.1

Many faults can be seen. These are just a few: -

1. The gas bottle should be in a restraining rack
2. The ladder access (and egress) is littered with trip hazards
3. Is any of the equipment contaminated?
4. Etc
5. This picture also reflects a management problem – the message from this photo is that the manager could not care tupence for safety.
6. The rest of the team will get this message loud and clear so the standards will spiral downwards.

Look round your own laboratories and you will see this picture in reality

Other incidents can be readily found in Loss Prevention Bulletins and ICI Safety Newsletters available from IChemE

Incident Studies more complex studies – Lessons Learned

The following are a simplification and adjustment of some real events which have an element of "*lessons learned*". The tutor can give as much background as is thought fit for that class.

There are a number of other incident studies which will be given later in this section.

The following are a bit advanced and may require some more background knowledge that might expected of a student.

Chernobyl is complex. A very good synopsis was written by Ned Franklin in tce November 1986. The paper is titled "The Accident at Chernobyl".

The Introductory paragraph reads "*The accident at Chernobyl was brought about by a series of deliberate actions which were either errors of judgement or disobedience of regulations in pursuit of an experimental test. Within 60 seconds of the start of the test there had been a gross but localised excess of power generation with insufficient cooling, a steam explosion and disruption of the whole top structure and shielding of the reactor* ;....."

The RBMK reactor was potentially unstable below about 20% of rated capacity. This was known and that zone of operation was forbidden.

The local electrical grid was prone to interruptions so an experiment was derived to bridge the power gap between the interruption and the emergency power generators coming up to speed. This gap would be a few seconds. The experiment was to use the kinetic energy in the turbo-alternator, as it ran down to produce electricity. The frequency would fall but be adjusted by thyristor controls.

It appears that the experimental program had not been planned in detail, more importantly the contingency planning for the experiment were nil. The preparation started at 01.00 25/4, this initiated a positive feedback to the reactor in the form of reactivity and neuron flux. At 02.00 the emergency cooling loop was disconnected from the forced circulation loop. Then there was a request to delay the unit test as there was an interruption to power supply to the area. At 23.10 (nearly a day later) "*they were unable to reduce power further*". This created unstable conditions. (Basically if in doubt go to a known stable condition and think it out!)

24 hours after the start it was possible to stabilise the conditions but still in the unstable regime because of the poisoning of the reactor it was difficult to control and control rods were withdrawn. At some point the staff over-rode emergency protective system (Help!). The control required was equivalent to inserting 30 control rods. At this point the reactor should have been shut down according to procedures.

"*At 01.23 4 seconds the stop control valves to the generator were closed. ....The available emergency protection for closing the stop control valves ....had been over-ridden so as to afford the possibility of repeating the test if the first attempt failed*". This was a deviation from the test program. Following this the thermal power started to increase. At 01.23 40 seconds the instruction was given to press the emergency protection button which would insert all control and emergency rods into the core. The rods did not descend fully. Maybe they were distorted by the experiment, and then there was a steam explosion.

The steam explosion resulted from heating of the fuel rods and the softening of their containment (zirconium). The boiler water and white hot fuel mixed and the sudden and violent evolution/generation

of steam resulted in the roof of the reactor containment being blown off. There followed some hydrogen explosions which resulted from the reaction of Zirconium with steam/water.

Following this incident the predictions were for 10,000 premature deaths mostly from thyroid cancers. To date the evidence suggests that this was too high. However it is of note that the premature deaths following Bhopal are in the region of 15,000 but no one talks about that event!

This case could be delivered as a simple transcription of the article (without the introduction shown above in italics) and then questions set such as: -

1. Was the experimental plan properly thought out?
2. What are the KEY safety features which must not be violated during this experiment?

Three Mile Island is also a nuclear incident but could be of use. A good synopsis is to be found in ICI Safety Newsletter 156.

LPB 102 gives a very useful case study on pages 17 – 19 involving the decomposition of organic peroxides and the resultant oxygen rich atmosphere. It may be a little complex for BEng students but it might be possible for the MEng students to unravel the threads.

Essentially an inerting system was inadvertently taken out of use while a compressor was repaired. As with many incidents the team did not recognise that there was a potential dead pocket while the compressor was off line. Oxygen rich hydrocarbons accumulated in the tank below the sample point (O_2 MW - 32 and hydrocarbons MW over 56 – butane.)

Key points for teaching

1. All maintenance has to be carefully planned
2. All maintenance has to be carefully risk assessed – as all maintenance carries an element of risk.
3. As the oxygen in the supporting atmosphere rises so the ignition energy falls. This was found in the Apollo 1 static fire disaster in the late 1960s.
4. LPB 102 was published after the Apollo 1 disaster. Did the company know of this incident and did they relate to it?
5. Lessons learned MUST BE circulated and read again and again.
6. This is main message of these incident studies.

Bhopal is a very complex incident which still creates much debate. Essentially water entered the storage for Methyl IsoCyanide and catalysed the exothermic decomposition of the material. There were a number of contributory causes:

1. A refrigeration unit was not available due to a lack of spare parts
2. There is debate as to the availability of an absorber unit in the vent system and also a flare stack (thermal oxidiser)
3. Some of the material had been contaminated with chloroform which was a catalyst to the decomposition
4. How the water entered the process is as yet still uncertain. Many theories have been proposed but none proven with certainty!

The main features of the incident were:

1. The amount of MIC stored was excessive and violated the INHERENT SAFETY PRINCIPLES

2. The public had moved towards the site and occupied what would be called a "*cordon sanitaire*"

The **PEMEX** incident in Mexico City has many of the features of Buncefield explosion.

There was a rather gruesome video titled "*The Day the Earth Caught Fire*" narrated by Orson Wells. This may not be available to most colleges. Some of the shots show partially cremated bodies so if it becomes available it may be necessary to carry out some prudent cutting/editing!

Essentially a large LPG storage and bottling facility expanded over the years until there were at least 4 large spheres and over 50 bullets (large horizontal storage vessels). As the site expanded the local housing moved towards the site. (Bhopal again?) The process relief was burned off in a remote ground flare. This is not uncommon in such facilities and can be found on sites in the UK.

As with Buncefield the stored material was produced some distance from the site and transferred to the storage/bottling site by pipeline.

One day there was a major leak of LPG. It is not clear if this was a joint leak or a pipeline rupture. The flammable gas cloud drifted towards the ground flare where it ignited some minutes later. The resultant fire generated a "domino effect" of rupturing (BLEVE) vessels. This suggests that the initial leakage was from a ruptured line. The causes of this are open to debate; it is unlikely that it was a trapped section of line without pressure relief as the leak would have died off quickly. It is more likely to have been a corroded line but the evidence is not available. It might appear that there was little (or no) remote isolation as the leak was not arrested.

The domino resulted in the rupture (BLEVE) of at least 4 spheres and most of the bullets. One section of a bullet travelled over 2 km.

The thermal pulse from a rupturing sphere would have been sufficient to kill anyone near the site fence. Houses were set on fire and over 500 persons were killed.

The damage profiles were such that most if not all of the site evidence was destroyed.

1. Was the leak site a line rupture and if so why? Was it due to corrosion and if so why had it not been spotted on inspection? (Was there any inspection of the piping in any case?) (See also Stockline Plastics – Maryhill, Glasgow)
2. Was there any semblance of sectional or remote isolation? The answer is probably "**no**".
3. Was a ground flare appropriate? The answer may be "**yes**".
4. Was there a structures planning development outside the site. The answer is certainly "**no**".
5. Could this event occur in the UK? A good question – large storage will come under COMAH but what about storage of camping gas cylinders at garden centres?

Clearly this installation would have failed the UK Safety Case. Mmmmmm! But the Buncefield Safety Case was accepted! Mmmmmmm!

Other Incident studies

There are potentially other useful studies in the BBC "Disaster series" and in the US Chemical Safety Board (CSB) Series. They can be played a number of ways to achieve an objective. However it is important that the study does not ignore the risk factor and differentiates the regulatory and cultural differences.

Each study has to be looked at carefully.

In the case of the Disaster series some of the quoted "facts" are inaccurate (*don't let the facts get in the way of a good story*) and in the case of the CSB there is a different cultural and regulatory regime which may confuse the analysis.

The **Challenger** disaster (BBC) was due, mainly, to the fact that the Solid Booster Rockets (SRB) were manufactured by Morton Thiokol and the contract was up for renewal. The pressures were immense! There was some evidence taken from the "web" which showed that the "blow-by erosion" on the seals in the SRBs DID increase with a reduction in ambient temperature. The data was a bit of a "scatter" but there was a trend and the conditions on the launch day were well outside the bounds of the data set.

There was the traditional "gung ho!"approach which might not apply in UK and some of the decisions were made at a high level without involving those who had all of the data. In this case the blow-by data. The telling comment is "*make a management decision*", note – "management" not "technical"!

The "lock all doors" is also procedural so as to preserve all data without any risk of corruption.

The **Piper Alpha** disaster (BBC) Spiral to Disaster has a number of inaccuracies which are discussed earlier.

The causes were:

1. Poor MoC
2. Poor design
3. Poor PtW
4. Poor isolation and control
5. Poor operating procedures
6. Poor emergency procedures
7. Poor practice of procedures
8. Poor planning of the fitting of the new riser (link between the platform and the sea bed)
9. Poor communication platform to beach inter and intra platforms
10. There must be more!!!

The **T2** (CSB) incident has a mix of cultural and regulatory differences. It could occur in UK but it is less likely. A (confidential) incident did enter the exothermic regime and although the pressure relief was designed to DIERS it did explode with fatal consequences. All the right things were done but they did not work as intended.

Texas City (CSB) misses a few critical aspects. Yes, there was operation outside the prescribed bands. Yes, the supervisor was not present. Yes, there was confusion as to the base level. There were a number of other factors discussed earlier.