

LINKING AN ACCIDENT DATABASE TO DESIGN AND OPERATIONAL SOFTWARE

Dr. John Bond. C-MIST

Abstract
The potential advantages of a linkage between an accident database and the software used in procedures for design, hazard and operability studies and in risk assessment are described.
An established software for the design of equipment is taken and the potential for linking it to an accident database demonstrated by simulating a design of a distillation column. This linkage will allow the design engineer to immediately learn lessons from past accidents and to incorporate them in the design at an early stage. A risk assessment procedure will be carried out using a "Risk Assessment Methodology" developed for the training of personnel. This procedure uses keywords and an accident database to identify hazards and to help in the provision of Control Measures. It will also assist in identifying hazards that may not be in the knowledge of the person carrying out the assessment. A HAZOP procedure software will also be used to show how linking with an accident database will assist in establishing a variety of possible scenarios and assist the team in reviewing the hazards that can occur.
The use of an accident database in combination with other software for design and operational work establishes a more user-friendly system for incorporating lessons learnt from accidents.

KEYWORDS**:** Accident database, design, risk assessment, HAZOP.

INTRODUCTION

Accidents that have occurred in the past have been investigated, often with associated research work, and have been adopted in engineering standards. Subsequent design work has used these standards to the benefit of the public, the employees and the company. Such a situation occurred after three very large crude oil carriers (VLCC) marine tankers were subject to explosions in December 1969. The *Mactra* was ripped open for 500 feet but reached port, the *King Haakon* was severely damaged but also reached port. The *Marpessa* caught fire and sank. In each case empty oil tanks were being cleaned by high pressure water washing equipment. Extensive research showed that ignition of flammable gases in the tanks was caused by induced electrostatic charges from the water washing equipment (1–5). This research work resulted in the adoption of inert gas systems on VLCCs and adopted in the International Convention for the Safety of Life at Sea (SOLAS). The marine chemical tankers were not required to have the inert gas systems due to research work (6,7) defining the maximum size of equipment to avoid the generation of incendive static charges. This was also incorporated in the SOLAS agreement. The research work of two major oil companies was shared with all companies, incorporated in the SOLAS agreement and became the standard for marine tanker design to the advantage of all companies, the crews of the tankers and the public.

However, due to a variety of reasons, not all lessons learnt are incorporated in standards or shared. Another marine example is in the carrying of 98% formic acid. An accident (8) on a marine chemical tanker occurred after discharging formic acid. The tank was washed with sea water followed by fresh water. A seaman entered the tank to mop out water and was asphyxiated by carbon monoxide. The ship's crew did not know that formic acid would decompose and that even if they had ventilated the tank and tested with an oxygen meter they would still have to test for residual carbon monoxide. The Material Safety Data Sheet at the time did not have this information but the information is shared in the Accident Database (9).

In order to be fully aware of hazards, engineers must consult an accident database to be certain that he is learning lessons from past accidents. This can be done by separately looking up in the database each and every piece of equipment that he is using and each chemical. Even then he may miss some hazards. Just as a person does not look up the spelling of words in a dictionary when he is writing a report, so an engineer may not always consult a database to identify hazards. The linking of an accident database to a software used in the design, risk assessment or review of design would make the process of learning lesson from accidents that more easy and user friendly. It could work in the same way that a dictionary is in the background of a word processor. Indeed, a facility for ensuring that a procedure adhered to the risk assessment could be likened to the grammar checker in a word processor, but that is for another paper.

The use of an accident database such as the IChemE Version 4 in conjunction with software for design, for risk assessment and in the review of a HAZOP flow sheet will be demonstrated.

DESIGN OF A DISTILLATION COLUMN

It is particularly important to identify the hazards at an early stage of the project as the capital expenditure rises as the project proceeds. Any modifications that may subsequently be necessary are more expensive the further you are into the project. With this in mind the design engineer must be aware of all the accidents involving the substances and equipment he is working on. If he is, say, designing the distillation column for ethylene oxide and had the Accident Database in the background of his design software the accidents associated with this equipment and chemical could be triggered. In this case he could find a message appearing on his screen as shown in Figure 1.

If the records for the 5 accidents are viewed, it will be seen that all involved explosions in the distillation column and were caused by:

- Leak from flange or weld
- Reaction in the insulation with water
- Auto-oxidation catalysed by rust with heating from an insulation fire

The lessons learnt are also given and can be incorporated in the design from the start.

- Reduction in the number of flanges or flanges to be left uninsulated. Areas of possible leak should be inspected and tested regularly.
- Upper part of reboiler must be covered. Avoid condensate backup.
- Positive purge of inert gases from shell.
- Ensure minimum heating temperature.
- Insulation non-absorbent and test for glycol formation.

- Avoid piping with no flow of ethylene oxide vapour or stagnant lines.
- Remove any rust from pipework.

Noting these lessons, and others, at this early stage of the design will ensure a saving of time at the HAZOP stage as well as making it unnecessary to make modifications later.

RISK ASSESSMENT

The stages of risk assessment for an individual task are:-

1. Identify the hazards for each task
2. Assess the risk associated with the hazard
3. Devise suitable control measures
4. Reassess the risk to ensure that it is reduced to an acceptable level
5. Produce a method statement

This process requires an experienced person or a team of people with an experienced chairperson to control the operation. Access to an accident database is also vital for the various stages to be fully assessed.

In the analysis that is done it is essential that all the reasonable hazards that are identified as possible are recorded and actions noted, even if the team decide the risk is so low that no action is necessary. Clearly a hazard that is so unlikely need not be recorded, e.g. being hit by a meteorite.

An accident database is an essential tool for identifying hazards and particularly if attached to the Risk Assessment Form software. Consider the risk assessment of a maintenance operation for the removal of a submerged pump from a vessel. Most hazards can be identified by an experienced maintenance person but other hazards can be identified from an accident database. The words maintenance and pump can be highlighted as shown in Figure 2 and the database questioned.

A flag could then come on the screen showing the accident given below.

No. 13152 **Date.** Unknown
Source: Loss Prevention Bulletin 078
Location: UK
Injured: 1 **Dead:** 0

Abstract:
A submerged pump on a horizontal vessel containing molten phthalic anhydride at 160°C was removed for repair at the workshop. To prevent fumes of phthalic anhydride leaving the 700 mm diameter manhole, a piece of jointing was placed over the hole with a piece of plywood to hold the jointing down. The electrical connections for the motor had been removed before the pump had been taken out. Nevertheless, a repair to the electrical connections was carried out by the electrician. During this work the electrician stepped onto the plywood which broke under his weight. The electrician managed to save himself by spreading out his arms. He managed to pull himself out without assistance, suffering only from shock

Lessons
Temporary covers over holes must be substantial. It is good practice to have a spare blank adjacent to the pumps for use when the submerged pump is removed.

The hazard of an open hole would be recognised and the lesson learnt. The control measure would be put into the Risk Assessment form for a blank to be bolted over the manhole even though it is outside the walkway.

After identifying the hazards, the next operation is assessing the risk. The risk is generally defined as:

RISK = PROBABILITY OF OCCURRENCE x SEVERITY

Table 1 shows the typical probability and severity tables used in a qualitative approach.

Table 1. Typical table used for establishing probability and occurrence

Rating	Probability of occurrence	Severity of occurrence
1	An unlikely/unknown occurrence. Very unlikely to occur during the operation/facility or process.	Scratches, minor burns, bruises or abrasions. Minor injury 1 person.
2	A remotely possible but known occurrence. Unlikely to occur during the life of operation/facility or process.	Minor injury, laceration requiring stitches, secondary degree burns or severe bruises. Minor injuries 2–10 people.
3	An occasional occurrence. Likely to occur once during the life of operation/facility or process.	Major injury to one person, broken bone, amputation, third degree burns. Major injury 1 person, Minor injuries to >10.
4	A frequent occurrence. Likely to occur from time to time during the life of the operation/facility or process.	Death or permanent severe disablement of one person. Major injury <5 people.
5	A highly likely occurrence Likely to occur repeatedly during the life of the operation/facility or process.	Multiple deaths or multiple severe permanent disablement. Major injuries >5 people or fatality.

These are, however, open to considerable variation of interpretation depending on the person carrying out the risk assessment and even with a group there can be considerable variations. A more definitive interpretation of the rating points is required. Table 2 gives a fuller interpretation of the ratings and should lead to less disagreement amongst the team.

Table 2. A more definitive table for establishing probability and occurrence

Rating	Probability of occurrence	Severity of occurrence
1	An unlikely/unknown occurrence. The team or person carrying out the Risk Assessment has never heard of such a hazard taking place either at his place of work or in another company, nor in any accident database, the media, his training etc.	Scratches, minor burns, bruises or abrasions. Minor injury 1 person.
2	A remote but possible occurrence: The team or person who is carrying out the Risk Assessment has heard about this hazard occurring in another company but not at his place of work, i.e. the hazard has not been experienced by the team or the person carrying out the Risk Assessment but it is reported in an accident database or the media.	Likely to result in minor injury, laceration requiring stitches, second degree burns or severe bruises. Minor injuries 2–10 people.
3	An occasional occurrence: The team or person who is carrying out the Risk Assessment has seldom experienced such a hazard at their place of work but it has occurred at another company and is found in an accident database.	Likely to result in major injury to a few persons, broken bone, amputation or third degree burns. Injuries reported in accident database or media reports. Major injury 1person. Minor injuries to >10.
4	A frequent occurrence: The team or person who is carrying out the Risk Assessment has frequently experienced such a hazard at their place of work and it is reported frequently in accident databases.	Likely to result in death or permanent severe disablement of one or more persons. Reported in accident databases or media with these conditions. Major injury <5 people.
5	A highly likely occurrence: The likelihood of the hazard taking place is very high and there is a greater chance that the hazard will take place than not.	Likely to result in multiple deaths or multiple severe permanent disablement. Reported in accident databases or media with these severe conditions. Major injuries > 5people or fatality.

Table 3 gives the risk ranking bands

Table 3. Table for establishing risk bands

Severity					
	5	10	15	20	25
	4	8	12	16	20
	3	6	9	12	15
	2	4	6	8	10
	1	2	3	4	5

Probability

Risk bands 12–25 Highly hazardous and highly likely event. In all cases the potential severity is too high to allow the operation to continue. Operation in this risk band be eliminated, avoided or totally replanned.

Risk bands 5–10 Within this band severity and probability are high and the work cannot be carried out until risk is reduced to an acceptable level. Mitigating the hazard can be via the provision of written procedures or work instructions, supervising the work, isolation or limiting exposure.

Risk bands 1–4 Within this band it is acceptable to carry out the work but with Appropriate personal protective equipment, warning signs, barriers, tannoy announcements etc to mitigate the initial risk.

In risk assessments the combination of the accident database with the software for the relevant forms provides a useful and user-friendly system for help in identifying and assessing the risks. Software for writing out Work Permits could be treated in a similar manner.

HAZARD AND OPERABILITY STUDY

The Hazard and Operability Study is clearly another area where an accident database should be linked to the software for carrying out the study. Take the case where a gasoline pipeline is being considered as the Node Point and "More Flow" is being considered. A possibility for more flow could result from rupture of the pipeline from internal or external corrosion. The pipeline metal is considered satisfactory for internal corrosion but the case of underlagging corrosion is considered a possibility due to its temperature of 40^{o}C. The Accident Database is consulted by the keywords 'pipeline' and 'corrosion' and the accident shown in Figure 3 would be brought up onto the screen.

The lessons learnt from this accident could then be incorporated into the main HAZOP document and control measures adopted from the lessons as shown in Figure 4.

CONCLUSIONS

An appropriate accident database with lessons learnt and a keywording system can be combined with modern design, risk assessment and Hazop software to provide a powerful tool for design and operational engineers to improve safety and hence reduce costs. The linking of the software is a logical step.

ACKNOWLEDGEMENTS

The author would like to thank Hyprotech (recently merged with Aspentech) the manufacturer of software for equipment design; C-MIST risk assessment consultants; and Rowan House hazard study consultants; for permission to use copies of their screens for this paper.

REFERENCES

1. Van der Meer, D. 1971. Pr. 3rd Conf. Static Electrification (Inst. Phys., Bristol) pp. 153–157.
2. Van der Weerd, J.M. 1971. Pr. 3rd Conf. Static Electrification (Inst. Phys., Bristol) pp. 158–173.
3. Smit, W., 1971. Pr. 3rd Conf. Static Electrification (Inst. Phys., Bristol) pp. 178–183.
4. Vos, B., 1971. Pr. 3rd Conf. Static Electrification (Inst. Phys., Bristol) pp. 184–192.
5. Van der Meer, D et al. 1973 2nd Int. Conf. Static Electricity Special Colloquim: Problems on Tank Washing in Very Large Crude Tankers (Dechema, Frankfurt).
6. Jones, M.R.O and Bond, J. Chem Eng Res , IChemE. Vol. 62 Sept 1984.
7. Jones, M.R.O and Bond, J. Chem Eng Res , IChemE. Vol. 63 Nov. 1985.
8. Bond, J. Loss Prevention Bulletin 056, pp. 24–25.
9. The Accident Database. Version 4. The Institution of Chemical Engineers.

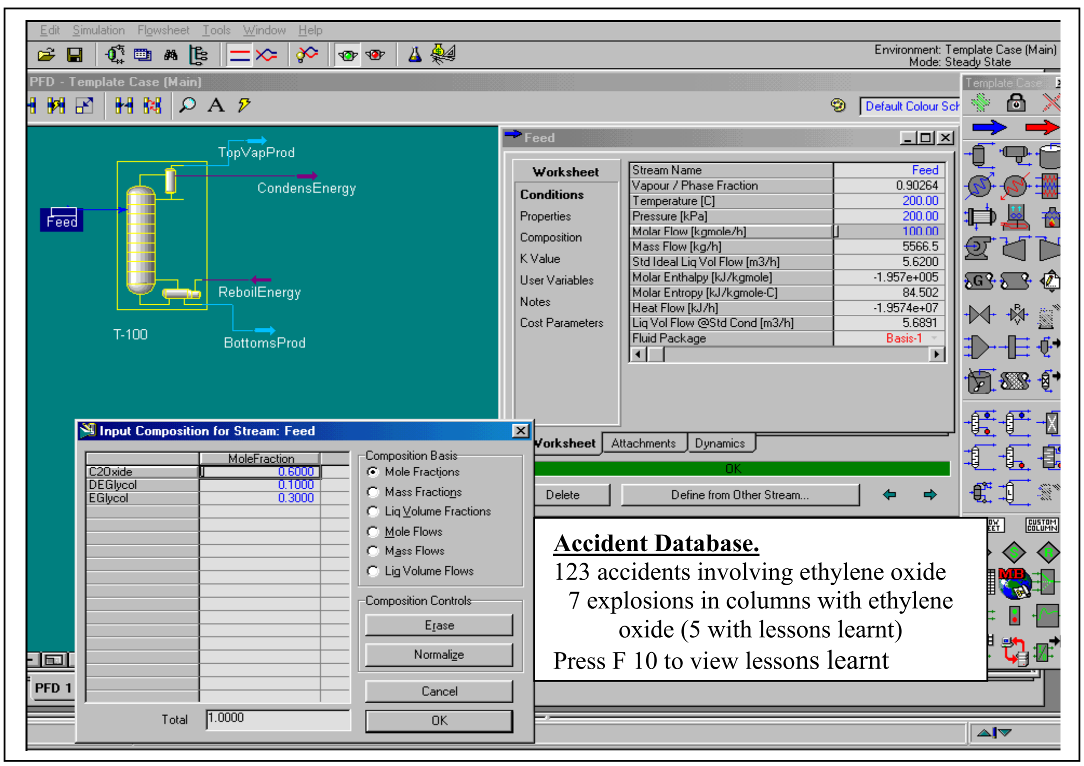

Figure 1. Hyprotech screen for design of distillation column for ethylene oxide and showing accident database warning

Risk Assessment Form

C-MIST

Site Location/Project:			
Work Activity/Task:	**REMOVE SUBMERGED PUMP**		
Reference No:	**MAINTENANCE TASK**		
Assessment carried out by:		**Assessment checked by:**	
Name	**Date**	**Name** ………	**Date**

Risk = Probability x Severity of consequence ; R = Risk, S = Severity, P = Probability

HAZARDS		**Risk**		
		R = P x S		
		P	**S**	**R**
1	Working on vessel top – falling			
2	Scaffolding requirements			
3	Lifting pump			
4	Open manhole			
5				

Figure 2. Part of a risk assessment form

No. 8720 Date. 09 March 1983
Source: Loss Prevention Bulletin136 21–23, Western Mail 1983, 10 March. Loss Prevention Bulletin. 083, 13-14 I.Chem.E.

Abstract: A major fire occurred on a gasoline treater unit in an Olefins complex. Prior to the incident the unit was operating at reduced rates. A fire occurred as a result of the ignition of a mixture of raw gasoline and hydrogen, which was released as a result of a rupture in the horizontal section of the 20 cm diameter, ferretic steel, insulated and clad feed-line between the preheater and the reactor. The impact energy from the violent movement of pipework associated with the failure was sufficient to cause the ignition, which occurred almost immediately after the failure. The fire was isolated and controlled within ten minutes and was eventually extinguished after ninety minutes, by which time some 40 tonnes of hydrocarbons had been consumed. Two operators were injured in the incident one severely and one superficially. Prompt action by the plant and local emergency services quickly contained the main fire and the secondary fires and prevented any further escalation. Fire damage was extensive with preliminary estimates for the rehabilitation costs of £1.25 million (1983). [fire - consequence, gas/vapour release, reactors and reaction equipment, processing, injury]

Lessons
External corrosion of carbon steel and low chrome ferretic steels beneath insulation has been a cause for concern for many years and has resulted in a number of serious incidents from sudden failure of high pressure containment. Although many of the reasons for under-lagging corrosion are well understood it is unfortunate that in many incidents, involving under-lagging corrosion, the known lessons learned are rarely put into practice or maintained. It is useful therefore to use this incident to remind ourselves of the lessons about under-lagging corrosion and the precautionary measures to be taken to prevent such occurrences:

1. The ingress of water through inadequate water proofing, or through damaged cladding, must be minimised or if possible eliminated.
2. The use of absorbent insulating materials must be avoided whenever possible, with the effect of such materials on corrosion rates fully taken into account.
3. Operations above ambient, and particularly in the temperature range 77–115 degrees C are susceptible to under-lagging corrosion.
4. Line preparation prior to insulation - i.e. painting, must be carefully monitored and maintained during construction and any maintenance phases.
5. She presence of chlorides originating from lagging material, process materials, plant, or environment conditions - sea air -- may also accelerate corrosion.

Since it is virtually impossible to guarantee that water will not permeate insulation, added protection can be achieved by metal coating systems.
Further protective measures to prevent under-lagging corrosion include:

1. Careful consideration at the design and construction phases of new plant to the potential problem with adequate consideration given to weather proofing around protrusions in insulation such as pipe supports and nozzles etc.
2. Facilitate ease of removal/replacement of cladding for inspection purposes
3. Actual operating conditions may differ from design specifications thereby increasing the possibility for corrosion
4. The possibility of leaks from small bore piping, steam tracing, with sampling systems another potential source of corrosion

A comprehensive maintenance inspection programme will reduce the likelihood of, and potential consequences from under-lagging corrosion. In the development of such a programme the following points are to be considered:

1. Materials of construction, and insulation material.
2. The age of the plant including a review of previous inspections undertaken and to follow up any actions.
3. The effect of normal operating conditions on the rate of corrosion.
4. Intermittent operations and the time out of service of any plant equipment.
5. The potential hazards from any loss of containment, flammable, toxic, corrosive etc.
6. The integrity of any steam/electric tracing systems.
7. Pipe diameters and pipework configuration - in particular to reduce or prevent areas for water build up.
8. The possibility of internal corrosion to be investigated.
   Plant layout and operating environment (i.e. close proximity to cooling towers, sea, rivers etc).

Figure 3. Accident database record relevant to the scenario raised in HAZOP case

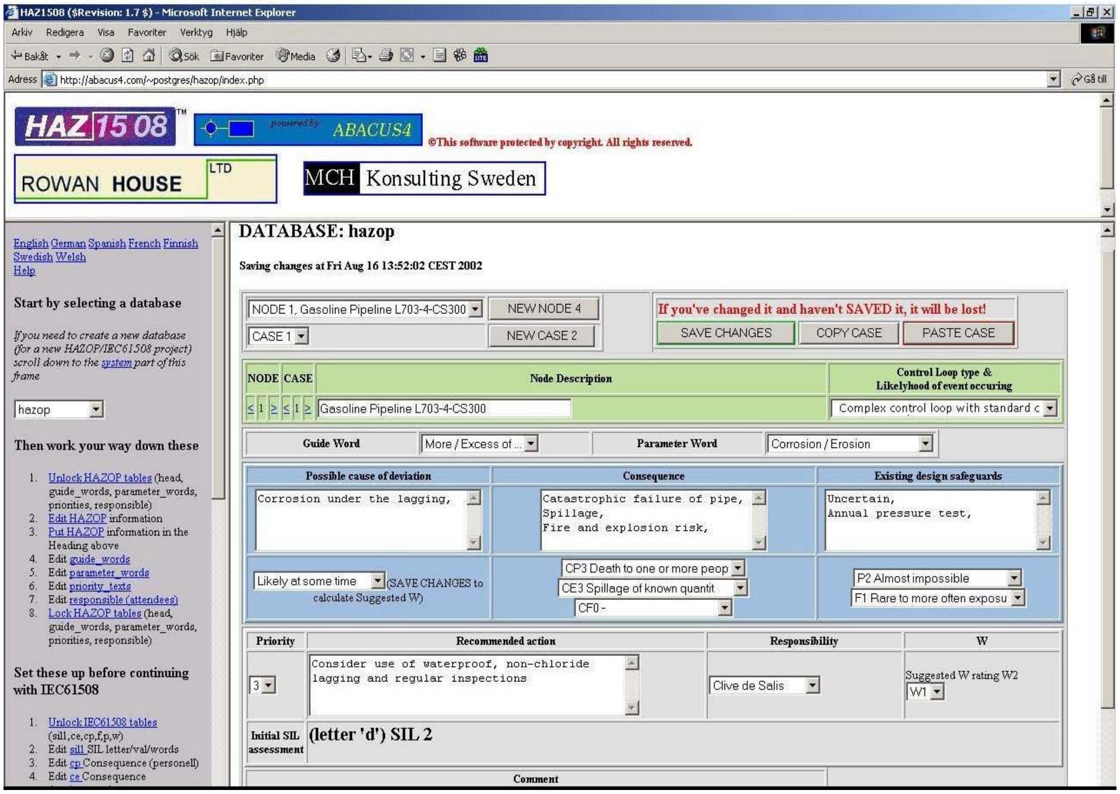

Figure 4. Screen from Rowan house HAZOP software with entry from accident databas