SURVEY OF DEFICIENCIES IN PTW SYSTEMS

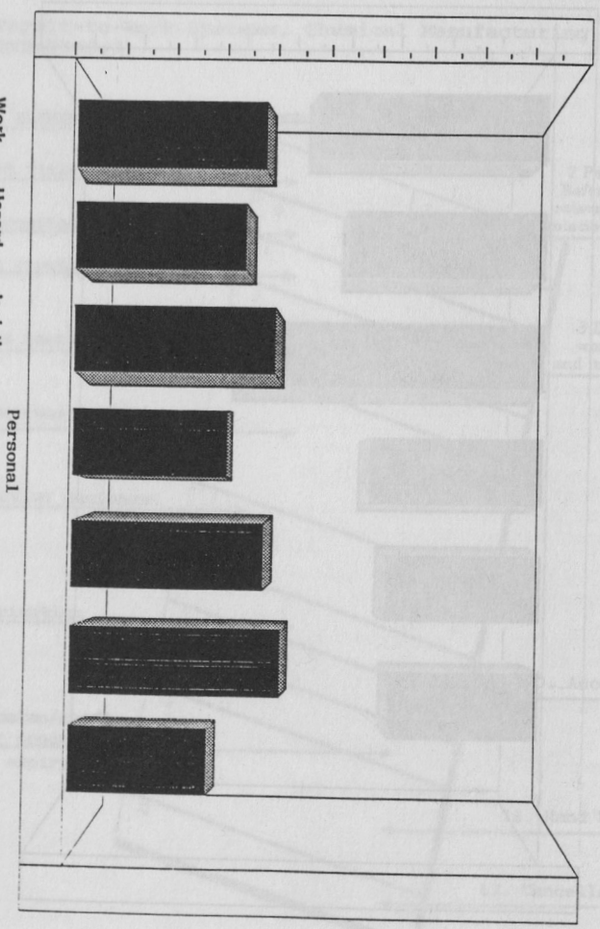


Fig.3

A.G. Rushton
Department of Chemical Engineering, Loughborough University of Technology, Loughborough, LE11 3TU.

An *integrated* fault condition is defined here as one which can contribute to both *minor loss* and *major hazard* events. Such fault conditions are common in protective systems and may be *benign* or *malign* in their effects on the assurance that can be ascribed to the avoidance of the *major hazard*. An attempt is made to classify *integrated* fault conditions for the purposes of plant description and design.
The qualitative features of a given level of protection (*integrity*) achieved through different combinations of *inherent* and *engineered* contributions and the redirection of threats from *major hazard* to *minor loss* events is also discussed.
Terms in italics are given working definitions for this paper.

Keywords : Fault, protective device, fault tree, hazard.

INTRODUCTION

In general it is possible to distinguish between two classes of undesirable acute events. On the one hand there are events with safety or environmental consequences. The expected frequency of such events must be very low to be acceptable. On the other hand there are events with economic or nuisance consequences. These would affect the quality of plant output or the ease of plant operation. This class would include, for example, the production of off-specification output, reduced output capacity and operability problems requiring greater effort on the part of plant personnel.

The range of severity of these consequences is very wide, but here only the sub-classes of high severity safety and environmental consequences and low severity economic or nuisance consequences is to be considered. In the following treatment the terms ***major hazard*** and ***minor loss*** are used to refer to events in these sub-classes respectively.

Where inherently safer operation is not feasible, it is common to obtain protection from *major hazards* by pursuing the philosophy of defence in depth (1), whereby the realisation of the hazard requires a number of (nominally independent) fault conditions to be satisfied. Such protection can be undermined in two distinct ways: directly, if the fault conditions are not truly independent, and insidiously, if some of the various fault conditions can accumulate over time.

A particular fault condition may be contributary to both a *minor loss* event and a *major hazard* event. Such a fault is defined here as ***integrated*** in the sense that it is common to both consequences. The purpose of this paper is to show that, dependent on the configuration of plant components, a classification of fault conditions as *non-integrated*, *neutrally integrated*, *benignly integrated* or *malignly integrated* is useful in describing the configuration and setting design objectives.

DEMAND AND PROTECTION IN DEFENCE IN DEPTH

Figure 1 illustrates the defence in depth philosophy represented in the form of a generalised fault tree.

For any set of fault conditions that could lead to a *major hazard* (i.e. a cut set), it is normally possible to identify two complementary sub-sets. One sub-set, in combination, will lead to an excursion in the relevant process variable. The second sub-set, in combination, would leave that excursion unchecked and, therefore, lead to the *major hazard*. In fault tree terms, the incipient excursion is the intermediate event which heads the *demand* sub-tree within which the first sub-set of fault conditions appear. The members of the second sub-set of fault conditions will normally be associated with protective devices. In fault tree terms, the *demand* AND the protective device faults are necessary to reach the *top event*. [It is conventional to regard the normally operating plant control systems as contributing to the demand by their failure, but it is equally possible to treat these as the first line of protective devices.]

The plant designer can influence the expected frequency of a *major hazard*, firstly by configuring the process in such a way that the demand rate is controlled and secondly by installing protective devices to limit the fraction of demands that go unchecked. The focus of this paper is on the protective devices and their dependability.

Such devices are required to act, reliably, on demand and many are normally dormant. This is a severe duty for any system component and requires a high standard of management providing for the testing and maintenance of equipment.

For the purposes of this discussion the term "protective device" is used to refer to any plant item which has a protective function. This clearly includes components of conventional alarm and trip systems (explicit protective devices) but also, for example, would encompass a heat exchanger which is intended, when necessary to perform an emergency cooling action (an implicit protective device). For clarity only protective devices which are intended to prevent an event in the *major hazard* class are considered.

In principle, protective devices can reduce by orders of magnitude the frequency of the undesired event. In practice, there are many case histories in which it is evident that the protective devices have not been managed to the standard required to maintain a high level of protection, and, consequently, any analysis of event frequency which might have been performed prior to the incident has been undermined and the forecast frequency has been invalid.

As a simple hypothetical example, the refrigerated storage of a flashing toxic material is considered. Protection against a release of the toxic material through overpressure (due to loss of cooling) might be afforded by a pressure relief valve venting through a scrubber to a flare. The essentials of such a system are shown in Figure 2. The corresponding fault tree for the *top event* "Toxic Release" is shown in Figure 3. Figure 3a shows a simplified tree with a format comparable with that of Figure 1, Figure 3b shows a fuller tree in which relief valve functional failure is taken into account. The situation appears to be well controlled, but the successful operation of the protective devices is not essential to normal plant performance. All these devices are therefore vulnerable to a kind of common cause failure through lapses of good management.

INHERENT AND *ENGINEERED* CONTRIBUTIONS TO *INTEGRITY*

Whilst accepting that, to an extent, the demand rate (i.e. loss of cooling) is also dependent on management, it can be argued that, since loss of cooling can produce operability difficulties and the cooling service may be integrated with the production processes, there will be effective management pressures to maintain the cooling service. This provides some assurance that cooling service maintenance will be achieved. [There is, of course, a risk that other process demands on an integrated cooling system may induce failures which increase the demand rate for the storage vessel protective devices.]

It is thus possible to distinguish two frequencies of system failure, the *inherent* frequency, (in this case solely dependent on the demand rate) 10^{-2} yr^{-1}, and the overall frequency, here 2×10^{-6} yr^{-1}. The factor separating these frequencies represents, very crudely, the vulnerability of the plant to management failure. It is helpful to express as a "contribution to plant integrity" the negative of the logarithm (base 10) of the factors by which the overall frequency is influenced by *inherent* and protective (*engineered*) elements. Figure 4 shows how the overall "integrity" is built up from an *inherent* and an *engineered* contribution. [As defined here, these contributions can equally be seen as the logarithms of the factors in the nominal mean time between failures.] The choice of 1 yr^{-1} as the datum on the integrity scale is arbitrary.

It is evident that two plants with similar *top event* frequencies might be qualitatively differentiated by the contributions made by *inherent* and *engineered* elements.

FAULT CONDITIONS *INTEGRATED* IN *MINOR LOSS* AND *MAJOR HAZARD* EVENTS

The fault conditions of the pressure relief valve (functional failure), the scrubber and the flare in the example described above can be classified as *non-integrated*, i.e. they contribute to an event from one class (in this case a *major hazard*) but do not contribute to an event from the other class (*minor loss*).

A desirable objective is, by design, to divert the influence of faults from contributing to hazards to contributing to operability problems. If this can be achieved then rare events (the fault conditions) will contribute a little to plant unreliability (dominated by other, more common faults) instead of contributing a lot to loss of plant integrity. At the same time the confidence which can be placed in the maintenance of hazard protection will be enhanced. One means to this end is to arrange the plant configuration such that latent failures in a *major hazard* fault tree become revealed failures in a *minor loss* fault tree. The deliberate choice of plant configuration to achieve this amounts to a paradigm for design for graceful degradation.

The configuration of a protective device in such a way that its continued functionality in its protective role is necessary to fulfil a second function, and such that loss of this second function leads to a *minor loss* event is defined here as ***benign integration***.

In the case of the storage system described above, the flare could be used in normal plant operation for some minor service, such as providing indirect heating. The need to maintain this minor service would give greater assurance that the desired availability of the flare for its protective role will be attained.

Care must be taken that the consequences of integrating a component into the *major hazard* and *minor loss* fault trees does not result in a production side failure placing a demand on the safety side. Such a linkage is defined here as a ***fault loop*** and constitutes ***malign integration***.

A concise example of such a *fault loop* is illustrated in Figure 5. Here one level transducer is used to both alter the set point of a flow controller and to trigger a high level alarm. The most likely source of a demand on the alarm will be the mis-direction of the valve to the fully open position consequent on the level transducer giving a false indication of low level. A similar example of the dangers in using common equipment for control and protective functions is given by Kletz (2).

In the storage system, for example, the scrubber could be used to provide indirect cooling for a product stream. Now a failure of the scrubber could place extra strain on the plant cooling systems and thereby increase the likelihood of a failure in the storage cooling service. Just how malign such a configuration would be depends on features not detailed here.

In general, the character of the *integration* of a fault condition will not be clear-cut. There will be a point on the spectrum between the malign and benign extremes where the character of the *integration* is indeterminate. Cases which lie near this point would qualify for the classification ***neutrally integrated***.

THE RE-DIRECTION OF THREATS - AN EXAMPLE

Beside the scope that exists for the deliberate arrangement of plant configuration to introduce *benign fault integration* and eliminate *malign fault integration*, it is often possible to alter the configuration so as to redirect threats resulting from a fault condition away from *major hazards* and towards *minor losses*.

The example cited here is realistic rather than real. It is loosely based on a plant described by Lawley (3). The author is not sufficiently acquainted with the original process to know whether assumptions implied in the treatment given here are pertinent to that process. Comments made here should not, therefore, be interpreted as critical of the reported design. However, the assumptions are, at least, self-consistent and might well apply to a similar process.

Figure 6 shows a simplified piping and instrumentation diagram for a three stage crystallisation process. Figure 7 shows a fault tree with the *top event* "Low pressure discharge of slurry to atmosphere". [This is not the only *major hazard*, but is the one to which the following comments are addressed.]

The low value of the *top event* frequency is achieved through the protection afforded by indicators and alarms (and the likely response of operators to these) and the effective maintenance of the stack and its drain. The expected rate at which loss of level will occur leading to a potential release is 11.8 yr^{-1}. (made up from contributions of 5.6, 5.6 and 0.6 from the three crystallisers respectively) but the overall hazard rate forecast is 8.9×10^{-5} yr^{-1}.

The contributions to "integrity", as defined above, from *inherent* and *engineered* elements are shown in Figure 8.

A modified flowsheet is shown in Figure 9. Here the pressure in the first and second crystallisers is controlled by venting excess gas into the next crystalliser, and, in the event of loss of effective level control, liquid will overflow through this route. The effect of this is to redirect some of the threats (11.2 yr^{-1}) in such a way that protective system failure will more often result in poor product quality than in loss of containment. There would be a need to reconsider the basis for sizing the pressure control lines, and to reconsider the arrangements for pressure relief.

For the modified plant the frequency of level loss is the same but only a fraction of such events are likely to lead to a release, the expected rate being 0.6 yr^{-1}. The overall hazard rate is then 5×10^{-6} yr^{-1}.

The really significant difference between the two designs is not the value of the *top event* frequency (in both cases in the region of 10^{-5} yr^{-1}) but the assurance that this value can be maintained. Level indicators 1 and 2 require scant attention for routine operation and so the likelihood that they will fall into an unrevealed failed state or will not be attended to by the operators is much greater than for level indicator 3. Confidence in the protection afforded by level indicator 3 is therefore relatively high but, whereas it is relevant to only one in twenty of the demands in the original design, it is relevant to all of the demands in the modified design. Whereas the overall hazard rate for the original design can easily become very much worse than that forecast from the fault tree analysis, that of the modified plant is relatively robust.

A less tangible benefit of the modification follows from the greater dependence on instruments for productive plant operation. This will militate against the development of a culture in which instrument failures are neglected.

CONCLUSIONS

Protective devices are prone to a type of common cause failure through neglect. For this reason analysis of hazard frequency based on the assumed independence of protective devices must be treated with caution.

A way of expressing contributions to the "integrity" of a plant has been given, where integrity is defined as $\log_{10}$ of the mean expected time between *major hazard* events. The confidence that can be placed in any contribution depends on its character (*inherent* or *engineered*) and that of the plant configuration by which it is achieved.

One contribution, the *inherent* contribution, is secured by plant design and normal operating procedures and is closely related to the rate at which incipient excursions arise which could lead to the hazard (the demand rate). A second contribution, the *engineered* contribution, is associated with protective devices (explicit or implicit) and is secured primarily by vigilant management.

In this paper two important classes of protective device configuration have been identified.

In one class a fault will not only disable the protective system but also cause a demand on the protective system itself. This is defined here as *malign integration.*

In the other class a latent fault, which either disables a protective system or increases the likelihood of a demand on a protective system, will also have a consequence which is tolerable from the point of view of safety, health and environmental damage, but is intolerable from an economic point of view, thus forcing a reinstatement of the faulty device to a serviceable state. This is defined here as *benign integration.*

Fault trees provide a formal framework for describing these classes of configuration.

Malign integration is identified where the functional failure of a component (normally a protective device) can cause a demand on the component itself. In a fault tree this will be revealed where the functional failure of the device appears as a basic event leading to a demand on the device.

Benign integration can be thought of as a hardware interlock between the protection and production features of the plant. A fault which degrades the protection is revealed as a production failure or inconvenience (*minor loss*), and maintenance of the protective system is thus assured. *Benign integration* will normally improve the likelihood that the *engineered* contribution to plant integrity will be secured in practice.

An example has been given where re-configuration of the plant diverts threats away from *major hazards* and towards *minor losses*. In the modified design the *engineered* contribution to plant integrity is more benignly integrated and this gives increased confidence that the (very low) forecast event frequency will be achieved.

The introduction of *benign integration* to and the elimination of *malign integration* from the plant configuration are desirable objectives in design. The change in the forecast event frequency resulting from *benign integration* may be marginal, but there will be a substantial improvement in the confidence which can be placed in that forecast.

REFERENCES

1. Rasmussen, J., 1988, *Preventing Major Chemical and Related Process Accidents*, I. Chem. E. Symposium Series No. 110, 533-551.

2. Kletz, T.A., 1983, in Hazop and Hazan, Chapter 3, I. Chem. E., Rugby.

3. Lawley, H.G., 1974, Loss Prevention, 8, 105.

4. Lees, F.P., 1980, Loss Prevention in the Process Industries, Butterworth, Oxford.

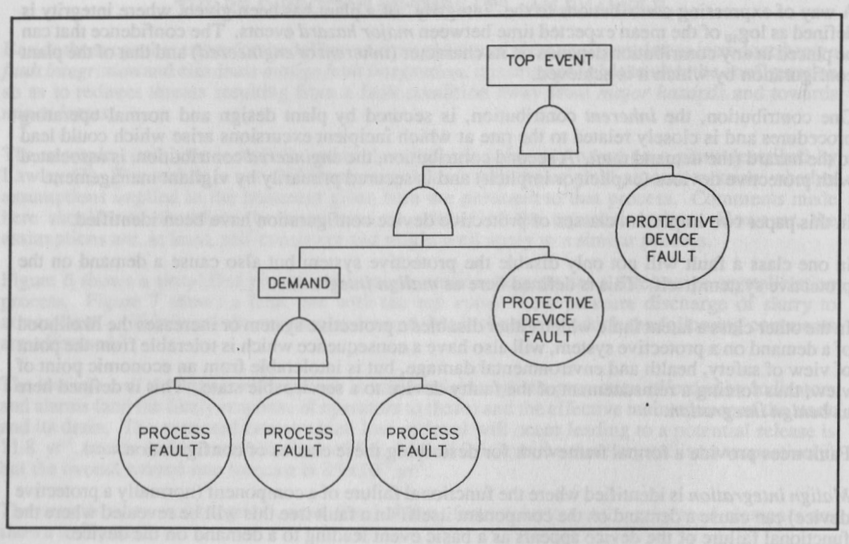


Figure 1 A Generalised Fault Tree for a Plant with Defence in Depth.

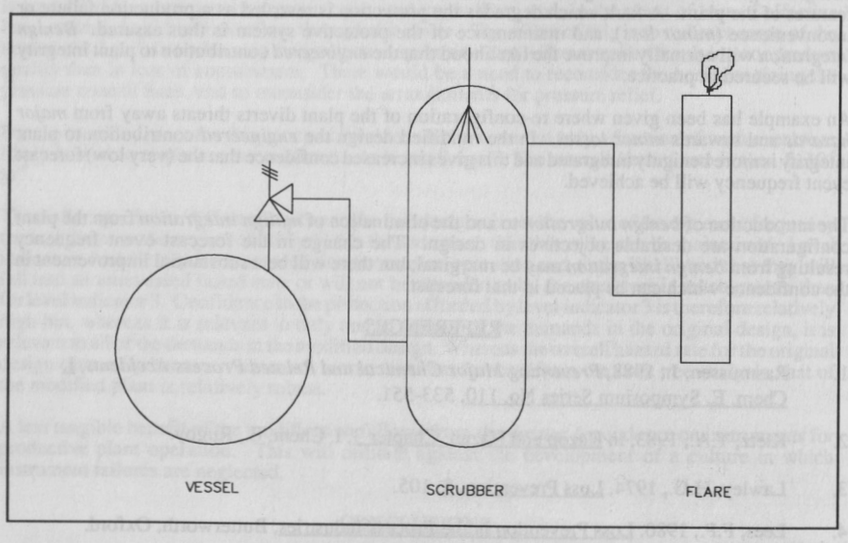
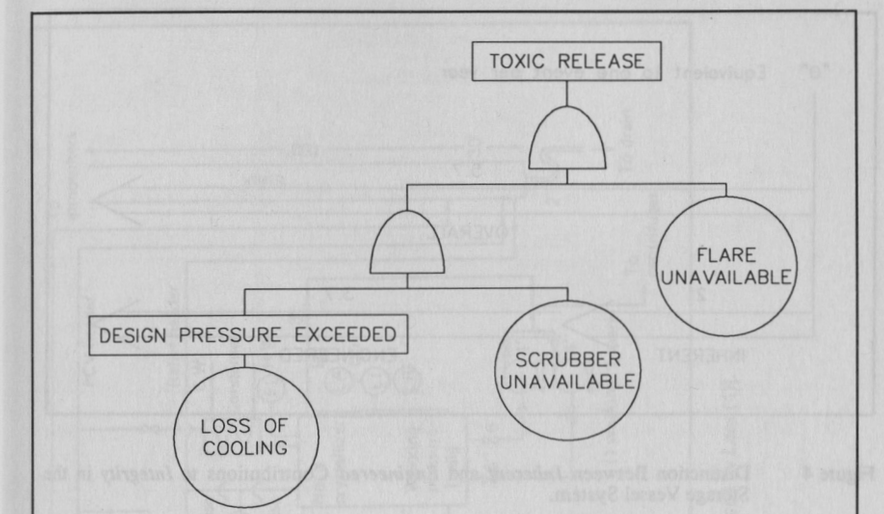
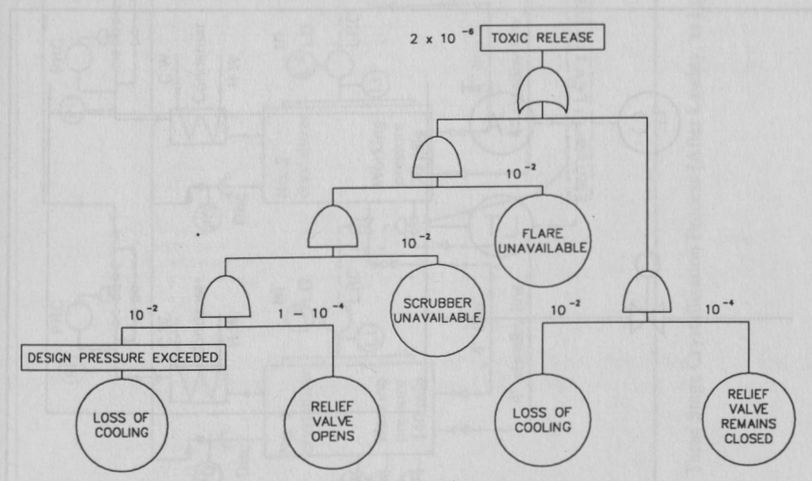


Figure 2 Essentials of the Hypothetical Protection System for a Storage Vessel.



a) Simplified for comparison with Figure 1.



b) Accounting for relief valve failure.

Figure 3 Fault Tree for the *Top Event* "Toxic Release" - Frequencies and probabilities are illustrative.

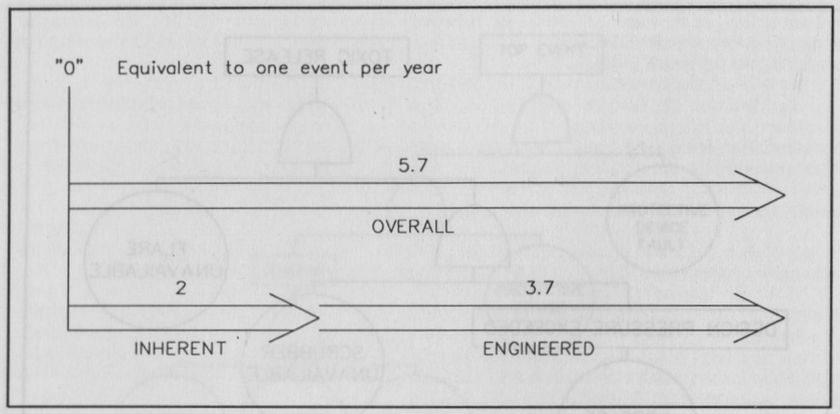


Figure 4 Distinction Between *Inherent* and *Engineered* Contributions to *Integrity* in the Storage Vessel System.

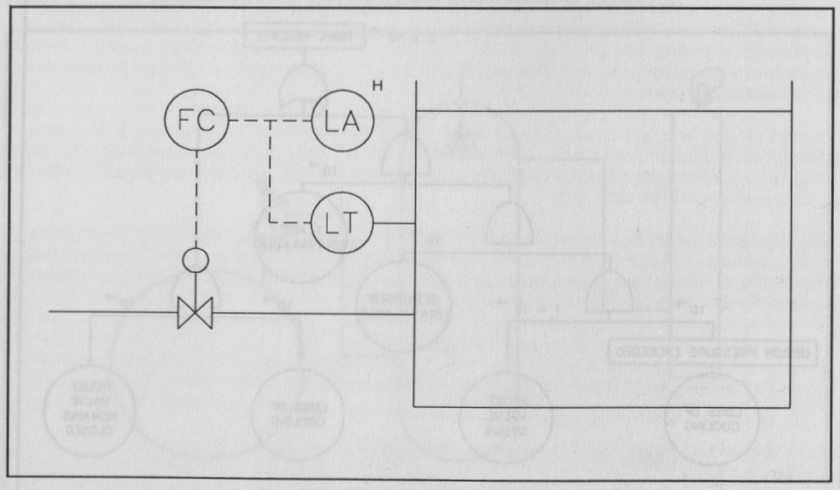


Figure 5 Illustration of a level control system with a *Fault Loop*.

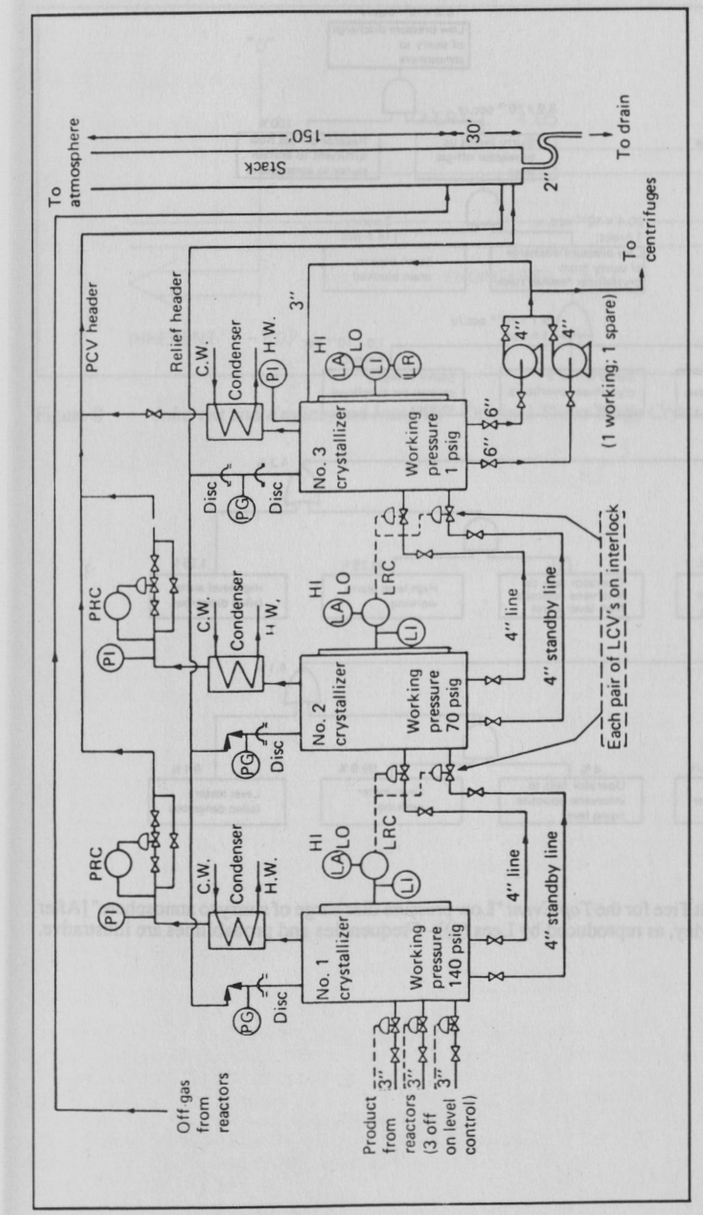


Figure 6 Three Stage Crystallisation Process [After Lawley, as reproduced by Lees (4)].

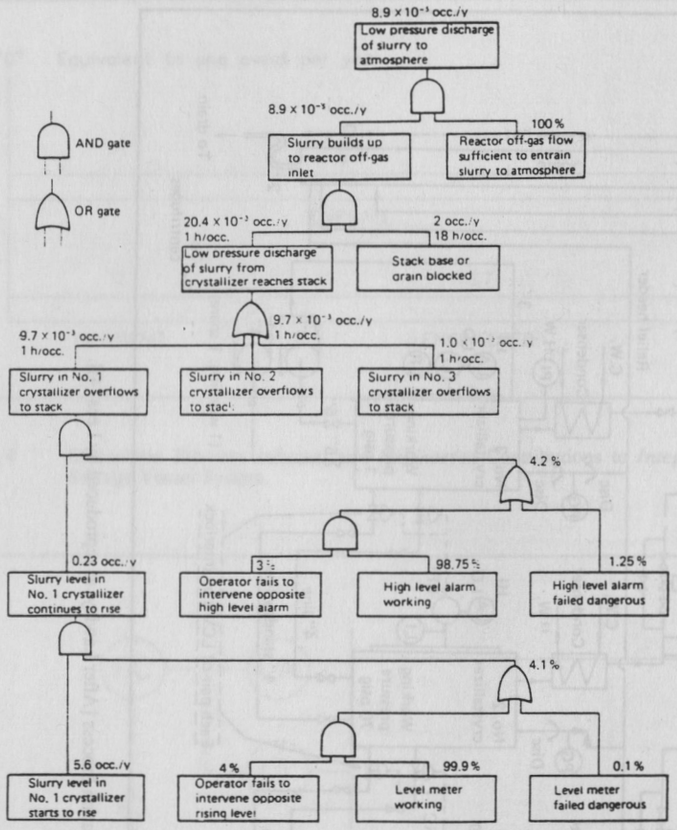


Figure 7 Fault Tree for the *Top Event* "Low pressure discharge of slurry to atmosphere" [After Lawley, as reproduced by Lees (4)] - Frequencies and probabilities are illustrative.

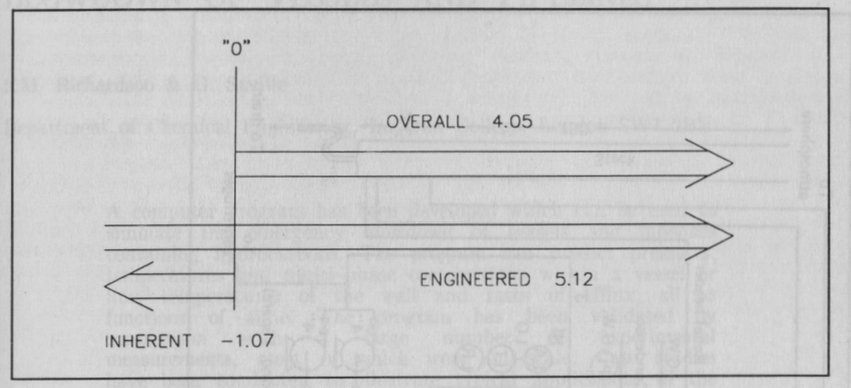


Figure 8 *Inherent* and *Engineered Integrity* - Original Three Stage Crystallisation Process.

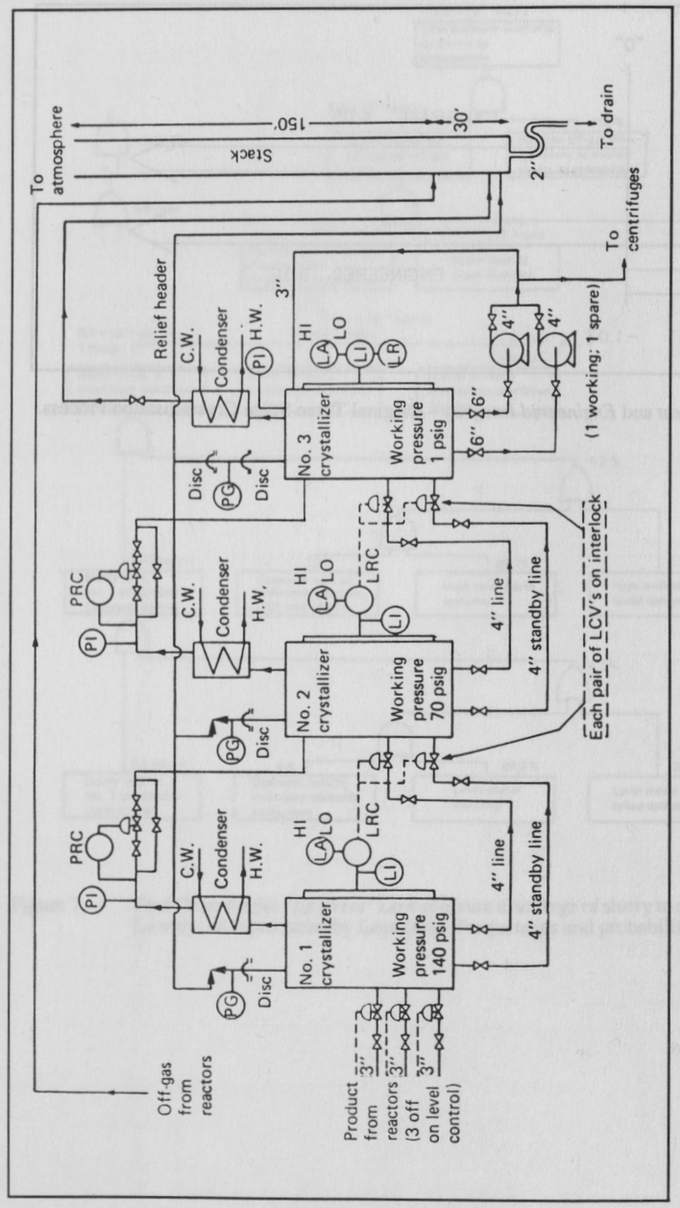


Figure 9 Modified Three Stage Crystallisation Process.

BLOWDOWN OF VESSELS AND PIPELINES

S.M. Richardson & G. Saville

Department of Chemical Engineering, Imperial College, London SW7 2BY

A computer program has been developed which can be used to simulate the emergency blowdown of vessels and pipelines containing hydrocarbons. The program can predict pressures, temperatures and multi–phase compositions within a vessel or line, temperatures of the wall and rates of efflux, all as functions of time. The program has been validated by comparison with a large number of experimental measurements, most of which were full–scale. Case studies have been conducted to illustrate typical applications of the program.

Keywords: Blowdown, Depressurisation, Pressure Vessels, Pipelines, Safety, Oil & Gas Processing

INTRODUCTION

The rapid depressurisation or blowdown of high pressure vessels and pipelines is a hazardous operation. Such vessels and lines can occur both onshore, for example in a natural gas transmission system, and offshore, on and between platforms. Blowdown can be deliberate, so as to avoid the possiblity of rupture in the event of a fire or to minimise emissions at undesirable locations in the event of a leak, or accidental, if part of a vessel (or its associated pipework or valving) or line is ruptured.

In the case of vessels, blowdown leads to a hazard because of the very low temperatures generated within the fluid in the vessel. This leads to a reduction in the temperature of the vessel walls and possibly to a temperature below the ductile–brittle transition temperature of the steel from which the vessel is fabricated. It can also lead to the formation of hydrates in cases when free water is present in the vessel or to the formation of liquid condensate which can get carried over into a flare or vent system. For blowdown from the top of a slugcatcher of inside diameter 4 m, wall thickness 150 mm and length 50 m containing mainly methane at an initial pressure of 110 bara and temperature of 278 K (5 C) through an orifice of equivalent diameter 50 mm, the minimum gas temperature is about 228 K (–45 C) and the minimum temperature of the inside of the vessel wall in contact with gas is about 243 K (–30 C).

In the case of pipelines, the hazard from blowdown arises not only because of the low temperatures that can arise in the pipe walls but also because of the large total efflux and high efflux rates that arise when the very large inventory in a typical line is blown down. For a 40 km long 0.4191 m (16.5 in) bore gas line containing mainly methane initially at 120 bara and 283 K (10 C), the initial efflux rate following a full–bore rupture is about 3 te/s and a total of about 1000 te can escape if the line is not fitted with sub–sea isolation valves.