# THE PROTECTION OF EXOTHERMIC PROCESSES

N F Scilly; Technology Division, Health and Safety Executive, Bootle, Merseyside.

**Abstract**

Exothermic processes are potential sources of runaway reactions and have generally been protected, in the past, by relief devices. For a variety of reasons it may not be practicable to fit a relief device and alternative forms of process protection need to be considered. This paper examines this problem and outlines a strategy for achieving comparable process reliability.

KEYWORDS: Venting, Instrumented Reactor Protection; Fault Tree Analysis

## 1. Introduction

Exothermic reactions can cause problems when control of the process is lost causing the reaction mass to overheat thereby creating an accompanying increase in pressure. Traditionally in the past HSE has required operators of exothermic processes to improve, where necessary, the control system and its instrumentation.

Typically, this has meant the provision of alarms and instruments to indicate stirrer and cooling water flow failure and cooling water high temperature. Additionally, HSE has also required the fitting of an adequately sized relief device venting to a safe place.

HSE has underwritten this strategy by placing several research contracts with the Polytechnic of the South Bank relating to, inter alia, the design of Dewar calorimeters for reaction study and research and development studies on the Accelerating Rate Calorimeter (ARC), the Fike Vent Sizing Package (VSP) and the Mettler Heat Flow Calorimeter. These contracts ultimately led to the setting up of a Chemical Reaction Hazards Centre at the Polytechnic of the South Bank which opened on 15 July 1987. This centre provides a service to industry for the assessment of the thermal hazards of both materials and reaction systems thus facilitating the safe design of chemical processes.

However, within the last few years several instances have arisen in which the operator of an exothermic process has not been able, or wished, to fit reactor relief but was prepared either to improve the reliability of the control system fitted to the reactor or adopt some alternative protective measures or to fit some combination of the two approaches.

Reasons for not wishing to fit a relief system have included difficulty in fitting or sizing an adequate relief system and difficulty in venting to a safe place. Other reasons could be an economic factor such as the provision of a flare or scrubber and environmental issues. It is anticipated that this last reason will become increasingly important.

Accordingly, HSE has had to formulate a strategy for evaluating the relative safety of various methods of reactor protection and the present position and some of the outstanding problems still to be fully resolved will be outlined in this paper.

## 2. Criteria and strategy for non-relieved reactor systems

When faced with the dichotomy "To vent or not to vent" the initial conclusion was that the proposed design for the non-vented reactor should be at least as safe as the "traditional" vented alterative. This answer is somewhat simplistic and immediately poses a number of subsidiary questions which will be examined later. Furthermore, in order to determine whether a non-vented reactor is as safe as, or as reliable as, a vented reactor, quantification of the relative likelihood of failure would be necessary. It quickly became apparent that reliability data for bursting discs and relief valves was scanty and that more information concerning the various failure modes of reactors and their relative importance was required. Therefore, a contract was set up with the University of Loughborough to examine these, and other, problems and the first part of that contract has been completed. The results will be published shortly (1).

It is appropriate, at this point, to summarise the conclusions of this study which are most pertinent to the present discussion.

The study was solely confined to batch and semi-batch processes. Examination of past overpressure incidents with reactors showed:-

(a) incidents could be attributed, largely, to lack of relief capacity ie inadequate sizing rather than inherent unreliability of the relief device.

(b) Nationally there were 66 overpressure incidents in a 12 year period. The proportion of overpressure excursions to the number of incidents observed, based on estimates, was 5%. Since this value is significantly higher than the failure frequencies of bursting discs or relief valves it indicates that failure to vent by either device is not a primary cause of escalation into an incident. Insurance company estimates place the national reactor inventory at about 2100.

(c) Two major difficulties in quantification of reactor reliability were adduced, namely the identification of all failure modes, in particular those involving human error, and the effect of mitigatory measures particularly those which involve the process operator.

(d) In previous fault tree studies it was found that there had been a tendency to underplay mitigating factors and relatively rare failures were frequently overestimated.

As an example of this failure of works cooling water could be cited. This is a fairly common initiating event and intuition would suggest that some incidents could be directly attributed to this fault condition: however, none were found. In part this could be ascribed to the presence of a standby system but these are by no means universal and additionally one might expect that, like most stand-by systems with a low demand rate, the reliability on demand could be quite low. The inference that unidentifiable mitigating factors may be present is unavoidable.

(e) various failure modes for bursting discs were identified. These included undersizing, blanking off, blockage, corrosion, fatigue, creep, wrong disc installed, two or more discs installed, vacuum support installed downstream, disc installed upside down, roll through, defective knife, disc holder failure and other faults for discs in series and disc/relief valve combinations.

The predicted probability of failure on demand for a bursting disc with a one year inspection interval was 0.012 with 95% confidence limits of 0.0035 - 0.03. This failure rate does not take account of the dominant failure mode identified above, namely undersizing, for which the failure frequency is estimated as 0.03 per demand.

(f) the probability of failure on demand of a vent system by blockage, which is inspected once a year, is estimated at 0.002 and the probability of failure from undersizing or other incorrect design feature is 0.006 giving a total probability of failure of 0.008 on demand.

(g) the effectiveness of non-relief protection was estimated for a large number of initiating causes of runaway in batch processes eg impurities, inadequate cooling, undesired catalysis, exotherm of unknown type etc. It was found that the initiating incident modes could be divided into three categories. Under the first category there is a probability of about 0.9 that non-relief protection would have prevented the incidents which occurred. This category included causative events such as inadequate reaction characterisation and stirrer failure. For the second category, which included events such as incorrect charging, inadequate cooling, excessive heating and poor batch control, it was estimated that non-relief protection might have prevented about 50% of the incidents. The third category, where non-relief protection would have been virtually ineffective, included causes such as undesired catalysis, impurity, reaction exotherm, water ingress and subsequent vaporisation and high pressure gas ingress. Overall, it was estimated that non-relief protection would give effective protection in slightly more than 50% of all batch processes.

The conclusion is that for initiating modes other than inadequate information or process characterisation and agitation failure it is difficult to devise countermeasures which are sufficiently comprehensive for batch reactions.

(h) the failure rate data included in (e) and (f) above indicates that the overall failure rate for a bursting disc and the vent system is 0.05 failures per demand. Overall it was estimated that relief protection might not be effective in 16% of cases and non-relief protection is likely to be ineffective in 44% of the cases. It must be stressed that these conclusions apply principally to "all-in" batch systems. In a semi-batch or continuous process, where it is possible to install a trip which shuts off a reactant feed, a degree of protection similar to that for a relief system may be achievable.

(i) an important point, raised by the study, was that the operation of a relief system, whether prematurely or as the result of a demand due to a pressure excursion, could itself give rise to a hazard. This point will be discussed in more detail later.

The work described above was completed in October 1987 and a second phase of this project is expected to commence in September 1989.

## Criteria for relieved and non-relieved chemical processes

The consequences of overpressurising a reactor or other process plant can range from gasket or flange failure and the explosion of possibly hot, but otherwise relatively harmless, material to the release of large quantities of flammable or highly toxic vapours or gases and, occasionally, to the fragmentation of a vessel leading to the rupture of other process plant or storage facilities and the interruption of vital services. The probable consequences of an exothermic runaway should be identified and their severity should be reflected in the reliability of the control system and protection fitted to the process. Therefore, before a decision to vent or protect a system by trips or other measures is made, the hazard associated with the undesirable or top event (in fault tree analysis terms) should be identified. If the top event is solely overpressurisation of a vessel it may be noted, that irrespective of any instrumented protective system fitted, such as a trip preventing material flow into the system, reactor safeguarding will be improved by fitting a relief device. In this case the relief and trip system are complementary to one another and the probability of failure of the vessel is the product of the probabilities of failure of the two individual methods of protection. HSE would not normally expect or require this "belt and braces" approach.

Accordingly, a non-relief protective system may be fitted in lieu of a relief device provided that its reliability is at least as high as that of the "traditional" system it is replacing. It must be stressed that the overall hazard rate (the product of the failure rate or demand rate of the control system and the probability of failure on demand or fractional dead time of the protective system) must be compatible with the potential consequences of the top event.

The situation where the consequences of the escape of the reactor contents to atmosphere is considered to outweigh significantly the consequences of vessel rupture is likely to be more common. The analysis necessary to justify the choice of an instrumented protective system (I.P.S) over a relief system becomes very complicated. The top event is now the release of hazardous material, probably flammable or toxic vapours or gases and to vent these materials safely will require some secondary system such as a containment vessel, scrubber, flare or a vent stack which is sufficiently high to allow safe dispersion. Furthermore premature failure of a bursting disc or a relief valve lifting light, which are normally considered to be fail to safety modes in the context of vessel protection, are now possible fail to danger events since they place a demand on the flare or scrubber etc. This needs to be taken into account in any analysis of system reliability.

Typically the system employed for the protection of a semi-batch or continuous process is a shut-off valve situated in a reactant feed line which closes on detection of high pressure or temperature in the reactor. Depending on the level of reliability deemed necessary diversity and redundancy may be added by employing both temperature and pressure sensors to close the valve or by adopting a majority voting system. The shut-off valve should not be used for any other purpose such as flow control.

This protective system could conceivably fail if, despite its flow being stopped by the shut-off valve tripping, a reactant is present in the reactor in appreciable amounts. This could occur due to instrument dynamic response or slow reaction rates, possibly due to too low a reaction temperature, and to produce a hazard it may have to occur simultaneously with cooling failure. This problem commonly called accumulation and the effects of impurities, excess flow, cooling failure and other parameters is to be examined.

Although one of the conclusions of the study carried out at the University of Loughborough was that protection of an "all-in" batch process was best accomplished by fitting a relief system, there are other types of protection for these processes which might achieve the desired level of reliability. These include

(i) Addition of catalyst killer
(ii) Quench reactor contents
(iii) Stop agitation in Phase Transfer Catalysis.

The reliability, and hence the feasibility of these methods of process safeguarding has not, so far, been examined. It is planned to examine these in the study outlinnd above.

The possibility of re-designing a process to render it intrinsically safe should also be explored.

## 3. Reliability data for relief devices

In the analysis by Lees, et al, described earlier, a failure rate of 0.012 failures per demand was derived for bursting discs which were correctly sized.

For relief valves the situation is more complicated. The failure modes of safety valves which are of significance to this study, are premature opening below the set pressure, rupture of the valve body and failure to open below the bursting pressure of the vessel. Leakage through the valve seat and body may also be significant if the leak rate is high.

The published data for failure to open on demand will, in the main, be derived from testing schedules where a valve will be reported as failed closed if it does not open at a level which is 10% (but occasionally 50%) above the set pressure, allowing for accumulation and tolerance. Failure in these circumstances could be due to inaccurate or incorrect initial set-up procedures and it is probable that in many instances the valve would have lifted in time to afford protection to the vessel. Vessel failure is most likely to occur when a valve becomes jammed due to such causes as a bent spindle, deposits on the valve seat etc. However, it should be appreciated that although a valve lifting appreciably above the set pressure may still afford protection to the reactor it may impose excessive stresses or forces upon the vent lines or secondary systems and cause their failure.

A questionnaire was circulated to oil and gas production facilities, refineries, chemical plants, pipelines and terminal facilities relating to their experience with various types of valve (2). About 6.5% out of a total of 24,000 relief valves had given problems ie 3.3% leaked, 1.1% exhibited erosion, 1.1% had jammed and in 0.5% there were material faults.

In another study carried out with pressure relief valves used in three different environments it was concluded that less than 1% lifted heavy in a clean duty, 10% lifted heavy in an average duty and 14% lifted heavy in a dirty duty.

Further data on the reliability of pressure relief valves is contained in references 3 and 4. These suggest values of $2 \times 10^{-5}$ per hour and $3 \times 10^{-2}$ per demand for fail to close and 1 to $2 \times 10^{-5}$ per hour and $1 \times 10^{-5}$ per demand for fail to open.

The reliability of the relief system should also include an analysis of the secondary system ie scrubber, flare, vent lines etc.

It is hoped that with the growing use of computer aided maintenance schemes better reliability data will eventually become available.

## 4. Case Study

Material A is manufactured according to the following reaction schemes.

A + B  C
C + D  A

and is removed from the reaction by continuous distillation. Thus it features in the process as solvent, reactant and product. The process is continuous and takes place under reflux conditions with the necessary energy being provided by the heat(s) of reaction. Reactor cooling is provided by a water condenser and a water jacket which supply, respectively, about 65% and 35% of the cooling capability.

B is fed, as a gas, into the reactor via several dip legs and D is added in specified increments throughout the reaction campaign at intervals determined by the instrumentation. The second of the two reaction schemes is significantly faster and more exothermic. Both A and C react violently and exothermically with water at the reaction temperature. For several reasons the company operating the process wished to rely on an instrumented protective system rather than provide relief and a scrubber.

The reactor is fitted with two temperature probes one of which is used, in conjunction with temperature sensing in the condenser, to provide a read-out of the differential temperature existing between the reactor contents and the refluxate. Two pressure switches set to high and ultra-high respectively close a shut-off valve in the gas (B) feedline on demand. Agitator failure is detected and alarmed using two independent and diverse systems. Cooling water flow and temperature is monitored and any deviation would initiate alarms.

In any chemical process where two reactions occur in sequence to give the desired product safe process design is made considerably easier if the second reaction proceeds more quickly. In this instance the second stage is much quicker and under normal circumstances the concentration of C is very small. The key to maintaining this position is to ensure that reactant D is present at all times. D is appreciably soluble in the product (solvent) A which is reflected in the temperature difference between the refluxing material and the reactor contents. Addition of D is carried out when the temperature differential starts to decrease. This system is supplemented by, firstly, a watch-dog timer which is started when addition of D takes place and sounds an alarm after a set period and, secondly, a computer which monitors the amounts of B and D added against the amount of A produced and in the event of an imbalance will sound an alarm.

Other events which could initiate an exothermic process were identified and considered in the fault tree analysis. These included condenser leaks causing hydrolysis of reactor contents, liquid breakthrough of B (stored as a pressurised liquefied gas), agitator failure etc. The fault tree analysis in figures 1 to 3 are largely generic and mainly for illustrative purposes. A more complete analysis of this process will be given in the presentation.

## 5. Conclusions

Before a decision "To vent or not to vent" can be reached it is necessary to:-

(i) Identify the top event ie vessel rupture or escape of hazardous material.

(ii) Identify all initiating events which can lead to the top event preferably using HAZOPS. It must be stressed that the usual characterisation of the chemistry, thermochemistry and kinetics of the process and side reactions should still be carried out.

(iii) Assess the consequences of the top event and decide what level of reliability is commensurate with the hazard posed.

(iv) Undertake a reliability study of the system proposed and compare, if necessary, with what is normally common practice.

Some of the views and opinions expressed in this paper are those of the author and are not necessarily shared by the Health and Safety Executive.

**References**

1. G P Marrs, F P Lees, J Barton and N Scilly:
"Protection of Batch Chemical Reactors"
Submitted for publication to I Chem E

2. M J Billington, D Harrison and B E Vivian
"A practical approach towards solving valve problems" I Mech E evening seminar; Lord Daresbury Hotel, Warrington 10th Feb, 1987.

3. Component Reliability Data for use in Probabilistic Safety Assessments: International Atomic Energy Agency, Vienna, 1988.

4. Reliability and Maintainability in Perspective;
D J Smith, 1988, MacMillan Education

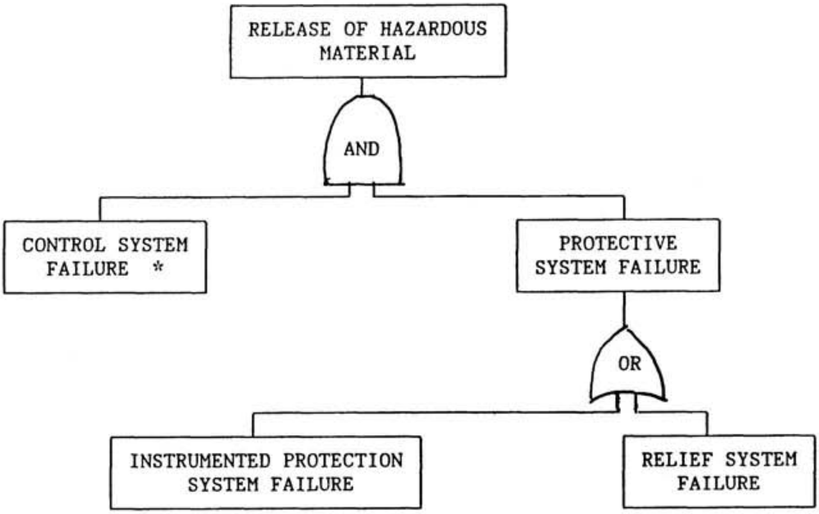



**FIGURE 1**

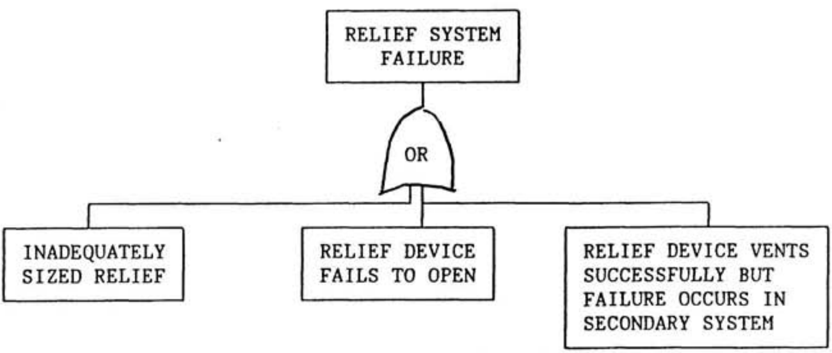
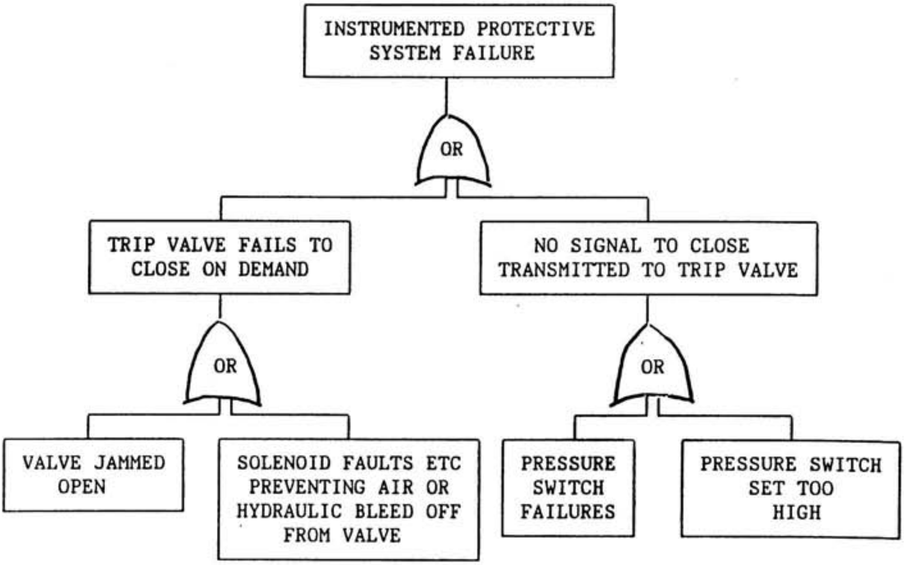



**FIGURE 2**

* NOTE: PREMATURE OPENING OF A RELIEF DEVICE WILL PLACE A DEMAND ON A SCRUBBER ETC AND MAY NOT BE CAUSED BY CONTROL SYSTEM FAILURE


INSTRUMENTED PROTECTIVE SYSTEM FAILURE
OR
TRIP VALVE FAILS TO CLOSE ON DEMAND
NO SIGNAL TO CLOSE TRANSMITTED TO TRIP VALVE
OR
OR
VALVE JAMMED OPEN
SOLENOID FAULTS ETC PREVENTING AIR OR HYDRAULIC BLEED OFF FROM VALVE
PRESSURE SWITCH FAILURES
PRESSURE SWITCH SET TOO HIGH