How safe is safe?

Michael Dixey and **John Gallimore** examine how protective systems can fail to protect, and outline ways in which their reliability can be optimised

WITHIN the home and across a broad range of industries, society has become increasingly dependent on protective systems. These range from simple smoke detectors at home to complex systems on industrial plant which shut down the equipment if there is a serious malfunction.

The purpose of all protective systems is to minimise the consequences or the incidence of failure – failure, that is, of both the protective system and whatever is being protected. Examples include:

- warning of a malfunction or abnormal condition: monitoring equipment, fire alarms, smoke or gas detectors;
- relieving an abnormal condition: pressure relief valves, explosion panels, bursting discs, lightning conductors;
- shuting down plant in the event of a malfunction: fusible links and plugs, vibration switches, E-stops, high temperature trips, interlocks;
- taking over where equipment has failed: back-up equipment, secondary containment (such as bund walls), emergency lighting;
- guarding against hazardous situations: flame arrestors, purging systems, non-return valves, machine guarding, light barriers; and
- mitigating the consequences of failure: fire suppression equipment, emergency showers, emergency medical equipment.

There is an increasing trend towards using software in operating these systems and this trend is likely to continue. Many of these systems are relatively small and are 'out-of-sight, out-of-mind', often perceived as being 'maintenance-free'. Yet we rely on them to protect us against serious malfunctions.

> *"The majority of fail-safe failures are inconvenient but on rare occasions they can be disastrous. Twenty died on a Russian nuclear submarine when the fire extinguishing system released poisonous gas"*

failure of protective systems

Protective systems can fail in one of two ways. They can:

- operate when not required, ie 'fail-safe', or
- fail to protect when needed, ie 'fail-unsafe', 'fail to danger', or 'fail dangerously' (different industries use different terms).

fail-safe failures

The majority of fail-safe failures are inconvenient, eg alarms going off for no good reason. These spurious alarms, however, can have an insidious effect over time as they encourage plant operators to ignore or override the alarms or, even worse, to disable them.

In other circumstances, they can be very costly. Space shuttle launches have been postponed due to faulty alarms, and major chemical plants have been shut down due to spurious signals.

On rare occasions they can be disastrous. Twenty died of suffocation on a Russian nuclear submarine when the fire extinguishing system released poisonous gas into part of the vessel.

It can be very difficult to prevent a protective system from failing occasionally. No maintenance routine can guarantee that it will never fail. Ways of reducing the incidence of this problem (other than by preventive maintenance) are:

- improving the design of the protective system (including the software) to minimise false operation;
- improving the reliability of the components and their assembly; and
- using voting systems where the failure of a single device or sensor will not initiate, say, a shut-down sequence.

fail-unsafe failures

Unsafe failures are the most dangerous – as protection has been lost. Almost all protective

systems can fail unsafe including self-monitoring and self-testing systems – despite claims to the contrary by some vendors.

For many failure modes, this loss of protection will not be apparent to those concerned. These unsafe failures are usually called 'hidden failures'. Other terms include 'unrevealed' or 'dormant' failures.

It is these failures which have been a significant factor in many of the world's worst industrial accidents over the last 40–50 years, including Bhopal, Three Mile Island, Piper Alpha, the Mexico City LPG explosion and Buncefield.

the causes of failure

Protective systems can fail to protect if the hazard has not been correctly identified or the protection is not fit for purpose, for example an undersized pressure relief valve. Assuming that the system has been correctly specified, there are many reasons why protective systems can fail unsafe, and these include:

- **system design errors:** it can be very difficult to ensure that there are no design flaws in complex protective systems such as those on the latest generation of civil aircraft or those used in nuclear power plants which depend on software;
- **component failure**: the most reliable components can fail, and these failures are usually random and unpredictable;
- **faulty installation:** even in the best run organisations, mistakes will be made;
- **post-maintenance burn-in:** intrusive maintenance can result in the protective system being less reliable after the work has been completed. This can be caused by a number of factors including inappropriate maintenance procedures, faulty spare parts, human error, etc;
- **calibration drift:** for process sensors;
- **plant or process modification:** protective systems can be made ineffective where the plant or the process has been modified;
- **accidental damage:** this type of failure is difficult to predict but can be minimised through care in the design and positioning of protective systems and robust procedures;
- **human intervention:** this is one of the major reasons for the failure of protective systems in the manufacturing and process industries. People ignore, disable or bypass protective systems because they cause delays (eg isolation procedures) or because they are causing spurious trips (and shutting down the process);
- **build-up of dirt and debris:** this can make protective systems inoperable or inaccessible;
- **environmental influences:** for example electromagnetic interference, high ambient temperature or humidity;
- **seizing due to lack of use:** overload clutches, pressure relief valves and ultimate high- or low-level switches are examples of protective systems which can fail due to lack of use;
- **wear and tear:** less common with protective systems which may only operate occasionally, but guard interlocks and non-return valves may be subject to wear and tear and relay contacts to welding;
- **corrosion:** more common in the process industries where probes or sensors may be exposed to corrosive chemicals;
- **loss or disturbance of services:** these include power, air, cooling water, trace heating, ventilation fans, etc.

The root causes for these failures can best be identified using a rigorous failure modes and effects analysis (FMEA). For complex systems, a fault tree analysis (FTA) may be also necessary.

preventing failure

The reliability of protective systems against unsafe failures can be optimised by:

- **inspections and preventive maintenance:** appropriate in the minority of cases where the protective system is subject to wear, corrosion or degradation, and regular inspections or time-based overhauls or replacements are appropriate. Cleaning or lubrication may also be appropriate in some cases. However, condition monitoring is seldom applicable as few protective systems give any indication that they are going to fail before they fail.
- **design improvements:** modifications to the design of the protective system or improving the reliability of its components may be necessary for a number of reasons including:

– the system can be readily bypassed or disabled, or the settings altered;
– the system is inherently unreliable or it cannot give the required level of protection;
– multiple protective systems that share common cause failure modes;
– the system cannot be tested at all or cannot be tested as often as is necessary;
– the testing involves dismantling or disconnecting the system – with the risk of leaving the system in a failed state after re-assembly;
– the test itself may increase the risk of the multiple failure – for example where the protective system is not protecting while being tested;
– the test procedure is complex with many procedural steps;
– the frequency of testing is relatively high; and
– the cost of testing is excessive.

> *"Less than ten percent of failure modes have age-related failure patterns...For complex systems that percentage is even lower: ie most protective systems will fail randomly"*

- **regular testing of the protective system:** the pioneering work carried out in the civil airline industry (Nowlan & Heap) demonstrated that less than 10% of failure modes have age-related failure patterns and that for complex systems such as protective systems the percentage is even lower, ie most protective systems will fail randomly. Therefore, as the failure of these systems cannot be predicted on an age or condition basis, their failure cannot be prevented in most cases. To reduce the loss of protection to acceptable levels, regular testing or inspection of significant protective systems is therefore essential to check that they are still operational. Determining the frequency of this failure finding or testing task is discussed below.

testing intervals for single-channel protective systems

For single-channel protective systems, there are two basic approaches for determining the frequency of testing – depending on the consequences of the ultimate 'multiple failure' (ie the failure of the protective system and the failure of the protected function).

If the consequences of the multiple failure are only economic (which includes not just the repair costs but also the cost of lost production, reduced yields, etc), the optimum test interval will be based on minimising cost. However, if there are safety or environmental consequences, ALARP or BAT

principles will apply. The approach for each is detailed next.

economic consequences

The optimum test interval, where the consequences of the multiple failure are economic will be when, over a period of time, the sum of the cost of testing the protective system and the cost of the multiple failures is at a minimum.

The basic formula for optimum test interval for a single-channel protective system is:

$$T_{opt} = \left[\frac{2 \times C_{ff}}{\lambda_d \times \lambda_v \times C_{mf}} \right]^{1/2}$$

where C_{ff} = the cost of carrying out the failure-finding task

C_{mf} = the total cost of a multiple failure

λ_d = the failure rate of the protected function, ie the demand rate

λ_v = the unsafe failure rate of the protective system

safety and environmental consequences

Calculating test intervals for protective systems where there are safety and/or environmental consequences requires the level of tolerable risk of a multiple failure to be determined – bearing in mind that zero risk is rarely, if ever, achievable. For safety consequences, this will need to take into account the overall level of risk, and ensure that it is in the appropriate region of the ALARP triangle.

The basic formula for the test interval is:

$$T_{ff} = \frac{2 \times \lambda_{mf}}{\lambda_d \times \lambda_v}$$

where λ_{mf} = the tolerable failure rate for multiple failures

λ_d = the failure rate of the protected function

λ_v = the unsafe failure rate of the protective system

testing intervals for more complex protective systems

Protective systems are becoming increasingly complex, and the formulae outlined above do not cover:

- multiple/redundant systems;
- voting systems;
- common cause failure;
- that the test itself might cause the protective system to fail;
- cases where it is only possible to test part of the system;
- cases where, during the testing procedure, the protective system will not be functional;
- systems where the failure patterns are not random;
- systems where repair times for the protected function/system are significant; and
- human error.

To further complicate matters, robust data are seldom available for failure rates. Manufacturers' data will generally relate to ideal operating conditions and therefore be unrepresentative for the operating context under consideration. And data on human error rates may be of doubtful validity.

We have developed formulae to cover the above complexities, and using software, the protective system can be modelled, sensitivities tested and assumptions evaluated.

The outcomes can be surprising and illuminating. For example, if the risk of leaving the protective system in a failed state after the test is even as low as 1 in 1000, the test may well increase the risk of a multiple failure. Design or procedure changes will be necessary if the required safety levels cannot be achieved or the frequency of testing is unacceptably high.

Ensuring the safe operation of plant through the correct application and maintenance of protective systems is a complicated issue. Yet no organisation can afford to ignore it.

For many companies, regular inspections and testing will suffice. However for critical and complex situations, both the design and maintenance of the protective systems need to be considered in greater depth.

The computer-based modelling approach we favour enables the risks and sensitivities to be evaluated. The outcome is a better understanding of the issues which, in turn, leads to the establishment of soundly-based and robust protective systems. **tce**

The consequences of failure of those systems we use to protect us can be serious

further reading

1. *Reliability-centred maintenance*, Nowlan, FS, and Heap, HF, US Department of Commerce, 1978
2. *The tolerability of risk from nuclear power stations*, HSE, 1992
3. *Reliability, maintainability and risk*, David J Smith, Butterworth-Heinemann, 2005
4. *Reliability and risk assessment*, Andrews, JD, Moss, DR, Longman, 1993
5. "Safety-related systems", *Hazards Forum*, 1995
6. "Evaluation of significant transitions in the influencing factors of human reliability", Konstandinidou, M, Nivolianitou, Z, Kiranoudis, C and Markatos, N, *Journal of Risk and Reliability*, IMechE, 2008
7. *Functional safety of electrical/ electronic/ programmable electronic safety-related systems*, IEC 61508, 2005
8. *Functional safety – safety instrumented systems for the process industry sector*, IEC 61511, 2003
9. *Principles for proof testing of safety instrumented systems in the chemical industry*, HSE, 2002

Michael Dixey and John Gallimore are principal consultants with GGR Associates (info@ggrassociates.co.uk)