

# SIL Rating Fire Protection Equipment

**Richard M Robinson, Kevin J Anderson**

Risk & Reliability Associates Pty Ltd  
Level 2, 56 Hardware Lane, Melbourne VIC 3000, Australia

richard.robinson@r2a.com.au

kevin.anderson@r2a.com.au

## Abstract

SIL's (Safety Integrity Levels) are used by IEC 61508:1998 [1] to characterise the required functional safety of computer control systems. For example, SIL 4, the highest rating is for fly by wire aircraft and weapons systems and track circuited train signalling systems while SIL 2 is typical of certain Programmable Logic Controllers (PLC). Fire control panels have not been SIL rated to date even though certification organisations like Factory Mutual provide SIL for various PLCs in their approvals guides. This paper addresses 'SIL' derivation/allocation to fire systems and fire control panels in particular.

*Keywords:* Fire systems, fire control panels, SIL .

## 1 Introduction

The Functional Safety standard IEC 61508:1998 [1] sets out requirements for electrical /electronic and programmable electronic (E/E/PES) systems. A system is said to be safety-related if any failure to function can present a prospect of harm to people.

The standard has had a long gestation through the 1990's. IEC 61508 is very general and allows application sector standards to be developed under its umbrella. However only a few application sector standards such as the process industry standard IEC 61511 have addressed functional safety for their particular domain and even that remains under debate. The process industry has a particular 'layer of protection' approach where the safe state is to shut-down the process.

Fire life safety on the other hand is primarily concerned with time, given an ignition: what are the detection, evacuation and response times to avoid untenable conditions?

Fire is such an obvious hazard and fire detection systems arguably should be certified to the functional safety standard. Fire control systems cover detection, evacuation and firefighting phases.

Sub-systems include CCTV systems, break glass alarms and fire phones connected to a control room; automatic smoke and heat detection systems (the latter requiring a fire to have reached a sufficient size); callout of fire brigade, smoke control, evacuation procedures, public address and siren systems, emergency and exit signage, sprinklers and deluge systems, hose reels, hydrants and lastly, burnout minimisation through structural measures.

Some of these systems, particularly those relating to an operations control centre are programmable. Other constitute necessary risk reduction through 'other technology' and 'external risk reduction facilities'.

Compliance of the programmable systems with IEC 61508 remains rare and product certification can add considerably to the cost of a product. For example, the Allen Bradley range of programmable logic controllers (PLC) are certified by TUV, Germany [2] but more often than not are installed without strict compliance.

Certification by TUV to IEC 61508 includes field data to confirm reliability metrics including Mean Time Between Failures (MTBF) and independent analysis of probability of Failure on Demand. TUV TYPE approval relates only to hardware, with implementation rules for software configuration to suit a particular control system application. Functional safety assessment is still required of the specific application.

Such certification can considerably increase project costs and industry has been reluctant to follow the lead. Critics of the standard have also been strident. For example, O'Connor 'Practical Reliability Engineering' [3]:

- 'The standard (IEC 61508) is without practical value or merit. The methods described are inconsistent with accepted industry practices, and many of them are known only to specialist academics, presumably including the members of the drafting committee'.

As a contractually enforceable document, the authors only agree with O'Connor that the standard is not practicable where there is no form of third party certification such as TUV Germany or Factory Mutual USA [4] which provides an agreed interpretation.

The objective of this paper is to show how a target SIL would be derived for fire protection systems. However, it does not attempt to assess whether current technologies would meet those targets.

Factory Mutual personal communication [5] notes that fire panels do not have a SIL rating but observes as 'a very important part of a safety system, I believe that they should have a SIL rating.'

The contention is that the SIL rating should depend on the risk level. For example, the SIL rating of a fire panel for a facility of 20 employees and a small building would probably be much less than the SIL rating for a complex of several buildings and 1000 employees'.

In the discussion below, the idea of SIL is briefly explained in section 2 and then a case study is presented in three parts (concept, risk analysis and requirements) in sections 3, 4 and 5. The discussion in sections 6 and 7 then addresses a perceived gulf between the risk-based approach adopted by IEC 61508 for safety-related systems and the so-called 'confidence' that reliability engineers have that fire control system 'work' and thus do not require safety-related certification.

## 2 SIL Levels

Safety Integrity Level (SIL) is a measure of the probability that the safety related system may fail in a dangerous manner. The value of SIL ranges from 1 (the lowest) to 4 (the highest). The table below is adapted from IEC 61508-1:7.6.2.9 [1]:

Safety integrity level (SIL)	Low demand mode of operation (Average probability of failure to perform its designed function on demand)	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

**Table 1 SIL levels**

In determining a SIL, parts 1 and 5 of IEC 61508 take a hazard and risk based approach with progressive refinement through three stages;

- Concept & scope (1:7.2 and 1:7.3),
- Hazard & risk analysis (1:7.4),
- Safety requirements definition & allocation (1:7.5 and 1:7.6).

These are discussed in sections 3, 4 and 5 respectively:

## 3 Concept & Scope

The objective as to concept is to provide an understanding of the domain sufficient to establish 'due diligence' as to causation. The case study considered here is a revisitation of earlier work by the authors' previous firm into application of a Fire Risk Management Information System (FRMIS) to a multi-campus Victorian University. [6]

A University campus comprises a great many buildings and activities and a systematic method was required for establishing priorities for improving fire safety. At the time of the initial work, the *Occupiers Liability Act* 1983 and now *Wrongs Act* (1958 as amended 2000) and *Occupational Health and Safety Act* (1985 as amended 2003) impose duties of care for building owners, occupiers, staff, students and visitors.

Various studies including the seminal Health and Safety Executive, UK [7] suggested a target (acceptable) individual fatality risk of one chance per million years. Societal risk approaches suggested one or even two orders of magnitude lowering of acceptable likelihood for each order of magnitude increase in consequence.

The road toll sits at two orders of magnitude higher, i.e. at about one hundred chances per million years and represents an 'undesirable' risk. The reality: 'tolerable' risk is in between and subject to the ALARP principle to reduce risks..'As Low As Reasonably Practicable'.

## 3.1 Physical equipment within scope

The objective as to scope is to determine the boundary of the equipment-under-control (EUC) and its control systems.

Physical equipment and systems installed in buildings to aid life safety when threatened by fire include:

- fire detection and control systems,
- alert and communications systems,
- smoke control and air handling systems,
- emergency and evacuation procedures,
- exits, exit signs and emergency lighting.

The fire control panel represents a common mode point of failure across each of the detection, response and evacuation sub-systems.

Interactions between the various systems also need to be considered. Fire panels are usually separately wired to a Facilities Control Centre where operators will also have access to security CCTV cameras and Building Control systems including ventilation and plant. These provide alternative pathways for fire detection and response and mitigation of potential losses.

## 3.2 External events and Accident initiating events

In any building, equipment may catch fire due to electrical fault for example or occupants may themselves cause a fire. In the latter case, ignition is not itself the threat, the threat is undetected escalation of combustion.

Conversely, the social mores that castigate smoking inside buildings have enhanced the widespread deployment of very early smoke detection alarm (VESDA).

Sabotage and terrorism are increasingly credible threats and centralised building control systems are now driven by these considerations.

In the terminology of IEC 61508 [1], a manifest hazard becomes a hazardous situation when a circumstance arises in which a person is actually exposed to hazards. Successful deployment of sensible precautions including sprinklers and deluge systems can but may not prevent such escalation.

A hazardous event or accident is then the balance of probability that the hazardous situation actually results in harm. In legal terms, once the precautions fail, control has been lost.

#### 4 Hazard and Risk Analysis

The objective of hazard and risk analysis is to determine the hazards (credible threats) and hazardous events (accidents) in all reasonably foreseeable circumstances. A time sequence model is suggested as a beginning towards structuring the analysis as a cause-consequence model. In this model, time flows from left to right, with loss expectancy escalating as precautions fail. Refer Figure 2:

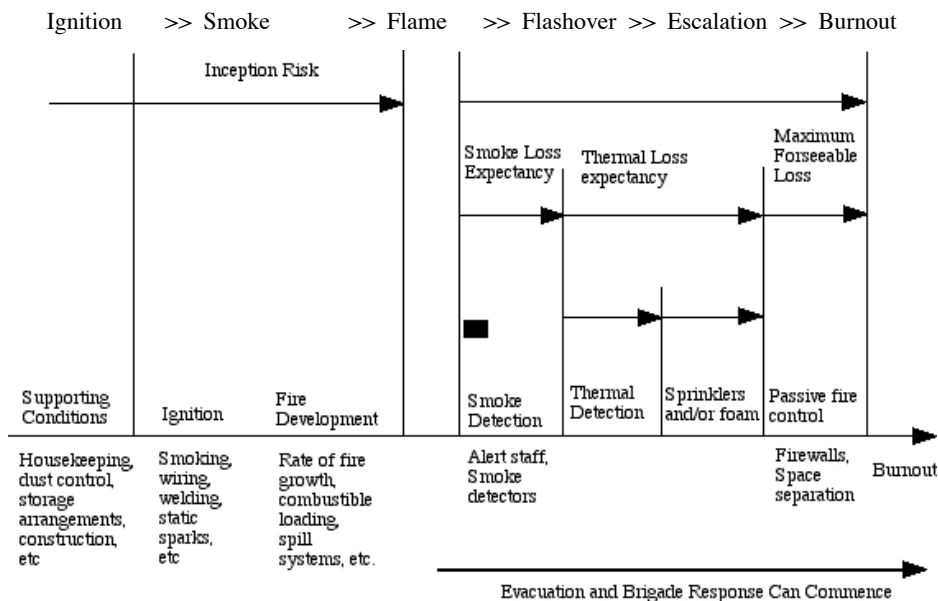


Figure 2 A Time Sequence Model for Fire

Fire start frequencies are used to express credible threats in terms of what size fire requires brigade attendance and may result in significant property damage and possible loss of life. Given a major fire, the balance of probability of an unwanted outcome depends on the success or otherwise of early detection, containment, evacuation and fire fighting strategies.

Figure 3 shows the application of the event tree analysis technique (the outcome side of a cause-consequence model). Domestic fire start data suggests 1 in 1000 houses per year has a fire and 1 in 1000 of those results in fatality(ies).

This is indicated in generic terms on the right hand side of Figure 1.

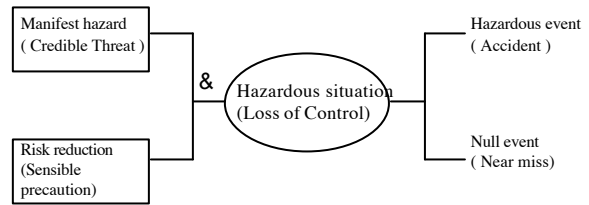


Figure 1 Concept Cause-consequence Model

Allowing one in a million therefore appears relevant to domestic conditions as per Figure 3 below. However, this figure is largely dependent on occupants saving themselves rather than brigade response with 2 hour fire rating between occupancies as per Building Codes containing escalation to adjoining occupancies.

Reliance on programmable fire control systems in multiple occupancy buildings could constitute a common mode failure in relation to both Question 1 and Question 2 hence, depending on the number of persons at risk, 99% to 99% reliability should be expected of such systems, that is 1% to 0.1% failure on demand, which is the SIL 2 range.

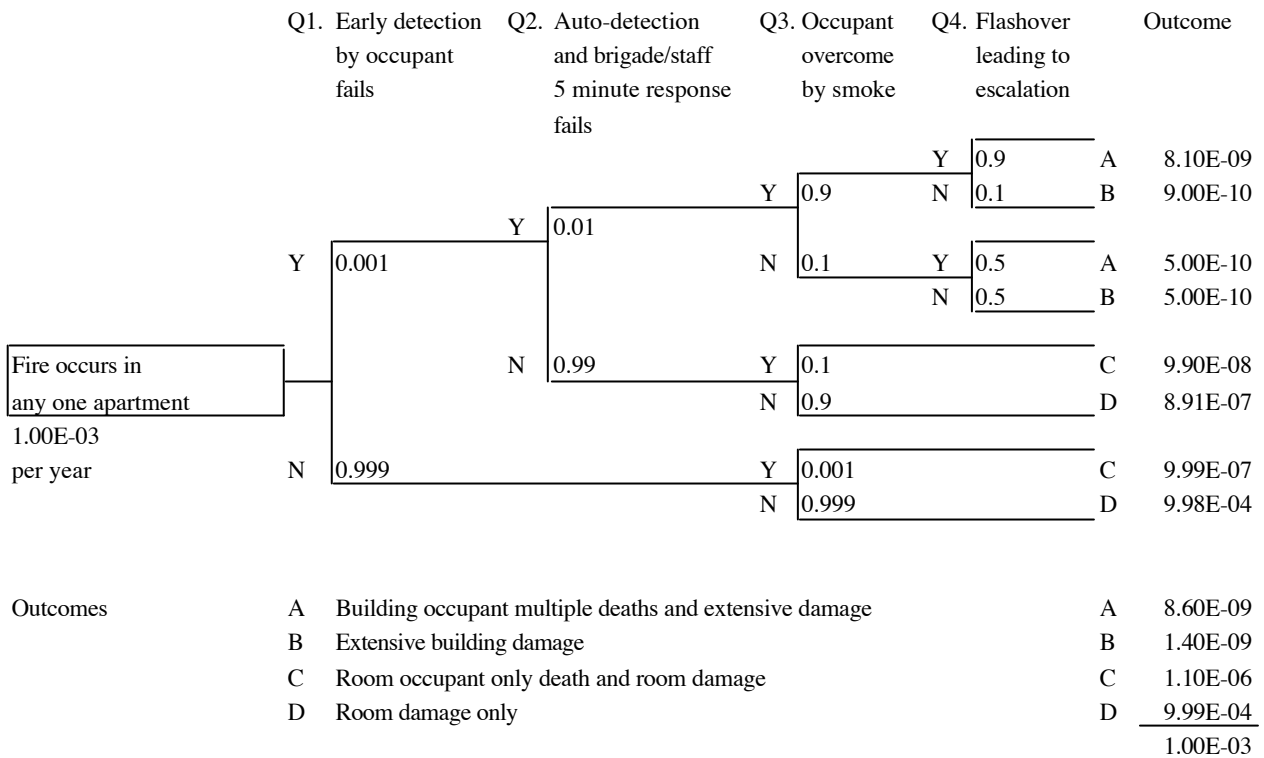


Figure 3 Event Tree Analysis of fire outcome

Figure 4 show a notional run of a Fire Risk Management Information System (FRMIS) model for a hypothetical building.

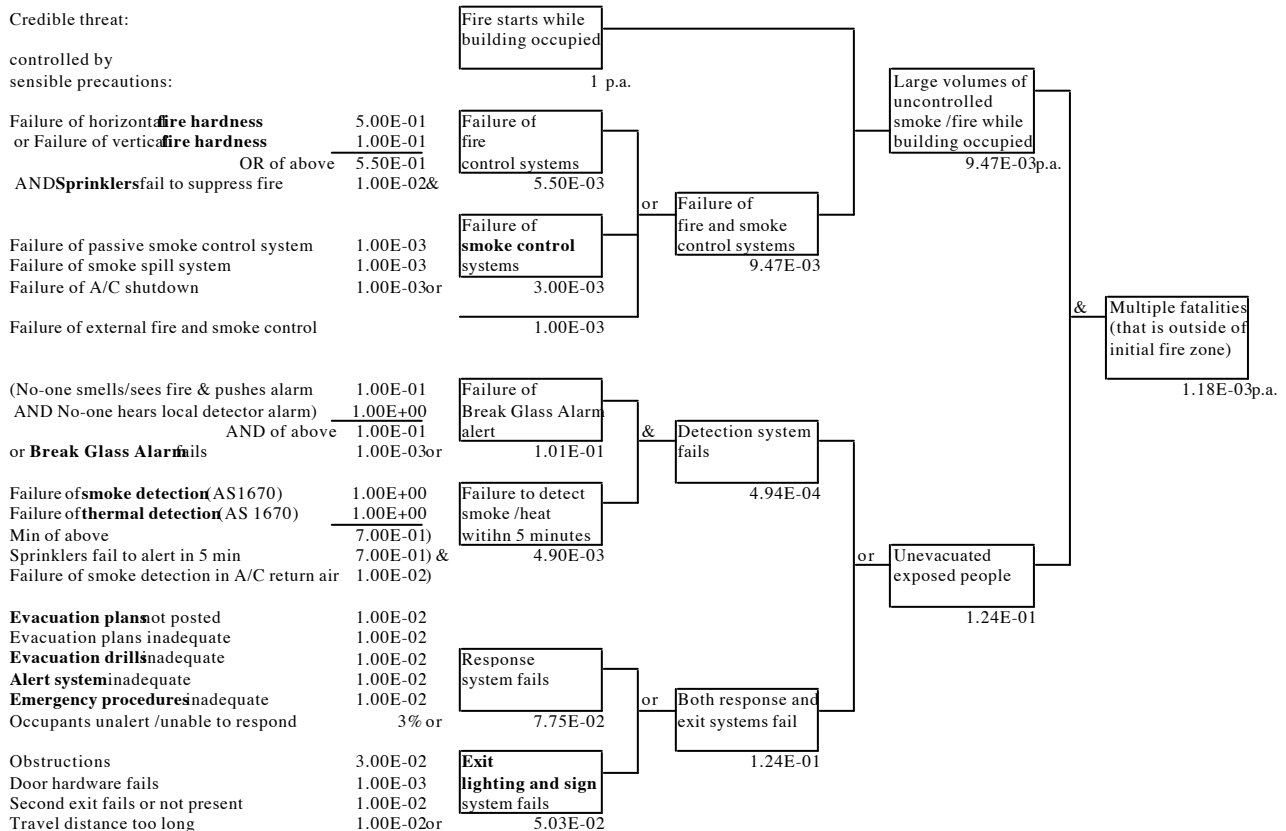


Figure 4 Fault Tree Analysis of fire control

(Note 12 items in bold further discussed in section 5)

The fault tree analysis presented in Figure 4 is used to assess the relative effectiveness of measures such as:

- smoke detection and alert system (if any),
- thermal detection and alert system,
- occupant response to evacuation plans,
- fire rating of doors, walls etc.,
- sprinkler system operation.

In the above example, the concern is focussed on multiple life loss expectancy. Conditional probabilities are based on engineering judgement, reliability data and failure rate analysis.

For example, the event 'Early detection by occupants' is modelled by fault tree inputs:

- alertness of occupants,
- adequacy of emergency procedures,
- availability of alert system,
- existence of evacuation system,
- efficacy of training.

Again, programmable fire control systems could constitute a common mode failure against any or all of the detection system, response system or fire/smoke control systems. Taking the latter claim of  $9.47E-3$  failure rate for example, a good SIL 2 claim of  $1E-3$  is a small fraction, but the other end of SIL 2 at  $1E-2$  failure rate is significant.

Tolerable risk for a given floor of a building is then derived in terms of comparative necessary risk reduction for various types of occupancy:

- Residential occupancy,
- Office occupancy,
- Public occupancy,
- Laboratory occupancy.

The asset and threat vulnerability approach focuses attention on the University libraries - the primary source of intellectual property - while the life safety approach emphasise residential halls - due to overnight occupancy.

The societal risk argument raised in section 3 is that orders of magnitude increase in consequence should be compensated for by at least one order of magnitude decrease in likelihood. For consequences greater than one hundred fatalities, two orders of magnitude reduction should be sought, while for thousands of possible fatalities, likelihood arguments are possibly not cogent.

In any event, the 'due diligence' defence after the event must be that all sensible precautions were employed and whatever it was that did go wrong was either not a matter of causation, nor foreseeable, nor preventable. The reasonableness or ALARP defence has increasingly been eroded though over-reliance.

## 5 Safety Requirements Definition & Allocation

Necessary risk reduction can be achieved by external risk reduction facilities (ERRF), other technology and independent safety-related systems.

The FRMIS model depicted on Figure 4 above represents in **bold** 12 important factors relating to the probability of successful escape from a building when a large fire occurs. In the application of the model to particular buildings, three levels of success are assigned to each factor:

- not installed (failure probability certain = 1.0),
- installed but not maintained (0.1 - one in ten),
- installed and being adequately maintained (but probability nevertheless prescribed by SIL rating - assign a rating between 0.01 and 0.001).

As noted in section 3, the fire control panel represents a common mode point of failure across each of the detection, response and evacuation sub-systems and this suggests a higher level of assurance than for the individual sub-systems. Rather than assess SIL on a continuous control basis, note that the 'per demand' approach is intended to apply to reactive systems where the demand is less than one per year. This is the case for most fire situations.

The separation of systems required to satisfy diversity of different SIL imposes integration responsibilities on operators and concomitant understanding in the human factors of emergency response. There have been a number of classic examples of multiple alarms being ignored until external confirmation asserted that the fire was 'real'.

Applying the fire start frequencies to the conditional probabilities from the fault and event trees (including a 'hot spot' allowance for obvious hazards such as petrol bowsers located inside a maintenance building) provides an estimate for every building of multiple death fire risk.

Sensitivity testing of variations in installed and maintained items allows calculation of greatest risk reductions achievable per dollar spent. Following the immediate need for emergency and evacuation planning, it was found that satisfactorily maintaining a building's smoke control system provided the best medium term solution with installation of sprinklers in buildings the next priority.

For both the ETA techniques (Figure 3) and the FTA techniques (Figure 4), the conclusion is that a requirement of necessary risk reduction of 999 in 1000 is necessary to successfully control fire starts.

The authors note that the SIL range is rather loose and that SIL 2 delivers between 99 and 99.9% risk reduction. But how to arrive at a judgement as to which end of the scale? A very good SIL 2 may well be satisfactory. So would an indifferent SIL 3!

In availability terms, the authors experience is that Commercial-off-the shelf (COTS) systems only deliver 95% availability simply through 'best practice' good quality systems and software engineering requiring some form of redundancy or diversity to deliver very high reliability. 95% AND 95% = 99.75%.

Requirements for independence between the various claims for necessary risk reduction by different sub-systems are specified in terms of diversity and not sharing common parts such as power supplies.

## 6 The void between risk theory and reliability theory

Suppliers of fire control panels are no doubt confident as to the reliability of their products. However, a problem seems to arise between domains satisfied with the dependability of their systems and the IEC 61508 approach when reliability becomes safety related and thus has liability overtones. Figure 5 shows this in terms of shareholder versus judicial scrutiny.

Obviously risk and reliability are related concepts. Low risk high reliability systems are considered desirable and in many cases risk is expressed as the complement of reliability. In one sense at least, as further discussed in section 6.2 below, risk is a subset of reliability.

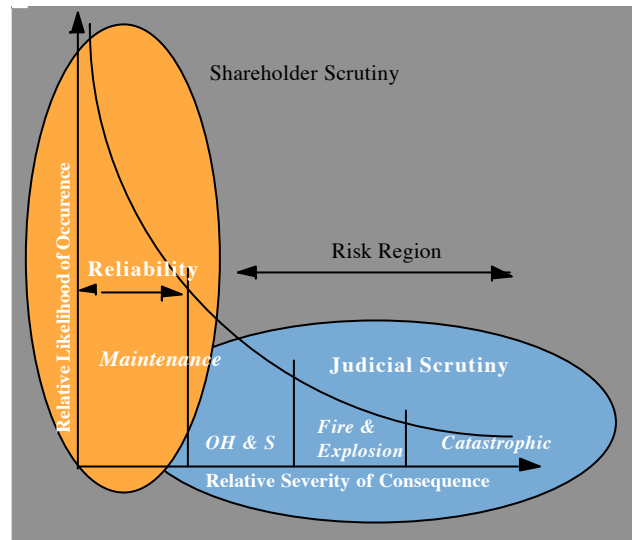


Figure 5 Shareholder scrutiny vs Judicial Scrutiny

Reliability is also inextricably entwined with availability and maintainability (the RAM acronym). If availability is thought of in terms of a repairable system being “up” and “down” then a number of concepts and terms can be simply defined as per Figure 6:

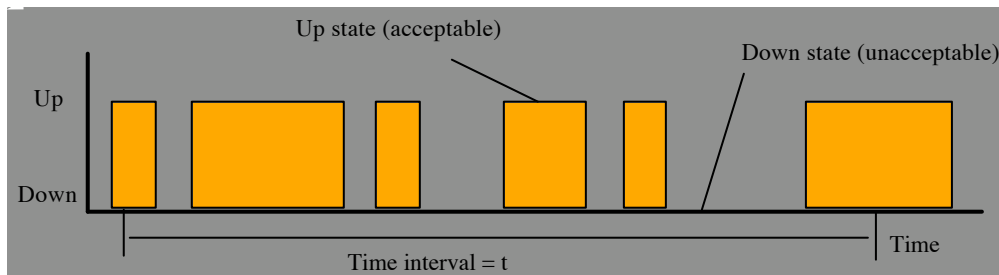


Figure 6 Two State Availability Concept

### 6.1 Reliability Theory

The time in the up state is related to reliability and the time to repair in the down state. Relevant definitions are:

- MDT or Mean Down Time, that is, the average time the system is in a down state,
- MTTR or Mean Time To Repair, that is, the average time to restore to the up state,
- MTBF or Mean Time Between Failure, that is, the average up time.

For a system where the breakdown failure rate is constant with respect to time (or random), reliability is:

$$R = e^{-\lambda t} = e^{-t/MTBF} \text{ where}$$

R is reliability

e = 2.718218 (a constant)

t is mission time in hours

$\lambda = 1/MTBF$  and is the (average) failure rate per hour. MTBF is in hours

For example, if  $\lambda = 0.01$  per hour (1 per 100 hours) and  $t = 10$  hours then  $R = 0.9$ . That is, a device has a 90% chance of operating continuously for a 10 hour period.

Where the mission time equals the MTBF, the reliability formula reduces to:  $R = e^{-1} = 0.368$ . This predicts that 37% of the population will survive until the MTBF which is to say reliability at the mean is slightly under-predicted. Where t is small in relation to MTBF the advantage is that only a single parameter is needed to predict the reliability.

Note that unreliability =  $1 - e^{-\lambda t}$  For  $t=1$  and  $\lambda$  very small ( $10^{-5}$ ) then:  $1 - e^{-\lambda t} \sim \lambda$ . Unreliability (1 year) =  $\lambda$  p.a.

This is the point at which the reliability engineer's fault rate seems to become equivalent to the risk engineer's failure frequency. Mathematically at least, it means that risk is a simplification of reliability at this point. But it

may not be that simple as there is an apparent void between risk concepts and reliability concepts.

## 6.2 The Existence of the Void

The existence of the void between reliability and risk can be demonstrated in at least five ways:

Firstly, the psychology of reliability people is positive (the likelihood of success) versus the risk people who are negative (the possibility of failure). Risk engineers and reliability engineers give a very different meaning to the term 'failure'. Refer Figure 7:

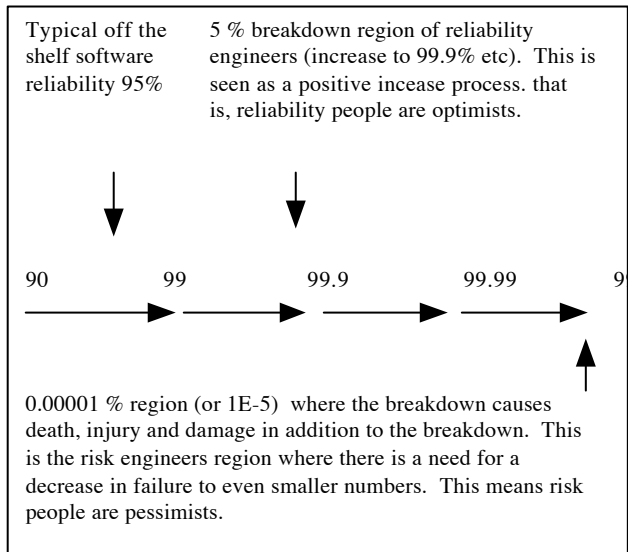


Figure 7 Fault vs Failure

Failure (fault) to a reliability engineer usually means 'unavailability' whereas failure to a risk engineer means the loss of control of a damaging energy with some form of consequence (death, injury or damage) beyond the equipment or process merely coming to a stop. Further, the 'failures' discussed by risk engineers have a much lower likelihood of occurrence than the failures (faults) of the reliability engineers.

Consider for example, the time that a plant will be unavailable due to a serious fire in the factory (a risk engineer's failure) versus the time that it is unavailable due to machinery breakdown (the reliability engineer's failure).

To draw the distinction between the two types of failure it is proposed that the following terms be used when the distinction appears important:

- for failure (breakdown), the term "fault", and
- for failure (risk) the term "failure".

This parallels an apparent effort by the British Standards Institution (BS 5760: Part 2: 1994)[8] to have the technique of "Failure Modes and Effects Analysis" renamed "Fault Modes and Effects Analysis (FMEA)". This has also been adopted in AS 3931:1998, *Risk Analysis of Technological Systems - Application Guide*. [9]

Secondly, the difference in viewpoints explains O'Connor's views [3] about IEC 61508 being without practical value or merit.

Thirdly, there are two reasons for maintenance tasks – to optimise availability and reliability, and minimise liability.

It is very difficult for the reliability people to deal with going from 1E-5 to 1E-7 compared to 99.999% to 99.99999% availability. However, a seemingly small difference of 0.00099% is also the difference between injury and multiple fatalities. This is where criminal and common law liability arises. Enter the liability dragon.

The following table expresses this dichotomy in terms of "nines":

Downtime p.a.	Availability
30 secs	is 99.999905% or "6 nines"
up to 1 min	is 99.999810%
up to 5 min	is 99.999049% or "5 nines"
up to 10 mins	is 99.998097%
up to 30 mins	is 99.994292%
up to 45 mins	is 99.991438% or "4 nines"
up to 1 hr	is 99.988584%
up to 2 hrs	is 99.977169%
up to 10 hrs	is 99.885845% or "3 nines"

Table 2: Summary of Availability Numbers

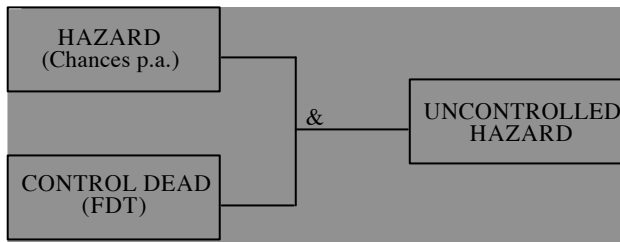
Fourthly, IEC 61508 is a very continental inquisitorial standard (as opposed to a jousting (adversarial) conflict standard). A Functional Safety Assessment (FSA) goes in search of information until sufficient evidence has been gathered to come to a judgement. It is a very European way of fighting the liability dragon. It seems difficult to understand for those in an adversarial liability system.

Fifthly, the chemical industry has been calling up SIL rated circuits for some time in relation to major hazard Safety Cases. Why? We suspect that they have been looking for a risk based approach to reliability and liability. Hence use of IEC 61508.

## 7 Suggested Synthesis

Fault Tree Diagrams are good for analysing particular hazards and complementary to Reliability Block Diagrams (RBD). This section examines an alternative approach as a means of cross-checking the calculation.

Fractional Dead Time Mathematics is useful here. Fractional Dead Time (FDT) is the fraction of time that the equipment is dead (cannot operate properly). It is referred to as FDT because the failure of the equipment itself does not pose a threat until there is a realisation of another hazard, such as fire. The probability of the uncontrolled hazard (hence, the overall failure rate) can be determined through a simple AND gate argument:



**Figure 7 AND Gate Argument**

For example, a fire detection system that is checked weekly and takes one hour to repair has a maximum dead time of one week and one hour, that is, if failure occurs immediately after inspection and is not detected until the next inspection. Note that failure immediately after inspection is as much likely due to testing or repair defect or incorrect re-commissioning as is a random failure.

Assuming one equipment failure on average per year gives a maximum FDT of 0.01928 (169 hours per 8,760 hours). Similarly, equipment averaging 2 failures per year has a FDT of 0.03856.

If the building typically experiences a fire once every 10 years (or, 0.1 chances p.a.), then the probability of an undetected fire is:

$$- \quad 0.1 \times 0.01928 = 0.001928 \text{ chances p.a.}$$

The occurrence of equipment failure can be estimated as the Mean Time Between Failure (MTBF). MTBF is the reciprocal of the equipment failure rate, with the above example having a MTBF of 1 year. It should be noted that the MTBF is characteristic of the equipment item, and is independent of the frequency of testing.

IEC 61508 [1#7:C5.1] suggests probabilistic testing is a very difficult way to demonstrate ultra-high levels of reliability. At 95% confidence the formula for zero failures over  $n$  test cases is  $3/n$ . At 99%:  $4.5/n$ . These therefore require huge numbers of cases to prove SIL 2 or SIL3. It also means that a risk engineers view of confidence in a failure rate derived from an MTBF claim is pessimistic compared to the reliability engineer. The risk approach is concerned at the consequences of the first failure, while the reliability approach attempts to optimise the overall lifecycle cost including faults over the life of a project.

Analogous to MTBF is the Mean Time Between Hazard (MTBH), which is the reciprocal of the probability of the overall hazard (fire with no detection). In our example, the MTBH is 518 years ( $1/0.001928$ ).

If the system was checked once every year, it would have an FDT of almost certain failure - at best  $4381/8750 = 50\%$  - an MTBH of 20 years. These examples show the importance of checking equipment regularly, as the time between checks is usually much greater than the time required to repair the equipment.

Given the reciprocal relationship between MTBH and FDT, using the worst case scenario for FDT produces a minimum MTBH. In practice however, if the system

fails randomly then, as an average, we could say it fails mid term between testing periods. For the above example, the FDT would be one half week plus one hour (85 hours per 8,760 hours), or 0.0097.

$$- \text{ Mean Time Between Hazard} = 1/(0.1 \times 0.0097) = 1,030 \text{ yr}$$

This is an order of magnitude more pessimistic than the 99.9% claim for risk reduction derived from the fault tree presented at Figure 4. The conclusion from this is that equipment with a high MTBF but only weekly checks may NOT be acceptable.

The question of which calculation is a closer approximation to reality depends on the failure curve after testing. That is, if failure is most likely to occur immediately after the equipment goes on line after testing (often the case) rather than randomly, then the minimum Mean Time Between Hazard is probably the prudent design assumption.

In the final example above, an average FDT of 0.0097 is derived. This necessitates a corresponding software SIL of SIL 2 that is, any programmable components within the fire control system should be demonstrated as sufficiently reliable not to compromise those systems.

For multiple fatality consequences SIL 3 is indicated due to societal concern for multiple fatality accidents.

## 8 Conclusion

In conclusion:

- Fire control systems including fire control panels face a number of safety assurance issues and there is as yet no commonly accepted means for deriving Safety Integrity Levels (SILs).
- Functional Safety Assessment for the case Study indicates IEC 61508 SIL 2-3 would be required to guard against systemic failures such as those involving software and programmable devices.
- Reliability analysis using Fractional Dead Time suggests frequent and regular in-service testing is required to assure safety against risk of random failure.

## 9 References

- [1] IEC 61508:1998 (aka AS 61508:2000) Functional Safety of electrical /electronic and programmable electronic (E/E/ES) safety-related systems.
- [2] Allen Bradley *ControlLogix receives TUV certification for use in SIL 2 Applications* <http://www.ab.com/logix/controllogix/sil2.html>.
- [3] O'Connor, PD *Practical Reliability Engineering*. Wiley, 2002.
- [4] Factory Mutual Research Approval Guide (2001). Chapter 4, *Functional Safety of Safety Related Systems and Components*.
- [5] Personal Communication. Electrical Systems Group FM Approvals. 4 June 2003.
- [6] Jarman, M, Tillman C and Robinson (1989) *Management of building fire risks through quantified*

*risk assessment techniques - a case study.* NSCA Convention. Monash University.

[7] Health and Safety Executive, UK *The tolerability of risk from nuclear power stations.* London HMSO, 1988.

[8] British Standard BS 5760: Part 2: 1994. Reliability of systems, equipment and components. Guide to the assessment of reliability.

[9] AS 3931:1998, Risk Analysis of Technological Systems - Application Guide.

## 10 Glossary

ALARP As Low As Reasonably Practicable

CCTV Closed Circuit Television

COTS Commercial Off The Shelf

E/E/PE Electrical /Electronic Programmable Electronic

ERRF External Risk Reduction Facilities

ETA Event Tree Analysis

EUC Equipment Under Control

FDT Fractional Dead Time

FM Factory Mutual Research Corporation, a global testing and assessment service

FMEA Fault Mode Effects Analysis

FRMIS Fire Risk Management Information System

FSA Functional Safety Assessment

FTA Fault Tree Analysis

IEC International Electrotechnical Commission

MDT Mean Down Time

MTBF Mean Time Between Failures

MTBH Mean Time Between Hazards

MTTR Mean Time To Repair

PLC Programmable Logic Controller

RAM Reliability, Availability, Maintainability

RBD Reliability Block Diagram

SIL Safety Integrity Level

TUV TUV Rheinland Berlin Brandenburg Group - a global testing and assessment service

VESDA Very Early Smoke Detection Alarm