What is Good Practice for the Proof Testing of Safety Instrumented Systems of Low Safety Integrity?

Jeff Wood BSc, CEng, FIMC, MIET, Ineos ChlorVinyls Runcorn Site, PO Box 9, Runcorn, Cheshire WA7 4JE.

Where safety instrumented systems are intended to provide risk reduction of greater than a factor of ten (SIL 1 or above), recognised good practice for their implementation and management is provided by BS EN 61508 and sector-specific standards such as BS EN 61511. These standards require robust design, verification, and in particular, routine proof testing. However, there is very little guidance available on how to handle those safety instrumented systems that are not required to provide a factor of ten risk reduction but which, never the less, still providea contribution to the safe operation of plants.

The Health and Safety Executive (HSE) have described such systems as 'instrumented systems implementing a low integrity safety function' and have published guidance to their specialist inspectors (SPC/Technical/General/51) that requires, amongst other things, that such systems should be periodically proof tested for the purpose of revealing dangerous undetected faults. Whilst, on the face of it, such a requirement seems sensible it does beg the question, with modern, reliable instrumentation on low integrity duties; is such proof testing really justified?

Instrument protection systems (interlocks and alarms) which are designed and implemented to modern instrument standards provide a good standard of reliability without any special maintenance and testing arrangements in place. The testing of all low integrity instrument systems on plants is costly and resource intensive and there is a risk that it utilises available resources in a non optimal way by diverting them from other work which would deliver greater safety improvement benefit.

Background

INEOS ChlorVinyls, Runcorn Site, UK is a large complex manufacturing chlorine, chlorinated methanes and ethylene dichloride for PVC end use. It is a ‘top tier’ COMAH site, which was under ICI ownership before INEOS acquisition in 2001. The site has been producing and using hazardous chemicals for well over 100 years. The importance of instrumented protective systems, such as trips and alarms, in contributing to the safe operation of these processes has long been recognised. By the 1980s, there were so many of these systems it was recognised that it was necessary to be able to separately identify those that were really important for the safety of the plants from those that had a more minor influence on safety or were just there for operational reasons. Those systems that were seen as providing the last line of defence against a hazardous event were classified as SHE (Safety, Heath and Environment) Critical whilst those that made a less significant contribution to safety were classified as SHE Related. The SHE Critical Systems were then targeted for the highest levels of proof testing and reporting whilst maintenance of the SHE Related systems was left more to the discretion of the individual plant control and electrical engineers.

With the publication of the IEC (later BS EN) 61508 standard in 1998, which gave a rather different meaning to the term ‘safety related’ it was agreed to move away from the old, consequence based, system of classification and adopt the risk reduction based system of classification contained within the standard. Those systems that were classified as Safety Integrity Level (SIL) 1 or SIL 2 (we do not have any SIL 3 systems) continued to be described as SHE Critical systems. Those systems that were seen as making a contribution to safety but which were not required to provide a risk reduction greater or equal to a factor of 10 were described by a new term Safety Enhancing. This was, perhaps inevitably, abbreviated as SIL E.

The Risk Graph method of SIL determination was adopted as detailed in Annex D of BS EN 61508-5 and subsequently Annex D of IEC (later BS EN) 61511 when that was published in 2003. The business already had in place tolerability of risk criteria which were displayed graphically on a risk matrix with tolerable, intolerable and tolerable if as low as reasonably practical (TIFALARP) regions (Figure 1). The risk graph was calibrated so as to target reducing frequencies of hazardous event to values that fall in the middle of the TIFALARP region on the matrix. This resulted in a slightly modified form of the graph to that in the standards as shown in Figure 2. The risk graph is used for the initial screening of protective systems and it is backed up with more detailed, quantified fault tree analysis for systems that the risk graph suggested need to be SIL 2 or above or where the hazardous event has particularly serious consequences.

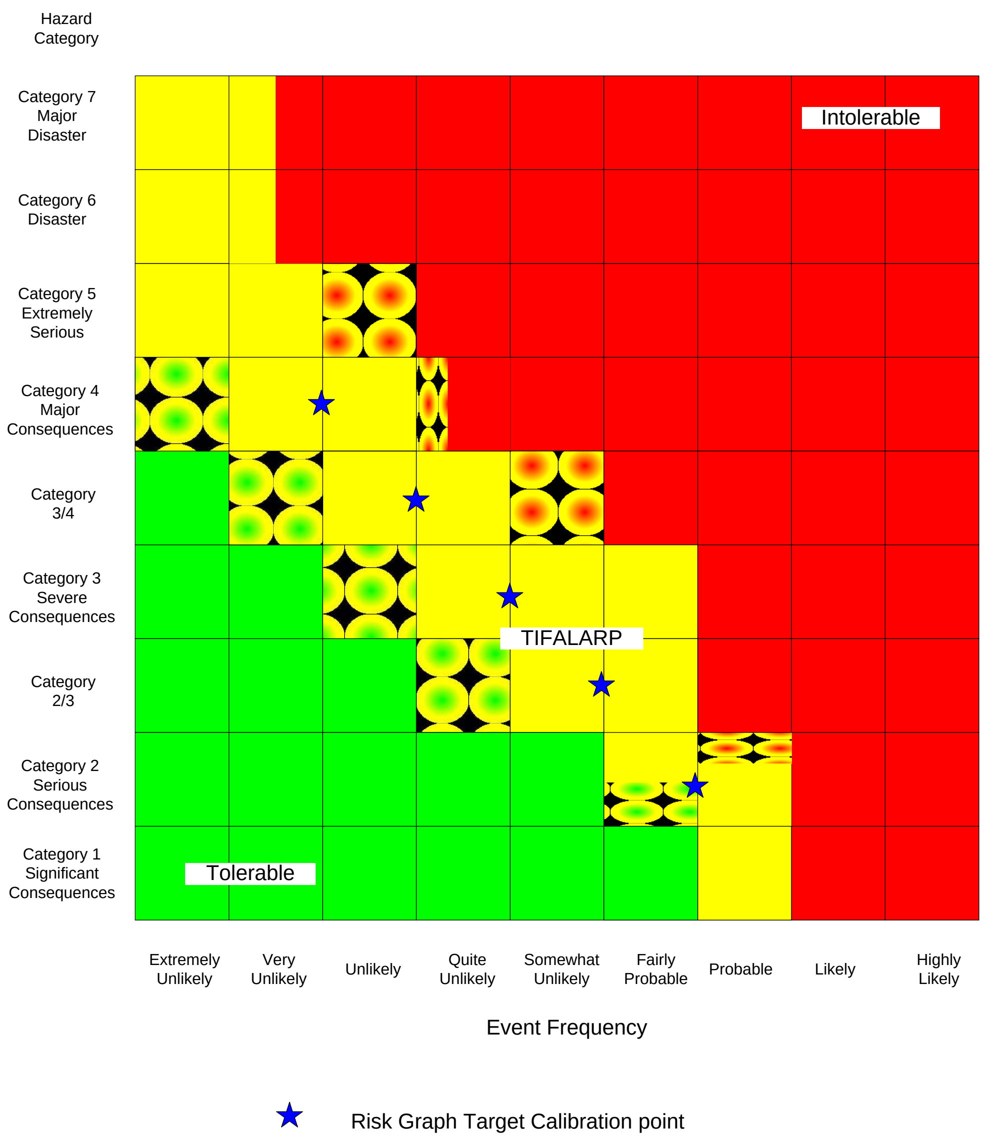
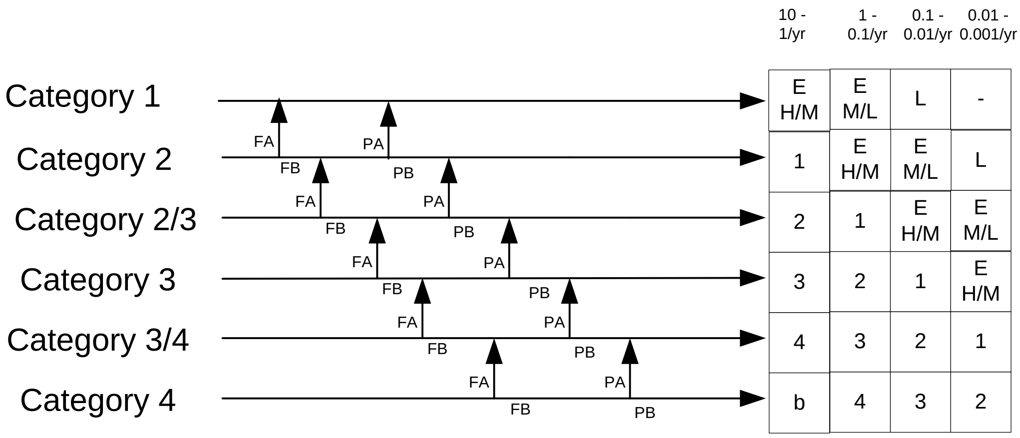


Figure 1. Tolerability of Risk Matrix



F = Exposure time parameter
(FA=<10%, FB = >10%)
P = Possibility of failing to avoid hazard parameter
(PA=>90%, PB=<90%)
W = Demand rate on protective system

2, 3, 4 = Critical System - SIL 2, 3 or 4 Trip (to be confirmed by hazard analysis)
1 = Critical System - SIL 1 Trip or Critical Alarm
E - Safety Enhancing system - DCS Interlock or alarm
H/M = DCS High or Medium priority alarm (depending of time available to respond)
M/L = DCS Medium or Low priority alarm (depending of time available to respond)
L = Low Priority Alarm
- = No requirements for protective system
b = Redesign of process likely to be required

Figure 2. Risk Graph for SIL Determination – Original Version

As can be seen from Fig 2, the Categorisation SIL E was used for the two orders of magnitude of risk reduction less than SIL 1. Subsequently, recognising that many SIL E systems would actually be alarms rather than trips and these alarms would need to be prioritised in line with the EEMUA 191 guidelines, the two SIL E boxes in the risk graph were labelled as SIL E H/M and SIL E M/L to represent high, medium and low priority alarms. Spreading the SIL E classification over two orders of magnitude of risk reduction like this was seen as being a conservative approach compared to that in the standards which labelled the first order of magnitude of risk reduction less than SIL 1 as 'a' – 'No Special Safety Requirements' and the second as '-' – 'No safety requirements'.

Using this approach, protective systems across the site were classified during a retrospective review of compliance with the 61511 standard. The split between the number of systems assigned the different classifications is shown in Table 1. It should be stressed that, as the exercise was primarily aimed at identifying SIL 1 and above systems, it is unlikely that all the SIL E systems have been identified.

SIL	Number	%
SIL 2	140	3%
SIL 1	1120	25%
SIL E	3200	72%
Total	4460	

Table 1 – Split in the integrity of instrument protective systems across the site

The SIL 1 and 2 systems are operated and maintained in line with the requirements of the BS EN 61511 standard, so far as was reasonably practical given that most of the systems had been designed and installed before the standard was published. These systems are independent from the basic process control system and are subject to formally documented and controlled periodic proof testing. The SIL E systems are typically implemented within the basic process control system and proof testing carried out at the discretion of the local plant control/electrical engineer.

Management of low integrity safety functions

The site was reasonably comfortable with the approach that had been taken until it received the following action relating to SIL E Systems – Policies and Procedures, arising from a specialist HSE inspectors visit under the COMAH regulations:

> Review the approach to periodic inspection, maintenance and proof testing of instrumented safety functions that have been assessed not to be subject to the more rigorous requirements of BS EN 61511. The outcome of the review should include the following:
>
> - Policies/procedures to enable a consistent approach to be adopted across installations.
> - A summary of where the Runcorn site stands in terms of compliance with the procedures developed. This should include an indication of how many such functions there are, subdivided by installation, automatic function or alarm, SIL E H/M or SIL E M/L.
> - A time bound proposal for full implementation of the policies/procedures developed.

At the same time HSE drew attention to what was, at that time, draft guidance they had developed 'Management of low integrity safety functions and safety functions of undefined integrity in the onshore chemical and specialist industries'. At this stage, this draft guidance argued that, although BS EN 61511 explicitly states it does not apply to systems with a level of performance below SIL 1, the more general BS EN 61508 should be applied to many systems that have a safety risk reduction requirement below a factor of ten (this argument was subsequently dropped for the final published version of the guidance).

The prospect of having to apply BS EN 61508 to all the identified SIL E systems caused real concern, not just because of the high level of work and cost involved but also because it would dilute the importance of, and the level of attention that could be paid to, the SIL 1 and 2 systems.

The first step in developing the policies and procedures requested by HSE was to go back and look at the definition that had been used to generate the list of SIL E systems in the first place.

Whilst the written definition of a SIL E system as:

> *A Safety Enhancing Instrumented System is one that makes a contribution towards the reduction of an identified risk to safety, health or the environment or serious financial loss but where that contribution to risk reduction is not required to be greater than a factor of 10 in order for the risk to reach an acceptable level.*

remained appropriate, a review of the calibration of the risk graph showed that the systems that had been classified as SIL E were, in practice, further reducing the risk of a hazardous event that would already be considered tolerable if as low as reasonably practical (TIFALARP) without the SIL E system. Whether such systems are really necessary than comes down to a cost benefit argument i.e. does the benefit (in terms of risk reduction) from the system justify the cost of installing and maintaining the system. It was concluded that, whilst the SIL E H/M systems could be justified on this basis, the SIL E M/L systems could not. It was therefore decided that whilst the M/L systems would be retained for operationally purposes they would no longer be considered to be safety related and the SIL E designation would be dropped. The risk graph was therefore updated to more closely reflect that in the standards as shown in Fig 3.

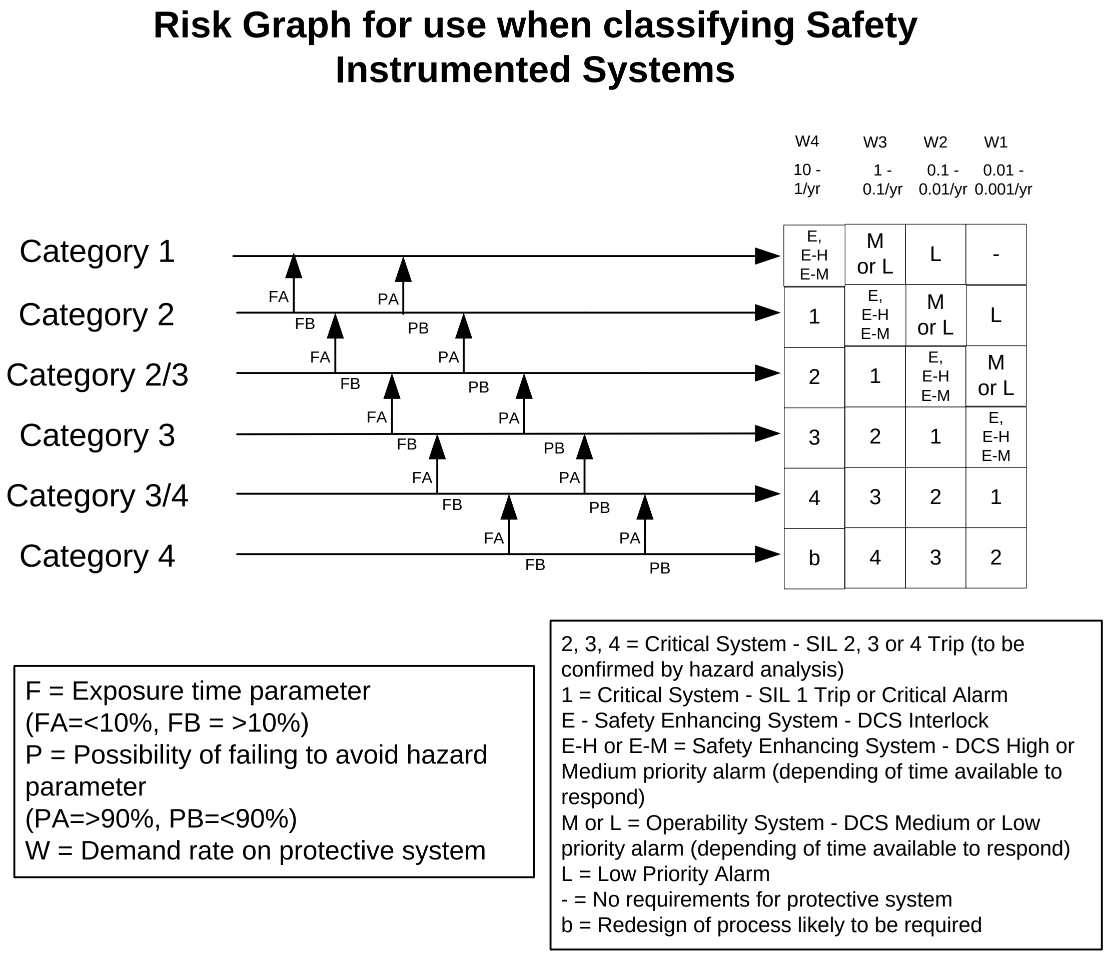


Figure 3. Risk Graph for SIL Determination – Updated Version

Plotting the results from this risk graph back on the tolerability of risk matrix shows that if a risk is in the TIFALARP region but above the target point then a SIL E system will be required to reduce its frequency but if the risk is already below the target point a M/L operational system will suffice (See Figure 4).

The justification for dropping SIL E from the M/L categorisation can be further illustrated by considering the average probability of failure on demand (PFD_{avg}) requirements for the various SIL ratings as you go from SIL 2 (0.001 - 0.01) to SIL 1 (0.01 - 0.1) to SIL E H/M (0.1 to 1). Following this progression suggests SIL E M/L should have a probability of failure on demand of between 1 and 10 which is clearly makes no sense.

Restricting the SIL E categorization to those systems previously identified as SIL E H/M reduced the number of SIL E systems from some 3200 to 1900. Whilst this was a significant reduction it still left a large number of systems that need to be managed and more thought was given to how such systems should be implemented and, in particular, to their proof testing.

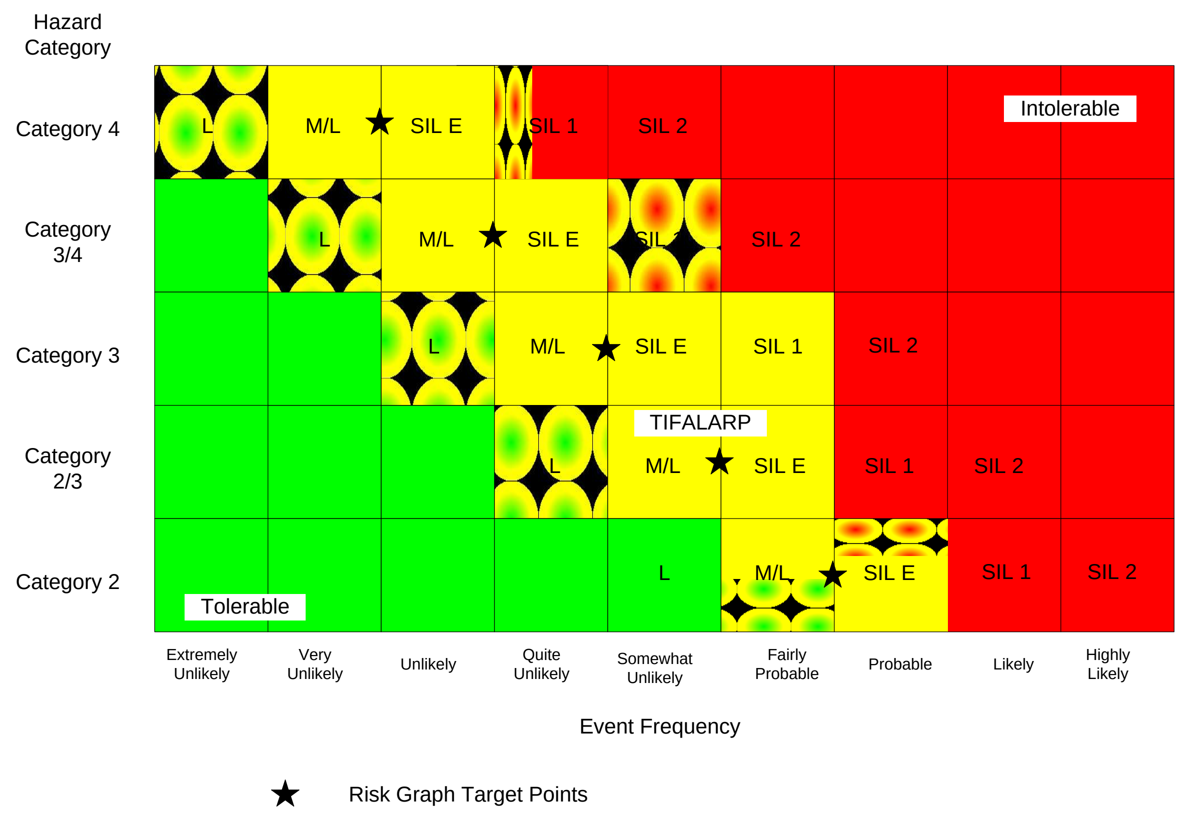


Figure 4. Tolerability of Risk Matrix showing SIS integrity requirements

Design and Implementation

As SIL E systems are not required to make an order of magnitude risk reduction they fall outside the requirements of the BS EN 61511 standard and so are designed to normal good engineering practises along with the rest of the plant control and instrumentation systems. SIL E alarms and automated functions (usually referred to as interlocks rather than trips) are generally implemented within the plant basic control system although in some cases where there are common mode issues they may be implemented independently from the control system (e.g. within the safety instrumented system used for SIL 1 and above systems).

The implementation of SIL E systems within the control system is justified on the basis that such systems are, in practise, highly reliable. BS EN 61511 accepts that the basic process control system acts as one of the multiple layers of protection found in a typical process plant and allows a risk reduction factor of up to 10 to be claimed for its use even if it has not been designed to the requirements of that standard.

In practise, SIL E systems tend to be implemented with the same type of sensor and final element hardware as is used for the SIL 1 and above systems. As overall system failure rates tend to be dominated by these field mounted elements rather than the logic solver it is likely that SIL 1 and SIL E systems will experience the same rate of random hardware failure. With less rigorous design processes being applied to SIL E systems than SIL 1 and above systems the systematic failure rate is likely to be slightly higher.

Reliability calculations are not generally carried out for these systems (by definition, any system will have a PFD_{avg} that is less than or equal to 1 so calculating the PFD_{avg} of a SIL E system with a required PFD_{avg} of between 0.1 and 1 is a fairly pointless exercise).

Proof Testing

Requirement for Proof Testing

There is a clear requirement within in BS EN 61511-1 to carry out routine proof testing of SIL 1 and above systems in order to reveal otherwise unrevealed failures to danger. The required frequency of testing can be determined by calculation from the equipment failure rates and the required SIL.

The situation with SIL E systems is less clear cut. SIL E systems are generally installed as reasonably practical risk reduction measures for risks that are not intolerable. The decision of whether a risk has been reduced ALARP is down to a cost benefit argument i.e. are the costs incurred in further reducing the risk disproportionate compared to the benefits gained. Hence the decision on whether or not to test a SIL E system can be taken on cost benefit grounds i.e. is the cost of carrying out the testing disproportionate to the reduction in risk that it provides.

The consequence of failing to test a protective system is that, eventually, the system will fail in an unrevealed manor and when a demand is next placed upon that system the hazardous event that the system is protecting against will occur. In many cases, this results in a demand on another layer of protection. Testing a safety instrumented system will reduce the average probability that the system is in a failed state when a demand is placed on it (PFDavg) and hence will reduce the hazardous event rate. Detailed consideration of the benefit from this reduction in hazardous event rate compared with the cost of carrying out the test, using the methodology and cost of injury data from the HSE 'Cost Benefit Analysis Checklist', draws the conclusion (summarised in table 2) that it is beneficial to test SIL E systems protecting against Category 2/3 or higher consequence hazards but that it is not cost beneficial to test SIL E systems protecting against the lower consequence category 1 or 2 hazards or to test operational instrumented protective systems. (A Category 2 hazard is taken to be one resulting in an injury leading to more than three days off work or the low probability of a major injury).

Hazard Category	SIL 1	SIL E	M/L
Category 1	N/A	No Test	No Test
Category 2	Test	No Test	No Test
Category 2/3	Test	Test	No Test
Category 3	Test	Test	No Test
Category 3/4	Test	Test	No Test
Category 4	Test	Test	No Test

Table 2 - Conclusions on the benefit of testing instrumented systems protecting against various categories of hazard.

Test Frequency

The required frequency of testing of SIL 1 and above systems is defined by calculation in order to achieve the required PFD_{avg}. Typically the required PFD_{avg} can be achieved with annual or maybe even 2 yearly testing. SIL E systems do not have a defined PFD_{avg} requirement but since they are not required to be as reliable as SIL 1 systems and given that the hardware of a SIL E system is likely to have a similar failure rate as that of a SIL 1 system it is reasonable to assume that they can be tested less often. Allowing for other factors that may reduce the integrity of a SIL E system it is assumed that, where testing is necessary, it can be carried out at around half the frequency of a SIL 1 system i.e. typically once every 2 to 4 years.

High Demand Rate Systems

It is not generally necessary to test SIL E systems that have a high demand rate as failures to danger are far more likely to be revealed by the demand than by a test and if this were not acceptable the system would have been given a higher SIL rating. Guidance given in section 3.6 of the second edition of EEMUA 191 – Alarm Systems: a Guide to Design, Management and Procurement, states that safety related (i.e. SIL 1) alarms should be tested at a frequency to achieve the required PFD. It goes on to suggest that testing of other high priority alarms may be required where there is a financial or environmental justification but that testing is unlikely to be necessary if the correct functioning of the alarm is regularly demonstrated in normal operation. The first edition of the guide had suggested a demand rate of greater than 2/yr should be the cut off point for not testing alarms. It has therefore been accepted that SIL E systems with an observed demand rate of greater than twice a year need not be subject to formal proof testing.

Credit for demands

For simple systems (alarms or single input, single output trips or interlocks) it is possible to take credit for a recent demand on the system. If plant records indicate that a system has operated successfully in say the last 12 months then credit can be taken for this operation rather than needing to carry out the test. To do this there needs to be evidence that the whole system worked i.e. for an interlock there needs to be evidence that the output operated e.g. valve shown closed by a limit switch, pump shown stopped or flow dropping to zero. Where the measurement is based on an analogue variable (e.g. pressure or temperature as opposed to something like a tuning fork level switch) there should be some independent evidence (e.g. separate measurement used for control) to confirm that the system activated at the correct setting.

Test Methods

The PFDavg of a system depends not only on the frequency of the proof test but also on the quality of the test i.e. on the proportion of otherwise unrevealed failures to danger that are revealed by the proof test. Given that the same sort of hardware, with the same sort of failure rate is being used for both SIL 1 and SIL E systems, not only might it be appropriate to test SIL E systems less often than SIL 1 systems it might also be appropriate to test them less thoroughly either in terms of the test method used or the formality with which the test is carried out.

The ideal proof test will fully test the whole system from the process initiation of the input to the process effect of the output (a full end-to-end test). Whilst for some forms of instrumentation, such as pressure transmitters, full wet testing is relatively easy to achieve, for others, such as in-line flow meters and level measuring devices, it can be quite difficult and hence the potential to make use of in-built testing functions for testing SIL E systems becomes attractive. Such in-built test functions will only reveal a proportion of otherwise unrevealed failures and so their use can only be regarded as a partial test. It has long been accepted (see for example HSE document 'Proof Testing of Safety Instrumented Systems in the Onshore Chemical / Specialist Industry' - SPC/Technical/General/48) that a regime that is a mixture of partial tests (e.g. when the plant is running) and full tests (e.g. at plant overhauls) is potentially acceptable even for SIL 1 and above systems provided that the overall PFDavg target is still met. Whilst partial testing is perhaps most often used with regard to final elements (e.g. trip valves) where it is not possible to fully test the element whilst the plant is running, it can equally be applied to sensing elements or other parts of the loop.

The partial test, which will identify some, but not all, of the otherwise unrevealed failures to danger of the system, is carried out at a higher frequency than a full test which will reveal all the otherwise unrevealed failures to danger of the system. The proportion of the failures revealed by the partial test is sometimes referred to as the coverage of the test. This should not be confused with the term diagnostic coverage which is usually used to refer to the proportion of failures to danger that are revealed during normal operation of the system (e.g. by diagnostic software built into a sensor or logic solver).

Calculation of PFD_{avg} for Systems with Partial Testing

If the normal proof test period is T_1 and this only detects a proportion of the potential faults P and all faults are detected by a separate test carried out at test period T_2 (or instrument is replaced after this time) the average probability of failure on demand is given by:

$$PFD_{avg} = \tfrac{1}{2}\,\lambda_{du}\,(P.T_1 + (1-P).T_2) \qquad (1)$$

where λ_{du} is the undetected fail danger rate.

NB this is the normally used simplified equation that only strictly applies when

$\lambda_{du}.T << 1$ and $DT << 1$ (where D is the demand rate). It also assumes that the contribution due to the time to repair a revealed fault is small.

For SIL E systems, carrying out partial tests using in-built test facilities every 2 years with full tests carried out at much longer intervals such as 10 or 20 years can be acceptable. With older systems it may be more cost effective to replace the equipment than to fully test it. In the extreme this may mean that SIL E systems are only fully tested once in their lifetime i.e. at initial installation.

Example One – Tuning Fork Level Switch

Take, for example, a tuning fork level switch. As is often the case with modern instruments with a high level of in built diagnostics, a certain series of tuning forks are stated by the vendor to be suitable for use as a single device in a SIL 2 application. The device can be used as a direct input to a logic solver or can use a signal conditioning unit with a test button facility that enables a partial test of the system to be carried out but, unfortunately, adds additional failure modes to the system. The following data is provided by the vendor:

Level sensor - Type A, Safe Failure Fraction (SFF) 91%, $\lambda_{du} = 2.2\text{x}10^{-4}$/yr

Signal conditioning unit $\lambda_{du} = 9.4\text{x}10^{-4}$/yr, test button coverage (of sensor) 52% (of signal conditioning unit) 100%

Wet test coverage 100%

If the same device is used in a SIL E system one might propose that it is only ever tested using the test button and, apart from an initial commissioning test, is never subjected to a full wet test but is replaced at the end of its working life (i.e. before it reaches the end of the flat section of the bath tub curve and enters the wear out phase) after say 20 years. In this case then the partial test interval is 2 years say and the interval for the full test essentially becomes 20 years.

PFD_{avg} (sensor) = $0.5 \text{ x } 2.2\text{x}10^{-4} \text{ x } (0.52 \text{ x } 2 + 0.48 \text{ x } 20) = 1.2\text{x}10^{-3}$

PFD_{avg} (conditioning unit) = $0.5 \text{ x } 9.4 \text{ x}10^{-4} \text{ x } 2 = 9.4\text{x}10^{-4}$

Hence overall PFD_{avg} for sensor circuit = $1.2\text{x}10^{-3} + 9.4\text{x}10^{-4} = 0.002$

This is sufficiently small compared to the requirements of a SIL E system ($PFD_{avg} > 0.1$) that it can be seen that, even if the manufacture's failure rate figures were unrealistically optimistic for the actual service conditions, it is still going to be acceptable to rely on the partial test offered by the test button facility throughout the life of the installation.

NB As indicated above, the simplified equations only strictly apply to conditions where $\lambda_{du}.T << 1$ and $DT << 1$. In this case, with an effective test interval of 20 years, whilst $\lambda_{du}.T$ at $2.2x10^{-4}$ x 20 = $4.4x10^{-3}$ is still much less than 1 it is possible that DT will not be much less than 1. Detailed calculations of PFDavg for systems where DT is not much less than 1 are outside the scope of this paper, suffice is to say that, in these circumstances, the simplified approximation is pessimistic and as the test interval increases the actual PFD_{avg} is lower than that predicted, so the conclusions on testing interval remain valid.

Example Two – Vortex Flowmeter

For a second example consider a vortex flow meter. A certain meter is stated by the vendor to be suitable for use as a single device in a SIL 1 application. The following data is provided by the vendor:

Type B, SFF 85.8%, λ_{du} = 126 FIT = $1.1x10^{-3}$/yr

The vendor also states that a partial test using the digital communications ability of the sensor to simulate the flow has a coverage of 82%. With these types of in-line meter it is difficult to carry out a full wet test unless there happen to be duplicate meters installed in the same line. In practise 100% coverage can probably only be achieved by carrying out a full calibration on a meter proving rig.

If the system is tested every 2 years using the simulated flow but, apart for an initial commissioning test, is never subjected to a full wet test but is replaced at the end of its working life (i.e. before it reaches the end of the flat section of the bath tub curve and enters the wear out phase) after say 20 years, the interval for the full test essentially becomes 20 years.

PFD_{avg} (sensor) = 0.5 x $1.1x10^{-3}$ x (0.82 x 2 + 0.18 x 20) = 0.003

Once again, this is sufficiently small compared to the requirements of a SIL E system (PFD_{avg} >0.1) that it can be seen that, even if the manufacture's failure rate figures were unrealistically optimistic for the actual service conditions, it is still going to be acceptable to rely on the partial test offered by the simulation of the flow throughout the life of the installation. The exception to this assumption would be if the meter is used on a particularly arduous duty where the failure rate could be expected to be considerably higher than predicted by the vendor.

Conclusions

Low integrity safety functions, sometimes referred to as 'SIL 0', 'SIL a' or, as in this paper, as 'SIL E' systems, whilst falling outside the requirements of the BS EN 61508 and 61511 standards do still need to be properly managed. Such systems typically serve to reduce a risk that is already not intolerable to a level that can be considered to be as low as reasonably practical (ALARP). Care should be taken to draw a distinction between such systems and other systems that may be present for operability reasons but which are not required from a risk reduction point of view. This will allow the appropriate level of attention to be given to the low integrity safety functions without this becoming an excessive burden. This level of attention falls somewhere between that required to be given to SIL 1 systems and that given to a basic control function.

Low integrity safety functions will need to be proof tested unless they are protecting against particularly low consequence hazard or are subject to a high demand rate. The frequency of testing and thoroughness of testing may be less than that applied to SIL 1 systems. It is likely to be appropriate to make use of generic test methods rather than have detailed individually written step-by-step methods for each system. It is also likely to be appropriate to use in-built test facilities available with modern instrumentation. Whilst these facilities may only provide partial coverage their use may be all that is required for the lifetime of the instrument. In other cases it might be necessary to back-up the partial test with a less frequent more thorough test. It may be possible to take credit for a recent demand on the system, where records show it operated correctly, in lieu of carrying out a formal proof test.

References

BS EN 61508 – Functional Safety of Electrical/Electronic/Programmable Electronic Systems

BS EN 61511 – Functional Safety: Safety Instrumented Systems for the Process Industry Sector

Management of instrumented systems providing safety functions of low/undefined safety integrity – SPC/Technical/General/51 – HSE

http://www.hse.gov.uk/foi/internalops/hid_circs/technical_general/spc-tech-gen-51.htm

Alarm Systems – A guide to design management and procurement – EEMUA Publication No. 191 First Edition 1999, Second edition 2007

'Cost Benefit Analysis Checklist' – HSE

http://www.hse.gov.uk/risk/theory/alarpcheck.htm

'Proof Testing of Safety Instrumented Systems in the Onshore Chemical / Specialist Industry' - SPC/Technical/General/48 – HSE

http://www.hse.gov.uk/foi/internalops/hid_circs/technical_general/spc_tech_gen_48.htm