

Session Five: Who's Afraid of IEC 61508/61511?

Harvey Dearden

Consulting Engineer: Time Domain Solutions

Abstract

This paper (originally published in the November 2005 issue of the journal of the Institute of Measurement & Control) highlights some key issues for owner/operators that may help maintain the right perspective on the requirements as they apply to the limited circumstances that are typical of most process operations.

Introduction

It has to be said that the 61508 standard is something of a monster. That is not to say that we should turn tail and run however. But how are we to respond? The key is to keep the thing in perspective. In detailing a completely comprehensive, rigorous approach for the lifecycle requirements for protection systems from the simplest through to the most complex, the standard does become somewhat impenetrable. Things do improve with 61511, but it still could not be described as an easy read. The intention here is to highlight some key issues for owner/operators that may help you keep the right perspective on the requirements as they apply to the limited circumstances that are more typical of most process operations.

The philosophy underpinning the standard is that the protection provision should be designed, and maintained in a manner commensurate with the risk. Life was simpler when there was a straightforward prescriptive rulebook to follow, but this approach can itself produce distorted provisions. The standards provide a systematic risk based approach. However, if historically you have been adopting good practice in the engineering of your protection systems, there should be little adrift with your existing physical installations. Where there may be weaknesses when measured against the new standard, is in the traceability of the design, the administrative arrangements for control of change and in the arrangements for proof testing and recording of reliability data.

Regulatory Position

A couple of points to be clear on straight away: The standard is not mandatory and is not retrospective. So you cannot be prosecuted for not being compliant with the standard. It is however now promoted by the HSE as good practice and you can of course always be prosecuted if you are found to be negligent in your approach to maintaining safety. There is, I would suggest, a world of difference between non-compliance in terms of strict observance of the standard and true negligence (See Reference 1). No need to rip it all out and start again. A considered and systematic approach is required.

Responsible Disciplines

One of the difficulties is that the standards, quite properly, raise issues that cross several disciplines. Do not imagine you can simply leave it to the instrument engineer to sort it out; he may not have the insights into process/risk reduction issues. The process hazard/safety engineer may not have the necessary insights into equipment architecture possibilities and system design. It would be very easy for someone without the necessary insight into other disciplines to inadvertently specify measures that are completely over the top or completely inadequate. I don't see a simple answer to this, but at least you should be alert to the possibility.

Qualitative versus Quantitative Approach

Much appears to be made of the risk graph as a qualitative approach for establishing SILs, but the appealing simplicity of this approach can lead to significant distortions in the allocation of SILs. The vagueness of the descriptions and a natural tendency towards conservatism may well be compounded at different points to produce unrealistic SIL allocations. An alternative is to use a quantitative approach to calculate explicitly the required probability of failure, which then determines the SIL. (LOPA – Layers of Protection Analysis). A simplified LOPA is hardly more onerous (depending on the degree of rigour adopted), but has the virtue of producing a tailored 'probability of failure' requirement and corresponding SIL allocation.

Most applications within the process industries are likely to be SIL 1 or SIL 2. If you find you are getting higher SILs than this, the likelihood is that you are doing it wrong. (Either the system analysis or the process design itself). Higher level SILs will be required only where the hazard carries severe consequences, the demand frequency is high and there are no other risk reduction measures.

Comparable assessments may be made in relation to hazards that may give rise to non-fatal injuries, environmental damage or plant damage/production/financial loss.

Be wary of setting unreasonably low targets for tolerable risk; you are likely to drive yourself into unwarranted difficulties with the engineering. Having said that however, remember that there is an overriding requirement for risk to be ALARP (As Low As Reasonably Practicable). If some additional risk reduction is practicable (perhaps by design provisions unrelated to instrumented safety systems), then there is a requirement to effect the reduction.

Be wary of making much in the way of claims of risk reduction by operator intervention. An assumed failure rate for operator intervention of 0.1fails/demand is typical of what might be reasonable. With the very best circumstances with near perfect ergonomics, the most that could reasonably be claimed is 0.01fail/demand. Operator intervention may also be delayed; you need to consider the time available for effective intervention.

Redundancy and Diversity

Under 61511 requirements, for SIL 1 & 2 applications it is acceptable to use 'simplex' systems i.e., systems with a single channel and therefore no redundancy, provided that the sensors/final elements/non-programmable logic solvers (e.g., relays) are 'proven in use'.

Where not proven in use, provided the equipment has a dominant failure mode that is to a safe state, it is still acceptable to use a single channel for a SIL1 application.

Beyond these circumstances (higher SILs or where there is less confidence in the failure characteristics), it is necessary to have a multiple channels. These may be redundant (ie two identical channels) or diverse (two non-identical channels).

Diversity could include using two different sensors from two different manufacturers or using two different measurement techniques (ie flow measurement by vortex flowmeter and coriolis flowmeter). The latter would protect against common-mode failures such as maintenance errors, plugging, environmental conditions, etc.

'Proven in use' means that there is evidence of suitability based on:

- adequate identification and specification of equipment
- confidence in the manufacturer's QA and management systems
- demonstration of performance (ie testing/independent testing)
- volume of operating experience in similar applications

In respect of programmable systems e.g. PLC, a single channel may be used provided that the safe failure fraction of the solver is >60% for SIL1, >90% for SIL2. [Safe Failure Fraction is the number of revealed hazardous failures + safe failures, as a proportion of all failures, including unrevealed hazardous failures.]

Frankly, unless you want to invoke some serious engineering muscle, I would hesitate to use programmable systems (including smart transmitters and actuators) for anything higher than SIL2. It may be appropriate, but be clear about what you are getting into.

Certification

Although it is possible to buy equipment that has been certified as being suitable for use in a given SIL, there is no absolute requirement to use certified equipment. Certification is one way to acquire confidence in the fitness for purpose of equipment but it is not the only way. If certified equipment is used on an inappropriate duty, the certification will be meaningless. A considered review of the nature of the equipment, its specification, its history, the proposed duty, whether it has been proven in use etc. may establish that it is fit for purpose.

Reliability Calculations

Much is made of reliability calculations which can become extremely complex as greater degrees of refinement (e.g. mean time to repair, detected versus undetected failures to danger) are used in the mathematical modelling. (Although very often this is taken care of by calculation software or look up tables). You should keep in mind however that in the face of the uncertainties in failure rates, tolerable risk and demand frequency, the refinements may be of questionable value.

For most simplex systems at SIL 1 & 2, with relatively low demand frequencies, the basic formula for average probability of failure on demand ($\frac{1}{2} \times$ dangerous failure rate \times test interval) is perfectly adequate. Very often there will be parallel branches within an overall simplex system (e.g., a single transmitter/trip amp 'cause' might have the 'effect' of shutting two valves, either of which would provide protection. The overall system reliability will tend to be dominated by the non-redundant provisions in the system. Any combination of parallel components (even when taking common mode failures into

account) will often be so relatively reliable that they effectively become irrelevant in the calculation of overall system reliability.

The influence of common mode failures certainly does significantly impact on truly redundant systems (duplex, triplex), and an attempt to calculate overall reliability without account of common mode effects will lead to gross errors. Two identical 10^{-2} fail/demand systems do not give 10^{-4} fail/demand. The engineering of systems to the 10^{-4} (SIL3/4) level becomes very onerous; if you really need this kind of performance you will need expert help.

Remember that the reliability of your system is likely to be dominated by the sensors and actuators/valves; there is unlikely to be much point in additional expenditure solely to improve the reliability of the logic solving equipment.

Separation of Control and Protection

Do separate protection systems from control systems. Although the implementation of trips within a control system is not prohibited, it makes proper management of the protection system life cycle that much more difficult. Remember that one 'cause' may be the failure of the control system itself. Only mix the two systems if careful consideration of the particular circumstances satisfies you that this is appropriate.

Be wary of repeating the trip matrix functionality in your DCS. The relative unreliability of the DCS means that the overall system reliability (with typical single sensor or final element configuration) will not increase significantly, and you will create difficulty in managing the system and its documentation and in proof testing. When testing a given 'cause' you would need to establish which system initiated the 'effects'. If the systems operate in parallel, failure of one system might be masked by the operation of the other.

Equipment Failure Rates

In assessing failure rates it is often useful to consider the population that would be required for a failure every year. For example a device with an MTBF of 50 years means that if there were 50 such devices on site, you should expect a failure every year on average. This more intuitive expression allows a reality check with experience on site. (It is much harder to see the significance of a failure rate of $2.0 \text{ E-}02 \text{ yr}^{-1}$, which is the same thing.) I did see a figure of $1.1\text{E}+00 \text{ yr}^{-1}$ used for flow sensors; this means each sensor will fail more than once every year! The particular duty and environment on site may lead to much higher failure rates than may be quoted in nominal figures from vendors.

Beware of manufacturer quoted failure rates; occasionally instruments have a quoted MTBF of as much as 1200 years! Figures such as these have often been derived from entirely theoretical studies (FMEDAs) based on lab environments and benign measurement duties. You need to consider the context in which your equipment is deployed.

Proof Testing

If you find that proof test interval required to achieve the required probability of failure on demand is less than 3 months, you should consider whether further risk reduction

measures are appropriate. I would be concerned about a system with a requirement to test more frequently than this.

When developing test procedures, the approach should be to disturb the installation as little as is consistent with the aims of testing. There is otherwise a real danger that you may do more harm than good. I have seen tests that call for umpteen jumpers to be installed on a shutdown plant to make the system healthy so that a given trip could be exercised!

Be wary of modifying trip points to force a trip action; failure to properly reinstate the trip setting may compromise the protection.

Be wary of falling into the trap of, for example, testing a high level trip by raising the level. If the trip fails you may cause the very incident you intended to protect against. This technique may be acceptable provided there are adequate additional precautions. Clearly being able to produce the actual hazard under controlled conditions is the best way of testing the entire safety system from 'end-to-end'. Everything else is simulation in one form or another.

On test documentation be sure to record 'passed first time' as distinct from 'failed but now fixed' to capture those occasions where the test is passed after some corrective action. The failures, however simple they may be to fix, need to be reported so that design flaws may be corrected and actual failure rates established.

Project Management

Understandably, the requirements for project management become increasingly onerous as SILs increase e.g., with increasing independence of parties responsible for inspection/validation from those responsible for design. However, those operations that currently use a disciplined, good QA practice, approach to project management (and operation/maintenance) will probably find that their existing procedures and in-house resources are essentially adequate for SIL 1&2 applications. It may be appropriate to prepare a generic project quality plan that shows the activities and responsibilities related to implementation of IEC 61508 projects. Similarly it may be appropriate to prepare a generic document detailing design and testing requirements for nominated standard systems with standard architecture and equipment types.

Conclusion

It is easy with these standards to spend a great deal of time and money to no good purpose. A relatively straightforward approach may be perfectly viable for many process operations. Many operations may find conventional spreadsheet tools are perfectly adequate for their purposes. (A spreadsheet tool for system reliability assessment is available from the author). The fundamental requirement is to bring a considered, systematic approach to the design, operation and maintenance of safety instrumented systems. Be wary of 'enthusiasts' that may well tend to over egg the pudding.

It is easy, in all good faith, to pursue a wrong-headed approach that does not recognise the operational context and ultimate aim of the mission. It is vitally important that you occasionally step back and consider whether the mechanics of the assessment process and the numbers 'game' are driving you into unduly conservative and complex provisions or leading you to overlook fundamental concerns that might cut right across your

evaluation. Niceties of precisely how you “dot your i’s and cross your t’s” are less of a concern.

Profile

Harvey T. Dearden used to be an Engineering Manager working at the sharp (making things) end of the chemical industry. He now works as a consultant in matters of process measurement, control and management. He is Chairman of the Manchester & Chester Section of the IM&C. He can be contacted at htdearden@tdsl.org.uk.
[[Reference: Dearden, H.T., Safety Management; Beware the Reality Gap, IEE Management Magazine, Nov/Dec 2003.