IEC 61508 – Is it pain or gain?

Clive Timms,

Director, C&C Technical Support Services Ltd.

Introduction

IEC 61508 (Ref. 1) provides designers and operators with the first generic internationally accepted benchmark standard for determining the Safety Integrity Level (SIL), the design requirements and test intervals for Safety Instrumented Functions (SIF). It covers every aspect of the full lifecycle management requirements for Safety Instrumented Systems (SIS). Before the introduction of IEC 61508, the most widely accepted standard was ANSI/ISA SP84.01 (Ref.2), but it is most likely that ISA SP84-01 will be superseded in 2003 by the publication of IEC 61511 (Ref.3) which is the process sector specific version of IEC 61508.

The IEC 61508 standard provides a lifecycle road map for any SIS, yet is widely regarded as difficult to use and costly to implement. Numerous articles, presentations and training courses have addressed details of the standard but to date there has been little practical application advice available.

This situation is now changing; by utilising experienced practitioners and appropriate software tools users of the standard can assure asset integrity whilst reducing the capital cost of new projects and the maintenance costs for existing facilities.

Misconceptions

Practical interpretation of the standard is often perceived as difficult but with appropriate guidance and training, engineers soon become comfortable with the methodology and the lifecycle concept simply amounts to common sense.

There is often concern that a SIL determination exercise for an existing facility will reveal large numbers of functions with a high requirement and result in costly re-engineering. In reality, this is seldom the case. A SIL assessment will identify the protective functions that really matter and this must surely be an essential objective for any responsible plant operator, but experience has also shown that many existing safety system designs are too complex with scope to delete significant numbers of functions or re-engineer them into non-safety systems.

The opportunities for significant cost savings from the optimisation of maintenance routines are common to both new and existing facilities. Savings from reduced production deferment can also be significant. Finally, if testing and maintenance routines can be calculated and scheduled to fit into planned shut down periods then even greater savings can be achieved and SIL assessment and optimisation tools are available to help with this task.

Problems and Issues

Uptake of IEC 61508 has been relatively slow. This is unfortunate as application of the methodology is not only cost effective but provides demonstrable evidence of industry best practice. In the event of an incident involving an SIS it is of potential concern for client and design house alike if best practice has not been followed and it is to be expected that an increasing number of governmental agencies worldwide will use IEC 61508 as a benchmark.

Published in Measurement & Control, July 2002

Whilst the standard contains some guidance on the field devices, it can be argued that the focus is generally on the hardware and software requirements of logic solvers. The failure rates of field devices usually dominate the Probability of Failure on Demand (PFD) calculation for IPFs and therefore determine the ability of the loop to meet the required SIL. Introduction of industry specific guidance based on IEC 61508 can provide more guidance on this issue. The UKOOA 'Guidelines for Instrument-Based Protective Systems' were first introduced in 1997 to provide IEC 61508 interpretation for the offshore based hydrocarbon processing sector and IEC 61511 will shortly be issued to assist the process sector with practical application.

Reliability data is fundamental to calculating the PFD. Although reliability data is generally readily available from the logic solver suppliers, obtaining reliability data for field devices is often difficult. Larger organisations have historically recorded this data in their maintenance management systems and data collected in this way takes into consideration local issues such as the environment, operating conditions and standards of maintenance. Smaller companies may not have such data which can be a problem when selecting field device architecture and determining test and maintenance frequencies. In the absence of company specific data, there are credible public domain sources that can be used but a conservative approach in the design, testing and maintenance regime should be taken at the outset. This can then be adjusted as experience with the equipment matures and data from the facility is captured.

Several organisations offer IEC 61508 training courses. While some courses are well conceived, many tend to focus on conveying the content of the standard rather than its practical application. When selecting a course, care should be taken to ensure that the tutors have experience of applying the standard and the focus is appropriate for the requirements of the participants.

Having determined a SIL for a function there are many practical hardware design issues to be addressed. Not all protective functions are simple series networks comprising an initiator, logic solver and final element. Many functions are made up of arrangements of series and parallel networks, particularly the final element where combinations of devices may be required to change state. Inter-trips between various levels of logic systems also create difficulties and the functionality can become complex. Calculating the PFD of these complex functions can be difficult. However, with an appropriate methodology to reduce the complexity and suitable software tools to facilitate the calculation, these difficulties can be overcome.

To minimise cost and to have confidence in the application of the standard it is important that an experienced facilitator is used during a SIL assessment and that suitable training is provided for the team.

Effective management of the data for the lifecycle phases of SIL determination, design and maintenance is essential if an adequate audit trail is to be maintained. There will be a large number functions on a typical process facility and paper-based or spreadsheet risk assessment and design exercises have proven to be problematical. Specifically designed software tools can eliminate these problems.

How Software Tools can Optimise the process and Maximise the Opportunities

There have been important developments in IEC 61508 based software tools. Experience with these tools has shown that significant savings can be made in the cost of conducting a SIL determination exercise and reducing the design time.

Opportunities to reduce costs are not just design based. Full lifecycle considerations also require alignment of appropriate maintenance and testing strategies with a design. Interactive software applications are available to remove the manual iterative calculations required to quickly solve the mathematical relationships, thus optimising design, testing and maintenance requirements.

Such tools aid IEC 61508 compliance and realise cost saving opportunities. The software usually works with a relational database that is structured to take the user through the main facets of the lifecycle process. This starts with the SIL determination process that sets the Probability of Failure on Demand (PFD) to be achieved.

Risk graphs may be used for this purpose as experience with undertaking SIL determinations on facilities with a large number of functions has shown them to be expedient and consistent.

Although safety criticality is the focus of a SIL determination exercise, the same technique can be used concurrently to assess the environmental and economic criticality of IPF's. A similar risk graph format may be used and the results are portrayed as SIL equivalents. The safety economic and environmental SIL and SIL equivalent are compared and the highest SIL requirement for that function is selected. If appropriate tools are used, the resulting SIL is automatically identified and the risk graph data and narrative records are stored in the database to provide a complete audit trail of the risk analysis. Many thousands of functions can be maintained and sorted for report production in this type of database.

On completion of the SIL determination exercise the next step is to select components for each function (initiators, logic solvers and final elements) and determine physical architectures to satisfy the SIL criteria. For example, should the initiator be a single device (1 out of 1 voting) or comprise a more complex 2 out of 3 voting arrangement.

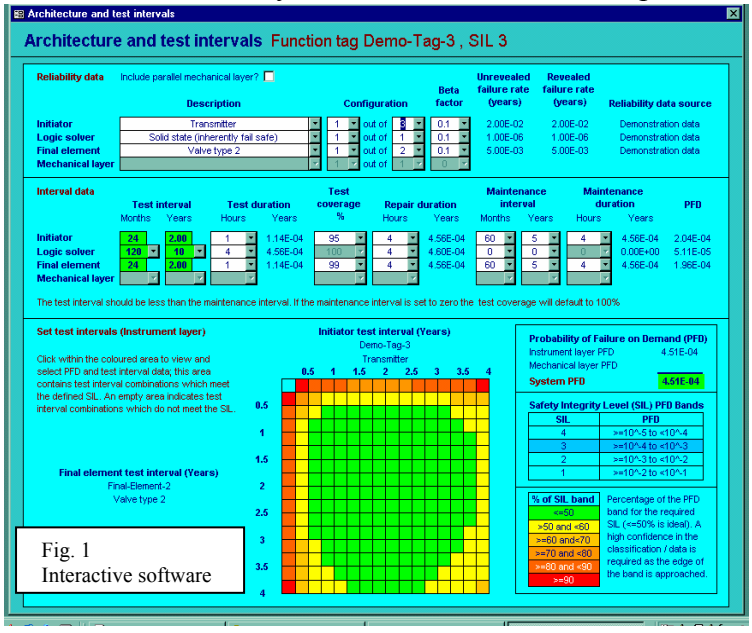

Fig. 1
Interactive software

It should be noted that if the SIL determination has been undertaken for an existing facility the existing architecture would be used for the configuration.

Failure rate data for the selected elements is key to establishing the physical design architecture of the initiators, logic solvers and final elements that can be used to achieve the required PFD. An effective tool will hold a configurable selection of elements of different types and manufacture for initiators, logic solvers and final elements, along with corresponding reliability data. Components can then be selected like building blocks to configure any required protective function. The selection of components, configuration of the architecture and frequency of test and maintenance intervals determine the PFD and hence the SIL that can be achieved. Factors should also be applied to take account of common cause failures for multiple devices and the effectiveness of the test methods in revealing hidden failures. A well-designed tool such as shown in

Figure 1 will allow iterative changes to these variables to quickly establish optimal design, test and maintenance intervals.

IEC 61508 requires the hardware fault tolerance to be checked for system components. The standard provides tabular relationships between the hardware fault tolerance and a calculation of the Safe Failure Fraction, where the safe failure fraction of a subsystem is defined as the ratio of the average rate of safe failures plus detected failures of the subsystem to the total average failure rate of the subsystem. This process assists in defining the requirement for multiple devices and is automatically integrated into some software tools.

It is important to select software tools that have been subjected to independent verification since the user will need assurance of the functionality and consistency of performance.

Optimising Testing and Maintenance Strategies

Project engineers are primarily concerned with the capital spend to ensure that they do not go over budget and often give little consideration to future operating costs. In addition, design houses may not always consider operating costs when they prepare their designs

This lack of ownership for the lifecycle considerations often fails to provide the client with an optimal balance between design and operating costs. This is not only impacts on the man-hours required for testing and maintenance of safety systems, but as these activities are often disruptive to operations they can result in significant costs for deferment or loss of production while they are undertaken.

It is prudent to ensure that designs embrace optimal testing and maintenance with full consideration of the lifecycle implications. Integrated software tools can optimise design, safety and maintenance requirements.

The design, frequency of testing and periodic maintenance interval, the time taken for testing and maintenance/repair all interrelate and have an impact on the PFD calculation. An important point to make is that testing alone is not sufficient, as this may not identify all possible hidden failures. A good analogy is to consider the brakes on a car. They are tested and operated regularly to ensure the safety of the occupants. However, if the braking system is not maintained, it will eventually fail at an unacceptable rate. Instrument based protective functions are no different. For example a blocked transmitter impulse line may not be identified during routine testing and little information is available about the internal condition of a valve and its actuator by simply testing. Just like the braking system, maintenance is required at some stage to bring the instrument protective system back to the 'as new' condition.

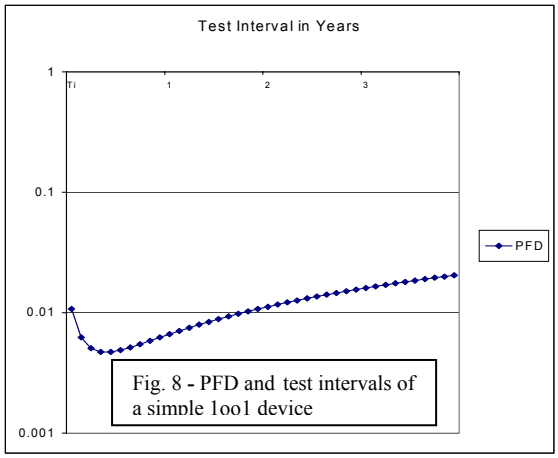

Fig. 8 - PFD and test intervals of a simple 1oo1 device

Testing is normally undertaken at more regular intervals than maintenance since maintenance is often scheduled for periods of plant shutdown, in order to minimise operational disruption. Thus an online test without maintenance is referred to as 'imperfect proof test'; the component is returned to the 'as new' condition at the maintenance interval. With suitable

selection of equipment, architecture configuration and test interval, the maintenance interval can be designed to coincide with planned shutdowns thus avoiding deferred production.

It is important to appreciate that testing too frequently can actually increase the PFD of an IPF in some instances. The time taken to undertake each test and the time taken to carry out the maintenance can mean that the function may not be available to protect against a hazard and the fractional dead time may become significant particularly for single components. The test duration and maintenance duration can have a significant impact on the PFD. This is best demonstrated by the graph shown in Figure 2. The plot shows how the PFD can increase when the test intervals are too frequent. This clearly demonstrates that the testing of a function and maintenance of its subsystems need to be performed at the most optimal intervals, not too long but not too often. Typical software tools can plot the resultant PFD for every combination of test initiator and final element test intervals in graphical form, identifying whether the required SIL (from the SIL determination result) is met.

Harmonisation with a Mechanical Layer

There are often instances where protection against a hazard consists of a combination of an instrumented protective function working with mechanical devices to form parallel protective layers. This is common where over-pressure protection is concerned and a mechanical device such as relief valve forms a protective layer in addition to an instrument based pressure trip function. Total over-pressure protection is provided by the combination of both layers and a SIL can be determined based on the consequences of complete failure of all layers. In this way, the contribution that each layer makes can be determined in the design, and the PFD is a combination of the PFDs for all layers.

Historically, when designing each layer, assumptions have often been made that the other layers will ‘always operate’. This is unrealistic and the design, testing and maintenance of the instrumented and the mechanical layers need to be harmonised so that they provide the required integrity. The main issue is how to maintain the overall system integrity. In many organisations the test and maintenance regimes for the different layers will be independently managed. For example, the mechanical devices may be the responsibility of the mechanical maintenance and the instrumented layer the responsibility of instrument maintenance. Both disciplines will probably be striving to reduce their maintenance costs by seeking to extend test and maintenance intervals without realising that changes to the test and maintenance strategies of their layer may well compromise the overall system integrity.

The various layers need to be considered as a single protective entity. Software tools exist that integrate the design and perform the necessary PFD calculations. Adjustments to any of the parameters, for example test intervals, will automatically be reflected in the PFD that can be achieved for the combined layers.

Conclusions

The application of IEC 61508 can be daunting to the uninitiated. However, the standard provides an opportunity to meet industry best while presenting opportunities for significant cost savings.

The utilisation of software tools is essential if the application of the standard is to be implemented efficiently, with auditable database controls, for full lifecycle management of safety instrumented systems.

References

1. IEC 61508 – Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems. International Electrotechnical Commission.
2. ANSI/ISA S.84.01 – Application of Safety Instrumented Systems for the Process Industries. American National Standards Institute.
3. IEC 61511 – Functional safety: Safety Instrumented Systems for the process industry sector. International Electrotechnical Commission.

Biography:

Clive Timms

Clive has over 38 years experience in the petrochemical industry with offshore and onshore plants experience. He recently retired from Shell UK Exploration and production where he was Head of Automation and Control. He is now a Director of C&C Technical Support Services Ltd, which specialises in the application of the IEC 61508 standard, and was a founder Director of the CASS Scheme Ltd for conformity assessment to IEC 61508. He chaired the UKOOA working group that produced the UKOOA Guidelines for Instrument-based Protective Systems, as an offshore sector interpretation of IEC 61508. He has a BSc. and MPhil in Control Engineering, is a Member of the IEE and currently chairs the Institute of Measurement and Control Safety Panel.

Contact Details:

Clive Timms
C&C Technical Support Services Ltd
Strathayr
Rhu-Na-Haven Road
Aboyne
Aberdeenshire, AB34 5JB, U.K.

Tel: + 44 (0) 1339 886618
Fax: +44 (0) 1339 885637
email: c.timms@ifb.co.uk
Web: http://www.silsupport.com