Instrumented Protective Systems - SIL Classification and Lifecycle Integrity Management to comply with BS EN 61508 / 61511

Jane Capewell and Lyn Fernie, AK EHS & Risk

Synopsis

IEC 61508 was adopted in full as a British Standard in March 2000, yet many companies are only just getting to grips with the application of the standard. Difficulties with SIL (Safety Integrity Level) classification can lead to instrumented protective systems being over or under specified, use of some of the common qualitative techniques such as risk graphs and layers of protection analysis can lead to pessimism or optimism being built into the risk assessment. The assessment of existing instrumented protective system integrity has also proven to be a daunting challenge due to the large volume of data manipulation required. Much of this data resides in business systems such as SAP and Maximo and needs to be extracted prior to input into standalone trip management software packages. The presenter will outline a SAP based solution aimed at addressing the data handling requirements and allowing the operator to maximise the existing system rather than creating islands of information by installing another "bolt on" system. This solution forms the basis for ongoing trip and alarm management throughout the lifecycle of a system.

Introduction

British Standard BS EN 61508 (2000) came into ‘official’ existence in the UK in 1998 as IEC 61508. It was adopted in full as a British Standard in March 2000, yet many companies are only just getting to grips with the application of the standard.

The standard itself has two main aims:
- To act as a framework for the preparation of sector specific standards based upon this parent standard.
- To guide the design of safety related systems for sectors where there is no specific guidance.

BS EN 61508 (British Standards Institute, 2000) is a large document in seven parts and due to its high level of technical detail, can be hard to digest for those not involved in the detailed design of safety related systems. It is easy to find yourself lost in the detail of redundancy and reliability calculations and miss the smaller (in volume) but equally (and perhaps more) important aspects related to management systems. The general requirements section of the standard only makes up one seventh of the volume of the standard and yet this is the area where more of the difficulties of implementation tend to lie.

Since much of the work used to develop the IEC 61508 standard was based on work in the process industries, one of the first sector specific standards issued was for this industry. BS IEC 61511 (British Standards Institute, 2004) was published in 2003 and was adopted as a European standard in 2004. For process engineers this standard is easier to handle as it uses language that is much more familiar and rather than giving all the detail used in BS EN 61508 it refers back to BS EN 61508 where required. This is illustrated in the diagram below:
PROCESS SECTOR SAFETY

INSTRUMENTED SYSTEM

STANDARD

PROCESS SECTOR HARDWARE

PROCESS SECTOR SOFTWARE

Developing New Hardware Devices
Follow BS EN 61508

Using Proven-In-Use Hardware Devices
Follow BS EN 61511

Using Hardware Developed and Accessed According to BS IEC 61508
Follow BS EN 61511

Developing Embedded (System) Software
Follow BS EN 61508-3

Developing Application Software Using Full Variability Languages
Follow BS EN 61508-3

Developing Application Software Using Limited variability Languages or Fixed Programs
Follow BS IEC 61511

FIGURE 1: BS EN 61511 STRUCTURE AND ITS LINKS TO BS EN 61508

BS EN 61511 is structured around safety lifecycle phases. The safety lifecycle phases are listed below:

- Hazard and risk assessment
- Allocation of safety functions to protection layers
- Safety requirements specification for the safety instrumented system
- Design and engineering of safety instrumented systems
- Installation, commissioning and validation
- Operation and maintenance
- Modification
- Decommissioning

The above phases are supported by the management, planning and verification phases of the standard. Further details of the lifecycle phases are provided in Figure 5.

WHY APPLY BS EN 61511?

The Health and Safety Executive (HSE) in the UK uses authoritative good practice such as that found in industry guidelines, codes of practice, widely recognised standards and Approved Codes of Practice as benchmarks for enforcing health and safety law. BS EN 61511 Functional Safety – Safety Instrumented Systems for the Process Industry Sector is one of the standards that HSE uses to benchmark performance.

BS EN 61511 Functional Safety – Safety Instrumented Systems for the Process Industry Sector is specifically designed for use in the process industries. BS EN 61508 Functional Safety of Electrical / Electronic / Programmable Electronic Safety Related Systems is designed for use
by the manufacturers and suppliers of devices to the process industries. This is illustrated in Figure 1 above.

In a recent paper from the HSE by Vernon (2004) a top tier COMAH site is described where BS EN 61508 has been applied. This site has found that its application has lead to a significant reduction in maintenance overheads. This has been achieved through designing systems such that they require less frequent maintenance and also by setting maintenance frequencies using a risk based approach. It was found that in many areas the site had been over-maintaining its equipment. This reduction in maintenance and the consideration of how plant would be maintained at the design phase can also lead to reduced plant downtime for maintenance.

The use of BS EN 61511 or BS EN 61508 for safety related systems can also be a valuable tool in ALARP (As Low As Reasonably Practicable) demonstrations for sites. Although a site’s own management system can be used in COMAH Safety Reports and ALARP demonstrations, the HSE may well ask how the system applied on the site relates to the recognised standard for that topic.

Links with Corporate Management Systems

Gap analyses against BS EN 61511 often reveal that much of the spirit of the system required by the standard is in place as a result of pre-existing corporate systems. This tends to be particularly the case in the design areas of the system. It is in the functional safety assessment, management systems and detail areas of the standard that sites tend to have gaps. Often the difficulty in completing the gap analysis is in identifying how the site’s existing system links to the requirements of the standard. One way of avoiding this and helping to demonstrate compliance with the standard is by applying the language of the standard to the corporate system. BS EN 61511 uses process industry type language but also introduces new terms such as functional safety assessment. It can also cause some confusion in that it terms commissioning to be the installation of the instrument whereas commonly the process industry would term commissioning to be the operational testing of the installed instrument. Operational testing of the installed instrument is termed validation in BS EN 61511. These differences in language may appear minor but they can lead to significant confusion. Also using the language of the standard helps to understand the standard, demonstrate compliance to the standard and ease identification of gaps in the system.

Difficulties in SIL Classification

Difficulties with Safety Integrity Level (SIL) classification can lead to instrumented protective systems being over or under specified, use of some of the common qualitative techniques such as risk graphs and layers of protection analysis can lead to pessimism or optimism being built into the risk assessment.

The SIL is the required reliability of the safety function and is related to the probability of the safety related system satisfactorily performing the required safety function. Under the standards, SIL classifications are divided into four discrete levels. SIL rankings can be defined in terms of the probability of failure of that system on demand or the factor by which the risk of failure must be reduced to achieve that SIL ranking.

Two types of operation are defined within the standards; demand and continuous mode operation. Continuous mode operation is relatively rare in the process industries and is more typically found in systems like “fly by wire” used in aeroplanes. These are systems where the demand for the safety function is more frequent than once per year. Process industry
applications tend to have hazard occurrence frequencies of less than once per year and are thus considered under the low demand SIL rankings. The low demand SIL rankings are listed below:

<table>
<thead>
<tr>
<th>Safety Integrity Level (SIL)</th>
<th>Probability of Failure on Demand</th>
<th>Target Risk Reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>( \geq 10^{-5} \text{ to } &lt; 10^{-4} )</td>
<td>( 10,000 \text{ to } \leq 100,000 )</td>
</tr>
<tr>
<td>3</td>
<td>( \geq 10^{-4} \text{ to } &lt; 10^{-3} )</td>
<td>( 1000 \text{ to } \leq 10,000 )</td>
</tr>
<tr>
<td>2</td>
<td>( \geq 10^{-3} \text{ to } &lt; 10^{-2} )</td>
<td>( 100 \text{ to } \leq 1000 )</td>
</tr>
<tr>
<td>1</td>
<td>( \geq 10^{-2} \text{ to } &lt; 10^{-1} )</td>
<td>( 10 \text{ to } \leq 100 )</td>
</tr>
<tr>
<td>a</td>
<td>( \geq 10^{-1} \text{ to } &lt; 10 )</td>
<td>( 1 \text{ to } \leq 10 )</td>
</tr>
<tr>
<td>-</td>
<td>( \geq 10 )</td>
<td>( \leq 1 )</td>
</tr>
</tbody>
</table>

The type of instrumentation required for each SIL is indicated below:

- **SIL -** An alarm may be sufficient.
- **SIL a** Normally requires a system that automatically intervenes.
- **SIL 1** Low level of risk reduction required.
- **SIL 2** Likely to require some redundancy or a high degree of smart instruments.
- **SIL 3** Significant risk reduction required. Diversity will be required within system.
- **SIL 4** Not recommended in BS EN 61511.

The key approach of both standards is the use of risk assessment to determine the design of control systems. The standards require the use of risk assessment to determine what the necessary risk reduction is for the process and then taking account of inherent safety allocate that risk reduction to safety systems. These safety systems can be mechanical devices such as relief valves as well as instrumented protective systems. In fact, appropriately applied Safety Integrity Level (SIL) assessment often leads to a re-consideration of how the necessary risk reduction may be achieved. The necessity to design and maintain a SIL rated system can lead to more lateral thinking in terms of alternative risk reduction methods and helps to avoid the “belt and braces” approach that is often the natural tendency of the design team.

**Approach adopted to SIL Classification**

The methodology adopted was to use the semi-quantitative approach using calibrated risk graphs as an initial screening exercise followed by fault tree analysis of scenarios that are identified to have SIL rankings greater than 1. The semi-quantitative approach using risk graphs requires that the consequences, demand rate, probability of staff being present and the probability of avoiding harm are assessed. It was found that when trying to apply the demand rate and consequence categories suggested in BS EN 61511 members of the assessment team found it hard to place events in a specific category. Often the demand rate or consequences suggested by the team fell immediately on the boundary between categories and also lead to events being placed higher up the demand rate or consequence rankings. Ultimately this lead to higher SIL rankings than the consequences or their demand rate implied were necessary. This problem was eliminated by using a finer resolution for the frequency and consequence categories, in particular using twelve categories for consequence, allowing differentiation between singular and multiple consequences, for example differentiation between one and one hundred fatalities. A similar approach was applied to the demand rate categories, such that an
event that occurs once every ten years can be differentiated from an event that occurs every one hundred thousand years.

Once the event categories have been defined the risk graph must be calibrated for the site on which it is to be used.

The routine of identifying the hazard scenarios and formally applying consequence and demand rate criteria can lead to some surprising results. Where the methodology has been applied to existing systems it has been found that some of the safety related systems previously considered to be critical are not necessarily so and it may often be adequate to use them for process control functions only. It has also, conversely (but rarely) been shown that some systems that were deemed non-critical require higher SIL rankings than the assessment team would have anticipated. The advantage of the application of a formal SIL assessment procedure is that it provides a logical documented and justified rating for safety related functions. It helps to remove the reliance on “gut feel” and it also means that the maintenance frequency assigned to the safety function is optimal for the reliability required.

Integration of BS EN 61511 with Existing Business Systems

The assessment of existing instrumented protective system integrity has also proven to be a daunting challenge due to the large volume of data manipulation required. Much of this data resides in business systems such as SAP and Maximo and needs to be extracted prior to input into stand alone trip management software packages.

There are a range of stand alone trip management software packages on the market. These can perform a range of functions from calculating SIL rankings for instruments to managing the whole maintenance programme for a site’s instruments. The disadvantage of these systems is that they require the transfer of the site’s design, maintenance and instrument information to yet another system. These systems can be maintained on site by in-house personnel but can also be contracted out to the software supplier. This results in an extremely large data transfer requirement and has an inbuilt ability to produce mistakes, both at the initial transfer of the data but also during the running of the systems as data is transferred.

Surveys within major corporations have identified that companies typically have large numbers of databases:

? One large UK refinery site has over 120 Access / Excel databases
? One large European plastics manufacturer has over 70 databases
? One large bulk chemical manufacturer has over 100 Access / Excel / Manual databases
? One large petrochemicals plant has over 200 Access / Excel / Foxbase / SQL databases

This large number of information stores leads to either a significant workload in maintaining all of the disparate information sources in an up to date form or, more commonly, leads to varying information for which it is difficult to determine what is correct and current. Each database then becomes an “island of information” sometimes leading to ineffective, inconsistent and inaccurate actions. This is illustrated in Figure 2 below:
Often the simplest solution is perceived to be the purchase of a proprietary software package for lifecycle integrity management.

Many companies have business management systems such as SAP and Maximo that are used to manage a range of company information from accounting to maintenance and inspection functions. These typically contain details of the instrumentation systems used on site and are often used for maintenance planning. Since this is the case they already contain much of the information already required for managing safety related systems under BS EN 61511. The use of a SAP based management system allows the use of a single existing business system avoiding the need to transfer data, preventing the production of “islands of information” and avoiding the need to change several systems to perform BS EN 61511 functions. Figure 3 below illustrates the benefits of an integrated management information system.
SAP based solutions aimed at addressing the data handling requirements of BS EN 61511 allow the operator to maximise the use of the existing system rather than creating “islands of information” by installing another "bolt on" system. This solution forms the basis for ongoing trip and alarm management throughout the lifecycle of a system.

Case Study – Implementing a SAP based Integrity Management System

A SAP based Integrity Management System has been developed for a large petrochemicals complex. The choice of SAP was in line with a corporate requirement to move to integrated management systems based on SAP.

The site’s current organisation of information systems had lead to the creation of a number of “islands of information”, as is illustrated in Figure 4 below:

![Figure 4: Current Organisation of Databases](image)

**Figure 4: Current Organisation of Databases**

The first step in assessing what the site needed to do to comply with BS EN 61511 using SAP was to review the site’s current practices and procedures against BS EN 61511 and identify how the various elements of the standard were met and what systems were used for each of the elements. This was done by a group of on site personnel who had responsibilities for instrumented protective systems, a SAP expert and an external facilitator. The team consisted of safety, projects and maintenance personnel to ensure the full range of instrumented protective system activities were covered. The assessment was done using an audit proforma based on the standard. The assessment resulted in both a gap analysis against the standard but also in a list of activities that could be based in SAP. One of the main advantages of the team approach was that it allowed the site to fully understand the scope of work required to achieve BS EN 61511 compliance and it also created “buy in” from site based personnel who would be the owners of the system once built.

The BS EN 61511 lifecycle is illustrated in Figure 5 below. It indicates the range of activities that need to be considered under the standard.
It was found during the assessment of the site’s activities against the standard that it was necessary to pedantically adhere to the detail of the standard. This at times appeared to be cumbersome but it ensured that all the clauses were adequately considered.

BS EN 61511 requires a management system and this like all management systems to contain the standard elements below:

- Policy
- Planning
- Implementation and operation
- Checking and corrective action
- Management review

It is often these elements of BS EN 61511 that are missed or forgotten in the headlong rush to classify SILs and check the SIL rating of existing instrumented protective systems. However, in a recent paper from the HSE by Vernon (2004), a review by the HSE of links between COMAH and BS EN 61511 found that over half the links were related to management system issues.

Prior to the team assessment the site had done a considerable amount of work on BS EN 61511 and already had in place procedures to cover the first five phases of the standard related to hazard and operability assessments and SIL allocation. The site was also in the process of SIL assessing their existing instrumented protective systems. The general feeling was that they were well on their way to compliance with the standard, however the outcome of the team assessment showed that along with some overview procedures relating the standard to their systems, there were still some significant links that needed to be built into the system to...
achieve compliance to the standard. These links were largely around “joining up” existing systems and procedures and putting them into the language of the standard. There were no significant elements of the standard that were not at least partially addressed by existing systems and procedures.

In terms of SAP, there were a surprisingly small core of systems and programming that needed to be built into SAP. As was illustrated in Figure 4, the site had a number of database systems and much of the SAP related work was around the linking of these systems to the instrumented protective functions identified and detailed within SAP. The site runs a document management system and this proved to be a valuable resource to link the SAP data to the work carried out on site.

The site currently stores information on instrumented protective systems in SAP and runs its maintenance programme through SAP. SAP generates the work orders for maintenance work. The maintenance programme is to be revised to ensure that requirements for additional assessments, such as functional safety assessments are built into the programme and work orders are automatically generated and their progress tracked. Since not all of the elements of the safety function are allocated to instrumented systems, the non-instrumented systems must also be part of the maintenance programme and their reliability recorded. It is proposed that all elements of safety related functions will be flagged within SAP to allow for easy identification.

To achieve BS EN 61511 compliance the site is to set up a standardised document file structure for instrumented protective systems. This structure will include items such as the design information, the SIL assessment, the equipment safety manual and functional safety assessments. This file structure will be linked to the instrument protective system within SAP such that all the necessary documentation and records are readily available.

The approach to the calculations for probability of failure on demand required to determine the SIL ranking of equipment has been to use a proprietary software package. This choice was made on the basis that these packages contain the necessary reliability information and are written by experts in reliability calculations. No advantage was identified in the site writing and producing their own reliability calculation methods and building them into SAP. The complexity of the calculations was such that the necessary skills were not available on site and any such system would need to be validated. In addition, the proprietary package provider supplies support in the use of their software and maintains the software and its reliability data. One word of caution to be applied when selecting proprietary software for probability of failure on demand calculations is that in a review of the reliability data in these packages there was in some cases a wide variation in the reliability assigned to individual components. The site selected their software on the basis that it contained corporate reliability data for their organisation.

The most complex area to resolve was around generating the necessary data for ongoing functional safety assessments and proven in use data. This is partly related to identifying what data it is required to collect but is largely down to the complexity of collecting that data. For functional safety assessments it is important to verify that the demand rates used in the SIL assessment are appropriate and correct. This means that demands on the safety related system must be recorded. For trip systems, especially those run independently of process control systems, there was no electronic means of registering the demand. The trips are noted and acted upon through operational and safety procedures but a formal system of reporting needs to be instigated to ensure that those demands are appropriately recorded and logged against the safety function.
From the standard the failure types that need to be recorded fall into four categories:

- Safe detected
- Safe undetected
- Dangerous detected
- Dangerous undetected

This failure information can come from a number of sources and typically would not be recorded against these categories. In addition to the failure mode it is necessary to define each element of the safety related system component by component and to know its length of time in service. Components may be regularly changed and the means by which “real” in service time can be measured is difficult as it would need to take account of periods of shutdown as well as physical changes. It is also necessary to know the type of instrument and the type of service the instrument is in to ensure that like with like systems are compared.

The main stumbling block for any site trying to generate this information is that their data population for any particular instrument is relatively small, especially within safety related systems. Typically populations are not adequate to build sufficient statistically reliable data based on safety related systems alone. To build adequate data a site would need to record the data described above for every element of all instrumented systems on site. This would be a large workload and would require every component of every instrumented system to be recorded within SAP. The site in the case study has taken the view it will build its system to comply with BS EN 61511 based upon the available proprietary reliability data and that it will build its recording system for safety instrumented protective systems around the proven in use data requirements. This system may be extended to cover other instrumented systems at a later date. The current reliability data used is based upon its company’s corporate experience. It is also anticipated that as BS EN 61511 is more widely taken up, more detailed and extensive reliability data will be collected and become available.

Conclusion

This paper provides details on the BS EN 61508 and 61511 standards and why there is a need to apply them in the process industries. It also describes some of the potential problems associated with the use of some of the common qualitative techniques for risk assessment needed to define Safety Integrity Levels that can lead to over or under specification of safety related systems. It goes on to describe a method developed and used by AK EHS & Risk to minimise the potential of inaccurate specification.

The paper also addresses how BS EN 61511 can be applied using a SAP based system and describes how this has been approached for a specific site. It details the advantages of this approach that makes use of existing systems and avoids the creation of disparate “islands of information”.

References