

Two Birds With One Stone

How IEC 61508 and IEC 61511 aid Safety Case development.

(Presented at the IBC's Safety Case Experience conference April 2003)

C R Timms,

Director, Asset Integrity Management Limited

INTRODUCTION

Safety Cases have been a legal requirement for the UK Offshore sector ⁽¹⁾ since 1992 to implement the findings of the Lord Cullen Enquiry ⁽²⁾ following the 1988 Piper Alpha disaster, which took 167 lives. The Safety Case Regulations (SCR) requires a Safety Case to be submitted to the UK Health and Safety Executive for every offshore installation. These have to 'address hazards with the potential to cause a major accident' and 'demonstration of the adequacy of the safety management system'.

SCR are also underpinned by the Offshore Installation (Prevention of Fire and Explosion, and Emergency Response) Regulations 1995 (SI 1995/743) (PFEER)⁽³⁾, and the Offshore Installations and Wells (Design and Construction, etc) Regulations (SI 1996/913) (DCR)⁽⁴⁾.

PFEER is focussed on identifying and preventing fire and explosion hazards, protecting persons from the effects, and securing effective response to emergencies, whilst DCR seek to 'ensure that the level of the integrity of the installation is as high as reasonably practicable at all times, and that risks to people on an installation arising from matters of integrity, are kept as low as reasonably practicable'. This includes the design, modifications, operation and maintenance.

DCR also amend the SCR to 'require an installation duty holder to ensure that a verification scheme is drawn up covering the safety-critical elements of the installation'.

So some of the main Safety Case requirements are that:

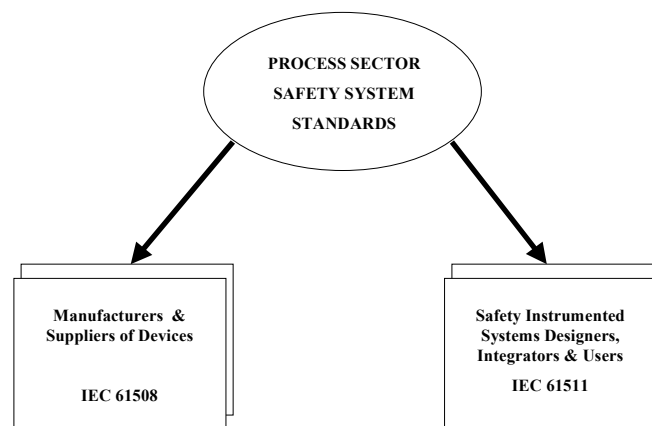
- Hazards are identified;
- Safety critical elements protecting persons from hazards are identified;
- Risks are kept as low as reasonably practicable;
- Design is appropriate;
- There is an audit trail for the decision making process;
- Modifications are properly designed and controlled;
- Operations do not compromise integrity;
- Performance standards are set;
- Operation against performance standards are verified;
- The integrity of the facility is maintained throughout its lifecycle;
- Performance is reviewed and modifications made where necessary;
- Safety critical roles are identified;
- People in safety critical roles are assessed as competent to perform those roles.

Thus developing a Safety Case is quite an onerous task, and it makes a great deal of sense to take advantage of other standards that have been set and adopted, providing they can be shown to have the appropriate dovetailing synergy.

Safety Case Requirements cover safety critical elements and activities over the entire spectrum of disciplines and roles, from the designers, through construction, operations and maintenance, but when they are viewed from an instrumentation perspective there is a very neat fit with the requirements of IEC 61508 ⁽⁵⁾ and IEC 61511 ⁽⁶⁾.

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

IEC 61511 is a process sector standard of IEC 61508 and is applicable to a wide range of industries including chemical, oil refining, oil and gas production, pulp and paper, non nuclear power generation, etc. Figure 1 shows the relationship between IEC 61508 and IEC 61511.



Relationship of IEC 61508 & IEC 61511

Figure 1 - Relationship between IEC 61508 & IEC 61511

IEC 61511 is a three-part standard that focuses on Safety Instrumented Systems (SIS):

- Part 1: General framework, definitions system software and hardware requirements
- Part 2: Guidelines on the application of Part 1
- Part 3: Guidelines on the application of hazard and risk analysis

IEC 61511 is concerned with the functional safety of safety instrumented systems and:

- Requires that a hazard and risk assessment is carried out to identify the overall safety requirements;
- Requires that an allocation of the safety requirements to the safety-instrumented system(s) is carried out;
- Works within a framework which is applicable to all instrumented methods of achieving functional safety;
- Details the use of certain activities, such as safety management, which may be applicable to all methods of achieving functional safety.

It is not simply concerned with the aspects of design but it addresses all the relevant safety lifecycle stages including the initial concept, design, implementation, operation and maintenance through to decommissioning as shown in Figure 2.

Since IEC 61511 is so comprehensive, it also provides a framework for harmonising with

Overall Safety Lifecycle

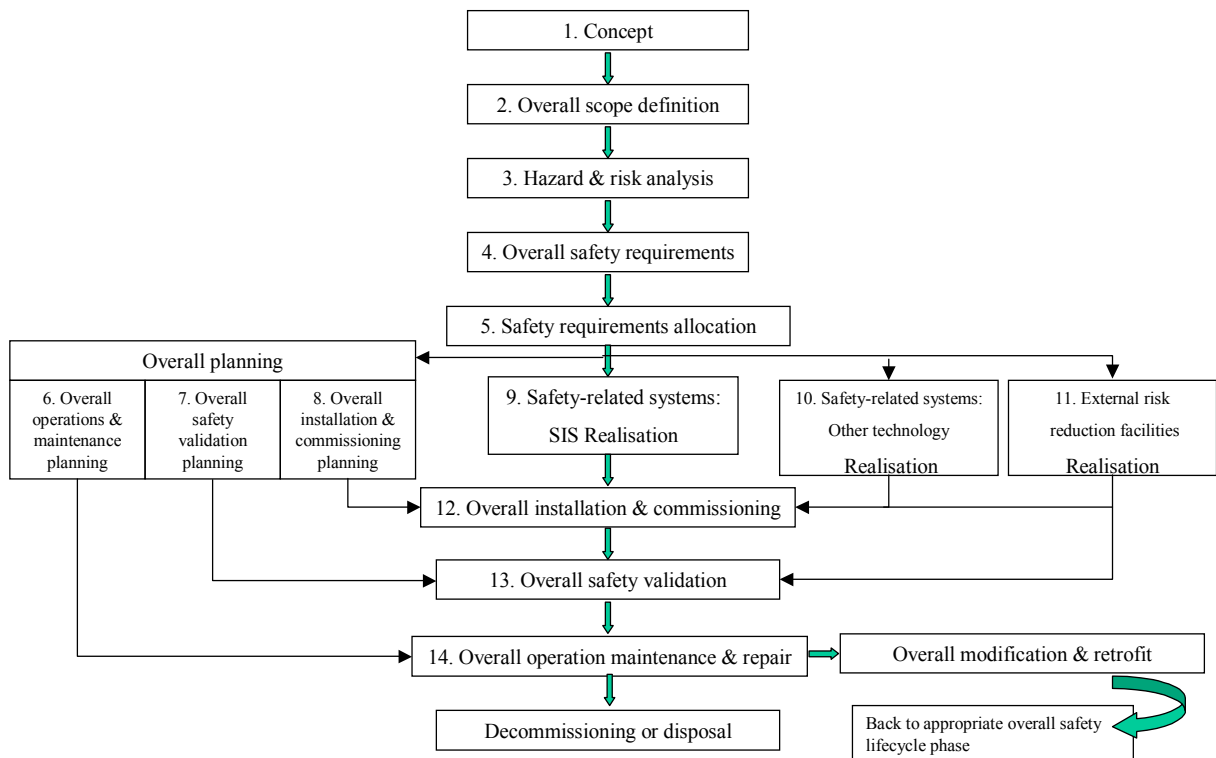


Figure 2 – Overall safety lifecycle

country specific process sector standards and legislation such as Safety Case Regulations.

Process Safety Target

The main emphasis of the IEC 61511 standard is concerned with the identification of hazards and reducing the associated risks from a level that is intolerable to a residual risk that is tolerable or ‘as low as reasonably practicable’ (ALARP) Figure 3.

Tolerability of risk and ALARP

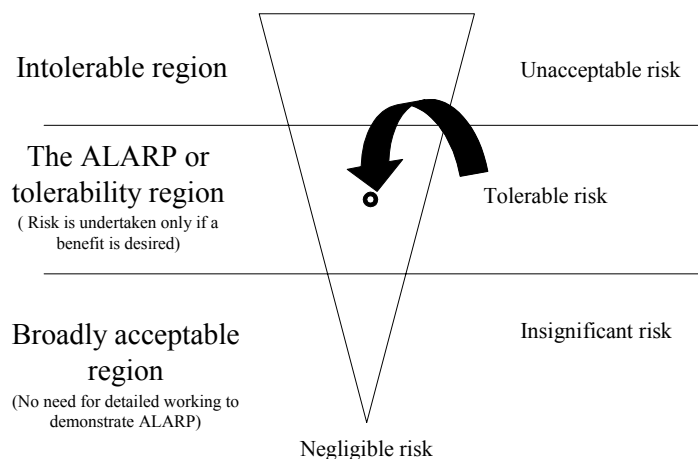


Figure 3 – The ALARP principal

- **What is risk?**
Risk = harm x probability

Risk is the combination of the severity of harm that can result from a hazardous event and the probability of that event actually occurring.

Operators need to define their corporate safety targets for individual risk (i.e. risks per year of the most exposed individual) and societal risk (i.e. the total risk per year of all exposed individuals). They then have to demonstrate ALARP by ensuring that the residual risk is tolerable only if further risk reduction is impracticable, or the cost and time involved is grossly disproportionate to the any further risk reduction achieved.

Hazard Analysis

•What is a hazard?

The potential source of harm, damage to property, production or the environment, production losses or increased liabilities.

Hazard identification is often undertaken by a technique known as Hazard and Operability (HAZOP) analysis that was first developed by ICI in the United Kingdom but became more generally adopted following the Flixborough (Nypro UK) chemical disaster in June 1974 that killed 28 people.

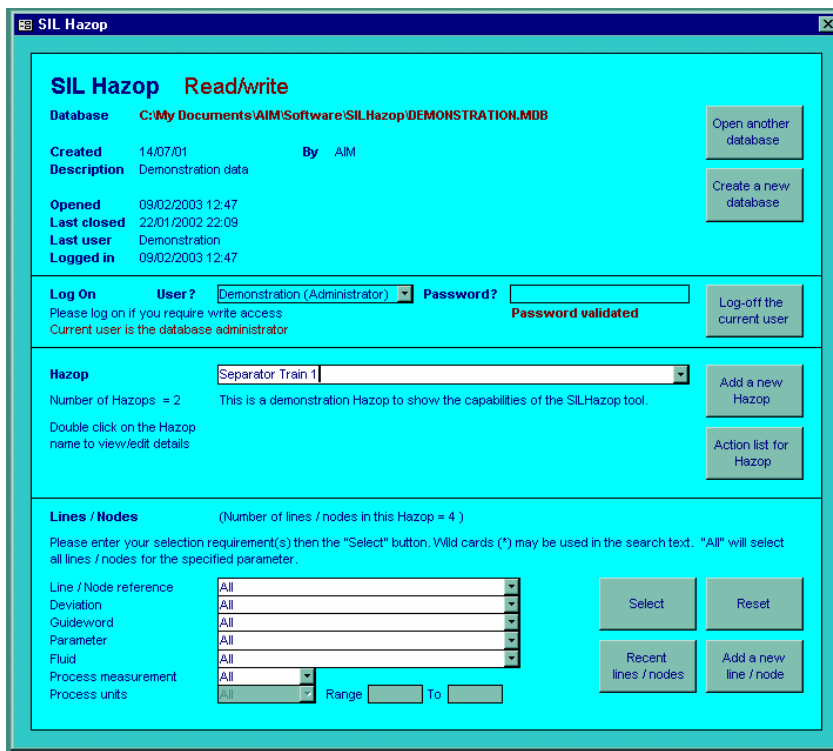


Figure 4 – The SILHazop software tool

These actions are either:

- To remove the cause
- To mitigate or eliminate the consequences.

The Hazop process systematically questions every part of a process to establish how deviations from design intent can occur. The consequences of the deviations are then assessed to determine if they would have an adverse effect upon the safe operation of the process.

Existing protective devices that prevent or safeguard against the adverse consequences of hazards are considered and actions are raised where the protection is considered inadequate.

Where it is not possible to remove the cause additional safeguarding is required. Safety Instrumented Systems (SIS) play a significant role in preventing or safeguarding against hazards.

The Hazop process demands full recording and reporting to demonstrate that the rigour of process has been thoroughly carried out, and this is extremely time consuming, particularly if undertaken as a paper exercise. The effort can be greatly reduced with computer power and there are numerous packages available to make the process more efficient such as the AIM SILHazop application in Figure 4. As well as offering the advantages of secure database records and comprehensive reporting for audit purposes, this particular package has links with a classification package (SILClass) for undertaking the criticality assessment of the instrument based safeguarding systems.

Risk Reduction

Having identified the potential hazards, measures must be taken to reduce residual risk to the ‘tolerability region’ (Figure 2), and total risk reduction is usually achieved by using a combination of protective systems that may cover a number of technologies. These can include mechanical, pneumatic, hydraulic, electrical, electronic, programmable electronic, etc.

IEC 61511 requires all technologies to be considered before establishing the need for a safety instrumented system (SIS). Process is design, the chosen materials and their strength form an essential part of process safety and risk reduction, but these factors alone may not reduce the risk of averting a hazard to a level that is ALARP.

The usual model that represents the concepts of risk reduction (Figure 5) includes:

- Process design;
- A process control system;
- Associated human factor issues;
- Safety protective systems comprising:
 - External risk reduction facilities;
 - Safety Instrumented Systems;
 - Other technology safety-related systems.

Risk Reduction - General Concepts

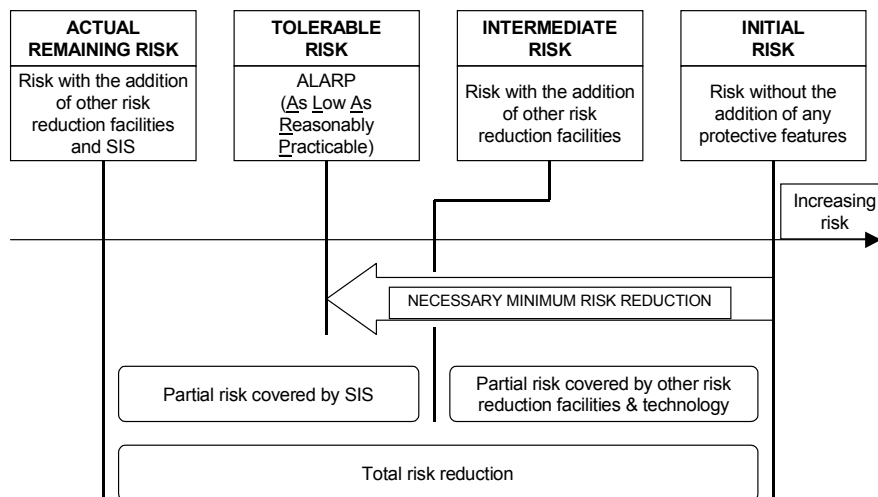
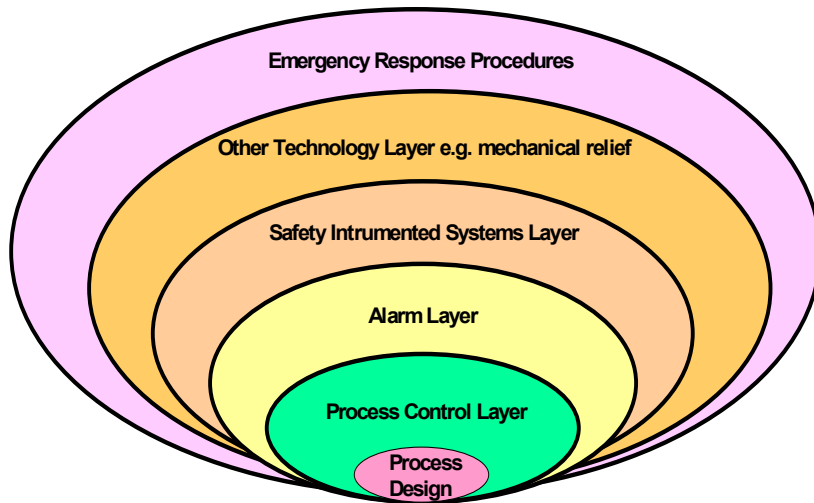


Figure 5 – Risk reduction concepts

The different facets of risk reduction can be represented as separate layers (Figure 6).

Risk Reduction Layers



Process design has been discussed above, and the objective of process control is to keep operation within the normal operating envelope, and properly configured alarms ⁽⁷⁾ will alert the operator to deviations from the normal so that corrective action can be taken if there is time to react.

A process may also have a number of protective

Figure 6 – Risk reduction layers

layers and examples include mechanical relief devices to protect against overpressure and over speed protection for rotating equipment machinery, etc and a responsible operator will ensure that there are also properly implemented emergency response procedures to mitigate the consequences of a hazardous event.

However, all of these measures may still not achieve the total risk reduction necessary for the target safety level and safety instrumented systems often form an essential and integral part of the overall risk reduction.

Safety Instrumented Systems

A SIS may contain a number of specific safety instrumented functions (SIF) to sense abnormal conditions and automatically return the process to a safe condition. This is usually achieved by performing a partial shutdown or complete shutdown of the process.

SIS = Safety Instrumented System

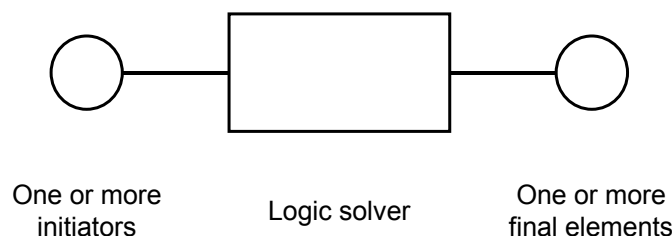


Figure 7 – Safety Instrumented System

A SIS may comprise one or more initiators (i.e. sensors and measurement devices), a logic solver (relay based, solid state, magnetic core, etc.) and one or more final elements (i.e. valves, dampers, motor drives, etc.) as shown in Figure 7. The initiators and final elements

are connected through the logic of the logic solver to achieve specific functional safety protection within the process such as over/under pressure protection, high/low temperature protection, high/low flow protection, etc.

Assessing the criticality of safety instrumented functions

It is necessary to establish the criticality of a SIF to ensure that it is properly designed, tested and maintained. IEC 61511 provides a measurement of criticality as a Safety Integrity Level (SIL) with a range from SIL 1 to SIL 4, where SIL 1 represents the lowest integrity requirement and SIL 4 the highest integrity requirement.

There are numerous ways to make the criticality assessment, which is known as SIL determination, and two of the most popular methods are Risk Graphs and Layers of Protection Analysis (LOPA). The risk graphs shown in Figure 8 enable three risk assessments to be made covering personnel safety, asset loss and environmental risk. They use a combination of the demand rate, i.e. the probability, and the consequence severity that would occur if the SIF failed on demand, i.e. the harm.

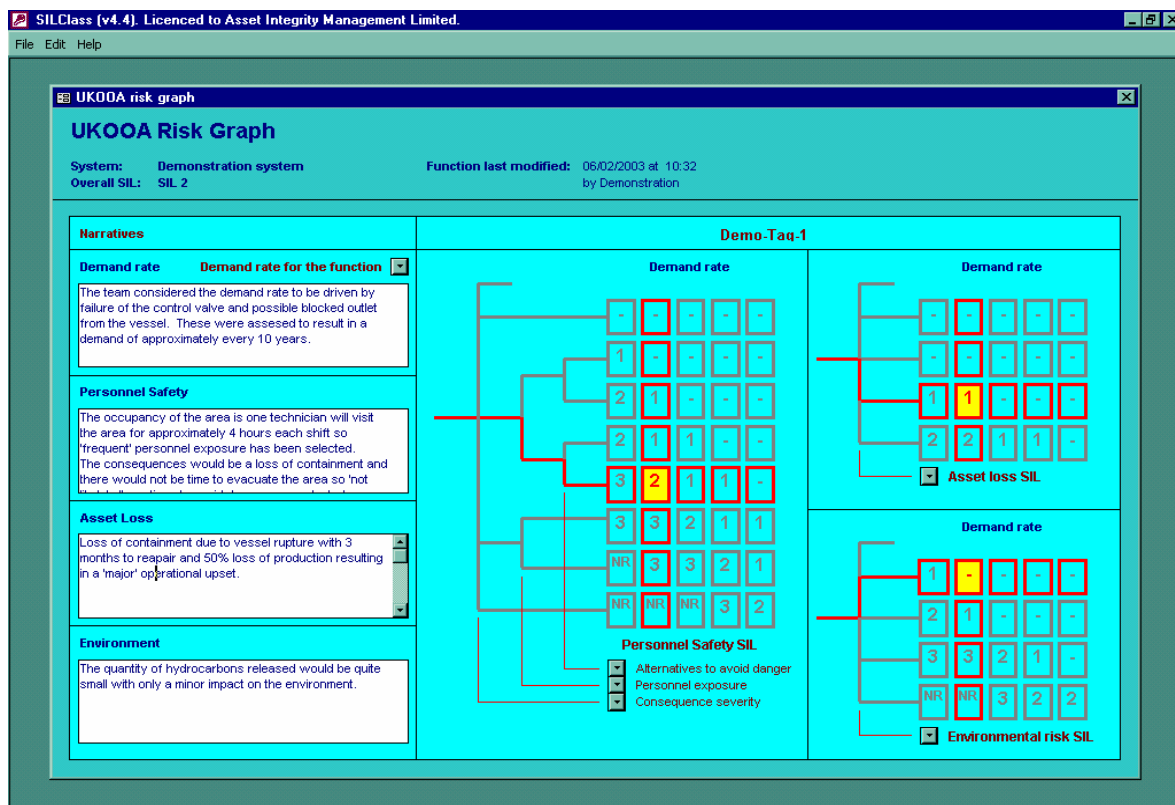


Figure 8 -AIM SILClass software with UKOOA risk graph.

Whatever risk assessment method is chosen, it is essential to have the appropriate skills represented for the decision making process. A multiple discipline team should undertake this activity with the following skills composition:

- A facilitator (skilled in the IEC 61508/61511 risk assessment process)
- Process Engineer
- Instrument Engineer
- Operations representative
- Safety specialist

A SIL determination study requires considerable commitment of time and resource, and this needs to be recognised by management, but it should not be an issue if management are genuinely committed to safety.

SIL determination will generate a significant amount of data this must be recorded to provide a complete audit trail to the background behind the decisions that are made during the process. If these are recorded on paper they will represent a snapshot in time and as the process changes, either through design modifications or process dynamics, then it will become an onerous task to keep the records updated.

Selecting a comprehensive software application and database tool such as SILClass will aid the analysis process and maintain the records with the integrity afforded by databases. In addition the analysis method can be chosen from risk graphs (Figure 7 shows an example using the UK Offshore Operators Association -UKOOA- risk graph), risk matrices or LOPA and can be customised to meet specific process sector requirements.

Using this kind of tool will ensure the background information, to support the SIL determination, is recorded in comprehensive high integrity database with secure password protection. The information recorded will include the drivers behind the selected demand rates, the consequences of SIF failure with respect to the safety of personnel, the possible total asset losses and the extent of any environmental damage.

The database records can then be easily sorted, e.g. to generate reporting for performance standards purposes, and they can be easily updated and maintained throughout the lifetime of the process. Thus these features cover a significant part of the Safety Case requirements.

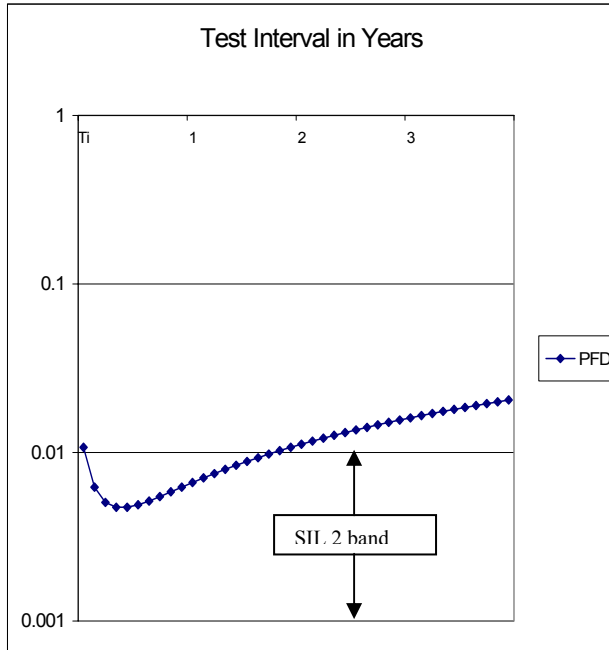
Ensuring that the design, testing and maintenance are appropriate

Once the criticality has been established in the range SIL 1 to SIL 4, this corresponds to the level of integrity required for the SIF design. The standard sets a reliability requirement, or the Probability of Failure on Demand (PFD), for each SIL band and this represents the level of risk reduction to be achieved for each SIL as shown in Figure 9. The PFD requirements actually comprise the performance standard to be achieved, since the more critical the function the lower the failure probability that must be achieved.

Safety Integrity Level (SIL)	Probability of Failure on Demand (PFD)	Risk Reduction
4	$\leq 10^{-4} - \geq 10^{-5}$	10,000 – 100,000
3	$\leq 10^{-3} - \geq 10^{-4}$	1,000 – 10,000
2	$\leq 10^{-2} - \geq 10^{-3}$	100 – 1,000
1	$\leq 10^{-1} - \geq 10^{-2}$	10 - 100

Figure 9 –Relationship between SIL, probability of failure on demand & risk reduction

The PFD is a dimensionless probability, but it is based on a relationship between the failure rate and frequency at which tests are carried out to reveal any hidden or covert failures that would prevent the function working on a real demand, Figure 10. In this example if the SIF was intended to meet a SIL 2 the test interval must not exceed 1.5 years.



For a single device:

$$PFD = 1/2 \lambda_d T_i$$

Where:

λ_d = the dangerous failure rate

T_i = the testing interval

This basic relationship provides the foundations for calculating the most appropriate SIF architecture in terms of the initiators, logic devices and final elements. If devices with a poor record of reliability are selected then they will require more frequent testing. If the test interval is extended then there is a higher probability that the device will fail.

Figure 10 – Relationship between testing and the probability of failure on demand

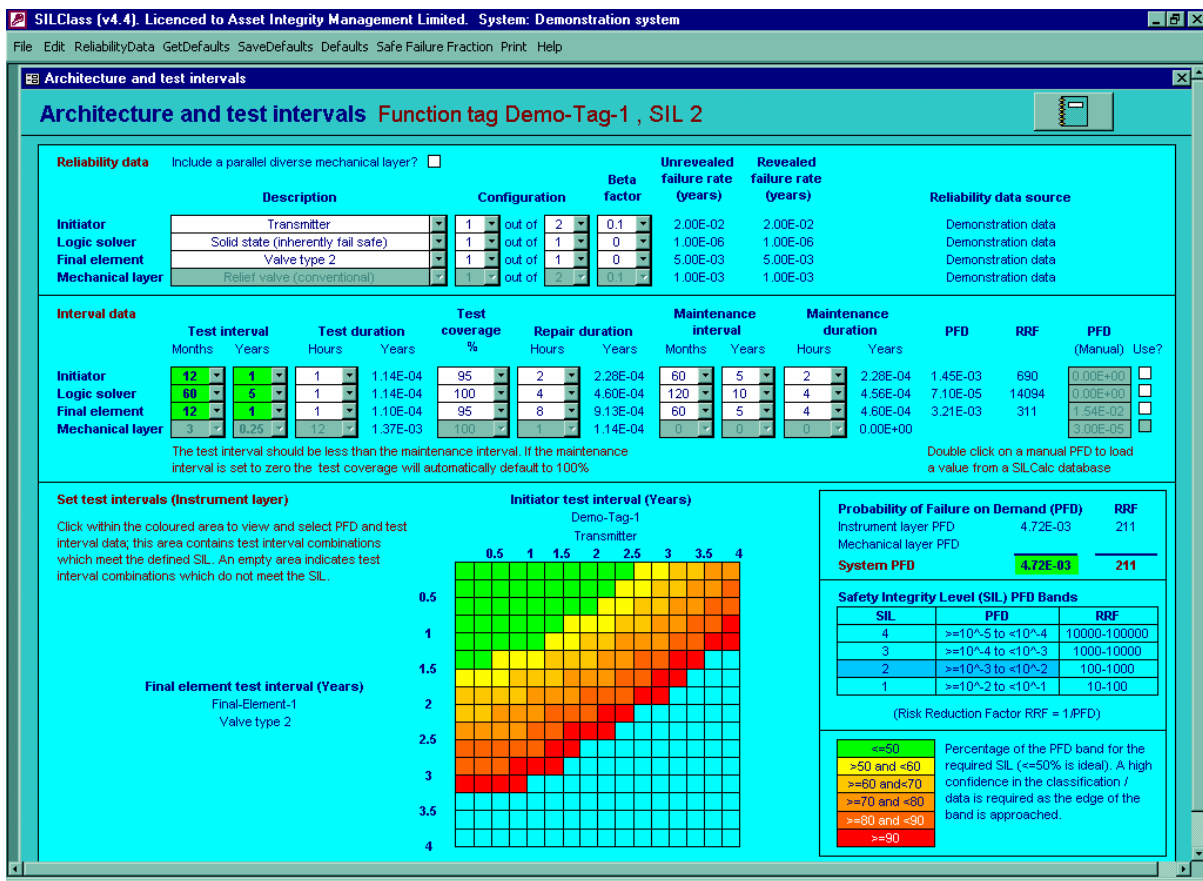


Figure 11 – Relationship between design architecture, test and maintenance intervals

In reality, the calculations are far more complex as factors such as the time taken to carry out the test, the coverage of the test (i.e. does the test cover every aspect that can cause failure), the period at which routine maintenance will be undertaken and the time taken to repair or

return the device to the ‘as new’ condition, all need to be considered. In addition, the architecture will often be far more complex than single devices for the initiators, logic and final elements, and there may also be common mode failure influences to be considered.

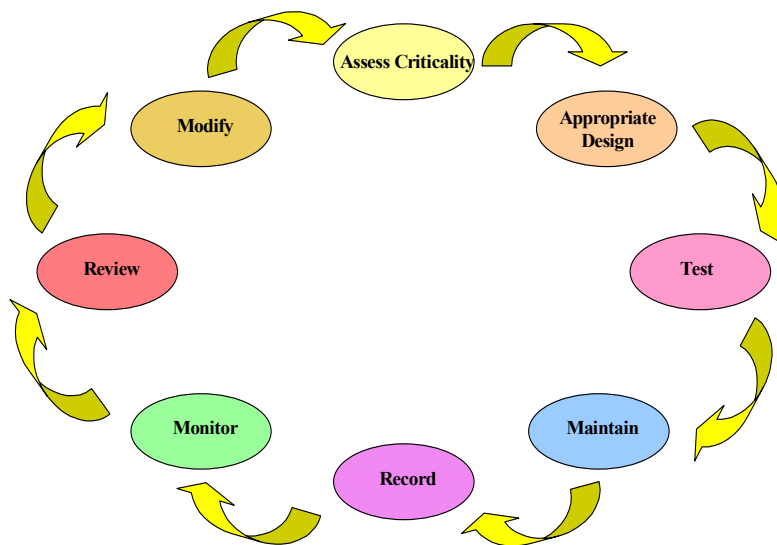
So there are many parameters and variables that can influence the probability that the protective function will actually operate on a demand, and they all need to be managed through the design stage and the operational lifetime. It is also essential to maintain the audit trail of how a particular design was selected and why a particular test and maintenance strategy has been adopted

Figure 11 demonstrates how the power of design tools, such as the AIM SILClass software, can pre-calculate the interaction of all the variables to help the selection of the most appropriate design and optimal test and maintenance requirements. This gives assurance that the design, testing and maintenance meet the required PFD criteria for the determined SIL and, since all the information resides in the database records, this actually represents the performance standard for each function.

Performance Monitoring and Verification

Having assessed the criticality of the SIF, established an appropriate design and set the test and maintenance strategy, then IEC 61511 requires the actual performance to be monitored and verified throughout its operational lifetime.

Performance Monitoring



This will include all the activities shown in Figure 12. Records must be maintained of testing and maintenance so that deviations and failures can be reviewed and modifications made to ensure that performance meets the set standards and

Figure 12 – Performance monitoring

integrity is not compromised. If records show better or worse than expected performance then the reliability data must be updated to take account of the operating experience. Poor performance may require additional test and maintenance or even modifications to design, whilst better than expected performance could indicate that the test and maintenance intervals can be extended, and experience shows that these result in significant cost savings.

Fixed format reporting for testing and maintenance activities will ensure consistency for analysing the records and these will aid the verification process.

Modifications and Change control

Any change to the process such as the process dynamics, the mode of operation or the design, may have an impact on the integrity of the process. Consequently the design and integrity of the protective functions, such as safety-instrumented functions, will also need to be reviewed.

Thus, from a Safety Case and IEC 61511 perspective, all changes must be flagged and managed by a formalised change control process. This must have the mechanisms in place to make proper assessments of the changes and their impact upon integrity. The impact of change may result in plant modifications or changes in operating and maintenance strategy or all of these things.

Some of the common changes that can have an impact on a SIF include changes to the affecting the frequency of demand on the protective function, or the range characteristics of the measured parameters may vary and require different trip settings, or the mechanical strength of materials could be compromised if the pressures, temperatures or products are modified etc.

The SIL may need to be reviewed, the architecture modified and/or the test and maintenance frequency changed. This is a relatively straightforward process if everything has been recorded within a database mechanism and the audit trail will be readily maintained at the same time.

Competency

Since Safety Instrumented Systems (SIS) are intended to protect against hazards which could cause serious injury or loss of life, it is necessary to have competent individuals involved in each of the different lifecycle phases indicated in Figure 2.

The safety critical roles and activities need to be identified (IEC 61511–1, Clause 5.2.2.2.) and documented, and the people who perform such activities must be assessed as competent to undertake those activities.

The following organisations will have people with specific safety critical roles with respect to the specification, design, implementation, and operation of SIS:

- engineering design contractors;
- vendors;
- system integrators;
- installation contractors;
- maintenance contractors;
- operating organisation.

The competence of the designer is not the only important consideration and equally important is the competence of the technician who calibrates the instruments and performs the testing.

Thus competence assurance at both the engineering and technical levels plays a vital part in maintaining the safety integrity and suitable schemes are required to ensure that individuals involved in the lifecycle process are assessed as competent. The IEE publication, “Safety, Competency, and Commitment: Competency Guidelines for Safety-Related System Practitioners”⁽⁸⁾ details a suitable competency scheme specifically developed for safety-related systems.

Conclusions

Safety Instrumented Systems have a significant role in protecting people from hazards. They generally form part of an overall risk reduction framework but they can often make a major contribution to the total risk reduction. They are, in Safety Case terminology, safety critical elements that come under the Safety Case requirements, and we have seen that some of the main requirements are that:

- Hazards are identified;
- Safety critical elements protecting persons from hazards are identified;
- Risks are kept as low as reasonably practicable;
- Design is appropriate;
- There is an audit trail for the decision making process;
- Modifications are properly designed and controlled;
- Operations do not compromise integrity;
- Performance standards are set;
- Operation against performance standards are verified:
- The integrity of the facility is maintained throughout its lifecycle;
- Performance is reviewed and modifications made where necessary;
- Safety critical roles are identified;
- People in safety critical roles are assessed as competent to perform those roles.

These requirements form a lifecycle framework, and from the outset of Safety Case requirements, instrumentation engineers recognised that there was a very neat dovetail with the requirements of the IEC 61508 and, more recently, the IEC 61511 standards. Thus compliance with the IEC 61511 standard, for Safety Instrumented Systems, will provide assurance that the Safety Case requirements are also met for these systems.

The whole lifecycle needs careful controls and management, because it forms an integral part of a safety management system, and keeping records throughout the entire lifecycle is essential for maintaining and demonstrating integrity. All of these factors demand considerable time and effort, but there are specialised software applications available to aid compliance and reduce the effort involved.

References:

1. The Offshore Installations (Safety Case) Regulations 1992 SI1992/2885 HMSO ISBN 0 11 025869 X.
2. The Public Enquiry into Piper Alpha Disaster (Cullen Report) Cm 1310 Department of Energy HMSO 1990 ISBN 0 10 113102 X (2 volumes).
3. Offshore Installation (Prevention of Fire and Explosion, and Emergency Response) Regulations 1995. Approved Code of Practice and Guidance on Regulations L65 HSE Books 1995 ISBN 0 7176 0874 3.
4. Offshore Installations and Wells (Design and Construction, etc) Regulations 1996, SI 1996/913 HMSO 1996 ISBN 0 11 054451 X.
5. Functional Safety of electrical/electronic/programmable electronic safety-related systems - BS IEC 61508: 1998.
6. Functional safety: Safety Instrumented Systems for the process industry sector CEI IEC 61511 draft.
7. How to achieve 90% of the gain without too much pain - C. Timms IBC Alarm Systems Conference June 2002.
8. Safety, Competency & Commitment – Competency Guidelines for Safety-Related System Practitioners – IEE 1999

Biography:

Clive Timms

Clive has over 30 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 Asset Integrity Management Ltd, which specialises in the application of the IEC 61508 standard, and he is also a 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 on the Institute of Measurement and Control Safety Panel.

Contact Details:

Clive Timms
Asset Integrity Management Ltd
South Steading
Sunnyside, Maryculter
Aberdeen, UK, AB12 5GT
Tel: + 44 (0) 1339 886618
Fax: +44 (0) 1224 735883
email: clive.timms@assetintegrity.co.uk
Web: <http://www.assetintegrity.co.uk>