The Safety Integrity Verification of Legacy Systems

Author: Colin Easton
ProSalus Limited – Independent Safety Consultants

1. Overview

Within the United Kingdom process industries IEC 61511 is recognised by the Health and Safety Executive (HSE) as relevant good practice for functional safety of safety instrumented systems (SIS) in the process industry sector. It is HSE’s view that if the requirements of IEC 61511 are met, thereby demonstrating that the risks under the control of safety instrumented systems have been reduced to a level that is as low as reasonably practicable ‘ALARP’, enough will have been done to comply with UK law so far as safety instrumented systems are concerned.

This paper is based on a project undertaken by the author following a HSE visit to an existing facility. The objective is to describe how the issues raised by the HSE during that visit with respect to the site legacy SIS have been addressed by applying the guidance in IEC 61511 as the basis for safety assurance that the existing safety instrumented functions (SIF) are capable of achieving the required contribution to risk reduction when applying the ALARP principle. The concepts described in this paper will be applicable to the assessment of the majority of legacy SIS systems used within the process industries.

The Safety Integrity level (SIL) verification of legacy SIS is a process that reviews and assesses a SIS based on the consequences of previously identified hazardous events. The legacy verification process focuses on the ability of an existing SIS to meet the recommendations of IEC 61511 and the current process plant design intent. It recognises that the legacy system has been designed to meet the standards of the day and applies the techniques and measures in IEC 61511 as a performance benchmark for the verification of the legacy SIS in terms of fitness for purpose through the proven in use argument supported by SIL calculations.

The process examines the installed safety instrumented sub system components and functions for purpose and adequacy and determines what measures of protection and intervention they perform to minimise the risks of an incident and establishes what, if any remedial works are required to the SIS.

The IEC 61511 standard is concerned with the functional safety of process plant safety instrumented systems. It requires:

- That a hazard and risk assessment is carried out to identify the overall safety requirements, this usually takes the form of a HAZOP study which is then used to develop the site’s safety management system and COMAH compliance strategy.
- That an allocation of the safety requirements to the safety-instrumented system(s) is carried out, this is discussed in more detail in section 3 of this paper.
- That a business works within a framework which is applicable to all instrumented methods of achieving functional safety; in this case it took the form of a long term maintenance strategy.
- Detailed use of certain activities, such as safety management, which may be applicable to all methods of achieving functional safety, this is addressed by the site’s safety management system.

IEC 61511 is not simply concerned with the aspects of design, but addresses all the relevant safety lifecycle stages including the initial concept, design, implementation, operation and maintenance through to SIS decommissioning.
2. Introduction

2.1. Background

As a result of an HSE visit to an existing waste chemical incineration plant the author was contracted to address the issues raised by the HSE and to carry out a SIL verification of the legacy SIS used to provide plant protection. The verification was required to evaluate if the legacy system provided a sufficient level of protection and met the ALARP requirements in terms of risk contribution. The framework used for the basis of the study was the widely recognised international standards for safety systems, IEC 61508 and IEC 61511 (Ref 1 & 2).

The verification process comprises two main stages. The first stage is an evaluation of the risk reduction contribution required from the Safety Instrumented Systems. It considers existing passive and active protection devices in terms of prevention and mitigation of the identified plant hazards and assesses their contribution towards the overall risk reduction target. For example, if a tank bund area is adequately sized to provide over spill mitigation in addition to the prevention provided by a high level switch. This stage used a combination of visual inspection and interrogation of existing hazard study reports, drawings and documents to gain an impression of the state of the SIS and other protection layers contributing to the overall risk reduction requirement.

The second stage is a numerical evaluation of legacy Safety Instrumented functions to verify that the required risk reduction contribution (target safety integrity level) can be achieved. For this stage the manufacturers of equipment were contacted (where possible) and information about the quality systems / control, current status, remaining life and serviceability of equipment obtained. Where possible, data sheets for either the installed equipment or suitable replacements were reviewed from manufacturers.

2.2. Documentation Reviewed during Verification of Legacy SIS

The following documents were reviewed during the study: -

1. Plant Hazard and Operability Study
2. Plant Process and Instrument diagrams
3. System Block Diagrams
4. Panel drawings
5. Circuit Diagrams
6. General arrangement drawings
7. System Visual Alarm Panel
9. Alarm System Circuit Diagrams
10. Emergency Stop Circuit diagrams
11. Sampling System Components diagrams
12. Operating and Maintenance Manuals for equipment
13. Plant Operating Procedures
14. Site Safety Health and Environmental (SHE) Management System
15. Site Quality Management System
16. Site computerised maintenance system (including test records)
17. Site Maintenance training records
2.3. Methodology Flowchart for Review of Legacy Safety Instrumented Systems

- Review existing HAZOP’s, Risk Assessments, COMAH Safety Report and PID’s to identify existing safeguards and Site Tolerability of Risk criteria
- Prepare inventory of safety instrumented functions and prepare Safety requirements Specification table for Legacy Systems (Refer Table 3)
- Allocate Safeguards to Protection Layers & Identify Independent Protection Layers (Refer Figure 1 and 2)
- Prepare Risk Models and evaluate using risk contribution estimates in Table 1 and determine risk contribution required for SIF in terms of target SIL from Table 2
- Review plant drawings, operation, maintenance records and inspection history for SIFs and complete Proven In Use table 4 to assess SIF functional safety capability
- Compare estimated system functional capability of SIF with safety requirements specification, if target not achieved consider replacement of existing SIF
- Update existing Site COMAH Safety Report and operation, maintenance and inspection procedures and prepare functional safety management systems and obsolescence policy
- Proof testing, inspection, audits and reviews to maintain functional safety capability of SIFs at required SIL
3. Identification of Safeguards and Tolerability of Risk

The verification of legacy systems commences with the review of the existing hazard and operability study report, (HAZOP), plant risk assessments and the as built plant PID’s to identify existing safe guards and the plant control of major accident hazard (COMAH) report to ascertain the site tolerability of risk criteria.

The existing safeguards are required to achieve or to maintain a safe state of the process and, contribute towards the necessary risk reduction to meet the tolerable risk determined by a company as a part of the COMAH report ALARP argument.

The ALARP argument essentially means weighing a risk against the trouble, time and money needed to control it. The decision making process requires the company to exercise ‘judgement’, apply ‘good practice’ and for high risk situations use formal techniques including cost benefit analysis to form a judgement. IEC 61511 is recognised by the Health and Safety Executive (HSE) as relevant good practice and as such is acceptable as a part of the ALARP argument (Ref 4, 5, 6 & 7)

The necessary risk reduction may be achieved by either one or a combination of SIS or other protection layers, such as mechanical protection in the form of venting or passive protection in the form of a tank bund of fire wall. Fig-1 gives an overview of typical risk reduction methods as identified in IEC 61511

As in the case of the tanker off loading procedures in section 2.6 a person could be an integral part of a safety function providing a risk reduction in this case all human factors should be considered and any claim limited by complexity of the task, training and experience (Ref 15 & 16).

Fig-2 from IEC 61511 above illustrates the general concepts of risk reduction and is taken from IEC 61511. The various risks indicated are as follows:

**Process risk:**

The hazards and risks for a specific plant as identified in the HAZOP, these hazards are generally realised due to failures of the BPCS or human error. Existing safeguards are not considered when evaluating the process risk although the control system risk reduction can be considered, but, IEC-61511 limits the claim by setting the probability of failure on demand at a maximum of 0.1.
Tolerable risk:
The tolerable risk criteria has been identified in the risk ranking matrix figure 3 which is typical of the process industries and is generally in line with the R2P2 TOR Framework used in HSE guidance references 4, 5, 6 and 7. R2P2 indicates an upper limit of a risk of death to any individual worker at a frequency of one in one thousand per annum and the boundary between tolerable and broadly acceptable risk to any individual worker at a frequency of one in one million per annum.

It is important to note that there is not a standard risk ranking matrix and that many variations exist according to company and industry sector. Each company must develop a matrix that meets their own risk criteria and potential for hazards.

Residual risk:
The residual risk is the risk of a hazardous event occurring after the addition of all protection layers and is sometimes designated as the background risk, for example slips trips and falls.

3.1. **Tolerable Risk for Worse Case Scenario as Risk Reduction Factor**
The worse case scenario identified in the HAZOP was a loss of containment leading to a possible ignition of a vapour cloud or asphyxiation of an operator. Historical plant data showed that a loss of containment had occurred once in 16 years of operation.

The risk reduction provided by the existing safeguards is termed by IEC 61511 as the Risk Reduction Factor (RRF) and each protect layer contributes to the overall RRF

Based on the risk ranking matrix, refer figure 3 and the calibration parameters for people, asset, environment and reputation the following parameters were selected:

i) Consequence severity S3 using the asset parameter “Local damage – partial shutdown (can be restarted but costs up to £500,000)

ii) Frequency ranking PE based on 1 loss of containment in 16 years of operation.

So stated the present risk is intolerable (100) and based on HSE advice (Ref 4) the risk required should be set to at least two orders of magnitude less than the present risk value to be considered ALARP (1) for any one significant event.

The company tolerable criteria has been set two orders of magnitude below the HSE advice at (0.01) and therefore the tolerable risk target for any one significant event was set at a Risk Reduction Factor of 10000. The example risk model developed below is based on the 10000 risk reduction factor

3.2. **Allocation of Safeguards to Protection Layers and Risk Modelling**
The process is to compare the RRF = 10000, refer to section 2.4.1, with the risk reduction provided by all of the existing safeguards that prevent or mitigate an individual hazardous event and to estimate the risk reduction contribution from each safeguard in order to determine the RRF required from the SIF.

3.2.1. **Protection Layers and Independence**
The protection layers that prevent or mitigate an individual hazardous event are reviewed and allocated a RRF considering the criteria summarised in Table - 1. These criteria are set using IEC-61511 and plant failure data (Ref 8).

3.2.2. **Independence from IEC-61511**
For a preventative or mitigation layer to be considered independent it must be capable of achieving the independent protections layers criteria set out in IEC 61511-3 Annex F –F9.
3.3. **Typical Risk Reduction Model – Tank farm Overspill Scenario**

The risk reduction model below represents the overall risk reduction requirements of the Tank Farm Scenario. The protection layers available for consideration are taken from Table 1:

Tolerable Risk Frequency Target = $RRF_T = 10000$

Overall $RRF$ Achieved: $RRF_A = RRF_1 \times RRF_2 \times RRF_3 \times RRF_4$

**Table - 1: Estimate of Risk Reduction Contribution of Typical Protection Layers**

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Protection Layer</th>
<th>Risk Reduction Factor Value</th>
<th>Reference</th>
<th>SIL improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPL1</td>
<td>General &amp; Inherently Safe including: Vessel pressure rating above maximum challenge from internal and external pressure sources Or better, if vessel integrity is maintained (that is, corrosion is understood, inspections and maintenance is performed on schedule)</td>
<td>100 - 1000</td>
<td>IEC-61511</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Control of ignition sources – Area Classification to Zone 1 standard</td>
<td></td>
<td>Ref 8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Separation distances of Tanks</td>
<td></td>
<td>Ref 8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Operating Procedures</td>
<td>10 - 100</td>
<td>IEC-61511</td>
<td>1</td>
</tr>
<tr>
<td>IPL2</td>
<td>BPCS</td>
<td>0 - 10</td>
<td>IEC-61511</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Operator response to alarms</td>
<td>10 - 100</td>
<td>IEC-61511</td>
<td>1</td>
</tr>
<tr>
<td>IPL3</td>
<td>SIS - Single loop</td>
<td>10 - 100</td>
<td>Calculation</td>
<td>1</td>
</tr>
<tr>
<td>IPL4</td>
<td>Independent/diverse mechanical or relief devices including:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Pressure Relief Valves</td>
<td>10 - 100</td>
<td>IEC-61511</td>
<td>1</td>
</tr>
<tr>
<td>IPL5</td>
<td>Passive protection including:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Bund (110% Tank Capacity)</td>
<td>10 - 100</td>
<td>Ref 8</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Active Protection including:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Deluge System</td>
<td>10 - 100</td>
<td>Ref 8</td>
<td>1</td>
</tr>
<tr>
<td>Consequence</td>
<td>Severity Ranking</td>
<td>Frequency Ranking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------</td>
<td>-------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>People, Asset, Environment, Reputation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiple fatalities or permanent total disabilities</td>
<td>Catastrophic</td>
<td>S5</td>
<td>10000</td>
<td>1</td>
</tr>
<tr>
<td>Single fatality or permanent total disability</td>
<td>Severe</td>
<td>S4</td>
<td>1000</td>
<td>0.1</td>
</tr>
<tr>
<td>Major Injury or health effects</td>
<td>Critical</td>
<td>S3</td>
<td>1000</td>
<td>0.01</td>
</tr>
<tr>
<td>Minor Injury or health effects</td>
<td>Marginal</td>
<td>S2</td>
<td>100</td>
<td>0.001</td>
</tr>
<tr>
<td>Slight Injury or health effects</td>
<td>Negligible</td>
<td>S1</td>
<td>10</td>
<td>0.0001</td>
</tr>
</tbody>
</table>

- Risk is unacceptable and further risk reduction measures shall be considered.
- Risk is in the ALARP region (ALARP principles should be applied).
- No further justification required risk can be considered as acceptable.

**Fig-3: Typical Process Plant Risk Ranking Matrix**
3.4. Tank Farm Overspill Scenario Protection Layers
The risk reduction contribution claimed for each protection layer is taken from table 1 above.

RRF₁ – (Preventative) represents the existing offloading procedures. These procedural controls are well practiced and implemented by trained scientists and operations staff and are considered to be reliable, but a RRF of 10 only is claimed to take into consideration the human interaction. This is a conservative estimate as it is the minimum allowable for an IPL.

RRF₂ – (Preventative) represents the existing tank level SIF. The data provided by the manufacturers and taken from recognised sources (references 1, 2, 3, 9, 10, & 11) substantiates that the system will meet the required target SIL1 refer to section 4 for verification results and proven in use methodology. Therefore a RRF of 10 has been claimed.

RRF₃ – (Mitigation) represents the Tank Bund that has been sized to accommodate a 110% tank loss of containment. The bund area is regularly inspected and is designed as a holding area only until the product can be removed to safe storage. A RRF of 10 is therefore claimed and can be substantiated by good industry practice (Reference 8).

RRF₄ – (Mitigation) represents the deluge system inside the tank area and protects against a possible ignition with in the bund area and reduces the possibility of the spread of a fire to other tanks. The systems have a long service history with out a dangerous failure and have been designed to meet British standard for deluge systems. The system is considered to be reliable therefore an RRF of 10 has been claimed.

3.4.1. Risk Reduction Factor Calculation
The Risk Reduction factor for each IPL has been set at 10. This a conservative value and can easily be achieved with the existing systems and equipment presently in use on the site.

Overall RRF Achieved:  \( RRF_A = RRF_1 \times RRF_2 \times RRF_3 \times RRF_4 \)

Is equivalent to 10 x 10 x 10 x 10 = 10000

Therefore the overall RRF achieved with the existing systems meets the Tolerable risk ranking target of 0.01 (100) for any one significant event. (i.e. the overall RRF is 10000).

NOTE: The allocation of protection layers may be iterative in order to optimise the design to meet the various hazardous event requirements

3.5. Safety Integrity of Safety Instrumented Functions
The relationship between risk reduction factors (RRF), probability of failure on demand (PFDavg) and Safety Integrity Level (SIL) is shown in IEC61511-1 Table - 3: Safety Integrity Levels (Low Demand Mode). As stated in section 2.6.1 above a RRF of 10 has been allocated to the existing tank high high level safety instrument function this RRF value equates to a target PFDavg of 0.1 and a target SIL of 1 for a SIF operating in a low demand mode of operation

3.6. Safety Requirements Specification
The process now advances to check if the SIF claim of RRF 10 can be achieved by the existing equipment. The process commences with a safety requirements capture exercise using table 2 below to capture the functional and integrity requirements for each of the SIF. Table 3 will be fully populated during the SIL verification and Proven in Use process.
4. SIL Verification

The lifecycle approach now advances to check the validity of the claim of RRF 10 and SIL1 capability for the Safety Instrumented Function. The SIL Verification has been carried out using the techniques referenced in IEC 61511-2 Annex A / B using the Asset Integrity Management “SILCalc” tool and the prior-use argument in IEC 61511-1 clause 11.5.3.

Safety integrity is considered to be composed of the following two elements.

**Hardware safety integrity and Architectural Constraints** – that part of safety integrity relating to random hardware failures in a dangerous mode of failure. The achievement of the specified level of hardware safety integrity can be estimated to a reasonable level of accuracy using either plant historical data, manufacturers’ data or generic industry failure such as the FARADIP database and the simplified formulas in IEC 61511-2 Annex A and B.

The verification must include analysis of hardware fault tolerance for each sub-system. As no programmable logic solver forms a part of the plant SIS table 6 IEC61511-1 can be applied, this table allows the historical plant failure data to be taken into consideration to assess minimum fault tolerance requirements. IEC61511 requires a minimum fault tolerance of “0” for SIL1 (i.e. permits use of a single channel system).

The plant instrumentation is of an age where self-diagnostics are not available and any failure (dangerous or safe) will either be detected by an operator (under normal or adverse operations) or under the manual proof test regime.

**Systematic safety integrity** – that part of safety integrity relating to systematic failures in a dangerous mode of failure. IEC 61508-2 Annex B gives a selection of techniques and measures for the avoidance of systematic failures during the different phases of the lifecycle. These qualitative requirements must be met in order for a given SIL to be claimed for a SIS and assure that systematic safety integrity is preserved during operation, maintenance and subsequent modification.

An important requirement to remember is that all sub systems must meet the target SIL in terms of hardware and systematic safety integrity.

4.1.1. Typical Supporting Documentation

The following documents were used as referenced for the study:

1. Plant Process and Instrument diagrams
2. System Block Diagram
3. Panel drawings
4. Circuit Diagrams
5. General arrangement drawings
7. Function Charts.
8. Alarm System Circuit Diagrams
9. Emergency Stop Circuit diagrams
10. Sampling System Components

4.1.2. System breakdown into components/sub-systems

The verification requires that the SIF is broken down into sub-systems. Typically these are the sensor subsystem; logic solver; and final element subsystem. These are broken down further if subsystems contain more than one component of a significantly different type or design.
For each subsystem, its “SIL capability” is identified, that is the maximum SIL for which it can be used within a SIF while meeting the requirements of IEC 61508 or IEC61511. This is achieved in one of three ways.

1. Component or sub-system certification, or evaluation which deems it suitable for use up to a given SIL
2. Demonstrate “prior use” according to IEC61511 in which case a simplified set of requirements, as defined by IEC61511 are applied to evaluate SIL capability
3. If “Prior Use” cannot be demonstrated, then IEC61508 is used to identify SIL capability.

4.1.3. Prior Use Claim

The IEC 61511-1 clause 11.5.3 requirements for the selection of components and subsystems based on prior use are set out in table 3, the process commences with a SIF sub systems certification or prior use requirements capture exercise using table 3.

Typically the plant SIF equipment met the prior-use argument in that they all provide a greater than 1 year operating experience, have an extended CMMS maintenance history, including annual proof tests with no recorded failures and are subject to maintenance procedures that are based on the manufacturer’s recommendations and vendor control.

4.1.4. Confirmation of achieved SIL for Safety Instrumented Functions

The achieved SIL is confirmed as the lowest of the achieved SIL ratings identified for:

Each subsystem;
The system as a whole as governed by its average PFD;
The system as a whole as constrained by the systematic / qualitative requirements.

4.1.5. Mode of operation

Key aspects of the verification are dependant upon the system-operating mode, which is defined as either Low Demand or High Demand (or continuous) Mode. Based on plant historical data a Low Demand Mode of operation has been selected, as it is considered a demand will not placed on any SIF more often than once per year.

5. Safety Instrumented Functions Verification Result

Typical Serial System Calculation for the tank level system

<table>
<thead>
<tr>
<th>Level Switch</th>
<th>Relay Card</th>
<th>Interposing Relay</th>
<th>Interposing Relay</th>
<th>Circuit Breaker</th>
<th>Pump</th>
</tr>
</thead>
<tbody>
<tr>
<td>PFDavg</td>
<td>PFDavg</td>
<td>PFDavg</td>
<td>PFDavg</td>
<td>PFDavg</td>
<td>PFDavg</td>
</tr>
<tr>
<td>2.23E-03</td>
<td>1.76E-02</td>
<td>4.62E-03</td>
<td>4.62E-03</td>
<td>1.76E-02</td>
<td>1.18E-02</td>
</tr>
</tbody>
</table>

Safety Instrumented Function Overall PFDavg = 5.85E-02

6. Conclusion

The report demonstrates that the existing protection systems provide adequate risk reduction and that the legacy SIF achieves the target SIL. The report was submitted to the HSE in response to the issues raised and following review by HSE specialists has been accepted as providing adequate evidence to support the risk reduction claimed.
Table - 2: Typical Safety Requirements Specification Table for use with Legacy System Evaluations

<table>
<thead>
<tr>
<th>Loop Tag</th>
<th>SIS Safety Requirements Specification Table for Legacy Systems</th>
<th>Safety Integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Safety Function</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hazard Study</td>
<td>SIL Target</td>
</tr>
<tr>
<td></td>
<td>Safeguard Function</td>
<td>SIL Achieved</td>
</tr>
<tr>
<td></td>
<td>Function Confirmated</td>
<td>SIL Hardware</td>
</tr>
<tr>
<td></td>
<td>Process Safety Time Confirmated</td>
<td>Fault Tolerance</td>
</tr>
<tr>
<td></td>
<td>Cause &amp; Effect Detail Confirmated</td>
<td>Completed</td>
</tr>
<tr>
<td></td>
<td>Fail Safe Action Confirmated</td>
<td>Pass / Fail</td>
</tr>
<tr>
<td></td>
<td>P&amp;ID Detail Confirmated</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Effect Detail Confirmated</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Trip &amp; Alarm Schedule Detail Confirmated</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Loop Diagram Detail Confirmated</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Operator Interface Confirmated</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fail Safe Action Confirmated</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cause &amp; Effect Detail Confirmated</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Loop Diagram Detail Confirmated</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Operator Interface Confirmated</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fail Safe Action Confirmated</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cause &amp; Effect Detail Confirmated</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Loop Diagram Detail Confirmated</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Operator Interface Confirmated</td>
<td></td>
</tr>
</tbody>
</table>

Table - 3: Typical SIF Function Safety Capability Assessment Table for use with Legacy System Evaluations

<table>
<thead>
<tr>
<th>SIS COMPONENTS</th>
<th>IEC61508 Certified</th>
<th>Prior Use (In Accordance with IEC 61511)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor subsystem</td>
<td>Hardware TÜV certified compliant with IEC 61508-2 (specify SIL) Yes/No</td>
<td>Evidence of manufacturers Quality Plan</td>
</tr>
<tr>
<td>Logic Solver Subsystem</td>
<td>Software TÜV certified compliant with IEC 61508-3 (specify SIL) Yes/No</td>
<td>Evidence of manufacturers hardware and configuration documentation</td>
</tr>
<tr>
<td>Final element Subsystem</td>
<td>Evidence of manufacturers hardware and configuration systems</td>
<td>Specification sheet for subsystem</td>
</tr>
<tr>
<td></td>
<td>Evidence of performance in a similar operational profile and environment (safety and non-safety applications)</td>
<td>Confirmation that subsystem is suitable for use in a Safety Instrumented System</td>
</tr>
<tr>
<td></td>
<td>Evidence of reliability data</td>
<td>Volume of operating experience</td>
</tr>
<tr>
<td></td>
<td>Evidence of reliability data</td>
<td>Evidence of reliability data</td>
</tr>
<tr>
<td></td>
<td>Identification of unused features and confirmation that they are unlikely to jeopardise the required safety instrumented function</td>
<td>Consideration of specific configuration and operations with respect to characteristics of input and output signals</td>
</tr>
<tr>
<td></td>
<td>Modes of use</td>
<td>Functions and configurations used in similar applications and environments</td>
</tr>
</tbody>
</table>
7. References

1. IEC 61508 Functional safety of E/E/PES systems, Parts 0-7
2. IEC 61511 Safety Instrumented systems for the process industry sector, Parts 1-3
3. BS EN 6739 Instrumentation in Process control systems: installation design & practice
4. Reducing Risks, Protecting People, HSE decision making process (R2P2) ISBN 0 7176 2151 0
5. HSE - Principles and guidelines to assist HSE in its judgement that duty-holders have reduced risk as low as reasonably practicable.
6. HSE – Assessing compliance with the law in individual cases and the use of good practice
7. HSE – Policy and Guidance on reducing risks as low as reasonably practicable in design
13. Health and Safety at Work Act etc., 1974
14. SI 1999/743 Control of Major Accident Hazards Regulations 1999
15. SI 1999/3242 The Management of Health and Safety at Work Regulations 1999
17. Safety, Competency and Commitment – Competency Guidelines for Safety-Related Systems Practitioners 1999; The Institution of Electrical Engineers
18. The CASS Guide 26th April 2000 Issue 2.a