GUIDELINES

on

the Interpretation of

BS EN 61508 – The functional safety standard

for the

Valve and Actuator Industry

prepared by

BVAA
The British Valve and
Actuator Association

© BVAA - MARCH 2013

Disclaimer:
The publishers endeavour to ensure the accuracy of the contents of this document. However, the publishers do not warrant the accuracy and completeness of the material in this publication and cannot accept responsibility for any error and subsequent claims made by any third parties. The contents of this publication should not be construed as professional advice and the publishers disclaim liability for any loss, howsoever caused, arising directly or indirectly from the information in this publication.

BVAA GUIDELINES ON THE INTERPETATION OF THE FUNCTIONAL SAFETY STANDARD: BS EN 61508- 2010

INDEX

Page

Some commonly used functional safety terms and abbreviations

AC	Architectural Constraints
ALARP	As Low as Reasonably practicable
CCF	Common Cause Failure
COMAH	Control of Major Accident Hazards
DC	Diagnostic Coverage
DPCS	Distributed Process Control System
E/E/PE	Electrical/Electronic/Programmable-Electronic (Technology used in a product or system)
EUC	Equipment under control
FIT	Failures in Time (10^{-9}/hr)
FMEA	Failure Modes and Effects Analysis
FMEDA	Failure modes effects and diagnostics analysis
FSM	Functional Safety Management
FTA	Fault Tree Analysis
FVL	Full Variability Language
HAZOP	Hazards and Operability Study
HFT	Hardware fault tolerance
HLA	High Level Alarm
HSE	Health and Safety Executive
LoPA	Layer of protection Analysis
LVL	Limited variability language
MDT	Mean Down Time
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failure
MTTR	Mean Time to Repair
NCR	Non-Conformity Report
OEL	Occupational Exposure Level
P&ID	Piping and Instrumentation Diagram
PES	Programmable Electronic System
PFD_{AVG}	Probability of Failure on Demand (average)
PL	Performance Level
PLC	Programmable Logic Controller
PVST	Partial Valve Stroke Testing
RBD	Reliability Block Diagram
RRF	Risk Reduction Factor
RTD	Resistance Temperature Detector
SC	Systematic Capability (1 to 4)
SFF	Safety Failure Fraction
SIF	Safety Instrumented System
SIL	Safety Integrity Level
SIS	Safety Instrumented System
T	Proof test interval
T/C	Thermocouple
TOE	Target of Evaluation (used in CASS methodology)
Type A	Non-complex component or sub-system (e.g., switch, mechanical device)
Type B	Complex component or sub-system (e.g., programmable device)
UKAS	United Kingdom Accreditation Service
1oo1,1oo2, etc.	Nomenclature to indicate voting channels
PFD	Probability of failure on demand

Revision	Date	Author	Reviewer	Approver	Description
A.1	06/03/2013	P. R. Smith	P.R. Smith		Internal Review
A.2	08/03/2013	P. R. Smith	R. Bartlett / P. Churrn		Initial draft for client comment
A.3	11/03/2013	P. R. Smith	P. Reeve		Technical Review
A.4	27/03/2013	P. R. Smith	P. Reeve		Firm Issue to BVAA

BVAA GUIDELINES ON THE INTERPRETATION

of the

Functional Safety Standard BS EN 61508

for the

VALVE AND ACTUATOR INDUSTRY

Introduction – Background and Objectives

What importance has it to the Valve and actuator Industry?

It is extremely important to the valve industry as HSE data indicates that the final actuator (generally a valve actuator combination of some description) accounts for 50% of the failures of safety loops. At the moment (March 2013) most SIL assessments are FMEDA based and use 'generic' failure rate data, i.e. failure rate data collated by independent bodies and sourced from across various industries. This means that current SIL calculations are generically based and may be grossly incorrect in many applications. By performing valve and actuator FMEDA using specific failure rate data it might be expected that the accuracy of SIL calculations will improve with consequent advantages to both functional safety AND the credibility of individual manufacturers.

Also:

1. **Uptake of BS EN 61508 is now increasing rapidly as the HSE and the Courts of Law recognise it as engineering good practise and consequently use it as a yardstick when industrial accidents are brought before them.**
2. **Functional Safety is increasingly recognised in diverse process industries and hence the demand for SIL capable equipment is also increasing rapidly.**
3. **The necessity for improving the safety of operations staff and the public is undeniable and essential as process industries are developing more hazardous chemical processes, oil and gas are more difficult to access under the sea and nuclear power use is once again recognised as a necessary source of clean, renewable energy.**

Background and Objectives

This guide has, therefore, been prepared by the BVAA as an aid to the interpretation of the requirements **of the Functional Safety standard BS EN 61508:2010** "Functional safety of electrical/electronic/programmable electronic safety-related systems" **as it applies to the manufacturers of valves and associated equipment. It is not an authoritative interpretation of the standard and must be read in conjunction with the standard.**

i) The purpose of BS EN 61508 is to provide a top level generic set of requirements for the achievement of Functional Safety that is relevant to all sectors of industry. From this top level generic standard it is expected that sector specific standards may be derived.
BS EN 61511 results as the Process Control sector derivative
BS EN 61513 results as the Nuclear Sector derivative
Others standards cover Machinery (BS EN 62061) and medical (unnumbered).

ii) BS EN 61508 is not a mandatory standard so there is no legal obligation on Industry to use it. HOWEVER, it has been established and accepted by the UK and international law courts as 'good' engineering practice and as such is used as reference in cases of industrial accident.

A recent example being the Buncefield Tank Farm. The HSE has published many papers and reports culminating in legal action being taken against several equipment suppliers and citing BS EN 61508 as good engineering practice.

iii) BS EN 61508 is entitled 'Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems'. **This title has led many to believe that it does not apply to purely mechanical, pneumatic or hydraulic devices. This is a misunderstanding; it applies to a complete safety instrumented loop whatever that may be composed of, but typically sensor(s), logic solver(s) and final element(s). Final element being a valve/actuator, contactor or whatever.** All elements (as well as their integration) have to be assessed under BS EN 61508 if the loop has some safety significance in the context of the control system it relates to.

iv) The current version of BS EN 61508 was published 2010. All earlier versions are now obsolete.

v) Regarding the use of this guideline, readers are encouraged to read Part 1for an overview of how BS EN 61508 is intended to support the achievement of Functional Safety. Safety Integrity Level (SIL) Determination (section 1.5) is interesting but less essential to those suppliers involved purely with satisfying a request for so called 'SIL rated' equipment.
Part 2 & 3: are essential reading for those wishing to supply 'SIL rated' equipment.
Part 4: Provides useful additional reading for those who are inclined to learn more.

vi) **It is essential that element manufacturers, such as those producing valves and actuators, understand that a single component CANNOT have a SIL! SIL is effectively a level of risk reduction which is applied to and achieved by a complete safety instrumented function, often simply called a safety loop.**

vii) SIL does NOT apply to non-return valves, pressure relief valves, bursting discs and the like as the BS EN 61508:2010 classifies them as 'Other Technology'. However, each of these devices does make a contribution to the SIL determination process as they provide 'layers of protection', where each layer reduces the risk by a small amount. As the SIL of any resulting E/E/PES safety function will be determined by a consideration of the existing available risk reduction for a particular part of a process it follows that the assumed failure rates of these ‘other technology’ measures making up these layers of protection must be reliable and quantified. Probability of Failure on Demand (PFD) is the inverse of Risk Reduction Factor (RRF) and hence it is still necessary to perform failure mode effects and diagnostics analysis (FMEDA) and provide validation of the RRF achieved.

viii Any claim to compliance with this standard must be based on available supporting evidence! If a Company cannot provide evidence of ‘x’ then ‘x’ does not exist.

Finally, it is important to understand the meaning of ‘element’ as used in the standard. Previous versions of the standard have referred to ‘component’ when referring to loop ‘elements’ such as the sensor or the actuator. The latest version refers to all devices making up a safety loop as ‘elements’; this is to avoid confusion when discussing ‘components’ within an element – such as transistors, valve stem or seal, etc.

PART 1: OVERVIEW OF FUNCTIONAL SAFETY CONCEPTS AND STANDARDS

1 Definition of “Functional Safety”

“**Functional Safety** is the part of the overall **safety** of a **system** or piece of equipment that depends on the system or equipment operating correctly in response to its inputs”. For example, where a safety application relies on a valve responding reliably to a close command under certain hazardous plant conditions. It includes the safe management of likely operator errors, potential design flaws, hardware failures and environmental changes, known as systematic failures as well as the random failures that occur due to hidden material flaws.

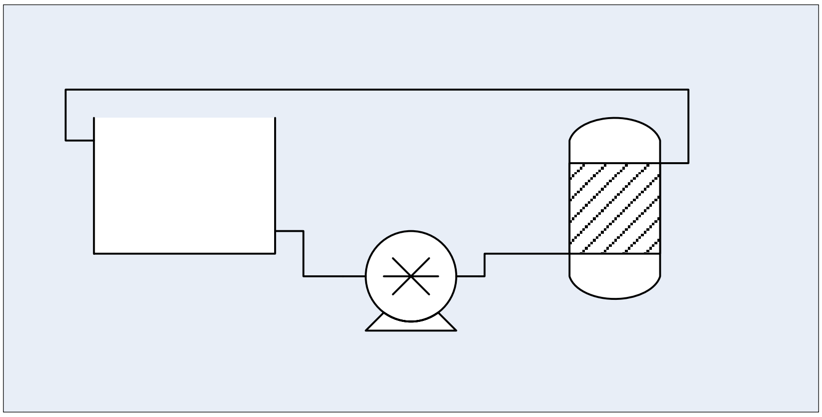
Functional Safety concerns safety hazards caused by mal-operation of ‘control’ systems such as the automatic door closing mechanism of a lift. If the door control fails to detect an obstruction then severe injury could result as a body part may be trapped between door and lift wall with the result that the trapped person may be dragged down (or up) with the lift movement or even suffer crush injuries due to the force available to the door closing mechanism.

Alternatively **Physical Safety** relates to **hazards** which are **constant** and which can be removed or minimised by careful design. A good example is a ‘lift’, the gap between landing and lift floor is a physical safety feature, too wide and injuries due to trapping may occur, but easily solved by designing the gap to be as small as practically possible.

For Example:

In Process terms we have a process which may be chemical, nuclear, biological, pharmaceutical, mechanical, etc.:

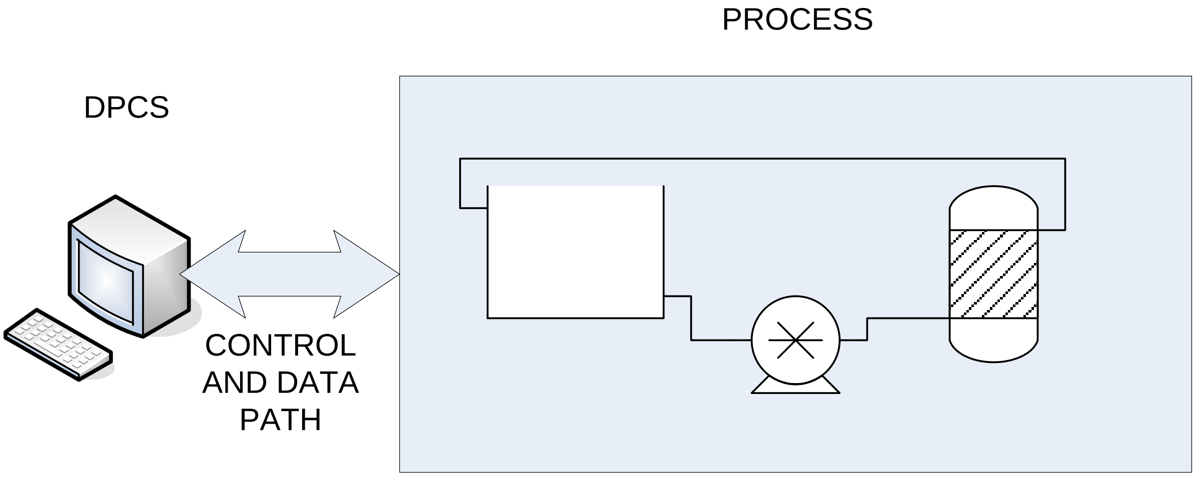
Sketch One



Sketch One represents a hypothetical process……..

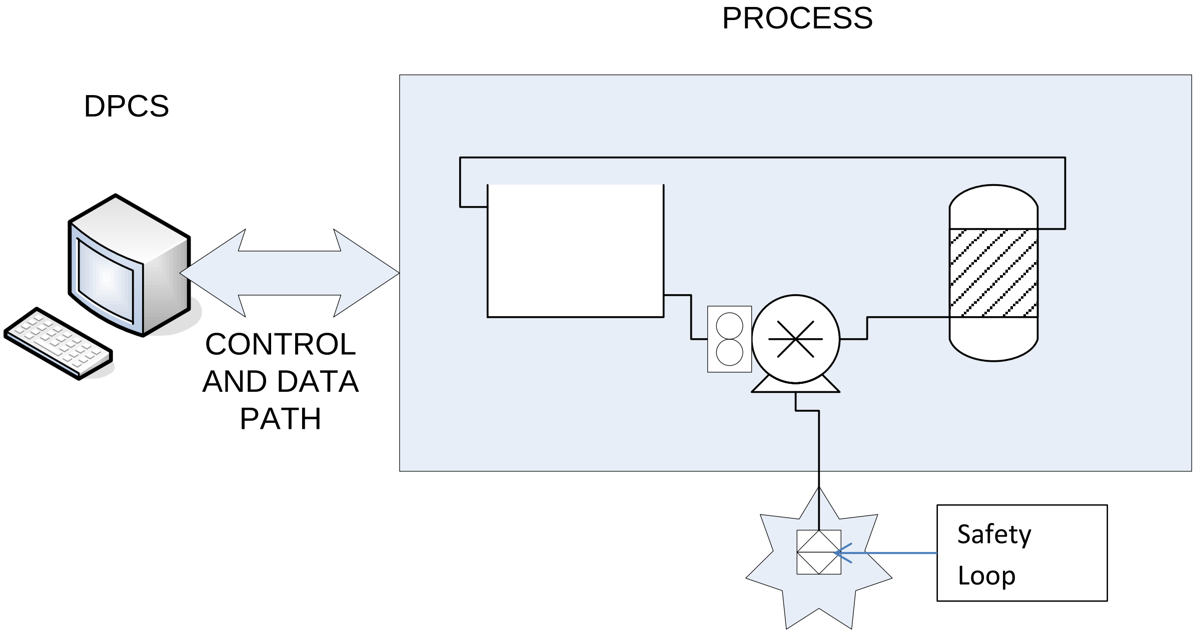
To control the reaction which is the heart of the process (maybe producing ammonia for instance) we need a DPCS, computer based system for controlling the pump and collecting useful and essential data.

Sketch Two



Sketch Two represents a functioning process producing chemical ‘X’ which can be hazardous if not kept cool enough. Controlled by DPCS.

Sketch Three



And, in this last sketch (three) the star represents an independent safety function which is the subject of BS EN 61508 – IT MUST BE INDEPENDENT! I.e. The operation of the safety function must be entirely separate from the DPCS using separate sensors and final actuator. It is not permissible to ‘share’ the final actuator and valve as this would be a common point of failure. I.e. If the final valve is ‘stuck’ then both protection AND control would be ineffective with possibly disastrous consequences.

1.1 What is SIL?

SIL stands for **S**afety **I**ntegrity **L**evel*. There are four SIL levels SIL 1, SIL 2, SIL 3 and SIL 4; SIL 1 is the lowest level and SIL 4 the highest. SIL is a parameter that is used in two ways:

1) Firstly, it is initially determined by the amount of risk reduction required by a safety function to prevent a particular hazard from occurring. This SIL determination is normally performed by the plant operator through a quantitative analysis of the potential hazard(s). More information is given in section 1.5 of this guide.

2) Secondly, once the SIL has been determined, it has implications on the design of the system that performs the safety function. In that sense, the SIL is used as a design integrity parameter for the safety-related system that has to perform the safety function. This guideline generally uses the word SIL in this sense (apart from section 1.5).

When SIL is referred to in the second sense (as a system design requirement), it is important to realise that it is a *system* parameter and its achievement cannot be fully determined by an individual element. It is therefore incorrect to claim that (for example) a valve achieves or performs a particular SIL. However, there are certain design requirements for elements (such as valves, actuators and other instruments) that can make them suitable for consideration in a system which is to be designed to achieve a particular SIL. Elements (including mass produced instruments), can therefore be characterised (through deliberate design methods and verified by assessment) for use in safety functions at certain SILs.

It is important to note that combining SIL ‘y’ capable elements does NOT guarantee a SIL ‘y’ loop as SIL does NOT work the same way as ATEX.

There are six separate assessments required to be performed before an element can be considered to be suitable for use in a system at a particular SIL. The assessment falls into two main categories which reflect the two main types of failure that systems are beset with:

Hardware Safety Integrity:

a. Probability of Failure on Demand (See Section 2 of this guide)**
b. Architectural Constraints (See Section 2 of this guide)**

Systematic Safety Integrity

c. Software/Firmware (See Section 1.2 of this guide)**
d. Realisation lifecycle
e. Techniques and Measures (See Section 2.6 of this guide)**
f. Management of functional safety

Note: ‘*’ EIL is now frequently used for ‘Environmental Integrity Level’ and AIL for ‘Asset Integrity Level’.

‘**’ indicates a direct SIL relationship.

Each of these individual assessments can limit the SIL for which the product can be used in and it is the lowest SIL estimate of the six that applies and may ultimately be claimed. The two assessments with indirect SIL relationships (d. and f.) should be viewed as ‘approved’ or ‘not approved’, if the former then a judgement will have been made by an independent assessor determining what limiting SIL the manufacturer may work to, if the latter then the manufacturer may not manufacture any SIL related equipment without first adjusting his management systems to comply with BS EN 61508-1:2010.

When calculating SIL capability for an element it is the lowest of the four assessments a, b, c and e that must be considered and it is the lowest of these that applies, assuming that compliance with d and f is achieved by the manufacturer.

Obviously the software assessment does not apply if the element / loop of interest contains no software / firmware.

For example:

We have a safety function which is implemented with a range of components and for which we have determined the following results for the four assessments a, b, c & e (it is assumed that d. and f. have been assessed and are valid for SILs up to SIL 3:

PFD = 0.015. 0.015 is within the PFD range for SIL 1

AC = SIL 3 using tables 2 and 3 of BS EN 61508-2:2010

Software/Firmware is assessed as SIL 2

Techniques and Measures is assessed as SIL 2

The lowest SIL estimate of the four is PFD which gives SIL 1; the claimable SIL for our example loop is consequently limited to SIL 1.

The same argument applies when we are assessing a single element for use in a loop only then we do not estimate a firm SIL but a SIL capability which will show whether the element is suitable for use in a safety loop. In this case it may be that the element is constructed using an actuator, a solenoid valve and a mechanical Ball valve and it has been determined that the actuator is capable of SIL 2, the solenoid, SIL 2 and the ball valve, SIL 3. The element SIL capability is SIL 2 which is the lowest of the three SIL estimates.

The hardware safety integrity assessments are concerned with the control of so called ‘random hardware failures’. These failures occur due to degradation mechanisms in the hardware which produce failures that occur at unpredictable (random) times but at predictable rates.

The systematic safety integrity assessments are concerned with failure mechanisms that are related in a deterministic way to a certain cause, which can only be minimised by deliberate design methodologies, processes, operational procedures, documentation, etc., such as the use of a Functional Safety Management System (of which ISO9001 comprises a significant contribution to compliance).

Regardless of whether the element or system uses electronic, programmable electronic or hydraulic, pneumatic etc. technology, the hardware needs to comply with BS EN 61508-2.

a. Probability of Failure on Demand (PFD)

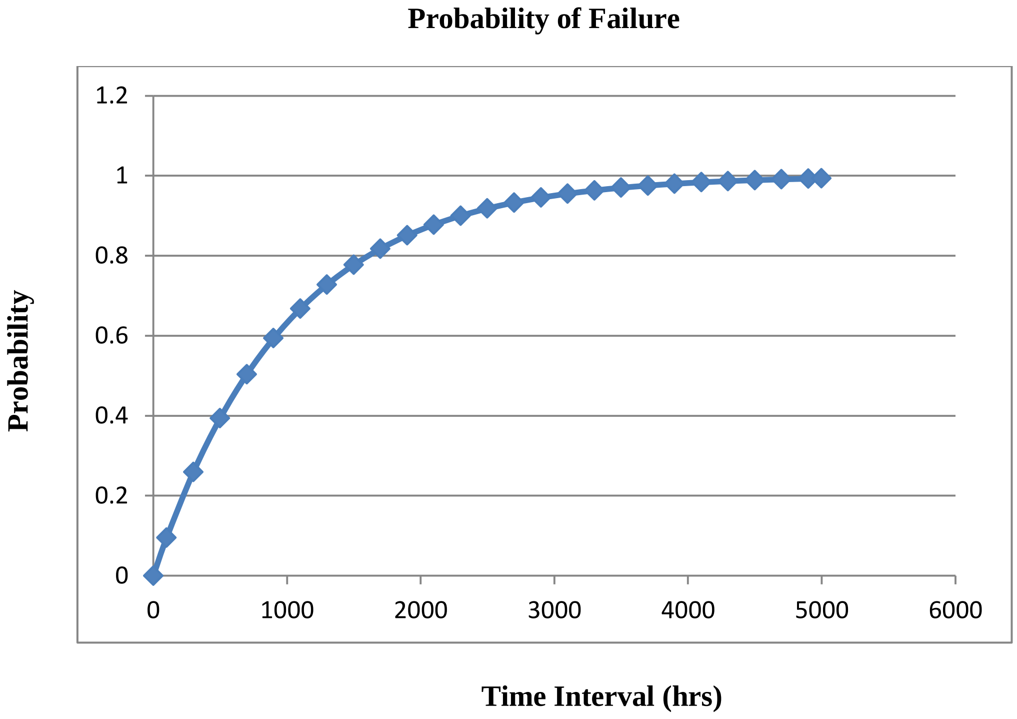


Figure One. Graph of Probability of failure to operate versus operating time

Figure One shows a graph of a probability function against time and it demonstrates the typical failure performance of a manufactured component or system. It can be seen that, as time interval increases the probability of a failure increases due to unreliability caused by random failures. In the example case the probability of a successful operation is virtually zero at five thousand hours whilst the probability of failure is close to unity. In other words by 5000 hrs the unit will almost certainly have failed. Note that wear out mechanisms are excluded from this graph.

It is this ‘probability of failure’ that is represented by PFD, e.g. a SIL of 1 represents a PFD of between 0.1 and 0.01 for a specified time interval, the specified time interval we call the proof test interval, denoted by ‘T’. Another interpretation is that a SIL 1 loop will be available to protect the process 90 - 99% of the time.

Each SIL represents a PFD range (Probability of Failure on Demand), each range covers a factor of 10 and the ranges are contiguous, hence:

Non SIL = 0 to 0.1

SIL 1 = 0.1 to 0.01 (alternatively $\geq 10^{-2}$ to $<10^{-1}$)

SIL 2 = 0.01 to 0.001 (alternatively $\geq 10^{-3}$ to $<10^{-2}$)

SIL 3 = 0.001 to 0.0001 (alternatively $\geq 10^{-4}$ to $<10^{-3}$)

SIL 4 = 0.0001 to 0.00001 (alternatively $\geq 10^{-5}$ to $<10^{-4}$)

PFD is the inverse of the Risk Reduction Factor (RRF) and consequently it can be seen that SIL 1 represents a low RRF and SIL 4 a very high RRF. (10 – 100 and 10,000 – 100,000 respectively)

These ranges are intended to provide increasing levels of dependability. For example, if a SIL 1 safety function is applied to a hazardous process in such a way that its correct operation will prevent a hazard from happening then it will provide a confidence level of 90% - 99% that the hazard will be prevented. The balance of uncertainty is due to the potential for 'dangerous' random failures of the safety function, these cannot be avoided only controlled and minimised. Hence SIL 4 is the most dependable case providing a reliability of operation of the safety function of between 99.99% and 99.999%. To achieve this inevitably means the choice of the most highly reliable components for the safety function and in fact it is impractical for most commercial applications. Where SIL 4 is essential (aircraft systems for example) it is necessary to resort to higher architectures providing multiple redundancy.

In most normal commercial processes the balance of safety functions is typically less than 20% and 80% of these are usually SIL1 or non SIL whilst the balance are SIL2. SIL3 may occur very occasionally but generally the HSE advice to the end-user is to redesign the process where a SIL3 loops is identified.

For examples of PFD assessment see 2.1.1 and 2.1.2 of this guide.

b. Architectural Constraints

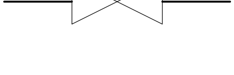
This part of the assessments compares quantified characteristics of the element with fixed tables provided within BS EN 61508 to provide a sufficiently robust architecture appropriate to the SIL.

Hardware Fault Tolerance (HFT) is a number 0 to 2 and it represents the ability of the element or loop to function in the face of a fault; HFT = 0 means that a single fault will cause mal-operation. HFT = 2 means that the element or loop can maintain function with two faults.

For Example: 1oo1 (One out of One to trip and stop the process flow)

Sketch Four shows one process valve providing an architecture of 1oo1 to trip

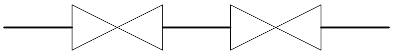
Sketch Four



For Example: 1oo2 (One out of two to trip)

Sketch Five shows two process valves providing an architecture of 1oo2 to trip

Sketch Five



In this sketch it will be apparent that either valve may close to implement the safety function and stop the process flow. Only a common mode fault would potentially prevent the safety function being completed on demand.

Safe Failure Fraction (SFF) is a percentage between 0% and 100% and is calculated using the ratio:

Safe Failure Rate / Total Failure Rate

For examples of AC assessment see 2.1.1 and 2.1.2 of this guide.

c. Software/Firmware

Software/firmware does not fail randomly it only fails when systematic failure potential has been inadvertently designed in to the software. Hence SIL assessment relies on the control of systematic failure potential using good and proven procedures and software construction methodologies.

SIL assessment of Software /firmware is an extremely complex procedure requiring the application of stringent design, development and management methodologies, including the control of systematic failures of the design and development process. It requires a high degree of expertise in the development processes for software. For the valve and actuator manufacturer it is largely not applicable unless Partial Valve Stroke Testing (PVST) is being used. PVST contributes to diagnostic capability which can potentially improve SIL capability of the valve – actuator system and hence its software must comply with BS EN 61508-3.

d. Techniques and Measures

Techniques and Measures are presented in the standard as guidance on the control of systematic failures and also what techniques make a reasonable claim for diagnostic coverage and typically how much may be claimed.

Both hardware and software require the use of certain techniques and measures that are prescribed in BS EN 61508. The use of more techniques and measures, especially those with a higher defence against systematic defects are required with increasing SIL. The application of these methods is required for the design of elements, sub-systems and complete systems.

Hardware Techniques and measures are to be found in BS EN 61508-2 Appendices and Software Techniques and Measures in BS EN 61508-3 Appendices. Hardware Techniques and Measures are discussed in more detail in section 2.6 of this guide.

1.2 A brief overview of BS EN 61508 structure and content

BS EN 61508 consists of eight parts:

0	An introduction
1	General Requirements
2	Requirements for Electrical/Electronic/Programmable Electronic safety-related systems
3	Software Requirements
4	Definitions and abbreviations
5	Examples of methods for the determination of safety integrity levels
6	Guidelines on the application of IEC61508-2 and IEC61508-3
7	Overview of techniques and measures

The essential parts that are recommended for valve and actuator manufacturers are shown in bold text below.

1.2.1 Part 0 Introduction – As the title implies this is merely an overview of the standard.

1.2.1.1 Part 1 General Requirements – This is an essential part covering functional safety management which is a mandatory requirement for those wishing to claim compliance with the standard. Functional Safety Management is essential for the control of potential systematic failures. Basically it is ISO 9001 plus. The mandatory requirements over and above ISO 9001 being:

A policy for functional safety
Management of competence
Allocation of individual responsibility
Identification and control of the potential for systematic failure
Requirement for independence of checkers and reviewers in accordance with SIL

1.2.1.2 Part 2 Requirements for Electrical/Electronic/Programmable Electronic safety-related systems – This part is also essential as it covers hardware. The title in this case is misleading as it might be taken to imply that it only covers electrical/electronic and programmable electronic systems, It actually includes the word 'systems' and in this manner it also relates to all 'elements' that might be required to form part of an Electrical/Electronic/programmable electronic safety-related system. This means that it is applicable to electrical contactors, pneumatic actuators and of course process control and shut off valves as well as any other component that might be required and which the author may have omitted.

1.2.1.3 Part 3 Software Requirements – This part is essential if software is involved in the design and operation of the element of interest. Generally not particularly applicable to valve and actuator manufacturers BUT, if 'partial stroke testing mechanisms' are involved to increase the 'Safe Failure Fraction (SFF)' claim on an

element then it will be necessary to apply the appropriate requirements of this part. In general any programmable electronic device where the software is designed to either perform the safety function or diagnose and report dangerous hardware failures will need to be compliant with BS EN 61508 parts 2 and 3.

1.2.1.4 Part 4 Definitions and Abbreviations – This part is not essential reading but the reader may find it a useful reference if the terminology of functional safety is alien to you.

1.2.1.5 Part 5 Examples of methods for the determination of safety integrity levels – This part is only of interest to those who wish to broaden their knowledge of the standard and wish, or are requested, to get involved with the determination of a loop SIL requirement. Generally, this part is of direct concern to the safety system end user and his contractor.

1.2.1.6 Part 6 Guidelines on the application of IEC61508-2 and IEC61508-3 – This part is of crucial importance to those requiring to calculate a SIL capability for a piece of equipment (an element) or a complete loop. Most of the normally applicable calculation formulae are available here for reference and use.

1.2.1.7 Part 7 Overview of Techniques and Measures – This part is not essential reading but the reader may find it a useful reference especially if software/firmware is involved.

1.3 Relevance and use of related standards

The important related standards which the valve and actuator manufacturers may come across are:

BS EN 61511 – Functional Safety – Safety Instrumented Systems for the Process Industry Sector

BS EN 61513 – Nuclear Power Plants – instrumentation and control for systems important to safety – General requirements for systems

1.2.2.1.1 BS EN 61511 – This standard is relevant to all process industries and may be used by that process industry ‘end-user’, system integrators and engineering & procurement contractors (EPC); however, its stated scope excludes suppliers and manufacturers!

This standard must not be used by the valve and actuator manufacturer for mass-produced products; if an end-user asks your company to use it then it is correct and proper for you to reject its use. The only standard that the supplier and manufacturer may use is the generic standard BS EN 61508.

1.2.2.1.2 BS EN 61513 – This standard is unique to the Nuclear Industry and, whilst the supplier and manufacturer must in the first place use BS EN 61508 it should also ensure that it understands any additional requirements of this particular standard.

1.4 The 61508 ‘approach’

BS EN 61508 is described as a ‘risk’ based standard, this is because it attempts to control and maximise functional safety by recognising, quantifying and reducing ‘risk’ to people and the environment and sometimes, informally, assets. Here’s how it does it:

Recognising:

1. **Hazards and Operability Study (HAZOP)** meetings composed of local ‘experts’ in various fields are held at end-user or contractor premises. These meetings identify as many process related hazards as possible using brain storming and key word techniques. The hazard may be over pressure in a vessel, a runaway reaction or overfilling of a tank containing toxic material. For each hazard the hazop team will determine the likely frequency of the hazardous event, the consequences, how many people are likely to be affected or what environmental affect and finally what means are available to those people to avoid the hazard or minimise the risk – for instance by wearing personal protective equipment.

Quantifying:

2. **SIL determination** meetings will follow on from the HAZOP meeting, sometimes using the same team of experts. The SIL determination team will use a suitable technique to assess the loop SIL that will be required to reduce the process risk from a particular hazard to an acceptable level. Typical methods are ‘Risk Graph’, Layer of Protection Analysis (LoPA) and Event Tree. Generally, Risk Graphs are used to provide a quick answer which is generally pessimistic and then LoPA is used to provide a more accurate assessment. Where SIL3 appears to be a necessary outcome then often Event Tree analysis is used to confirm this.
   All of these three techniques consider:
   The hazard frequency rate
   The severity of any consequence
   The avoidability of the hazard
   The impact of ‘other’ risk reduction mechanisms – such as pressure relief valves
   The exposure time of personnel to the potential risk area
   The output is the RRF of any E/E/PES that may be required. RRF is the inverse of PFD and it is PFD that is used in the allocation of SIL. However, it is the balance of RRF after all Layers of Protection have been accounted for which determines the PFD requirement for any E/E/PES loop as it is this loop which will be designed to reduce the human or environmental risk (tolerable risk) to an acceptable level.

Reducing:

3. **SIL Assessment** will be carried out on a loop by loop basis in order to confirm that the final safety loop designs achieve or exceed the determined SIL levels of 2. above. It is this process that requires the input of failure rate data from element manufacturers such as the valve and actuator industry.

The above three stages are concerned with reducing risk and the failure of the risk reduction facility due to the effect of ‘random’ failure of equipment, for example if a protective or control device breaks with the result that the protective action will not be performed – termed a dangerous failure.

This risk reduction process ensures that risk is quantified and related to socially acceptable limits calculated by the HSE but the responsibility of the end user to select and apply within these proposed limits. Once quantified, available data is used to calculate the theoretical reduction in risk due to the application of protection systems which are both passive and active. This process provides an evidential path from risk quantification to final risk reduced process and through it we are able to demonstrate that the final remaining risk is socially acceptable.

However, the risk reduction process doesn't stop there as a second essential part of the process is to control the 'introduction' of faults due to incomplete design processes. For example, many software packages are extremely difficult to fully test due to their complexity. There is no random failure effect as there is for hardware; software is either correct or faulty. If faulty then it is possible that the fault may only reveal itself under a particular set of conditions that maybe weren't for seen during specification production. All software defects are called 'systematic' failures and require careful management of development processes to minimise the potential for them to occur.

4. **Control of Systematic failures**

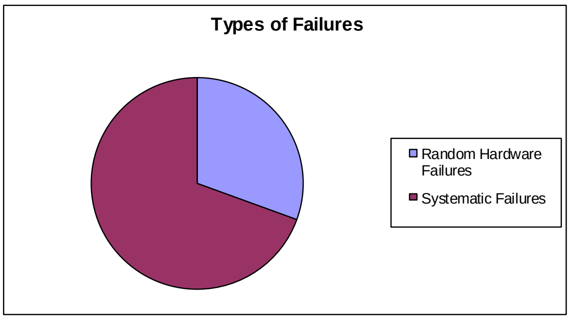


Figure Two

The results of a study of 34 industrial incidents by the HSE resulted in the chart shown above in figure two. Approximately one third of the incidents were due to random failure of equipment whilst two thirds were due to human failures in design, maintenance, specification, installation and repair, so a significant part of BS EN 61508 is applied to recognising and attempting to provide means of controlling the introduction of these problems. Hence the introduction of the concept of 'Functional Safety Management'.

Emphasis on this is introduced in BS EN 61508:2010 where **'competence assessment'** is a **mandatory requirement** along with 'specification' which now merits a section to itself. If you are building a safety element for use in a safety loop then it is mandatory to produce a clear specification for review by peers. If you are supplying and integrating a system for functional safety use to a third party then the third party is responsible for supplying a clear specification against which the system may be verified.

Control of systematic failures throughout the design and production processes requires compliance with BS EN61508-1 – see paragraph 2.6.

Note that it is also a mandatory requirement that any element proposed for functional safety use MUST be fully testable.

1.5 SIL Determination methodology

This is not a procedure that the Valve or actuator manufacturer might be expected to be involved with BUT it is important to understand the process of determining a SIL so that there is no misunderstanding when it comes to SIL verification so we describe the process for completeness:

It is usual to establish a multi-disciplinary team composed of:

Chemical Engineer
Instrument Engineer
Maintenance Engineer
Works Manager

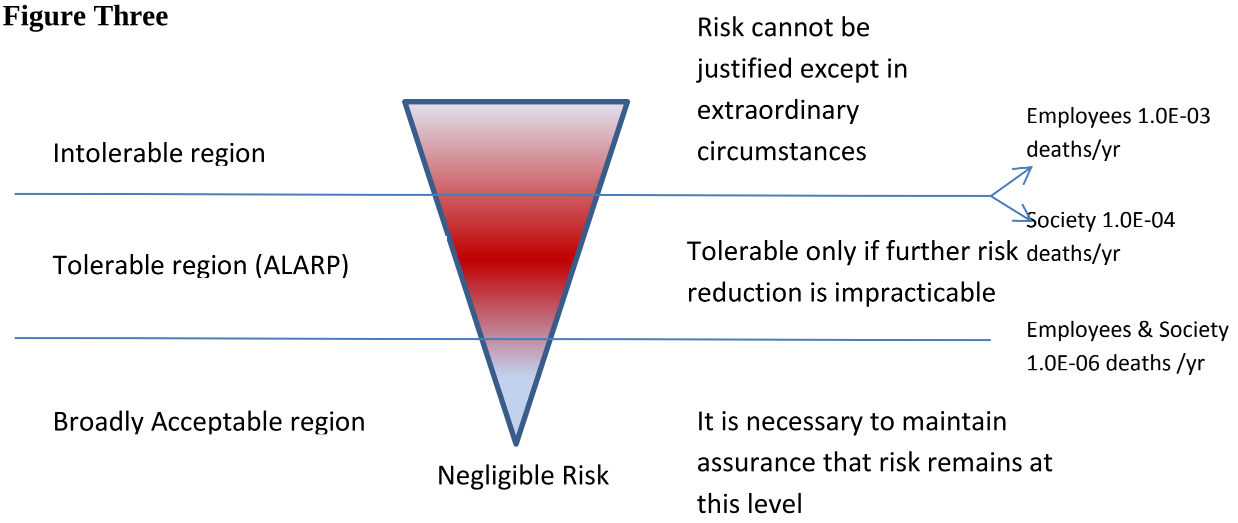
A secretary is required to keep minutes as evidence of due process.
The team should have suitable reference documentation available:

Piping and Instrumentation Diagrams (P&ID's)
Instrument Loops
HAZOP record sheets

1.5.1 Tolerable Risk

Identify the applicable societal or employee 'tolerable' risk, BS EN 61508:2010, table B.1 provides guidance on choosing an appropriate figure. See table B.1 repeated below for information:

Figure Three


Risk cannot be justified except in extraordinary circumstances
Intolerable region
Employees 1.0E-03 deaths/yr
Society 1.0E-04 deaths/yr
Tolerable region (ALARP)
Tolerable only if further risk reduction is impractiable
Employees & Society 1.0E-06 deaths /yr
Broadly Acceptable region
It is necessary to maintain assurance that risk remains at this level
Negligible Risk

HOWEVER, NOTE THAT RESPONSIBILITY FOR THE CHOSEN TOLERABILITY LEVEL MUST BE WITH THE COMPANY BOARD OF DIRECTORS OR A BOARD MEMBER.

Guidance would be to start with a tolerable individual risk of 1.0E-06 deaths/yr for both employees and society, however, if a particular process is close to public areas such as schools, office buildings, etc., then it may be prudent to start with a much lower figure, e.g. 1.0E-08 deaths/yr.

If this results in impractical SIL levels then it will be necessary to reconsider the effects of the hazard and if necessary move the process further away from the public areas, erect blast walls or take whatever actions are necessary to reduce the consequences of the hazard as it may affect the public.

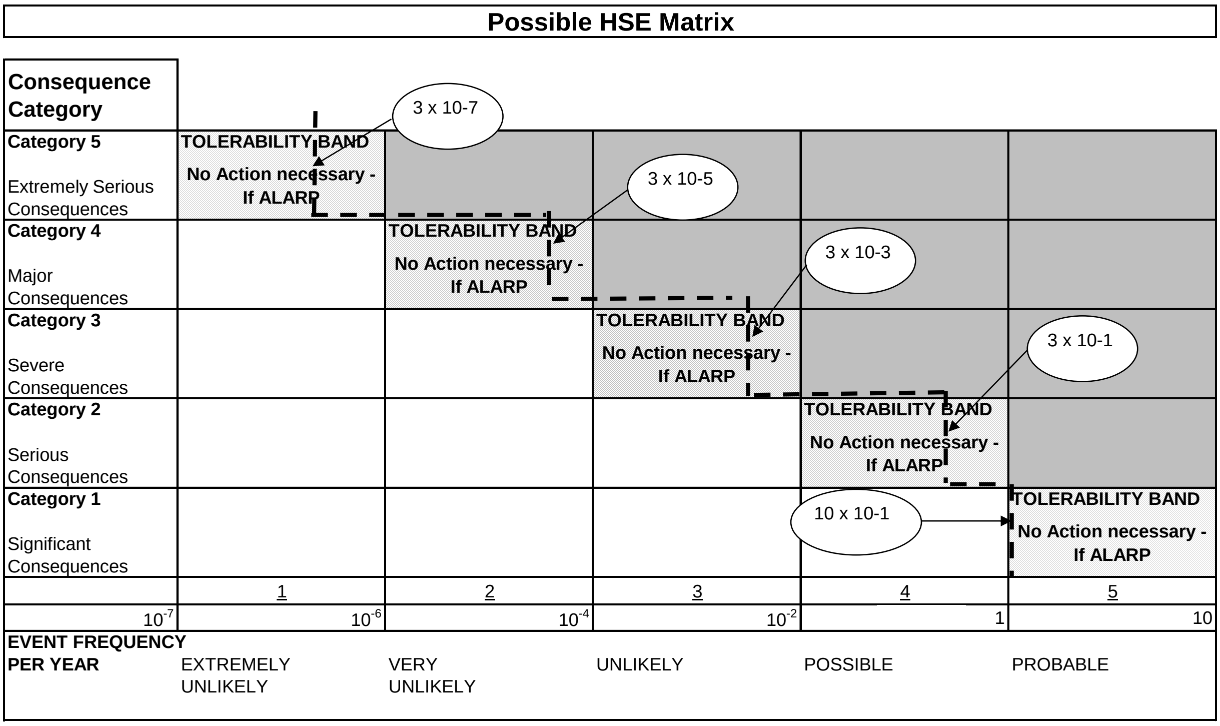
1.5.2 HSE Matrix Guidelines

The LoPA team should first establish a suitable, relevant HSE Matrix relating a consequence category to an event frequency per year, for example:

Figure Four

Possible HSE Matrix Guidelines

	Safety Effects	**Health Effects**	**Air**	**Liquid**
Category 5 Extremely Serious	>=5 employee/contractor fatalities Fatality/fatalities offsite or many serious injuries	Health risk to employee/contractors unacceptable due to continuous or discrete large releases	Release of large quantity of carcinogenic /toxic material Major damage to wildlife Large scale offsite evacuation	Major loss of very harmful or toxic liquid 5-10 mile district effect Major accident as per COMAH
Category 4 Major	<5 employee/contractor fatalities onsite >5 serious injuries/hospitalisation offsite	Exposure of employees/contractors to high levels of carcinogens >2*OEL	Repeated releases affecting off-site areas for >15 mins Explosion shock wave, Large Dust or soot fall out	Large Loss of listed substances Disturbing visible evidence - foam, colour, oil slick - up to 1 mile from release point Fish Killed
Category 3 Severe	>=5 Major employee/contractor injuries <5 serious injuries/hospitalisation offsite	Distressing onsite exposure Irreversible unacceptable health effects Sensitisation effects Exposure to carcinogens above 2 *OEL	Fire and smoke affecting off-site areas for >15 minutes Explosion shock wave, Large Dust or soot fall out	Significant amount of listed substance lost More than 2 times consent limit Definite visible evidence Low fish kill potential
Category 2 Serious	Recordable (lost time) employee/contractor injury	Persistent onsite releases above limits - 2 to 5 times occupational limits of non-carcinogen	Sustained nuisance - noise, unpleasant and persistent smell, dust, soot fall out, including flaring or venting.	Upto 2 times consent limit
Category 1 Significant	Recordable (Medical) employee/contractor injury	Occasional onsite releases above occupational limits - OEL Unpleasant onsite working conditions	Short duration nuisance -unusual noises - smoke, offensive smell - flaring or venting leading to the above	Spillage mostly contained Small amount lost to site drain. Possible visible effect in nearby rivers Within or slightly outside consent limits



Possible HSE Matrix

Consequence Category					
Category 5 Extremely Serious Consequences	**TOLERABILITY BAND** **No Action necessary - If ALARP**	▨	▨	▨	▨
Category 4 Major Consequences		**TOLERABILITY BAND** **No Action necessary - If ALARP**	▨	▨	▨
Category 3 Severe Consequences			**TOLERABILITY BAND** **No Action necessary - If ALARP**	▨	▨
Category 2 Serious Consequences				**TOLERABILITY BAND** **No Action necessary - If ALARP**	▨
Category 1 Significant Consequences					**TOLERABILITY BAND** **No Action necessary - If ALARP**
	1	2	3	4	5
10^{-7}	10^{-6}	10^{-4}	10^{-2}	1	10
EVENT FREQUENCY PER YEAR	EXTREMELY UNLIKELY	VERY UNLIKELY	UNLIKELY	POSSIBLE	PROBABLE

NOTE: THIS IS AN EXAMPLE ONLY AND MUST NOT BE USED AS THE BASIS FOR A PRACTICAL LoPA.

It is important that the LoPA team generates its own HSE Matrix with which to classify and quantify consequence and tolerability levels and documents the reasoning behind its choice. For the purpose of this guideline we will assume the use of the example.

Explanation:

For a Category 1 consequence the team has determined a tolerable frequency of the event of 1 to 10 times per year and that its safety effect relates to a recordable injury such as a cut or abrasion to an individual be it contractor or employee but not a member of the public.

In environmental terms the equivalent may be smoke, offensive smell, etc. into the atmosphere causing a short term nuisance or a mostly contained spillage where a small amount goes to site drain and may slightly exceed consent limits.

For Category 5 we have the opposite extreme where the consequence is in excess of 5 employee/contractor fatalities and there may be fatalities or at least serious injury offsite, i.e. to members of the public. The tolerable frequency of this extremely serious event is determined to be between once every million and once every 10 million years. For the purpose of the LoPA the team has selected a representative frequency of once every 3.3 million years.

1.5.3 Layer of Protection Analysis (LoPA)

Preliminary

a. Document the Event description, For Example:
"Flame Off and gas still admitted to the machine"
b. Document the Event Consequences, for Example:
"Explosion in the boiler or the gas turbine – potential for flying debris and serious injury to multiple persons including operators and members of the public".
c. Allocate a target frequency using the constructed Company HSE matrix (see example on page 19)
d. Define the proposed safety function trip action – Note that the chosen safety function must be capable of preventing the event documented in a) and b) above.

Initiating Causes
Units are Frequency/year.
a. Document all the possible initiating causes for the subject event.

For example – human error. A source of failure rate data suggests that an operator might fail to respond to an alarm once every 10,000 times that alarm is raised. Hence the frequency to be applied would be related to the expected number of alarms per year. The team might, from experience, claim that such an alarm is raised once per hour, in which case the annual frequency would be approximately 1.0/yr.

b. Repeat the above with any further initiating cause that might be recognised.

Independent Layers of protection

a. Consider which parts of the process design might contribute to preventing the event happening. Independent Layers of Protection have units of PFDaverage.
   Typical parts may be:
   1. A Distributed Control System (DPCS) – would in normal operation respond to a sensors in order to maintain the process operating normally by opening/closing final actuators to steer the process away from danger or, in the event of a serious deviation, take action to put the process in a safe 'low' energy' state. The BS EN 61508 daughter standard for the process industry, BS EN 61511, allows a PFD claim of 0.1, i.e. a probability of failure on demand of once in every ten demands. The actual figure is 0.0995, notice that this is just short of SIL1. So SIL 1 <u>cannot</u> be claimed for a DPCS.
   2. Occupancy – in the absence of operators and maintenance personnel the event may not be lethal in consequence. It may be a financial hazard but it would not injure or kill anyone. The proportion of time that personnel is close to the event location must be considered as potentially lethal, hence if an operator only spends 0.5 hr of his shift in the lethal area then credit may be given in reducing his risk. 0.5 hrs every day would be a probability of being in the event location, in the event of the hazard occurring, of 0.5 hr per 24 hours. Assuming a shift rota of six days per week and six weeks annual leave this would be a probability of 138 hours – in 8760hrs (1 year) or 0.016.
   3. Other possible layers of protection in general are:
      i. Pressure relief valves
      ii. Check Valves
      iii. Bund Wall
      iv. Gas Detection
      v. Flare stack

b. Note that selected layers of protection must be capable of either preventing the hazardous event or reducing the consequences AND each layer MUST be independent of the next. It is clearly incorrect to claim several layers of protection which are related so that if one fails some of the others do too. Independence is crucial.

1.5.4 Selection of the required SIL

a. Once a list of initiating causes and independent layers of protection have been established the following calculations are carried out to determine the total risk reduction (RRF = Risk Reduction Factor) in the absence of a E/E/PES safety function:

  i. Multiply the frequency/year of every initiating cause by the relevant independent layers of protection, this may give you anything from one to ten or twelve results depending on the complexity of the process.
  ii. Sum all results of i. and this is the actual predicted event frequency as modified by the independent layers of protection.
  iii. Divide the selected tolerable frequency by the total event frequency of ii. and the PFD of the existing protection systems result. This figure may then be related to SIL using table 2 of BS EN 61508.

Table One

"Table 2 of BS EN 61508 represented here for clarity (for Low demand mode of operation):"

Safety Integrity level	**Low demand mode of operation** (Average probability of failure to perform its design function on demand)
4	$\geq 10^{-5}$ to $<10^{-4}$
3	$\geq 10^{-4}$ to $<10^{-3}$
2	$\geq 10^{-3}$ to $<10^{-2}$
1	$\geq 10^{-2}$ to $<10^{-1}$

If it is less than the figures shown in the table (see above) then the process risk is too high to be satisfied by an E/E/PES system and other means must be found to reduce the risk, generally by redesigning the process or re-siting the process to an area where there is less risk to the public or removing operators completely away from the hazardous area. If it is higher than the figures shown in the table then the tolerability level is already acceptable, the risk to the onsite staff and offsite public is low enough to be acceptable without the further addition of an E/E/PES system.

  iv. Finally note down for future reference, all the sources of data that have been used and keep them together with the SIL determination records.

Note 1, The process risk is required legally to be, '**A**s **L**ow **A**s **R**easonably **P**racticable' (ALARP), that is, if the risk can be further reduced by a relatively small amount of cost then the process operator is required by law (Health and Safety at Work Act) to incur that cost and minimise the risk. However, if the cost of reducing the risk further is disproportionate to the risk reduction achieved then no further work is required provided that the risk is within the tolerable region as shown in figure three above.

Note 2, The determined SIL should be viewed as a snap shot in time so that, if any of the process details change or are found to be incorrect then it will be necessary to re-visit the LoPA process to determine whether the implemented safety systems are still adequate. By process details we mean:

1. Failure rates of LoPA elements greater than assumed during the LoPA process;
2. Frequency of the hazardous event being greater than that predicted during the LoPA process.

Note 3, It may be that the event frequency is so much higher than assumed that it must be considered to be operating in a continuous mode of operation. This is not usually the case for a well-designed process in which actuators and valves may be used and consequently continuous mode has not been dealt with in this guide.

The reader is advised that a similar SIL determination process is required but using a different approach. Table 3 of BS EN 61508 is the appropriate table to use but because continuous mode applications are often cases of machinery safety the reader is advised to reference a companion BVAA guideline, ‘Guidelines on the interpretation of The Machinery Directive for the Valve and Actuator Industry’.

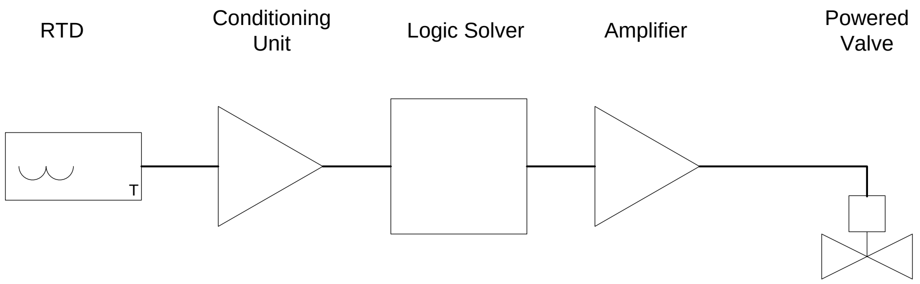
PART 2: APPLICATION OF BS EN 61508 TO VALVE AND ACTUATOR MANUFACTURERS

2 SIL Assessment methodology

The following is not essential reading to members of the Valve and Actuator fraternity but it may be useful if you want to understand how the characteristics of your product are required to enable a SIL calculation to be performed.

2.1 The Instrument loop

Sketch Six



Element 1 element 2 element 3 element 4 element 5

Sketch Six represents the possible construction of a safety function such as that shown in Sketch Three shown in safety loop form, its safety function, in this case, is to close the powered valve when the temperature sensor detects a temperature above 200^{o}C. It is composed of five elements and its architecture is 1oo1 (should be read '**One-o**ut-**o**f- **One** to trip', meaning that fault tolerance =0, a single fault may be safe or dangerous and will either cause a spurious trip or a dangerous failure), i.e. there is no redundancy and the first high excursion of the sensor will trip the safety function providing all components are healthy:

Element 1 Resistance Temperature Detector (RTD)

Element 2 Resistance temperature detector conditioning unit to convert resistance to mA.

Element 3 A Logic solver, in this case a comparator which will detect when the mA level out of the RTD Conditioning unit exceeds a current equivalent to 200^{o}C and change the output from a logic 'hi' to a logic 'lo'. Note that when a safety function is designed it is generally essential that the output goes to a logic zero to implement the safety function. There are exceptional cases where this is not so but these are rare and for very special circumstances. The reason is that on loss of power or component failure (which will generally cause a low output though not always) the safety function is performed.

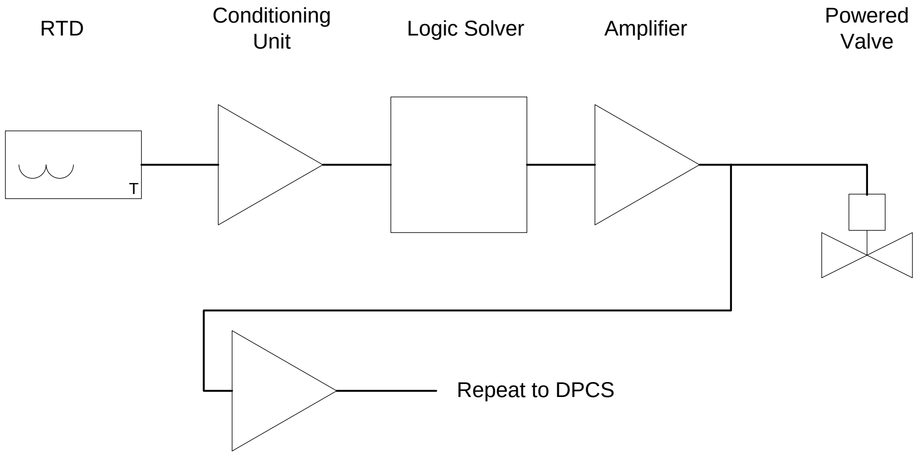
Element 4 The amplifier, in this case, merely provides a logic output capable of driving the powered valve which may require 12Watts or more.

Element 5 The final actuator which will implement the safety function. It is a powered valve (maybe a solenoid valve) in this case but this is not always the case and across the process industry it could be a variety of valve and valve actuator types or electrical contactors (to stop electrical pumps etc.)

In this example every element is critical to the safety function and consequently all five elements must be assessed in the SIL assessment. However, other loops may contain elements that do not contribute directly to the safety function; Sketch Seven illustrates such a loop. In this case the assessment mirrors that for Sketch six except that the effect of the additional element providing the Distributed Process Control System (DPCS) repeat must be considered, it is not part of the safety loop BUT its failure could affect the safety loop! For instance if a fault (in the DPCS repeat) caused its input to freeze at some fixed voltage then the output of the solenoid driver amplifier would also be clamped to that voltage with the result that the solenoid valve would be either held active (assuming the fault voltage was recognised as a logic ‘high’) OR would be de-activated (if the fault voltage was recognised as a logic ‘low’). If we make the assumption that the solenoid must be de-activated to initiate the safety function then the former (logic ‘high’ would be a dangerous failure as the solenoid would not turn off on demand, and the latter a spurious trip as the safety function would be initiated unnecessarily.

This example should show the importance of considering the direct safety path first of all and then examining all ancillary components to see whether they have the capability to influence the safety loop indirectly.

Sketch Seven



Once the safety loop is fully understood it is necessary to allocate failure modes and failure rates to each component, remembering that the safety function is to close the powered valve on demand hence for SIL we are only interested in those failure modes which will maintain the valve in a powered condition:

2.1.1 Example One

Calculation of PFD, the first part of the SIL assessment process.

Considering Sketch six in the first place and assuming that there are no diagnostics and therefore all failures are ‘undetected’.

Table Two

Element No.	**Description**	**Relevant** Failure Mode**	**Proportion of total element failure rate**	**Total Failure Rate, FIT***	**Architecture**	**Common Mode Factor, β**	**Dangerous Failure Rate, FIT***
1	RTD	Low or stuck	95%	5000	1oo1	Not applicable	4750
2	Conditioning unit	Low or Stuck	40%	2000	1oo1	Not applicable	800
3	Logic Solver	High	68%	367	1oo1	Not applicable	250
4	Output Drive Amp	High	0%	86	1oo1	Not applicable	0
5	Powered Valve	Open	25%	4000	1oo1	Not applicable	1250
			Summation	11453			7050

'*' FIT (Unit known as 'Failures in Time') = 10^{-9}/hr

'**' Relevant to Dangerous Failures.

Summing the figures in column 8 gives us 7050 FITs and Column 5 gives us 11453FITs.

The first figure is the dangerous failure rate for the complete safety function (i.e. failure to close the valve on demand) whilst the second figure is the total failure rate. The difference between 'Total failure rate' and 'dangerous failure rate' is, in this case, the 'safe failure rate'.

Note that a practical fmeda will generally identify many failures as 'no effect failures', for example – a label falling off. These are not considered when calculating Probability of Failure on Demand as they are not 'safe failures' as defined by BS EN 61508. This figure of 'no effect failures' will appear in the total failure rate when extracting failure rate data from generic sources such as Reliability, maintainability and Risk [Ref 1] but it must NOT be used and therefore for the purpose of Functional Safety calculations **total failure rate** $\lambda_{total} = \lambda_{SU} + \lambda_{SD} + \lambda_{DU} + \lambda_{DD}$ where λ_{total} = (generic total failure rate – $\lambda_{no\ effects}$).

NOTE:

We give these figures Greek letters, λ represents a failure rate and various subscripts define the precise type of failure rate, hence:

λ_{total} is the sum of all failure rates neglecting no effect failures ($\lambda_{no\ effect}$)

λ_{SU} = Safe undetected failure rate, i.e. those failures that are safe and would cause a spurious trip but remain undetected until the spurious trip occurs. Such failures do not have the potential to put the safety related system into a hazardous or fail to function state.

λ_{SD} = Safe detected failure rate, i.e. those failures that are safe and would cause a spurious trip but are detected prior to the spurious trip occurring. Such failures do not have the potential to put the safety related system into a hazardous or fail to function state.

λ_{DU} = Dangerous undetected failure rate, i.e. those failures that have the potential to put the safety related system in a hazardous or fail function state but that remain undetected until revealed by either proof test or a demand on the safety function which is unfulfilled and results in the unwanted hazardous situation. Hence this is a dangerous failure.

λ_{DD} = Dangerous detected failure rate, i.e. those failures that have the potential to put the safety related system in a hazardous or fail function state but that are detected (perhaps by internal diagnostic software) and either the fault is alarmed to the operator so that repair is performed within the MTTR (Mean time to repair) period OR the safety related system is caused to implement the safety function putting the associated process in a safe state where the hazard cannot occur.

$\lambda_{no\ effect}$ = No effect failure rate, i.e. those failures that will never have the potential to put the safety related system either in a hazardous or fail function state NOR do they have the potential to cause a spurious trip. Such failures are associated with less critical components such as labels. **These failures will be counted in an MTTF (Mean Time To Failure) but must not be counted as safe failures in a SIL related calculation.** MTTF is the sum of all failures for an element, a related figure MTBF (Mean time Between failures) is related as follows:

MTBF=MTTF+MTTR where MTTR = Mean time to repair.

We can now calculate SIL according to Probability of Failure on Demand (PFD) and Architectural Constraints (AC).

For a 1oo1 architecture dangerous failure rate λ_D is related to PFD by the equation:

$$PFD = \lambda_D\ T_{1/}2$$

This is for a simple system with no revealed failure rates, hence λ_{DD} and $\lambda_{SD} = 0$.

$\lambda_D = \lambda_{DU} + \lambda_{DD,\,,}$ so we know that $\lambda_D = 7050\ x10^{-9} + 0$

The proof test interval is usually selected according to the end users requirements but overruled by the need to achieve the determined Risk Reduction Factor (RRF) for the particular safety function. (RRF=1/PFD)

Often the end user will ask for the proof testing to be carried out at his normal ‘outages’ i.e. when his plant would normally be shut down to carry out essential maintenance, often every 2-3 years.

For a critical safety system such a long proof test interval may not achieve the desired SIL, in such a case the end user is obliged to interrupt his production or find inventive ways of performing a proof test without shutting the process down completely. Higher architectures can be helpful in this case.

Manufacturers of instrumentation generally assume a proof test interval of 1 year (8760 hours) when performing calculations to determine the SIL ‘capability’ of their instrument. We will use 1 year in the first case but aim for application at SIL 2.

Hence, PFD = 7050 x 10^{-9} * 8760/2 = 0.031 – Referring to Table One, this PFD value is in the range ($\geq 10^{-2}$ to $<10^{-1}$) 0.1 to 0.01 which is SIL1 with a RRF of 1/0.031 = 322. This falls short of the required SIL2 and consequently a shorter proof test interval may be necessary (alternatively we could investigate loop elements with better failure characteristics).

It may be determined that a three month proof test interval gives a SIL2 result:

PFD = 7050 x 10^{-9} * 2190/2 = 0.00772.

This figure is now in the range of PFD for SIL2, ($\geq 10^{-3}$ to $<10^{-2}$).

This completes the first part of the SIL assessment process.

Architectural constraints – the second part of the SIL assessment process.

For this part of the assessment we need to determine a ‘type’ and use the tables of BS EN 61508-2, paragraph 7.4.4.2.2.

Table Three

Reference BS EN 61508 paragraph 7.4.4.2.2 Table 2, page 26.

“Table 2 – Maximum allowable safety integrity level for a safety function carried out by a **type A** safety-related element or sub-system”

Safe failure fraction of an element	Hardware Fault Tolerance		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % - < 90 %	SIL 2	SIL 3	SIL 4
90 % - < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Table Four

Reference BS EN 61508 paragraph 7.4.4.2.2 Table 3.

"Table 3 – Maximum allowable safety integrity level for a safety function carried out by a **type B** safety-related element or sub-system"

Safe failure fraction of an element	Hardware Fault Tolerance		
	0	1	2
< 60 %	SIL 0	SIL 1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Discussion of type

The following are references from BS EN 61508-2:

BS EN 61508-2, para 7.4.4.1.2: An element can be regarded as type A if, for the components required to achieve the safety function

a. *the failure modes of all constituent components are well defined; and*
b. *the behaviour of the element under fault conditions can be completely determined; and*
c. *there is sufficient dependable failure data to show that the claimed rates of failure for detected and undetected dangerous failure are met.*

BS EN 61508-2, para 7.4.4.1.3: An element can be regarded as type B if, for the components required to achieve the safety function

a. *the failure modes of all constituent component is not well defined; or*
b. *the behaviour of the element under fault conditions cannot be completely determined; or*
c. *there is insufficient dependable failure data to support claims for rates of failure for detected and undetected dangerous failure are met.*

Unless your Company has a competent, experienced person who can make this selection with confidence it is probably best to employ the services of an independent competent and experienced person. However, in general for mechanical devices such as valves and actuators it is most likely that the conditions for type A will be met provided an fmeda (failure modes diagnostics and effects analysis) has been competently performed. Type B is normally associated with complex electronic equipment which may well contain a microprocessor(s) and consequently firmware/software. It is this type of device where a multiplicity of failure modes exist and which cannot be fully tested that is the reason for type B. As always where functional safety is concerned, if you are not sure then assume the worst case until you can prove otherwise.

Selection of SIL according to Architectural Constraints (AC)

Referring to Tables three and four it can be seen that there is a vertical column labelled SFF (Safe Failure Fraction) of an element and a horizontal row labelled Hardware Fault Tolerance.

To deal with Hardware fault Tolerance first, we must know the redundant capability of the loop. In our two examples the architecture is 1oo1 and this means that there is NO redundancy, i.e. HFT = 0. For the purpose of the examples we are therefore concerned only with column two where the heading is HFT = 0.

Selection of SFF

SFF must be calculated using the relationship:

$$\frac{\text{Sum of Safe Failures}}{\text{Sum of all failures}}$$

Using the Greek lettering nomenclature this ratio may be further defined as:

$$\frac{\lambda_{SU} + \lambda_{SD} + \lambda_{DD}}{\lambda_{SU} + \lambda_{SD} + \lambda_{DD} + \lambda_{DU}}$$

For this example we have no detected failures and hence we can reduce the ratio further:

$$\frac{\lambda_{SU}}{\lambda_{SU} + \lambda_{DU}}$$

Entering the data from Table Two gives

$$\frac{11453- 7050}{11453} = 38\ \%$$

The SFF of our safety function of example One is 38%. Referencing Table Three above we can see that HFT = 0, SFF = 38% so **SIL1** is the maximum that may be claimed for Architectural Constraints

Result: SIL 1 is the estimate for Architectural Constraints and SIL 2 for the PFD hence, with reference to BS EN 61508-2:2010, 7.4.4.2.1, the highest loop SIL that may be claimed is SIL 1.

As SIL 2 was the target it would now be necessary to redesign the loop using elements possessing a higher individual SFF. Reference to Table Two should show that elements one and three were the limiting factors for this particular loop design. Element one having a SFF of only 5% (without diagnostics) and element three having an SFF of only 32%.

This is a pessimistic example used to illustrate the loop SIL assessment process, however, in practice sufficient diagnostic would normally be available in element two to detect open/short circuit failure of element one (the RTD) and thus increase its SFF to >60% whilst element three is simply a poor choice of logic solver and must be replaced.

2.1.3 Example Two

Considering Sketch Seven and assuming that there are no diagnostics and therefore all failures are ‘undetected’.

Table Five

Element No.	Description	Relevant Failure Mode**	Proportion of total failure rate	Total Failure Rate, FIT*	Architecture	Common Mode Factor, β	Dangerous Failure Rate, FIT*
1	RTD	Low or stuck	95%	5000	1oo1	Not applicable	4750
2	Conditioning unit	Low or Stuck	40%	2000	1oo1	Not applicable	800
3	Logic Solver	High	68%	367	1001	Not applicable	250
4	Output Drive Amp	High	0%	86	1oo1	Not applicable	0
5	Powered Valve	Open	25%	4000	1oo1	Not applicable	1250
6	DPCS Repeat	Logic High appears at the input	10%	500***	Not applicable	Not applicable	250
			Summation	11953			7300

‘*’ FIT = 10^{-9}/hr

‘**’ Relevant to Dangerous failures

‘***’ This total failure rate is ONLY for the failures that affect the input NOT the whole of the element – this is because it is only the input that (in this case) might affect the safety loop.

Summing the figures in column 8 gives us 7300 FITs and Column 5 13953FITs.

The first figure is the dangerous failure rate for the complete safety function (i.e. failure to close the valve on demand) whilst the second figure is the total failure rate (ignoring no effects failures).

This calculation follows Example One precisely with the addition of the failure rate for the DPCS repeat input which adds an additional dangerous failure rate of 250FIT. The reader is recommended to repeat the calculations of Example One and show that the PFD is now 0.00799 and the SFF is 38.9%.

The results are, of course, still unacceptable for SIL 2 and it will be necessary to take the same steps in redesigning the loop.

2.1.2 The data that an actuator and valve manufacturer need to supply so that the end user can do the calculations of 9.1.1 and 9.1.2

The loop calculations used failure modes and failure rate data to calculate the loop SIL and to show that the safety function achieved its target and the input to those calculation is failure mode and failure rate data for each element of the loop. It is this data that the ‘system builder’ should be requesting of the valve and actuator manufacturer NOT a SIL!

The full list is given in BS EN 61508-2, 7.4.9.3, 7.4.9.4 and Annex D but this includes at least the following:

Permissible modes of use (e.g. Fail open, fail close for a typical ESD valve)

Safe Failure rates for each permissible mode of use

Dangerous failure rates for each permissible mode of use

Identification of any detected (revealed) failure rates for each mode of use

Fault Tolerance

Safe Failure Fraction for each permissible mode of use

A Restrictions in use report (which includes all the above)

Recommended minimum proof test interval and a recommended proof test.

Mean Time to Repair

A recommended maintenance interval and identification of all wear out mechanisms such as gaskets, seals and valve seats.

The information above is generally contained in the Safety Manual (see BS EN 61508-2 Annex D) and should be available with every element to facilitate its safe selection, integration, installation, operation and maintenance.

2.2 Finding Failure Rate Data

2.2.1 Sources and discussion

There are many sources of failure rate data but for them to be useful to your particular application they have to be relevant. Much failure rate data is derived from the military which keeps excellent records and the resulting data can be found in works such as NPRD (Non Electronic Parts Reliability Database)Ref[9] produced by the Department of Defence of the U.S.A. This work is available off the internet for around $200 (March 2013). It is potentially useful to the valve and actuator industry covering as it does, such items as springs and washers, rubber seals etc. The downside of this data source is that most component data is derived from military applications on vehicles and consequently may not be entirely relevant to the valve and actuator industry. As always though, when considering reliability, any source of data is some use as it can help by providing typical data for comparison purposes. It is then a judgement whether the application being considered is liable to be less or more harsh and therefore whether the data may be used as a first pass.

Works such as 'Reliability, Maintainability and Risk **Ref.[1]'** by Dr David Smith offer some excellent generic data for electrical and electronic equipment, although not so much for mechanical, but again the key is to obtain a wide variety of data sources and look for commonality in results or merely use worst case data as a starting point.

'Safety Equipment Reliability Handbook **Ref[.10]**' by Exida provides a mix of composite failure rates for items such as valves, actuators and various instruments. You as a representative of the valve and actuator industry will not have much need of the instrument data but the valve and actuator failure rates should help by providing comparative information. A similar design of ball valve, for instance, might be expected to present similar failure modes and characteristics.

OREDA$_{\text{Ref[11]}}$ provides failure rate data from the offshore oil and gas rigs and provides another excellent reference source for comparative use.

Ideally, the best failure rate data is that applying to the equipment designed and built by your own Company and determined by testing.

However, it is your Companies responsibility to establish failure rate data for use in the FMEDA and provide validation information in support. Being statistical in nature it is unlikely that you will ever have precise failure data +/- 0.1%! It is establishing a data set that is important, and then maintaining that set and adjusting it as supporting or contradictory evidence presents itself.

Field returns data is often cited in SIL claims. This data is generally unacceptable, especially for valves where process fluids, environments and operating temperatures can vary enormously. However, it is some use as calibration. If the field data is consistently worse than that being used or predicted in FMEDA then clearly your first assumptions were incorrect and must be revised.

If you are to make guarded use of field returns then make sure that you have allowed for shelf time – it may be you supplied it 5 years ago but has it been sat on a stores shelf for 4 years. Unless the valve is very large and expensive and is unlikely to be merely thrown away – make sure that you make allowances for end-users merely scrapping faulty out of warranty components.

Finally, do try to establish a relationship with your end-users and encourage them to provide you with their own field statistics – it is considerably to their advantage.

If none of the above is able to provide a source of reliable failure rate data then it is permissible to establish a team of experienced company design, material and maintenance engineers and use brain storming methods to make an objective estimate of failure rate. It is essential that the meeting is documented and that, should circumstances result in a challenge to any value so determined the team is able to re-address the problem and agree a modified estimate. In practise you will probably find that most valve and actuator components have a very low failure rate and that an FMEDA will be dominated by just one or two components. For example a typical valve spring may have a failure rate of between 0.1 x 10^{-6} and 0.5 x 10^{-6} failures per hour $_{\text{REF[8]}}$ whilst failure of a valve body casting may well be 1 x 10^{-10} failures per hour $_{\text{REF[5]}}$; clearly any FMEDA will be dominated by the spring failure value. Similarly a typical 'O' ring $_{\text{REF[8]}}$ has a failure rate of 0.02 x 10^{-6} to 0.5 x 10^{-6} failures per hour. These figures are several orders of ten worse than the valve body hence making any 'estimate' of valve body failure rate unimportant – though they should still be listed and a value applied purely for completeness.

2.2.2 Interpreting Failure Rate Data

Failure rate data is usually presented in a complex manner and in one or two units.

a. FIT = Failures in Time and is interpreted as 1 x 10^{-9} failures per hour
b. Per hour – usually this implies 10^{-6} failures per hour

Failure rate data is statistical; its reliability relies on the size of the sample. A large sample (>10 results) would imply reasonable accuracy. A small sample (<5) would imply that the sample is liable to be unrepresentative.

Often data is presented in the following manner (for example "Reliability, Maintainability and Risk" Ref.[1]):

0.01 1 100

This is interpreted as:

Best prediction from available data = 0.01 x 10^{-6} failures per hour

Worst prediction from available data = 100 x 10^{-6} failures per hour

Geometric Mean = 1 x 10^{-6} failure per hour

Such a wide spread of results might imply a small sample database and hence beware. BS EN 61508 requires that failure rate data has a 90% confidence interval, i.e. λ is the interval $\lambda_{5\%,}$ $\lambda_{95\%}$ there is only a 5% probability that the actual failure rate will be better than $\lambda_{5\%}$ and worse than $\lambda_{95\%.}$

As a practical guide without recourse to in-depth statistics Geometric Mean (GM) is reckoned to be the most representative figure and if it is not available in the data base you have it may be calculated by

GM = √ (L*H), where √ is the square root, L is the lowest reliability value and H is the highest reliability value.

Hence L = 0.1 x 10^{-6}, H = 1.0 x 10^{-6} gives GM = 0.316 x 10^{-6}.

However, a wise starting point is to use the worst case data in the first place and then investigate environmental factoring.

2.2.3 Factoring

Generic Data may or may not be representative of the application that you are required to consider. Data such as that provided by "Dr David Smith in his book "Reliability, Maintainability and Risk Ref[.]1" and his database "Faradip Ref.[8]" are derived from many different sources and experience and comparisons with other databases indicate these figures are generally pessimistic. Dr David Smith suggests that his results should be factored according to the adversity of the conditions in which the element will be required to perform. By far the worst conditions are extremes of vibration and temperature.

Other factors to be taken into account are 'Quality' – has the element been burnt-in and 100% tested?

Suggested Quality factors are:

Normal commercial procurement	λ x 2
Procured to some agreed specification and quality management system	λ x 1
100% Screening and burn in	λ x 0.4

Additional Environmental factors are:

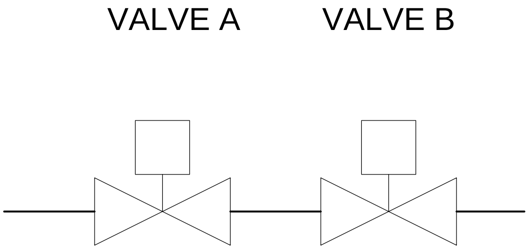
Dormant (little stress)	λ x 0.1
Benign (e.g. air conditioned)	λ x 0.5
Fixed Ground (no adverse vibration, temperature cycling, etc.)	λ x 1
Mobile/portable (high vibration and some temperature cycling)	λ x 4

These factors should be summed as appropriate, hence Quality factor of 0.4 and Environmental factor 1 should result in a multiplication of the selected failure rate by 0.4 x 1 = 0.4. This factor must be declared in calculations in reliability calculations and reasons for selection given.

2.3 Architecture and Beta Factor

Architecture relates to Architectural Constraints as discussed in BS EN 61508-2 and section nine of these guidelines. It is an indication of the amount of redundancy built in to a design. Redundancy can appear within component designs, multiple seals for instance, or it can appear as redundancy in elements. For example:

Sketch Eight



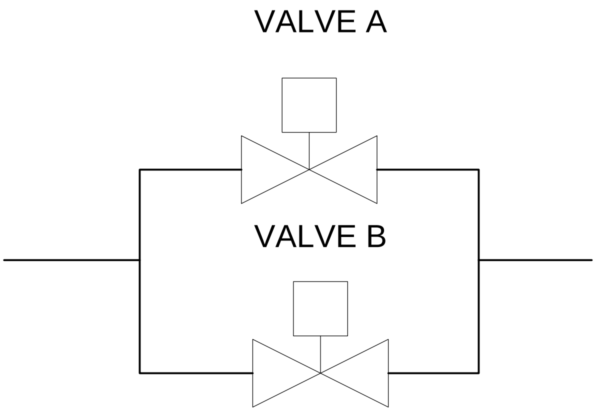
In sketch eight, valve A and B are connected in a redundant 1oo2 (one out of two) arrangement to stop flow on demand. Either valve will stop the flow under normal conditions so that should one of them become stuck or fail to respond to a close signal the safety function will still be performed. This latter case of a failure would be a dangerous undetected failure. Should one of the valves fail closed then this would be a safe undetected failure as the safety function would be performed unnecessarily, a spurious trip.

It may be recognised that if the safety function was to open on demand then this architecture would offer no protection whatsoever and the effective architecture would be 2oo2 to trip. This is potentially dangerous as a dangerous failure of just one of the valves would mean the loss of protection intended by the safety function.

So architecture is dependent on safety function.

If we required a 1oo2 to trip as in the first safety function, then the following arrangement of valves would be necessary:

Sketch Nine



In this case it can be seen that only one valve need open to fulfil the safety function and provide process flow. This arrangement is 1oo2 to provide flow on demand.

In all the above cases a Fault Tolerance of one is provided (in BS EN 61508 terminology).

In both of these cases the use of two valves to improve reliability to trip due to redundancy improves the failure rate of the combination though not of course the individual valve. Ideally if the probability of failure of one valve is ‘A’ then we would expect the probability of failure of two working to the same effect to be A^2 (i.e. A x A). In practice this is not achieved due to so called ‘common mode’ effects.

Common Mode is denoted by the Greek letter β. Common Mode effects are caused by similarities in design and installation that might cause a failure of both elements together. For example, if, due to a manufacturing fault, both valve actuators were fitted with faulty springs which failed on the first demand. The result would be no advantage from redundancy. However, it would be unlikely that both springs would fail simultaneously so from a random failure point of view the safety function may still function due to the second valve. We account for β by subtracting a percentage from the overall probability, i.e. $A^2 – B$ where B is related to element failure rate and a small fraction (typically less than one tenth). This β factor must be included in any calculation of PFD for a safety function with a Hardware Fault Tolerance greater than zero. For those less mathematically inclined it is recommended that the formulae presented in BS EN 61508-6 are used after reading the supporting text. This part of the standard covers a popular selection (though not all), for example 1oo2:

$$t_{CE} = l_{DU}/l_D[(T_1/2)+MTTR] + (l_{DD}/l_D)MTTR$$

$$t_{GE} = l_{DU}/l_D[(T_1/3)+MTTR] + (l_{DD}/l_D)MTTR$$

$$\mathbf{PFD_G = 2((1\text{-}b_D)\lambda_{DD} + (1\text{-}b)l_{DU})^{2.}t_{CE}.t_{GE}+b_Dl_{DD}MTTR+bl_{DU}((T1/2)+MTTR)}$$

Note that $\beta = 2\beta_{D.}$

NOTE: NOT ALL HIGHER ARCHITECTURES ARE SAFE! 2oo2 (to trip) is an architecture attractive to end users because it appears to offer both increased safety and increased reliability. This is not so and in such a configuration, should either element fail to danger so that it cannot fulfil the safety function then by definition the whole safety function has failed to danger hence

this particular configuration should be used only with understanding and care – preferably it should NOT be used at all!

The assessment of common mode factor is not a trivial exercise for a loop installation and whilst it will probably necessary to estimate a worst case value in the first place it should be confirmed on the final installation by a competent end user. For the element manufacturer, such as the valve and actuator manufacturer, who might use redundancy within an element, for example two seals where one would normally be sufficient or two springs in an actuator to ensure that return of the valve to its safe state is reasonably assured. Both of these cases would require an estimate of common mode factor, to take account of the redundancy provided by the seal or spring, in order to correctly calculate the element dangerous failure rate. A typical worst case value in these cases would be 5% (β).

A good idea when designing in redundancy, whether for loop or element, is to use diversity of components. Different makes of spring, different seal supplier, this helps to minimise the possibility of simultaneous failure and consequently allows for an argument for an improved common mode factor.

2.4 Determining the Proof Test Interval

The proof test interval is a "Periodic test performed to detect failures in a safety-related system so that, if necessary, the system can be restored to an "as new" condition or as close as practical to this condition". (Ref. BS EN 61508-4:1998 paragraph 3.8.5).

The inference from this is that the test has to be 100% complete, or near enough. So time has to be allowed in the operations plan sufficient to carry out the test without compromising the SIL (because each SIL by implication has a maximum unavailability before it ceases to qualify a SIL x, see Table Six.

Table Six

Availability	SIL	Max Unavailability – hrs per year
99.99 – 99.999%	4	0.876 (53 Mins)
99.9 – 99.99%	3	8.76
99 – 99.9%	2	87.6
90 – 99%	1	876

This means that if the down time, for all reasons, of a SIL 4 loop exceeds 53 Minutes then it reverts to a SIL 3 loop with a consequent significant drop in integrity.

In the case of a SIL 1 loop it is quite easy to establish a proof test interval that:

a. Gives sufficient time for testing
b. Is sufficiently flexible to minimise disruption to production

Normally, Proof Testing is arranged to coincide with a natural 'outage' and this is the first period to be input to the PFD calculation, if it provides an acceptable result then no further estimation is required. If the outage period does not allow an acceptable SIL then it will be necessary to make special provision for testing of the loop in between outages or this might provide justification for designing a higher architecture and more expensive loop that can be tested without interrupting production.

2.5 Diagnostics

For the valve and actuator manufacturer the only available diagnostics is generally by the application of a ‘partial valve stroke testing’ package (PVST). This a programmable electronic facility that is commercially available and that will, on demand, cause the valve to be moved over a small region of its stroke. The advantage of this facility is that it will ‘reveal’ many faults applicable to the valve and actuator package, for instance sticking of the valve. With the back-up of a DPCS it is possible on some facilities to record the amount of torque required to move the valve through this portion of stroke and consequently maintain a regular record that will show when the valve mechanism is showing signs of stiffening up prior to sticking. Maintenance may then be called in a timely manner.

In this manner several otherwise ‘unrevealed’ failures may also be recognised before they lead to complete failure of the valve actuator package. Typically 60 to 80% of dangerous failures (failures that would lead to the valve and actuator package failing to perform the safety function) would be revealed.

However, care should be taken in the analysis as the frequency of performing the PVST is quite important. If performed too infrequently then any advantage might be lost.

In the examples One and Two of these guidelines this would change some of the λ_{DU} to λ_{DD} with the consequence that AC SIL may improve, due to the effect on SFF, also the introduction of diagnostics requires the use of more complex PFD formulae so that now, for a 1oo1 Architecture:

$PFD = (\lambda_{DU} + \lambda_{DD}).t_{CE}$ and

$t_{CE} = (\lambda_{DU}/\lambda_{D}(T1/2 + MTTR) + \lambda_{DD}/\lambda_{D}(MTTR)$

It can be seen that the Right hand term of the equation is now non zero with the effect that t_{CE} actually decreases consequently increasing the PFD which means that a longer proof test interval is permissible.

Important Note. Advantage can only be claimed for Diagnostics on the basis that on detection of a fault either:

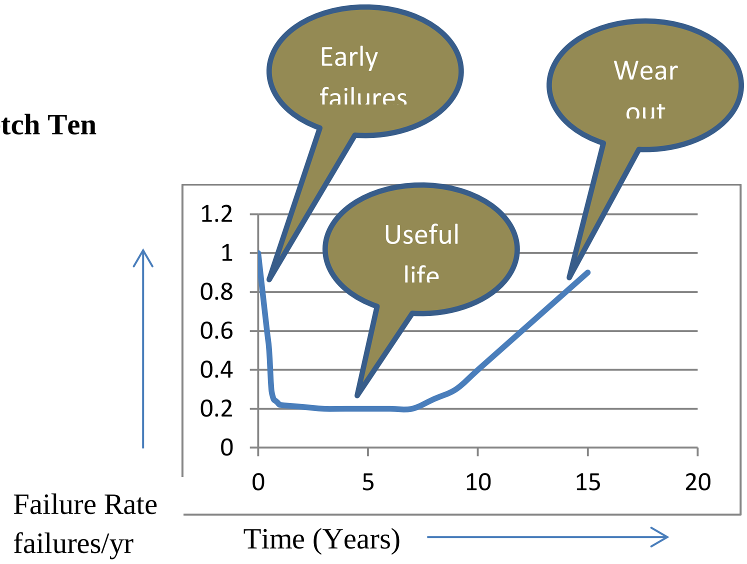
> Action is taken is taken to achieve or maintain a safe process state; OR
>
> The faulty element is repaired within the MTTR assumed in the PFD calculation for the loop (typically < 24 Hrs).

A potential downside of the use of PVST is that the software MUST comply with the requirements of BS EN 61508-3 if advantage is to be claimed by the valve manufacturer regarding SIL-capability.. Assuming that the PVST and associated devices are software/firmware based.

2.6 Controlling Systematic Failures

Systematic failures are those failures that have an originating cause which is non-random. PFD calculations are based on failure rate data which is for random failures that occur after infant mortality has been passed and prior to the onset of wear out mechanisms (this depends on the element and the application but BS EN 61508 says typically 8 to 12 years). If a curve were to be plotted of reliability against time it would appear in the shape of a bathtub, hence the bathtub curve (See Sketch Ten).

Sketch Ten



PFD calculations are only accurate where failure rates are constant and this only occurs on the flat part of the bathtub curve. The interested reader may note that this is the reason why many firms misleadingly quote MTBF data of hundreds and even thousands of years. The reality is that wear out will happen to switches, seals, electrolytic capacitors, mechanical rubbing parts, etc. well before the theoretical figure of MTBF.

The only way to control systematic failures is by strict use of procedures and the employment of trained, competent staff who have a clear understanding of their responsibilities (Ref. BS EN 61508-1:2010, paragraph 6.2.14). The Appendices of BS EN 61508-2:2010 and BS EN 61508-3:2010 provide suitable 'Techniques and Measures' for use during the different stages of development of a safety function, e.g. specification, design, testing, documentation; etc. Do review these and select ones that are applicable to your Company, compliance with these constitute a further part of the SIL compliance as most are SIL related. For Instance, BS EN 61508-2:2010, Table B.2 – Techniques and measures to avoid introducing faults during E/E/PE system design and development. As an example we have reproduced part of the table below:

Table Seven (– Reproduction of Table B.2 of BS EN 61508-2:2010)

	Technique/measure	See IEC61508-7	SIL 1	SIL 2	SIL 3	SIL 4
	Observance of guidelines and standards	B.3.1	M high	M high	M high	M high
	Project management	B.1.1	M low	M low	M medium	M high
	Documentation	B.1.2	M Low	M low	M medium	M high
	Structured design	B.3.2	HR low	HR low	HR medium	HR high
	Modularisation	B.3.4	HR low	HR low	HR medium	HR high
▨	Use of well-tried components	B.3.3	R low	R low	R medium	R high
▨	Semi-formal methods	B.2.3. see also Table B.7 of IEC 61508-3	R low	R low	HR medium	HR high
▨	Checklists	B.2.5	- low	R low	R medium	R high
▨	Computer-aided design tools	B.3.5	- low	R low	R medium	R high

▨	Simulation	B.3.7	- low	R low	R medium	R high
▨	Inspection of the hardware or walk-through of the hardware	B.3.7 B.3.8	- low	R low	R medium	R high
▨	Formal methods	B.2.2	- low	- low	R medium	R high

All techniques marked 'R' in the grey shaded group are replaceable, but at least one of these is required.

For the verification of this safety lifecycle phase, at least one of the techniques or measures shaded grey in this table or listed in Table B.5 shall be used.

NOTE 1 For the meaning of the entries under each safety integrity level, see the text preceding Table B.1.

NOTE 2 Most of these measures in this table can be used to varying effectiveness according to Table B.6. which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in Annex B of IEC 61508-7. Relevant subclauses are referenced in the second column.

For information (Ref BS EN 61508-2 Appendix B):
M: the technique or measure is required (mandatory) for this safety integrity level.
HR: the technique or measure is highly recommended for this safety integrity level. If this technique or measure is not used then the rationale behind not using it shall be detailed.
R: the technique or measure is recommended for this safety integrity level.
-: the technique or measure has no recommendation for or against being used.
NR: the technique or measure is positively not recommended for this safety integrity level.
If this technique or measure is used then the rationale behind using it shall be detailed.
The required effectiveness is signified as follows:

- Low: If used, the technique or measure shall be used to the extent necessary to give at least a low effectiveness against systematic failures.
- Medium: If used, the technique or measure shall be used to the extent necessary to give at least a medium effectiveness against systematic failures.
- High: If used, the technique or measure shall be used to the extent necessary to give high effectiveness against systematic failures.

The interpretation that you should take from this table is that when developing or designing elements for use in an E/E/PE safety function, including actuators and final actuators whether electrical or mechanical or any other technology, the management system MUST:

1. Apply all of the unshaded techniques and measures marked 'M' and as appropriate to the SIL target; whilst all unshaded techniques and measures marked HR MUST be either used or a written record established, for the element records, of why it wasn't used.

2. Use at least one of the shaded techniques and measures as appropriate to the SIL target.

Note that many of the techniques and measures appear to be repeated throughout the tables, this is not the case! Each techniques and measure appears so that is can be allocated a significance directly related to the particular lifecycle phase. For instance, Project Management appears many times, this does not mean that merely having a project manager is sufficient technique and measure – the project manager must be effective as required in each of the different lifecycles. So it maybe that a specialist project manager is required for a testing phase and a separate one for the specification phase. Most likely, though it implies that a chosen project manager must be trained and competent in all those areas in which the use of project management is chosen as a technique and/or measure.

Additionally, a Company involved in functional safety and wishing to claim either compliance with BS EN 61508-1, 2 or 3, must also be actively and continuously taking steps to recognise where systematic failures might occur in an organisation and to take action and implement procedures that can control them.

Without compliance with techniques and measures a loop element CANNOT be claimed to be either SIL compliant, SIL capable or suitable for use in a safety related system.

PART 3: PRACTICAL CONSIDERATIONS

3 Practical Considerations

3.1 Performing an FMEDA to comply with BS EN 61508

For the actuator and valve designer the only route permissible for establishing a SIL capability for his loop element is to perform a failure modes and effects analysis in the first place. To do this it is necessary to reduce the element design to a list of parts and then consider the possible failure modes for each part. Document those failure modes and consider what the effect will be on the performance of the complete element, e.g. if it is a normally closed mechanical ball valve with a spring return then consider what happens if the spring fails – the valve will fail to close.

Typically you should finish up with a spread sheet that looks something like the example below (though hopefully more complex in terms of quantity of components):

Table Eight Hypothetical valve/actuator FMEDA with a safety function of ‘close on demand’. Fail to close is the dangerous failure mode and fail closed is a safe failure mode. The table shows all identified failures and the result of the failures on the safety function.

Valve component	**Failure mode**	**Effect**	**Safe (S), dangerous (D) or no effect (NE)**	**λ (failure rate /hr)**
Valve - Body	Deflection	Failure to Close	D	1.00E-10
Valve – Bonnet	Deflection	Failure to Close	D	1.00E-10
Valve – Seat Ring	Damage	Failure to Close	D	4.00E-09
Valve – Seat ring	Damage	Failure to Close	D	4.00E-09
Valve – position indicator pointer	Damage causing detachment from the valve stem	Failure to Close	NE	1.00E-5
Valve – Stem	Damage/deflection	Failure to Close	D	3.75E-08
Valve – Seal skirt	Deflection	Failure to Close	D	2.00E-08
Actuator - Spring failure	Valve fails open due to loss actuation to close.	Failure to Close	D	1.0E-07
Loss of actuator air pressure	Valve closes under spring force	Fails Closed	S	6.0E-06
No Effect Failures			**NE**	1.0E-05
Safe Failures			**S**	6.0E-06
Dangerous Failures			**D**	1.66E-07
Total Failures =				1.62E-05

Note: In the past ‘no effect’ failures have been counted by some as ‘safe’ failures with a consequent exaggeration of SFF. This approach is quite incorrect, it was implicit in BS EN 61508-2:1998 but not explicit. BS EN 61508-2:2010 explicitly states that ‘no effect’ failures must not be considered to be ‘safe failures’.

Using the highlighted data of Table Eight we can calculate PFD and SFF:

PFD = λ_D.T/2 where λ_D = the total dangerous failure rate and T = the proof test interval.

From Table Eight we have λ_D = 1.66E-07 and we may first of all assume a proof test interval of 8760hrs (1 year). Hence, substituting into the equation for PFD gives:

1.66E-7*8760/2 = 7.3E-04 or 0.00073

This figure would be in the SIL 2 range.

SFF = λ_S / (λ_{TOTAL}- $\lambda_{no\ effect}$)

= 6.0E-06/ (1.62E-05 – 1.0E-05)

= 97%

Referring to Table Three and noting that we are not considering a system here only a valve and actuator combination and hence HFT = 0

This would give an AC SIL of SIL 3 but as it is the lowest of the assessments that apply we must give the valve actuator combination a SIL capability of SIL 2, i.e. it can be used in a SIL safety function up to SIL 2.

Remember that this neglects Techniques and Measures so we would now have to demonstrate that our design and manufacturing FSM achieved SIL 2.

3.2 Proven in Use, Route 2_s?

BS EN 61508 only permits a proven- in- use argument under very specific circumstances, such circumstances are rarely achievable by the manufacturer. The proven-in-use argument is specifically aimed at the end –user who may have statistically significant numbers of individual element on site and consequently his failure rate data, if correctly compiled using an accepted procedure will have greater validity for that site than any generic data.

Proven in use data may NOT be used by the element manufacturer.

By implication then, the manufacturer and designer MUST select route 1_S when developing hardware and software.

3.3 Functional Safety Assessment

What is a Functional Safety Assessment? Section Eight of BS EN 61508-1 refers, “One or more persons shall be appointed to carry out one or more functional safety assessments in order to arrive at a judgement on the adequacy of the functional safety achieved by the E/E/PE safety-related system(s) or compliant items (i.e. elements/subsystems) based on compliance with the relevant clauses of this standard.”

This is not a validation or verification exercise, as these should be performed and documented as part of any good ISO 9001 quality system. It is a review of available evidence, and there is a requirement on the system builder to ensure that he identifies and collects appropriate evidence which may be used by the assessor. There is a requirement for independence within the standard and this requirement is SIL related such that SIL 1 may use an independent person (within the company), SIL 2 requires an independent department and SIL 3and independent organisation.

The outcome from the independent assessment should be a report or reports documenting compliance, non-compliance and corrective actions but importantly declaring the necessary judgement that, in the opinion of the assessors, functional safety has or has not been achieved.

3.4 The importance of certification – To certify or not to certify?

Certification is not required by BS EN 61508; however, the independence of certification bodies does make them ideal for the task of independent FSA.

Sometimes also the system builder finds a certificate helpful as a measure of assurance that the assessment has been performed fully and correctly. Such certificates should be supplied by a UKAS approved certifier, which ensures that the body has the technical competence, the correct assessment procedures and is independent (has not been involved in consultancy related to the subject under evaluation). Furthermore, a certificate without an associated report is worse than useless. The system builder needs to know failure rates for safe and dangerous modes, Architectural Constraints, any restrictions in use (such as limits on process fluids), useful lifetime or cycle time before wear-out failures occur and any recommendations to avoid wear out by timely replacement of vulnerable components such as rubber seals, gaskets etc. systematic capability, etc. In addition to the above information (or reference to where it resides), any certificate should clearly state the identification/configuration of the element and it's safety manual, and the report reference. The latter should ideally be available to anyone with a valid reason for needing it.

Random failures and failure rate assumptions are based on the flat part of the life curve (more commonly known as the useful life section of the bathtub curve) after infant mortality and before wear out. It is necessary therefore to identify to the user when the onset of wear is expected to occur for his application so that he can arrange maintenance activities to avoid entering this unpredictable stage of the elements life.

3.5 Marking

BS EN 61508 invokes no special marking requirements. Good accepted practice is to separate safety instruments from normal control instruments and clearly label them with the instrument tag no. and the loop SIL and preferably isolated from other non SIL equipment with suitable labelling to inform operators and maintenance staff that ONLY competent staff may work on Functional Safety Equipment.

3.6 Where to source the standard?

The standard can be sourced from various places but the best is probably:

BSI Shop, bsi. http//shop.bsigroup.com

Or

BSI Customer Services
389 Chiswick High Road
London
W4 4AL
United Kingdom

PART 4: USEFUL REFERENCES

4 Useful References

4.1 Further learning on BS EN 61508

BVAA run regular one day courses on various topics including Safety Integrity Levels (SILs). Contact BVAA for a latest list of courses and dates.

4.2 Other Useful Publications

1. Reliability, Maintainability and Risk, Dr David Smith – ISBN978-0-7506-6696-7
2. Final Elements & the IEC 61508 and IEC61511 Functional Safety Standards by Chris O'Brien & Lindsey Bredmeyer – ISBN 978-1-934977-01-9
3. Safety Integrity Level Selection, Ed Marzal and Eric Scharpf – ISBN1-55617-777-1
4. Safety Instrumented Systems Verification, William M. Goble and Harry Cheddie – ISBN 1-55617-909-x.
5. Safety Shutdown Systems: Design, Analysis and Justification, Paul Gruhn and Harry L. Cheddie – ISBN-1-55617-665-1
6. Control Systems Safety Evaluation & Reliability, William M. Goble – ISBN1-55617-636-8.
7. Out of Control – Why control systems go wrong and how to prevent failure. HSE Books – ISBN0 7176-0847-6.
8. FARADIP .THREE Available from Technis.
9. NPRD-2011 – Non-electronic Parts Reliability Data by RIAC
10. Safety Equipment Reliability Handbook, Exida.com
11. Oreda – **O**ffshore **Re**liability **Da**ta

4.3 Useful websites

1. The IEC website has a well-structured and informative questions and answers section: www.iec.ch/functionalsafety/faq-ed2
2. The 61508 Association has useful information and downloads such as tool box talks and guides on what to look for on a certificate of conformity, cross referencing between different functional safety requirements, managing the lifecycle across the supply chain, etc.

4.4 BVAA Contact Details

For further information on available publications and regular training courses contact:

The British Valve and Actuator Association Ltd
9 Manor Park
Banbury
Oxfordshire OX16 3TB (UK)
Website: www.bvaa.org.uk Telephone: +44(0)1295 221270 Email: enquiry@bvaa.org.uk

4.5 Acknowledgements

This document was written By P R Smith BA CEng FInstMC MIET but grateful acknowledgement goes to my fellow BVAA SILs Course Lecturer,

Mr Paul Reeve BEng CEng MIET MInstMC for Technical reviewing over and above the call of duty.

My thanks also to BVAA Technical Consultant, Mr Peter Churm, for his excellent contribution on behalf of the BVAA.

And last but not least Mr Rob Bartlett FIAM for his for sight in commissioning this document and for his help in providing structure and purpose.

VERSION A.4a 27032013