GUIDELINES

On supplying

Valves and Actuators

capable of use in applications with a

Safety Integrity Level (SIL)

---

prepared by

The British Valve and Actuator Association

Acknowledgements:

This document was produced by members of the BVAA Technical Expert Group (TEG) on safety integrity levels (SILs) formed in 2015 to whom the BVAA offers its grateful thanks.

Revision	Date	Author(s)	Reviewer(s)	Comments
0.1 (draft)	12/10/2015	PR	TEG	Skeleton draft
0.2 (draft)	30/04/2016	PR	TEG	Draft for industry comment
0.3 (draft)	17/11/2016	PR	TEG	Comments incorporated
1.0 (released)	02/02/2017	PR	TEG	Minor text revisions; appendix 1 added

ALL COMMENTS ARE WELCOMED AND SHOULD BE SENT TO: Rob@bvaa.org.uk

Contents

Glossary of commonly used terms and abbreviations

The following list includes abbreviations used in this document or commonly associated with functional safety. For a full explanation of many of these terms refer to BS EN 61508-4:2010 or BS EN 61511-1:2016 (section 3).

AC	Architectural constraints
ALARP	As low as reasonably practicable
CASS	Conformity assessment of safety-related systems
CCF	Common cause failure
COMAH	Control of Major Accident Hazards
DC	Diagnostic coverage
BPCS	Basic process control system
E/E/PE	Electrical/Electronic/Programmable-Electronic (technology)
EUC	Equipment under control
FE	Final element
FIT	Failures in time (10^{-9}/hr)
FMEA	Failure modes and effects analysis
FMEDA	Failure modes effects and diagnostics analysis
FSM	Functional safety management
HAZOP	Hazards and operability study
HFT	Hardware fault tolerance
HSE	Health and Safety Executive
LoPA	Layer of protection analysis
MDT	Mean down time
MTBF	Mean time between failures
MTTF	Mean time to failure
MTTR	Mean time to repair
NCR	Non-conformity report
P&ID	Piping and instrumentation diagram
PES	Programmable electronic system
PFD_{AVG}	Probability of failure on demand (average)
PFH	Probability of failure per hour
PLC	Programmable logic controller
PMH	Per million hours
PVST or PST	Partial valve stroke testing
RBD	Reliability block diagram
RRF	Risk Reduction Factor
SC	Systematic capability (1 to 4)
SFF	Safe failure fraction
SIF	Safety instrumented function
SIL	Safety integrity level (1 to 4)
SIS	Safety instrumented system
T	Proof test interval
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)
1oo1,1oo2, etc.	Nomenclature to indicate voting of channels (e.g., vote: 1-out-of-2)

BVAA GUIDELINES ON SUPPLYING VALVES AND ACTUATORS FOR USE IN APPLICATIONS WITH A SAFETY INTEGRITY LEVEL (SIL)

1. Introduction and Scope

This document is intended to provide practical guidance for manufacturers of valves and actuators whose customers are requesting a 'safety integrity level (SIL) capability'. It is aimed at those who are responsible for preparing a proposed design, typically at the bid stage. It is not intended to be a comprehensive training manual on the subject of functional safety or SILs, but rather a guide to explain how to deal with the practical issues that are specific to valve and actuator suppliers. (It is, of course, certainly advisable for suppliers to have engineers who are fully competent in the technical aspects of functional safety as far as it applies to their scope of supply so they can handle bespoke requirements and the more challenging or esoteric problems that may arise).

Experience has shown that when it comes to providing SIL capability data, unnecessary expense can be incurred if pre-assessment analysis is carried out for system elements based on certain assumptions, only to find that the analysis has to be repeated once the whole system is designed and configured. It is therefore a key objective of this document that a better and more uniform understanding of what SIL capability data is required by the various parties across the supply chain and how that data can be presented in order to avoid unnecessary effort or expense later in the process.

With the above objectives in mind, the target readership of this document is aimed at:

- Manufacturers or suppliers of valves or actuators being offered as elements for use in a safety instrumented system
- Integrators of an actuated valve package (with or without associated instrumentation) for use in a safety instrumented system
- Purchasers of the above who need to provide the right information concerning the required system application in order for the supplier to provide the right SIL capability data

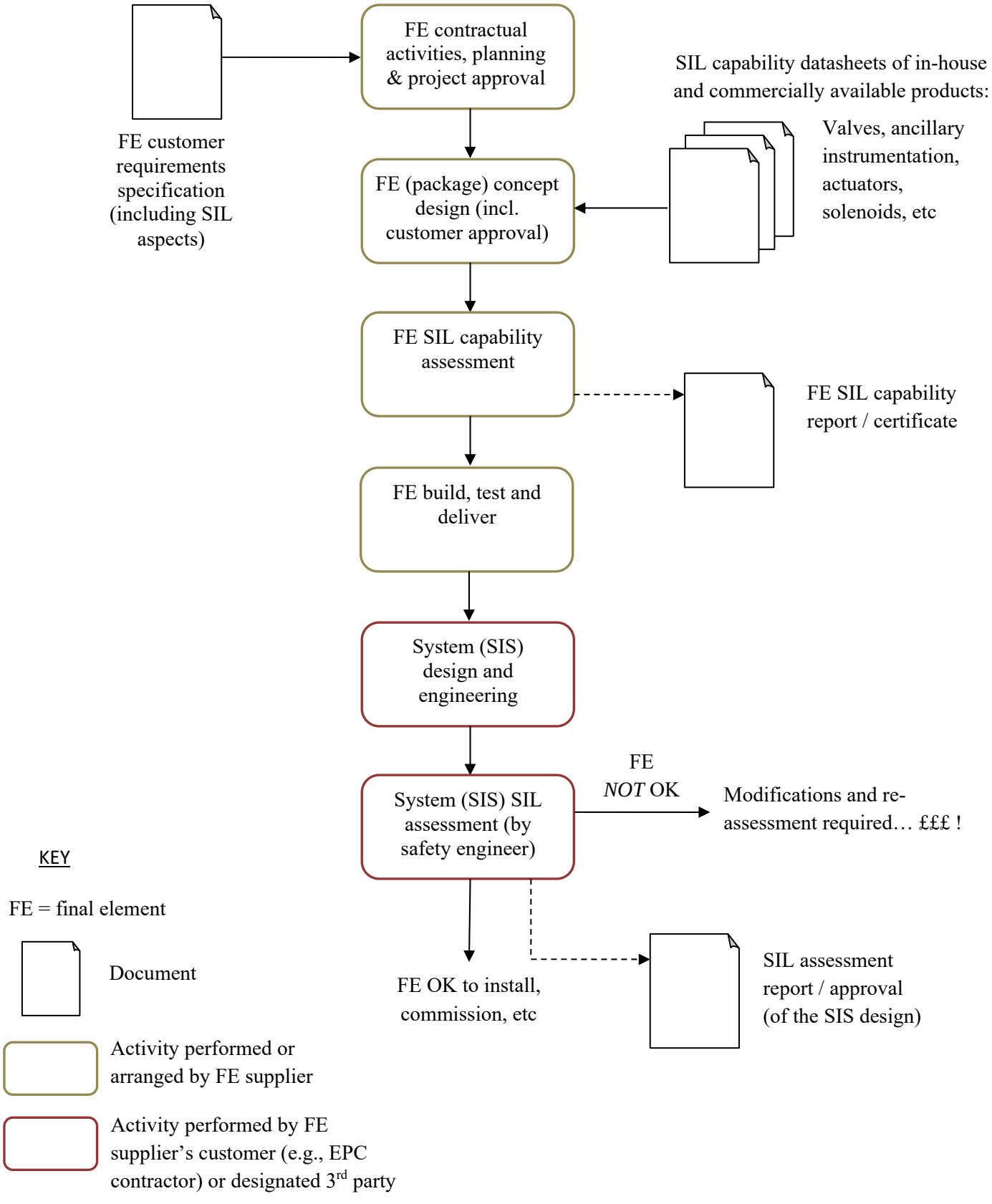
The generic functional safety requirements for the design of safety system elements such as valves and actuators are given in BS EN 61508-2[REF 1].

System design or engineering companies (e.g., EPCs) should select suitable devices for their application in accordance with BS EN 61511-1[REF 3]. In certain circumstances this may be based on a 'proven in use' qualification, however, these guidelines are aimed at element suppliers needing to implement the requirements of [REF 1].

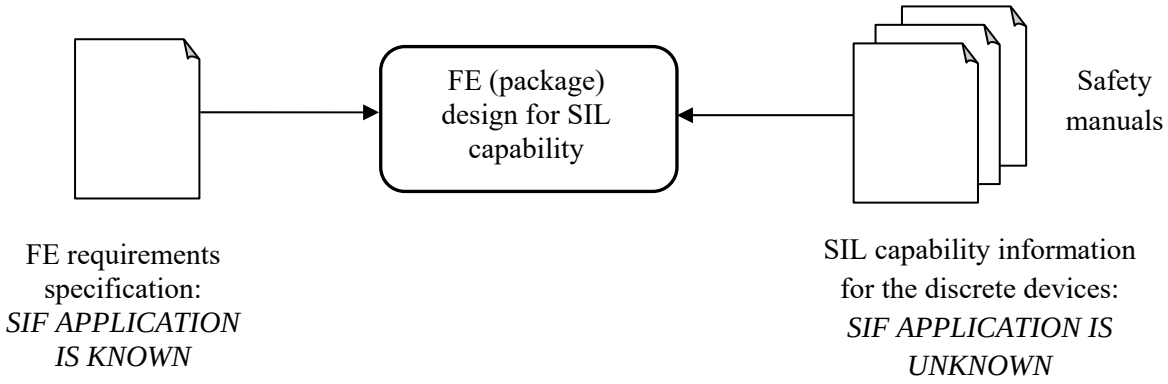
In these Guidelines, the term 'SIL *n* capability' for a device is used (n = 1, 2, 3 or 4). This term is not actually defined or used in BS EN 61508 but is commonly used by engineers as a *provisional indicator* of the SIL that could be achieved for a SIF that uses the device, if all stated conditions and assumptions are complied with. A more detailed explanation of this term is provided in Appendix 1.

2. Typical supply chain model

A typical model for the engineering of process industry final elements (FE) in terms of the SIL related activities may look like the following:



To avoid misunderstandings and costly re-work, it is important that the right information is obtained, used, and communicated between the parties who are involved in SIL-related activities. For the FE (package) designer, this involves obtaining and using information from two sources as shown below:



As the vendors of mass produced devices typically do not know anything about a specific SIF application, it is important that all the SIL related attributes of their devices are presented in a form that can be applied by those who are designing FE packages for a specific application. This means much more than just claiming the device is capable of, say, "SIL 3". For that statement to be the case there have to be many assumptions about the application it is used in, which may well require certain conditions and restrictions in its use, not to mention a long list of device attributes and failure data that the SIF designer needs to know before any "SIL 3" application can actually be achieved. All this is generally ensured by producing a 'safety manual' to accompany the device that contains all the information listed in BS EN 61508-2 Annex D (as mandated for 'compliant items'). An example format of a safety manual is shown in Appendix 3 of this document.

Equally important is the need for the customer to provide a detailed requirements specification of what the FE needs to do in terms of achieving the SIF. This is what will be used to verify the design of the FE against, so any mistakes or omissions in this information will most likely just follow through into the FE design. For this reason it is important that the requirements specification is carefully and formally reviewed by the FE designer before it is fully adopted.

The FE designer needs to be competent in understanding how to apply the data in the device safety manual(s) to the specific application in hand. For example, in regard to the failure data of a pilot valve (λ_D, λ_S, SFF, etc), what failure modes of the device are these referring to and are they the failure modes that are relevant to the target SIF application? Are the assumptions used for the SFF figure still valid and if not is the SIL capability of the pilot valve reduced when used in this way?

Good information management is important if the FE needs to be modified or upgraded at any point. This is covered under the FE manufacturer's procedures for 'configuration management'. Modifications of any aspect of a safety system (such as the final element) is an area that needs to be managed strictly in accordance with BS EN 61508 / 61511.

3. Common confusions and misconceptions

The following table should help to correct some common points of confusion about how functional safety and SIL apply to final elements.

Typical confusion or misconception	Correct position or statement
1. Buyers insist on requiring a "SIL certified device"	None of the functional safety standards require 'certification', or indeed even mention the word. Likewise, there are no 'Notified Body' requirements for functional safety compliance as there are under certain EU Directives (e.g., ATEX). BS EN 61508 requires an independent 'functional safety assessment' for all aspects of the SIS, which should include the FE devices and a packaged FE. The assessment is a formal documented activity by a competent person or organisation that is independent from the item being assessed. However, the buyer may prefer to obtain 'certification' for contractual or other reasons in addition to the mandatory requirements of the standard.
2. A device can be claimed as "SIL <number>" compliant, approved or certified?	Whenever SIL is used, it refers to the safety performance of the entire SIF. Strictly speaking, a SIL (1, 2, 3 or 4) should not be given to a discrete device, although the device could be said to be capable, or suitable, of being used in a SIL (1, 2, 3 or 4) application if certain ways of using it are adhered to (often involving assumptions, conditions and restrictions). Normally, if a device is claimed as being "SIL (1, 2, 3 or 4)" compliant, it is used in a marketing context, i.e., a SIF with that SIL number might be possible if the device is used under the most favourable conditions and depending on other system factors not associated with the device. An alternative might be to describe the device as "SIL capable" (with no number) and refer to the list of reliability parameters, which implies it can be considered for its suitability in SIFs at all SILs depending on the application and other system parameters which should be known to the system designer.
3. Combining a "SIL 2 capable" sensor, logic solver and FE will create a SIS capable of performing a SIL 2 SIF	As explained above, a "SIL 2 capable" device implies many assumptions, conditions and restrictions apply. Creating a SIS from devices that each claim to have the same SIL number is not guaranteed to yield a system capable of performing a SIF at that number. There is no short cut to a competent integrator having to do an analysis of all the discrete device parameters together with the SIF application considerations.
4. Compliance to BS EN 61508-2 edition 1 (1998) is still valid for my FE	There were some areas that were not clearly defined in edition 1 of BS EN 61508-2, e.g., for SFF where it was not explicitly stated that 'no-part' failures were not to be used in the calculation.

	Furthermore, older compliance statements (including 'certificates') only considered the hardware failure rates and did not assess all the systematic integrity requirements. Edition 2 of the standard introduced the term 'Systematic Capability' (with a number 1 to 4) for an element that could be directly attributed to the device which corresponds to the suitability for use at a SIL (1 to 4), in respect of the device's systematic integrity. In terms of validity of an older standard once a new version is published, as far as the publication is concerned, the old is obsolete and superseded immediately the new one is published. As regards a reasonable grace period to allow for industry to make the transition as typically announced under regulatory schemes (such as European directives with harmonised standards), there is currently no such directive or scheme for SIS.
5. The precision of the failure data is important	The standards require that failure rates only need to be estimated. In reality, it is not possible (or indeed necessary) to predict these figures with accuracy, hence a precision of 1 significant figure (plus the order of magnitude) is adequate (e.g., $5\ 10^{-7}$). Failure rate figures with several significant figures are commonplace and the reader might as well apply suitable rounding. Furthermore, failure rate predictions should always be conservative. If the insignificant figures are needed to pull the result one side of a criterion, then this calls into question the conservatism of the approach.

4. Typical valve/actuator example datasheets

Datasheets come in all forms and degrees of detail, but in terms of the minimum SIL-related information required by an integrator, the following is required to design safety functions:

Device parameter	Symbol
Type	A / B
Dangerous failure rate	λ_D
Dangerous diagnosed failure rate *	λ_{DD}
Dangerous undiagnosed failure rate *	λ_{DU}
Safe failure rate	λ_S
Diagnostic coverage (if any) *	DC
Safe Failure Fraction	SFF
Systematic capability	SC

* Only relevant if diagnostic facilities are provided by the supplier

The data above presupposes the failure modes of the device are known with respect to the safety application and hence quantitative figures can be attributed as 'safe' or 'dangerous'.

Valve and actuator manufacturers should therefore endeavour to establish the data types above for their products. Integrators of FE packages will require the above data types from the discrete devices in order to establish the SIL capability of the package.

A type A element can become type B by the addition of any associated component in the sub-system that is type B, with consequent changes to the architectural constraints and PFD.

5. Worked example to meet a bid request

In order to perform a worked example of how a valve / actuator package could be integrated from discrete devices to achieve a specified SIL capability, let us assume the following data is available for the solenoid, pneumatic actuator and ball valve that are proposed for the package. It is important to realise that the failure data has to relate to the safety function that is being designed. For this example we shall assume the FE safety function is: to close the ball valve on removal of the electrical supply to the solenoid coil. Let's assume the expected demand rate is less than once a year so this a low demand safety function. Thus, we need to identify the required 'element safety function' for each device and ensure the failure data provided by the device manufacturer relates to this.

Device parameter	Solenoid	Actuator	Ball Valve
Element safety function (for which failure data below relates)	To relieve pneumatic pressure (return spool under spring force) on removal of electrical signal	To return spindle to de-energised position under spring force on removal of pneumatic pressure	To close valve by rotation of stem under actuator control
Type A/B	type A	type A	type A
Dangerous failure rate, λ_D	5.0E-07	2.0E-07	3.5E-07
Dangerous diagnosed failure rate, λ_{DD}	0	0	0
Dangerous undiagnosed failure rate, λ_{DU}	5.0E-07	2.0E-07	3.5E-07
Safe failure rate, λ_S	3.5E-07	5.6E-07	1.2E-06
Diagnostic coverage, DC	0%	0%	0%
Safe Failure Fraction, SFF	41%	74%	77%
Systematic capability, SC	SC 2	SC 3	SC 3

Initially, as basic standalone devices with no auxiliary instrumentation, there is no diagnostic capability at this point, so the DC and λ_{DD} values are zero for each device.

It will be necessary to refer to tables 2 (or 3) in BS EN 61508 Part 1 for how PFD_{AVG} (or PFH, respectively) corresponds to SIL. Likewise, it will be necessary to refer to tables 2 and 3 of BS EN 61508 Part 2 for the architectural constraints. See Appendix 2 of this document for convenience.

A worksheet can be developed to create a reliability model of the actuated valve into which the failure data of each device can be inserted. Equations for calculating the PFD_{AVG} are taken from BS EN 61508-6 (section 3.2.2). This is shown on the next page.

Failure Data Calculations - 1oo1, no diagnostics, low demand

RELIABILITY BLOCK DIAGRAM

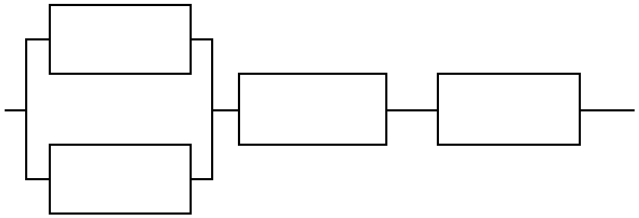
User parameter	Symbol	Value (for illustration)
Proof Test Interval	T_1	8760
Mean Time To Repair	MTTR	24

Device parameter	Symbol	Equation / source	SOLENOID	ACTUATOR	BALL VALVE	PACKAGE
Hardware Fault Tolerance	HFT	Self-evident	0	0	0	0
Type A/B	type A	Self-evident/manufacturers data	type A	type A	type A	type A
Dangerous failures:	λ_D	Manufacturers data	5.0E-07	2.0E-07	3.5E-07	1.1E-06
Dangerous diagnosed failures:	λ_{DD}	Manufacturers data	0.0E+00	0.0E+00	0.0E+00	0.0E+00
Dangerous undiagnosed failures:	λ_{DU}	Manufacturers data	5.0E-07	2.0E-07	3.5E-07	1.1E-06
Safe failures:	λ_S	Manufacturers data	3.5E-07	5.6E-07	1.2E-06	2.1E-06
Diagnostic coverage:	DC	$\lambda_{DD} / (\lambda_{DU} + \lambda_{DD})$	0%	0%	0%	
Safe Failure Fraction:	SFF	$(\lambda_S + \lambda_{DD}) / (\lambda_S + \lambda_{DD})$	41%	74%	77%	
Channel equivalent down time	t_{CE}	$(\lambda_{DU} / \lambda_D)(T/2 + MTTR) + \lambda_{DD} / \lambda_D MTTR$	4.4E+03	4.4E+03	4.4E+03	
Probability of failure on demand	PFD_{AVG}	$(\lambda_{DU} + \lambda_{DD}) t_{CE}$	2.2E-03	8.8E-04	1.5E-03	**4.6E-03**
Systematic capability	SC	Manufacturers data	SC 2	SC 3	SC 3	SC 2
Architectural constraints	SIL_{AC}	From inspection of HFT, type and SFF	SIL 1	SIL 2	SIL 2	SIL 1
Overall SIL capability (low demand)		From inspection of SC, SIL_{AC} and PFD_{AVG}	SIL 1	SIL 2	SIL 2	**SIL 1**

The worksheet above shows how a single channel architecture (1oo1 voting configuration) for the FE safety function is limited to SIL 1. It can be seen that the main limiting factor is the architectural constraints of the solenoid valve, in particular the SFF being 41% (being < 60% according to the rules in BS EN 61508-2 section 7.4.4). This limits the final SIL of the package to SIL 1 even though a PFD_{AVG} of 4.6E-03 would otherwise allow the package to meet SIL 2.

Failure Data Calculations - 1oo2 (solenoid), no diagnostics, low demand

RELIABILITY BLOCK DIAGRAM



User parameter	Symbol	Value (for illustration)
Proof Test Interval	T_1	8760
Mean Time To Repair	MTTR	24
CCF	β	0.1

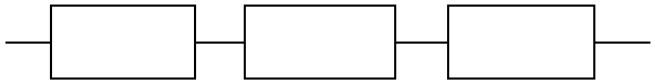
Device parameter	Symbol	Equation / source	SOLENOID	ACTUATOR	BALL VALVE	PACKAGE
Hardware Fault Tolerance	HFT	Self-evident	1	AS FIGURES FOR 1oo1 FOR APPLICABLE PARAMETERS		0
Type A/B	type A	Self-evident/manufacturers data	type A			type A
Beta factor (common cause failures)	β	Assumed for illustration	0.1			
System equivalent down time	t_{GE}	$(\lambda_{DU} / \lambda_D)(T/3 + MTTR) + \lambda_{DD} / \lambda_D$ MTTR	2.94E+03			
Probability of failure on demand	PFD_{AVG}	$2[(1-\beta)\lambda_{DD} + (1-\beta)\lambda_{DU}]^2 t_{CE} t_{GE} + \beta\lambda_{DD}$ MTTR + $\beta\lambda_{DU}$ ((T/2)+MTTR)	2.25E-04			**2.6E-03**
Systematic capability	SC	Man. data and 61508-2, 7.4.3 rules	SC 3			SC 3
Architectural constraints	SIL_{AC}	From inspection of HFT, type and SFF	SIL 2			SIL 2
Overall SIL capability (low demand)		From inspection of SC, SIL_{AC} and PFD_{AVG}	SIL 2			**SIL 2**

The worksheet above shows that by duplicating the solenoid valve (1oo2 voting configuration for the solenoid only) the FE safety function is now limited to SIL 2. To gain any further improvement will either require duplicating more of the channel or adding some diagnostics. See the next worksheet where diagnostics have been added. Note that the increase to SC 3 in this example assumes that 'sufficient independence' is achieved between the two devices (e.g., using diverse solenoids from different manufacturers and possibly other measures).

Failure Data Calculations - 1oo1, with diagnostics, low demand

User parameter	Symbol	Value (for illustration)
Proof Test Interval	T_1	8760
Mean Time To Repair	MTTR	24

RELIABILITY BLOCK DIAGRAM



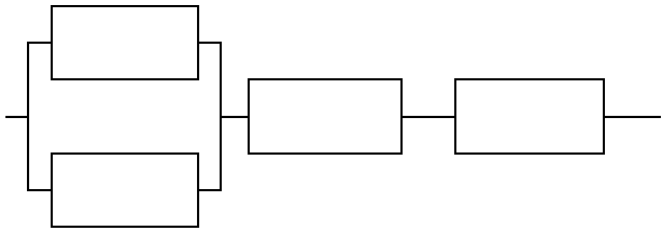
Device parameter	Symbol	Equation / source	SOLENOID	ACTUATOR	BALL VALVE	PACKAGE
Hardware Fault Tolerance	HFT	Self-evident	0	0	0	0
Type A/B	type A	Self-evident/manufacturers data	type A	type A	type A	type A
Dangerous failures:	λ_D	Manufacturers data	5.0E-07	2.0E-07	3.5E-07	1.1E-06
Dangerous diagnosed failures:	λ_{DD}	Manufacturers data	3.0E-07	1.5E-07	3.2E-07	7.7E-07
Dangerous undiagnosed failures:	λ_{DU}	Manufacturers data	2.0E-07	5.0E-08	3.5E-08	2.9E-07
Safe failures:	λ_S	Manufacturers data	3.5E-07	5.6E-07	1.2E-06	2.1E-06
Diagnostic coverage:	DC	λ_{DD} / (λ_{DU} + λ_{DD})	60%	75%	90%	
Safe Failure Fraction:	SFF	(λ_S + λ_{DD}) / (λ_S + λ_{DD})	76%	93%	98%	
Channel equivalent down time	t_{CE}	(λ_{DU} / λ_D)(T/2 + MTTR) + λ_{DD} / λ_D MTTR	1.8E+03	1.1E+03	4.6E+02	
Probability of failure on demand	PFD_{AVG}	(λ_{DU} + λ_{DD}) t_{CE}	8.9E-04	2.2E-04	1.6E-04	**1.3E-03**
Systematic capability	SC	Manufacturers data	SC 2	SC 3	SC 3	SC 2
Architectural constraints	SIL_{AC}	From inspection of HFT, type and SFF	SIL 2	SIL 3	SC 3	SIL 2
Overall SIL capability (low demand)		From inspection of SC, SIL_{AC} and PFD_{AVG}	SIL 2	SIL 3	SIL 3	**SIL 2**

The worksheet above shows the benefit from adding diagnostics to the single channel (1oo1) configuration. The DC value for each element is a judgement of the proportion of failure modes of the element that will be revealed by the diagnostic, for example by adding valve positioning instrumentation. Note that the DC will most likely be a different value for each element. In this case SIL 2 is achieved. It can be seen that the actuator and ball valve are capable of supporting a higher SIL and the limiting factor is back to the architectural constraints of the solenoid again. See next worksheet for a further improvement.

Failure Data Calculations - 1oo2 (solenoid), low demand

User parameter	Symbol	Value (for illustration)
Proof Test Interval	T_1	8760
Mean Time To Repair	MTTR	24
CCF	β	0.1

RELIABILITY BLOCK DIAGRAM



Device parameter	Symbol	Equation / source	SOLENOID	ACTUATOR	BALL VALVE	PACKAGE
Hardware Fault Tolerance	HFT	Self-evident	1			0
Type A/B	type A	Self-evident/manufacturers data	type A			type A
Beta factor (common cause failures)	β	Assumed for illustration	0.1			
System equivalent down time	t_{GE}	$(\lambda_{DU} / \lambda_D)(T/3 + MTTR) + \lambda_{DD} / \lambda_D MTTR$	1.19E+03			
Probability of failure on demand	PFD_{AVG}	$2[(1-\beta)\lambda_{DD} + (1-\beta)\lambda_{DU}]^2 t_{CE} t_{GE} + \beta\lambda_{DD} MTTR + \beta\lambda_{DU} ((T/2)+MTTR)$	8.97E-05			**4.8E-04**
Systematic capability	SC	Manuftrs. data and 61508-2, 7.4.3 rules	SC 3			SC 3
Architectural constraints	SIL_{AC}	From inspection of HFT, type and SFF	SIL 3			SIL 3
Overall SIL capability (low demand)		From inspection of SC, SIL_{AC} and PFD_{AVG}	SIL 3			**SIL 3**

AS FIGURES FOR 1oo1 FOR APPLICABLE PARAMETERS

The worksheet above shows the benefit from adding diagnostics and duplicating the solenoid valve. Here, SIL 3 is achieved.

Notice here that:

- the PFD_{AVG} of 4.8E-04 uses half the SIL 3 budget
- all devices (as configured in 1oo2 or 1oo1) have a systematic capability of SC 3 giving the subsystem SC 3
- the architectural constraints of the elements (as configured in 1oo2 or 1oo1) are now all SIL 3, limiting the subsystem to SIL 3

6. Increasing the SIL capability

Sometimes, as in the example above, the analysis does not yield the SIL capability that is required at first. In this case it may be possible to increase SIL capability by one or both of the following methods:

- Reduce the proof test interval (T_1) which decreases the PFD_{AVG}
- Increase the hardware fault tolerance HFT (redundancy)
- Provide external diagnostics

Note that to achieve a specified SIL capability, each subsystem that is performing the SIF has architectural constraints ('type', SFF and HFT), PFD_{AVG} and Systematic Capability requirements to meet.

If the problem lies with the PFD_{AVG} (not being low enough), the user may be able to reduce the interval T_1. The FE manufacturer should make it clear that any PFD_{AVG} figure stated for the FE uses a figure for T_1 (and mean time to repair, MTTR, for that matter) in order to demonstrate PFD_{AVG} for illustration. If the user wants to use different figures for T_1 and MTTR then the PFD_{AVG} needs to be recalculated to ensure that aspect of the required SIL is met.

If the user cannot reduce the proof test interval another approach may be to apply partial valve stroke testing (PST) to reduce the PFD_{AVG}. See section 11 for more details.

If the problem lies with the architectural constraints, increasing the HFT lifts this limit by one SIL in accordance with BS EN 61508-2 tables 2 (for type A) and 3 (for type B), or BS EN 61511-1 table 6. The added benefit with this approach is that it also significantly reduces the PFD_{AVG} of the redundant combination, although it is essential to consider any common mode failures which typically become the dominant factors in the new PFD_{AVG} value. Using the simplified equations for the standard architectures with HFT and voting provided in BS EN 61508-6 (section B.3.2.2) require a figure for the beta factor that addresses the common cause failures. Many of the considerations that contribute to the beta factor are related to the installation, environment or application. If a worst case figure (e.g., 10 – 20%) was used by the manufacturer for illustration (again, like the values for T_1 and MTTR), then this should be clearly stated as such in the safety manual.

7. The safety manual

The safety manual is a mandatory document required by BS EN 61508-2: 2010 (Annex D, normative) which should accompany any device that the manufacturer claims complies with the standard. Hence the title of Annex D is 'Safety manual for compliant items'. The purpose of the safety manual for compliant items *is to document all the information, relating to a compliant item, which is required to enable the integration of the compliant item into a safety-related system, or a subsystem or element, in compliance with the requirements of this standard*. (BS EN 61508-2:2010, Annex D, paragraph D.1).

A 'compliant item' can be a subsystem, element or anything that can be used in one of these that is claimed as being compliant such as a limit switch, solenoid, a partial valve stroke testing device, etc.

An example format for a safety manual is given in Appendix 3 for illustration. This example has cross references to each of the clause in the standard to demonstrate traceability to the origin of these requirements.

It is generally considered not essential that the safety manual needs to be a separate document; it could be included as a separate section in another user manual, although it should be clearly identified as such in a prominent place in the document (e.g., within the document title or on the front cover).

8. Sources of failure data

An important aspect of functional safety is about predicting the reliability of the safety system or product for a future application based on historical reliability performance. The best reliability data to base this prediction on would be derived from a large number of the items used in a similar application and environment to that which will apply to the future scenario. Unfortunately, this type of data is rarely available, and a prediction has to be made from a reliability model that uses parts for which more generic failure data is available. Like all reliability predictions, ample use of conservatism is very important when making assumptions about service, ratings, environment, etc.

Failure data for mechanical, electrical and electronic components is available in two broad forms:

- Data based on real field failures with varying degrees of statistical confidence (influenced by the number of operating unit-hours, the number of failures that occurred and to some degree the nature of the fault – whether truly 'random', or whether the data also included some systematic faults)
- Data that is derived from a mathematical model which includes modifying stress factors for temperature, environment, cycling, ratings, etc

When creating a reliability model like a failure modes and effects analysis, it is better to use component data from the same type of source if possible for consistency. The data should include the failure rate and its division between the various failure modes of the component (as exhibited by the physical behaviour or response of the component). The failure data should be chosen to be consistent with the type of installation, service and environment of the intended application for which the prediction is being sought.

Some component failure databases for component parts are:

- US MIL HDBK 217
- OREDA offshore reliability equipment data
- SINTEF
- NPRD non-electrical parts reliability data (from RIAC)
- EPRD electrical parts reliability data (from RIAC)
- Exida safety equipment reliability handbooks
- UKAEA (SRD)
- Faradip.three (from Technis)
- IEC TR 62380:2004 (modelled data for electronic parts)

Creation of the reliability model and the analysis of each component fault can get very complicated and requires experience and judgment on the part of the analyst. It is also essential that the analyst and

designer work together on this task to ensure the effect of each possible component failure mode on the overall function is fully understood and taken account of.

When constructing a FE (package) reliability model from the failure data of discrete devices' element safety function, the failure data should always be reviewed critically before use. Sometimes, failure data for a device looks rather more optimistic than conservative, presumably in order to infer a better 'SIL n Capability'. If in doubt, it is always sensible to compare vendor's claims against the range of similar types of device, service and application that is being claimed.

9. Definition of failure types

Failures can be categorised in terms of their effect on the element safety function as follows:

Failure	Termination of the ability of the equipment to provide a required function or operation of the equipment in any way other than as required. This failure could be either *random hardware failure* or *systematic failure* – refer to BS EN 61508-4:2010 for further definition. Random hardware failures are repeatable (following repair/replacement) and hence their failure *rate* can be quantified (Greek symbol 'λ' is used). Sub-divisions of random hardware failure are described below.
Dangerous Failure, λ_D	Failure of an equipment that plays a part in implementing the safety function that: a) Prevents a safety function from operating when required, OR causes a safety function to fail, such that the EUC is put into a hazardous or potential hazardous state. Or, b) Decreases the probability that the safety function operates correctly when required. If the equipment has self-diagnostics, dangerous failures can be further sub-divided into: • Dangerous Detected Failures,(λ_{DD}); Dangerous Undetected Failures, (λ_{DU})
Safe Failure, λ_S	A failure in the equipment that: a) Results in the spurious operation of the safety function to put the EUC into a safe state or maintain a safe state. Or b) Increases the probability of the spurious operation of the safety function to put the EUC into a safe state, or maintain a safe state. If the equipment has self-diagnostics, safe failures can be further sub-divided into: • Safe Detected Failures,(λ_{SD}); Safe Undetected Failures, (λ_{SU})
No effect failure or No part failure	A failure in the equipment that plays not part in implementing the safety function, or has no direct effect on the safety function. These failures do not contribute to the SFF calculation.

When performing an analysis (e.g., by FMEA) it is essential to use the correct divisions of failure mode (according to the type of application the device is being assessed for). A common mistake is to attribute failure modes to be 'Safe' that are in fact 'No Part' failures. This mistake will inflate the SFF erroneously and may very well indicate a higher SIL capability.

10. Systematic capability

Many types of failures in SIS are not actually due to 'random' failures of components (seals, stems, seats, solenoid coils, electronic components, etc) that result in quantifying a 'failure rate' figure. Many failures of modern control and safety systems are due to weaknesses or defects in the design (e.g., in the conceptual or detailed design – either hardware or software), the testing, documentation, environmental endurance, operation and maintenance regime, human error, etc.

Problems of this type do not produce the odd random failure in a sample batch of items; they tend to affect all items in the same way because the problem is systematic in origin. Hence they are collectively referred to as systematic failures. These types of failures can creep in or occur at any phase of the SIS lifecycle and hence need to be addressed with measures that are systematic, methodical and appropriate for the target SIL involved. These measures, when applied properly throughout the realisation lifecycle of a SIS element, define the element's 'Systematic Capability' (SC number 1 to 4). What is helpful about this attribute is that:

- SC 1, 2, 3 or 4 corresponds directly to suitability for use at SIL 1, 2, 3 or 4, respectively (as far as systematic failures are concened)
- SC is a parameter that can be attributed directly to the element (e.g., valve or actuator) itself, rather than 'SIL' which applies to the safety function performed by the entire safety system

When considering the 'SIL capability' of the valve or actuator, the SC criterion is independent to the need to meet the quantitative (probabilistic) failure measures. Hence it is quite possible to have an element whose SC is higher or lower than the 'SIL capability' number of the system safety function that might be inferred purely by considering the quantitative failure data of the device.

In practice, SC comes down to the effectiveness of the manufacturer's quality management system (QMS) to control and avoid systematic weaknesses in the product design, manufacture and user documentation. For example, in areas such as:

- Clear and comprehensive specifications (including drawings and datasheets)
- The design and verification methodology used
- Features in the design that make it robust against environmental stress (electrical and mechanical)
- Features that make the product resilient against human interference (operational and maintenance considerations)
- The competence of the persons performing realisation (development and manufacture)
- The overall QMS to ensure control of supplied parts, documentation control, configuration management, hardware (and software) design tools, staged verification and validation, etc

Systematic measures to address the above requirements are stipulated in BS EN 61508-2 (with further elaboration in BS EN 61508-7 on the 'techniques and measures' to be used). A few of these measures are, to some extent at least, provided within a compliant ISO 9001 QMS, although documenting which ones are used and to what level of effectiveness is not covered in the ISO quality standard. Furthermore, more techniques are required, and to a greater effectiveness, as the target SIL goes up.

A conformity assessment of the measures used in the design, the realisation process and the user documentation will define the SC (1, 2, 3 or 4) for the product. To ensure the assessment goes

smoothly, it is often best to recreate the tables of techniques and measures from BS EN 61508-2 Annex B and document which ones are to be used and to what level, as required by the target SIL shown in the various tables.

Finally, the manufacturer should ensure the SC (1, 2, 3, or 4) is stated in the safety manual.

11. Proof test and partial stroke test

It is possible to improve safety function performance in terms of reducing the average probability of failure on demand (PFD_{AVG}), and therefore increasing availability, by the use of partial stroke testing (PST) of the FE. Effectively, PST is a type of partial proof test typically performed on high integrity valves. Unlike a proof test which can achieve a higher test coverage, the test coverage for a PST is generally much lower. This means that repeated PSTs can only extend the interval between full proof tests to achieve the same PFD_{AVG} (and hence SIL), so full proof tests will be required eventually. However, PST can enable cheaper operating costs and hence improved plant efficiency.

It is important to realise that when applying PST externally to the FE, this does not change the physical integrity or architecture inherent in the valve or actuators themselves. Also, when applied in that way, it is not considered a diagnostic at the device level in the sense that a diagnostic increases λ_{DD} and hence SFF. For these reasons a device manufacturer should not use PST as the basis of an increased 'SIL *n* capability' of the device if the PST then has to be implemented by the user.

If PST is designed-in by the device manufacturer, it may be possible to take credit in terms of improved diagnostic coverage and SFF but:

- this will probably be counteracted by the subsystem being changed from 'type A' to 'type B', imposing stricter limits on the architectural constraints
- the failure rate of the diagnostics needs to be assessed and declared in the safety manual
- the PST interval will need to be very short when compared to the process safety time (and it should consider any FE reliability issues due to the higher cycle rate)

Of course, if running a PST, the revelation of a fault or degraded valve function may lead to an unplanned shutdown (depending on how the PST result is configured) so the impact of this should be considered by the operations team.

PST requires a figure for the test coverage factor. This depends on aspects like the stroke angle (which may be user configured) and the distribution of the device failure rate between the various failure modes which need to be considered for the application. These are aspects that are best judged by the analyst when analysing the failure modes of the device. For a non-redundant FE, the PFD_{AVG} can be calculated using the formula:

$$PFD_{AVG} = [(1\text{-}PTC)\times\lambda_D\times(T_1/2)] + [PTC\times\lambda_D\times(T_{PST}/2)]$$

Where:

PTC = Proof test coverage of the partial stroke test

λ_D = The dangerous failure rate of the safety function

T_1 = Proof test interval (full stroke)

T_{PST} = Partial stroke test interval

12. Assessment and Certification

As regards an independent assessment of the functional safety aspects of systems, including their elements (such as a valves or actuators), BS EN 61508-1 devotes a whole section (8) on this issue. The requirements are given in rather generic language, but essentially an assessment should:

- Be planned, procedural, taking account of previous and future assessments
- Be done by persons who are suitably competent and independent from the item being assessed
- Be fully documented, referring to the criteria (61508 clauses) and evidence of compliance

The BS EN 61508-1 reference above defines the level of independence of the assessor(s) depending on the SIL and the systematic capability (SC) involved. At lower SCs, there may be someone in-house who is suitably independent and competent to perform a full assessment while at higher SCs this is much less likely to be the case. In practice, even at lower SILs/SCs, most manufacturers contract an external specialist organisation to provide the services.

The output of the assessment should be fully documented (e.g., a detailed assessment report), whether this is accompanied by a 'certificate' or not. Certification is not a requirement of the standard in the same way that it is where certain EU Directives apply such as ATEX, with the concept of nationally regulated 'Notified Bodies' appointed under the Directive. Having said that, there are certification bodies that do offer functional safety certification services. There is therefore a wide choice of assessment providers which may be influenced by factors such as price, geographic marketing regions (where certain expectations may vary), the SIL involved, existing relationships with assessment bodies, the assessors' functional safety assessment procedures, tools and competence, accreditations, etc.

When making and reading claims for product 'SIL *n* capability' of the element safety function, it should never be forgotten that there is typically a marketing motivation behind the claim which means that it may well reflect favourable conditions for the product. To this end, all parties submitting or scrutinising claims should:

- Appreciate what is realistic
- Expect full documentation to be available stating the conditions and restrictions of use on which the stated 'SIL *n* capability' (1, 2, 3 or 4) relies (should be contained in the safety manual)
- Understand how the stated data and conditions apply to the intended application(s)

Furthermore, it should always be realised that the party responsible for the overall safety function engineering (e.g., the EPC) should verify the SIF and its SIL, considering all the application and system considerations (which the device/subsystem supplier is not normally fully informed of).

13. Reference documents and bibliography

[1] BS EN 61508-1:2010 Functional safety of electrical, electronic and programmable electronic safety-related systems – general requirements

[2] BS EN 61508-2:2010 Functional safety of electrical, electronic and programmable electronic safety-related systems – system requirements

[3] BS EN 61511-1:2016 Functional safety - safety-instrumented systems for the process industry sector – Part 1: framework, definitions, system, hardware and application programming requirements

[4] BVAA Guidelines on the interpretation of BS EN 61508 – the functional safety standard for the valve and actuator industry

14. Failure rate units and conversions

Common units used for failure rates are shown below, together with their numerical equivalence.

Notation	Symbol (unit)	Example
Scientific	E-XX	1.23E-07
Index	10^{-XX}	1.23 10^{-07}
Failures in time	FIT	123 FIT (per 10^9 hrs)
Failures per million hrs	PMH	0.123

Appendix 1 – Definition of the 'SIL *n* Capability' term

Safety Integrity Level *n* Capability (*n* = 1, 2, 3 or 4)

Valves and actuators are often required to be used in safety systems that perform safety instrumented functions (SIF).

The safety integrity level (SIL 1, 2, 3 or 4) is a dependability metric of a safety instrumented function (SIF) which is performed by a safety system comprising sensor, logic and final element (FE) sub-systems. The SIL takes into account many application, operational and overall system considerations.

Valves, actuators and associated instrumentation do not have SIL ratings as discrete system elements. However, it could be said that an element is "capable for use" in a SIF which needs to achieve a specified SIL (1, 2, 3 or 4).

This has led to the common use of the term 'SIL *n* Capability' (where *n* = 1, 2, 3 or 4), particularly in product marketing or contractual documents. However, this term is not actually defined explicitly in BS EN 61508 and without a clear definition it can be interpreted in different ways. The purpose of this appendix is to provide a definition so it can be understood consistently within this document (and hopefully by all members of the valve and actuator supply chain).

The 'SIL *n* Capability' term may be used to summarise the functional safety properties of an element that can affect the SIL of the SIF it is used in. The number (*n*) should only be regarded as a *provisional indicator* of the potential SIL that can be achieved. It should always be subject to verification once all the other application, operational and system considerations including the other elements are known (which may place further limitations on the SIL). This verification should be done by the organisation (or its appointed agent) responsible for the overall SIF design.

The following table provides information related to the meaning of this term. The word 'element' means a valve, actuator, or some combination of these (e.g., in a final element integrated package).

SIL *n* Capability (*n* = 1, 2, 3 or 4)	
Definition:	A provisional indicator that the safety instrumented system in which the element is used is potentially capable of supporting safety instrumented functions with a SIL up to *n*. (This definition can be compared with the definition for SIL in BS EN 61508-4:2010, Note 3).
Purpose and use of the term:	To support product marketing and contractual specifications. SIL verification must always be performed when all operational, application and overall system factors are known.
How it is derived:	'Bottom up', from a study of the reliability and integrity properties of the element with stated assumptions about the effects (either safe or dangerous) of failure modes in a general type of application. This can be contrasted with how a SIL is determined: 'Top down' from a hazard and risk study, prior to the design or selection of any safety system elements.
What the term refers to:	The properties of an element relating to its hardware reliability and systematic integrity in respect of the specified function(s) of the element that could limit the overall SIL of a SIF that uses the element. (See note 2 below).

Additional notes for clarification:

1. The ‘SIL *n* Capability’ supplied by the manufacturer makes some basic assumptions about the way the element safety function is used in a SIF, for example, whether certain failure modes are safe or dangerous.

2. There is a distinction in the standards between the SIF and the function that each element performs to support the SIF. Each element contributing to the SIF will have its own defined ‘*element safety function’*. This term is defined in BS EN 61508-4, clause 3.5.3.

3. The element safety function will have associated properties relating to its hardware reliability and systematic capability that will place a limit on the SIL of the SIF in which the element is used. The hardware reliability and systematic capability may impose different SIL limits, in which case the lowest number is dominant.

4. When customers (typically EPC contractors) ask for a “SIL rating” for the valve or actuator, device suppliers (or FE integrators) can only be expected to state a ‘SIL *n* Capability’ and to provide the safety manual plus any relevant supporting information. Those responsible for the overall system (e.g., EPC contractors) should be reminded that it is their responsibility to perform the SIF and SIL verification to confirm suitability in their application.

Appendix 2 – Some key reference information from BS EN 61508

This appendix provides a quick reference of some key SIL design information from BS EN 61508. For an explanation of how BS EN 61508 and SILs apply to valve and actuator manufacturers, refer to the [REF 1] or attend the BVAA training course on SILs.

The average probability of failure on demand (PFD_{AVG}) of a low demand safety instrumented function (SIF) required to achieve a SIL, given in BS EN 61508-1 Table 2, is as follows:

Safety Integrity Level (SIL)	Average probability of failure on demand (PFD_{AVG}) for a low demand safety function
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$

Table 1: PFD requirements against SIL

The SIF is typically engineered as 3 subsystems, as represented in Figure 1 below:

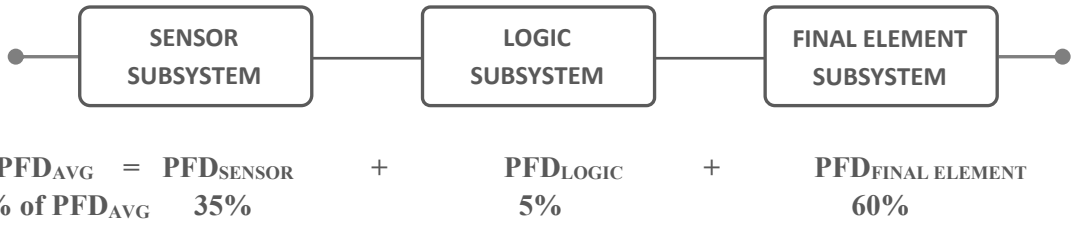


Figure 1: System diagram of a generic SIF

The division of the system PFD_{AVG} into the three percentages shown above is not in the standard but seems to be widely accepted as reasonable targets for the subsystem vendors in the valve and actuator industry.

Each subsystem may be formed from redundant elements to improve dependability (and hence SIL capability) of the safety function. BS EN 61508-2 sets limits on the maximum SIL that a subsystem can be used in, known as *architectural constraints* (BS EN 61508-2 Tables 2 and 3). This limit is determined by the 'hardware fault tolerance' (HFT) within the subsystem (i.e., the redundancy of elements), the 'safe failure fraction' (SFF) of the element(s) and whether the elements used are of simple technology (type A) or more complex technology (type B) in terms of how they can fail.

Safe Failure Fraction (SFF)	Type A element or subsystem (BS EN 61508-2 Table 2)			Type B element or subsystem (BS EN 61508-2 Table 3)		
	Hardware Fault Tolerance (HFT)			Hardware Fault Tolerance (HFT)		
	0	1	2	0	1	2
<60 %	SIL 1	SIL 2	SIL 3	NO SIL	SIL 1	SIL 2
60 % - < 90 %	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

Table 2: Subsystem architectural constraints

Unlike PFD, architectural constraints only apply to subsystems and elements (not systems); the SILs in the table are effectively the limit that the subsystem or element can be used in (unless further architectural measures are used).

SIS designers in the process industry will normally be using BS EN 61511-1. The architectural constraints for final elements in that standard do not assume any SFF; the requirements differ slightly and depend on the demand mode of the safety function, as shown below:

SIL	Minimum Hardware Fault Tolerance (HFT) From BS EN 61511-1 Table 6
1 (any mode)	0
2 (low demand mode)	0
2 (continuous demand mode)	1
3 (high or continuous demand mode)	1
4 (any mode)	2

Appendix 3 – An example safety manual format (for illustration)

1. Introduction

This manual contains the information needed to use the <V/A product> as an element in a safety-instrumented system that needs to perform safety instrumented functions with a specified Safety Integrity Level (SIL 1, 2, 3 or 4). This includes the quantitative failure data of the element together with the assumptions, conditions and restrictions that must be taken into account by the user.

The reliability of the product has been assessed in accordance with BS EN 61508 (equivalent to IEC 61508) for use in SIL applications. Compliance with BS EN 61508 involves ensuring the hardware reliability (in terms of probabilistic type failures) and the measures used to avoid systematic type failures meet the requirements of the SIL for which this product will be used in.

The information in this manual is intended to facilitate the design, integration, installation, operation and maintenance of SIL-rated safety-related systems, as far as this product is concerned. The actual SIL (number) will depend on the specific application and many system considerations that are outside the scope of this safety manual.

In using this product in safety-related systems, it is assumed that the user is competent in the functional safety lifecycle activity they are dealing with and is familiar with the relevant parts of BS EN 61508 (or related standard). If necessary, refer to BS EN 61508-2 and BS EN 61508-6 for further information regarding how elements can be used in the design of safety functions according to the SIL required. (Note that safety functions with higher SILs may be possible with redundant element configurations).

2. Using the product in safety instrumented functions

The following ‘element safety functions’ have been assessed by a failure modes and effects analysis (FMEA) to determine their suitability in the following system safety instrumented function(s):

1. Removal of pneumatic pressure is used to…
2. Application of pneumatic pressure is used to…

The failure data reproduced in the table in section 6 below is considered ‘worst case’ and suitable when using the product in any of the safety applications envisaged above.

3. Conditions or restrictions for use in SIL applications

The failure data and information in section 6 is only valid under the following conditions or restrictions:

1. The product is only used in applications that make use of the element safety function(s) stated above.
2. The product is not to be used in environments that could damage the internal or external parts, e.g., by temperatures, humidity, corrosion, excessive mechanical shock that exceed the published specification.
3. The manufacturer's instructions for installation, operation and maintenance should be complied with.
4. In most applications, the SIL relies on any dangerous diagnosed failures (λ_{DD}) to be repaired within the Mean Time To Repair (MTTR) assumed in the PFD/PFH calculations, unless the detection of such a failure is used to remove the risk (e.g., by shutdown of the affected plant). Likewise, the SIL may rely on periodic proof testing to be performed within the interval assumed in the PFD calculations.
5. Periodic proof testing (at the specified interval T_1) must result in the immediate repair of any failures (λ_{DU}) identified by the test.
6. If the mean time to repair (MTTR) or the proof test interval (T_1) are different from those assumed in the assessment (shown in the table below), then the PFD_{AVG} must be re-calculated and the SIL capability re-verified accordingly. (Refer to section 4 of this manual).
7. The element 'SIL capability' considers the HFT, SFF, Systematic Capability, and the element PFD_{AVG} (for a low demand safety function) and/or PFH (for a high demand safety function). The integrator of the safety instrumented system needs to take into account all other elements, subsystems and lifecycle phases.

4. Proof Testing

The manufacturer recommends that the <V/A product> is periodically proof tested to verify the element safety function, particularly when it is used in 'low demand' safety functions. (Low demand is defined in BS EN 61508-4 as a demand from the plant or machine less frequently than once a year).

A suitable proof test interval (T_1) should be used in order to achieve the required average probability of failure on demand (PFD_{AVG}). Nominal intervals for the proof test interval and Mean Time To Repair (MTTR) have been used in the data (section 6 below) for PFD_{AVG} illustration purposes. If different values are used, the PFD_{AVG} for a non-redundant arrangement (i.e., where the safety function relies on a single element) can be re-calculated as follows:

$$PFD_{AVG} = (\lambda_{DU} + \lambda_{DD})\, t_{CE}$$

Where t_{CE} (the channel equivalent down time) $= (\lambda_{DU} / \lambda_{DD})\,(T_1/2 + MTTR) + (\lambda_{DD} / \lambda_{D})\, MTTR$

For redundant arrangements and non-prefect proof testing refer to BS EN 61508-6 for the equations.

The periodic proof test should be performed of the product, if possible in its installed position, in order to verify all aspects of the functional specification required for the application, for example:

1. Apply the demand signal (e.g., de-energise the solenoid)
2. Verify the <V/A product> responds correctly, within the specified time
3. Repeat the above steps to ensure consistent behaviour
4. Log the successful proof test and/or any servicing/repairs in accordance with local procedures

In addition to the steps above for testing the element safety function, the product must be visually inspected. Any repairs undertaken to restore the product to its fully working condition must be carried out by the assigned competent person and local records maintained. In particular, check for any signs that could lead to loss of integrity (e.g., contact with incompatible chemicals, rust, corrosion, mechanical damage, loosening, unauthorized tampering, etc.)

5. Fault Reporting

If for any reason a functional failure of the <V/A product> is revealed, the manufacturer should be informed directly by notifying them with:

- The serial number(s) of the affected unit(s)
- A brief description of the fault (e.g., description of response when given a demand to perform the element safety function)
- When the fault was discovered or occurred, in particular:
  - □ Prior to commissioning (i.e., transit, storage or during initial installation)
  - □ Post commissioning (during the operational phase)

Fault reports should be marked for the attention of the Quality Manager and sent via:

Email to: info@companyXYZ.co.uk

Telephone: +44(0) 1234 567 890

Note: the above fault reporting is required for internal reliability monitoring, independent of contractual warranty arrangements.

6. Functional safety specification

The following information must be used when using this product as an element in a safety-related system. (Information is arranged against the corresponding clauses in BS EN 61508-2 for user traceability and compliance purposes).

BS EN 61508-2 CLAUSE		INFORMATION REQUIRED BY BS EN 61508 FOR ELEMENTS	SYMBOL	INFORMATION FOR THE <V/A PRODUCT>	
7.4.9.2		Product ID / document no.:		<V/A Product Name>: refer to product datasheet	
7.4.9.3 (a)	D.2.1 (a)	Functional specification of the element safety functions:		Removal of pneumatic pressure is used to…	Application of pneumatic pressure is used to…
7.4.9.3 (b)	D.2.1 (c)	Constraints on the use/application of the element on which the hardware failure rate analysis is based:		None, other than adhering to the conditions or restrictions stated above (section 3)	
7.4.9.3 (d)	D.2.1 (b)	ID of the hardware/software configuration of the element to support the configuration management of the system:		None for these products	
7.4.9.3 (e)		Verification report of the functional specification and Systematic Capability:		RPT12345-1	
7.4.9.4 (a)	D.2.2 (a)	Dangerous failure modes (in terms of behaviour of outputs) not detected by any internal diagnostics: (Note failure rate figures below are worst case of all modes)		Failure to…	Failure to…
7.4.9.4 (b)	D.2.2 (b)	Estimated failure rate of the dangerous failure mode:	λ_D	7.3E-08	3.2E-08
7.4.9.4 (c)	D.2.2 (c)	Dangerous failure modes (in terms of behaviour of outputs) that are detected by any internal diagnostics:		N/A - there are no in-built diagnostics	
7.4.9.4 (d)	D.2.2 (e)	Estimated failure rate of the dangerous detected failure mode:	λ_{DD}	N/A - there are no in-built diagnostics	
	D.2.2 (d)	Failure modes of the internal diagnostics (in terms of behaviour of outputs) that result in failure of the diagnostics:		N/A - there are no in-built diagnostics	
7.4.9.4 (j)	D.2.2 (e)	Estimated failure rate of the internal diagnostics:		N/A - there are no in-built diagnostics	
7.4.9.4 (i)	D.2.2 (f)	The diagnostic test interval for the dangerous detected failures:		N/A - there are no in-built diagnostics	

BS EN 61508-2 CLAUSE		INFORMATION REQUIRED BY BS EN 61508 FOR ELEMENTS	SYMBOL	INFORMATION FOR THE <V/A PRODUCT>	
	D.2.2 (g)	The outputs initiated by the internal diagnostics:		N/A - there are no in-built diagnostics	
7.4.9.4 (g)	D.2.2 (h)	Any periodic proof test or maintenance requirements for the element:		Refer to section above on proof test; Refer to user manual for maintenance requirements; Repairs may also be carried out by the manufacturer	
	D.2.2 (i)	Information to enable the development of external diagnostics, where possible, including details of failure modes and rates:		Provide details…	
7.4.9.4 (m)	D.2.2 (j)	The hardware fault tolerance of the element:	HFT	0	
7.4.9.4 (l)	D.2.2 (k)	Classification of the element:	Type A/B	Type A (all constituent component failure modes are fully defined)	
7.4.9.4 (h)	D.2.2 (k)	The diagnostic coverage, according to the constraints / assumptions governing the application of the item:	DC	0%	
7.4.9.4 (l)	D.2.2 (k)	The safe failure fraction of the element, according to the constraints/assumptions governing the application of the item:	SFF	65%	45%
7.4.9.3 (c)	D.2.3 (a)	The systematic capability of the item:	SC [N]	SC 2	
	D.2.3 (b)	Any instructions or constraints relating to the use of the item in order to prevent systematic failures of the item:		Refer to conditions or restrictions for use in SIL applications (section 3 above).	
7.4.9.4 (e)		Any environmental limits of the element on which the validity of the failure rates (above) depend:		Not exceeding the published product specification	
7.4.9.4 (f)		Any lifetime limits of the element on which the validity of the failure rates (above) depend:		10 years (nominal) with regular maintenance and servicing; 10^5 cycles (if subject to repeated cycling)	
7.4.9.4 (k)		Any information needed to derive the mean repair time (MRT) following detection of a dangerous fault:		N/A from a product design perspective (determined by installation)	