A methodology
For the achievement of Target SIL

Power and productivity
for a better world™

Contents

1.0 Methodology

The purpose of this document is to describe a methodology by which an organisation can demonstrate that the Target Safety Integrity Level (SIL) of a safety instrumented function has been achieved. Throughout this document this methodology is referred to as SIL Achievement.

Successful demonstration that the Target SIL for a safety instrumented function has been achieved is reliant on many aspects of the overall safety lifecycle, such as Hazard and Risk Assessment, SIL Determination, Safety Requirements Allocation, and Realisation - phases 1 to 10 of the IEC 61508 safety lifecycle.

These phases are described in detail elsewhere in this manual. The evidence required in order to demonstrate that a safety instrumented system function meets its Target SIL (i.e. the SIL Achievement exercise) is far more than a quantitative exercise, based solely on target failure measure. Architectural constraints and Systematic capability must also be taken into account. How all of this data is identified, interpreted and used for SIL achievement is described in the following sections.

1.1 SIL achievement - a definition

SIL Achievement is a demonstration that for each Safety Instrumented Function, the Target SIL, as derived from SIL Determination, has been met in accordance with the requirements of IEC61508. Achievement of SIL, for a safety instrumented function, is dependent on the following parameters;

- Architectural Constraint, in terms of - Safe Failure Fraction (SFF) and - Hardware Fault Tolerance (HFT)
- Target Failure Measure, expressed as either:
  - Pfd, or
  - Dangerous Failure Rate (hour)
- Systematic Capability, in terms of
  - Each element* that carries out the safety function
  - The method by which the safety instrumented function was designed and implemented

* An element relates to a piece of equipment, such as a limit switch or a barrier. Multiple elements are connected to form the subsystems (Sensor, Logic Solver and Output) of a safety instrumented function. Refer to section 1.5 for further information.

Only when a safety instrumented function meets the criteria set by IEC 61508 in terms of architectural constraint, target failure measure and systematic capability, can the Target SIL be said to be achieved.

The following sections provide guidance on;

- Responsibilities – the responsibilities of End User/ Operators and Engineering/Equipment suppliers in providing, compiling and demonstrating that the target SIL has been achieved
- Identification of Hazards and SIL Determination – identifying the safety instrumented functions, and assigning a Target SIL
- Safety Requirements – The importance of Safety Requirements in specifying the safety instrumented function
- Design and Engineering – the importance of correctly specifying and integrating the equipment to be used to perform the safety instrumented function
- SIL Achievement – how to demonstrate that SIL has been achieved for a specified safety instrumented function in respect of a Safety Instrumented System.

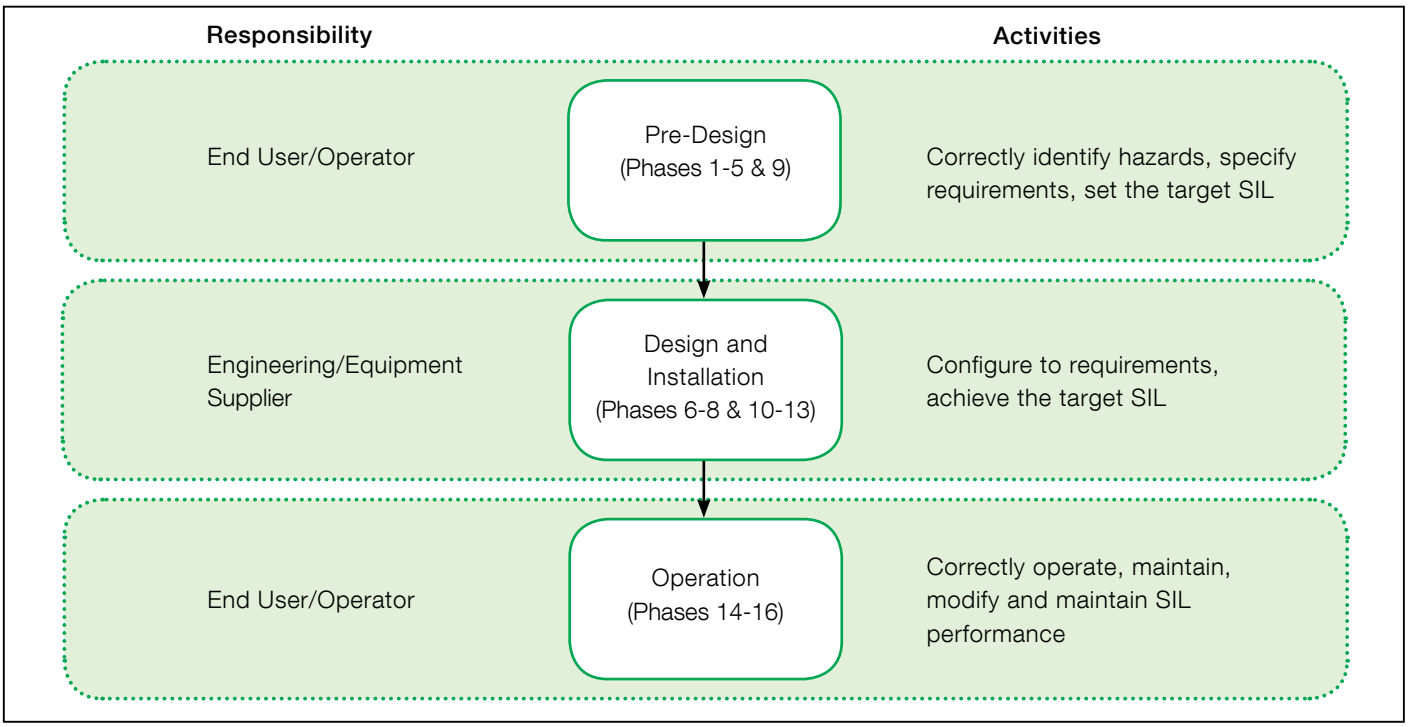
1.2 Responsibilities

In implementing any phase of the safety lifecycle, it is important to understand, and clearly define, the responsibilities assigned to each organisation involved in delivering the safety instrumented system. When performing SIL Achievement, this is particularly important, because without the correct activities, processes and data (outputs) specified during the front end activities of the Overall Safety Lifecycle, SIL Achievement not only becomes very difficult to perform, but the accuracy of the results and how they relate to each safety instrumented function could be brought into question, challenging the initial design assumptions. Failure to achieve the Target SIL, as well as questioning whether the Safety Instrumented System is deemed fit for purpose, may well have other far-reaching effects, such as affecting the fundamental architecture of the Safety Instrumented System and the resulting impact on schedule and cost.

The safety lifecycle can be broken down into three key stages, Pre-Design, Design and Installation and Operation. For each of these stages, responsibility can be assigned as follows;

Responsibilities may be delegated to third parties, for example:

- An Engineering/Procurement/Construction (EPC) company operating in the generic role of Engineering/Equipment Supplier (see diagram) may be appointed by the End User to perform pre-design; the EPC is responsible for delivering the required information to the next organisation in the supply chain.
- A System Integrator may be appointed by the Engineering/Equipment supplier to perform the design of the logic solver subsystem. The system integrator is responsible for engineering the logic solver in accordance with the safety requirements, and following good practice as defined in IEC 61508 and IEC 61511 during the design engineering process. It is the responsibility of the Engineering/Equipment supplier to provide all the necessary information to the System Integrator in order that the latter can build the Safety Instrumented System to meet the specified functional safety requirements.



It can be seen from the diagram above, that each organisation has a responsibility to implement processes and to deliver packages of work to the next organisation in the supply chain. For example, the End User or Operator has a responsibility to provide sufficient information to the Engineering/Equipment Supplier to allow them to complete the design stage of the safety lifecycle.

In terms of SIL Achievement, it is normally the responsibility of the Engineering/Equipment supplier to demonstrate that the Target SIL has been achieved for each safety function, but this is based on the premise that hazards have been correctly identified and safety requirements correctly specified by the End User/plant operator.

1.3 Identification of hazards and SIL determination

With reference to IEC61508-5 (clause A.2), the concept of risk reduction, 'is of fundamental importance in the development of the safety requirements specification for the E/E/PE safety-related systems (in particular, the safety integrity requirements part of the safety requirements specification). The purpose of determining the tolerable risk for a specific hazardous event is to state what is deemed reasonable with respect to both the frequency (or probability) of the hazardous event and its specific consequences. Safety-related systems are designed to reduce the frequency (or probability) of the hazardous event and/or the consequences of the hazardous event.' It is necessary that a hazard and risk analysis be undertaken on the Equipment Under Control (EUC) and the EUC control system in order to identify the process hazards; the risk resulting from the hazardous event(s) associated with the identified hazard and, if necessary, identify what has to be done (prevention and/or mitigation) and to what performance criteria, to ensure that the tolerable risk is achieved. Further information relating to the concept of tolerable risk can be found in IEC61511-3 (Annex A). To achieve functional safety it is necessary to determine:

- What has to be done to prevent the hazardous event (the safety function);
- The required performance of each safety function (the Safety Integrity Level). Therefore, for each identified hazard, which requires a risk reduction measure, a safety function is identified, which is required to meet a specified (Target) SIL. Typically Hazard and Operability Studies (HAZOP) are used to identify where protection is required and the safety function required, whilst SIL determination methods are employed (such as LOPA or Risk Graph) to determine the required (target) SIL. These concepts are described in detail elsewhere in this document.

For example, after performing a HAZOP study on the Equipment Under Control (EUC) and the EUC control system, the functionality of the safety function shall be specified. For example: 'In order to prevent the rupture of pressure tank VS-01, Valve V-01-01 must be opened within 2 seconds, when the pressure in vessel VS-01 rises to 2.6 bar' This is the functionality of the safety function.

After performing the risk assessment, the safety integrity of the safety function shall be specified. For example:

'The safety integrity of the safety function must be SIL 1' This is the Target SIL of the safety function.

In conclusion:
'In order to prevent the rupture of pressure tank VS-01, Valve V-01-01 must be opened within 2 seconds, when the pressure in vessel VS-01 rises to 2.6 bar'. The safety integrity of the safety function shall be SIL 1'

An important concept here is that safety integrity is applied to a safety function, not to the safety-related system so;

- It is correct to say that 'Safety Function x requires a Target SIL of y'
- It would be incorrect to say that the 'safety related system requires a target SIL of y', without also providing the required safety integrity of each of the safety functions executed by the safety-related system.

The safety function descriptions and their associated target SIL's need to be provided to the Engineering/Equipment Supplier, to enable them to complete Phase 10 of the Overall Safety Lifecycle, and ultimately demonstrate SIL Achievement. The mechanism by which this information (functionality of the safety function and safety integrity of the safety function) is provided is through the Safety Requirements Specification.

1.4 Safety requirements

For every Safety Instrumented System, it is the responsibility of the end user/operator to provide a Safety Requirements Specification to the engineering/equipment supplier. This is identified as Phase 4, Overall Requirements, in the IEC 61508 safety lifecycle model.

Guidance is provided in IEC 61508 Part 1 clause 7.10 regarding the content of the Safety Requirements Specification, this is strengthened, for the process industry, in IEC 61511 part 1 clause 10.3.1. For completeness this guidance is given below:

Ref	Requirement to be considered/addressed
1	A description of all the safety instrumented functions necessary to achieve the required functional safety
2	Requirements to identify and take account of common cause failures
3	A definition of the safe state of the process for each identified safety instrumented function
4	A definition of any individually safe process states which, when occurring concurrently, create a separate hazard (for example, overload of emergency storage, multiple relief to flare system)
5	The assumed sources of demand and demand rate on the safety instrumented function
6	Requirement for proof-test intervals
7	Response time requirements for the SIS to bring the process to a safe state
8	The safety integrity level and mode of operation (demand/continuous) for each safety instrumented function
9	A description of SIS process measurements and their trip points
10	A description of SIS process output actions and the criteria for successful operation, for example, requirements for tight shut-off valves
11	The functional relationship between process inputs and outputs, including logic, mathematical functions and any required permissives
12	Requirements for manual shutdown
13	Requirements relating to energize or de-energize to trip
14	Requirements for resetting the SIS after a shutdown
15	Maximum allowable spurious trip rate
16	Failure modes and desired response of the SIS (for example, alarms, automatic shutdown)
17	Any specific requirements related to the procedures for starting up and restarting the SIS
18	All interfaces between the SIS and any other system (including the BPCS and operators)

1.4 Safety requirements continued

19	A description of the modes of operation of the plant and identification of the safety instrumented functions required to operate within each mode
20	The application software safety requirements as listed in section 12.2.2 of IEC 61511-1(2003-01)
21	Requirements for overrides/inhibits/bypasses including how they will be cleared; the specification of any action necessary to achieve or maintain a safe state in the event of fault(s) being detected in the SIS. Any such action shall be determined taking account of all relevant human factors
22	The mean time to repair which is feasible for the SIS, taking into account the travel time, location, spares holding, service contracts, environmental constraints
23	Identification of the dangerous combinations of output states of the SIS that need to be avoided
24	The extremes of all environmental conditions that are likely to be encountered by the SIS shall be identified. This may require consideration of the following: temperature, humidity, contaminants, grounding, electromagnetic interference/radio frequency interference (EMI/RFI), shock/vibration, electrostatic discharge, electrical area classification, flooding, lightning, and other related factors
25	Identification to normal and abnormal modes for both the plant as a whole (for example, plant start-up) and individual plant operational procedures (for example, equipment maintenance, sensor calibration and/or repair). Additional safety instrumented functions may be required to support these modes of operation
26	Definition of the requirements for any safety instrumented function necessary to survive a major accident event, for example, time required for a valve to remain operational in the event of a fire

There is also an additional requirement to add to the table above regarding the consideration of the potential of cyber security threats to the system which should be identified during the earlier hazard and risk assessment phases. A number of these requirements are a pre-requisite to performing an accurate and complete SIL Achievement. For the purpose of this section, only those pre-requisite requirements will be discussed.

1.4.1 Safety Functions and Target SIL

From section 1.2, it can be seen that a key feature of the safety requirements specification is to clearly identify each safety function in terms of its functionality and its Target SIL. Specifically: IEC61511-1 (Clause 10.3.1) requires:

‘A description of all the safety instrumented functions necessary to achieve the required functional safety’

‘The safety integrity level and mode of operation (demand/continuous) for each safety instrumented function’

Frequent use is made of Cause and Effect charts, often as a substitute for Safety Requirements Specifications. However, whilst the chart does provide the logic requirements for the safety system, it does not traditionally identify safety instrumented functions and the Target SIL’s. The cause and effect charts may be supported by a ‘generic specification’ which addresses such items as demand response times, maintenance override schemes, and the required SIL for the ‘system’.

Consider the following extract from a generic specification: ‘The ESD system shall be a PLC based system and shall be certified by TUV for safety related interlocks for SIL 3 as a minimum’

Cause and Effect Emergency Shutdown Logic Pressure Vessel VS-01

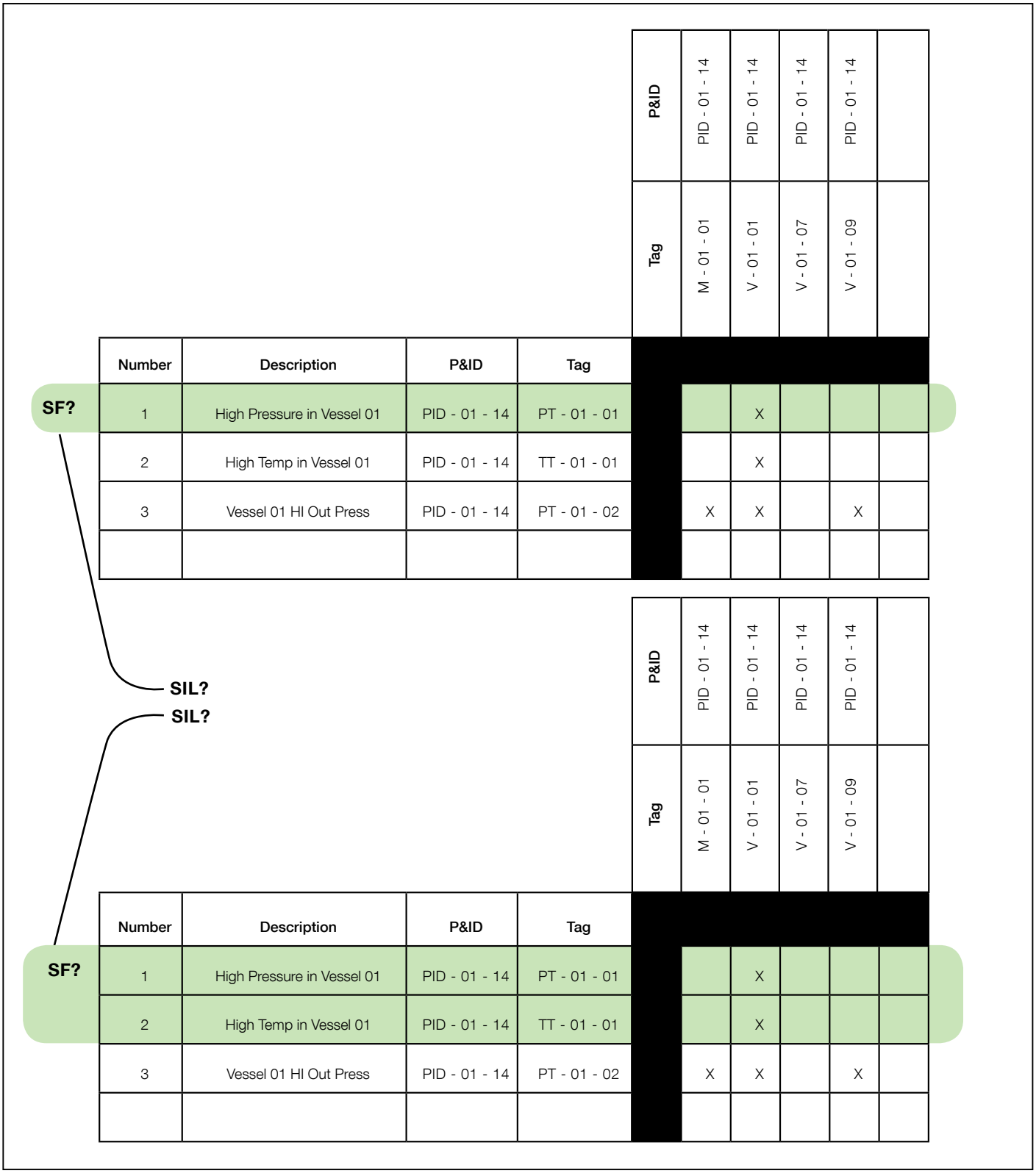
Number	Description	P&ID	Tag		Stop Discharge Pump	Open Vent Valve	Open Cooling Valve	Close Inlet Valve	
				Description	Stop Discharge Pump	Open Vent Valve	Open Cooling Valve	Close Inlet Valve	
				P&ID	PID - 01 - 14	PID - 01 - 14	PID - 01 - 14	PID - 01 - 14	
				Tag	M - 01 - 01	V - 01 - 01	V - 01 - 07	V - 01 - 09	
1	High Pressure in Vessel 01	PID - 01 - 14	PT - 01 - 01			X			
2	High Temp in Vessel 01	PID - 01 - 14	TT - 01 - 01			X			
3	Vessel 01 HI Out Press	PID - 01 - 14	PT - 01 - 02		X	X		X	

Two important questions can be asked:

1. How can individual Safety Instrumented Functions (SIF) be identified? Does cause 1 and 2 or only cause 1 constitute the safety instrumented function? Consider the following extract from a generic specification: ‘The ESD system shall be a PLC based system and shall be certified by TUV for safety related interlocks for SIL 3 as a minimum’

2. What is the Target SIL of the safety instrumented function? The basic specification stated that the PLC system was required to be certified to SIL3.

1.4 Safety requirements continued



Number	Description	P&ID	Tag	P&ID	P&ID	P&ID	P&ID	
				PID - 01 - 14	PID - 01 - 14	PID - 01 - 14	PID - 01 - 14	
				M - 01 - 01	V - 01 - 01	V - 01 - 07	V - 01 - 09	
1	High Pressure in Vessel 01	PID - 01 - 14	PT - 01 - 01		X			
2	High Temp in Vessel 01	PID - 01 - 14	TT - 01 - 01		X			
3	Vessel 01 HI Out Press	PID - 01 - 14	PT - 01 - 02	X	X		X	

Number	Description	P&ID	Tag	P&ID	P&ID	P&ID	P&ID	
				PID - 01 - 14	PID - 01 - 14	PID - 01 - 14	PID - 01 - 14	
				M - 01 - 01	V - 01 - 01	V - 01 - 07	V - 01 - 09	
1	High Pressure in Vessel 01	PID - 01 - 14	PT - 01 - 01		X			
2	High Temp in Vessel 01	PID - 01 - 14	TT - 01 - 01		X			
3	Vessel 01 HI Out Press	PID - 01 - 14	PT - 01 - 02	X	X		X	

If a comprehensive safety requirements specification is produced, we would know that:
'In order to prevent the rupture of pressure tank VS-01, Valve V-01-01 must be opened within 2 seconds, when the pressure in vessel VS-01 rises to 2.6 bar' and 'The safety integrity of the safety instrumented function must be SIL 1'

This provides a clear description of the required functionality of the safety instrumented function and the Target SIL for the safety function.

1.4.2 Mode of Operation

The required mode of operation of the safety instrumented function is important when assessing the target failure measure. IEC61511 Part 1 Clause 10.3.1 requires: 'The safety integrity level and mode of operation (demand/continuous) for each safety instrumented function to be defined. The mode of operation of each safety function impacts the calculation of achieved SIL for the target failure measure; refer to IEC61508 Part 1 Clause 7.6.2.9:

Table 1: Target failure Measures for a Safety Function Operating in Low Demand Mode of Operation

Safety Integrity Level	Low Demand Mode of Operation Average probability of the failure to perform its design function on demand (Pfdavg)
4 3 2 1	$> 10^{-5}$ to $< 10^{-4}$ $> 10^{-4}$ to $< 10^{-3}$ $> 10^{-3}$ to $< 10^{-2}$ $> 10^{-2}$ to $< 10^{-1}$

Table 2: Target failure Measures for a Safety Function Operating in High Demand Mode of Operation

Safety Integrity Level	High Demand or Continuous Mode of Operation Probability of a dangerous failure per hour
4 3 2 1	$> 10^{-9}$ to $< 10^{-8}$ $> 10^{-8}$ to $< 10^{-7}$ $> 10^{-7}$ to $< 10^{-6}$ $> 10^{-6}$ to $< 10^{-5}$

It can be seen from Tables 1 and 2, that the target failure measure is: For low demand mode of operation, the average probability of the failure to perform its design function on demand (Pfd_{avg}) For high demand or continuous mode of operation, the probability of dangerous failures per hour (Pfh) These different target failure measures for the different modes of operation have a have a significant impact on how the required SIL is determined.

For example:
A safety controller is selected by the Engineering/Equipment Supplier. The element is certified by a third party, and the supporting certification documentation states that 2.25×10^{-5} has been achieved for the element.

This raises two questions:
a) Does this refer to a safety function operating in a low demand mode of operation and 2.25×10^{-5} represents the average probability of failure on demand of the element for dangerous random hardware failures (Pfd_{avg})?; or

b) Does this refer to a safety function operating in a high demand or continuous mode of operation and 2.25×10^{-5} represents the probability of dangerous failures per hour (Pfh)?

If the answer is (a), then the Pfdavg achieved is in the SIL 4 band. Whereas if the answer is (b), then the Pfh is only in the SIL 1 band.

1.4.3 Proof Test Interval

It is a requirement in both IEC 61508 and IEC 61511 that for a specified safety instrumented function, being carried out by a Safety Instrumented System, the Pfd_{avg} of the dangerous random hardware failures be evaluated. It is possible to do this by estimating the Pfdavg for each subsystem and then summating them to find the total for the Safety Instrumented System (see IEC 61508-6 (Annex B).

An important parameter when undertaking such an evaluation is the proof-test interval. IEC61511-1 (Clause 10.3.1) requires a specification of the: 'Requirement for proof-test intervals'

The calculated Pfd_{avg} for a subsystem is based on the following calculation (Note that this is a very simplistic calculation; refer to IEC61508-6 (Annex B) for a fuller account of this issue): For a 1oo1 architecture, $PFD = \lambda_{DU} \times T/2$

Where:
Pfd_{avg} = Average probability of failure on demand for the group of voted channels in respect of the dangerous random hardware failures
λ_{DU} = Undetected dangerous failure rate for random hardware failures
T = Proof Test Interval in hours

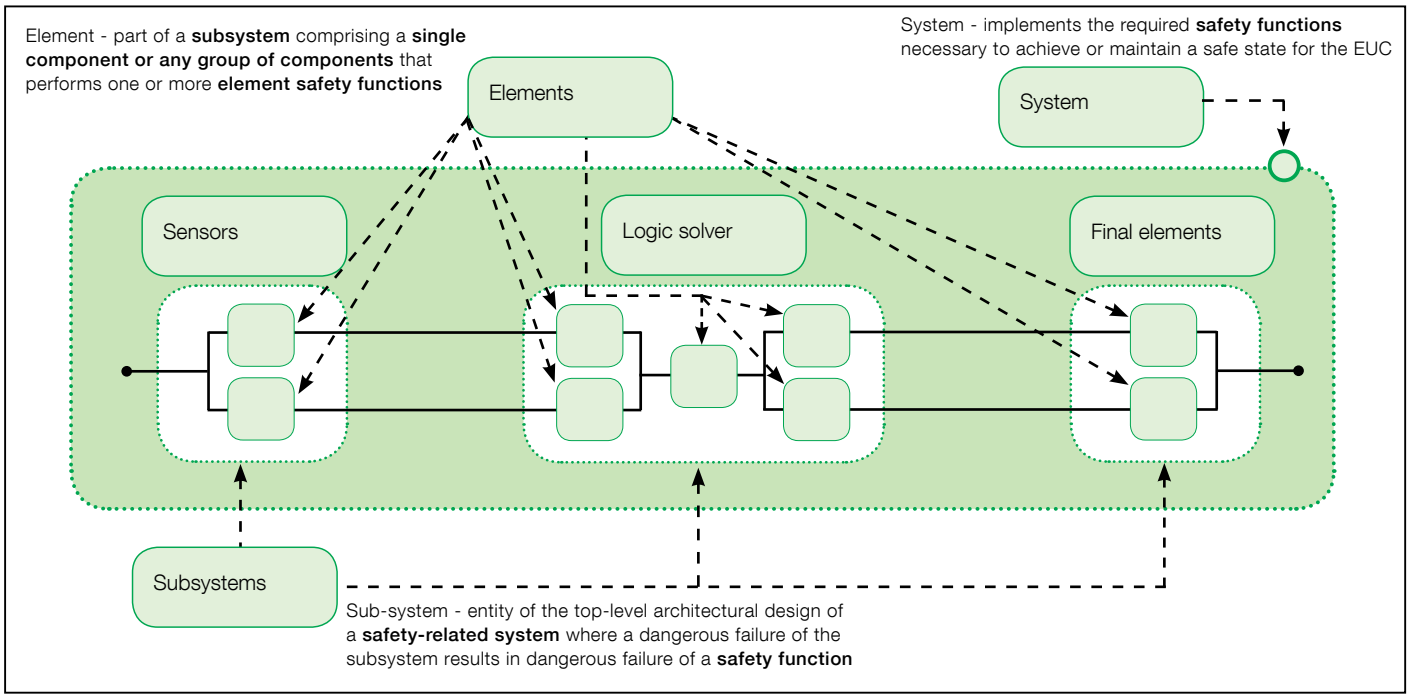
It can be seen from the calculation that, without knowing the required proof test interval, the Pfd_{avg} cannot be determined. An example of how the change of the proof test interval can affect the Pfd_{avg} is as follows:

A safety controller is selected by the Engineering/Equipment Supplier. The safety controller has been certified by a third party, and the supporting certification documentation states that a Pfd of 2.25×10^{-5} has been achieved based on a proof test interval of 8 years. It can be seen that if the proof test interval was to be changed to, say 6 months, then assuming all the other reliability parameters where to remain the same then the Pfd_{avg} for the safety controller would be reduced by a factor of 16.

1.5 Design and engineering

The following section provides an example SIF architecture arranged to emphasise the importance of architectural hierarchies as required of IEC 61508. The key issue is to determine the maximum allowable SIL for a safety function and this is dependent on whether the element is a type A or type B device and is also reliant on both the SFF and the HFT of the element.

The requirements for determining the maximum SIL with respect to the parameters previously mentioned, are specified in clause 7.4.4.2 of 61508 Ed 2, Part 2 if Route 1H is to be used for compliance. Also with respect to Ed 2 of the standard, an uplift can be made for SIL level use based on systematic claims providing independence can be demonstrated between the sub-system elements.



With reference to the simple example above, it is important to stress that the designer needs to define the architecture, elements, subsystems, and overall system and fully understand how failures will impact on the ability of the individual SIF's to perform on demand. These requirements should be undertaken before commencing the SIL Achievement exercise. Also it is an essential stepping stone for providing the necessary assessment information for future SIF SIL Achievement demonstration. See IEC 61508 Ed 2 Part 2, 7.4.2.

Phase 10 of IEC 61508, realisation of the safety lifecycle, relies on information produced by the end user/operator during phases 4, 5 & 9 of the safety lifecycle, Overall Safety Requirements and Safety Requirements Allocation. Based on the safety requirements specification the engineering/ equipment supplier can begin to allocate safety functions and design the safety system.

As part of the design and engineering process, each safety function defined in the safety requirements specification, is deconstructed into the sub-systems and elements required in order to execute that function:

Where:

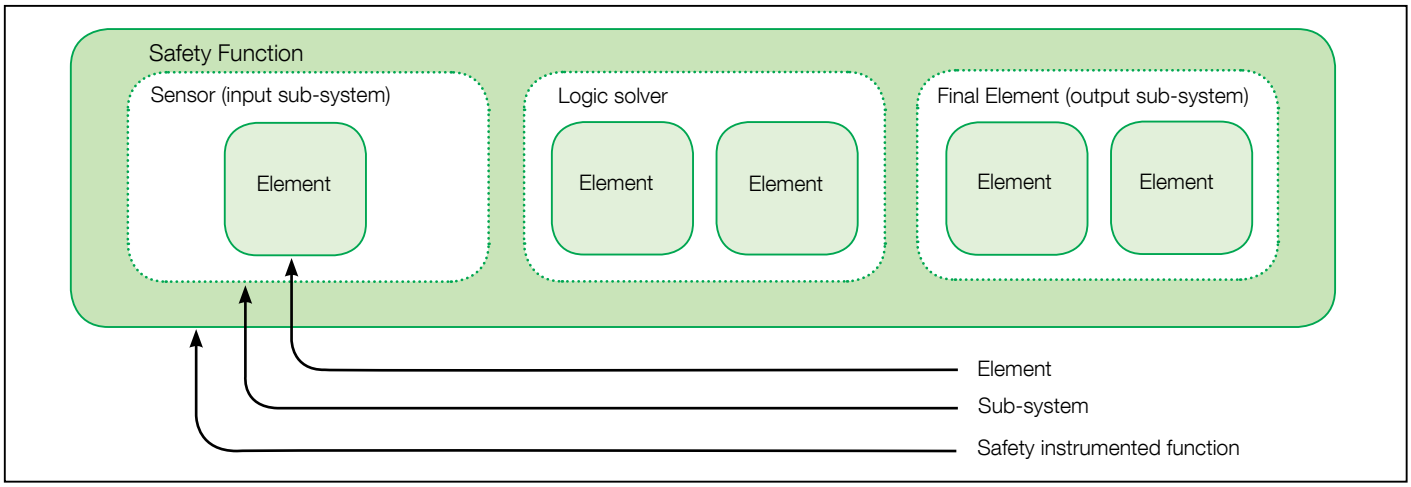
- The Safety Instrumented System, to carry out the safety instrumented function, comprises of an Input Sub-System, Logic Solver and Output Subsystem
- Sub-Systems comprise of single or multiple elements.
- Elements are identifiable pieces of equipment, consisting of individual components, for example a pressure transmitter, safety controller.

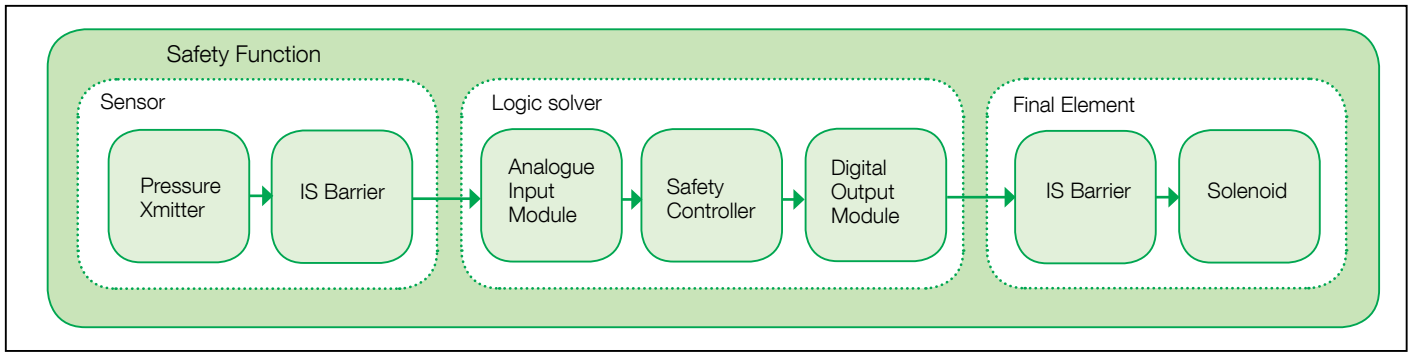
Consider the design of the high pressure safety function described in section 1.2;

'In order to prevent the rupture of pressure tank VS-01, Valve V-01-01 must be opened within 2 seconds, when the pressure in vessel VS-01 rises to 2.6 bar'

'The safety integrity of the safety function must be SIL 1'

The architecture for this high pressure safety function can be interpreted as opposite.





In the example above, it can be seen that the Safety Instrumented System comprises of three subsystems and seven elements:

- Sensor Sub-System
  - Pressure Transmitter Element
  - IS Barrier Element
- Logic Solver Sub-System
  - Analogue Input Module Element
  - Safety Controller Element
  - Digital Output Module Element
- Output Sub-System
  - IS Barrier Element
  - Solenoid Element

In addition to the above subsystems, the Safety Instrumented System will also comprise of additional ancillary elements such as cables and power supplies and power voters that may not have a direct impact on the achievement of SIL. How to deal with this equipment is described in section 1.5.1 and 1.5.2.

When considering what equipment to select for each defined element of the Safety Instrumented System, the Engineering/ Equipment Supplier must consider the following:

- The technical suitability of the element [Does the element provide the technical functionality required for the loop]
- The safety suitability of the element [Is the element certified or assessed for the application it is intended for]

Technical suitability will be addressed as part of the standard design process. As will be seen in the following sub-sections, wherever possible elements should be selected based on their compliance and certification or assessment to IEC 61508.

1.5.1 Adoption of Good Practice Design and Installation Standards

For any Safety Instrumented System, there are elements where the adoption of good installation practice is deemed reasonable to achieve the degree of safety integrity required to prevent systematic failures from arising.

An example where the adoption of good practice may be sufficient would be failures arising from incorrect cable or module installation or termination. Failures from such causes may not be considered to be materially significant because of the adoption of appropriate installation guidelines and procedures including verification activities and appropriate proof test intervals.

(Note that this example is provided for guidance, and should not be interpreted as the rule. Clearly, the higher the SIL of the safety instrumented function, the more rigorous need to be the measures to protect against systematic failures).

1.5 Design and engineering continued

1.5.2 Power supplies

In the context of Power Supplies and Power Voting devices for de-energise to trip safety instrumented functions, no special measures for functional safety need be taken providing that it can be established that the power supplies and power voting devices have no dangerous undetected failure modes. For energise to trip safety functions, power supplies and voting devices may have dangerous undetected failure modes, and therefore will require consideration during SIL Achievement.Whether an element of a safety instrumented function is considered during SIL Achievement or not is of course dependant upon the safety instrumented function itself and each must be assessed individually. Wherever an element is excluded from SIL Achievement, the rationale for this exclusion must be clearly stated.

1.5.3 Suitability of Safety Elements

Before selecting elements for a safety system, it is first important to understand what safety related data is required. In order to demonstrate compliance to IEC 61508 in terms of SIL Capability, each element should have the following information available:

- Safe Failure Fraction (SFF)
- Hardware Fault Tolerance (HFT)
- Type Classification A or B
- Target Failure Measure, expressed as either:
  - Pfd_{avg}, or
  - Dangerous Failure Rate [hour-]
- Systematic Capability (SC)

The objective of gathering the data above for each element of the logic solver is to enable SIL Achievement for the end to end safety function to be performed. Consideration must be given to the availability and supportive evidence of these parameters for each element when selecting those elements on the basis of their functional safety suitability. In the case of elements being supplied from a third party, a validated claim that the elements supplied have the claimed parameters. In the absence of a validated (validated by either an accredited certification body, or independent assessor) claim of any of these parameters from the supplier of the equipment, this should be declared as 'Not Available' in the SIL Achievement Report.

Sound judgment should be used in the selection of equipment without substantiated data – Demonstration of SIL Achievement for a safety function could be considered ineffective if elements are selected that have no available data, the question would be asked as to why the element was selected in the first place!

Note that care should be taken when selecting elements as to their Type classification (i.e. Type A or Type B; see IEC 61508-2 clauses 7.4.4.1.2 and 7.4.4.1.3). Type A and Type B subsystems (or elements) are described below:

- Type A: A device (subsystem/element) can be regarded as a Type 'A' device, if, for the components required to achieve the safety function:
  - the failure modes of all constituent components are well defined; and
  - the behaviour of the subsystem under fault conditions can be completely determined; and
  - there is sufficient dependable failure data from field experience to show that the claimed rates of failure for detected and undetected dangerous failures are met
- Type B: A device (subsystem/element) can be regarded as a Type 'B' device, if, for the components required to achieve the safety function:
  - the failure mode of at least one constituent component is not well defined; or
  - the behaviour of the subsystem under fault conditions cannot be completely determined; or
  - there is insufficient dependable failure data from field experience to support claims for rates of failure for detected and undetected dangerous failures

An elements compliance to, and certification or assessment against IEC 61508, should clearly have identified the type classification.

1.5.4 Legacy Standards

Should the element certification state compliance to DIN V 19250 (or DIN 19250/19251) and DIN V VDE 0801 then the certification will have been based on the safety categories of DIN 19250/19251and the safety requirements of DIN V VDE 0801.

The safety categories relating to these legacy standards are based on classification to AK classes (AK1-AK8) and as such no linkage

of these safety categories can be made to quantified target failure measures (as exists in IEC 61508). Any linkages to SIL's (based on IEC 61508) are based on pragmatic judgments. Therefore, systems which have safety categories classified to DIN V 19250/19251 and designed to DIN V VDE 0801 cannot be claimed to be designed to IEC 61508 (even though there may be statements that a particular AK Class is equivalent to a specific SIL). Where a certificate states compliance to DIN V 19250 (or DIN 19250/19251) and DIN V VDE 0801, the Safe Failure Fraction, Hardware Fault Tolerance and Systematic Capability may not be available. Compliance with those standards, in respect of the specified AK classes, provides a systematic capability determined by the specified AK class, and not IEC 61508.

1.5.5 Determination of Parameters from First Principles

Where no substantiated data (refer to section 1.5.3), either offering compliance with IEC 61508 or legacy standards such as DIN V 19250 (or DIN 19250/19251) and DIN V VDE 0801, determination of the key parameters required from first principles will be required. This process requires very specific technical competency, and should only be attempted by the appropriate, qualified organisations and/or individuals. For each identified element the following shall be determined:

i. The failure modes (in terms of the behaviour of its outputs) due to random hardware failures that result in a failure of the safety function that are not detected by diagnostics internal to the element.

ii. The estimated failure rate for every failure mode in (i).

iii. The failure modes (in terms of the behaviour of its outputs) due to random hardware failures that results in a failure of the safety function that are detected by diagnostics internal to the element.

iv. The estimated failure rate for every failure mode in (iii).

v. The diagnostic test interval for every failure mode in (iii) that is detected by diagnostics internal to the element.

vi. The relevant part of the element that supports the function that is Type "A" and the relevant part of the element that supports the function that is Type "B".

For further guidance, refer to IEC 61508-2; clause 7.4.4.1.2 and 7.4.4.1.3.

1.6 Demonstrating SIL achievement

As part of the design process, the Safety Instrumented System has been deconstructed into Sub-Systems and Elements. For each of those elements, parameters relating to their suitability in terms of functional safety have been collected.

The next step in the process of SIL Achievement is to collate this information, and present the evidence necessary to substantiate the claim that the safety functions described in the safety requirements specification, achieve their Target SIL.

The evidence should be presented in the form of a SIL Achievement Report, which provides, for each safety function, the following:

(1) The Hardware Safety Integrity for the safety function achieved (in the form of the Pfd_{avg} or dangerous failure rate (hour) and HFT (for the specified SFF)); and,

(2) The Systematic Safety Integrity for the safety function achieved (in the form of the Systematic Capability for a subsystem element) including references to any appropriate Techniques and Methods adopted.

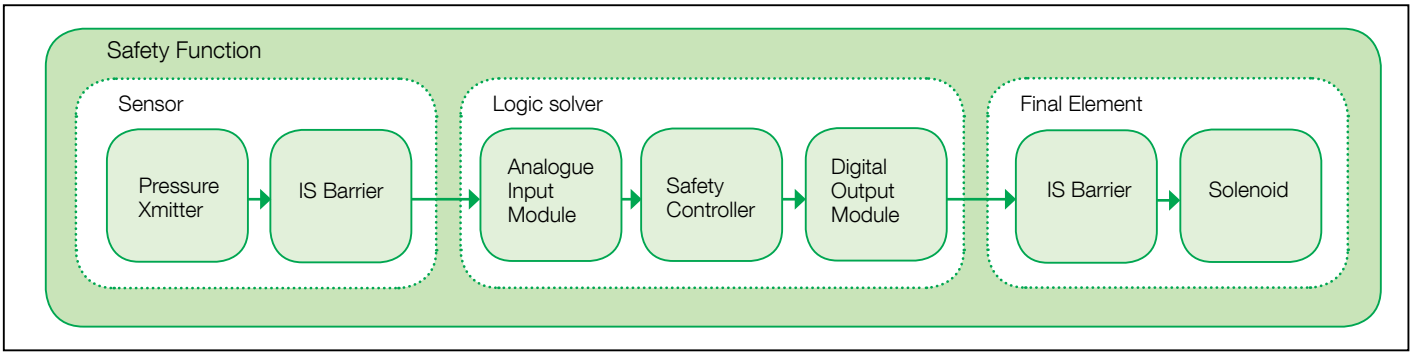
(3) Confirmation, that the targets for (1) and (2), specified in the Safety Requirements Specification, have been met or if the targets have not been met, the reasons.

Note: In respect of (2) above, Systematic Safety Integrity, the Systematic Capability may be claimed using evidence of proven in use. However, using this approach is strongly discouraged, based on the following difficulties:

– Evidence will be required as to how the data was collected many end users may simply discard faulty equipment, and replace with a spares holding, instead of returning to the manufacturer.

- Evidence will be required as to the environment the equipment was used in – a proven in use claim can only be made for devices used in the in the same way, for example the process environment.
- Evidence will be required to substantiate the sample size how many samples need to have been taken before the proven in use claim can be deemed as valid?
- Complexities in the supply chain may mean that accurate records are difficult to obtain – for example, the supplier of the device may not be the manufacturer of the device. The manufacturer of the device may appoint certified repairers.

Note that the concept of “proven in use” is solely related to systematic concepts; it has nothing to do with random hardware failures. The process of demonstrating SIL is described in the following sub-sections. Where examples are provided, these are based on the high pressure trip discussed in section 1.4, for ease of reference, this is shown again below:



1.6 Demonstrating SIL achievement cont

Note that all quantitative and qualitative data quoted in the examples do not relate to a specific product or range of products.

1.6.1 Identification of Generic Functions

SIL Achievement is required to be demonstrated for each safety function; however the concept of 'generic' functions may be identified, based on the following rationale: Where it is established that the route taken from input subsystem to output subsystem, in implementing the safety function, takes the same route then this can be defined as a generic function. In this situation it would be acceptable to provide the evidence of SIL. Achievement only once for this generic function.

This is based on the assumption that all those safety functions, that are to be regarded as generic, have associated with them identical dangerous modes of failure and identical safe modes of failure. If this is not the case then the concept of a generic function is not valid.

When generic safety functions are identified, and adopted in demonstrating SIL Achievement, it is critical that the individual safety functions associated with that generic type are clearly identified and listed.

1.6.2 Demonstration of Achieved Hardware Safety Integrity

The requirements for Hardware Safety Integrity comprise of:

- The Architectural Constraints expressed as a Safe Failure Fraction (SFF) and a Hardware Fault Tolerance (HFT)
- The Pfd_{avg} or dangerous failure rate relating to dangerous random hardware failures

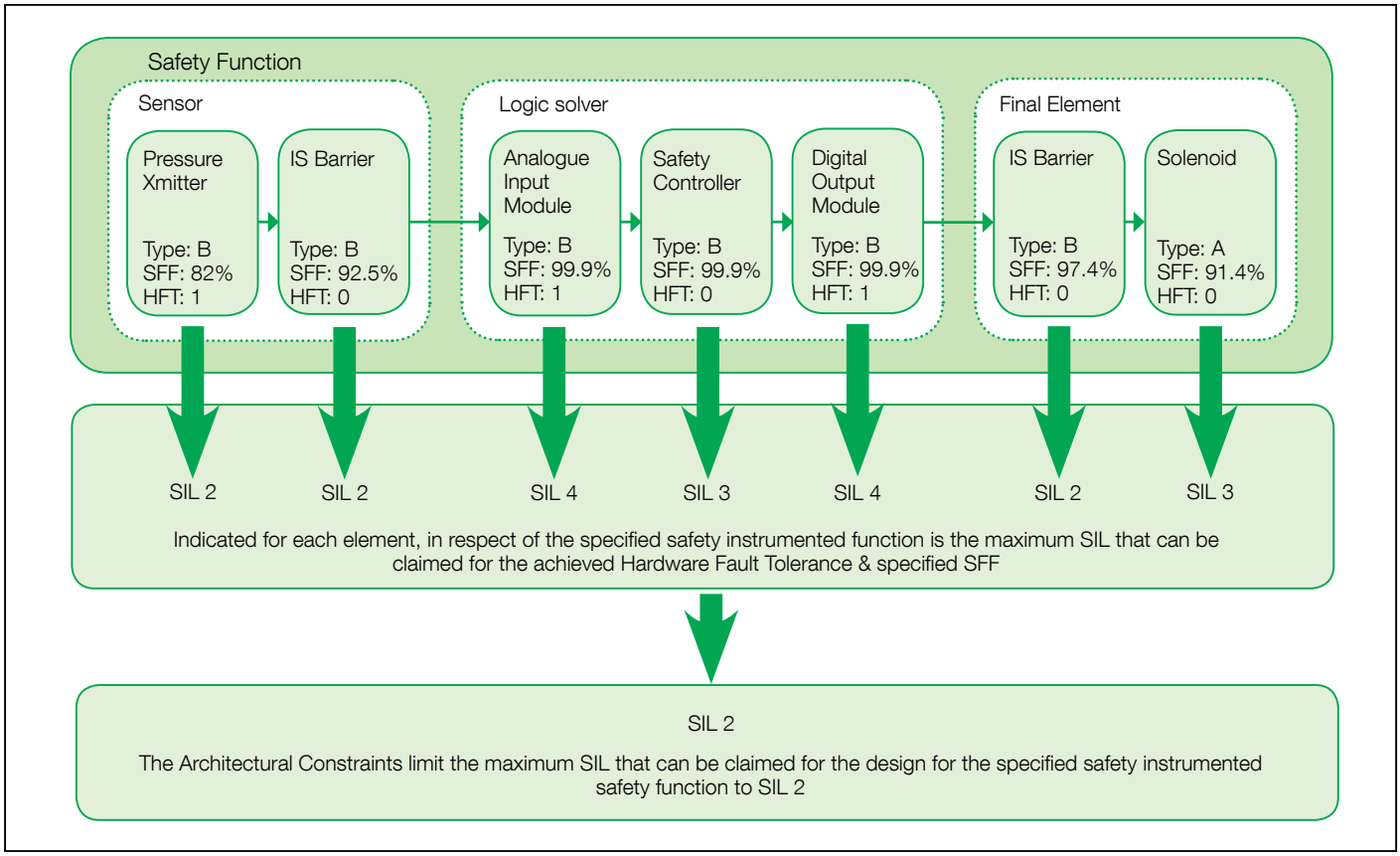
1.6.2.1 Architectural Constraints

Tables 1 and 2 in section 1.4.2 provide the SIL. Reference should be made to IEC61508-2 clauses 7.4.4 to 7.4.4.1.5 for details on interpreting the table.

The two tables address both Type A and Type B safety-related subsystems. The type, either 'A' or 'B', is required to be identified for each element that implements the safety function.

In some sub-system designs additional synthesis of elements can be considered to improve both architecture constraints and systematic capability claims by determining that the chosen sub-system can have an (N+1) argument applied. See IEC 61508 Part 2, clause 7.4.3.

The following diagram provides an example of calculating the architectural constraints for the high pressure trip.



As can be seen from the example on page 18, the architectural constraint has been calculated for each element of the safety function. The architectural constraint is limited by the lowest achieved SIL (in terms of architectural constraint), the Final Element IS Barrier, which is limited to SIL 2.

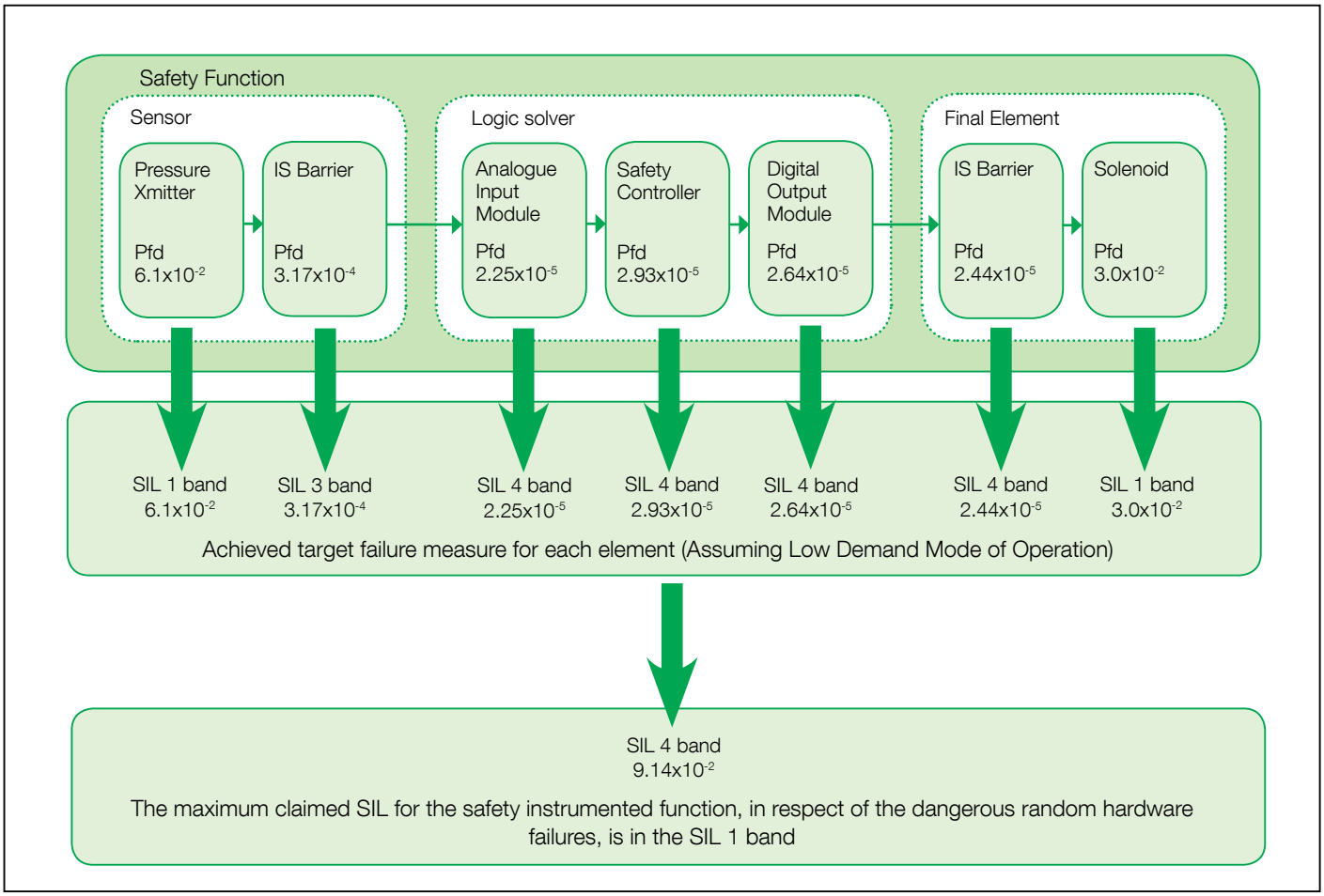
The maximum claimed SIL, in terms of architectural constraint, for the function is SIL 2.

1.6.2.2 Quantification of Dangerous Random Hardware Failures

Target Failure Measure is expressed as the Probability of failure on demand (Pfd) or Probability of failure per hour (Pfh)/dangerous failure rate per hour. The target failure measure, as a basis for determining the measures to be taken to achieve the required safety integrity, is dependent upon whether the safety instrumented function is considered to be operating in low demand (Pfd is used) or high demand mode of operation (Pfh/dangerous failure rate per hour is used).

Referring to section 1.4.2, Tables 1 and 2 provide the target criteria for the target failure measure for the target SIL. Each element, with respect to the specified safety function, is assessed independently.

The following diagram provides an example of calculating the target failure measure for the high pressure trip.



1.6 Demonstrating SIL achievement cont

As can be seen from the example on page 19, the target failure measure has been calculated for each element of the safety function. In the calculation, a low demand mode has been assumed, and it is also assumed that the proof test interval for each element is greater than the required minimum proof test interval required by the function.

Evaluating the total target failure measure achieved is obtained by summation of the Pfd_{avg} values for each subsystem. For more elaborate configurations, for example those that include voted sensor subsystems and which have redundant channels, it would be necessary, in determining the total target failure measure for the Safety Instrumented System, to take into account commoncause failures.

For further information, and examples of more complex target failure measure calculations, refer to IEC61508-6 (Annex B). The maximum claimed SIL, in terms of target failure measure, for the safety instrumented function is in the SIL 1 band.

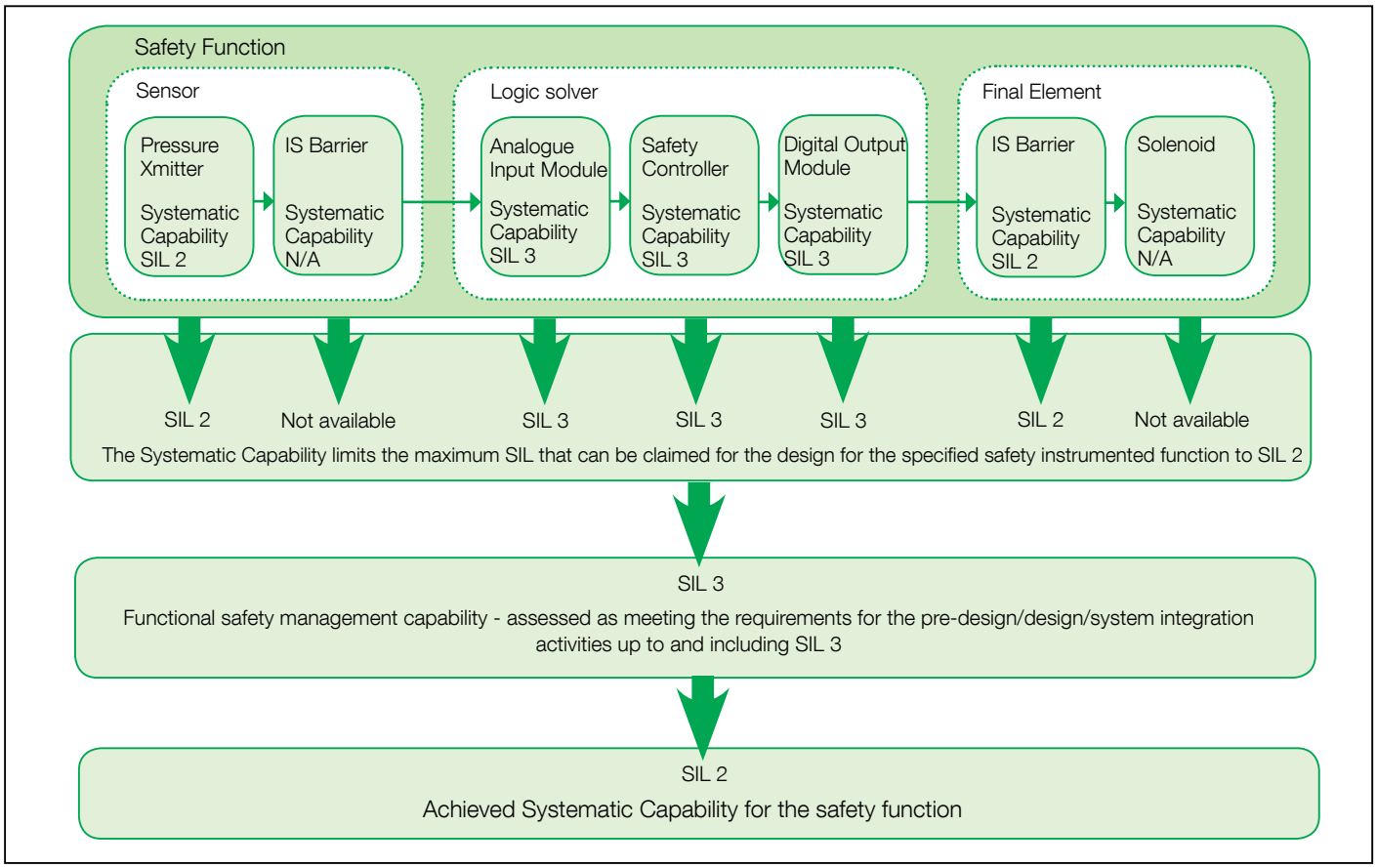
1.6.3 Demonstration of Achieved Systematic Safety Integrity

Systematic Safety Integrity cannot, in general, be quantified and is based on qualitative requirements and tables of specified techniques and measures in IEC61508. Assessment of systematic safety integrity utilises IEC61508, Part 7 Overview of techniques and measures: Annex B and Annex C.

It is necessary for each element involved in the implementation of the specified safety function to meet the systematic safety integrity requirements of the SIL of the safety function. In addition, it is also necessary to ensure that the integration activities and processes for all of the elements of the safety function are achieved in compliance with the requirements of IEC 61508 to ensure that the integration process itself does not lead to unacceptable systematic failures.

To this end, all organisations responsible in the Pre-Design and Design and Installation activities should provide evidence that the safety system has been developed under a functional safety management system, and the integration of the elements, relevant to the specified safety functions, have been performed using suitable techniques and methods. Further information can be found in the chapter 'A methodology for achieving organisational functional safety certification to IEC61508' of this document.

The following diagram provides an example of calculating the systematic capability for the high pressure trip.



As can be seen from the example on page 20, the systematic capability has been obtained for each element of the safety function; with the exception of the sensor IS barrier and the solenoid, where data relating to systematic capability is not available. Pre-design and Design activities have been implemented using a Functional Safety Management System, compliant with IEC61508, and utilising the recommended techniques and tools required to claim a systematic capability of SIL3.

The maximum claimed SIL, in terms of systematic capability, for the function is SIL 2, with the exception of the Sensor IS Barrier, and Final Elements Solenoid, for which no data is available.

1.6.4 SIL Achievement Summary

In the previous sections, a worked example of SIL Achievement has been shown for a simple safety instrumented function, a high pressure trip. A summary of the SIL Achievement exercise, for this high pressure trip is as follows.

Safety Instrumented Function:

'In order to prevent the rupture of pressure tank VS-01, Valve V-01-01 must be opened within 2 seconds, when the pressure in vessel VS-01 rises to 2.6 bar' Target: SIL 1 Mode: Low Demand

Summary of SIL achievement

- In terms of Architectural Constraint, SIL 2 is achieved
- In terms of the dangerous random hardware failures, the Pfd_{avg} achieved is in the SIL 1 band
- In terms of systematic safety integrity, SIL 2 is achieved with the exception of the Sensor IS Barrier, and Final Element Solenoid, for which no data is available

On this basis, the achieved SIL for the high Pressure Trip can be said to be SIL 1, with the exception of the systematic capability of the sensor IS barrier and final element solenoid, for which no data is available.

1.7 Summary

In summarising the methodology for the achievement of a target SIL, it is important to consider the following key points:

1. SIL Achievement relates to the ability of the designed Safety Instrumented System (SIS) to carry out the specified safety instrumented function to the required SIL.

Achievement of a target SIL is based on individual safety instrumented functions (or generic safety instrumented functions). This is an important concept, as without having a clear definition of each safety instrumented function, and a target SIL for each of those safety instrumented functions, SIL Achievement becomes an impossible task.

It is also important to understand that the concept of a 'SIL x Safety Instrumented System' is not correct, as SIL applies to safety instrumented functions that are part of a Safety Instrumented System. Elements of that Safety Instrumented System are required to be suitable for use in carrying out a SIL x safety function. Safety System Requirements Specifications need to avoid simply stating 'Supply a SIL x Safety System'.

2. Demonstration of SIL Achievement is not just about Pfd_{avg}. Producing a reliability and availability report for a Safety Instrumented System is not demonstrating that the target SIL has been met for each safety instrumented function. SIL Achievement is a far more complex process, involving Architectural Constraint, and Systematic Capability, as well as the Pfd_{avg}. Also remember that Pfdavg is not a suitable failure measure for a high demand/ continuous mode of operation.

Systematic Capability must also be considered during the design and engineering phase. Just because individual elements used to carry out the safety instrumented function are certified for use, does not mean that when those elements are bought together and configured that the requirements of the safety instrumented function have been achieved in the design of the Safety Instrumented System. The configuration of the Safety Instrumented System will have an impact on the Systematic Capability achieved. The integration and configuration of the safety instrumented function should also follow recognised techniques and methods as described in IEC 61508 to ensure systematic capability is achieved.

3. The importance of a good safety requirements specification. Without a good Safety Requirements Specification, the information necessary for the demonstration of SIL achievement may not be available. Apart from the obvious need to identify individual safety instrumented functions and their Target SIL, identifying the mode of operation and proof test requirements are also necessary in order to demonstrate SIL Achievement.

4. The importance of equipment selection. Once safety instrumented functions and their target SIL have been identified, it is critical that the correct elements are specified which will implement each safety instrumented function. Incorrect specification of these elements may mean that the target SIL is unachievable – impacting not only functional safety but also schedule and cost. For the Engineering/Equipment Supplier it is important to ensure that the correct equipment is identified during the proposal and initial design phases of the project – of course this process requires a good Safety Requirements Specification from the End User/Operator.

What of the future? It is clear that education is an important factor. Each organisation should clearly understand their position, and responsibilities in the supply chain. Specifically:

1. Equipment suppliers should provide comprehensive and complete data for their products – Hardware Fault Tolerance, Safe Failure Fraction, Target Failure Measure, device type and systematic capability.

2. All members of the supply chain should consider implementing comprehensive functional safety management systems. Certification of an organisations functional safety management system by third parties provides evidence to others in the supply chain that functional safety and thus systematic capability of that organisation can be demonstrated and substantiated. Finally, Industry in general should begin to understand that SIL is a characteristic of the Safety Instrumented Function, not the Safety Instrumented System, and the demonstration of SIL is not just about Pfd_{avg}!

Contact us

Assured and certified products, services, delivery and execution.

For further information please contact:
ABB Safety Lead Competency Centre
Howard Road, Eaton Socon, St Neots
Cambridgeshire, PE19 8EU
Phone: +44 (0)1480 475321
E-Mail: oilandgas@gb.abb.com

www.abb.com/oilandgas

Notes:
ABB reserves the right to make technical changes or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. ABB does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.

Printed in UK (01.2013)

3BGB 000939/01/13 .. ©ABB Limited 2013 Process Safety

Power and productivity
for a better world™