SIL methodology

A methodology for SIL verification in accordance with IEC 61508 and IEC 61511 requirements

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 (SIF) has been achieved. Throughout this document this methodology is referred to as SIL verification.

Contents

1.0 Methodology

Successful demonstration that the target SIL for a Safety Instrumented Function (SIF) 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 and phases 1 to 4 of the IEC 61511 safety lifecycle.

These phases are described in detail elsewhere in this document. The evidence required in order to demonstrate that a Safety Instrumented System (SIS) function meets its target SIL (i.e. the SIL verification 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 verification is described in the following sections.

1.1 SIL verification - a definition

Safety Integrity Level (SIL) verification is a demonstration that for each SIF, the target SIL, as derived from SIL determination, has been met in accordance with the requirements of of IEC 61508 / IEC 61511.

As part of SIL verification for a SIF, the SIL calculation aspects of this process 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 device* that carries out the safety function
  - The method by which the safety instrumented function was designed and implemented

Only when a SIF 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 correctly calculated..

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 SIFs and assigning a target SIL
- Safety requirements - The importance of safety requirements in specifying the SIF
- Design and engineering - the importance of correctly specifying and integrating the equipment to be used to perform the SIF
- SIL verification - how to demonstrate that SIL has been achieved for a specified SIF in respect of a SIS

—
*A device 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 SIF. Refer to section 1.5 for further information.

1.2 Responsibilities

In implementing any phase of the safety lifecycle, it is important to understand and clearly define the responsibilities of each organization involved in delivering the SIS. This is particularly important when performing SIL verification. Each activity, process and data output is specified during the front end activity of the overall safety lifecycle, but absence of such information can make SIL verification very difficult to perform. This is because each piece of information relates to a safety instrumented function. Absence of information raises questions about the accuracy of results and their relationship to each safety instrumented function.

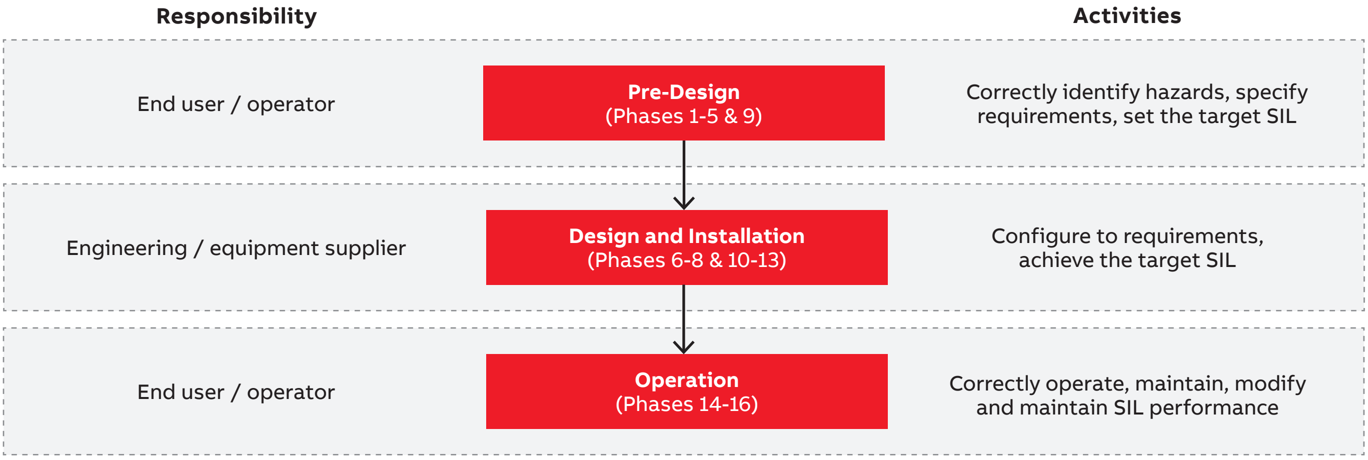
Failure to achieve target SIL can then have far-reaching effects that impact on the fundamental architecture of the SIS with further negative consequences for schedule and costs.
The safety lifecycle can be broken down into three key stages, pre-design, design and installation and operation. For each of these stages, responsibility can be assigned as shown in the diagram below.

It can be seen from the diagram below, 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.

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 SIS to meet the specified functional safety requirements

In terms of SIL verification, it is normally the responsibility of the engineering / equipment supplier 'the SIS designer' 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.


Responsibility
Activities
End user / operator
Pre-Design (Phases 1-5 & 9)
Correctly identify hazards, specify requirements, set the target SIL
Engineering / equipment supplier
Design and Installation (Phases 6-8 & 10-13)
Configure to requirements, achieve the target SIL
End user / operator
Operation (Phases 14-16)
Correctly operate, maintain, modify and maintain SIL performance

1.3 Identification of hazards and SIL determination

The concept of risk reduction, 'is of fundamental importance in the development of the safety requirements specification for the SIS (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. To identify the process hazards it is necessary to carry out a hazard and risk analysis on:

- The operating process plant and the basic control system (BPCS)
- Hazardous event(s) associated with the identified hazard and identify
- What has to be done (prevention or mitigation)?
- Identify what performance criteria will ensure that the tolerable risk is achieved?

Further information relating to the concept of tolerable risk can be found in IEC 61511-3 (Annex A). The following must be identified to achieve functional safety:

- What must be done to prevent the hazardous event (the safety function)
- The SIL of each safety function. For each identified hazard requiring a risk reduction measure, a 'safety function' is required to meet a specified target SIL. Typically Hazard and Operability Studies (HAZOP) are used to find where protection and the safety function are required. SIL determination methods such as fault tree analysis, LOPA or risk graph are used to determine the required target SIL i.e. identification of the 'safety integrity'.

For example, after performing a HAZOP study on the process plant and BPCS 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 SIS

The safety function descriptions and their associated target SIL's need to be provided to the engineering / equipment supplier, to enable them to complete their responsibilities within the overall safety lifecycle, and ultimately demonstrate SIL verification. 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 (SRS).

1.4 Safety requirements

For every Safety Instrumented System (SIS), it is the responsibility of the end user / operator to provide a Safety Requirements Specification (SRS) 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 SRS, this is strengthened, for the process industry, in IEC 61511 part 1 clause 10.3.

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. Refer to IEC 62443 for supporting details. A number of these requirements are a pre-requisite to performing an accurate and complete SIL verification. 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 10.3.2) 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 SRS. However, whilst the chart does provide the logic requirements for the safety system, it does not traditionally identify safety instrumented functions and the target SILs. 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’.

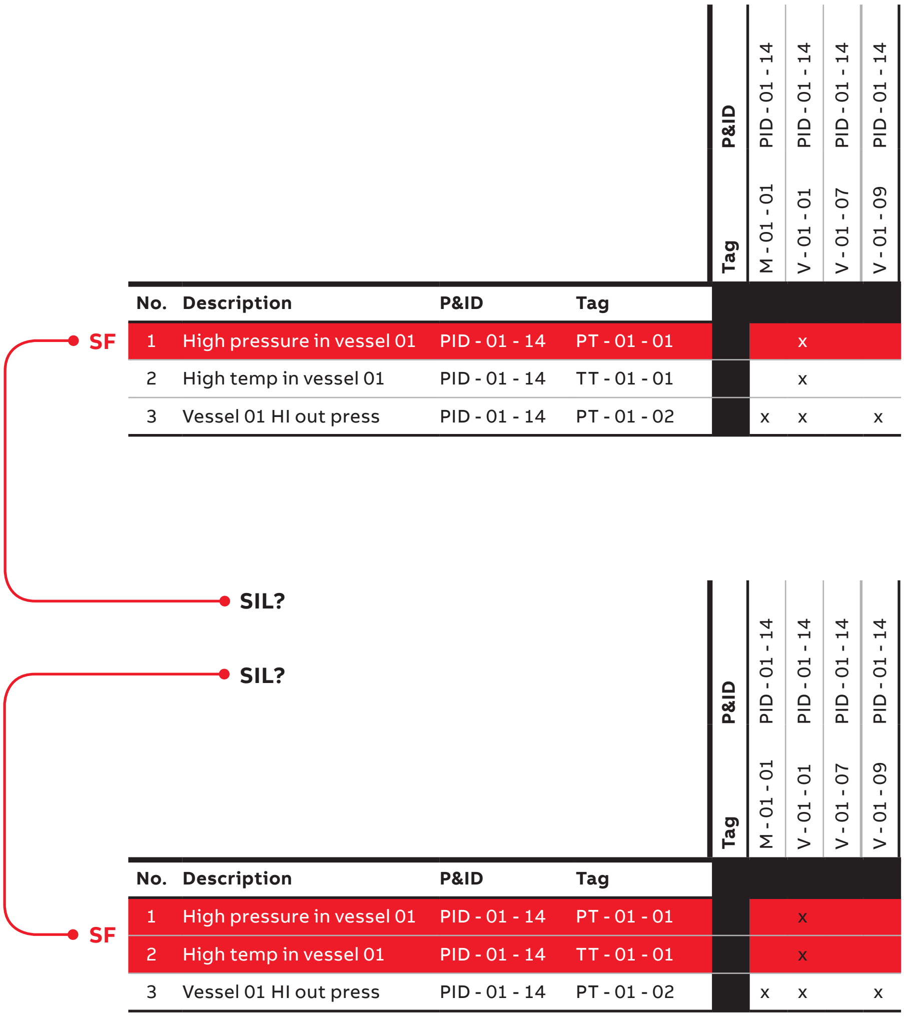
Cause and effect emergency shutdown logic pressure vessel VS-01

			Tag	M - 01 - 01	V - 01 - 01	V - 01 - 07	V - 01 - 09
			P&ID	PID - 01 - 14	PID - 01 - 14	PID - 01 - 14	PID - 01 - 14
			Description	Stop discharge pump	Open vent valve	Open cooling valve	Close inlet valve
No.	Description	P&ID	Tag				
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

Consider the following extract, left, from a generic specification: 'The ESD system shall be a PLC based system and shall be third party certified for safety related functions for SIL 3 as a minimum'.

Two important questions can be asked:

- 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 third party certified for safety related functions for SIL 3 as a minimum'
- 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



			Tag	M - 01 - 01	V - 01 - 01	V - 01 - 07	V - 01 - 09
			P&ID	PID - 01 - 14	PID - 01 - 14	PID - 01 - 14	PID - 01 - 14
No.	Description	P&ID	Tag				
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

			Tag	M - 01 - 01	V - 01 - 01	V - 01 - 07	V - 01 - 09
			P&ID	PID - 01 - 14	PID - 01 - 14	PID - 01 - 14	PID - 01 - 14
No.	Description	P&ID	Tag				
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 (SIF) must be SIL 1'.

This provides a clear description of the required functionality of the SIF and the target SIL for the safety function.

1.4.2 Mode of operation

The required mode of operation of the SIF is important when assessing the target failure measure. IEC 61511 part 1 clause 10.3 requires: ‘The safety integrity level and mode of operation (demand / continuous) for each SIF to be defined.

The mode of operation of each safety function impacts the calculation of achieved SIL for the target failure measure; refer to IEC 61508 part 1 clause 7.6.2.9:

—

Table 1: Target failure measures for a safety function operating in low demand mode of operation.

SIL	**Low demand mode of operation** Average probability of the failure to perform its design function on demand (PFDavg)
4	> 10^{-5} to < 10^{-4}
3	> 10^{-4} to < 10^{-3}
2	> 10^{-3} to < 10^{-2}
1	> 10^{-2} to < 10^{-1}

—

Table 2: Target failure measures for a safety function operating in high demand mode of operation.

SIL	**High demand or continuous mode of operation** Probability of a dangerous failure per hour
4	> 10^{-9} to < 10^{-8}
3	> 10^{-8} to < 10^{-7}
2	> 10^{-7} to < 10^{-6}
1	> 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 (PFDavg)
- 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 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 x 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 x 10-5 represents the average probability of failure on demand of the element for dangerous random hardware failures (PFDavg)? Or
b. Does this refer to a safety function operating in a high demand or continuous mode of operation and 2.25 x 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

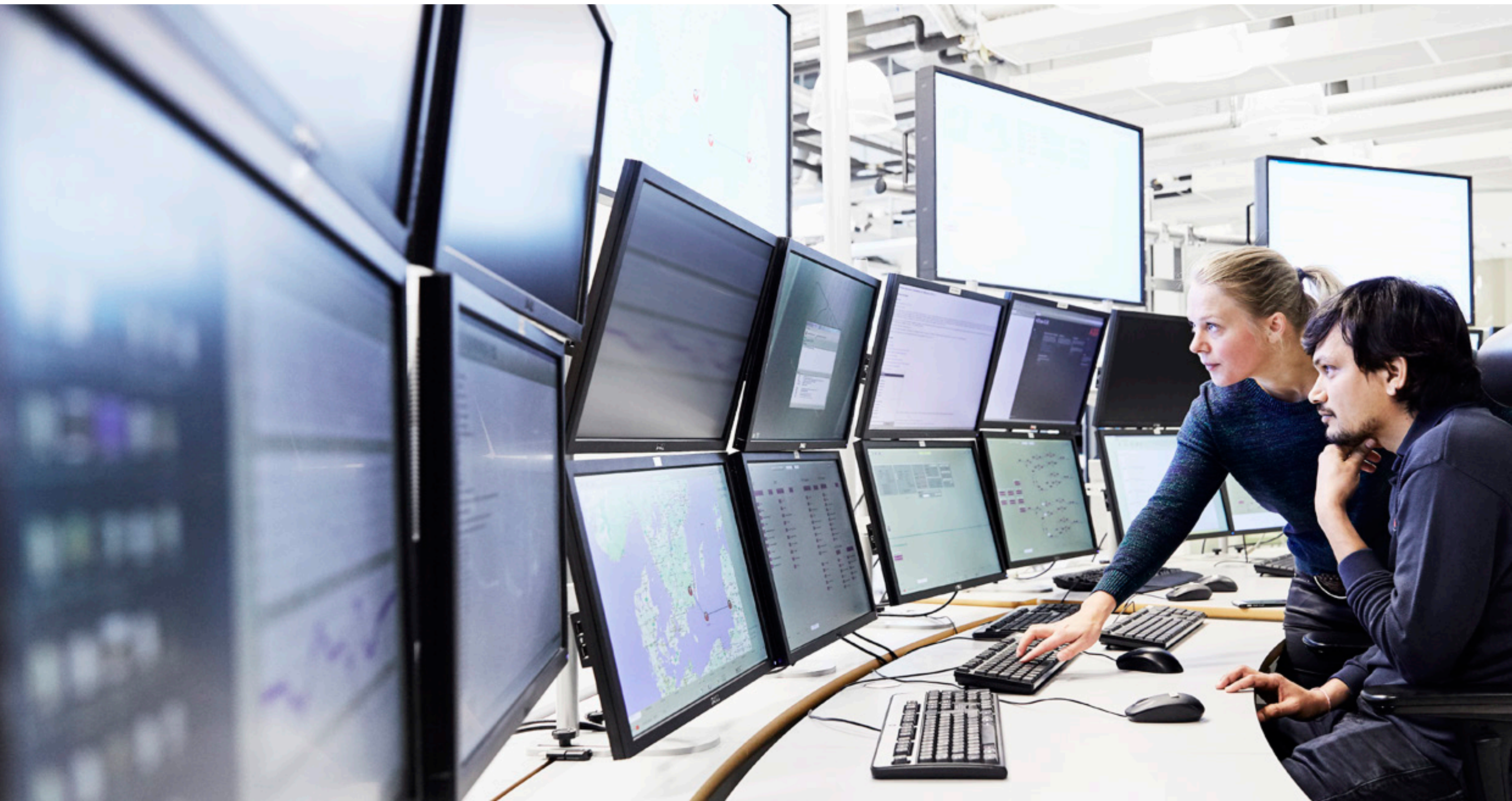
It is a requirement in both IEC 61508 and IEC 61511 that for a specified safety instrumented function, being carried out by a SIS, the PFDavg of the dangerous random hardware failures be evaluated. It is possible to do this by estimating the PFDavg for each subsystem and then summating them to find the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

An important parameter when undertaking such an evaluation is the proof-test interval. IEC 61511-1 (clause 10.3.2) requires a specification of the: 'requirement for proof-test intervals'
The calculated PFDavg for a subsystem is based on the following calculation (Note that this is a very simplistic calculation; refer to IEC 61508-6 (Annex B) for a fuller account of this issue): For a 1oo1 architecture, PFD = λ_{DU}X T/2

Where:
PFDavg = 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 PFDavg cannot be determined. An example of how the change of the proof test interval can affect the PFDavg is as follows:

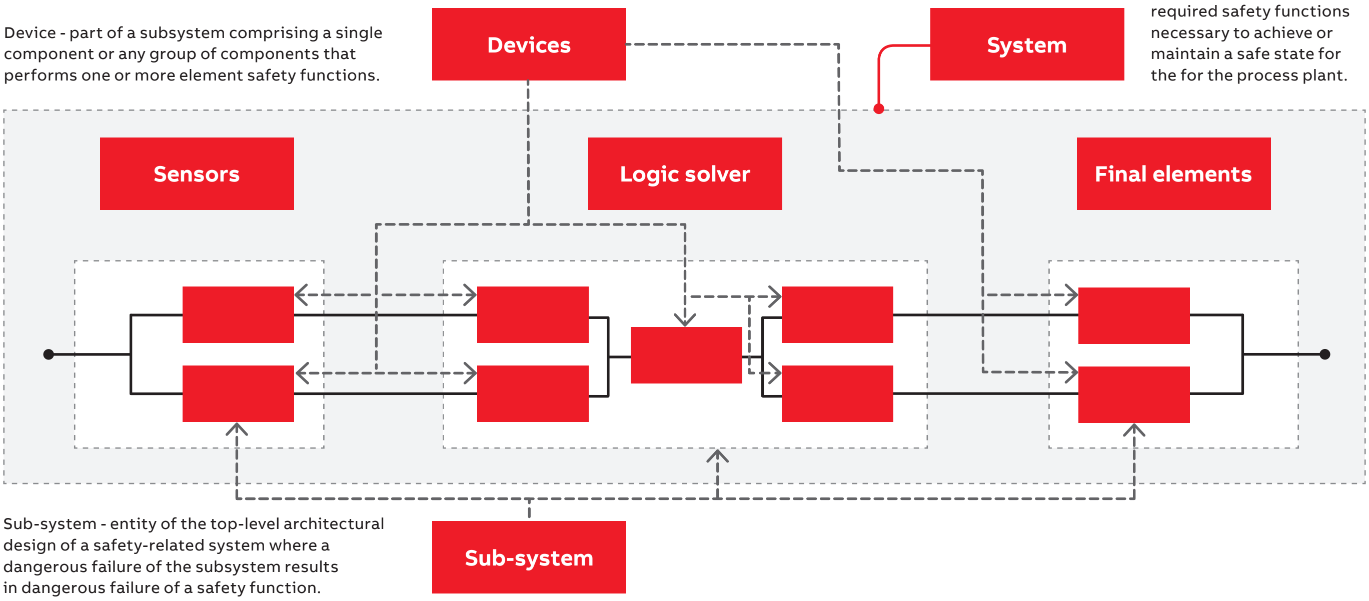
A safety controller is selected by the engineering / equipment supplier. The safety controller has been certified by a third party, and the supporting certification documentation states that a PFD of 2.25 x 10^{-5} has been achieved based on a proof test interval of 8 years. It can be seen that if the proof test interval was to be changed to, say 6 months, then assuming all the other reliability parameters were to remain the same then the PFDavg 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. 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.



Device - part of a subsystem comprising a single component or any group of components that performs one or more element safety functions.

System - implements the required safety functions necessary to achieve or maintain a safe state for the for the process plant.

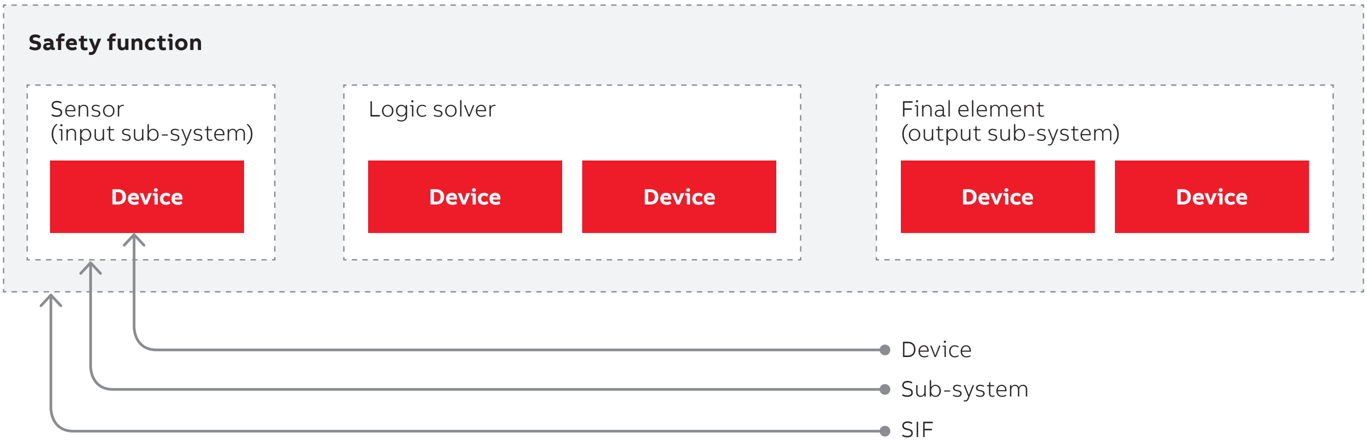
Sub-system - entity of the top-level architectural design of a safety-related system where a dangerous failure of the subsystem results in dangerous failure of a safety function.

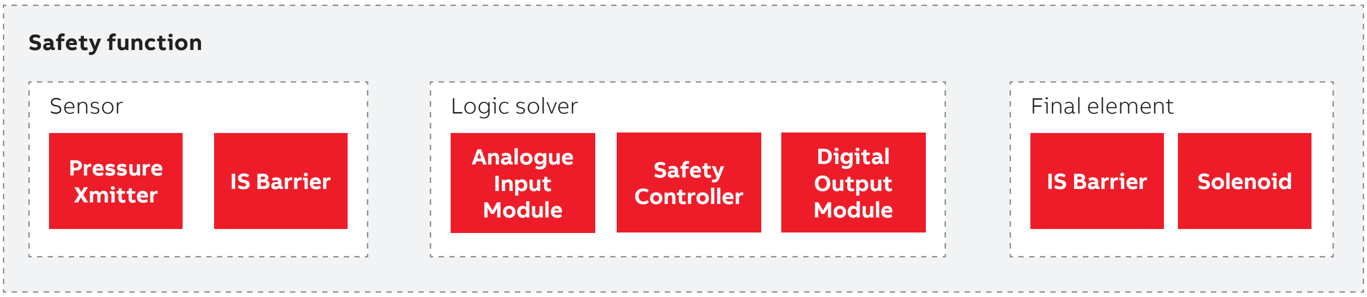
With reference to the simple example above, it is important to stress that the designer needs to define the architecture, devices, subsystems, and overall system and fully understand how failures will impact on the ability of the individual SIF's to perform on demand. These requirements should be undertaken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

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 SIS, 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
- Devices are identifiable pieces of equipment, consisting of individual components, for example a pressure transmitter, safety controller, etc.

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 SIS comprises of three subsystems and seven devices:

- Sensor sub-system
  - Pressure transmitter devices
  - IS barrier devices
- Logic solver sub-system
  - Analogue input module devices
  - Safety controller devices
  - Digital output module devices
- Output sub-system
  - IS barrier devices
  - Solenoid devices

In addition to the above sub-systems, the SIS 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 SIS, the engineering / equipment supplier must consider the following:

- The technical suitability of the device [does the device provide the technical functionality required for the loop]
- The safety suitability of the device [is the device 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 devices 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 SIS, 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 SIF, the more rigorous must be the measures to protect against systematic failures).

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 calculation. Whether a device of a SIF is considered during SIL calculation or not is, of course, dependant upon the SIF itself and each must be assessed individually. Wherever a device is excluded from SIL calculation, the rationale for this exclusion must be clearly stated.

1.5.3 Suitability of safety devices

Before selecting devices 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:
  - PFDavg, or
  - Dangerous failure rate [hour-]
- Systematic Capability (SC)
- Proof test interval

The objective of gathering the data above for each device of the SIS is to enable SIL calculation 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 devices being supplied from a third party, a validated claim that the devices supplied have the claimed parameter must be available. Validation must be by either an accredited certification body, or independent assessor. If a validated claim is absent, this should be declared as 'not available' in the SIL calculation report and a further substantiation identified for its continued use within the safety function.

Sound judgment should be used in the selection of equipment without substantiated data - demonstration of SIL calculation 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 devices as to their 'type' classification. See IEC 61508-2 clauses 7.4.4.1.2 and 7.4.4.1.3.

Type A

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

An element's compliance to IEC 61508 and certification or assessment against this standard should have clearly identified the type classification.

1.5.4 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, 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 device 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 verification

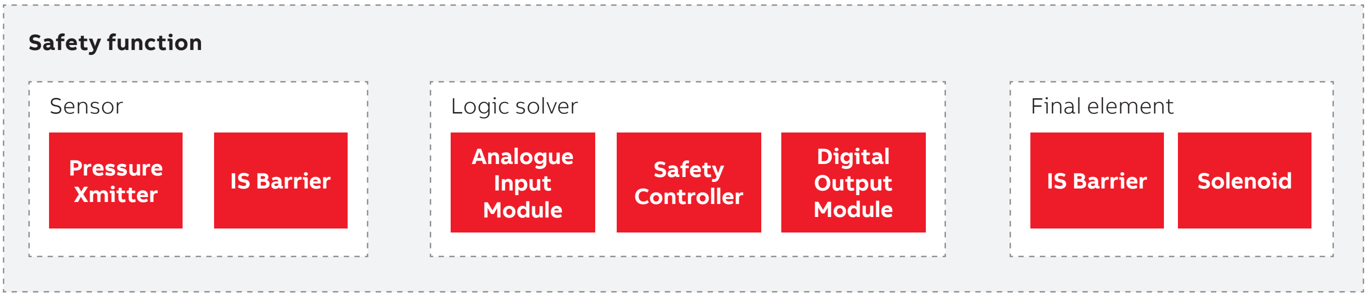
As part of the design process, the SIS has been deconstructed into sub-systems and devices. For each of those devices, parameters relating to their suitability in terms of functional safety have been collected.

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

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

1. The hardware safety integrity for the safety function achieved (in the form of the PFDavg or dangerous failure rate (hour) and HFT (for the specified SFF))
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 SRS, have been met or if the targets have not been met, the reasons
4. The design has considered the impact of any potential common cause, common mode and systematic failures, inclusive of any SIS diagnostics and spurious trip rate
5. The design has considered the requirements for an appropriate management system to be established for the SIS in assuring equipment will be inspected, maintained, tested and operated in a safe manner consistent with its risk reduction allocation

Note: In respect of systematic safety integrity, (2 above), the systematic capability may be claimed using evidence of prior use.



However, 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 within which the equipment was used because a prior use claim can only be made for devices used in the same way, for example, within the same process environment
- Evidence will be required to substantiate the sample size. How many samples are needed before a prior 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. The manufacturer of the device can appoint certified repairers

Note that the concept of prior 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 above.

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 calculation 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 calculation 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 calculation, 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 PFDavg or dangerous failure rate relating to dangerous random hardware failures

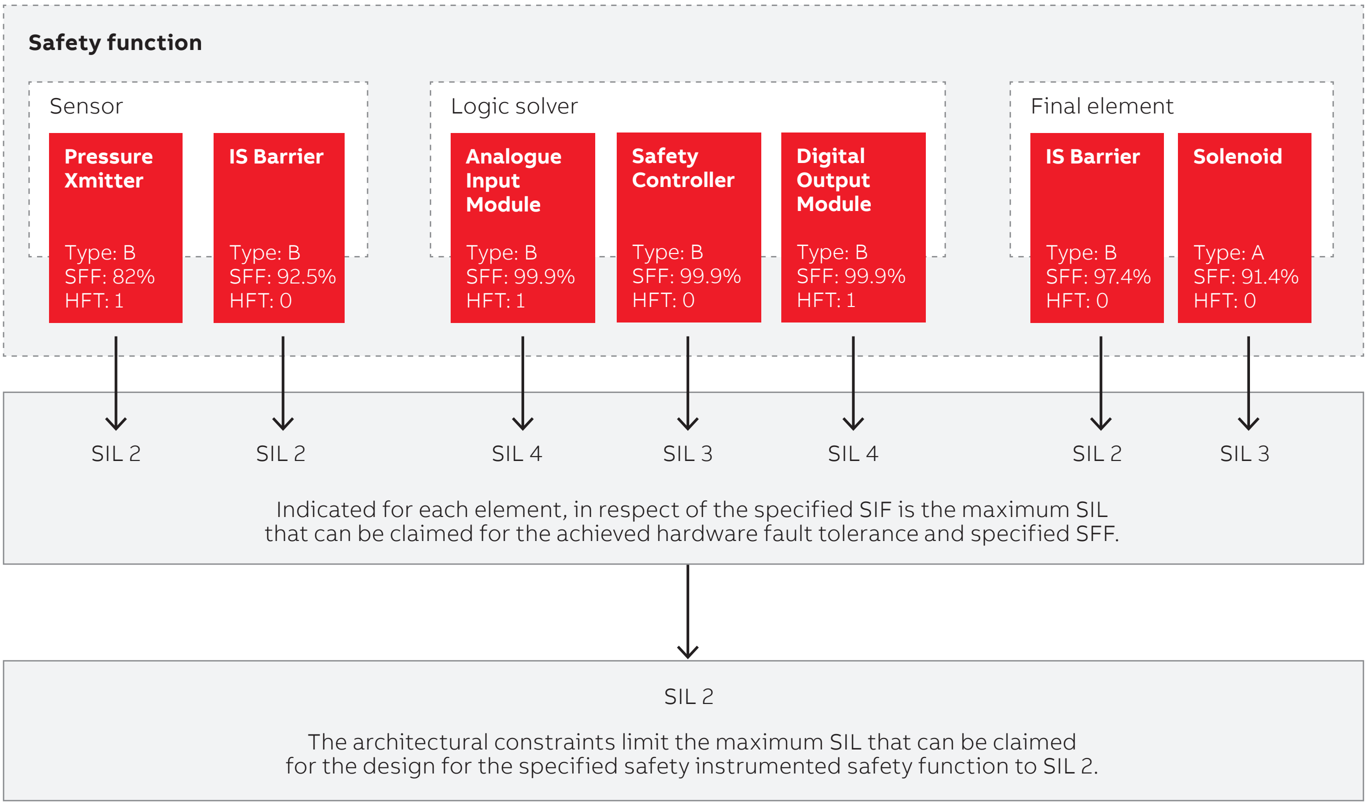
1.6.2.1 Architectural constraints

Tables 1 and 2 in section 1.4.2 provide the SIL. Reference should be made to IEC 61508-2 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 device 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 19, the architectural constraint has been calculated for each device 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.

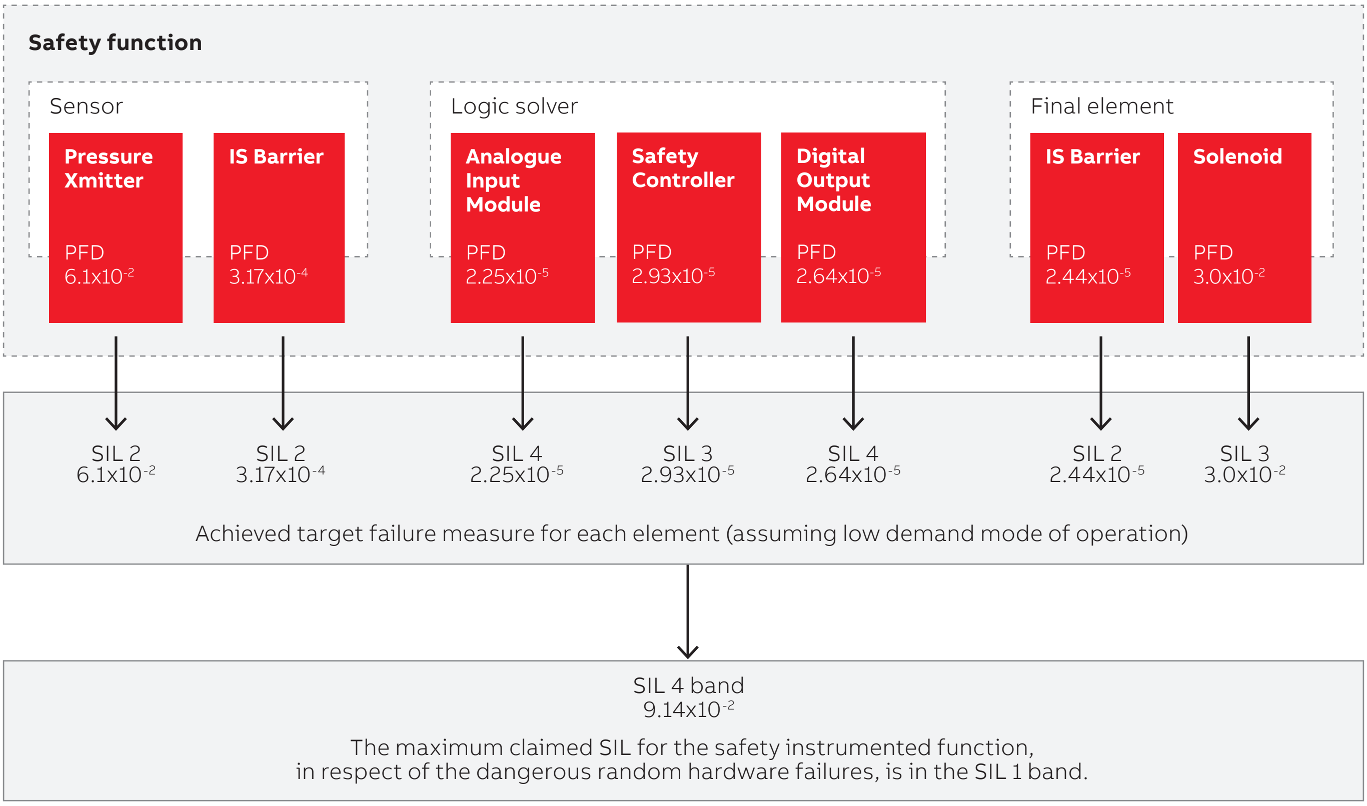
The maximum claimed SIL, in terms of architectural constraint, for the function is SIL 2.

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 SIF 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 device, 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.



As can be seen from the example on page 19, the target failure measure has been calculated for each device 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 device 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 PFDavg 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 SIS, to take into account common cause failures.

For further information, and examples of more complex target failure measure calculations, refer to IEC 61508-6 (Annex B). The maximum claimed SIL, in terms of target failure measure, for the SIF is in the SIL 1 band.

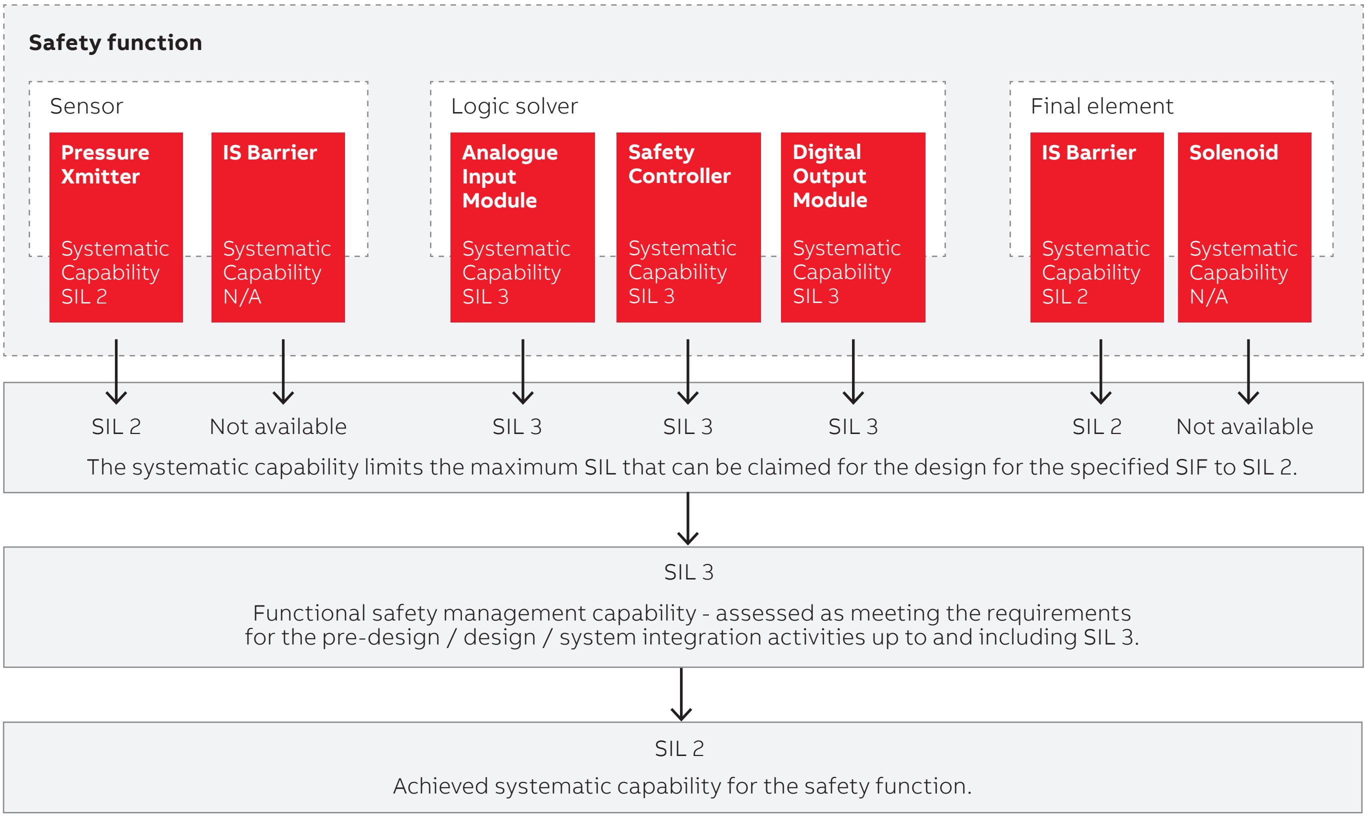
1.6.3 Demonstration of achieved systematic safety integrity

Systematic safety integrity cannot, in general, be quantified and is based on qualitative requirements and tables of specified techniques and measures in IEC 61508.

Assessment of systematic safety integrity utilises IEC 61508, Part 7 overview of techniques and measures: Annex B and Annex C.
It is necessary for each device 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 devices 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 IEC 61508’ of this document.

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



The systematic capability limits the maximum SIL that can be claimed for the design for the specified SIF to SIL 2.

SIL 3

Functional safety management capability - assessed as meeting the requirements for the pre-design / design / system integration activities up to and including SIL 3.

SIL 2

Achieved systematic capability for the safety function.

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 verification summary

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

Safety Instrumented Function (SIF)

'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 verification

- In terms of architectural constraint, SIL 2 is achieved
- In terms of the dangerous random hardware failures, the PFDavg 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
- In terms of meeting the safety function requirements, the SIF has been verified as been compliant to meet the requirements of the SRS

On this basis, the verified 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 verification relates to the ability of the designed SIS to carry out the specified SIF to the required SIL.

Calculation of a target SIL is based on individual SIFs (or generic SIFs). This is an important concept, as without having a clear definition of each SIF, and a target SIL for each of those SIFs, SIL verification becomes an impossible task.

It is also important to understand that the concept of a 'SIL x SIS' is not correct, as SIL applies to SIFs that are part of a SIS. Devices of that SIS are required to be suitable for use in carrying out a SIL x safety function. Safety Safety Requirements Specification (SRS) need to avoid simply stating 'Supply a SIL x safety system'.

2. Demonstration of SIL calculation is not just about PFDavg. Producing a reliability and availability report for a SIS is not demonstrating that the target SIL has been met for each SIF. SIL calculation is a far more complex process, involving architectural constraint, and systematic capability, as well as the PFDavg. 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 devices used to carry out the SIF are certified for use, does not mean that when those devices are bought together and configured that the requirements of the SIF have been achieved in the design of the SIS. The configuration of the SIS will have an impact on the systematic capability achieved. The integration and configuration of the SIF should also follow recognised techniques and methods as described in IEC 61508 to ensure systematic capability is achieved.

3. The importance of a good SRS. Without a good SRS, the information necessary for the demonstration of SIL calculation may not be available. Apart from the obvious need to identify individual SIFs and their target SIL, identifying the mode of operation and proof test requirements are also necessary in order to demonstrate SIL calculation.

4. The importance of equipment selection. Once SIFs and their target SIL have been identified, it is critical that the correct devices are specified which will implement each SIF. Incorrect specification of these devices 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 SRS 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 - HFT, SFF, target failure measure, device type and systematic capability.

2. SIF design verification needs to consider both the safety function and safety integrity requirements. The SIS designer will be required to verify if the proposed SIF design meets all necessary requirements as specified in the SRS. SIL verification is an essential lifecycle phase activity to ensure the successful engineering and subsequent validation of the installed SIS.

3. 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 SIF, not the SIS, and the demonstration of SIL is not just about PFDavg!

—

ABB FSM Technical Authority
Howard Road
Eaton Socon
St Neots
Cambridgeshire
PE19 8EU
United Kingdom
Phone: +44 (0)1480 475321
E-Mail: oilandgas@gb.abb.com

abb.com/oilandgas

—

We reserve 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. We reserve all rights in this document and in the subject matter and illustrations contained therein. Any reproduction, disclosure to third parties or utilisation of its contents - in whole or in parts - is forbidden without prior written consent of ABB.