T6A031

"The Requirements of a Design File for a Safety Instrumented System (SIS) in accordance with IEC 61511"

1. Contents

2. Revision History

Version	Date	Author	Comments
0.1	06/11/19	ANWD	First draft for review by WG.
1.0	31/12/20	ANWD	First issue.
2.0	26/09/22	PB	New template and editorial changes.

3. Acronyms

SIL Safety Integrity Level
SIF Safety Instrumented Function
SRS Safety Requirement Specification

4. Introduction

The purpose of this paper is to provide informative guidance on the content and information expected within a design file for a Safety Instrumented System (SIS) designed in accordance with IEC 61511. The standard for functional safety in the process industry, IEC 61511, does not make reference to a design file by name however the term *design file* is often used to refer to the information that is provided to the operator upon completion of a project.

The design file can take many forms and there is no clear single size fits all type of design file and can be provided by EPC, contractor or internal project team.

All of the information within the design file forms a significant part of what is required for the safety manual for an SIS, the design file contains information relevant to lifecycle phases 1 – 4 however the safety manual, which should be provided with each device forming part of an SIS, also captures the technical requirements for the operation and maintenance of the particular device.

These guidelines have been produced by *The 61508 Association* to assist its members and others to consider how to deal with the design file. The Association would welcome any comments on this publication, feedback via to www.61508.org/contact/index.php. Whilst every effort has been made to ensure the accuracy of the information contained in this document, neither *The 61508 Association* nor any of its members will assume liability for any use made thereof.

5. Intended Audience

This document and its supporting presentation are intended for use by managers and technical staff with roles and responsibilities relating to safety instrumented systems. The guidance is free to download from *The 61508 Association* website and it is intended to offer a consistent and systematic approach to the implementation of a design file.

The use of this guidance is without restriction and considered relevant to the following:

- Owners
- Company, site and operating unit managers
- Suppliers of systems, sub-systems and components
- Safety assessors
- Regulatory authorities
- Consulting engineers
- Organisations with contractual obligations.

6. Design File

Objective of the Design File

The objective of the design file is to collate all required technical information in order to reduce the likelihood of systematic errors during design and operations. It is not the intention of the design file to be a hard copy of all necessary information gathering dust on a shelf but rather a mapping of project deliverables against the requirements of the standard. The intention is for the design file to be used as either:

a. To enable the project team to demonstrate that their deliverables fulfil the requirements of the standard;
b. For the end user to verify that the project has provided the relevant documentation to fulfil the requirements of the standard

c. Provide external parties, such as the regulator, with a catalogue of reference documentation that supports a demonstration of compliance for a project.

Why is the design file important?

The functional safety lifecycle crosses several technical disciplines which produce deliverables that contribute to the overall compliance to functional safety. In order to ensure the final design meets the original intent it is important to ensure a line of sight is maintained across these deliverables. The design file provides an implementation structure to support this.

In addition, as per the second edition of IEC 61511 a safety manual is now a mandatory requirement (i.a.w. Clause 11.2.13), and therefore highlights the importance of the design file in fulfilling a significant part of this new requirement.

7. IEC 61511 Lifecycle and the Design File

IEC 61511, like all functional safety standards, follows a cradle to grave approach to a Safety Instrumented System (SIS), as shown in the IEC 61511 figure 2. The design is subsequently handed over to an operational facility for continuous management during its operational life and therefore the information provided to the operational team is pertinent to ensuring the safety system and its safety functions provide the adequate levels of required risk reduction against the unwanted hazardous scenarios for all of its operational life.

It is worth noting that the Safety Integrity Level (SIL) identified for a safety function is a definition of the required risk reduction for that individual Safety Instrumented Function (SIFs) which is identified against a defined hazardous scenario.

A Safety Instrumented System (SIS) is a collection of individual SIFs all performing a different function against a different potential hazard therefore the SIL rating is for the SIF and not the SIS as shown in Figure 1 opposite.

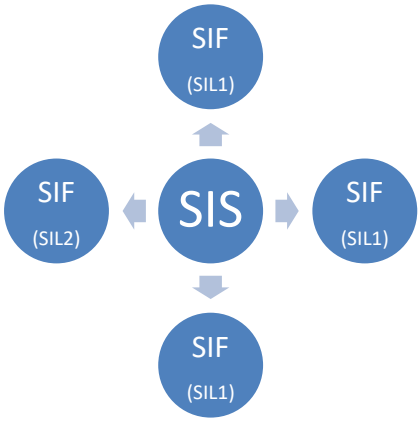


Figure 1 - Interaction between the SIS & SIFs

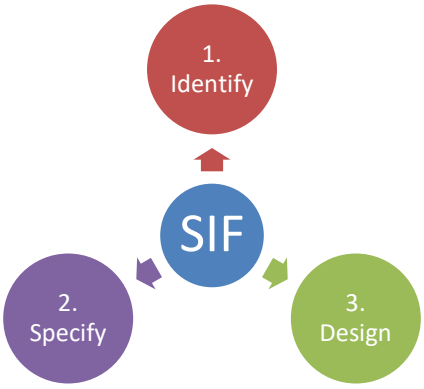


Figure 2 – Three Distinct phases

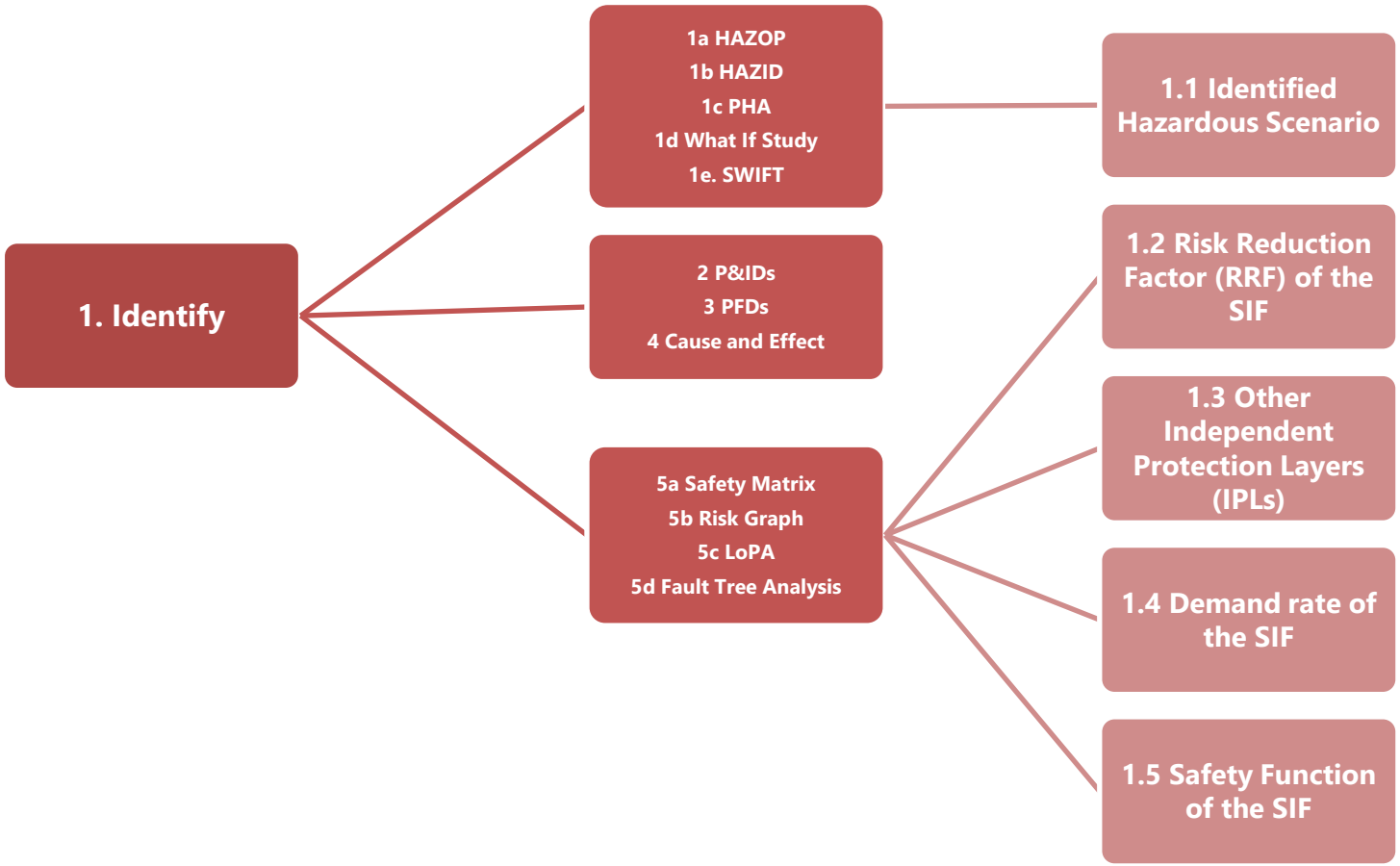
Therefore, since a SIS is a collection of SIL rated SIFs which can be identified, determined, and designed using various studies and techniques then it is considered appropriate to consider the requirements contained within the Design file to be for the individual SIFs. This is not to say a design file is required for each SIF but that the Design file should consider the requirements against each SIF and not the SIS.

The requirements of the Design File can be split into three distinct sections as shown in figure 2 opposite.

8. The Design File

Identify

Element		Documents in the Design File		Reasons for inclusion



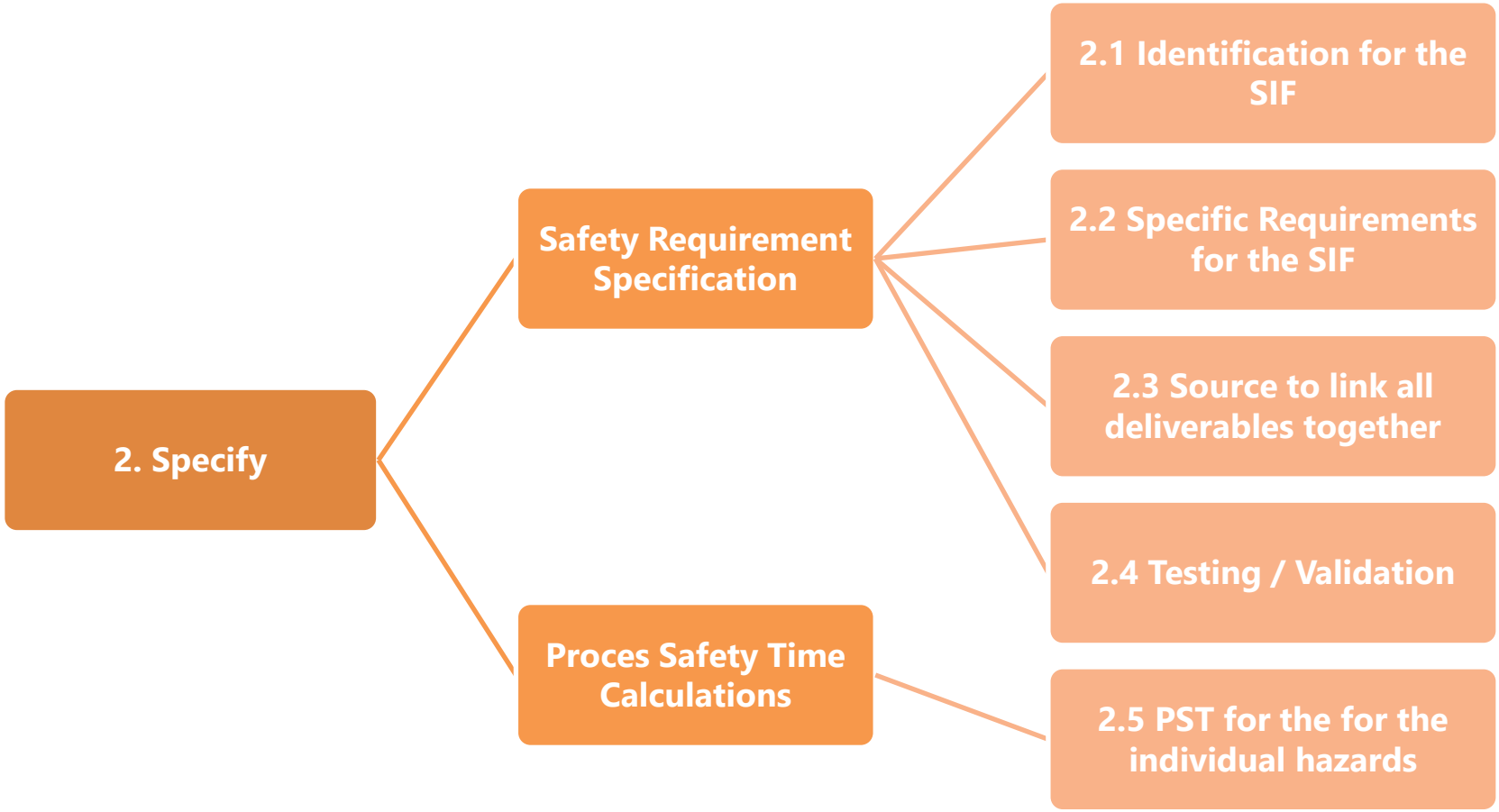
1. HRA Introduction:	This first element considers the identification and classification of an Instrumented Function (IF) which is usually achieved through hazard identification process and risk determination study where the function is identified as being a requirement to protect against an unwanted hazardous scenario and its integrity level defined (an Instrumented Function becomes a Safety Instrumented Function when a Safety Integrity Level is required). This first element also defines the required risk reduction of other means of risk reduction, such as passive and active protection layers. The information contained in this initial element will be found in earlier design related documentation however the importance of it being contained in the design file is to ensure there is a clear line of sight to the installed SIS so that during its operational life the systems owner understands the hazard that is being managed by the individual SIFs contained within the SIS. ***Note:*** *Whilst the H&R studies are usually performed in accordance with IEC 61511 for rotating equipment a vendor may have already performed such a study against the requirements of IEC 62061.*			
Sub-element	**Description**	**Where the Information can be found**	**Notes**	**Lessons Learnt**
1.1 Identified Hazardous Scenarios	The hazardous scenario that the SIF is protecting against.	HAZOP HAZID PHA What If Study SWIFT *As well as* SIF Register	A SIF is used to provide risk reduction against a defined hazardous scenario therefore it is critical for operations to understand the hazardous that are present for the individual SIFs. If no clear line of sight is maintained between the identified hazards and the implemented SIFs then managing hazards during the operational life of a system will prove challenging	*Operators unaware of the Dangers:* Experience has shown that an operator or maintenance team is not aware of the potential hazard that could be present as a result of a SIF not being available which could put lives in danger

Sub-element	Description	Where the Information can be found	Notes	Lessons Learnt
1.2 Risk Reduction Factor (RRF) of the SIF	The level of risk reduction required of the SIF against the unwanted hazardous scenario.	Safety Matrix Risk Graph LoPA FTA *As well as* SIF Register	Some techniques only yield a SIL band for the SIF whilst others provided a specific PFD so a specific PFD may not always be possible.	*Incomplete Risk Determination:* A clear link to the individual hazards in the risk study ensures complete coverage of all identified hazards in the earlier study. Experience has shown hazards which could be protected by a SIF have been omitted from the risk determination due to an inadequate line of sight.
1.3 Other Independent Protection Layers (IPLs)	Other means of risk reduction against the unwanted hazard scenarios.	Safety Matrix Risk Graph LoPA FTA *As well as* SIF Register	Some risk determination techniques don't fully quantify the other means of risk reduction such as risk Graph. The use of IPL has a direct impact on the SIL level required of the SIF and in a number of cases an Instrumented Function (IF) does not require a SIL level as a result of other means of risk reduction and therefore does not become a SIF.	*An IPL is as critical as the SIF:* If an IPL becomes unavailable or is decommissioned then this directly impacts the SIL level required of the SIF but without a clear line of sight between the IPLs and the SIF this can all too often get missed. Furthermore an IF may become a SIF if an IPL is proven to be less reliable or is no longer available so management of Non-SIF instrumentation is of equal importance.

Sub-element	Description	Where the Information can be found	Notes	Lessons Learnt
1.4 Demand Rate of the SIF	The demand required of the SIF	Safety Matrix Risk Graph LoPA FTA	A SIF that is protecting against several high frequency events may be classified as operating in a High demand mode of operation.	*Demand Rate based on hierarchy:* The demand rate on the SIF is very much dependant on whether its action is executed before or after other means of risk reduction, therefore it is critical to know the hierarchy of risk reduction
1.5 Safety Function of the SIF	The safety function required of the SIF	Safety Matrix Risk Graph LoPA FTA	The SIL Level of the SIF is associated with the Safety Function the SIF is to achieve	*Clearly Define the Safety Function:* The Safety Function is not always clearly defined and whilst in 99% of cases the function is obvious experience has shown it is not always the case.

Specify

Element		Documents in the Design File		Reasons for inclusion

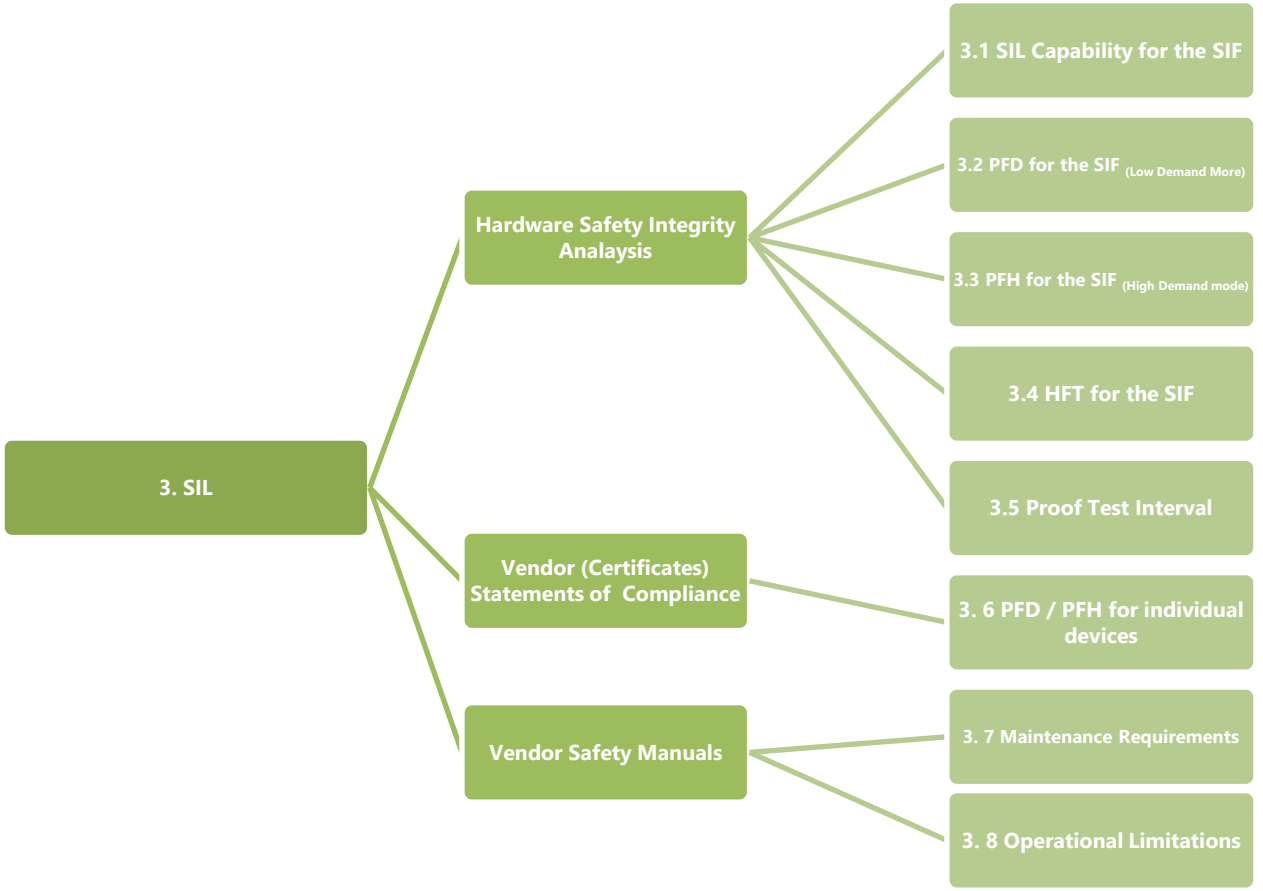


2. Safety Requirement Specification	This element considers the requirements of the Safety Instrumented Function and why these should be specified.			
Sub-element	**Description**	**Where the Information can be found**	**Notes**	**Lessons Learnt**
2.1 SIF Identification	Each SIF should have a unique Tag so that they can easily be distinguished	Safety Requirements Specification	For the Identification of a SIF it is common to use the Field Device as the SIF Tag however it is worth noting the SIF is not just the sensor and therefore having a different unique tag system can often provide a suitable divide between the field sensor and the complete SIF.	Risk Determination through SIF not Hazard: It is not uncommon to find the *'SIL Verification'* has been performed based on a standard 8760 hours (1 year) however it is likely, for low SIL rated SIFs that a less frequent proof test is possible. Furthermore, during operations, it is important to verify that the proof test frequency remains relevant based on operational experience.
2.2 Specific Requirements for the SIF	This is the Probability of Failure on Demand / Probability of Failure Per Hour required of the SIF when operating in Low demand mode of operation	Safety Requirements Specification	The SIL is defined through a Risk Determination study, see H&R element. The achieved (calculated) PFD for a SIF is defined in the Hardware Safety Integrity Analysis which is more often called 'SIL Verification', which is done in Detailed Design but the SRS needs to define what PFD is required of the SIF(s).	It is not uncommon to find the *'SIL Verification'* has been performed based on a standard 8760 hours (1 year) however it is likely, for low SIL rated SIFs that a less frequent proof test is possible. Furthermore, during operations, it is important to verify that the proof test frequency remains relevant based on operational experience.

Sub-element	Description	Where the Information can be found	Notes	Lessons Learnt
2.3 Source to link all deliverables	This is the evidence / reference documents where the source data has come from or where the requirements are defined in more detail. E.g. the LoPA / HAZOP should be clearly referenced in the SRS	Safety Requirements Specification	The SRS may be a single document or a signposting document to other documents where the information is defined that is required in the SRS.	Certain aspects of the SIF Requirements are never defined in the SRS e.g. Environmental / EMC requirements. Whilst this detail is not defined in the SRS they are usually defined in a Basis of Design document or similar and therefore these documents should be defined in the SRS for clear traceability. All associated documents should be included in the design file.
2.4 Testing / Validation	This is planning for Validation of the SIF against the SRS in the later commissioning phase.	Safety Requirements Specification	It can sometimes be found in the SRS however if the SRS was drafted early on in the design phase is not uncommon for validation plan to be drafted as a separate requirements as part of the commissioning phase.	The validation plan and records against the SRS should be included in the design file.
2.5 PST for the individual hazards	The Process Safety time is the time between the initiating event and the hazardous scenario occurring	Process Safety Time Calculations	The SIF has to respond within the PST	The PST calculations should be included in the Design File.

Safety Integrity Level

Element		Documents in the Design File		Reasons for inclusion



3. SIL Introduction:	This element considers the requirements set for the Safety Integrity Level assigned to a Safety Instrumented Function.			
Sub-element	**Description**	**Where the Information can be found**	**Notes**	**Lessons Learnt**
3.1 SIL Capability	This is the Probability of Failure on Demand / Per hour that has been achieved of the SIF	Hardware Safety Integrity Analysis Report, see notes.	The SIL is defined through a Risk Determination study, see H&R element. The calculated PFD for a SIF is defined in the Hardware Safety Integrity Analysis which is more often called 'SIL Verification'	It is not uncommon to find the *'SIL Verification'* has been performed based on a standard 8760 hours (1 year) however it is likely, for low SIL rated SIFs that a less frequent proof test is possible. Furthermore, during operations, it is important to verify that the achieved PFD remains relevant based on operational experience.
3.2 Probability of Failure on Demand	This is the Demand rate defied of the SIF which demonstrates if it is a Low / Continuous demand mode of operation	Hardware Safety Integrity Analysis Report, see notes.	The SIL is defined through a Risk Determination study, see H&R element. The demand rate for the SIF is usually defined in the SRS.	It is not uncommon to find the *'SIL Verification'* has been performed based on a standard 8760 hours (1 year) however it is likely, for low SIL rated SIFs that a less frequent proof test is possible. Furthermore, during operations, it is important to verify that the Demand rate remains relevant based on operational experience.
3.3 Probability of Failure Per Hour	This is the Probability of Failure per hour required of the SIF when operating in	Hardware Safety Integrity Analysis Report, see notes.	The SIL is defined through a Risk Determination study, see H&R element. The calculated PFH for a SIF is defined in the Hardware Safety Integrity	

	High / Continuous mode of operation		Analysis which is more often called 'SIL Verification'.	
Sub-element	**Description**	**Where the Information can be found**	**Notes**	**Lessons Learnt**
3.4 Hardware Fault Tolerance	This is of level of redundancy the SIF has	Hardware Safety Integrity Analysis Report / Safety Requirement specification, see notes.	It can sometimes be found in the SRS however if the SRS was drafted early on in the design phase it is not uncommon for the HFT of individual elements to be omitted from the SRS	
3.5 Proof Test Interval	This is the frequency of testing required for the SIF in order to meet the PFD for functions operating in a Low demand mode of operation	Hardware Safety Integrity Analysis Report / Safety Requirement specification, see notes.	It can sometimes be found in the SRS as the aspirational test frequency however the Hardware Safety Integrity Analysis Report shall define the achieved test frequency.	The SRS often defines a yearly test frequency as an aspiration and the PFD is calculated based on a 1 year test however the architecture may achieved a less onerous test frequency but is never determined which can inflate maintenance costs.
3.6 Vendor SIL Compliance Statements	The PFD / PFH achievable for the individual devices which form part of the SIF	Vendor Certificate or statement of conformity	The data contained within the vendor statement of conformity should be scrutinised to ensure the data seems reasonable against typical industry data	Experience has shown the data is not always credible and therefore may be questioned for use in the calculation
3.7 Maintenance Requirements	Maintenance required of the SIF during its operational life	Vendor Certificate or statement of conformity		
3.8 Operational Limitations	Limitation of use for the device	Vendor Safety Manual for the device		

9. SIF, Non-SIF & IPL Registers

One recommended practice, that is not defined in IEC 61511, that may have been adopt by the project at the end of the hazard and risk study(s) is to create a register of all SIFs, Non-SIFs & IPLs. As part of the risk determination and identification of safety function exercise a number of safeguards will have been identified. These can be in the form of:

Passive Protection
Active Protection
Mechanical Protection
Electrical Protection
Structural Protection

The registers are seen as a good way of managing all equipment types that form the necessary risk reduction measures for all hazardous deviations / events that may occur with the piece of equipment.

- SIF Register — All Instrumented Functions that have been assigned an Integrity Level (SIL 1 – 3) for the purposes of risk reduction.
- Non-SIF Register — All Instrumented Functions that do not require an integrity level for the purposes of risk reduction.
- IPL Register — All other equipment types such as passive protection, active protection, mechanical, electrical or structural protection for the purposes of risk reduction.

Example SIF Register is available on a separate Excel worksheet.

10. Existing and Emerging Standards

- IEC 61511:2017, *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements*.

11. 61508 Association Recommended Practices

This document sets out to describe current best practices in the application of a 'Design File' for Safety Instrumented Systems, in accordance with IEC 61511, but does not seek to prescribe specific measures, since these will depend on the application, and any existing constraints of the installation.

DISCLAIMER: Whilst every effort has been made to ensure the accuracy of the information contained in this document neither *The 61508 Association* nor its members will assume any liability for any use made thereof.

*** END OF DOCUMENT ***