

Hardware safety integrity *Guideline*

Comments on this report are gratefully received by
Johan Hedberg
at SP Swedish National Testing and Research Institute
mailto:johan.hedberg@sp.se

Quoting of this report is allowed but please remember to state the
source!

Summary

This report is focusing on those parts of IEC 61511 that contain requirements on hardware safety integrity. Hardware safety integrity addresses the following two aspects:

- Requirements for hardware fault tolerance (architectural constraints)
- SIF probability of failure

Both these aspects must be considered during the design of a *safety instrumented function* (SIF) in order to fulfil the hardware safety requirements for a certain *safety integrity level* (SIL).

Prior to describing in detail how to handle hardware safety integrity, the report presents shortly a method to break up the identified SIFs into function blocks/function block elements. The decomposition of these function blocks/function block elements into underlying subsystems/subsystem elements is also treated.

The parts concerning architectural constraints explain the term *safe failure fraction* (SFF) and describe the connection between reached SFF and the degree of redundancy required for the current subsystem/subsystem element. The report also describes how to calculate SFF by using *Failure Mode Effects and Diagnostic Analysis* (FMEDA).

The parts concerning probability of failure on demand (PFD) explains this term and how to calculate this value for different system configurations based on the results from the FMEDA.

The aim of this report is that the information in it shall be useful for both companies that handles individual subsystems/subsystem elements and companies that handles complete SIFs. Based on this the description of hardware safety integrity requirements are divided into the following categories:

- Requirements on hardware safety integrity for subsystems/subsystem elements
 - Subsystems/subsystem elements that already fulfils hardware safety integrity requirements up to a certain level are combined together
 - No information is available about which hardware safety integrity requirements that are fulfilled for a certain subsystem/subsystem element
- Hardware safety integrity requirements for the complete SIF

This report is one of the results of the research project SafeProd supported by VINNOVA (Swedish Agency for Innovation Systems). More information about the project could be found at www.sp.se/safeprod.

TABLE OF CONTENTS

1	Introduction	4
1.1	Purpose	4
1.2	References	4
1.3	Scope	4
1.4	Audience.....	5
2	Definitions and abbreviations.....	6
3	Breakdown of the safety instrumented function (SIF) into function blocks/subsystems. 10	
3.1	Identification of the function blocks/function block elements forming the SIF	11
3.2	Mapping of function blocks/function block elements to a subsystem/subsystem element	12
4	Hardware safety integrity requirements	13
4.1	Requirements on hardware safety integrity for subsystems/subsystem elements....	14
4.1.1	Use of a single subsystem or a combination of subsystem elements that already fulfils hardware safety integrity requirements up to a certain level.....	19
4.1.2	No information is available about which hardware safety integrity requirements that are fulfilled for a certain subsystem/subsystem element.....	31
4.2	Hardware safety integrity requirements for the complete safety instrumented function (SIF)	46
4.2.1	Architectural constraints on hardware safety integrity for the complete safety instrumented function (SIF)	47
4.2.2	Requirements for the probability of failure on demand for the complete safety instrumented function (SIF)	48

1 Introduction

1.1 Purpose

This aim of this report is to be a support during the hardware design and give guidelines on hardware safety integrity aspects in IEC 61511.

This report is only a guideline. In order to fulfil the requirements related to hardware safety IEC 61511 must be used.

This report is one of the results of the research project SafeProd supported by VINNOVA (Swedish Agency for Innovation Systems). More information about the project could be found at www.sp.se/safeprod.

1.2 References

- [1] IEC 61511-1 Functional safety- Safety instrumented systems for the process industry sector, Part 1: Framework, definitions, system, hardware and software requirements
- [2] IEC 61511-2 Functional safety- Safety instrumented systems for the process industry sector- Part 2: Guidelines for the application of IEC 61511-1
- [3] IEC 61511-3 Functional safety- Safety instrumented systems for the process industry sector- Part 3: Guidance for the determination of the required safety integrity level
- [4] IEC 62061 Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
- [5] IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems

1.3 Scope

This document gives guidelines on how to apply those parts in [1] that relates to hardware safety integrity.

Besides requirements concerning hardware safety integrity [1] also includes other requirements related to hardware.

The design and engineering of safety instrumented systems (4) is one of the most central parts of the safety life cycle according to [1]. See figure 1.

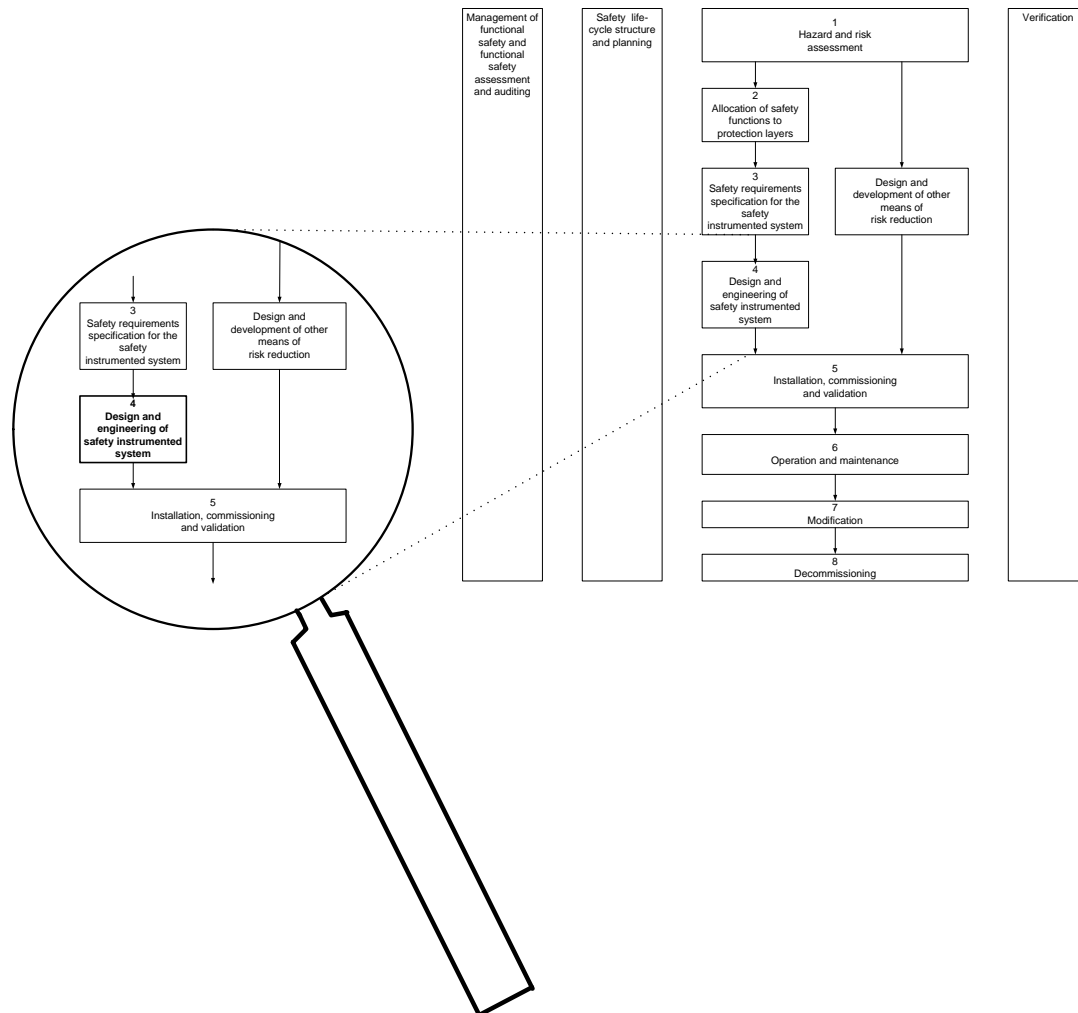


Figure 1. “Design and engineering of safety instrumented system” life-cycle phase in [1]

1.4 Audience

Persons involved in design and engineering of safety instrumented systems.

2 Definitions and abbreviations

basic process control system (BPCS)

system which responds to input signals from the process, its associated equipment, other programmable systems and/or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any safety instrumented functions with a claimed SIL ≥ 1 (3.2.3 in [1])

component

one of the parts of a system, subsystem, or device performing a specific function (3.2.7 in [1])

continuous mode safety instrumented function

where in the event of a dangerous failure of the safety instrumented function a potential hazard will occur without further failure unless action is taken to prevent it (3.2.43.2 in [1])

demand mode safety instrumented function

where a specified action (for example, closing of a valve) is taken in response to process conditions or other demands. In the event of a dangerous failure of the safety instrumented function a potential hazard only occurs in the event of a failure in the process or the BPCS. (3.2.43.1 in [1])

device

functional unit of hardware or software, or both, capable of accomplishing a specified purpose (for example, field devices; equipment connected to the field side of the SIS I/O terminals; such equipment includes field wiring, sensors, final elements, logic solvers, and those operator interface devices hard-wired to SIS I/O terminals) (3.2.14 in [1])

diagnostic coverage (DC)

ratio of the detected failure rate to the total failure rate of the component or subsystem as detected by diagnostic tests. Diagnostic coverage does not include any faults detected by proof tests. (3.2.15 in [1])

final element

part of a safety instrumented system which implements the physical action necessary to achieve a safe state (3.2.24 in [1])

hardware safety integrity

part of the safety integrity of the safety instrumented function relating to random hardware failures in a dangerous mode of failure (3.2.29 in [1])

instrument

apparatus used in performing an action (typically found in instrumented systems) (3.2.38 in [1]) (3.2.72 in [1]).

logic solver

that portion of either a BPCS or SIS that performs one or more logic function(s) (3.2.40 in [1])

mode of operation

way in which a safety instrumented function operates (3.2.43 in [1])

module

self-contained assembly of hardware components that performs a specific hardware function (i.e., digital input module, analogue output module), or reusable application program (can be portion of a computer program that carries out a specific function (3.2.44 in [1])

non-programmable system

system based on non-computer technologies (i.e., a system not based on programmable electronics [PE] or software) (3.2.47 in [1])

programmable electronics

electronic component or device forming part of a PES and based on computer technology. The term encompasses both hardware and software and input and output units (3.2.55 in [1])

proof test

test performed to reveal undetected faults in a safety instrumented system so that, if necessary, the system can be restored to its designed functionality (3.2.58 in [1])

proven-in-use

when a documented assessment has shown that there is appropriate evidence, based on the previous use of the component, that the component is suitable for use in a safety instrumented system (3.2.60 in [1])

random hardware failure

failure, occurring at a random time, which results from a variety of degradation mechanisms in the hardware (3.2.62 in [1])

redundancy

use of multiple elements or systems to perform the same function; redundancy can be implemented by identical elements (identical redundancy) or by diverse elements (diverse redundancy) (3.2.63 in [1])

safe failure fraction

fraction of the overall random hardware failure rate of a device that results in either a safe failure or a detected dangerous failure (3.2.65.1 in [1])

safety configured logic solver

general purpose industrial grade PE logic solver which is specifically configured for use in safety applications in accordance with chapter 11.5 in [1] (3.2.40.1 in [1])

safety instrumented function (SIF)

safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function (3.2.71 in [1])

safety instrumented system (SIS)

instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor (s), logic solver (s), and final element (s) (3.2.72 in [1])

safety integrity level

discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest (3.2.74 in [1])

sensor

device or combination of devices, which measure the process condition (for example, transmitters, transducers, process switches, position switches) (3.2.80 in [1])

system

set of elements, which interact according to a design; an element of a system can be another system, called a subsystem, which may be a controlling system or a controlled system and may include hardware, software and human interaction (3.2.84 in [1])

target failure measure

intended probability of dangerous mode failures to be achieved in respect of the safety integrity requirements, specified in terms of either the average probability of failure to perform the design function on demand (for a demand mode of operation) or the frequency of a dangerous failure to perform the SIF per hour (for a continuous mode of operation) (3.2.87 in [1])

undetected/unrevealed/covert

in relation to hardware and software faults not found by the diagnostic tests or during normal operation (3.2.90 in [1])

Abbreviations:

CCF	Common Cause Failure
FMEDA	Failure Mode Effects and Diagnostic Analysis
PFD	Probability of Failure on Demand
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
SIF	Safety Instrumented Function
SIS	Safety Instrumented System

3 Breakdown of the safety instrumented function (SIF) into function blocks/subsystems

Before going into the detailed description of hardware safety integrity requirements the following steps must be performed:

- Identification of the function blocks forming the SIF
- Mapping of function blocks/function block elements to subsystems/subsystem elements

It is important to point out that [1] covers both SIFs working in *demand mode of operation* and *continuous mode of operation*. Most of the SIFs in the process industry are typically of type *demand mode of operation*. The definition from [1] of a SIF working in *demand mode of operation* is:

“where a specified action (for example, closing of a valve) is taken in response to process conditions or other demands. In the event of a dangerous failure of the safety instrumented function a potential hazard only occurs in the event of a failure in the process or the BPCS”

This report will only focusing on SIFs working in demand mode of operation where the probability of dangerous random hardware failures are called PFD (Probability of Failure on Demand)

The result from the hazard and risk assessment is a number of SIFs with corresponding SILCL which are described more in detail in the safety requirements specification. For further work with hardware safety integrity:

Set hardware safety integrity = SIL derived from hazard and risk assessment

To simplify the understanding a practical example will be used in the rest of this report. In this example the hazard and risk assessment have identified the following SIF:

“Close an inlet valve when the liquid level inside a vessel increases a certain level (overflow protection). The SIL claim of this SIF is SIL 2”

3.1 Identification of the function blocks/function block elements forming the SIF

The definition of function block in [4] interpreted for the process sector could be:

“the smallest element of a SIF whose failure can result in a failure of the safety instrumented function”

A function block could be built up by a number of function block elements. A function block element is defined in the following way in [4]:

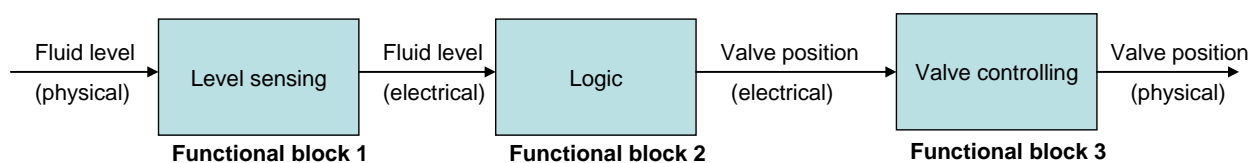
“part of a function block”

The reason to divide a function block into function block elements could for instance be:

- A SIF that shall be realised by a certain function block is most efficient built up by a number of individual function block elements
- A function block shall realise a number of different SIFs (some of the function block elements could be used by more than one SIF and some of the function block elements are specific for a certain SIF)

Functional breakdown of the SIF into function blocks/function block elements then allows for allocation of function blocks to subsystems/subsystem elements.

In our example it is quite obvious that the risk of failing to *close an inlet valve when the liquid level inside a vessel increases a certain level (overflow protection)* could depend on either a failure in the level sensing, logic or valve controlling and because of this all these parts must be visible in the function block description below:



Outgoing from the definition of function block above each function block must fulfil the SIL claim of the complete SIF. The SIL claim for the SIF described in our example is SIL 2 and that gives the following situation:

Part:	Function block:	SIL:
Level sensing	FB1	2
Logic	FB2	2
Valve controlling	FB3	2

3.2 Mapping of function blocks/function block elements to a subsystem/subsystem element

Before it is possible to decide the hardware safety integrity requirements it is necessary to decide which subsystem/subsystem element that should realise each function block/function block element in the SIF.

Each function block shall be mapped to a subsystem. Based on the definition of function block in [4] the following text describes what a subsystem is:

“entity of the top-level architectural design of the SIS where a failure of any subsystem will result in a failure of a SIF”

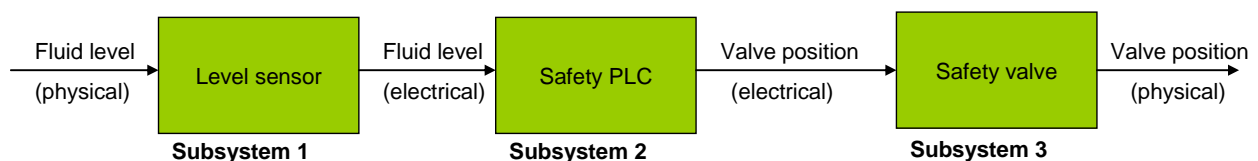
A subsystem could be built up by a number of subsystem elements. A subsystem element is defined in the following way in [4]:

“part of a subsystem, comprising a single component or any group of components”

The reason to divide a subsystem into subsystem elements could for instance be:

- A SIF that shall be realised by a certain subsystem is most efficient built up by a number of individual subsystem elements
- A subsystem shall realise a number of different SIFs (some of the subsystem elements could be used by more than one SIF and some of the subsystem elements are specific for a certain SIF)

In our example it is quite obvious that the risk of failing to *close an inlet valve when the liquid level inside a vessel increases a certain level (overflow protection)* could depend on either a failure in the level sensor, safety PLC or safety valve and because of this all these parts must be visible in the subsystem description below:



Outgoing from the definition of a subsystem above each subsystem must fulfil the SIL claim of the complete SIF. The SIL claim for the SIF described in our example is SIL 2 and that gives the following situation:

<u>Function block:</u>	<u>Subsystem:</u>	<u>SIL:</u>
Level sensing	Level sensor	2
Logic	Safety PLC	2
Valve controlling	Safety valve	2

4 Hardware safety integrity requirements

The next step after the SIF has been divided into a number of subsystems/subsystem elements is to decide which hardware safety integrity requirements that must be fulfilled.

Requirements related to hardware safety integrity are important for both companies that handles individual subsystems/subsystem elements and companies that handles complete SIFs. Based on this the below description of hardware safety integrity requirements are divided into the following categories:

- Requirements on hardware safety integrity for subsystems/subsystem elements
- Use of a single subsystem or a combination of subsystem elements that already fulfils hardware safety integrity requirements up to a certain level
- No information is available about which hardware safety integrity requirements that are fulfilled for a certain subsystem/subsystem element
- Hardware safety integrity requirements for the complete SIF

For each of the above categories the following two types of requirements from [1] will be described:

- Architectural constraints
- Requirements for the probability of failure on demand

To fulfil the requirements concerning hardware safety integrity both of these above types of requirements must be fulfilled.

4.1 Requirements on hardware safety integrity for subsystems/subsystem elements

The hazard and risk assessment has identified a number of SIFs with corresponding SIL:s.

Architectural constraints on hardware safety integrity for subsystems/subsystem elements:

The SIF is divided into a number of subsystems. Each of these subsystems must fulfil the architectural SIL claim for the complete SIF.

The following information is found in chapter 11.4.1 in [1]:

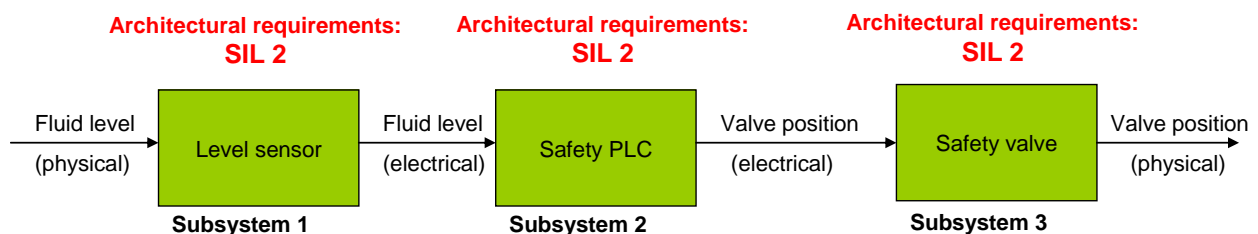
“For safety instrumented functions, the sensors, logic solvers and final elements shall have a minimum hardware fault tolerance”

“NOTE 1 Hardware fault tolerance is the ability of a component or subsystem to continue to be able to undertake the required safety instrumented function in the presence of one or more dangerous faults in hardware. A hardware fault tolerance of 1 means that there are, for example, two devices and the architecture is such that the dangerous failure of one of the two components or subsystems does not prevent the safety action from occurring.”

“NOTE 2 The minimum hardware fault tolerance has been defined to alleviate potential shortcomings in SIF design that may result due to the number of assumptions made in the design of the SIF, along with uncertainty in the failure rate of components or subsystems used in various process applications.”

“NOTE 3 It is important to note that the hardware fault tolerance requirements represent the minimum component or subsystem redundancy. Depending on the application, component failure rate and proof-testing interval, additional redundancy may be required to satisfy the SIL of the SIF according to 11.9.”

In our example this requirement brings about that each subsystem must fulfil SIL 2 architectural requirements:



The architectural SIL claim for a certain subsystem could be fulfilled by using a single subsystem or by combining subsystem elements.

Requirements for the probability of failure on demand for subsystems/subsystem elements:

As described earlier in this report [1] covers both SIFs working in *demand mode of operation* and *continuous mode of operation*.

Most of the SIFs in the process industry are typically of type *demand mode of operation*. The definition from [1] of a SIF working in *demand mode of operation* is:

“where a specified action (for example, closing of a valve) is taken in response to process conditions or other demands. In the event of a dangerous failure of the safety instrumented function a potential hazard only occurs in the event of a failure in the process or the BPCS”

This report will only focusing on SIFs working in demand mode of operation where the probability of dangerous random hardware failures are called PFD (Probability of Failure on Demand)

The overall PFD value of the complete SIF is built up by the individual PFD values of each subsystem:

$$PFD = PFD_1 + \dots + PFD_n + P_{TE}$$

PFD	Overall probability of failure on demand for the complete SIF
PFD ₁	Probability of failure on demand for subsystem 1
...	
PFD _n	Probability of failure on demand for subsystem n
P _{TE}	Probability of failure on demand for digital data communication processes

The overall PFD value of the complete SIF must be low enough to fulfil the requirements for a certain SIL. Following information could be found in chapter 11.9.1 in [1]:

“The probability of failure on demand of each safety instrumented function shall be equal to, or less than, the target failure measure as specified in the safety requirement specifications. This shall be verified by calculation.”

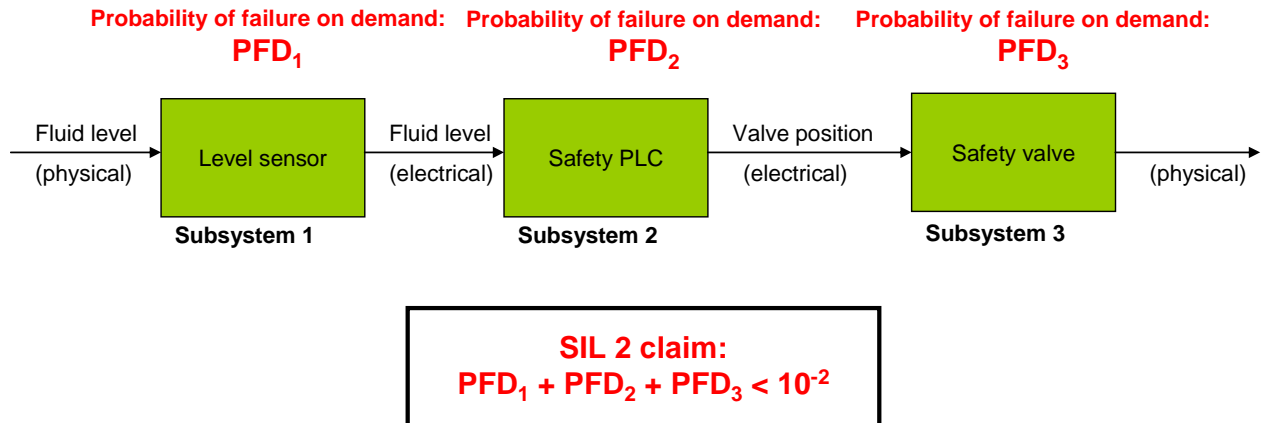
Below table shows the PFD value defined for the different SIL:s:

Probability of failure on demand
(PFD)

SIL	PFD	RRF
1	$<10^{-1}$ till $\geq 10^{-2}$	$10 \leq RRF \leq 100$
2	$<10^{-2}$ till $\geq 10^{-3}$	$100 \leq RRF \leq 1000$
3	$<10^{-3}$ till $\geq 10^{-4}$	$1000 \leq RRF \leq 10000$
4	$<10^{-4}$ till $\geq 10^{-5}$	$1000 \leq RRF \leq 10000$

The term *RRF* is an abbreviation of *Risk Reduction Factor* and the connection between PFD and RRF is as follows: $PFD=1/RRF$

In our example the hazard and risk assessment has identified that the probabilistic SIL claim for the complete SIF is SIL 2. SIL 2 requires that the overall probability of failure on demand for the complete SIF must be in the following interval, $10^{-2} \leq \text{PFD} < 10^{-3}$. Thus $\text{PFD}_1 + \text{PFD}_2 + \text{PFD}_3$ must be less than 10^{-2} :



Requirements on hardware safety integrity for subsystems/subsystem elements:

The following categories will be described:

- Use of a single subsystem or a combination of subsystem elements that already fulfils hardware safety integrity requirements up to a certain level
- No information is available about which hardware safety integrity requirements that are fulfilled for a certain subsystem/subsystem element

For each of the above categories the following two types of requirements from [1] will be described:

- Architectural constraints
- Requirements for the probability of failure on demand

To fulfil the requirements concerning hardware safety integrity both of these above types of requirements must be fulfilled.

4.1.1 Use of a single subsystem or a combination of subsystem elements that already fulfils hardware safety integrity requirements up to a certain level

The following situations will be described:

- PE logic solver subsystems/subsystem elements
- Sensors, final elements and non-PE logic solvers subsystems/subsystem elements

Before going into the detailed description of these situations it is important to point out the need of analysing the safety data received from the different manufacturers:

- If the calculation of the SFF and PFD value in a certain subsystem/subsystem element take credit for that internal faults in the subsystem/subsystem element shall be detected by another part of the system it is very important to detect and handle these faults otherwise the claimed SFF and PFD value will not be fulfilled.
- Another issue is that the calculated SFF and PFD value possibly could be based on the fact that the subsystem/subsystem elements shall be used in a certain way as a SIF. For example, if you have a valve as part of your SIF the value of SFF and PFD will differ if the safe state is “valve will not open” or “valve will not close” and thus it will be very important to choose the correct SFF and PFD value.

4.1.1.1 PE logic solver subsystems/subsystem elements

The following subsystem/subsystem element is an example of a PE logic solver subsystem/subsystem element:

- Safety PLC

The following information could be found in chapter 11.5.2.1 and 11.5.2.2 in [1]:

“Components and subsystems selected for use as part of a safety instrumented system for SIL 1 to SIL 3 applications shall either be in accordance with IEC 61508-2 and IEC 61508-3, as appropriate, or else they shall be in accordance with 11.4 and 11.5.3 to 11.5.6, as appropriate”

“Components and subsystems selected for use as part of a safety instrumented system for SIL 4 applications shall be in accordance with IEC 61508-2 and IEC 61508-3, as appropriate”

These requirements must be fulfilled for a PE logic solver. The following definition of *programmable electronics (PE)* is found in [1]:

“Electronic component or device forming part of a PES and based on computer technology. The term encompasses both hardware and software and input and output units”

Chapter 11.5.3 to 11.5.5 in [1] describes which requirements that must be fulfilled for a PE logic solver subsystem/subsystem element to be regarded as “based on prior use”. If these requirements are fulfilled it may be possible to use a PE logic solver that is not developed according to the requirements in [5] as part of a SIF. When this is allowed or not will not be further described in this report.

If a PE logic solver does not fulfil the requirements concerning “based on prior use” in [1] the manufacturer of the PE logic solver subsystem/subsystem element shall guarantee that they conform to the relevant requirements of IEC 61508-2 and IEC 61508-3.

It is the responsibility of the manufacturer of the SIL categorized PE logic solver subsystem/subsystem elements to give the following information:

- Reached architectural SIL level (including *Hardware Fault Tolerance* and *Safe Failure Fraction*) according to the requirements in:
 - Table 5 in [1] or
 - Table 3 in [5], if the requirements in chapter 11.4.5 in [1] are fulfilled
- Failure rate (λ_{du} , λ_{dd} , λ_s)
- Probability of failure on demand (PFD) versus Proof test interval for a single channel configuration
- Diagnostic test interval

The description of PE logic solver subsystems/subsystem elements is divided into the following two types of requirements from [1]:

- Architectural constraints
- Requirements for the probability of failure on demand

To fulfil the requirements concerning hardware safety integrity both of these above types of requirements must be fulfilled.

4.1.1.1.1 Architectural constraints on hardware safety integrity for PE logic solver subsystems/subsystem elements

In the situation that the design is based on bought PE logic solver subsystems/subsystem elements that already fulfil hardware safety integrity requirements up to a certain level, Table 5 in [1] or Table 3 in [5] could be interpreted as describing the internal architectural requirements of a certain subsystem/subsystem element.

SIL	Minimum hardware fault tolerance		
	SFF < 60 %	SFF 60 % to 90 %	SFF > 90 %
1	1	0	0
2	2	1	0
3	3	2	1
4	Special requirements apply (see IEC 61508)		

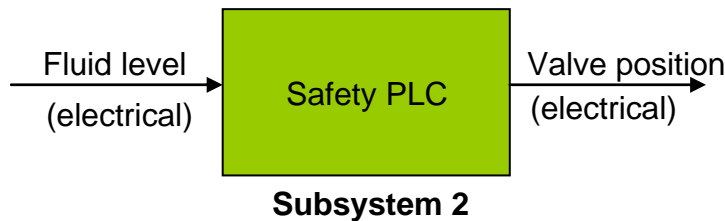
Safe Failure Fraction	Hardware fault tolerance		
	0	1	2
< 60%	Not allowed	SIL1	SIL2
60% - <90%	SIL1	SIL2	SIL3
90% - <99%	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4

In [1] *hardware fault tolerance* is defined in the following way:

“Hardware fault tolerance is the ability of a component or subsystem to continue to be able to undertake the required safety instrumented function in the presence of one or more dangerous faults in the hardware”

It is up to the user of [1] to decide which of these two tables above that shall be used when defining the architectural constraints reached by the PE logic solver subsystem/subsystem element.

In our example we could for instance focus on subsystem 2 called *Safety PLC*. In this example the Safety PLC is categorized as a PE logic solver. The hazard and risk assessment have given a SIL 2 claim.

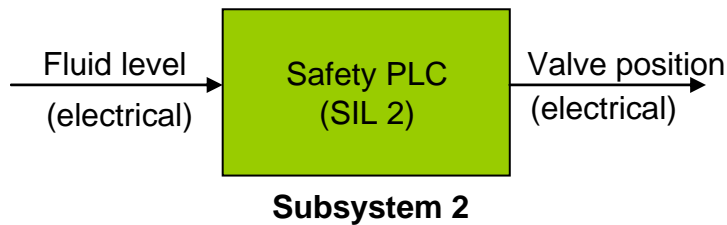


In our case two different situations exist:

- Use a single subsystem that fulfils SIL2 architectural requirements
- Connect in parallel two different subsystem elements that each fulfils SIL1 architectural requirements

Use a single subsystem that fulfils SIL 2 architectural requirements:

In this case it is necessary to first decide if Table 5 in [1] or Table 3 in [5] shall be used when defining reached architectural constraints. After that you have to check that the PE logic solver bought from the manufacturer fulfils the requirements for the Table you have decided to choose (including *Hardware Fault Tolerance* and *Safe Failure Fraction*)



Connect in parallel two different subsystem elements that each fulfils SIL 1 architectural requirement:

This is not the normal situation when buying a PE logic solver (for instance a Safety PLC) from a manufacturer. The typical situation is that the architectural constraints reached by the PE logic solver are high enough when it is used as a single subsystem. Based on this no example is given on how to connect in parallel two different PE logic solver subsystems connected in parallel.

4.1.1.1.2 Requirements for the probability of failure on demand for PE logic solver subsystems/subsystem elements

Two different situations exist:

- The subsystem only consists of a single PE logic solver subsystem
- The subsystem consists of a number of PE logic solver subsystem elements

Note 1 in chapter 11.9.2 in [1] informs about a number of different modelling methods that are available:

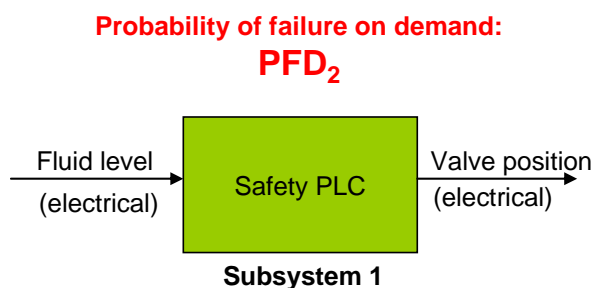
- Simulation
- Cause consequence analysis
- Fault-tree analysis
- Markov models
- Reliability block diagrams

By using these models it is possible to estimate which overall PFD value that is reached depending on how the individual subsystem elements are connected to each other.

The susceptibility of the subsystem to common cause failures is important to consider when the subsystem is realised by using subsystem elements. In this case it is important to estimate the contribution of common cause failure (CCF) by calculating the β -factor.

In our example we could for instance again focus on subsystem 2 called Safety PLC.

The hazard and risk assessment have given a SIL 2 claim for the complete SIF.



SIL 2 requires that the overall probability of failure on demand is below 10^{-2} :

SIL 2 claim:
 $PFD_1 + PFD_2 + PFD_3 < 10^{-2}$

Thus PFD₂ summarized together with PFD₁ and PFD₃ must be less than 10^{-2} .

4.1.1.2 Sensors, final elements and non-PE logic solvers subsystems/subsystem elements

- It is important to point out that also smart sensors and smart final elements is included in this category even though these subsystems/subsystem elements includes programmable electronics (PE).

It is the responsibility of the manufacturer of the sensors, final elements and non-PE logic solvers to give the following information:

- Reached architectural SIL level according to the requirements in:
 - Table 6 in [1] or
 - Table 2 in [5] (including *Hardware Fault Tolerance* and *Safe Failure Fraction*), if the requirements in chapter 11.4.5 in [1] are fulfilled or
 - Table 3 in [5] (including *Hardware Fault Tolerance* and *Safe Failure Fraction*), if the requirements in chapter 11.4.5 in [1] are fulfilled
- Failure rate (λ_{du} , λ_{dd} , λ_s)
- Probability of failure on demand (PFD) versus Proof test interval for a single channel configuration

The description of sensors, final elements and non-PE logic solvers subsystems/subsystem elements is divided into the following two types of requirements from [1]:

- Architectural constraints
- Requirements for the probability of failure on demand

To fulfil the requirements concerning hardware safety integrity both of these above types of requirements must be fulfilled.

4.1.1.2.1 Architectural constraints on hardware safety integrity for sensors, final elements and non-PE logic solvers subsystems/subsystem elements

In the situation that the design is based on bought sensors, final elements and non-PE logic solvers subsystems/subsystem elements that already fulfil hardware safety integrity requirements up to a certain level, Table 6 in [1] or Table 2 and 3 in [5] could be interpreted as describing the internal architectural requirements of a certain subsystem/subsystem element.

Table 6 - Minimum hardware fault tolerance of sensors and final elements and non-PE logic solver	
SIL	Minimum hardware fault tolerance (see chapter 11.4.3 and 11.4.4 in [1])
1	0
2	1
3	2
4	Special requirements apply (see IEC 61508)

Table 2 – Hardware safety integrity: architectural constraints on type A safety-related subsystems			
Safe Failure Fraction	Hardware fault tolerance		
	0	1	2
< 60%	SIL1	SIL2	SIL3
60% - <90%	SIL2	SIL3	SIL4
90% - <99%	SIL3	SIL4	SIL4
≥99%	SIL3	SIL4	SIL4

Table 3 – Hardware safety integrity: architectural constraints on type B safety-related subsystems			
Safe Failure Fraction	Hardware fault tolerance		
	0	1	2
< 60%	Not allowed	SIL1	SIL2
60% - <90%	SIL1	SIL2	SIL3
90% - <99%	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4

In [1] *hardware fault tolerance* is defined in the following way:

“Hardware fault tolerance is the ability of a component or subsystem to continue to be able to undertake the required safety instrumented function in the presence of one or more dangerous faults in the hardware”

It is up to the user of [1] to decide if Table 6 in [1] shall be used as a conservative approach or if Table 2 and 3 in [5] instead shall be used when defining the architectural constraints reached by the sensors, final elements and non-PE logic solvers.

Which one of Table 2 and 3 in [5] to use depends on if the safety-related subsystem is of type A or type B. The following definition of type A and type B safety-related subsystems could be found in chapter 7.4.3.1.2 and chapter 7.4.3.1.3 in [5]:

“A subsystem can be regarded as type A if, for the components required to achieve the safety function

- a) the failure modes of all constituent components are well defined; and*
- b) the behaviour of the subsystem under fault conditions can be completely determined; and*
- c) 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”*

“A subsystem shall be regarded as type B if, for the components required to achieve the safety function,

- a) the failure mode of at least one constituent component is not well defined; or*
- b) the behaviour of the subsystem under fault conditions cannot be completely determined; or*
- c) there is insufficient dependable failure data from field experience to support claims for rates of failure for detected and undetected dangerous failures.”*

In preparing [1] for the process sector it was considered that the requirements for fault tolerance of field devices and non PE logic solver could be simplified compared to the requirements on PE logic solvers.

As you can see above in Table 6 it does not include any information about the safe failure fraction (SFF) of low complexity subsystems/subsystem elements. Because of this the architectural SIL level that is possible to reach will be directly dependent on the chosen hardware fault tolerance.

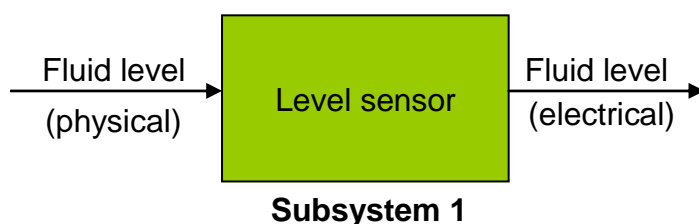
Following requirement from [1] must be considered before using Table 6 in [1]:

“For all subsystems (for example, sensors, final elements and non-PE logic solvers) except PE logic solvers the minimum hardware fault tolerance shall be as shown in Table 6 provided that the dominant failure mode is to the safe state or dangerous failures are detected (see chapter 11.3 in [1]), otherwise the fault tolerance shall be increased by one.”

As discussed above it also possible to use alternative fault tolerance requirements provided an assessment is made in accordance to the requirements of IEC 61508-2, Tables 2 and 3. This possibility is described in chapter 11.4.5 in [1].

In our example we could for instance focus on subsystem 1 called *Level sensor*. In this example the *Level sensor* is a low complexity subsystem.

The hazard and risk assessment have given a SIL 2 claim.

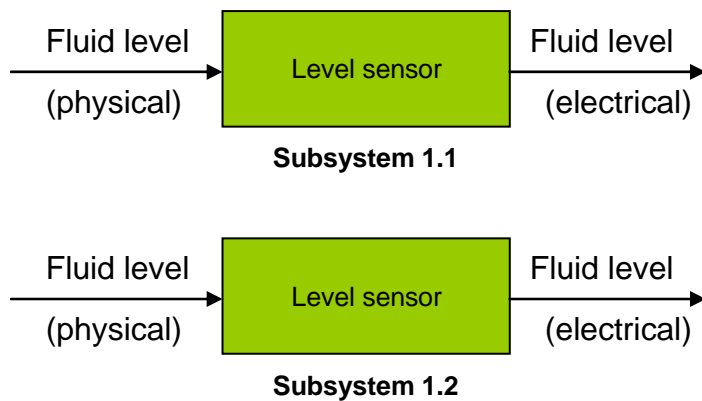


If it is decided to take a conservative approach in the design and use Table 6 in [1] for the level sensor (in this situation it is not any difference in architectural constraints required between a traditional sensor or a smart transmitter sensor). If the dominant failure modes are to the safe state or dangerous failures are detected and we have a SIL 2 claim, the following situation exist:

- Connect in parallel two different sensor subsystem elements that each fulfils SIL 1 architectural requirements

Connect in parallel two different sensor subsystem elements:

In this situation it could for instance be two level sensors.



By connecting these two level sensors in parallel the hardware fault tolerance will reach one and also the SIL will reach up to SIL 2 (see Table 6 below).

Table 6 - Minimum hardware fault tolerance of sensors and final elements and non-PE logic solver	
SIL	Minimum hardware fault tolerance (see chapter 11.4.3 and 11.4.4 in [1])
1	0
2	1
3	2
4	Special requirements apply (see IEC 61508)

4.1.1.2.2 Requirements for the probability of failure on demand for sensors, final elements and non-PE logic solvers

Two different situations exist:

- The subsystem only consists of a single sensor, final element or non-PE logic solver
- The subsystem consists of a number of subsystem elements

Note 1 in chapter 11.9.2 in [1] informs about a number of different modelling methods that are available:

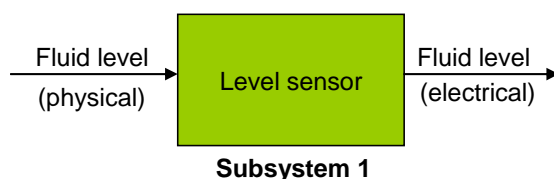
- Simulation
- Cause consequence analysis
- Fault-tree analysis
- Markov models
- Reliability block diagrams

By using these models it is possible to estimate which overall PFD value that is reached depending on how the individual subsystem elements are connected to each other.

The susceptibility of the subsystem to common cause failures is important to consider when the subsystem is realised by using subsystem elements. In this case it is important to estimate the contribution of common cause failure (CCF) by calculating the β -factor.

In our example we could for instance again focus on subsystem 1 called *Level sensor*. The hazard and risk assessment have given a SIL 2 claim for the complete SIF.

**Probability of failure on demand:
PFD₁**



SIL 2 requires that the overall probability of failure on demand is below 10^{-2} :

**SIL 2 claim:
 $PFD_1 + PFD_2 + PFD_3 < 10^{-2}$**

Thus PFD₁ summarized together with PFD₂ and PFD₃ must be less than 10^{-2} .

4.1.2 No information is available about which hardware safety integrity requirements that are fulfilled for a certain subsystem/subsystem element

A common situation in industry today is that no information is available about which hardware safety integrity requirements that are fulfilled for a certain subsystem/subsystem element.

The following situations will be described:

- PE logic solver subsystems/subsystem elements
- Sensors, final elements and non-PE logic solver

It is important to point out that it is quite complicated to perform the estimation of hardware safety integrity.

4.1.2.1 PE logic solver subsystems/subsystem elements

The following subsystem/subsystem element is an example of a PE logic solver subsystem/subsystem element:

- Safety PLC

The following information could be found in chapter 11.5.2.1 and 11.5.2.2 in [1]:

“Components and subsystems selected for use as part of a safety instrumented system for SIL 1 to SIL 3 applications shall either be in accordance with IEC 61508-2 and IEC 61508-3, as appropriate, or else they shall be in accordance with 11.4 and 11.5.3 to 11.5.6, as appropriate”

“Components and subsystems selected for use as part of a safety instrumented system for SIL 4 applications shall be in accordance with IEC 61508-2 and IEC 61508-3, as appropriate”

These requirements must be fulfilled for a PE logic solver. The following definition of *programmable electronics (PE)* is found in [1]:

“Electronic component or device forming part of a PES and based on computer technology. The term encompasses both hardware and software and input and output units”

Chapter 11.5.3 to 11.5.5 in [1] describes which requirements that must be fulfilled for a PE logic solver subsystem/subsystem element to be regarded as “based on prior use”. If all these requirements are fulfilled it may be possible to use a PE logic solver that is not developed according to the requirements in [5] as part of a SIF. When this is allowed or not will not be further described in this report.

If a PE logic solver does not fulfil the requirements concerning “based on prior use” in [1] it shall conform to the relevant requirements of IEC 61508-2 and IEC 61508-3.

Outgoing from the above description the following situations exists for a PE logic solver subsystem/subsystem element when no information is available about which hardware safety integrity requirements that are fulfilled:

- If the design is based on a bought PE logic solver subsystem/subsystem element it will be necessary to contact the manufacturer and ask them if the PE logic solver subsystem/subsystem element conforms to the relevant requirements of IEC 61508-2 and IEC 61508-3 or if the PE logic solver subsystem/subsystem element fulfils all requirements to be regarded as “based on prior use” as described in [1]
It is important to point out that even when a PE logic solver subsystem/subsystem element is developed according to the relevant requirements of IEC 61508-2 and IEC 61508-3 the architectural SIL that could be claimed could either be decided by Table 5 in [1] or Table 3 in [5]. It is up to the user of [1] to choose which architectural constraints to use for the PE logic solver subsystem/subsystem element in the design.
- If the design is based on a own-developed PE logic solver subsystem/subsystem element it must conform to the relevant requirements of IEC 61508-2 and IEC 61508-3 or it must fulfil all requirements to be regarded as “based on prior use” as described in [1]
It is important to point out that even when a PE logic solver subsystem/subsystem element is developed according to the relevant requirements of IEC 61508-2 and IEC 61508-3 the architectural SIL that could be claimed could either be decided by Table 5 in [1] or Table 3 in [5]. It is up to the user of [1] to choose which architectural constraints to use for the PE logic solver subsystem/subsystem element in the design.

The estimation of hardware safety integrity for a PE logic solver subsystem/subsystem element is divided into the following two parts:

- Estimation of safe failure fraction (SFF) by using FMEDA (Failure Mode Effects and Diagnostic Analysis).
- Estimation of the probability of failure on demand based on the results from the FMEDA

4.1.2.1.1 Estimation of safe failure fraction (SFF) for a PE logic solver subsystem/subsystem element by using FMEDA

Following information could be found in chapter 11.4.2 in [2]:

“In establishing the SFF it is acceptable to assume that the subsystem has been properly selected for the application and is adequately installed, commissioned and maintained such that early life failures and age related failure may be excluded from the assessment. Human factors do not need to be considered when determining SFF”

The following definition of safe failure fraction (SFF) is found in [1]:

“fraction of the overall failure rate of a subsystem that does not result in a dangerous failure”

The mathematical definition of safe failure fraction:

$$\text{SFF} = \frac{\sum \lambda_s + \sum \lambda_{dd}}{\sum \lambda_d + \sum \lambda_s} [\%]$$

where

λ_s is the rate of safe failure

$\sum \lambda_s + \sum \lambda_d$ is the overall failure rate

λ_{DD} is the rate of dangerous failure which is detected by diagnostic functions

λ_D is the rate of dangerous failure

$$\lambda_D = \lambda_{DD} + \lambda_{DU}$$

λ_{DD} is the rate of dangerous detected failure

λ_{DU} is the rate of dangerous undetected failure

Depending on which architectural constraints that are decided to be used when applying [1] either Table 5 in [1] or Table 3 in [5] gives information about which SIL level that is possible to reach when a certain SFF value is calculated.

Table 5 – Minimum hardware fault tolerance of PE logic solvers			
SIL	Minimum hardware fault tolerance		
	SFF < 60 %	SFF 60 % to 90 %	SFF > 90 %
1	1	0	0
2	2	1	0
3	3	2	1
4	Special requirements apply (see IEC 61508)		

Table 3 – Hardware safety integrity: architectural constraints on type B safety-related subsystems			
Safe Failure Fraction	Hardware fault tolerance		
	0	1	2
< 60%	Not allowed	SIL1	SIL2
60% - <90%	SIL1	SIL2	SIL3
90% - <99%	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4

In IEC 61511 *hardware fault tolerance* is defined in the following way:

“Hardware fault tolerance is the ability of a component or subsystem to continue to be able to undertake the required safety instrumented function in the presence of one or more dangerous faults in the hardware”

The following information is found in chapter 11.4.1 in [1]:

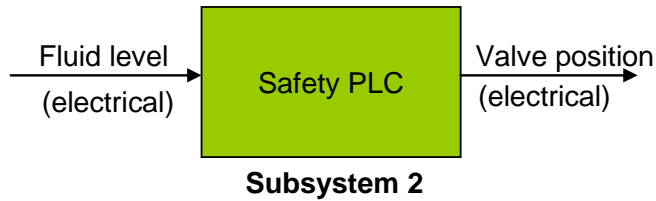
“For safety instrumented functions, the sensors, logic solvers and final elements shall have a minimum hardware fault tolerance”

“NOTE 1 Hardware fault tolerance is the ability of a component or subsystem to continue to be able to undertake the required safety instrumented function in the presence of one or more dangerous faults in hardware. A hardware fault tolerance of 1 means that there are, for example, two devices and the architecture is such that the dangerous failure of one of the two components or subsystems does not prevent the safety action from occurring.”

“NOTE 2 The minimum hardware fault tolerance has been defined to alleviate potential shortcomings in SIF design that may result due to the number of assumptions made in the design of the SIF, along with uncertainty in the failure rate of components or subsystems used in various process applications.”

“NOTE 3 It is important to note that the hardware fault tolerance requirements represent the minimum component or subsystem redundancy. Depending on the application, component failure rate and proof-testing interval, additional redundancy may be required to satisfy the SIL of the SIF according to 11.9.”

In our example we could for instance focus on subsystem 2 called Safety PLC. The hazard and risk assessment have given a SIL 2 claim.



If this subsystem is build up by a single subsystem, and it is decided to use the architectural constraints described in Table 5 in [1] it is possible to reach SIL 2 architectural requirements in three different ways:

- Hardware fault tolerance is equal to one and the safe failure fraction is in the interval between 60% and 90% for each individual subsystem element
- Hardware fault tolerance is equal to zero and the safe failure fraction is above 90% for each individual subsystem element
- Hardware fault tolerance is equal to two and the safe failure fraction is below 60 %

Table 5 – Minimum hardware fault tolerance of PE logic solvers			
SIL	Minimum hardware fault tolerance		
	SFF < 60 %	SFF 60 % to 90 %	SFF > 90 %
1	1	0	0
2	2	1	0
3	3	2	1
4	Special requirements apply (see IEC 61508)		

4.1.2.1.2 Estimation of the probability of failure on demand for a PE logic solver subsystem/subsystem element based on the results from the FMEDA (Failure Mode Effects and Diagnostic Analysis)

If your company earlier has performed an estimation of safe failure fraction for a certain specific PE logic solver subsystem/subsystem element the results of this work will be an important input when performing the calculation of the probability of failure on demand of a subsystem/subsystem element (see chapter 4.1.2.2.1).

The probability of failure on demand is dependent on how the subsystems/subsystem elements are built up and where many different aspects influence the result.

The following aspects shall be taken into consideration when estimating the probability of failure on demand (as described in chapter 11.9.2 in [1]):

- a) the architecture of the SIS as it relates to each safety instrumented function under consideration;*
 - b) the estimated rate of failure of each subsystem, due to random hardware faults, in any modes which would cause a dangerous failure of the SIS but which are detected by diagnostic tests;*
 - c) the estimated rate of failure of each subsystem, due to random hardware faults, in any modes which would cause a dangerous failure of the SIS which are undetected by the diagnostic tests;*
- NOTE The estimated rates of failure of a subsystem can be determined by a quantified failure-mode analysis of the design using component or subsystem failure data from a recognized industry source or from experience of the previous use of the subsystem in the same environment as for the intended application, and in which the experience is sufficient to demonstrate the claimed mean time to failure on a statistical basis to a single-sided lower confidence limit of at least 70 %.*
- d) the susceptibility of the SIS to common cause failures;*
 - e) the diagnostic coverage of any periodic diagnostic tests (determined according to IEC 61511-2), the associated diagnostic test interval and the reliability for the diagnostic facilities;*
 - f) the intervals at which proof tests are undertaken;*
 - g) the repair times for detected failures;*
 - h) the estimated rate of dangerous failure of any communication process in any modes which would cause a dangerous failure of the SIS (both detected and undetected by diagnostic tests);*
 - i) the estimated rate of dangerous failure of any human response in any modes which would cause a dangerous failure of the SIS (both detected and undetected by diagnostic tests);*
 - j) the susceptibility to EMC disturbances (for example, according to IEC 61326-1);*
 - k) the susceptibility to climatic and mechanical conditions (for example, according to IEC 60654-1 and IEC 60654-3).*

The susceptibility of the subsystem to common cause failures is important to consider when the subsystem is realised by using subsystem elements. In this case it is important to estimate the contribution of common cause failure (CCF) by calculating the β -factor.

4.1.2.2 Sensors, final elements and non-PE logic solver subsystems/subsystem elements

The following situations exist for sensors, final elements and non-PE logic solver subsystems/subsystem elements when no information is available about which hardware safety integrity requirements that are fulfilled:

- If the design is based on a bought sensor, final element and non-PE logic solver subsystem/subsystem element it will be necessary to contact the manufacturer and ask them if the subsystem/subsystem element conforms to the relevant requirements of [1]
- If the design is based on own-developed sensors, final elements and non-PE logic solve subsystems/subsystem elements they must conform to the relevant requirements of [1]

The estimation of hardware safety integrity for sensors, final elements and non-PE logic solver subsystem/subsystem element is divided into the following two parts:

- Estimation of safe failure fraction (SFF) by using FMEDA (Failure Mode Effects and Diagnostic Analysis). For a sensor, final element and non-PE logic solver subsystem/subsystem element it would in principle not be necessary to perform a calculation of SFF to be able to know which architectural SIL that is reached (because the reached architectural SIL according to table 6 in [1] only depends on the hardware fault tolerance). But anyway this will be necessary because this information is used as an input to the estimation of PFD (Probability of Failure on Demand)
- Estimation of the PFD (Probability of Failure on Demand), based on the results from the FMEDA

4.1.2.2.1 Estimation of safe failure fraction (SFF) for a sensor, final element and non-PE logic solver subsystem/subsystem element by using FMEDA

Following information could be found in chapter 11.4.2 in [2]:

“In establishing the SFF it is acceptable to assume that the subsystem has been properly selected for the application and is adequately installed, commissioned and maintained such that early life failures and age related failure may be excluded from the assessment. Human factors do not need to be considered when determining SFF”

The following definition of safe failure fraction (SFF) is found in [1]:

“fraction of the overall failure rate of a subsystem that does not result in a dangerous failure”

The mathematical definition of safe failure fraction:

$$\text{SFF} = \frac{\sum \lambda_s + \sum \lambda_{dd}}{\sum \lambda_d + \sum \lambda_s} \quad [\%]$$

where

λ_s is the rate of safe failure

$\sum \lambda_s + \sum \lambda_d$ is the overall failure rate

λ_{DD} is the rate of dangerous failure which is detected by diagnostic functions

λ_D is the rate of dangerous failure

$$\lambda_D = \lambda_{DD} + \lambda_{DU}$$

λ_{DD} is the rate of dangerous detected failure

λ_{DU} is the rate of dangerous undetected failure

Table 6 in [1] gives information about which SIL level that is possible to reach when a certain hardware fault tolerance is used.

Table 6 - Minimum hardware fault tolerance of sensors and final elements and non-PE logic solver	
SIL	Minimum hardware fault tolerance (see chapter 11.4.3 and 11.4.4 in [1])
1	0
2	1
3	2
4	Special requirements apply (see IEC 61508)

In IEC 61511 *hardware fault tolerance* is defined in the following way:

“Hardware fault tolerance is the ability of a component or subsystem to continue to be able to undertake the required safety instrumented function in the presence of one or more dangerous faults in the hardware”

The following information is found in chapter 11.4.1 in [1]:

“For safety instrumented functions, the sensors, logic solvers and final elements shall have a minimum hardware fault tolerance”

“NOTE 1 Hardware fault tolerance is the ability of a component or subsystem to continue to be able to undertake the required safety instrumented function in the presence of one or more dangerous faults in hardware. A hardware fault tolerance of 1 means that there are, for example, two devices and the architecture is such that the dangerous failure of one of the two components or subsystems does not prevent the safety action from occurring.”

“NOTE 2 The minimum hardware fault tolerance has been defined to alleviate potential shortcomings in SIF design that may result due to the number of assumptions made in the design of the SIF, along with uncertainty in the failure rate of components or subsystems used in various process applications.”

“NOTE 3 It is important to note that the hardware fault tolerance requirements represent the minimum component or subsystem redundancy. Depending on the application, component failure rate and proof-testing interval, additional redundancy may be required to satisfy the SIL of the SIF according to 11.9.”

In preparing [1] for the process sector it was considered that the requirements for fault tolerance of field devices and non PE logic solver could be simplified compared to the requirements on PE logic solvers.

As you can see above in Table 6 in [1] it does not include any information about the safe failure fraction (SFF) of sensors, final elements and non-PE logic solvers subsystems/subsystem elements. Because of this the architectural SIL level that is possible to reach will be directly dependent on the chosen hardware fault tolerance.

Following requirement from [1] must be considered before using Table 6 in [1]:

“For all subsystems (for example, sensors, final elements and non-PE logic solvers) except PE logic solvers the minimum hardware fault tolerance shall be as shown in Table 6 provided that the dominant failure mode is to the safe state or dangerous failures are detected (see chapter 11.3 in [1]), otherwise the fault tolerance shall be increased by one.”

Requirement that must be fulfilled to be allowed to reduce the hardware fault tolerance by one for sensors, final elements and non-PE logic solver subsystems/subsystem elements:

For sensors, final elements and non-PE logic solver subsystems/subsystem elements it is possible to reduce the hardware fault tolerance by one if the following requirements from [1] are fulfilled:

“For all subsystems (for example, sensor, final elements and non-PE logic solvers) excluding PE logic solvers the minimum fault tolerance specified in Table 6 in [1] may be reduced

by one if the devices used comply with all of the following:

- *the hardware of the device is selected on the basis of prior use (see chapter 11.5.3 in [1])*
- *the device allows adjustment of process-related parameters only, for example, measuring range, upscale or downscale failure direction*
- *the adjustment of the process-related parameters of the device is protected, for example, jumper, password*
- *the function has an SIL requirement of less than 4.”*

Alternative fault tolerance requirements:

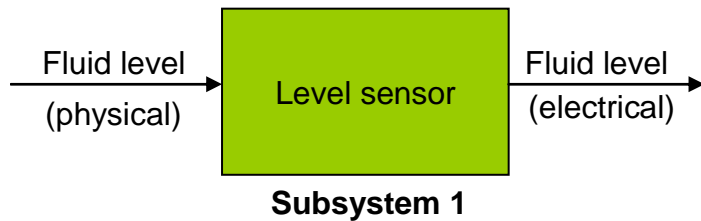
Following requirement is found in [1]:

“Alternative fault tolerance requirements may be used providing an assessment is made in accordance to the requirements of IEC 61508-2, Tables 2 and 3.”

As described above it may be possible to reduce the fault tolerance for sensors, final elements and non-PE logic solver subsystems/subsystem elements by following the fault tolerance requirements in [5] instead of following the requirement in Table 6 in [1]. An example could for instance be when a mechanical valve is equipped with a partial stroke test. Even if this mechanical valve in itself is a subsystem that typically should use Table 6 in [1] it is preferable to use the fault tolerance requirements in [5], because these requirements take into account the high degree of safe failure fraction (SFF) reached by using partial valve stroke.

In our example we could for instance again focus on subsystem 1 called *Level sensor*. In this case the level sensor **does not** fulfil above described requirements concerning *reduced hardware fault tolerance* and use of *alternative fault tolerance requirements*.

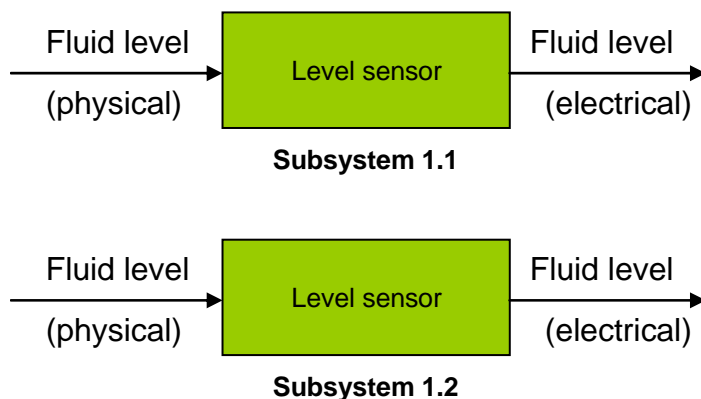
The design is based on level sensor subsystems/subsystem elements (where the dominant failure modes are to the safe state or dangerous failures are detected) and the hazard and risk assessment have given a SIL 2 claim.



It is shown below in Table 6 in [1] that it is necessary to have a minimum hardware fault tolerance of one to reach SIL 2 architectural requirements.

Table 6 - Minimum hardware fault tolerance of sensors and final elements and non-PE logic solver	
SIL	Minimum hardware fault tolerance (see chapter 11.4.3 and 11.4.4 in [1])
1	0
2	1
3	2
4	Special requirements apply (see IEC 61508)

So in this example it is necessary to connect two level sensors in parallel to reach SIL 2 architectural requirements according to Table 6 in [1].



4.1.2.2.2 Estimation of the probability of failure on demand for sensors, final elements and non-PE logic solver subsystem/subsystem element based on the results from the FMEDA (Failure Mode Effects and Diagnostic Analysis)

If your company earlier has performed an estimation of safe failure fraction for a certain specific sensor, final element and non-PE logic solver subsystem/subsystem element the results of this work will be an important input when performing the calculation of the probability of failure on demand of a subsystem/subsystem element (see chapter 4.1.2.2.1).

The probability of failure on demand is dependent on how the subsystems/subsystem elements are built up and where many different aspects influence the result.

The following aspects shall be taken into consideration when estimating the probability of failure on demand (as described in chapter 11.9.2 in [1]):

- a) the architecture of the SIS as it relates to each safety instrumented function under consideration;*
 - b) the estimated rate of failure of each subsystem, due to random hardware faults, in any modes which would cause a dangerous failure of the SIS but which are detected by diagnostic tests;*
 - c) the estimated rate of failure of each subsystem, due to random hardware faults, in any modes which would cause a dangerous failure of the SIS which are undetected by the diagnostic tests;*
- NOTE The estimated rates of failure of a subsystem can be determined by a quantified failure-mode analysis of the design using component or subsystem failure data from a recognized industry source or from experience of the previous use of the subsystem in the same environment as for the intended application, and in which the experience is sufficient to demonstrate the claimed mean time to failure on a statistical basis to a single-sided lower confidence limit of at least 70 %.*
- d) the susceptibility of the SIS to common cause failures;*
 - e) the diagnostic coverage of any periodic diagnostic tests (determined according to IEC 61511-2), the associated diagnostic test interval and the reliability for the diagnostic facilities;*
 - f) the intervals at which proof tests are undertaken;*
 - g) the repair times for detected failures;*
 - h) the estimated rate of dangerous failure of any communication process in any modes which would cause a dangerous failure of the SIS (both detected and undetected by diagnostic tests);*
 - i) the estimated rate of dangerous failure of any human response in any modes which would cause a dangerous failure of the SIS (both detected and undetected by diagnostic tests);*
 - j) the susceptibility to EMC disturbances (for example, according to IEC 61326-1);*
 - k) the susceptibility to climatic and mechanical conditions (for example, according to IEC 60654-1 and IEC 60654-3).*

The susceptibility of the subsystem to common cause failures is important to consider when the subsystem is realised by using subsystem elements. In this case it is important to estimate the contribution of common cause failure (CCF) by calculating the β -factor.

4.2 Hardware safety integrity requirements for the complete safety instrumented function (SIF)

In the same way as for subsystems/subsystem elements the following requirements must also be fulfilled for the complete SIF

- Architectural constraints
- Requirements for the probability of failure on demand

To fulfil the requirements concerning hardware safety integrity for the complete SIF both of these above types of requirements must be fulfilled.

4.2.1 Architectural constraints on hardware safety integrity for the complete safety instrumented function (SIF)

The SIF is divided into a number of subsystems. Each of these subsystems must fulfil the architectural SIL claim for the complete SIF.

The following information is found in chapter 11.4.1 in [1]:

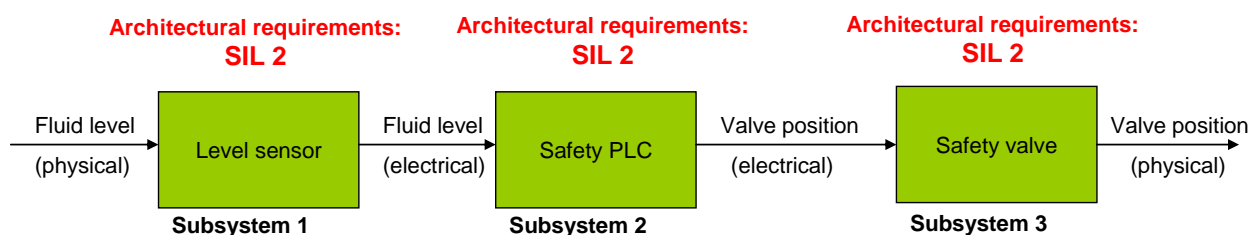
“For safety instrumented functions, the sensors, logic solvers and final elements shall have a minimum hardware fault tolerance”

“NOTE 1 Hardware fault tolerance is the ability of a component or subsystem to continue to be able to undertake the required safety instrumented function in the presence of one or more dangerous faults in hardware. A hardware fault tolerance of 1 means that there are, for example, two devices and the architecture is such that the dangerous failure of one of the two components or subsystems does not prevent the safety action from occurring.”

“NOTE 2 The minimum hardware fault tolerance has been defined to alleviate potential shortcomings in SIF design that may result due to the number of assumptions made in the design of the SIF, along with uncertainty in the failure rate of components or subsystems used in various process applications.”

“NOTE 3 It is important to note that the hardware fault tolerance requirements represent the minimum component or subsystem redundancy. Depending on the application, component failure rate and proof-testing interval, additional redundancy may be required to satisfy the SIL of the SIF according to 11.9.”

In our example this requirement brings about that each subsystem must fulfil SIL 2 architectural requirements:



The architectural SIL claim for a certain subsystem could be fulfilled by using a single subsystem or by combining subsystem elements. More information about this could be found in chapter 4.1.

4.2.2 Requirements for the probability of failure on demand for the complete safety instrumented function (SIF)

The overall PFD value of the complete SIF is built up by the individual PFD values of each subsystem:

$$PFD = PFD_1 + \dots + PFD_n + P_{TE}$$

- PFD Overall probability of failure on demand for the complete SIF
- PFD₁ Probability of failure on demand for subsystem 1
- ...
- PFD_n Probability of failure on demand for subsystem n
- P_{TE} Probability of dangerous transmission errors for digital data communication processes

The overall PFD value of the complete SIF must be low enough to fulfil the requirements for a certain SIL as described in below table:

Probability of failure on demand (PFD)

SIL	PFD	RRF
1	$<10^{-1}$ till $\geq 10^{-2}$	$10 \leq RRF \leq 100$
2	$<10^{-2}$ till $\geq 10^{-3}$	$100 \leq RRF \leq 1000$
3	$<10^{-3}$ till $\geq 10^{-4}$	$1000 \leq RRF \leq 10000$
4	$<10^{-4}$ till $\geq 10^{-5}$	$1000 \leq RRF \leq 10000$

The term *RRF* is an abbreviation of *Risk Reduction Factor* and the connection between PFD and RRF is as follows: $PFD=1/RRF$

In our example the hazard and risk assessment has identified that the probabilistic SIL claim for the complete SIF is SIL 2. SIL 2 requires that the overall probability of failure on demand for the complete SIF must be in the following interval, $10^{-3} \leq \text{PFD} < 10^{-2}$. Thus $\text{PFD}_1 + \text{PFD}_2 + \text{PFD}_3$ must be less than 10^{-2} :

