Elias Mabook

Failure Modes, Effects, and Diagnostic Analysis of a Safety Device

Helsinki Metropolia University of Applied Sciences

Bachelor of Engineering

Degree Programme in Electronics

Bachelor’s Thesis

24 April 2017

Helsinki
Metropolia
University of Applied Sciences

Abstract

Author(s)	Elias Mabook
Title	Failure Modes, Effects, and Diagnostic Analysis of a Safety Device
Number of Pages	43 pages + 2 appendices
Date	24 April 2017
Degree	Bachelor Degree of Engineering
Degree Programme	Degree Programme in Electronics
Specialisation option	
Instructor(s)	Petri Havanto, Functional Safety Architect (ABB Oy) Matti Fischer, Principal Lecturer (Metropolia UAS)

The purpose of this work was to perform FMEDA for the safety module developed in the PESTO project for ABB Oy Low Voltage Drives.

The safety module acts as an adapter between a PLC and the drive while supporting PROFINET functions, as well as PROFIsafe over PROFINET. The safety module has one safety function: STO.

The device was designed and developed to be able to perform up to SIL3 level according to IEC 61508:2010 and performance level PL E according to ISO 13849:2015.
Throughout this work, the safety device’s electronic circuitry will be analysed in order to ensure that it meets the design requirements from failure probability perspective.

The safety device will be a common option for the drive families that support F-series fieldbus adapter and has a built-in STO circuit (ACS880, ACS580 and ACS380). It is anticipated that the device will be released to public during Autumn 2017.

Following this thesis, fault insertion testing will be carried out to validate the results achieved in the FMEDA. In addition, a thorough report summarizing the FMEDA results will be written and submitted to a certified body for safety integrity level and performance level certification as a part of the design documentation.

Keywords	Functional Safety, FMEDA, Fault Insertion testing, STO, IEC 61508, ISO 13849

Contents

Appendices

List of Figures

List of Tables

Abbreviations

DC	**D**iagnostic **C**overage
FIT	**F**ailures **in** **T**ime
FMEA	**F**ailure **M**ode and **E**ffect **A**nalysis
FMEDA	**F**ailure **M**odes, **E**ffects, and **D**iagnostic **A**nalysis
FSO	**F**unctional **S**afety **O**ption
HFT	**H**ardware **F**ault **T**olerance
IEC	**I**nternational **E**lectrotechnical **C**ommission
ISO	**I**nternational **O**rganization for **S**tandardization
SFF	**S**afe **F**ailure **F**raction
SIF	**S**afety **I**nstrumented **F**unction
SIL	**S**afety **I**ntegrity **L**evel
SIS	**S**afety **I**nstrumented **S**ystem
STO	**S**afe **T**orque **O**ff
MCU	**M**icrocontroller **U**nit
MTBF	**M**ean **T**ime **b**etween **F**ailures
MTTF	**M**ean **T**ime **t**o **F**ailure
MTTR	**M**ean **T**ime **t**o **R**epair
PCB	**P**rinted **C**ircuit **B**oard
PFD	**P**robability of **F**ailure on **D**emand
PFD_{avg}	The Average **P**robability of **F**ailure on **D**emand
PFH	**P**robability of Dangerous **F**ailure per **H**our
PL	**P**erformance **L**evel

1 Introduction

Functional safety plays a vital and growing role in the industry aiming to minimize potential hazards and risks. Due to lethal industrial incidents and disasters witnessed in the past, regulations and rules have been formed to help in risk assessment and prevention.

With the increasing need of electrical/electronic/programmable-electronic safety-related systems, new standards had to be introduced to meet the new requirements and demands. In the EU, two standards are mainly followed: IEC 61508:2010 and ISO 13849:2015. These standards will be overviewed later.

The goal of this thesis was to perform a failure modes, effects, and diagnostic analysis (FMEDA) for the safety device developed in the PESTO project for ABB Oy. FMEDA is a systematic process used in the development stage of a product to ensure that it meets the pre-determined safety requirements. In the FMEDA, each component is analysed for possible failures and the consequences of these failures on the system.

Before heading to the FMEDA process, a general understanding of the safety levels, terms, and system architectures are a necessity. This work will provide the reader with a brief introduction to functional safety and the elementary knowledge required to understand the FMEDA procedure and its results.

In chapter 2, functional safety will be discussed. The terms commonly used will be presented and explained. In addition, IEC 61508 and ISO 13849 standards will be introduced.

In chapter 3, different safety system architectures will be explained and compared. The formulas to be used in each architecture will be presented as well.

Chapter 4 will focus on safety functions and provide several examples of different safety functions used in the industry.

Chapter 5 will provide an overview of the safety module developed in the PESTO project. The electronics and safety architecture used in the project will be discussed as well.

Chapter 6 will introduce the FMEDA analysis, the way it is applied for different components, and fault insertion testing method.

In chapter 7, the results achieved from the FMEDA analysis will be presented and a conclusion for this work will be given.

In appendix 1, argumentation for the β and β_D factors is given.

Finally, in appendix 2, failure rates and modes for FSB-21 are shown.

2 Functional Safety

Industrial machines, process plants and equipment may fail in a way that people are put at risk of harm. Failures may arise through random hardware failures, systematic failures and common cause failures. Functional safety is part of the overall safety of a system or a product used to perform safety function/s. Failure to carry out the safety function might lead to an immediate increase in the risks.

Functional safety levels are determined in several international standards. IEC 61508 and ISO 13849 are the main standards used in the machinery sector.

To determine the compliance of a product with specific standards and performance levels requirements created to protect against potential risks, injuries, and in the worst case, human death, a functional safety assessment shall be carried out.

To understand the difference between the two standards, few necessary terms will be presented.

2.1 Terms

2.1.1 Safety Instrumented System (SIS)

Safety Instrumented System is used to implement one or several safety functions (More about safety functions in chapter 4).

SIS, as shown in Figure 1 below, referred to as Electrical / Electronic / Programmable Electronic Safety-Related System in IEC 61508, is generally made up of three parts:

I. Sensor/Input interface: such as switches, sensors, signals
II. Logic solver: such as PLC, microprocessor.
III. Final element/Output interface: such as valve, pump.

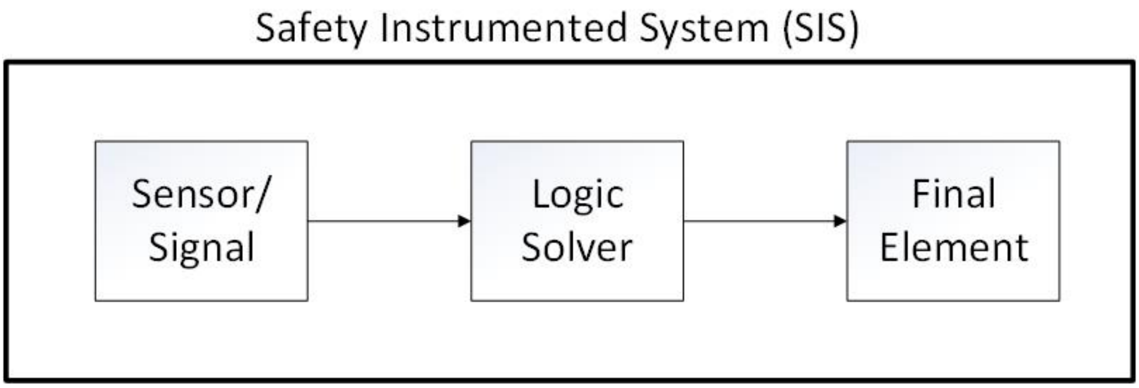


Figure 1 – Safety Instrumented System structure

2.1.2 Failure rate and modes

A failure arises when a component/device fails to perform its intended function. Failure rate, denoted as λ (Lambda), is a measure of reliability that gives the number of failures per unit time as shown in equation (1) below. Failure rate has the unit of 1/h and it is a common practise to use the unit of “failures per milliard (10^9) hours”, denoted as FIT. [1]

$$\lambda = \frac{Items\ failed}{Total\ operating\ time} \tag{1}$$

Failure rate calculations are based on complex models that take into account factors such as temperature, environment and stress.

Failures are classified as safe failures and dangerous failures as shown in Figure 2 below.

Dangerous Failures
Safe Failures

Figure 2 – Safe and Dangerous Failures

Safe Failure: A failure of a safety instrumented function component that has no effect on the ability of the system reaching to a safe state.

Dangerous Failure: A failure of a safety instrumented function component that has the potential in preventing the system from being able to reach fail-safe state when requested to do so.

Safe and dangerous failures are divided into two categories each as shown in Figure 3 below.

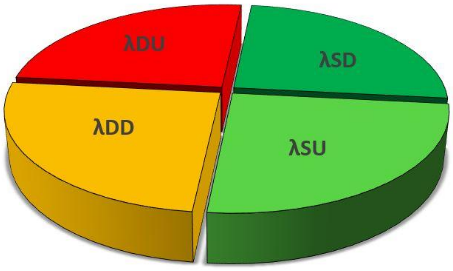


Figure 3 – Failure Modes

Safe Detected Failure (SD): A not dangerous failure that is detected by the SIS diagnostics.

Safe Undetected Failure (SU): A not dangerous failure that is not detected by the SIS diagnostics.

Dangerous Detected Failure (DD): A dangerous failure that is detected by the SIS diagnostics and which could possibly lead to a loss of a safety function.

Dangerous Undetected Failure (DU): A dangerous failure that is not detected by the SIS diagnostics and which could possibly lead to the loss of a safety function. This type of failures is regarded as the most dangerous failure and SIS designers put efforts to minimize them.

Electronic components follow the well-known bathtub curve shown below in Figure 4.

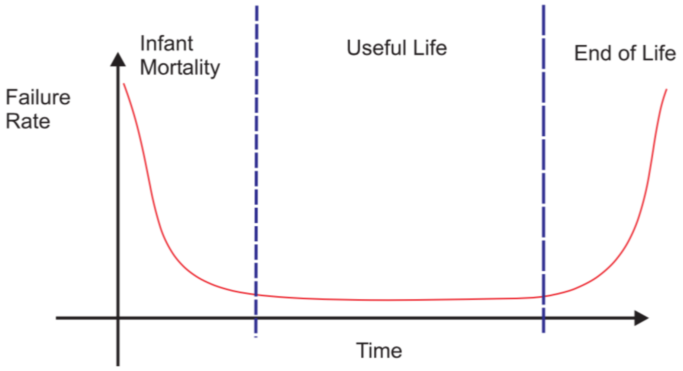


Figure 4 – The Bathtub Curve

The bathtub curve is divided into 3 sections:

Infant mortality: Many components fail as soon as they are put into use. The component might fail immediately or within a short time and generally, a defect or bad designs are the causes. The failure rate during this phase is relatively high. Manufacturers eliminate these failures with a ”burn in” period in which the components are put into use in similar conditions as they are intended to be used.

Useful lifetime: If a component doesn’t fail in the first stage, it tends to perform as expected during it is expected lifetime. The failure rate during this stage is typically low and constant.

End of life/Wear out: After a component passes its expected lifetime, it starts wearing out and the failures start increasing.

Throughout this work, failure rates are assumed to be constant.

2.1.3 Hardware Fault Tolerance (HFT)

Hardware fault tolerance is a term used in IEC 61508. HFT describes the ability of a system to continue carrying out the required safety function in the presence of one or more faults in its hardware.

A system having a hardware fault tolerance of N means that N+1 faults could cause the system to be unable to undertake the safety function.

When the safety architecture is known and it is expressed as MooN (M out of N), HFT can be simply calculated by N - M. In some cases, the term HFT is used to express whether a system has redundancy or not. This usage might create some confusion as HFT ≠ Redundancy.

2.1.4 Diagnostic Coverage (DC)

Diagnostic coverage is a term used in both standards and it describes the diagnostics ability of the safety system to detect dangerous failures out of the total number of dangerous failures. The DC is given in percentage (0-99%), which is then evaluated for every component separately.

As per ISO 13849-1, the average DC of a system can be calculated using the following formula:

$$DC_{avg} = \frac{\sum_{i=1}^{n} \frac{DC_i}{MTTF_{Di}}}{\sum_{i=1}^{n} \frac{1}{MTTF_{Di}}} \tag{2}$$

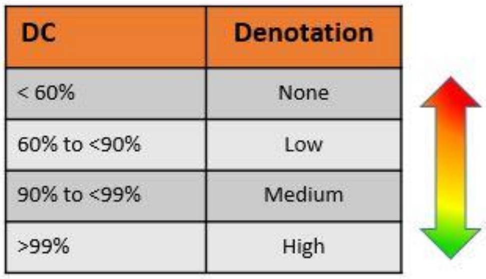
Where DC_i is a single component's diagnostic coverage and $MTTF_{Di}$ is a single component's mean time to dangerous failure.

IEC 61508 describes diagnostic coverage with the following formula as well

$$DC = \frac{\Sigma\lambda_{DD}}{\Sigma\lambda_{DD} + \Sigma\lambda_{DU}} = \frac{\Sigma\lambda_{DD}}{\Sigma\lambda_{D}} \tag{3}$$

In both standards, DC is classified in 4 categories as shown in the Table 1 below:

Table 1 – Diagnostic Coverage Classification, modified from IEC 61508 [2]



DC	Denotation
< 60%	None
60% to <90%	Low
90% to <99%	Medium
>99%	High

A higher value of DC represents a system with better diagnostics ability.

2.1.5 Safe Failure Fraction (SFF)

Safe Failure Fraction is a measure of the effectiveness of the built-in diagnostics. The safe failure fraction is similar to diagnostic coverage but additionally, it accounts for the tendency of the system to fail towards a safe state. SFF is presented in percentage and is given with the following formula

$$SFF = \frac{\Sigma\lambda_{SD}+\Sigma\lambda_{SU}+\Sigma\lambda_{DD}}{\Sigma\lambda_{SD}+\Sigma\lambda_{SU}+\Sigma\lambda_{DD}+\Sigma\lambda_{DU}} = \frac{\Sigma\lambda_{S}+\Sigma\lambda_{DD}}{\Sigma\lambda_{S}+\Sigma\lambda_{D}} = 1 - \frac{\Sigma\lambda_{DU}}{\Sigma\lambda} \qquad (4)$$

In words: The ratio of sum of safe failures (detected and undetected) plus the dangerous detected failures by the total number of all failures (safe and dangerous). Figure 5 below illustrated the SFF.

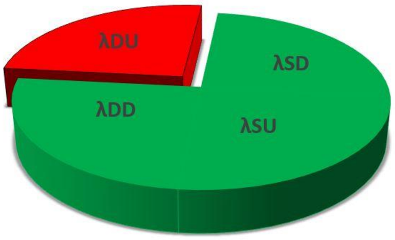


Figure 5 – Safe Failure Fraction (The green part in the pie chart)

2.1.6 Low Demand Mode and High Demand Mode

The IEC 61508 defines two fundamental operation modes:

- Demand mode: Also known as low demand mode. According to the IEC 61508 standard, it is defined as the mode in which the demands to activate the safety-instrumented function (SIF) are less than once per year (<1 per year).

- Continuous mode: Also known as high demand mode. According to the IEC 61508 standard, it is defined as the mode in which the demands to activate the SIF are more frequent compared to the low demand mode (>1 per year).

As can be understood from above, the difference between the operation modes is how often the safety-instrumented function is called into action.

2.1.7 Common Cause Failure (CCF)

A common cause failure (CCF) is a failure in which a single fault results in the failure of multiple components. Safety Instrumented Systems generally provide several advantages such as flexibility and diagnostics abilities. At the same time, there are many challenges when using a SIS. Some of these challenges are due to dependencies as a result of common design methods, same environment, operation, and maintenance procedures.

Both standards, IEC 61508 and ISO 13849, take into account CCF in the design process of a SIS. They provide means to evaluate how well the SIS is designed to cope with CCF.

IEC 61508 introduces the common cause factors β and β_D that are part of the probability of dangerous failure per hour (PFH) calculation formulas. The β factor provides the fraction of undetected dangerous failures that have a common cause while the β_D provides the fraction of detected dangerous failures that have a common cause [2]. To determine the value of β and β_D, several safety-related questions must be answered. These questions are related to the safety circuit design, analysis and environmental factors. A positive answer grants points for the X and Y variables. It is important to note that there are different X and Y variables for the different subsystems. When all questions have been answered, the following formulas can be used:

$-S = X + Y$ (To obtain the value of β) (5)

$-S_D = X(Z + 1) + Y$ (To obtain the value of β_D) (6)

To determine the value of Z, two tables, Table D.2 and Table D.3 are provided in the standard IEC 61508:6. (These tables aren't provided in this work)

After calculating the values of S and S_D, the following table is used to determine the values of β and β_D:

Table 2 – β and β_D factors, reprinted from IEC 61508[2]

Score (S or S_D)	**Corresponding value of β and β_D for the**	
	Logic subsystem	**Sensors or final elements**
120 or above	0.5%	1%
70 to 120	1%	2%
45 to 70	2%	5%
Less than 45	5%	10%

In more complicated system architectures the value of β and β_D have to be adjusted according to table D.5 in IEC 61508:6 (not provided in this work).

ISO 13849 provides a table (Table F.1, not provided in this work) that lists six groups of measures against CCF. Each group is aimed to different aspect in the design and use of the product such as separation, diversity and environmental factors. Similar to IEC 61508, points are granted if the conditions mentioned in each group are met. The maximum achievable points are 100. The value achieved is not used in any formula but it is a prerequisite for meeting a specific performance level. The CCF evaluation is relevant only in Categories (Cat.) 2, 3 and 4.

2.1.8 Type A and B devices

In IEC 61508 two types of elements are distinguished, type A and type B. The difference between the two lies in the complexity of the element, the level of confidence in understanding the failure modes of the components, the behaviour of the element under fault conditions and the failure data collected to provide confirmation of the theoretical analysis.

Type A elements are those with high level of confidence and are usually described as simple devices with well-known failure modes and a solid history of operation.
Type B elements are those with low level of confidence and are usually described as complex devices with unknown failure modes such as microprocessors, ASICS, etc. [2]

2.1.9 Average Probability of Failure, PFD_G, PFH_G

Average Probability of Failure on Demand PFD_G describes the mean probability of the system to fail dangerously and lose the ability to perform its safety function in low demand mode.

Average Probability of Failure per Hour PFH_G describes the probability of the system to fail dangerously and lose the ability to perform its safety function in continuous mode.

2.1.10 Proof test

Proof test is a periodic test executed to confirm that a SIS is still capable of performing its intended safety function. The proof test detects dangerous undetected errors that are not found by the diagnostics. If necessary, a repair procedure can be carried out to restore the system to “as new”.

2.1.11 Black Channel / White Channel

Safety systems have evolved in recent years and the use of digital communication is becoming a norm. Digital communication adds flexibility, lower cost and safer means to implement a safety function. When such data communication is used, failure measures shall be estimated accounting for transmission errors, data corruption, delays and other possible errors. In IEC 61508, two safety busses have been classified:

White channel: The entire communication channel complies with IEC 61508 and IEC 61784-3 or IEC 62280
Black channel: Parts of the communications channel is not implemented according to IEC 61508

Figure 6 below illustrates the difference between the two channels:

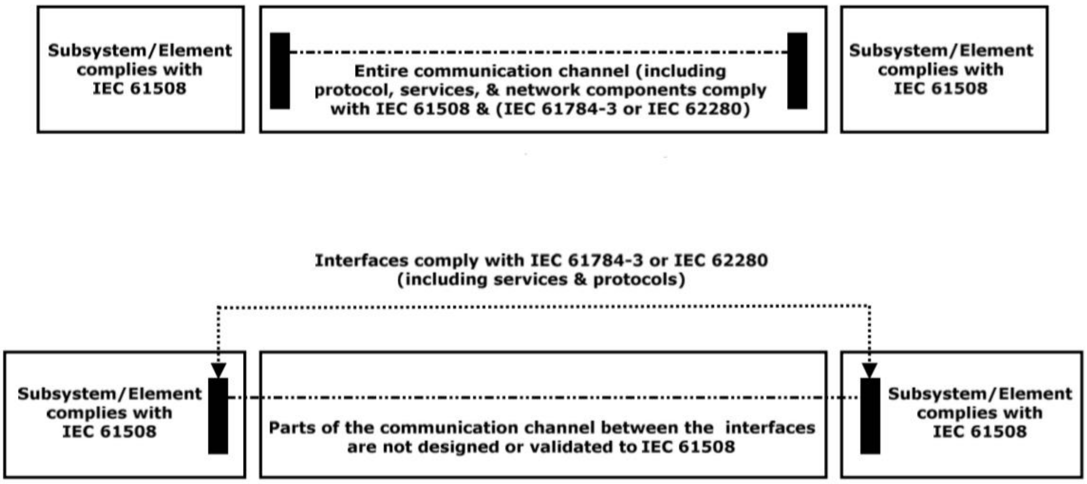

Subsystem/Element complies with IEC 61508
Entire communication channel (including protocol, services, & network components comply with IEC 61508 & (IEC 61784-3 or IEC 62280)
Subsystem/Element complies with IEC 61508
Interfaces comply with IEC 61784-3 or IEC 62280 (including services & protocols)
Subsystem/Element complies with IEC 61508
Parts of the communication channel between the interfaces are not designed or validated to IEC 61508
Subsystem/Element complies with IEC 61508

Figure 6 – Architectures for data communication, reprinted from IEC 61508 [2]

2.1.12 MTTF, MTBF, MTTR, MRT

Mean Time to Failure (MTTF) is a reliability term used to describe the mean time expected until the first unit fails. It is a statistical value that provides the mean over a long time period. MTTF should be used with non-repairable device, while MTBF should be used with repairable device. MTTF is sometimes misunderstood as it is thought to mean the guaranteed minimum lifetime.

Let’s take an example:

Table 3 – MTTF example

Component (All similar)	Time to Fail (Hours)
1	1000
2	1750
3	1500
4	1250
5	2000

In the example shown above in Table 3, the MTTF is calculated to be 1500 hours. However, a similar component can fail after 1000 hours.

Mean Time between Failures (MTBF) is one of the most commonly used reliability terms in the industry as it provides the amount of failures per million hours for a component.

$$MTBF = \frac{Total\ operating\ time}{Number\ of\ failures} => MTBF = \frac{1}{\lambda} \tag{7}$$

Mean Time to Restoration (MTTR) is a term used to describe the time for a system to be restored into operation since the system failed.
MTTR includes:

I. Failure detection time
II. Time spent until the repair took place
III. The effective repair time
IV. The time spent after the repair to put the component back into operation

In many cases, failed hardware is not repaired and rather replaced. To minimize MTTR, companies usually keep spare parts.

Mean Repair Time (MRT) is the time spent until the repair took place after the failure was detected until the system was back in order. MTR encompasses the times II+III+IV from MTTR.

2.1.13 Mean Time to Dangerous Failure - $MTTF_D$

Mean Time to Dangerous Failure $MTTF_D$, previously denoted as $MTTF_d$, is a term used in ISO 13849 and it can be easily mistaken for MTTF. The difference between the two is that $MTTF_D$ considers only the dangerous failures of the components.

2.2 Functional Safety Standards

IEC 61508 and ISO 13849 are the main standards used in the EU for functional safety in the machinery sector and are generally followed in designing and manufacturing of frequency inverters.

While these standards have similar requirements, differences exist. These differences increase the efforts of the system-designer to meet the requirements of both standards. IEC 61508 uses safety integrity level (SIL) for functional safety levels whereas ISO 13849 uses performance level (PL). While the functional safety levels given by the two standards seem to be different, similarities can be found.

2.2.1 IEC 61508 and Safety Integrity Levels (SIL)

IEC 61508 is an international standard for managing Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems. The Standard has been developed through many years to meet the up-to-date requirements and demands.

The standard provides a framework for:

- Assessing the level of risk of the equipment under control and determining if the risk is acceptable.
- Implementing a safety function for risk reduction in case the initial risk was not acceptable.
- Providing means to prove that the safety instrumented system is able to provide the required protection.

With varying levels of risk, different risk reductions majors are required for various systems. The standard provides 4 levels of risk reduction denoted by SIL (Safety Integrity

Level) with SIL 4 providing the highest degree of protection and SIL 1 providing the lowest. SIL 4 is rarely used in the process industry and it is out of the scope of this work.

To meet a specific safety integrity level, the device should be analysed from several aspects, namely:

- The device safety architecture used and the hardware fault tolerance (HFT)
- The effectiveness of the diagnostics and fraction of the safe failures from all failures (SFF)The complexity of the device (Type A/Type B)
- Determining the operation mode of the device (Low demand/High demand mode) for using the relevant formulas for calculating PFD_G/PFH_G
- Assessing the design process followed to prevent common cause failures (CCF)

In IEC 61508, two different tables are given for Type A and Type B subsystems. These tables are shown below. (Table 4 and Table 5)

Table 4 – Safety Integrity Level with Architecture for Type A Subsystems, reprinted from IEC 61508[2]

Safe Failure Fraction	**Hardware Fault Tolerance**		
	0	**1**	**2**
< 60%	SIL 1	SIL 2	SIL 3
60% to <90%	SIL 2	SIL 3	SIL 4
90% to <99%	SIL 3	SIL 4	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

Table 5 – Safety Integrity Level with Architecture for Type B Subsystems, reprinted from IEC 61508[2]

Safe Failure Fraction	**Hardware Fault Tolerance**		
	0	**1**	**2**
< 60%	Not allowed	SIL 1	SIL 2
60% to <90%	SIL 1	SIL 2	SIL 3
90% to <99%	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

As can be seen from Tables 4 and 5, to be able to meet a specific safety integrity level, the device type must be determined first. Once the device type has been determined, the safety architecture must be considered in order to get the HFT. Following, the relevant SIL can be chosen according to the calculated SFF.

In addition to above, the operation mode must be selected in order to use the relevant equations to calculate PFD_G and/or PFH_G. Some of the equations that can be used can be found in Tables 12 and 13. When PFD_G and/or PFH_G have been calculated, Table 6 must be used to determine the safety integrity level that the device can meet.

Table 6 – Low demand mode and continuos probabilities of failure, modified from IEC 61508[1]

Safety Integrity Level (SIL)	**Low demand mode of operation** (Average probability of failure to perform its design function on demand)	**High demand or continuous mode of operation** (Probability of dangerous failure per hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

In continuous mode and depending on the architecture, it might be required to assess the design process followed to prevent common cause failures in order to get the factors β and β_D as discussed earlier.

2.2.2 ISO 13849 and Performance Levels (PL)

ISO 13849 is a safety standard that provides guidance for designing safety-related control systems. The standard presents the safety requirements to be fulfilled to achieve a certain performance level.

Performance levels are classified into 5 categories with PL a offering the minimal risk reduction required and PL e with highest risk reduction.

To meet a specific performance level, the device should be analysed from several aspects, namely:

- The safety architecture used, denoted as Category in ISO 13849

- Mean Time to Dangerous Failure (MTTF$_D$)
- The average probability of failure per hour (PFH$_D$)
- The diagnostic coverage (DC)

Several tables are provided in the standard for the classification of different performance levels.

Table 7 below presents the classification of the performance levels according to PFH$_D$.

Table 7 – Performance Levels classification according to PFH$_D$, reprinted from ISO 13849[3]

PL	Average probability of failure per hour (PFH$_D$) 1/h
a	$\geq 10^{-5}\ to < 10^{-4}$
b	$\geq 3 * 10^{-6}\ to < 10^{-5}$
c	$\geq 10^{-6}\ to < 3 * 10^{-6}$
d	$\geq 10^{-7}\ to < 10^{-6}$
e	$\geq 10^{-8}\ to < 10^{-7}$

The standard provides a table for MTTF$_D$ classification. Table 8 below presents the three different denotations given for the MTTF$_D$. These denotations are used later for determining the performance level.

Table 8 – Mean time to dangerous failure of each channel (MTTF$_D$), reprinted from ISO 13849[3]

MTTF$_D$	
Denotation	**Range of each channel**
Low	$3\ years \leq MTTF_D < 10\ years$
Medium	$10\ years \leq MTTF_D < 30\ years$
High	$30\ years \leq MTTF_D \leq 100\ years$

Similar to MTTF$_D$ table, additional table is given for Diagnostic Coverage with three different denotations presented in Table 9 below.

Table 9 – Diagnostic coverage (DC), reprinted from ISO 13849[3]

DC	
Denotation	**Range**
None	$DC < 60\%$
Low	$60\% \leq DC < 90\%$
Medium	$90\% \leq DC < 99\%$
High	$99\% \leq DC$

When DC_{avg}, $MTTF_D$ have been calculated and the Category is known, Table 10 below can be used to determine the performance level.

Table 10 – Evaluating achieved Performance Level, reprinted from ISO 13849[2]

Category	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC_{avg}	None	None	Low	Medium	Low	Medium	High
MTTFD of each channel							
Low	a	Not covered	a	b	b	c	Not covered
Medium	b	Not covered	b	c	c	d	Not covered
High	Not covered	c	c	d	d	d	e

2.3 Estimation of Required SIL and PL

Risk graphs have been created to help in choosing the desired and/or required safety integrity level and performance level. These graphs account for the risk consequences, frequency and time of exposure to hazard/s, possibility of failing to avoid risk and the probability of the unwanted occurrence.

2.3.1 Estimation Method for Required SIL

Figure 7 below presents the graph in accordance with IEC 61508 for choosing safety integrity level.

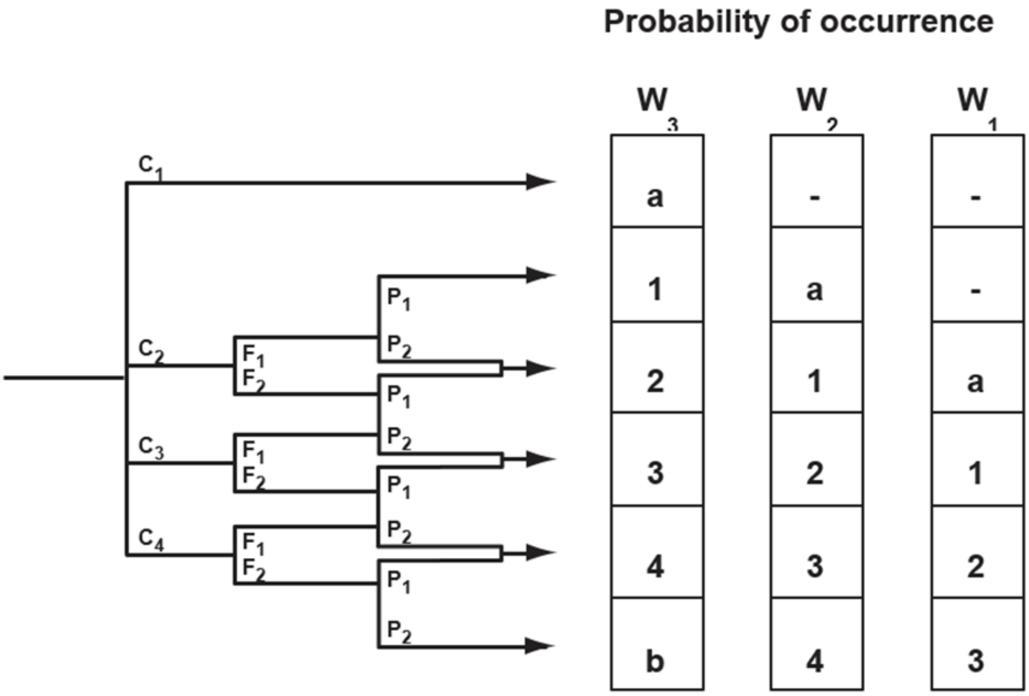


Figure 7 – Risk Graph for estimation of required SIL, reprinted from IEC 61508[2]

-- = No safety requirements

a = No special safety requirements

b = A single E/E/PE safety-related system is not sufficient

1,2,3,4= Safety Integrity Level

C = Consequence risk parameter

C_1 – Minor injury of a person

C_2 – Serious, irreversible injury of one or more people or death of one person

C_3 – Death of several people

C_4 – Disastrous effect with several dead

F = Frequency and exposure time risk parameter

F1 – Rarely to slightly more often

F2 – Frequently to continuously

P = Possibility of failing to avoid hazard risk parameter

P_1 – Possible under certain conditions

P_2 – Almost impossible

W = Probability of the unwanted occurrence

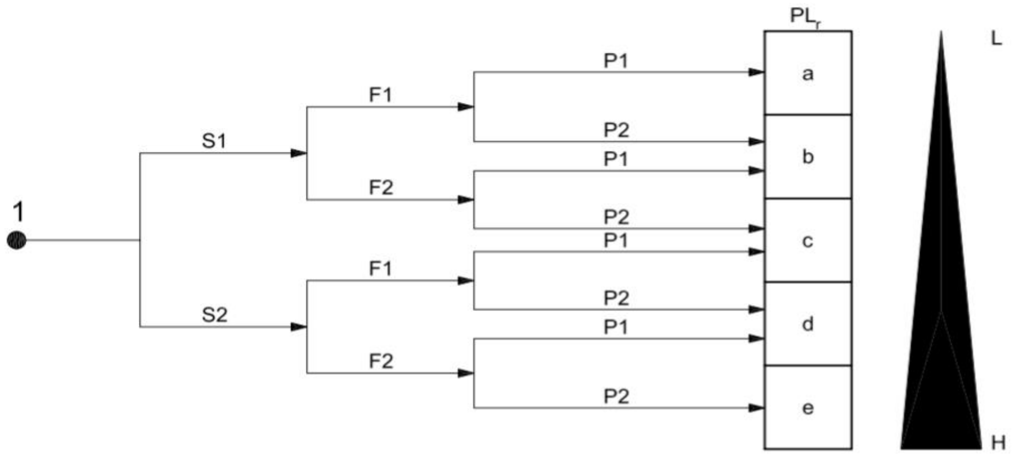
W_1 – Very small

W_2 – Small

W_3 – Relatively high

2.3.2 Estimation Method for Required PL

Figure 8 below presents the graph in accordance with ISO 13849 for choosing performance level.



Key

1	starting point for evaluation of safety function's contribution to risk reduction
L	low contribution to risk reduction
H	high contribution to risk reduction
PL$_r$	required performance level

Risk parameters:

S	severity of injury
S1	slight (normally reversible injury)
S2	serious (normally irreversible injury or death)
F	frequency and/or exposure to hazard
F1	seldom-to-less-often and/or exposure time is short
F2	frequent-to-continuous and/or exposure time is long
P	possibility of avoiding hazard or limiting harm
P1	possible under specific conditions
P2	scarcely possible

Figure 8 – Risk Graph for estimation of required PL, reprinted from ISO 13849[3]

3 Safety System Architectures

There are several architectures used in functional safety. This chapter will discuss and compare few of the commonly used ones.

A generally used terminology in safety standards for architectures is “MooN” or “XooY”.

- M out of N, X out of Y.

Most Safety Instrumented Systems are designed to de-energize the output when a dangerous condition is detected. For the sake of simplicity, simple examples will be provided for better explaination of the different architectures. These examples will include supply voltage, switch/es and one LED. Turning off the LED when needed is assumed to be the safety function that this system provides. The main interest is/are the switch/es.

Two failure modes are possible for each switch:

1. The switch is stuck open
2. The switch is stuck closed

3.1 1oo1 Architecture

This is the simplest and minimal system configuration possible. Failure of the one and only unit will cause the whole system to fail. This system offers no fault tolerance and therefore the HFT=0. In addition, no internal diagnostics are used, and thus no failure mode protection is present.

Figure 9 illustrates a “safety system”. This setup is 1oo1 as we have only 1 switch that controls turning off the LED. Two different cases can be considered:

1. The safety function should turn off the LED and the switch is stuck open. Safe failure
2. The safety function should turn off the LED and the switch is stuck closed. Dangerous failure

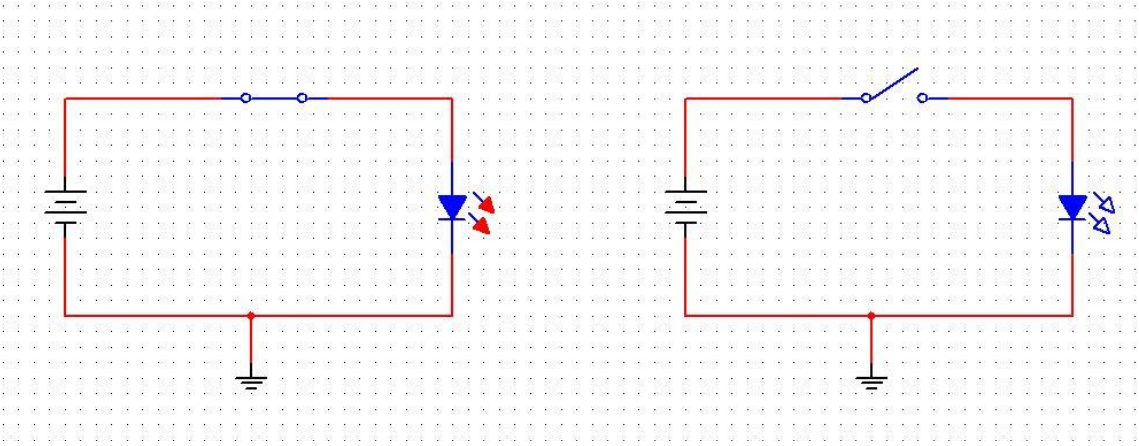


Figure 9 – 1oo1 Architecture example

3.2 1oo1d Architecture

This architecture expands the 1oo1 architecture by including a diagnostic channel. The addition of the diagnostics allows the conversion of dangerous detected failure into a safe failure [4].

3.3 1oo2 Architecture

This architecture is widely used in designs requiring redundancy, hardware fault tolerance and the output de-energized for safe state. Two separate units with ability to perform the safety function are used. Failure of one unit doesn’t result in the failure of the system and thus HFT=1. In addition, no diagnostics are used.

Figure 10 illustrates a safety system with 1oo2 architecture. Two switches in series are used with the ability of each one of them to turn off the L.E.D.

Few failure cases can be considered:

1. The safety function should turn off the LED and the 1st switch is stuck open, the 2nd switch is functioning properly.
2. The safety function should turn off the LED and the 1st switch is stuck closed, the 2nd switch B is functioning properly.
3. The safety function should turn off the LED and the 2nd switch is stuck open, the 1st switch is functioning properly.
4. The safety function should turn off the LED and the 2nd switch is stuck closed, the 1st switch is functioning properly.
5. The safety function should turn off the LED and both switches are stuck open.
6. The safety function should turn off the LED and both switches are stuck closed.

All these failures except the last failure would result in a safe failure. It can be clearly seen to reach a dangerous state, the two switches must fail and therefore the HFT=1.

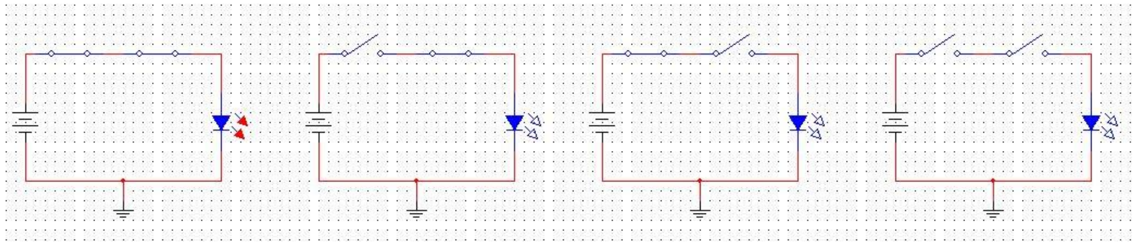


Figure 10 – 1oo2 Architecture example

3.4 1oo2d Architecture

This architecture is similar to 1oo2 architecture with additional diagnostics unit between the two channels. The diagnostics unit cross-monitors the two channels continuously. In case of a faulty channel, inequality will be detected by the diagnostic unit, which will signalize this to the faultless channel in order to achieve a fail-safe state.

If both systems fail independently due to a common cause fault, the system won’t be able to achieve safe state. For such cases, an external watchdog, temperature monitoring and voltage monitoring are used [4].

3.5 2oo2 Architecture

In this architecture two units are connected in parallel with the need of the two units to function properly for performing the safety function. This architecture doesn’t provide any hardware fault tolerance.

Figure 11 illustrates a safety system with 2oo2 architecture. The safety function needs to turn off the L.E.D and the switches are normally closed during regular operation.

Few failure cases can be considered:

1. The safety function should turn off the LED and the upper switch is stuck open, the lower switch is functioning properly. Safe failure.
2. The safety function should turn off the LED and the upper switch is stuck closed, the lower switch is functioning properly. Dangerous failure.
3. The safety function should turn off the LED and the lower switch is stuck open, the upper switch is functioning properly. Safe failure.

4. The safety function should turn off the LED and the lower switch is stuck closed, the upper switch is functioning properly. Dangerous failure.
5. The safety function should turn off the LED and both switches are stuck open. Safe failure.
6. The safety function should turn off the LED and both switches are stuck closed. Dangerous failure.

It can be clearly understood from above that in order to reach safe state both switches should be functioning properly or one switch should fail to the safe state while the other keeps functioning properly. This architecture has HFT=0.

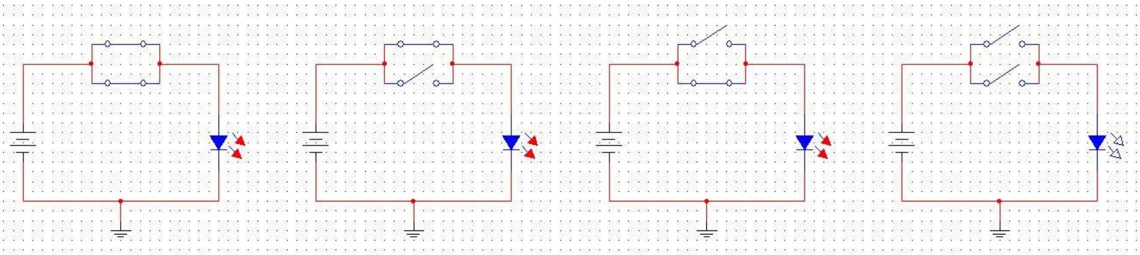


Figure 11 – 2oo2 Architecture example

3.6 2oo2d Architecture

This architecture consists of two 1oo1d subsystems connected in 2oo2 architecture. 1oo1d architecture protects against dangerous failures when the diagnostics detect the failure. Connecting two 1oo1d architectures in parallel can be used to prevent shutdowns.

3.7 Comparison and Formulas

Understanding different architectures and their capabilities is crucial during the design phase. IEC 61508 accounts for the HFT of the SIS as it plays a major role in the system ability reaching safe state in case of failure. Table 11 below lists the common architectures used. Architectures with diagnostics, don’t offer additional HFT. Voting is another commonly used term when talking about architectures. Voting simply means the number of votes needed to reach a safe state.

Table 11 – Different architectures voting and HFT

Architecture	Voting	HFT
1001	1	0
1001d	1	0
1oo2	1	1
1oo2d	1	1
2oo2	2	0
2oo2d	2	0

IEC 61508 provides different formulas for different architectures when calculating PFD$_G$ and PFH$_G$. These formulas are listed below in 2 separate tables with Table 12 providing the formulas used to calculate PFD$_G$ and Table 13 providing the formulas to calculate PFH$_G$.

Table 12 – Formulas to be used for Low Demand Mode according to IEC 61508

Architecture	Low Demand Mode
1oo1	$PFD_G = (\lambda_{DU} + \lambda_{DD}) * t_{ce}$ $t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$
1oo2	$PFD_G = 2\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$ $t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$ $t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$
1oo2D	$PFD_G = 2(1-\beta)\lambda_{DU}\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU} + \lambda_{SD}\right)t'_{CE} + t'_{GE} + \beta\lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$ $t'_{CE} = \frac{\lambda_{DU}\left(\frac{T_1}{2} + MRT\right) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}$ $t'_{GE} = \frac{T_1}{3} + MRT$
2oo2	$PFD_G = 2\lambda_D t_{CE}$ $t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$

Table 13 – Formulas to be used for Continuous Mode according to IEC 61508

Architecture	Continuous mode (High demand)
1oo1	$PFH_G = \lambda_{DU}$
1oo2	$PFH_G = 2\big((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\big)(1-\beta)\lambda_{DU}t_{CE} + \beta\lambda_{DU}$ $t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$
1oo2D	$PFH_G = 2(1-\beta_D)\lambda_{DD} + \big((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD}\big)t'_{CE} + 2(1-K)\lambda_{DD} + \beta\lambda_{DU}$ $t'_{CE} = \frac{\lambda_{DU}\left(\frac{T_1}{2} + MRT\right) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}$
2002	$PFH_G = 2\lambda_{DU}$

4 Functional Safety Functions

Safety functions are safety actions activated to avoid damage to persons, environment and material assets. Safety functions are meant to reduce risks and hazards that haven't been eliminated. As per the standards, these safety functions have minimum requirements for the reliability.

In this chapter, commonly used safety functions in the industry are presented.

Before proceeding to the safety functions, it is necessary to understand the three categories of stop functions:

- **Stop category 0:** an uncontrolled stop where power to the motor is removed immediately
- **Stop category 1:** a controlled stop where the motor has power for stopping, after which the power is removed
- **Stop category 2:** a controlled stop where the motor continues to have power. Stop category 0 and 1 definitions also apply to Emergency stop categories

4.1 Safe Torque off (STO)

This safety function is the most common function used in drives nowadays. This function cuts the power to the motor preventing it from generating torque. This function can be used to prevent an unexpected start-up as well (POUS below). It is quite common to combine STO with other safety functions. In STO stop categories 0 and 1 are used.

4.2 Safe Stop 1 (SS1)

In Safe Stop 1 (SS1) stop category 1 is applied. The drive is stopped using a quick stop ramp and following, the STO and SBC (if used) are automatically activated after a predefined time delay or a speed limit.

4.3 Safe Stop Emergency (SSE)

This safety function is mainly used for emergency stops. It can be configured to either execute STO or SS1 depending on the application and the need.

4.4 Safe Brake Control (SBC)

This safety function is mainly used with machines having an active load. The safety function provides an output signal that controls the activation of a mechanical holding brake.

4.5 Safely Limited Speed (SLS)

This safety function is used to prevent the motor from exceeding a defined speed limit. If the set speed is exceeded, the SLS safety function will activate STO or SSE.

4.6 Safe Maximum Speed (SMS)

This safety function is a variant of SLS safety function. SMS provides continuous monitoring of the maximum speed ensuring that the motor doesn’t exceed it.

4.7 Prevention of Unexpected Start-up (POUS)

This safety function prevents the machine from starting accidentally by activating the STO safety function.

4.8 Safe Speed Monitoring (SSM)

This safety function is used to provide a safe output signal indicating whether the motor is rotating in a speed range defined by the user.

4.9 Safe Direction (SDI)

This safety function monitors the rotation direction of the motor. This function activates SSE in case the motor rotates to the wrong direction exceeding the user defined SDI tolerance limit. This safety function requires the use of an encoder.

5 The PESTO Project

In the PESTO project, a new safety device (FSB-21) is developed. This device combines the functionality of the FENA-21 and some of the functionalities of FSO-12.

5.1 Ethernet Adapter Module (FENA-21)

FENA-21 is a drive option that is compatible with different ABB drives and solar inverters. It is an Ethernet adapter module that supports different communication protocols such as PROFINET and PROFIsafe over PROFINET [5].

FENA-21 adapter module can be seen in Figure 12 below.

Figure 12 – FENA-21 Ethernet adapter module

5.2 Functional Safety Option (FSO-12)

FSO-12 is a drive option that is compatible with ABB ACS880 drives. It is a safety module that has safety inputs/outputs and provides the user with several safety functions, such as: STO, SLS, SSE, SBC, SMS and POUS. FSO-12 acts as a PROFIsafe termination point as well [6].

FSO-12 safety module can be seen in Figure 13 below.

Figure 13 – FSO-12 safety module

5.3 Safety Module (FSB-21)

As mentioned earlier, the FSB-21 combines the functionality of FENA-21 and some of the functionalities of FSO-12. FSB-21 supports basic PROFINET communication and PROFIsafe over PROFINET. The FSB-21 has only one safety function, STO. FSB-21 offers a cheaper option for customers wanting to activate STO safety function over PROFIsafe while having the functionality of FENA-21.

Before the development of FSB-21, to achieve similar behaviour, FENA-21 and FSO-12 were required, resulting in a higher price solution. The FSB-21 doesn't replace FSO-12 as it provides only one safety function but it is a good and cheaper option for customers needing only STO safety function. The FSB-21 has a similar mechanical design as the FENA-21. It has a different colour and a STO connector though.

5.3.1 FSB-21 System Overview

Figure 14 presents the general structure of the system. The FSB-21 is connected to the drive (ACS380, ACS580, ACS880) using the F-option connector. This connector provides the main power to the FSB-21 (24V, 3.3V) and the communication between the drive and the module. This communication is non-safety related.

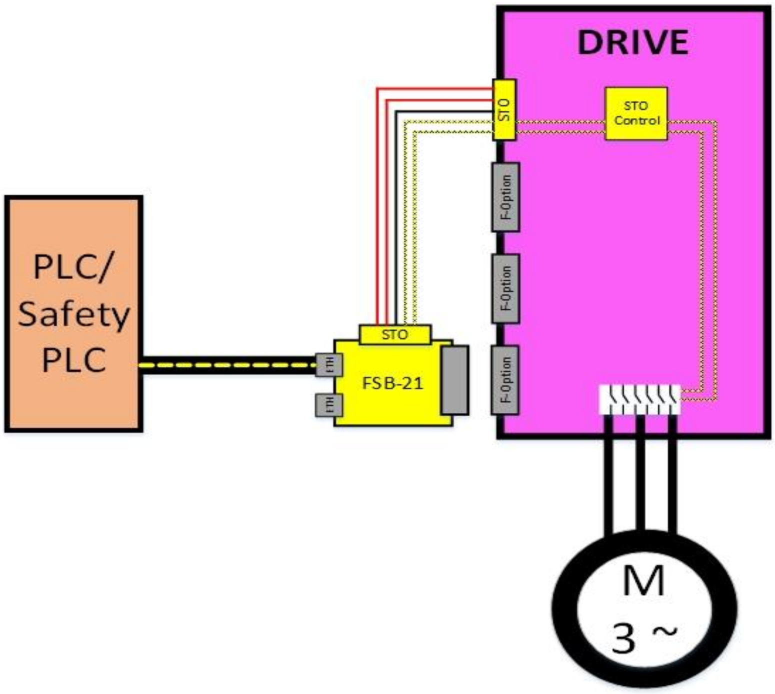


Figure 14 – FSB-21 System Overview

Additional wires are required to connect the STO connector of the module to the drive. The power to the STO circuit is provided by the drive and it is isolated on the FSB-21. Some drives use three wires for the power and others use two wires. STO control consists of two wires.

The PLC/safety PLC is connected to the FSB-21 using the Ethernet connector. The FSB-21 can be connected in a ring (as seen in Figure 15) and therefore a second Ethernet connector exists.

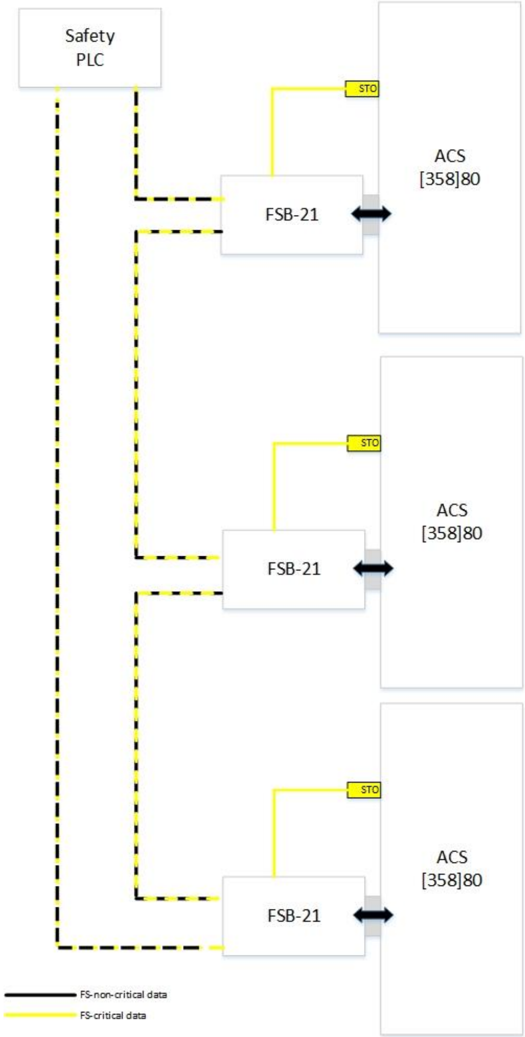


Figure 15 – FSB-21 in a Ring Connection

5.3.2 FSB-21 Electronics

Figure 16 presents a simplified block diagram of the module. The core of the FSB-21 is a safety microprocessor that has two cores running in lockstep mode. In addition to the safety microprocessor, an FPGA is used to handle the communication between the safety microprocessor and the PLC/safety PLC.

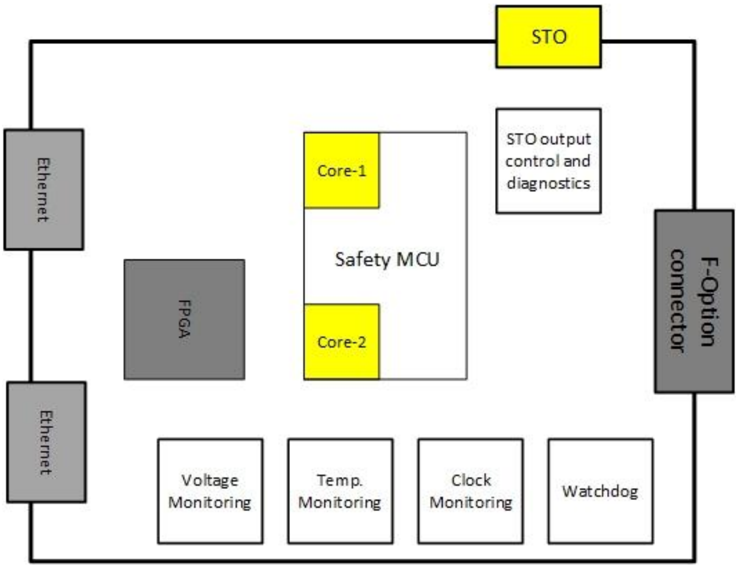


Figure 16 – FSB-21 electronics

As it is a safety module designed to perform to up to SIL3, some additional features are required, such as: voltage monitoring, temperature monitoring, clock monitoring and an external watchdog. The device has several diagnostics performed continuously to improve the diagnostic coverage of dangerous failures.

5.3.3 FSB-21 Safety Architecture

In order to describe the architecture used in FSB-21, the safety instrumented system (SIS) should be explored. Figure 17 below illustrates the SIS of the FSB-21.

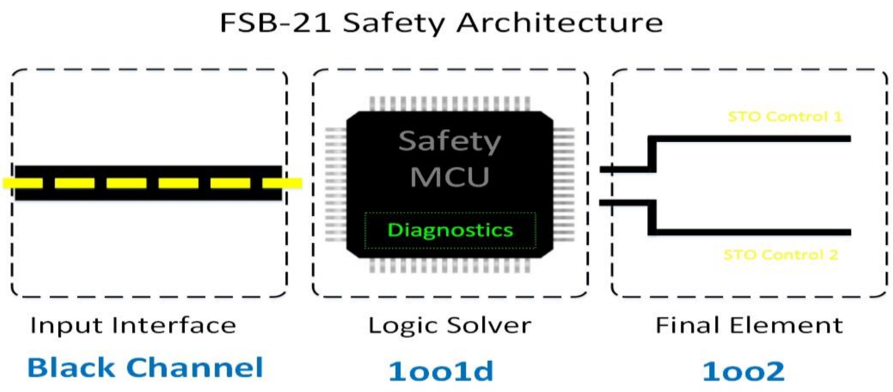


Figure 17 – FSB-21 Safety Architecture

The input interface/sensor subsystem includes the communication path between the safety PLC and the microprocessor. This communication is handled in the analysis as a black channel.

The logic subsystem includes the safety controller with 1oo1d architecture.

The final element subsystem includes the two separate channels for STO control and thus, it is 1oo2 architecture.

6 Failure Modes, Effects, and Diagnostic Analysis (FMEDA)

Failure Modes and Effects Analysis (FMEA) is a qualitative technique developed in the late 1950s by reliability engineers to study problems that might arise from malfunctions in military systems [7]. FMEA is used to identify all possible failures during the design phase of a new product. The technique addresses the failure modes, effects and analysis:
Failure modes: The possible ways of failure
Effects: The effects of each failure on the system
Analysis: Analyse the impact on the environment, people and the system

Failure Modes, Effects and Diagnostic Analysis (FEMDA) is a systematic analysis technique developed by exida engineers during the late 1980s and early 1990s. In addition to the qualitative approach of the FMEA, FMEDA added two additional pieces of information: quantitative failure data and probability of failure detection [8].

A FMEDA is widely used in functional safety as it provides means for hardware assessment to verify that the developed device meets the pre-determined safety requirements. While a FMEDA is very essential in the assessment of the safety integrity level and performance level, it is not sufficient. For full assessment, all requirements of both standards, IEC 61508 and ISO 13849, must be considered.

6.1 FMEDA Prerequisites

Performing a FMEDA for electronics device requires several items and information. The necessary items, information, and their role in the FMEDA procedure are presented below.

Schematics –

- Defining the safety related components among all components
- Understanding the functionality of each component and the system as a whole
- Understanding the effects of failures of each component on the system

Bill of materials –

- Finding the exact components types
- Finding the ratings of each component
- Finding the package type of the component

Layout –

- Determining pins orientation

PCB specifications report –

- Getting the specification of the products' PCBs that will be used later in determining PCBs failure rates

Specification of the applied diagnostics –

- Getting familiar with the applied diagnostics
- Understanding the abilities of the diagnostics

Datasheets of components –

- Getting any missing/required components ratings.

System architecture –

- Determining the hardware fault tolerance
- Determining the adequate analysis to be performed. (Is it enough to analyse 1 channel?)

Type A/ Type B, Cat., Low demand/Continuous demand mode –

- Determining the table to be followed

IEC 62380 or equivalent –

- Finding components' failure modes

Reliability data libraries –

- Getting components' failure rates

Some examples of reliability data libraries:

- Telcordia report SR332
- TUV Nord Workbench (Based on Telcordia report SR332)
- Texas Instruments Reliability Estimator
- Altera (Intel) Reliability Report
- Other manufactures reliability libraries

MTTR, MTR and Proof test interval –

- Determining required parameters to be used later in the equations

Environmental conditions –

- Determining the environmental conditions in which the device will be performing.

Standards –

- Getting guidance if needed
- Getting the necessary tables and formulas to be used and followed

In this work, IEC 61508 and ISO 13849 were followed.

Spreadsheet tool or equivalent –

- Providing an automated calculation process

In this work, ABB's Excel tool developed especially for FMEDA purposes was used.

6.2 FMEDA Procedure

A FMEDA is a systematic procedure and below are the necessary steps to perform it.

1. Reading all relevant documents from the developing process of the device, including the FMEA.
2. Understanding in depth the electronic circuitry and the products functionality.
3. Architecture, Cat., device type (Type A/Type B) and demand mode should be already known at this stage.
4. Determining the values to be used for β and β_d using the tables given in IEC 61508
5. Determining the environmental conditions in which the device will be functioning.
6. Determining all other relevant parameters such as MTR, MTTR, and proof test interval (can be changed later if needed).
7. Marking all safety-related components and pins (of the connectors) on the schematics (Schematics required). If there are redundant channels as in 1oo2 architecture, it is enough to perform the analysis for the channel with the worst probability of failure. Similar approach shall be applied for connectors' pins.
8. With the bill of materials in hand, all necessary calculation for relevant connectors and PCBs shall be performed as explained in sections 6.3.1 and 6.3.2. Connectors' datasheets, PCB specifications document/s and layout files are usually required to complete this step.
9. All safety-related components with their specifications shall be added to the excel FMEDA tool part list. If the device is built from several PCBs, separate sheets shall be used.
10. Failure modes and their probabilities for each component shall be added. Failure modes for connectors shall be performed as mentioned in section 6.3.2. IEC 62380 is a source for most of the common components.
11. FIT values shall be added for each component. For completing this work, TÜV (Technical Inspection Association) Nord workbench was mostly used. Other

sources such as Telcordia report can be used. FIT values for the connectors and PCBs are available after performing step 8.

12. Diagnostic analysis can be started at this point. Each component's failure modes shall be investigated with their effect on the whole system. The result of the failure shall be written. Each failure shall be classified whether it is safe/dangerous, detected/undetected and to provide with detection percentage (0-99%) with reasonable justification.
13. The Excel FMEDA tool calculates the values for $\Sigma\lambda_{SD}$, $\Sigma\lambda_{SU}$, $\Sigma\lambda_{DD}$, and $\Sigma\lambda_{DU}$ automatically. The calculations are rather simple.
14. Relevant equations shall be used for every part of the SIS. If the sensor/input element has architecture of 1oo1, 1oo1 equations given in IEC 61508 are to be used.
15. Results of all subsystem shall be added together to get the relevant values for the whole system
16. The achieved results shall be compared to the tables given in the standards to determine safety integrity level (SIL) according IEC 61508 and performance level (PL) according to ISO 13849.
17. The safety integrity level and PL level shall be compared to the pre-determined safety requirements.

6.3 Failures of Components

Different components fail in different ways. This section will present the factors taken into account when calculating failure rate for PCBs and connectors.

6.3.1 PCB Failure Rate

Various factors are considered when estimating the failure rate of a PCB. Board surface area, number of layers, holes, connections, tracks, track width and environmental factors are all taken into account. The technical report IEC 62380 [9] provides two formulas for calculating the failure rate of a PCB with formula A taking into account failure rates of components and connections and formula B taking into account the board itself.

Following good engineering practises, PCB failures modes are classified as shown in Table 14 below.

Table 14 – PCBs failure modes

Failure mode	Probability
Open circuit	20%
Short circuit	80%

6.3.2 Connectors Failure Rate

Several factors are taken into account when estimating the failure rate of connectors. The following formula is provided in IEC 62380 for connectors [9]:

$$\lambda = \lambda_0 \times \pi_t \times \pi_c \times \pi_M \times \pi_i \times \left(1 + 2.7 \times 10^{-3} \times \left[\sum_{i=1}^{j} (\pi_n)_i \times (\Delta T_i)^{0.68}\right]\right) \times \frac{10^{-9}}{h} \qquad (8)$$

$Where$:

λ_0 $- Connector\ type$

π_m $- Contact\ area\ material$

π_c $- Number\ of\ active\ contacts$

π_i $- Contact\ current\ intensity$

π_i $- Nominal\ current$

π_t $- Ambient\ temperature$

Connectors have two failure modes. These failures modes and their probabilities are presented in Table 15 and Table 16 below.

Table 15 – Failure modes for one-row connectors

Failure mode	Probability
Open circuit	60%
2-pins shorted	40%

Table 16 – Failure modes for two rows connectors

Failure mode	Probability
Open circuit	60%
2-pins shorted	35%
3-pins shorted	5%

6.4 FSB-21 FMEDA

FSB-21 will generally be used in continuous (high demand) mode. Due to customer requests, the safety module will be analysed also for low demand mode with 2 different proof test intervals.

As discussed earlier in 6.3.3, the sensor/signal element of the FSB-21, which provides the communication path between the safety PLC and the FSB-21, falls under the definition of black channel and therefore will be excluded from the FMEDA.

The logic solver of the FSB-21 consists of the safety MCU with 1oo1d architecture and is considered as Cat. 3. The final element consists of the STO control channels that are designed in 1oo2 architecture and is considered as Cat. 3 as well. FSB-21 is type B device as a result of the complex electronics used.

Before proceeding to FMEDA process, few parameters are defined:

- MTTR = 48 hours, the safety device is not repairable and the customer will receive a new replacement device within two days.
- MTR = 0 hours, the safety device is not repairable.
- Proof test interval, T_1 = 17520 hours (2 years), T_2 = 43800 hours (5 years). In continuous mode, T_1 is used. In low demand mode, two cases will be analysed, one with T_1 and the other with T_2.
- Environmental conditions:
    - Ambient temperature: t_A = 40 °C
    - Temperature variation amplitude: t_{ae} = 45 °C, t_{ac} = 85 °C (used for connectors and PCBs)

Now that the basic parameters have been defined, the FMEDA process can be started.

6.4.1 FSB-21 β and $β_D$

To determine the values to be used for β and $β_D$, the tables given in IEC 61508-6 are used. In Appendix 1, the argumentation for the values determined can be found.

The achieved values are:

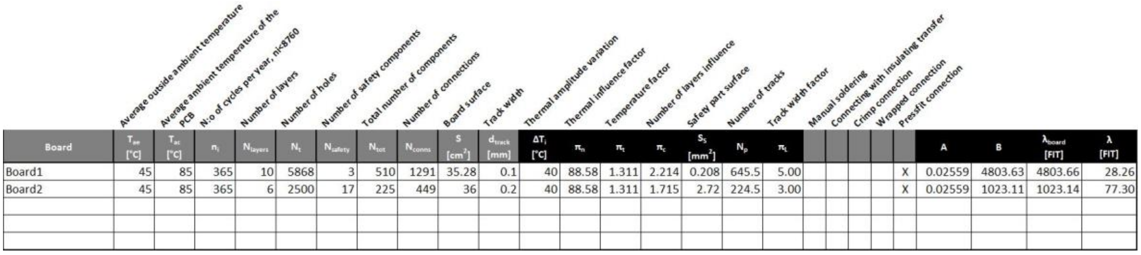
β = 5%

β_D = 2%

6.4.2 FSB-21 Printed Circuit Boards (PCBs)

FSB-21 is constructed from 2 PCBs assembled on top of each other with several connections between them. The upper PCB has the safety MCU (logic solver) and is treated as 1oo1d architecture. The lower PCB has the STO control electronics and is treated as 1oo2 architecture.

Figure 18 below shows the parameters taken into account when calculating the failure rate of PCBs as well as the achieved failure rate (in FIT). These calculations were performed using ABB Excel FMEDA tool.



	Average outside ambient temperature	Average ambient temperature of the PCB	N:o of cycles per year, ni<8760	Number of layers	Number of holes	Number of safety components	Total number of components	Number of connections	Board surface	Track width	Thermal amplitude variation	Thermal influence factor	Temperature factor	Number of layers influence	Safety part surface	Number of tracks	Track width factor	Manual soldering	Connecting with insulating transfer	Crimp connection	Wrapped connection	Pressfit connection				
Board	T_{ae} [°C]	T_{ac} [°C]	n_i	N_{layers}	N_t	N_{safety}	N_{tot}	N_{conns}	S [cm^2]	d_{track} [mm]	ΔT_i [°C]	π_n	π_t	π_c	S_S [mm^2]	N_p	π_L						A	B	λ_{board} [FIT]	λ [FIT]
Board1	45	85	365	10	5868	3	510	1291	35.28	0.1	40	88.58	1.311	2.214	0.208	645.5	5.00					X	0.02559	4803.63	4803.66	28.26
Board2	45	85	365	6	2500	17	225	449	36	0.2	40	88.58	1.311	1.715	2.72	224.5	3.00					X	0.02559	1023.11	1023.14	77.30

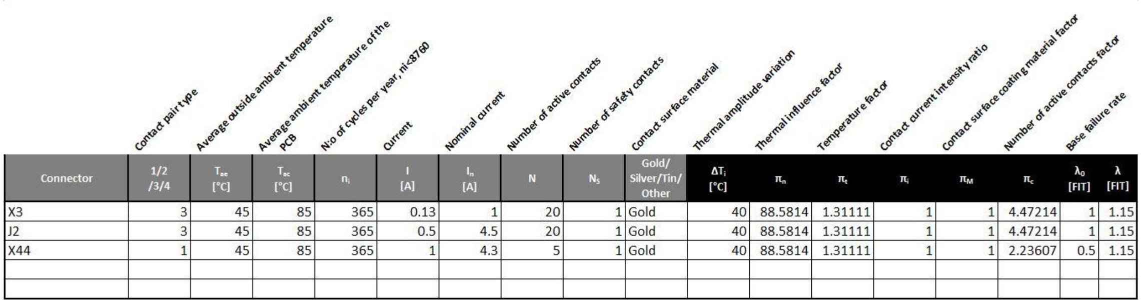
Figure 18 – PCBs calculations performed in ABB Excel FMEDA tool

6.4.3 FSB-21 Connectors

The FSB-21 has six connectors from which three are safety related and will be taken into account in the FMEDA. Two connectors are used to connect the PCBs together (male and female connectors) and one connector for the STO output.

All these connectors have only one safety related pin per analysed channel, which is used for the STO control. There are two channels for the STO control, and the channel with the greater probability of failures will be used in the analysis.

Figure 19 below shows the connectors’ parameters used in performing the calculations as well as the achieved failures rates (in FIT). These calculations were performed using ABB Excel FMEDA tool.

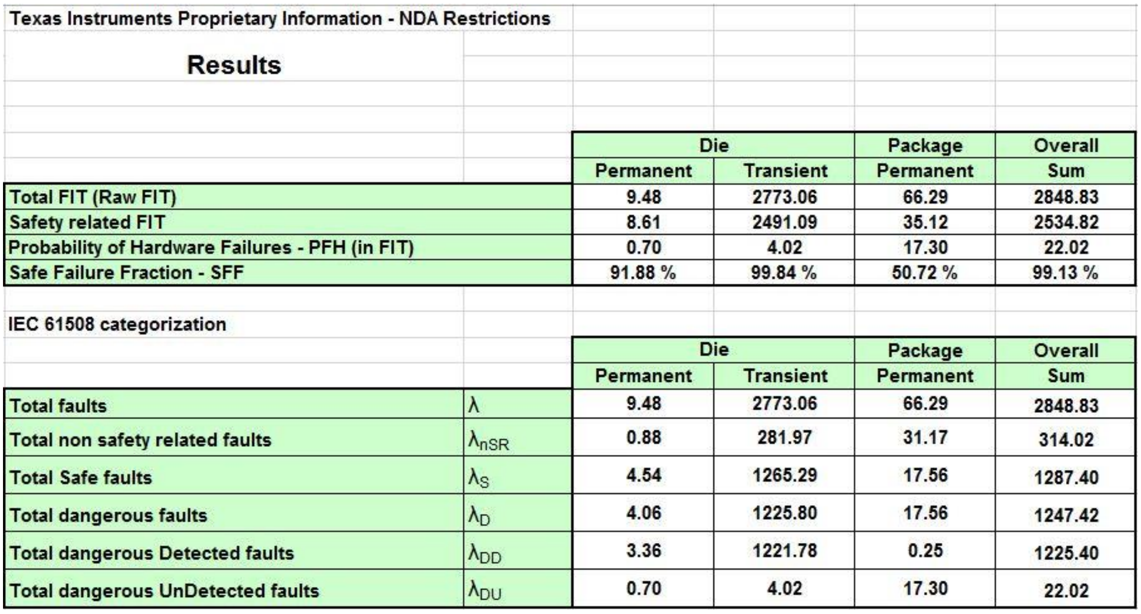


	Contact pair type	Average outside ambient temperature	Average ambient temperature of the PCB	N:o of cycles per year, ni<8760	Current	Nominal current	Number of active contacts	Number of safety contacts	Contact surface material	Thermal amplitude variation	Thermal influence factor	Temperature factor	Contact current intensity ratio	Contact surface coating material factor	Number of active contacts factor	Base failure rate	
Connector	1/2 /3/4	T_{ae} [°C]	T_{ac} [°C]	n_i	I [A]	I_n [A]	N	N_S	Gold/ Silver/Tin/ Other	ΔT_i [°C]	π_n	π_t	π_i	π_M	π_c	λ_0 [FIT]	λ [FIT]
X3	3	45	85	365	0.13	1	20	1	Gold	40	88.5814	1.31111	1	1	4.47214	1	1.15
J2	3	45	85	365	0.5	4.5	20	1	Gold	40	88.5814	1.31111	1	1	4.47214	1	1.15
X44	1	45	85	365	1	4.3	5	1	Gold	40	88.5814	1.31111	1	1	2.23607	0.5	1.15

Figure 19 – Connecters' parameters used in the ABB Excel FMEDA tool

6.4.4 FSB-21 Logic Solver

The safety MCU used in FSB-21 was analysed using the tool provided by Texas Instruments for this specific MCU. This tool aids exceptionally in the FMEDA process. Final results achieved using the tool can be seen in Figure 20 below.



Texas Instruments Proprietary Information - NDA Restrictions

Results

	Die		Package	Overall
	Permanent	Transient	Permanent	Sum
Total FIT (Raw FIT)	9.48	2773.06	66.29	2848.83
Safety related FIT	8.61	2491.09	35.12	2534.82
Probability of Hardware Failures - PFH (in FIT)	0.70	4.02	17.30	22.02
Safe Failure Fraction - SFF	91.88 %	99.84 %	50.72 %	99.13 %

IEC 61508 categorization

		Die		Package	Overall
		Permanent	Transient	Permanent	Sum
Total faults	λ	9.48	2773.06	66.29	2848.83
Total non safety related faults	λ_{nSR}	0.88	281.97	31.17	314.02
Total Safe faults	λ_S	4.54	1265.29	17.56	1287.40
Total dangerous faults	λ_D	4.06	1225.80	17.56	1247.42
Total dangerous Detected faults	λ_{DD}	3.36	1221.78	0.25	1225.40
Total dangerous UnDetected faults	λ_{DU}	0.70	4.02	17.30	22.02

Figure 20 – FMEDA results for the safety MCU using Texas Instruments FMEDA tool

6.4.5 FSB-21 Final Element

The Final Element on the FSB-21 consists of two channels used for STO control. As it is 2 channels architecture, it is enough to analyse only one channel. The schematic in Figure 21 below shows all safety related components taken into account. In Appendix 2, failure rates and modes for the final element are shown.

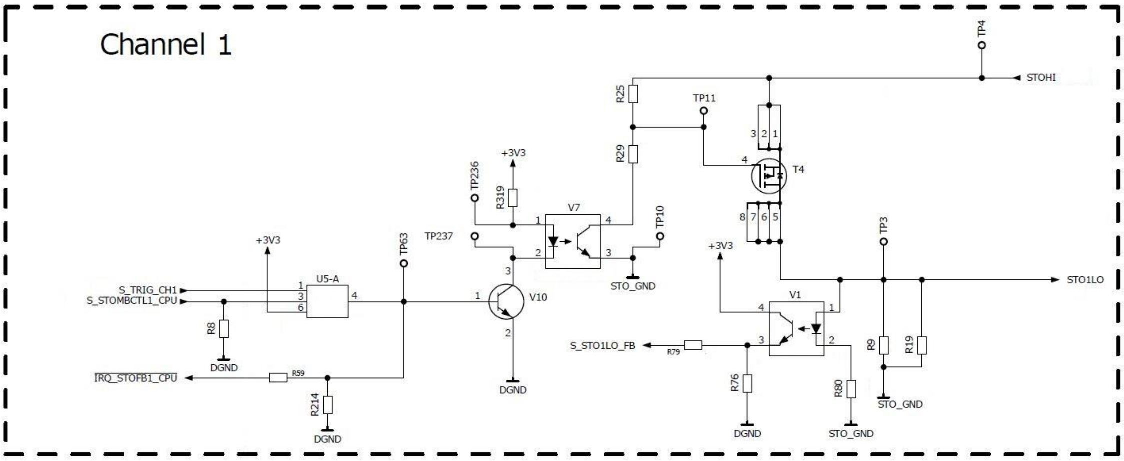


Figure 21 – STO Control Circuit

6.5 Fault Insertion Test

To verify the results achieved in the FMEDA, fault insertion test has to be carried out. In fault insertion, all dangerous failures are normally tested. In addition, some random safe failures are tested as well as some other components that might be applicable to test.

In the fault insertion test, the failures are injected to the device under test and the consequences are observed.

In addition to validating the results achieved in the FMEDA, fault insertion can validate the implemented diagnostic tests and the independence between safety-related and non-safety-related components.

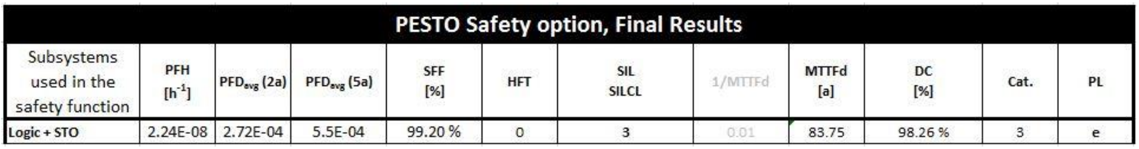
In order to perform fault insertion, the device shall be near finished, as the safety FW is required for the diagnostics of the faults. Due to this, fault insertion testing is out of the scope of this work.

7 Results and Conclusion

During the design phase of a safety product, Failure Modes and Effects Analysis (FMEA) procedure is performed to determine safety requirements and to help designers understand possible failures to be avoided by good engineering practices. When the design phase is completed, Failure Modes, Effects, and Diagnostic Analysis (FMEDA) procedure is performed. FMEDA validates the conformance of the implementation with regards to the design goals. Exact probabilities of different failures are an outcome of the FMEDA. Fault insertion test validates the results achieved in the FMEDA.

FMEDA is a systematic process and the complexity lies in understanding and interpreting the standards to be followed, which in this work were IEC 61508 and ISO 13849.

The goal of this work was to perform Failure Modes, Effects, and Diagnostic Analysis for the FSB-21. The FMEDA process for FSB-21 was performed successfully and the results are shown in Figure 22 below.



PESTO Safety option, Final Results

Subsystems used in the safety function	PFH [h^{-1}]	PFD_{avg} (2a)	PFD_{avg} (5a)	SFF [%]	HFT	SIL SILCL	1/MTTFd	MTTFd [a]	DC [%]	Cat.	PL
Logic + STO	2.24E-08	2.72E-04	5.5E-04	99.20 %	0	3	0.01	83.75	98.26 %	3	e

Figure 22 – FSB-21 FMEDA final results

As can be seen from Figure 22, the safety module achieved PFD_{avg} = 2.27E-4 with 2 years proof test interval and PFD_{avg} = 5.5E-4 with 5 years test interval. Neither of these results prevents the module from achieving SIL 3 according to IEC 61508. PFH = 2.24E-8 with 2 years proof test interval and SFF=99.2% giving the module SIL 3 according to IEC 61508. The safety module can be used in both low and continuous (high demand) modes with safety integrity level up to 3.

It can be seen as well that DC = 98.26% and $MTTF_D$ = 83.75 years and therefore the safety module is capable of achieving PL e according to ISO 13849 from the safety reliability perspective.

To sum up, the safety module met the pre-determined safety requirements that were assigned during the design phase and further improvements will be made as a result of the FMEDA.

References

1 William M. Goble. Control Systems Safety Evaluation and Reliability. 3rd edition. Ottsville, PA; 2010.

2 International Electrotechnical Commission (IEC). Standard IEC 61508:2010 2nd edition. Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems.

3 International Organization for Standardization (ISO). Standard ISO 13849:2015. Safety of machinery – Safety-related parts of control systems.

4 Deterministic Systems, Inc (DSi). DSi Control Systems Architecture Design [online]. http://dsicontrols.com/architecture.html. Accessed 3 May 2017.

5 ABB. FENA-01/-11/-21 Ethernet adapter module User's manual [online], 2016. URL: https://inverterdrive.com/file/ABB-FENA-01-11-21-Ehternet-Adapter-User-Manual. Accessed 3 May 2017.

6 ABB. FSO-21 safety function module User's manual [online], 2016. URL: https://library.e.abb.com/public/40ae84f29a4745e0a68241c26cf11779/EN_FSO_21_UM_C_A5.pdf. Accessed 3 May 2017.

7 Wikipedia. Failure mode and effect analysis [online], 2017. URL: https://en.wikipedia.org/wiki/Failure_mode_and_effects_analysis. Accessed 3 May 2017.

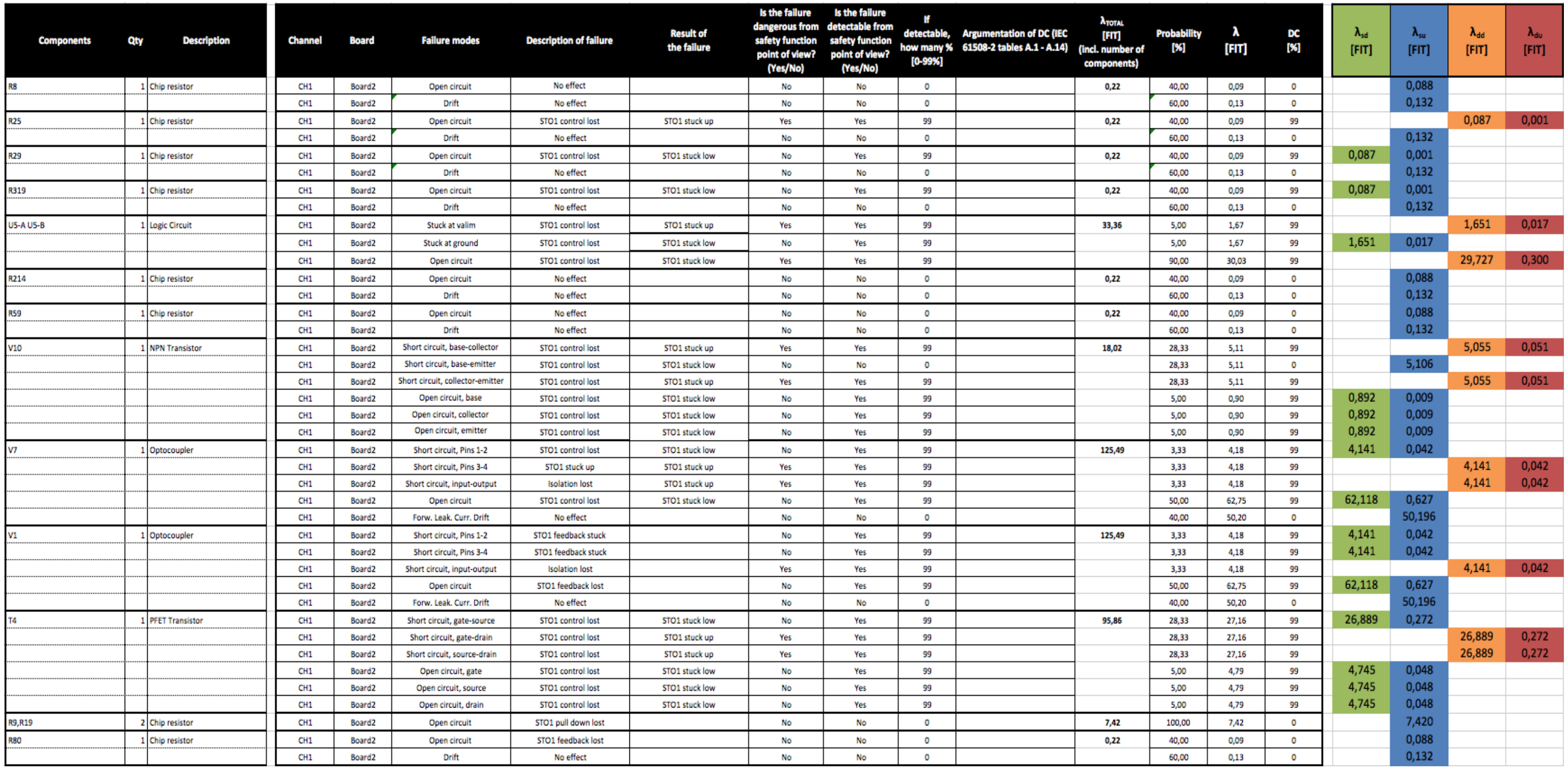
8 Wikipedia. Failure modes, effects, and diagnostic analysis [online], 2016. URL: https://en.wikipedia.org/wiki/Failure_modes,_effects,_and_diagnostic_analysis. Accessed 3 May 2017.

9 International Electrotechnical Commission (IEC). Standard IEC 62380:2004 1st edition. Reliability data handbook – Universal model for reliability prediction of electronic components, PCBs and equipment.

Argumentation for β and β_D Factors

Item	Logic subsystem		Sensors and final elements	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
Separation/segregation				
Are all signal cables for the channels routed separately at all positions?	1,5	1,5	1,0	2,0
Are the logic subsystem channels on separate printed-circuit boards?	3,0	1,0		
Are the logic subsystems physically separated in an effective manner? For example, in separate cabinets.	2,5	0,5		
If the sensors/final elements have dedicated control electronics, is the electronics for each channel on separate printed-circuit boards?			2,5	1,5
If the sensors/final elements have dedicated control electronics, is the electronics for each channel indoors and in separate cabinets?			2,5	0,5
Diversity/redundancy				
Do the channels employ different electrical technologies for example, one electronic or programmable electronic and the other relay?	8,0			
Do the channels employ different electrical technologies for example, one electronic, the other programmable electronic?	6,0			
Do the devices employ different physical principles for the sensing elements for example, pressure and temperature, vane anemometer and Doppler transducer, etc?			9,0	
Do the devices employ different electrical principles/designs for example, digital and analogue, different manufacturer (not re-badged) or different technology?			6,5	
Is low diversity used, for example hardware diagnostic tests using the same technology?	2,0	1,0		
Is medium diversity used, for example hardware diagnostic tests using different technology?	3,0	2,0		
Were the channels designed by different designers with no communication between them during the design activities?	1,5	1,5		
Are separate test methods and people used for each channel during commissioning?	1,0	0,5	1,0	2,0
Is maintenance on each channel carried out by different people at different times?	3,0		3,0	
Complexity/design/application/maturity/experience				
Does cross-connection between channels preclude the exchange of any information other than that used for diagnostic testing or voting purposes?	0,5	0,5	0,5	0,5
Is the design based on techniques used in equipment that has been used successfully in the field for > 5 years?	0,5	1,0	1,0	1,0
Is there more than 5 years experience with the same hardware used in similar environments?	1,0	1,5	1,5	1,5
Is the system simple, for example no more than 10 inputs or outputs per channel?		1,0		
Are the inputs and outputs protected from potential levels of over-voltage and over-current?	1,5	0,5	1,5	0,5
Are all devices/components conservatively rated (for example, by a factor of 2 or more)?	2,0		2,0	
Assessment/analysis and feedback of data				
Have the results of the failure modes and effects analysis or fault-tree analysis been examined to establish sources of common cause failure and have predetermined sources of common cause failure been eliminated by design?		3,0		3,0
Were common cause failures considered in design reviews with the result fed back into the design? (Documentary evidence of the design review activity is required.)		3,0		3,0
Are all field failures fully analyzed with the feedback into the design? (Documentary evidence of the procedure is required.)	0,5	3,5	0,5	3,5
Procedures/human interface				
Is there a written system of work to ensure that all component failures (or degradations) are detected, the root causes established and other similar items inspected for similar potential causes of failure?		1,5	0,5	1,5
Are procedures in place to ensure that: maintenace (including adjustment or calibration) of any part of the independent channels is staggered, and, in addition to the manual checks carried out following maintenance, the diagnostic tests are allowed to run satisfactorily between the completion of the maintenance on one channel and the start of maintenance on another?	1,5	0,5	2,0	1,0
Do the documented maintenance procedures specify that all parts of redundant systems (for example, cables, etc.) intended to be independent of each other, are not to be relocated?	0,5	0,5	0,5	0,5
Is all maintenance of printed-circuit boards, etc. carried out off-site at a qualified repair centre and have all the repaired items gone through a full pre-installation testing?	0,5	1,0	0,5	1,5
Does the system have low diagnostic coverage (60% to 90%) and report failures to the level of a field-replaceable module?	0,5			
Does the system have medium diagnostic coverage (90% to 99%) and report failures to the level of a field-replaceable module?	1,5	1,0		
Does the system have high diagnostic coverage (>99%) and report failures to the level of a field-replaceable module?	2,5	1,5		
Do the system diagnostic tests repor failures to the level of a field-replaceable module?			1,0	1,0
Competence/training/safety culture				
Have designers been trained (with training documentation) to understand the causes and consequences of common cause failures?	2,0	3,0	2,0	3,0
Have maintainers been trained (with training documentation) to understand the causes and consequences of common cause failures?	0,5	4,5	0,5	4,5
Environmental control				
Is personnel access limited (for example locked cabinets, inaccessible position)?	0,5	2,5	0,5	2,5
Is the system likely to operate always within the range of the temperature, humidity, corrosion, dust, vibration, etc., over which it has been tested, without the use of external environmental control?	3,0	1,0	3,0	1,0
Are all signal and power cables separate at all positions?	2,0	1,0	2,0	1,0
Environmental testing				
Has the system been tested for immunity to all relevant environmental influences (for example EMC, temperature, vibration, shock, humidity) to an appropriate level as specified in recognized standarts?	10,0	10,0	10,0	10,0

Failure rates and modes for FSB-21 Final Element



Components	Qty	Description	Channel	Board	Failure modes	Description of failure	Result of the failure	Is the failure dangerous from safety function point of view? (Yes/No)	Is the failure detectable from safety function point of view? (Yes/No)	If detectable, how many % [0-99%]	Argumentation of DC (IEC 61508-2 tables A.1 - A.14)	λ_{TOTAL} [FIT] (incl. number of components)	Probability [%]	λ [FIT]	DC [%]	λ_{sd} [FIT]	λ_{su} [FIT]	λ_{dd} [FIT]	λ_{du} [FIT]
R8	1	Chip resistor	CH1	Board2	Open circuit	No effect		No	No	0		**0,22**	40,00	0,09	0		0,088		
			CH1	Board2	Drift	No effect		No	No	0			60,00	0,13	0		0,132		
R25	1	Chip resistor	CH1	Board2	Open circuit	STO1 control lost	STO1 stuck up	Yes	Yes	99		**0,22**	40,00	0,09	99			0,087	0,001
			CH1	Board2	Drift	No effect		No	No	0			60,00	0,13	0		0,132		
R29	1	Chip resistor	CH1	Board2	Open circuit	STO1 control lost	STO1 stuck low	No	Yes	99		**0,22**	40,00	0,09	99	0,087	0,001		
			CH1	Board2	Drift	No effect		No	No	0			60,00	0,13	0		0,132		
R319	1	Chip resistor	CH1	Board2	Open circuit	STO1 control lost	STO1 stuck low	No	Yes	99		**0,22**	40,00	0,09	99	0,087	0,001		
			CH1	Board2	Drift	No effect		No	No	0			60,00	0,13	0		0,132		
U5-A U5-B	1	Logic Circuit	CH1	Board2	Stuck at valim	STO1 control lost	STO1 stuck up	Yes	Yes	99		**33,36**	5,00	1,67	99			1,651	0,017
			CH1	Board2	Stuck at ground	STO1 control lost	STO1 stuck low	No	Yes	99			5,00	1,67	99	1,651	0,017		
			CH1	Board2	Open circuit	STO1 control lost	STO1 stuck low	Yes	Yes	99			90,00	30,03	99			29,727	0,300
R214	1	Chip resistor	CH1	Board2	Open circuit	No effect		No	No	0		**0,22**	40,00	0,09	0		0,088		
			CH1	Board2	Drift	No effect		No	No	0			60,00	0,13	0		0,132		
R59	1	Chip resistor	CH1	Board2	Open circuit	No effect		No	No	0		**0,22**	40,00	0,09	0		0,088		
			CH1	Board2	Drift	No effect		No	No	0			60,00	0,13	0		0,132		
V10	1	NPN Transistor	CH1	Board2	Short circuit, base-collector	STO1 control lost	STO1 stuck up	Yes	Yes	99		**18,02**	28,33	5,11	99			5,055	0,051
			CH1	Board2	Short circuit, base-emitter	STO1 control lost	STO1 stuck low	No	No	0			28,33	5,11	0		5,106		
			CH1	Board2	Short circuit, collector-emitter	STO1 control lost	STO1 stuck up	Yes	Yes	99			28,33	5,11	99			5,055	0,051
			CH1	Board2	Open circuit, base	STO1 control lost	STO1 stuck low	No	Yes	99			5,00	0,90	99	0,892	0,009		
			CH1	Board2	Open circuit, collector	STO1 control lost	STO1 stuck low	No	Yes	99			5,00	0,90	99	0,892	0,009		
			CH1	Board2	Open circuit, emitter	STO1 control lost	STO1 stuck low	No	Yes	99			5,00	0,90	99	0,892	0,009		
V7	1	Optocoupler	CH1	Board2	Short circuit, Pins 1-2	STO1 control lost	STO1 stuck low	No	Yes	99		**125,49**	3,33	4,18	99	4,141	0,042		
			CH1	Board2	Short circuit, Pins 3-4	STO1 stuck up	STO1 stuck up	Yes	Yes	99			3,33	4,18	99			4,141	0,042
			CH1	Board2	Short circuit, input-output	Isolation lost	STO1 stuck up	Yes	Yes	99			3,33	4,18	99			4,141	0,042
			CH1	Board2	Open circuit	STO1 control lost	STO1 stuck low	No	Yes	99			50,00	62,75	99	62,118	0,627		
			CH1	Board2	Forw. Leak. Curr. Drift	No effect		No	No	0			40,00	50,20	0		50,196		
V1	1	Optocoupler	CH1	Board2	Short circuit, Pins 1-2	STO1 feedback stuck		No	Yes	99		**125,49**	3,33	4,18	99	4,141	0,042		
			CH1	Board2	Short circuit, Pins 3-4	STO1 feedback stuck		No	Yes	99			3,33	4,18	99	4,141	0,042		
			CH1	Board2	Short circuit, input-output	Isolation lost		Yes	Yes	99			3,33	4,18	99			4,141	0,042
			CH1	Board2	Open circuit	STO1 feedback lost		No	Yes	99			50,00	62,75	99	62,118	0,627		
			CH1	Board2	Forw. Leak. Curr. Drift	No effect		No	No	0			40,00	50,20	0		50,196		
T4	1	PFET Transistor	CH1	Board2	Short circuit, gate-source	STO1 control lost	STO1 stuck low	No	Yes	99		**95,86**	28,33	27,16	99	26,889	0,272		
			CH1	Board2	Short circuit, gate-drain	STO1 control lost	STO1 stuck up	Yes	Yes	99			28,33	27,16	99			26,889	0,272
			CH1	Board2	Short circuit, source-drain	STO1 control lost	STO1 stuck up	Yes	Yes	99			28,33	27,16	99			26,889	0,272
			CH1	Board2	Open circuit, gate	STO1 control lost	STO1 stuck low	No	Yes	99			5,00	4,79	99	4,745	0,048		
			CH1	Board2	Open circuit, source	STO1 control lost	STO1 stuck low	No	Yes	99			5,00	4,79	99	4,745	0,048		
			CH1	Board2	Open circuit, drain	STO1 control lost	STO1 stuck low	No	Yes	99			5,00	4,79	99	4,745	0,048		
R9,R19	2	Chip resistor	CH1	Board2	Open circuit	STO1 pull down lost		No	No	0		**7,42**	100,00	7,42	0		7,420		
R80	1	Chip resistor	CH1	Board2	Open circuit	STO1 feedback lost		No	No	0		**0,22**	40,00	0,09	0		0,088		
			CH1	Board2	Drift	No effect		No	No	0			60,00	0,13	0		0,132		