



Risk assessment of a practical environment and
develop of a station using openSAFETY technology

Thesis

TO ACHIEVE THE ACADEMIC DEGREE OF

Master in Mechatronics

BY

Salvador Jiménez Juárez

Santiago de Queretaro, Qro., Mexico, February 2017

Declaration of Authorship

I hereby declare that the following thesis submitted is my own work. No other person's work has been used without due acknowledgement in this thesis. All direct or indirect sources used are acknowledged as references.

This work has not been previously published or presented to another examination board before.

Aachen February 2017

Salvador Jiménez Juárez

Acknowledgment

I would like to take this to express my thanks to Prof. Dr.-Ing. Jörg Wollert for the knowledge and motivation I received during my thesis. With his expertise and guidance this work reaches a good end.

To all my Mexican friends, the new people that I met during my residence in Germany, thanks for being part of this journey and for the moments that we share. A particular gratitude to CONACyT for giving me the resources to study in Germany, to the people of CIDESI and the FH Aachen for given me the opportunity to be part of this program.

Finally a very special and deep thanks to my family; my parents and my sisters who always have been there for me, because without their support and understanding I wouldn't be able to reach this goal.

List of abbreviations

CCF	Common Cause Failure
CE	Communauté Européenne “European Conformity”
DC	Diagnostic Coverage
DIN	Deutsches Institut für Normung “German Institute for Standardization”
DPH	Degree of Possible Harm
EN	Euro Norm
FE	Frequency of Exposure
HRN	Hazard Rating Number
HSE	Health Survey for England
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
LO	Likelihood of Occurrence
MTTF _d	Mean Time to Dangerous Failure
NP	Number of Persons at risks
PFH _D	Probability of (dangerous) Failure per Hour
PL	Performance Level
PL _r	Performance Level Required
SIL	Safety Integrity Level
SISTEMA	Safety Integrity Software Tool for the Evaluation of Machine Applications
SRCF	Safety related control functions
T _M	Mission Time
TOR	Tolerability of Risk

Abstract

One of the most efficient ways to avoid hazards is to do it in the design phase; for that, a risk analysis should be made in order to evaluate the risks exposure to hazards. The EN ISO 12100 is a standard that specifies basic terminology, principles and methodology to achieve safety in the design of machinery. It specifies the principles of risks assessment and risk reduction to help designer to identify risk during the design stage of machine production to complete a safe design. The correct use of this guidelines will lead to a machine which fulfil all the safety requirements that are demanded in their application area. Once a machine is ready to hit the market, the manufacturer must declare that all directives that apply to the product have been considered, affirming in that way that their product is safe. The CE Marking on a product is a manufacture's declaration that the product complies with the essential requirements of the relevant European health, safety and environmental protection legislation. The "CE" stands for "Communauté Européenne" which literally means "European Conformity". In the European Union only safe system are implemented in the market, this is why all the products have the CE Marking also referred to as the "Passport to Europe".

All the previous concepts and standards are well known by the big companies however for small companies and educational environments these safety concepts are not so clear, thus the aim of this master's thesis is to introduce basic safety concepts into the educational environment, these concept will be introduced gradually by following the design's guideline of the EN ISO 12100. The work carried out in this Thesis acts a base to understand the basic concepts of risk assessment in the design process of a machine and must be developed and improved further to incorporate additional safety sensors and additional features to make the demonstrator more user friendly and functional.

Content

Chapter 1 Introduction.....	1
1.1 Problem statement	2
1.2 Justification	3
1.3 Objective	4
1.4 Hypothesis.....	4
1.5 Methodology.....	4
Chapter 2 State of the Art.....	5
2.1 IEC.....	5
2.2 DIN EN ISO 12100.....	5
2.3 Safety Integrity Level and Performance Level.....	10
2.4 EN 62061 Risk Assessment.....	13
2.5 Risk Quantification	16
2.6 EN ISO 13849-1 Risk Assessment	18
2.6 Safety Best Practices	22
2.6.1 Emergency stop shutdown to SIL 1 or PLC with a 3SK1 safety relay.....	22
2.6.2 Protective door monitoring to SIL 1 or PLC with a 3SK1 safety relay.....	23
2.6.3 Access monitoring using a light curtain to SIL 3 or PLe with a safety relay	24
Chapter 3 Design Process	25
3.1 Machine design	25
3.2 Element design.....	26
3.3 Previous considerations for the design.....	27
3.4 Hardware description.....	27
3.4.1 Power panel 4PP65.0571-P74 (PLC).....	27
3.4.2 Module X20IF10A1-1.....	28
3.4.3 Module X20BC1083.....	28
3.4.4 Module X20PS9400	29
3.4.5 Module X20AI4622.....	29
3.4.6 Module X20AO4632	29
3.4.7 Module X20DM9324	30
3.4.8 Module X20SM1426.....	30
3.4.9 Module X20 BT9400	31

3.4.10 Module X20 SL8001.....	31
3.4.11 Module X20 SI 4100	32
3.4.12 Module X20 SO 4110.....	32
3.4.13 E- stop button (Pull to release)	32
3.4.14 Standard (22 mm) start button	33
3.4.15 Standard (22 mm) reset button	33
3.4.16 Conveyor Belt	33
3.4.17 OY801S Light Curtain.....	33
3.5 Software description	34
3.5.1 Automation Studio	34
3.5.2 SISTEMA Safety tool	35
3.5.3 Autodesk Inventor.....	35
Chapter 4 Risk Assessment of the design.....	36
4.1 Early designs.....	36
4.2 Final design:.....	38
4.3 Static Analysis of the structure	39
4.4 Safety distance for the light curtains	41
4.5 Design and calculation for the safeguards.....	43
4.6 Safety-Related System	46
4.6.1 openSAFETY.....	46
4.6.2 Enabling principles	46
4.7 SISTEMA validation process	48
Chapter 5 Conclusion and future work.....	49
5.1 Conclusions.....	49
5.2 Future work.....	49
References	50
Appendix	52

List of figures

Figure 1 Comprehensive view of injuries in EU-27 by injury prevention domain [5].	3
Figure 2 Risk assessment according to EN ISO 12100 [18].	6
Figure 3 Recommended application of IEC 62061 & ISO 13849-1 [15].	12
Figure 4 Tolerability and acceptability of risk [9].	16
Figure 5 The tolerability of risk summary [9].	17
Figure 6 Graphical Representation of the tolerability risk summary [9].	17
Figure 7 Risk estimation to calculate the PLr [1].	18
Figure 8 Categories system behaviour according to ISO 13849-1 [15].	20
Figure 9 The relationship between categories, the DC, MTTFd for each channel and PL [1].	21
Figure 10 Emergency stop shutdown to SIL 1 or PLc with a 3SK1 safety relay [16].	22
Figure 11 Safety- related component of the emergency stop shutdown [16].	22
Figure 12 Protective door monitoring to SIL 1 or PLc with a 3SK1 safety relay [16].	23
Figure 13 Safety related components for protective door monitoring to SIL 1 [16].	23
Figure 14 Access monitoring using a light curtain to SIL 3 or PLe with a safety relay [16].	24
Figure 15 Safety related components for Access monitoring using a light curtain to SIL 3 [16].	24
Figure 16 Design Process [3].	25
Figure 17 Basic Procedure of design of machine elements [3].	26
Figure 18 Power panel 4PP65.0571-P74 [2].	27
Figure 19 Module X20IF10A1-1 & X20BC1083 [2].	28
Figure 20 Modules X20PS9400, X20AI4622 & X20AO4632 [2].	29
Figure 21 Modules X20DM9324, X20SM1426 & BT9400 [2].	30
Figure 22 Safety Module X20 SL8001 [2].	31
Figure 23 Safety modules X20 SI4100 & X20 SO4110 [2].	32
Figure 24 Conveyor belt for the safety demonstrator.	33
Figure 25 Automation Studio Workspace.	34
Figure 26 SISTEMA software workspace.	35
Figure 27 First design of the safety demonstrator.	36
Figure 28 Revision 2 of the safety demonstrator.	37
Figure 29 Final design of the safety demonstrator.	38

Figure 30 Displacement of the structure after load.....	39
Figure 31 Selection of the type of safeguard [18].....	43
Figure 32 Design of the safeguards.	44
Figure 33 Displacement on the safeguards after load of 200 N.....	45
Figure 34 Connection of a "Direct" enabling principle on automation studio.....	46
Figure 35 Connection of a "Via SafeLOGIC" enabling principle on automation studio.....	47
Figure 36 Category selected (SISTEMA tool).....	48
Figure 37 Level of PL required for the safety demonstrator.	48

List of tables

Table 1 Risk level values	7
Table 2 Likelihood of occurrence (LO).....	8
Table 3 Frequency of exposure (FE).....	8
Table 4 Degree of possible harm (DPH).....	9
Table 5 Equivalent factor of number of person exposed to the hazard.....	9
Table 6 Relationship between the performance level (PL) and the Safety Integrity Level (SIL).....	11
Table 7 Severity classification (Se).....	13
Table 8 Frequency and duration of exposure classification (Fr)	14
Table 9 Probability classification (Pr)	14
Table 10 Probability of avoiding or limiting harm classification (Av)	15
Table 11 SIL assignment matrix.....	15
Table 12 Corresponding average PFHD according to SIL level.....	15
Table 13 Relationship between PL & PFHD	19
Table 14 Reliability levels of components.....	20
Table 15 Diagnostic Coverage	21
Table 16 Result summary of the static analysis.....	40
Table 17 Hazard identification for the installation of safeguards.	44
Table 18 Displacement of the safeguards applying a force of 200 N	45

Chapter 1 Introduction

In order to regulate all the electric, electronic, mechanical or hydraulic devices, the International Electrotechnical Commission (IEC) was founded in 1906. The IEC is the world's leading organization that prepares and published international Standards for all electrical, electronic and related technologies [10]. Every safe work related protocol and new technology must accomplish its standards. Nowadays there is a variety of standards for different designs, machines, devices, etc. This standards are in constant revisions to match the emergent technologies which like any other technology already established needs a standard to regulate the new features.

The current work is intended to design a safety demonstrator according to the methodology described in the EN ISO 12100. The evaluation of the design and the calculation of safety distances are discussed along with the results.

The outline of this work is as follows: Chapter 2 focuses in provides the fundamentals definitions related to safety and a short description of the standards necessary to identify safety levels, it also establishes the basics for a better understanding of the Chapter 4. Chapter 3 describes pieces of hardware that needs to be taken into consideration for the design and also gives a short description of the software used for the programming of some motion functions. In Chapter 4 all the previous concepts are applied for the risk assessment of the design of the demonstrator. Finally in Chapter 5 the conclusions are presented along with a small explanation of the future work.

1.1 Problem statement

In the academic and research area, the theoretical knowledge is usually complemented with practical training, allowing in that way an integral education. Engineering involves practical application of the knowledge of science, this is why practical laboratories in engineering departments are very common.

Although several educational institutes have laboratories with demonstrators that emulates production lines or automation system, which its main goal is to illustrate how this kind of process works, unfortunately this kind of demonstrators doesn't have all the safety devices available on the real system, when in reality the safety measures are a fundamental part in the design procedure of every machine and process.

Unfortunately in the educational environment there is not enough material that illustrate the importance of the safety measures, this is mostly due to the fact that safety topics take on consideration several standards, procedures and methodologies that are in some cases rigorous due to the fact that the process or the machine involves some kind of human interaction, the level of safety depends of several factors like the time of exposure to the hazard, the severity of the injury that could cause or the Possibility of avoiding the hazard, the combination of these factors will lead to a final safety level.

1.2 Justification

According to the European Association for injury Prevention and Safety Promotion, between 2008 and 2010 a total of 32 000 accidents in school environments required hospital admissions and a total of 1 250 fatalities [5]. The same association reported that a total of 38 000 accidents and 1 154 fatalities occurred by the years of 2010 – 2012, this represent a reduction of 8% of the fatalities [6].

	Road traffic	Work-place	School	Sports	Home, leisure	Total of unintentional injuries	Homicide, assault	Suicide, self-harm	Total of all injuries
Fatalities	38 119 16%	4 961 2%	1 250 1%	7 000 3%	98 891 42%	150 221 65%	4 704 2%	57 614 25%	232 869 100%
Hospital admissions	668 000 12%	252 000 4%	32 000 1%	419 000 7%	3 914 000 69%	5 285 000 93%	202 000 4%	213 000 4%	5 700 000 100%
Hospital outpatients	3 524 000 10%	3 553 000 10%	792 000 2%	5 644 000 17%	18 951 000 56%	32 465 000 96%	1 231 000 4%	205 000 1%	33 900 000 100%
All hospital patients	4 192 000 11%	3 805 000 9%	824 000 2%	6 063 000 14%	22 865 000 59%	37 750 000 95%	1 433 000 4%	418 000 1%	39 600 000 100%

Source: WHO – mortality database, WHO – Health for All database, Eurostat – hospital discharge statistics, EU IDB. See Annex “List of figures and tables” for more details.

Figure 1 Comprehensive view of injuries in EU-27 by injury prevention domain [5].

In occupational safety and health, professionals use a framework called the “hierarchy of controls” to select a ways of dealing with workplace hazards. This hierarchy prioritizes intervention strategies based on the premise that the best way to control a hazard is to systematically remove it from the workplace, rather than relying on workers to reduce their exposure [12].

The most effective measure to reduce hazards is the so call “Engineering controls”, this control involve making changes to the workplace to reduce work related hazards. The target of implementing a safety protocol in the lab is to make fixed changes to the work station in order to reduce the exposure to hazards. One of the main goals of the laboratories is to provide a safe learning environment for both, instructors and students, of course this goal cannot be achieve without performing a risk analysis. This is only a little display that the matter of safety is always a matter of interest of the industry, the educational sector and the government, who’s always investing in the development of new technology.

1.3 Objective

Design a safety demonstrator following the specifications dictated in the standard EN ISO 12100, accomplishing the principles of risk assessment and risk reduction to achieve the PL_r for the demonstrator.

1.4 Hypothesis

The elimination of hazard or sufficient risk reduction during the important phases of the machine life cycle will lead to a design that fulfil the requirements needed for the construction of the demonstrator.

1.5 Methodology

An already stablished engineering design methodology will be followed during the design process [4]; however a suggest risk reduction methodology will be also taking into account during the design process, the main steps to follow are:

- Research: Detection of information on the existing literature, best practices and available solutions.
- Design requirements: Define the basic characteristics of the design like the main function, specification, etc.
- Conceptualization: Generation of ideas and possible alternatives.
- Preliminary designs: elaboration of CAD schematics and layouts of the ideas presented in the conceptualization phase.
- Risk assessment: The identification of the hazards and its respectively risks reduction is necessary before the selection of the final design.
- Detailed design: Specifications and detail drawing of the final design.

Chapter 2 State of the Art

2.1 IEC

The International Electrotechnical Commission (IEC) is a non-for profit quasi-governmental organization. The IEC is the world's leading organization that prepares and published international Standards for all electrical, electronic and related technologies. Is one of the three global sister organizations (IEC, ISO, ITU) that develop International Standards for the world, it also cooperates with ISO (International Organization for Standardization) or ITU (International Telecommunication Union) to ensure that International Standards fir together seamlessly and complement each other. It was founded in 1906 and nowadays close to 20 000 experts from industry, commerce, government, test and research labs, academia and consumer groups participate in IEC Standardization work.

2.2 DIN EN ISO 12100

This international standard provides specific guidelines to designers for risk assessment and mitigation process; it also specifies the basic terminology, principles and methodology established to constructing safe machinery.

The concept of machine safety considers the ability of a machine to maintain its intended function during their lifetime, thereby reducing the risk sufficiently.

“This international standard forms the basis for a series of standards which has the following structure:

- **Type A standards** (basic safety standards) give basic concepts, principles for design and general aspects that can be applied to machines.
- **Type B standards** (generic safety standards) dealing with one safety aspect or one type of Protective equipment that can be used for a wide range of machines:
 - **Type B1 standards** for specific safety aspects (eg. safety distances, Temperature, noise).
 - **Type B2 standards** for protective devices (eg. two-hand circuits, locking devices, Pressure sensitive protective devices, separate protective devices).

- **Type-C standards** (machinery safety standards) dealing with detailed safety requirements for a certain machine or group of machines.

This International Standard is a Type A standard. If a Type C standard differs from one or more specifications set out in this International Standard or in a Type B standard, then the Type C standard takes precedence”. [7]

The chapter 4 of the standard is based on the strategy for risk assessment and risk reduction. The **risk assessment** is a series of logical steps, which the systematic analysis and allow evaluation of risks caused by the machinery. Where necessary, the risks assessment is followed by risk reduction. The iteration of this process can be necessary to eliminate hazards or reduced it to an adequate level.

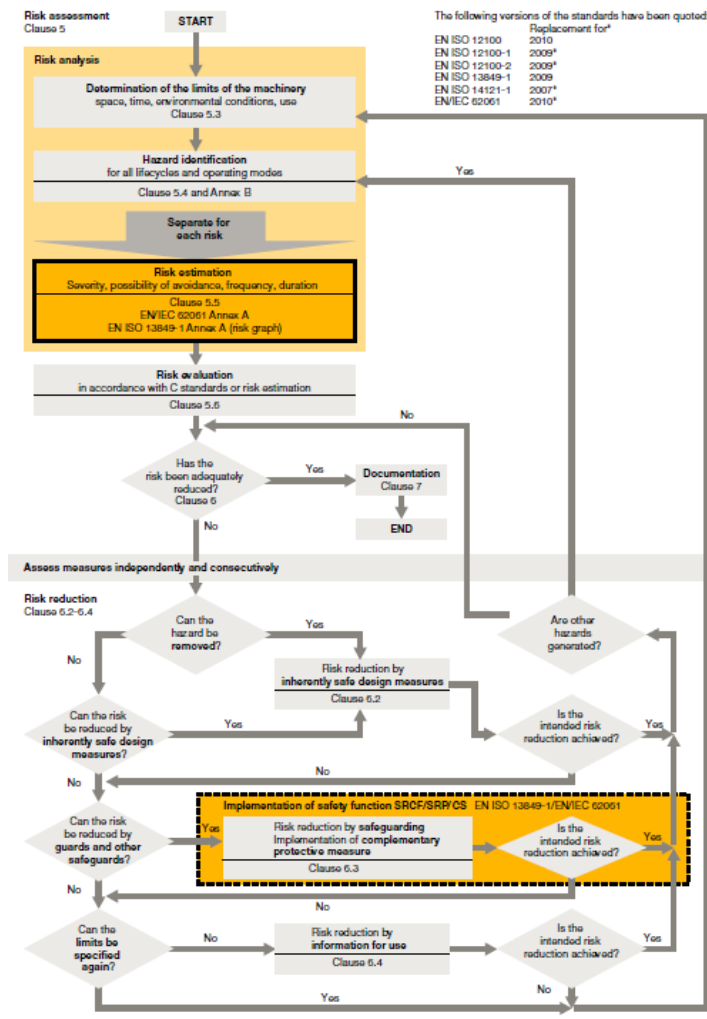


Figure 2 Risk assessment according to EN ISO 12100 [18].

It suggests that the designer must follow the steps below to perform a risk assessment and risk reduction.

- a) Establish the limits of the machine and the foreseeable misuse;
- b) Identification of the hazards and his associated hazardous situations;
- c) Estimate the risk for each identified hazard and hazardous situation;
- d) Evaluate the risk and make decision in order to make the risk reduction;
- e) Eliminate or reduce the risk.

The steps a) to d) are clearly related to the risk assessment process and the step e) at risk reduction.

The objective of the process is to achieve the greatest risk reduction by taking into account the four specific factors.

- Safety of the machine in all phases of its life;
- Ability of the machine to perform its function;
- Ease of use of the machine;
- Manufacturing, operating and disassembly cost of the machine.

Protective measures that can be made during the design phase are preferable to those which are made by the user.

According to [17] the **risk assessment** is linked to 4 factors: Likelihood of occurrence (LO), Frequency of exposure (FE), Degree of possible harm (DPH) and the numbers of persons at risk (NP). The risk level is calculated according to the next formula:

$$\text{Risk level} = LO * FE * DPH * NP$$

The Risk level is measured in 4 different levels shown in the Table 1, it is preferable that the risk level remains between 0-5 (Negligible level).

Risk level	
Negligible	0-5
Low but significant	5-50
High	50-500
Unacceptable	500+

Table 1 Risk level values

Likelihood of occurrence (LO)

Is how possible is to get in contact with some of the hazards.

Likelihood of occurrence (LO)		
Almost impossible	Possible only under extreme circumstances	0.033
Highly unlikely	Though conceivable	1
Unlikely	But could occur	1.5
Possible	But unusual	2
Even chance	Could happen	5
Probable	Not surprising	8
Likely	Only to be expected	10
Certain	No doubt	15

Table 2 Likelihood of occurrence (LO).

Frequency of exposure (FE)

This factors is linked to the amount of time that a person expend close to the hazard.

Frequency of exposure to the hazard (FE)	
Annually	0.5
Monthly	1
Weekly	1.5
Daily	2.5
Hourly	4
Constantly	5

Table 3 Frequency of exposure (FE)

Degree of possible harm (DPH)

Measures how severe is the damage, for this factor is recommended to take the worst possible harm into consideration.

Degree of possible harm (DPH), taking into account the worst possible case	
Scratch/bruise	0.1
Laceration/mild ill-effect	0.5
Break minor bone or minor illness (temporary)	2
Break major bone or major illness (temporary)	4
Loss of one limb, eye, hearing loss (permanent)	6
Loss of two limbs, eyes, (permanent)	10
Fatality	15

Table 4 Degree of possible harm (DPH)

Number of person exposed to the hazard (NP)

The factor provides an equivalent number of person at risk.

Number of persons exposed to the hazard (NP)	
1-2 persons	1
3-7 persons	2
8-15 persons	4
16-50 persons	8
50+ persons	12

Table 5 Equivalent factor of number of person exposed to the hazard.

Once all the factors are well identified, the Risk level can be calculated easily, if this value is greater than 5, then a risk assessment must take place in order to reduce the value to a negligible level.

Overall, ISO 12100 is a type A standard that can be applied to everything that is defined as a machine under the European Machine Directive, it also provides the risk manager framework for machinery by defining the principles of how to do the risk management for machinery.

2.3 Safety Integrity Level and Performance Level

In every machine or process it is necessary to have a safety standard who can deal with safety-related problems, does not matter if is electrical, mechanical, pneumatic, etc. Nowadays there are mainly two standards the EN ISO 13849-1 and the EN 62061, each one of them have different approaches, therefore the implementation depends on the demands of the costumer, the technology used and the complexity of the functionality.

In order to avoid confusion or misunderstanding and have a full comprehension of the following section, some terms needs to be define, for that some basic definition were taken from the EN 1200-1:2003:

Harm: physical injury or damage to health.

Hazard: potential source of harm.

Risk: combination of the probability of occurrence of harm and the severity of that harm.

Risk assessment: overall process comprising a risk analysis and a risk evaluation.

[10] Defines **safety** as the freedom from unacceptable risk of physical injury or of damage to the health of people, either directly or indirectly as a result of damage to property or to the environment.

Functional safety is the part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.

The two standards use the terminology “functional safety” to define the safety requirements base on the functional requirements. EN 62061 uses Safety Integrity Levels (SIL) and EN ISO 13849-1 uses Performance Levels (PL).

Both standards require the user to follow the same sequence of steps:

1. - Assess the Risks
2. - Allocate the Safety measures
3. - Design the Architecture
4. - Validate

Even though every standard make their own recommendations for the risk assessment, the outcome must be similar for every function. Both standards produce the same result, but use different methods; however there is one critical distinction: EN 62061 is limited to electrical system. EN ISO 13849-1 can be applied to pneumatic, mechanical, hydraulic and electrical system, this difference will be analyse in the following sections of this chapter.

Given that both standards classifies necessary safety levels in different discrete levels. As such, for simplification, the relationship between SIL and PL is suggested in the table below.

PL	SIL	Probability of dangerous failures per hour PFH _D [1/h]
a	No correspondence	$\geq 10^{-5}$ to $< 10^{-4}$
b	1	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$
c	1	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$
d	2	$\geq 10^{-7}$ to $< 10^{-6}$
e	3	$\geq 10^{-8}$ to $< 10^{-7}$

Table 6 Relationship between the performance level (PL) and the Safety Integrity Level (SIL)

[15] Resumes in the figure 3 the recommended application in both standards (ISO 13849-1 & IEC 62061).

Recommended application of IEC 62061 and ISO 13849-1			
Annex	Technology implementing the safety related control function (S)	ISO 13849-1	IEC 62061
A	Non electrical, e.g. hydraulics	X	Not covered
B	Electromechanical, e.g. relays, or non-complex electronics	Restricted to designated architectures (see Note 1) and up to PL=e	All architectures and up to SIL 3
C	Complex electronics, e.g. programmable	Restricted to designated architectures (see Note 1) and up to PL=d	All architectures and up to SIL 3
D	A combined with B	Restricted to designated architectures (see Note 1) and up to PL=e	X see Note 3
E	C combined with B	Restricted to designated architectures (see Note 1) and up to PL=d	All architectures and up to SIL 3
F	C combined with A, or C combined with A and B	X see Note 2	X see Note 3
<p>"X" indicates that this item is dealt with by the standard shown in the column heading.</p> <p>Note 1 Designated architecture are defined in Annex B of EN/ISO 13849-1 to give a simplified approach for qualification of performance level</p> <p>Note 2 For complex electronics: use of designated architecture according to EN/ISO 13849-1 up to PL=d or any architecture according to EN/IEC 62061</p> <p>Note 3 For non-electrical technology use parts according to EN/ISO 13849-1 as subsystems.</p>			

Figure 3 Recommended application of IEC 62061 & ISO 13849-1 [15].

2.4 EN 62061 Risk Assessment

The EN 62061 addresses the issue of risk assessment using a quantitative table. It also deals with the validation of safety functions based on statistical methods. The risks under this standard are estimated under the following points:

- Severity of injury (Se)
- Frequency and duration of exposure (Fr)
- Probability of occurrence of a hazardous event (Pr)
- Probability of avoiding or limiting harm (Av)

Severity of Injuries (Se)

The severity of injuries or the damage to health can be easily classify by taking into account the reversible and irreversible injuries.

Impact	Severity (Se)
Irreversible: death, losing an eye or arm	4
Irreversible: broken limb(s), losing a finger(s)	3
Reversible: requiring attention from a medical practitioner	2
Reversible: requiring first aid	1

Table 7 Severity classification (Se)

Frequency and duration of exposure (Fr)

The level of exposure is linked to the need to access the hazardous zone (normal operation, maintenance, etc.) and the type of access. With these two parameters it must be possible to estimate the average of exposure and its duration.

Frequency of exposure	Duration (Fr) > 10 m*
≤ 1 h	5
> 1h to ≤ 1 day	5
> 1 day to ≤ 2 weeks	4
> 2 weeks to ≤ 1 year	3
> 1 year	2

Table 8 Frequency and duration of exposure classification (Fr)

*If the duration is less than 10 min, the value can be rounded down to the next level.

Probability of occurrence of a hazardous event (Pr)

For the detection of the Pr two basic concepts must be taking into account:

- Predictability of the dangerous components in the various parts of the machine and its various operating modes (normal, troubleshooting, etc.), giving particular consideration to unexpected restarting.
- Behaviour of the person interacting with the machine: Fatigue, inexperience, stress, etc.

Probability of occurrence	Probability (Pr)
Very high	5
Likely	4
Possible	3
Rarely	2
Negligible	1

Table 9 Probability classification (Pr)

Probability of avoiding or limiting harm (Av)

This parameter take into account the suddenness of the occurrence of the hazardous event, the nature of the dangerous component (temperature, electrical, cutting) and the possibility for a person to identify a hazardous phenomenon.

Probability of avoiding or limiting harm	Avoiding and limiting (Av)
Impossible	5
Rarely	3
Probable	1

Table 10 Probability of avoiding or limiting harm classification (Av)

When the values all the above parameters have been detected, the SIL can be identified; the SIL is determined by the following table. The class (CI) is calculated as follows:

$$CI = Fr + Pr + Av$$

Severity (Se)	Class (CI) 3-4	Class (CI) 5-7	Class (CI) 8-11	Class (CI) 11-13	Class (CI) 14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)*	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

Table 11 SIL assignment matrix

* OM = other measures

PFH_d

Another important aspect is the probability of a dangerous failure of each safety-related control function (SRCF) as a result of a dangerous random hardware failures. The following table shows the permissible values corresponding to each SIL levels.

SIL level (EN 62061)	Average PFH _D [1/h]
SIL 3	$\geq 10^{-8}$ to 10^{-7}
SIL 2	$\geq 10^{-7}$ to 10^{-6}
SIL 1	$\geq 10^{-6}$ to 10^{-5}

Table 12 Corresponding average PFHD according to SIL level

2.5 Risk Quantification

According to [13] the quantification of the tolerability of risks to personal safety depends on how risks are perceived; this perception is related to several factors which can be included:

- Personal experience;
- Social or cultural background and beliefs;
- The degree of control on has over a particular risks;
- The extent to which information is gained from different sources.

[9] Proposes that an individual risks of death of one in a million, per year, for both employees and member of the public corresponds to a very low level of risks and should be used as the broadly acceptable risk boundary.

Related to this topic the Health Survey for England (HSE) also suggest that an individual risks of death of 1in 1000 per annum should represent the boundary condition between what is acceptable for a substantial category of workers during most of their working lives. This criteria can be demonstrated in a framework known as the tolerability of risk (TOR).

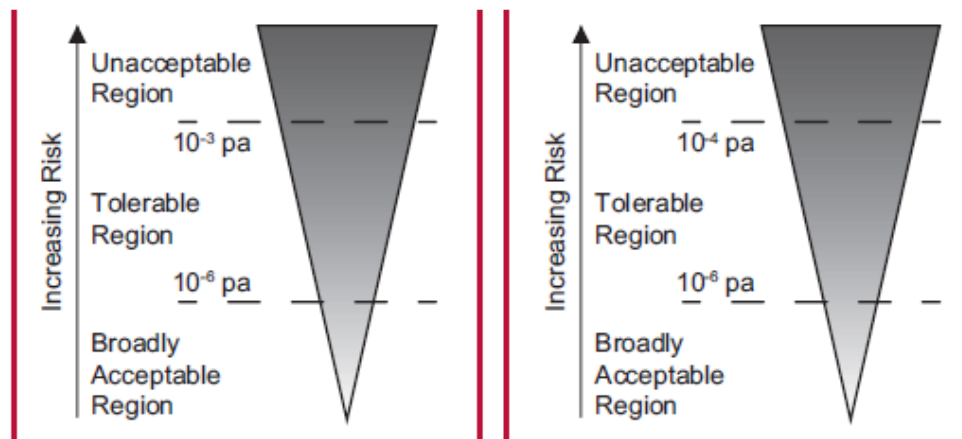


Figure 4 Tolerability and acceptability of risk [9].

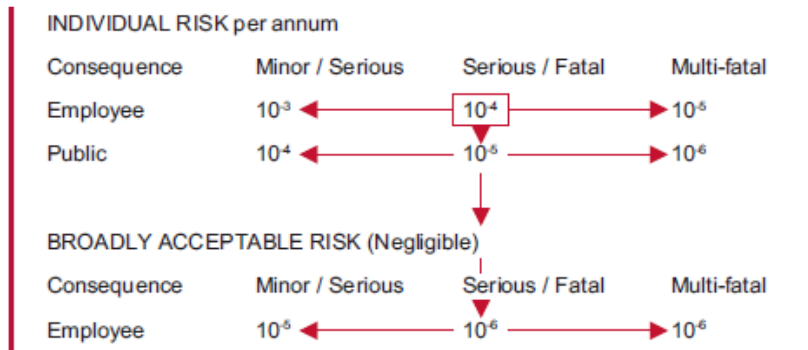


Figure 5 The tolerability of risk summary [9].

The tolerability of risk summary (Figure 5) can be represented graphically as shown in Figure 6.

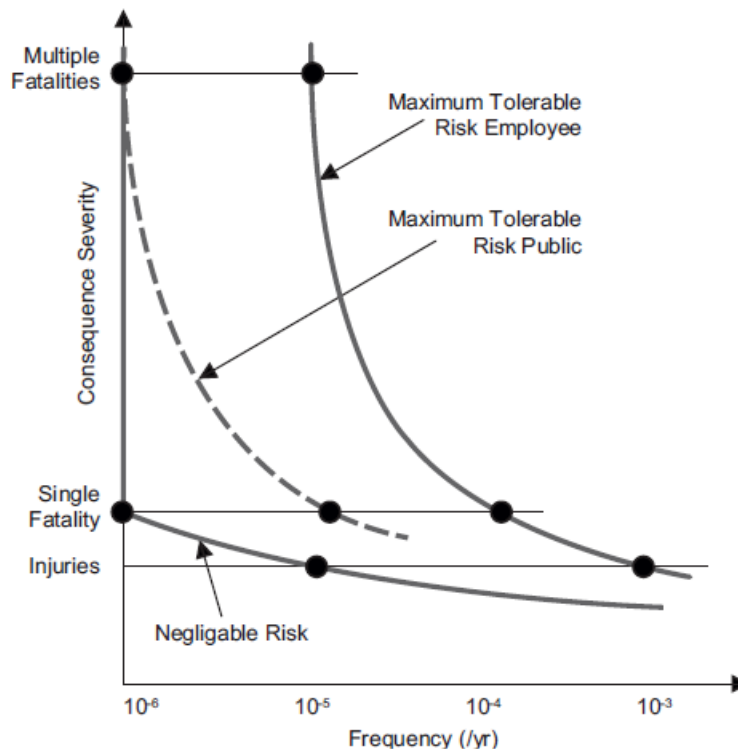


Figure 6 Graphical Representation of the tolerability risk summary [9].

2.6 EN ISO 13849-1 Risk Assessment

The EN ISO 13849-1 illustrate the risk assessment in the form of a qualitative risk graph. Even though the overall process is a based on a probabilistic approach, this method provide a guidance to help with the correct choices of parameters. These parameters are intended to overcome these drawbacks.

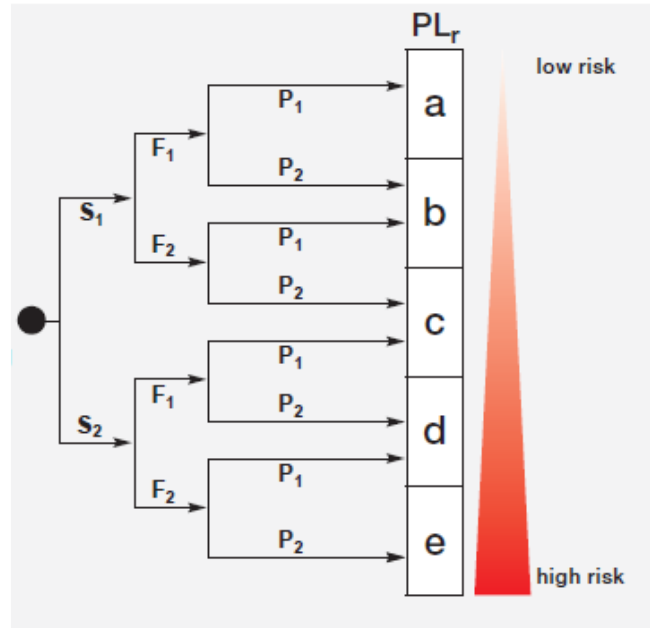


Figure 7 Risk estimation to calculate the PLr [1].

For the analysis of this method, only 3 parameters needs to be examined:

Severity of injury:

S₁: Slight (normally reversible injury)

S₂: Serious (normally irreversible injury or death)

Frequency and/ or exposure time to hazard

F₁: Seldom to less often and/ or the exposure time is short

F₂: Frequent to continuous and/or the exposure time is long

Possibility of avoiding the hazard or limiting the harm

P₁: Possible under specific conditions

P₂: Scarcely possible

Performance level required PL_r

The output of the risk graph specify a require performance level (PL_r). This level is represented by a letter from “a” to “e”. The EN ISO 13849-1 also defines the performance levels in terms of the average probability of a dangerous failure per hour (PFH_D).

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


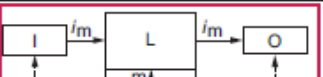
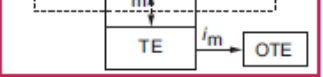
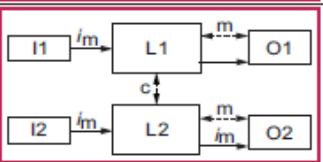
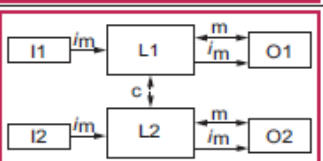
Table 13 Relationship between PL & PFH_D

Even though the PL_r can be estimated following the paths on the Figure 7, the designer can reach the same result with an estimation of several factors such as:

- Hardware and software of the system structure (Categories)
- Mechanism of failures, diagnostic coverage (DC)
- Components reliability, Mean time to dangerous failure (MTTF_d)
- Common Cause Failure (CCF)

Categories

The ISO 13849-1 designated some architectures, if one of these architectures is used, performance level can be calculated using the recommended methodology.

Cat.	System behaviour	Designated architectures
B	A fault can lead to loss of the safety function	
1	As for category B but the probability of this occurrence is lower than for the category B	
2	A fault can lead to loss of the safety function between two periodic inspections and loss of the safety function is detected by the control system at the next test.	
3	For a single fault, the safety function is always ensured. Only some faults will be detected. The accumulation of undetected faults can lead to loss of the safety function.	
4	When faults occur, the safety function is always ensured. Faults will be detected in time to prevent loss of the safety function	

Key:

<i>im</i> : Interconnecting means	<i>m</i> : Monitoring
<i>c</i> : Cross monitoring	O, O1, O2: Output device, e.g. main contactor
I, I1, I2: Input device, e.g. sensor	TE: Test equipment
L, L1, L2: Logic	OTE: Output of TE

Figure 8 Categories system behaviour according to ISO 13849-1 [15].

Mean time to dangerous failure $MTTF_d$

The value of the $MTTF_d$ of each channel is given in 3 levels and shall be taking into account for each channel individually.

Index	Range
Low	$3 \text{ years} \leq MTTF_d < 10 \text{ years}$
Medium	$10 \text{ years} \leq MTTF_d < 30 \text{ years}$
High	$30 \text{ years} \leq MTTF_d < 100 \text{ years}$

Table 14 Reliability levels of components

Diagnostic coverage DC

The DC is the term used to express as a percentage the ability to diagnose a dangerous failure.

Denotation	Range
Nil	$DC < 60\%$
Low	$60\% \leq DC < 90\%$
Medium	$90\% \leq DC < 99\%$
High	$99\% \leq DC$

Table 15 Diagnostic Coverage

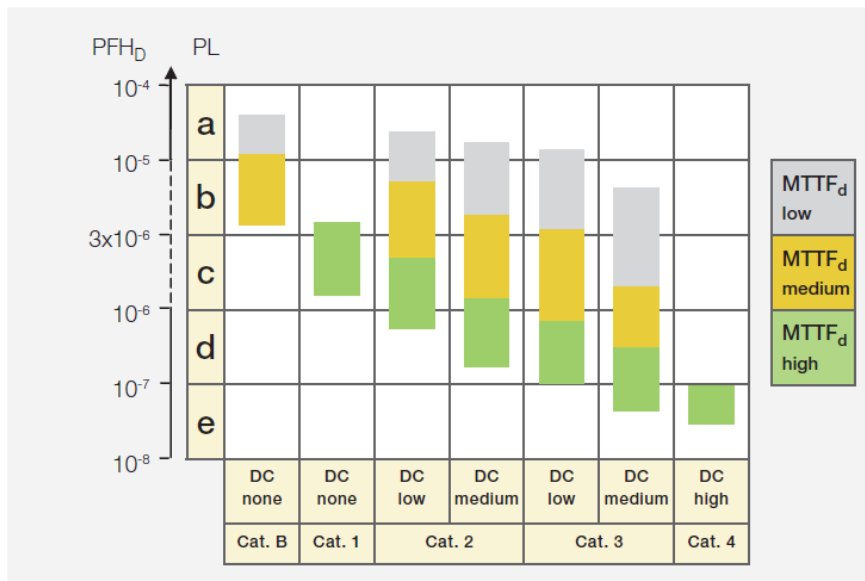


Figure 9 The relationship between categories, the DC, MTTF_d for each channel and PL [1].

By using the chart above (Figure 9) the designer/ tester can select the most appropriate architecture, the required Diagnostic Coverage as well as ensure that all the products selected for the application have the right MTTF_d values.

2.6 Safety Best Practices

Some companies illustrated the safety functions to an understandable way to his costumers, the following section present some of the most common safety functions [16].

2.6.1 Emergency stop shutdown to SIL 1or PLc with a 3SK1 safety relay

Application:

Single-channel emergency stop shutdown of a motor by a parameterizable 3RK3 Modular

Design:

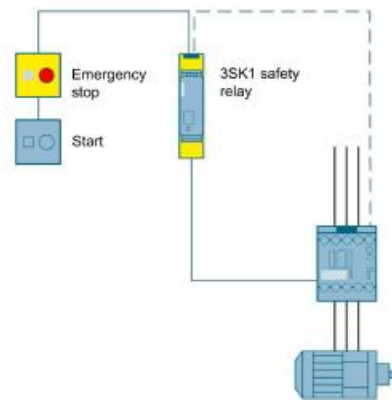


Figure 10 Emergency stop shutdown to SIL 1or PLc with a 3SK1 safety relay [16].

Operating principle:

The Modular Safety System monitors the emergency stop command device. When the emergency stop command device is actuated, the Modular Safety System opens the enabling circuits and switches the power contactor off in a safety-related manner. If the emergency stop command device is unlatched and the feedback circuit is closed, the Start button can be used to switch on again.

Safety-related component:

Emergency stop command device	Modular Safety System	Contactor
		
3SU1 (http://www.siemens.com/sirius-act)	3RK3 (http://www.siemens.com/sirius-mss)	3RT20 (http://www.siemens.com/sirius-switching)

Figure 11 Safety- related component of the emergency stop shutdown [16].

2.6.2 Protective door monitoring to SIL 1 or PLc with a 3SK1 safety relay

Application:

Protective doors are frequently used to fence off danger zones. These monitored for position and, if necessary, the area from which the hazard emanates is switched off.

Design:

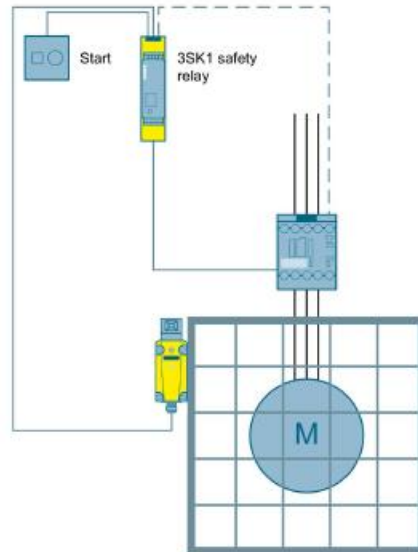


Figure 12 Protective door monitoring to SIL 1 or PLc with a 3SK1 safety relay [16].

Operating principle:

The position of a protective door is monitored via the contact of the safety switch. When the monitored door is opened, the modular safety system triggers and opens the enabling circuits, switching off the power contact in a safety related manner. If the door is closed and the feedback circuit is closed, the start button can be used to switch on again.

Safety-related components.

Safety switch	Modular Safety System	Contactors
		
3SE5 http://www.siemens.com/sirius-detecting	3RK3 http://www.siemens.com/sirius-mss	3RT20 http://www.siemens.com/sirius-switching

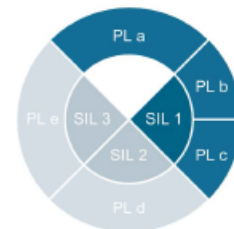


Figure 13 Safety related components for protective door monitoring to SIL 1 [16].

2.6.3 Access monitoring using a light curtain to SIL 3 or PLe with a safety relay

Application: To monitor access to an open danger zone, so-called non protective equipment such as a light curtain can be used. If the light beam is interrupted, a shutdown signal is triggered.

Design:

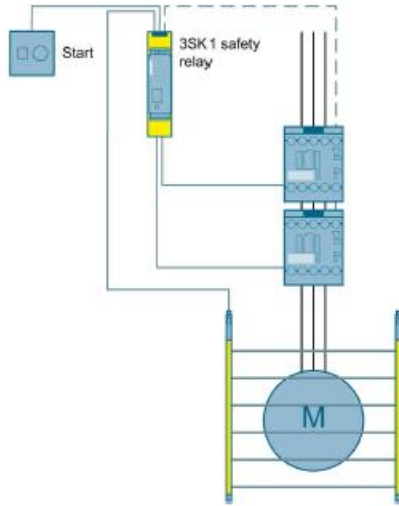


Figure 14 Access monitoring using a light curtain to SIL 3 or PLe with a safety relay [16].

Operating principle:

The light curtain consists of a send unit and a receive unit. Between the two is the protective zone. If the light beam is interrupted, the two outputs switch off the relay. When the light beam is interrupted, the two outputs switch off and the safety relay opens the enabling circuits, switching off the power contactors in a safety-related manner. If the light beam is uninterrupted and the feedback circuit is closed, you can switch on again. This can happen automatically or using a Start button, depending on the application.

Safety- related components:

Safety switch	Safety relay	Contactors
		
3SE5 http://www.siemens.com/sirius-detecting	3SK1 http://www.siemens.com/safety-relays	3RT20 http://www.siemens.com/sirius-switching

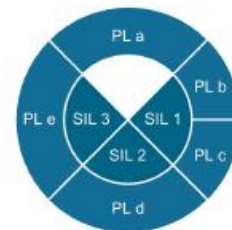


Figure 15 Safety related components for Access monitoring using a light curtain to SIL 3 [16].

Chapter 3 Design Process

3.1 Machine design

The basic procedure of machine design consists of a sequence of steps to fulfil functional requirements of a product to the complete description in the form of drawings of the final product.

[3] Establishes a logical sequence of steps, usually common to all design projects.

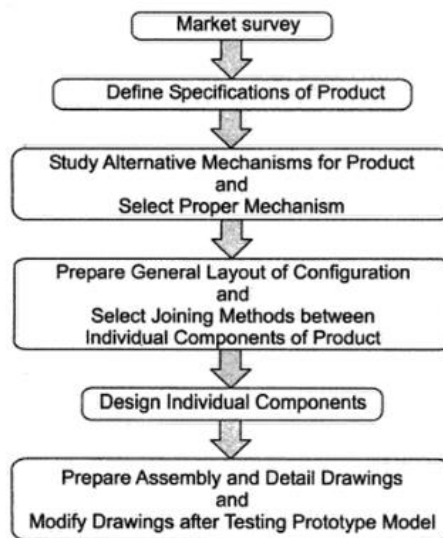


Figure 16 Design Process [3].

The following steps are involved in the process of machine design:

- 1. Product Specifications:** Preparing a full list of requirements of the product.
- 2. Selection of Mechanism:** The designer must prepare rough sketches of the possible mechanism of the product.
- 3. Layout of Configuration:** The designer specifies the joining methods to connect the individual components.
- 4. Design of individual components:** One of the most important steps of the whole process in this step the designer must determine the forces acting on the component, select the proper material and determine the mode of failure.
- 5. Preparation of drawings:** Prepare the drawings of the assembly and the individual components.

3.2 Element design

[3] Also establish the basic procedure of design of machine elements, and divides it in the following steps:

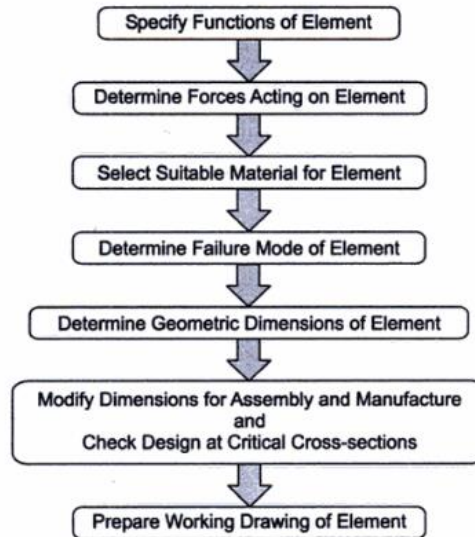


Figure 17 Basic Procedure of design of machine elements [3].

- 1. Specification of functions:** Short description of the functions of the elements.
- 2. Determination of forces:** In most of the cases a free-body diagram of forces is constructed to determine the forces acting on different parts of the machine.
- 3. Selection of the material:** For this step the designer must consider the following factors: availability, cost, mechanical properties and manufacturing considerations.
- 4. Failure Criterion:** Identify the three types of failure (by elastic deflection, by general yielding and failure by fracture) which can affect every component.
- 5. Determination of Dimensions:** The shape and the operation principle of the elements of the machine will lead to a final dimension of the design.
- 6. Design Modifications:** The geometric dimensions of the machine element are modified from assembly and manufacturing considerations.
- 7. Working Drawings:** In the last step the designer prepares a working drawing of the machine element showing dimensions, tolerances and special production requirements.

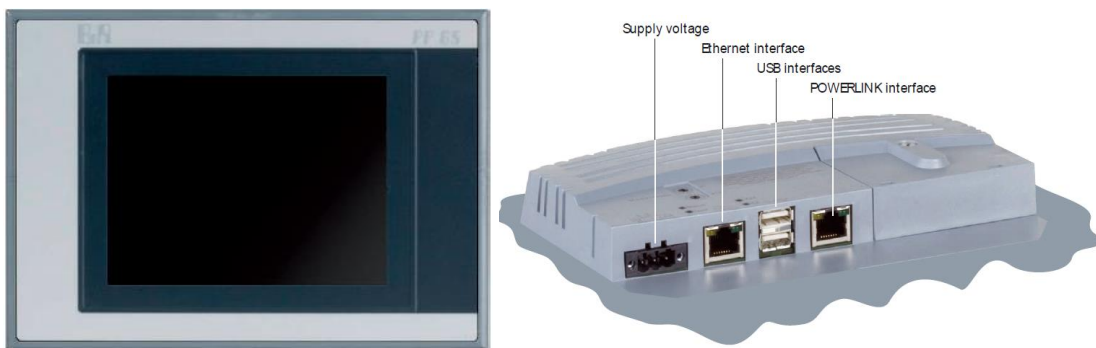
3.3 Previous considerations for the design

At the beginning of the design there is already some demands to fulfil:

1. The design must have a system to facilitate its transportation due to the fact that will be use it in educational fairs.
2. The design needs to incorporate all the elements of the “B&R Educational Board”. All the modules incorporated on the board have a specific function, which can be use it for future applications, e.g. the installation of a new sensor.
3. The height of the demonstrator must be similar to the other two demonstrators in the lab (Project cube, LEGO car assembly machine & ABB FlexPicker assembly cell).
4. To maintain a similar structure standard, the material must be aluminium profiles (8mm).
5. Use material already available at the lab in order to reduce the final cost of the construction.

According to previous demands the design will uses pieces of hardware already stablished. The following section will enumerate and describe the software and hardware that needs to be taken into consideration for the final design.

3.4 Hardware description



3.4.1

Figure 18 Power panel 4PP65.0571-P74 [2]

Power panel 4PP65.0571-P74 (PLC)

The fig. 18 shows the 4PP65.0571-P74 power panel from B&R®. This centralized operating and control unit is equipped with a 5.7" QVGA colour TFT display with touch screen (resistive), 128 MB DRAM, 232 kB SRAM, CompactFlash slot, Ethernet 10/100, POWERLINK, 2x USB and a IP65 protection on the front side.



Figure 19 Module X20IF10A1-1 & X20BC1083 [2]

3.4.2 Module X20IF10A1-1

The X20IF10A1-1 interface module is equipped with an AS-i interface. Using the AS-i interface eliminates the need for parallel wiring, where each individual sensor or actuator was connected to the input or output module via a separate wire. A dual-core wire is used instead, which transfers both power and information at the same time. The main features of this module are:

- AS interface master
- Electrically isolated
- 4-pin bus connector

3.4.3 Module X20BC1083

The X20BC1083 bus controller is used to connect X2X Link I/O nodes to POWERLINK. The bus can be expanded to the left allowing the connection of up to 2 interface modules. The main features of this module are:

- POWERLINK
- I/O configuration and firmware update via the fieldbus
- Integrated hub for efficient cabling
- Up to 2 slots for interface modules



Figure 20 Modules X20PS9400, X20AI4622 & X20AO4632 [2].

3.4.4 Module X20PS9400

The X20PS9400 is a 24 VDC supply module for the bus controller. It is equipped with a feed for the bus controller, the X2X Link and the internal I/O supply.

3.4.5 Module X20AI4622

The X20AI4622 is an analog input module, it is equipped with 4 inputs of 13 bit converter resolution and configurable input filter. This module can be configured in two different ways: current or voltage mode. In voltage mode the range is from -10 V to +10 V, in current mode the range is from 0 mA to 20 mA.

3.4.6 Module X20AO4632

The X20AO4632 analog output module, contain 4 outputs with a 16 bit digital converter resolution, using different connection terminal points the user can select between current and voltage signal. In voltage mode the range is from -10 V to +10 V, in current mode the range is from 0 mA to 20 mA.



Figure 21 Modules X20DM9324, X20SM1426 & BT9400 [2].

3.4.7 Module X20DM9324

The X20DM9324 module is equipped with 8 digital inputs designed for sink connections and 4 digital outputs designed for source connections.

3.4.8 Module X20SM1426

The X20SM1426 module is used to control stepper motors of 24 VDC at a motor current up to 1 A (1.2 A peak), it has 4 digital inputs that can be used as limit switches or as encoder inputs. The main features of this modules are:

- Maximum, rated and holding current configured independent of each other
- 38.5 kHz PWM frequency
- Integrated motor detection
- 256 micro-steps
- Stall detection
- Complete integration in Automation Studio and CNC applications
- Ramp function model based on the CANopen communication profile DS402

3.4.9 Module X20 BT9400

To connect an X20 system to an X67 system, a bus transmitter is simply added to the end of the X20 block, so that the X2X Link cable can be connected. The bus transmitter also provides the X2X supply voltage for the X67 system. There is no longer a need for an X67 system supply module.

The bus transmitter has an integrated internal I/O supply feed. This saves a supply module for the last potential group.

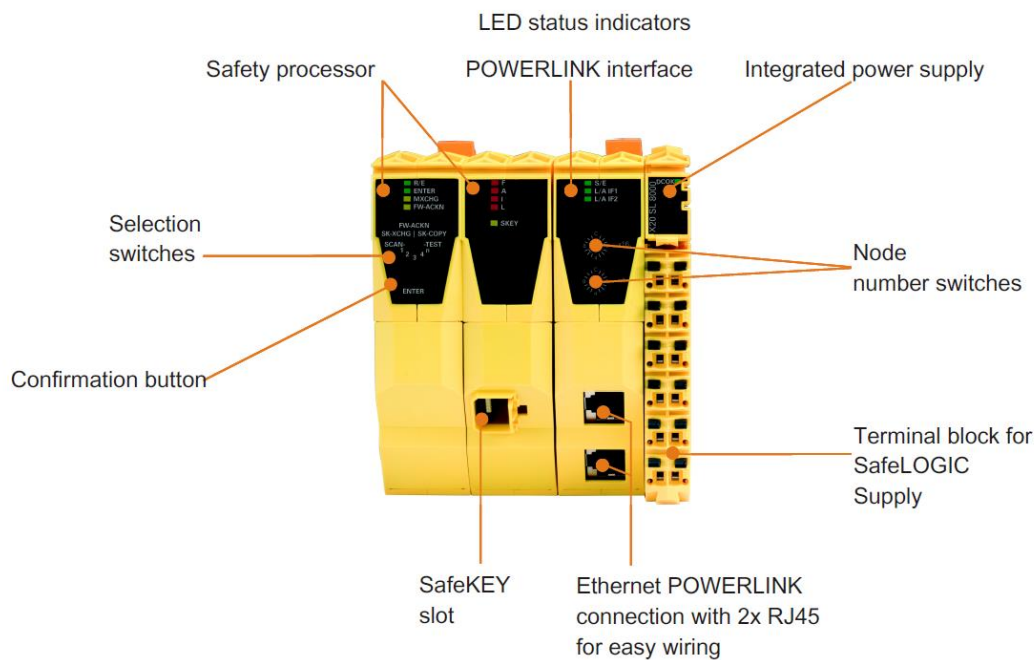


Figure 22 Safety Module X20 SL8001 [2].

3.4.10 Module X20 SL8001

The X20 SL8001 is a SafeLOGIC controller who can handle all central tasks within a safety-related applications, it has 3 different functional areas:

1. - The configuration management
2. - Parameter management system
3. – SafeLOGIC



Figure 23 Safety modules X20 SI4100 & X20 SO4110 [2].

3.4.11 Module X20 SI 4100

This module is equipped with 4 failsafe digital inputs channels, it can be used for safety applications up to PL_e or SIL 3; for the transmission of data to the bus system this module uses openSAFETY (the data is securely encapsulated) so all the components on the network that are involved in the transfer do not require any additional safety-related features [2].

3.4.12 Module X20 SO 4110

This module can be used for applications up to PL_e or SIL 3; is equipped with 4 failsafe digital semiconductor outputs with current monitoring, when network errors occurs the safe digital output channels provide protection against this kind of situations and avoiding automatic restart, similar to the X20 SI 4100 this module also uses openSAFETY for the data transmission.

3.4.13 E- stop button (Pull to release)

According to EN/IEC 60947-5-5, EN/IEC 60204-1, and EN ISO 13850, buttons used as actuators of an emergency stop device shall be colored red. When a background exists behind the actuator, and as far as it is practicable, it shall be colored yellow. Most suppliers of push buttons accomplish the yellow background in one of three ways:

1. Use of a yellow enclosure.
2. Use of a large Emergency Stop legend that is yellow.
3. Coloring the “stem” of the push button yellow.

3.4.14 Standard (22 mm) start button

This button follows the standard IEC/EN 60947-5-1 for control and signalling units, it is also according to the IEC 536 standard a class I button against electric shocks, its front is green.[14]

3.4.15 Standard (22 mm) reset button

Same as the start, this button fulfils the IEC/EN 60947-5-1 standard, but its colour is blue.

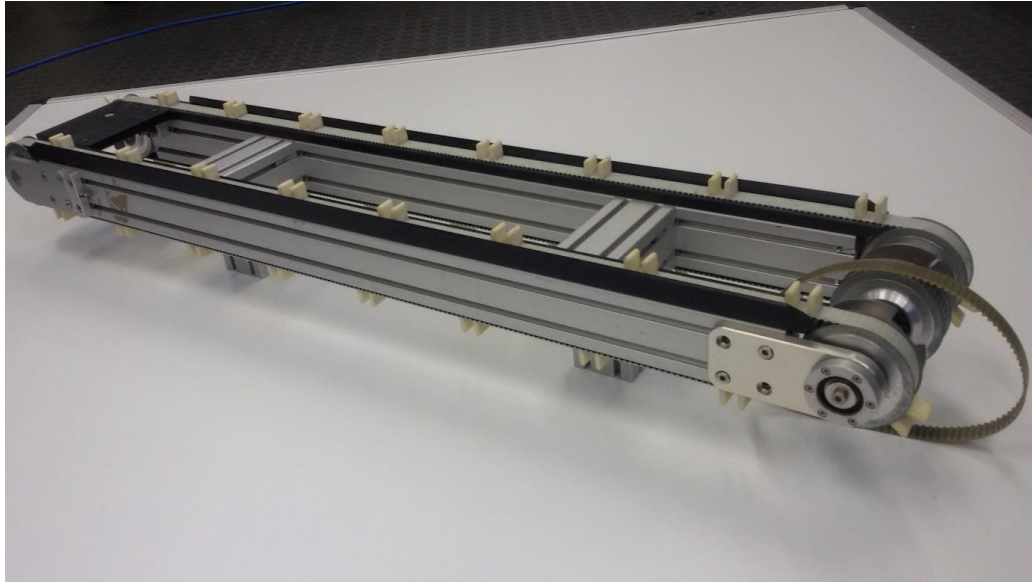


Figure 24 Conveyor belt for the safety demonstrator.

3.4.16 Conveyor Belt

For the transport system function a conveyor available at the laboratory will be used, a few modifications need to be made in order that the conveyor transport the material in a non-stop loop. The modification of the height of the supports is one of the main changes.

3.4.17 OY801S Light Curtain

Due to the dimension of the conveyor a light curtain with finger protection is preferable, for that the light curtain from the ifm manufacturer is suitable for the current application, it is a 14 mm resolution light curtain with a response time of 3 msec.

3.5 Software description

3.5.1 Automation Studio

B&R Automation Studio is the software development environment in which the program will be written. The capacity of configuring the controller, communication and visualization in just one environment reduce integration time and maintenance costs.

In this software the user can choose between several ranges of programming languages, editors and diagnostic tools.

The layout of automation studio is shown in the following image:

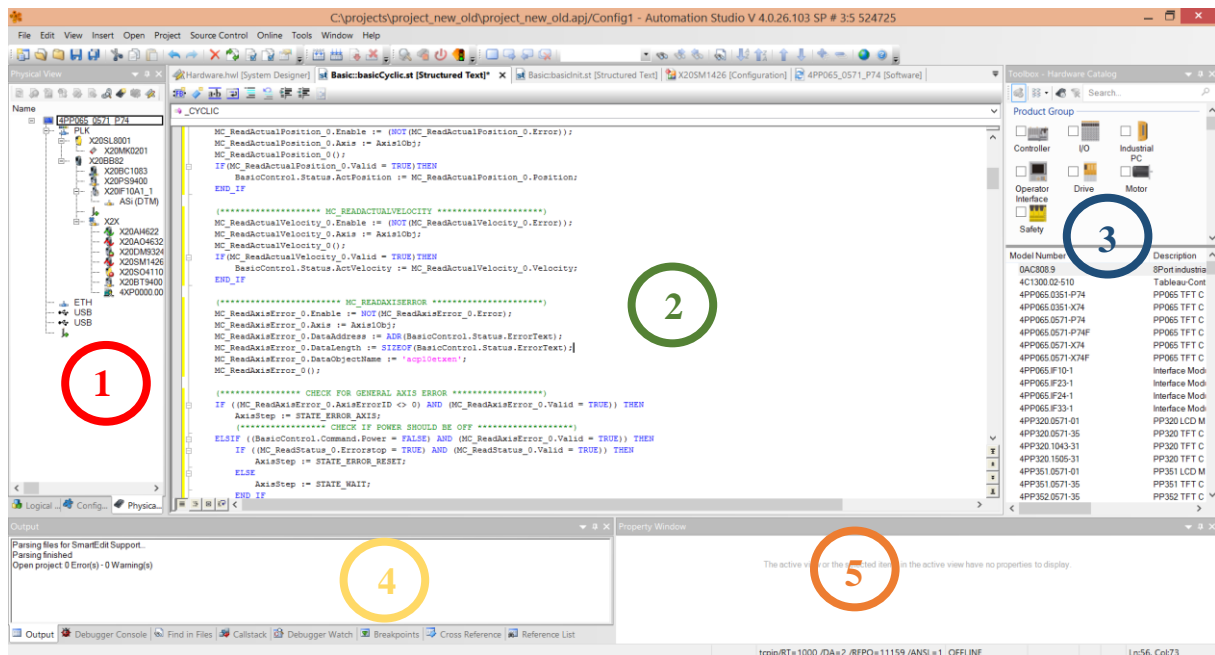


Figure 25 Automation Studio Workspace.

- 1) Project explorer is used to managed and edit software and for the configuration of objects in a project.
- 2) The center of the screen is the area where open documents are worked on. In this area the configuration of the modules used in the application is possible.
- 3) The toolbox window allows the selection of hardware modules, program functions or software objects.
- 4) The output window display information associated with the project. Important information during the building of the project is displayed in this area.

- 5) The properties window display configuration options for object of hardware modules. It also used to edit the properties of selected objects.

3.5.2 SISTEMA Safety tool

The SISTEMA (Safety Integrity Software Tool for the Evaluation of Machine Applications) is a free software that provides developers and testers of safety related machine controls with comprehensive support in the evaluation of safety following the context of ISO 13849-1.

By modelling of the structure of the safety-related control components upon the designated architectures, the tool is capable of the automatic calculation of the reliability values with several levels of details, including the PL.

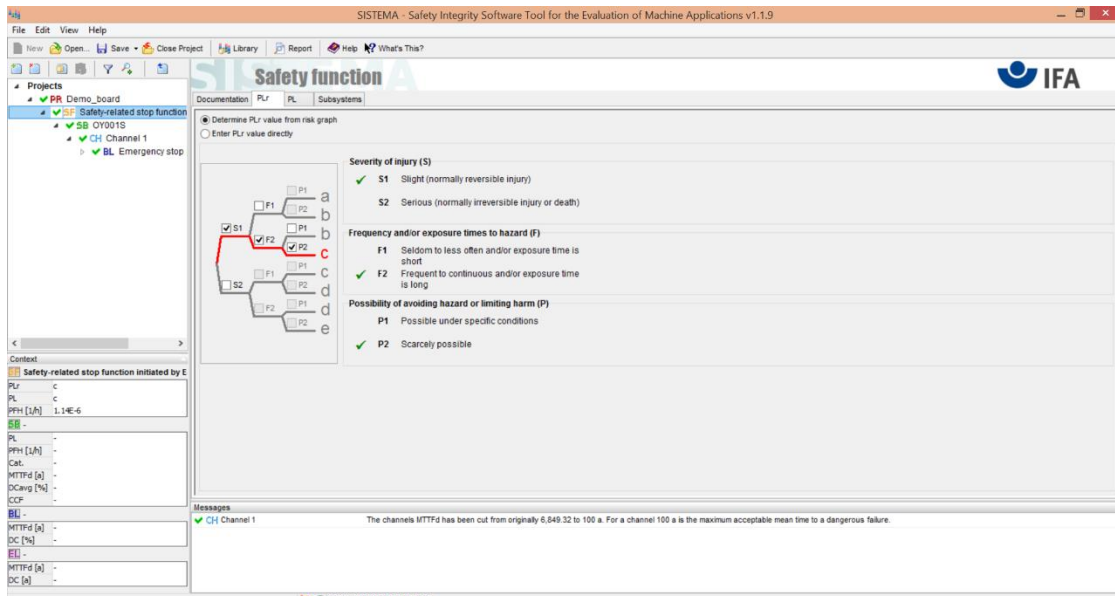


Figure 26 SISTEMA software workspace

3.5.3 Autodesk Inventor

Inventor Professional 3D is a software that offers an easy to use set of tools for 3D mechanical design, product simulation and documentation. This software is used for the design of the demonstrator along with its multiple parts.

Chapter 4 Risk Assessment of the design

This section is dedicated to show the early designs of the demonstrator along with the final design and the safety measures implemented.

4.1 Early designs

Given the previous considerations mentioned in Chapter 3, the design process take place with some early designs, these first attempt fulfil the previous considerations; however following the philosophy that every design can be improved, the pros and cons of these designs are mentioned.

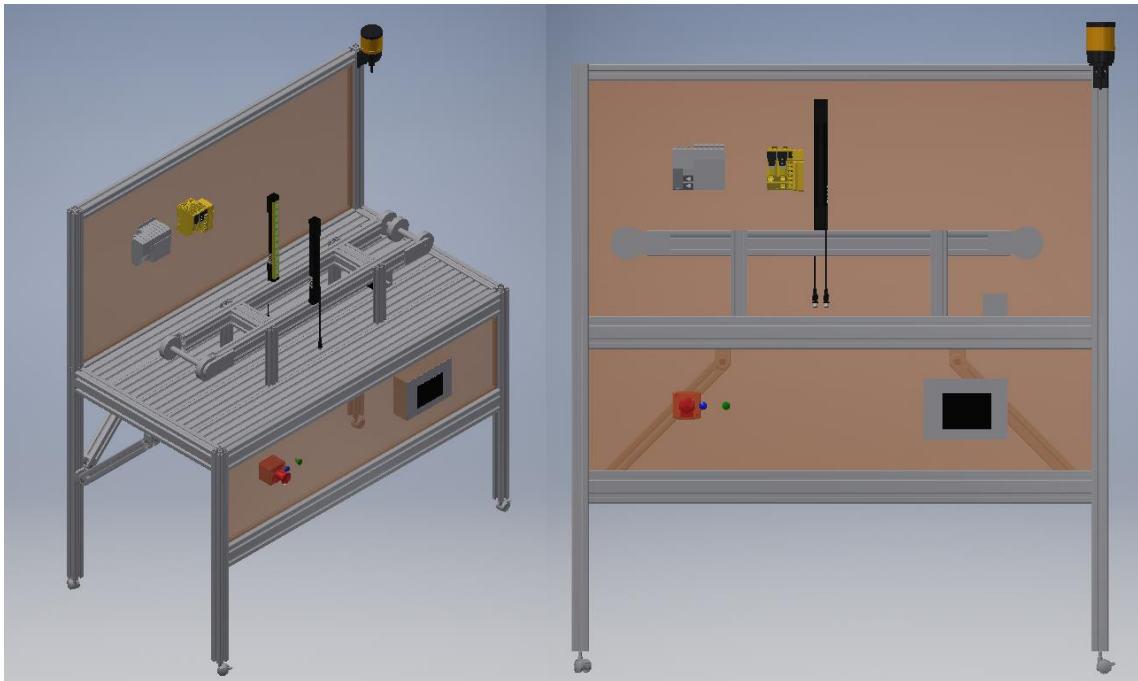


Figure 27 First design of the safety demonstrator.

Pros:

- Enables future expansion by having enough space to add more modules.
- All the modules (Safety and control) are visible.

Cons:

- The user can interact directly with the modules, it can potentially lead to a malfunction by the interaction with the connections.
- Too much wasted space (having all these big areas of acrylic; these pieces can be broken much easier).
- The position of the screen is relatively low.

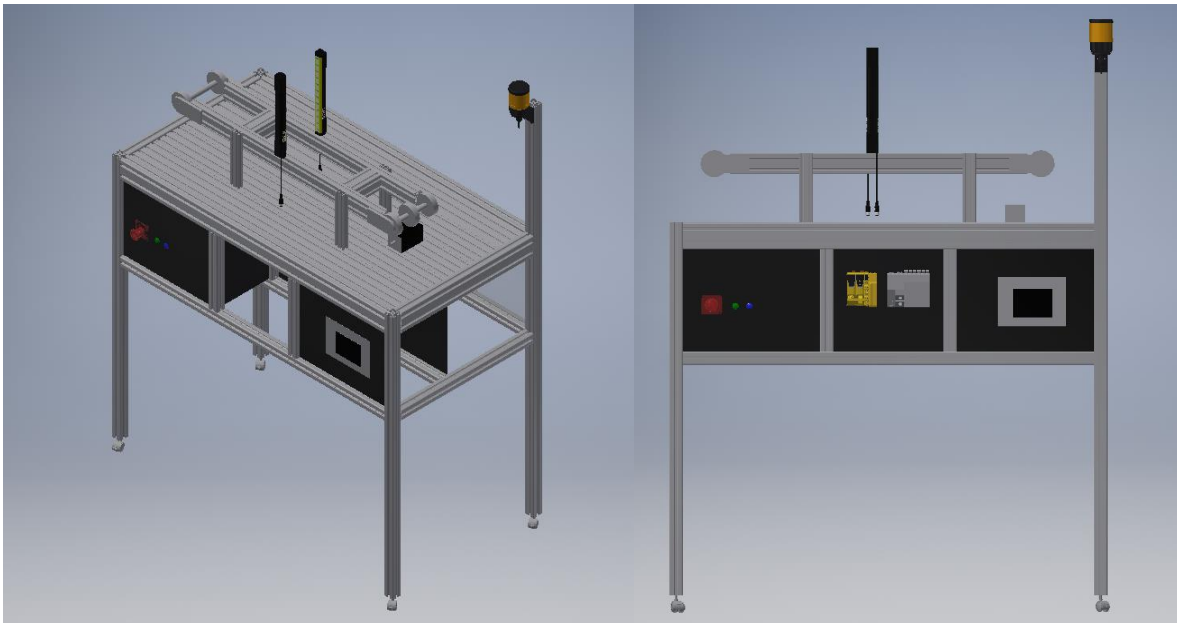


Figure 28 Revision 2 of the safety demonstrator.

Pros:

- The direct interaction with the connections of the modules is no longer possible, but its visualization is completely clear.
- Bottom design is completely close, however any modification or maintenance is possible by using the right tools.

Cons:

- By dividing the bottom part in 3 sections, the space for adding more modules is reduced.
- Lack of an area capable of illustrate the “danger zone”.

4.2 Final design:

Pros:

- A well-defined safety zone.
- Full addition of the elements of the elements of the demo board.
- Future expansion of the modules is possible.
- All the modules are visible, the direct interaction with the connections (for maintenance) can be done by using the right tools.
- Maintenance is relatively easy, by removing the aluminium profiles of the bottom part.
- The electrical connections of all the buttons are invisible by using black acrylic, giving a more esthetic presentation.

Cons:

- The modification of the light curtain position will also affect the length of the safety zone; this distance is linked to a safety distance calculation.

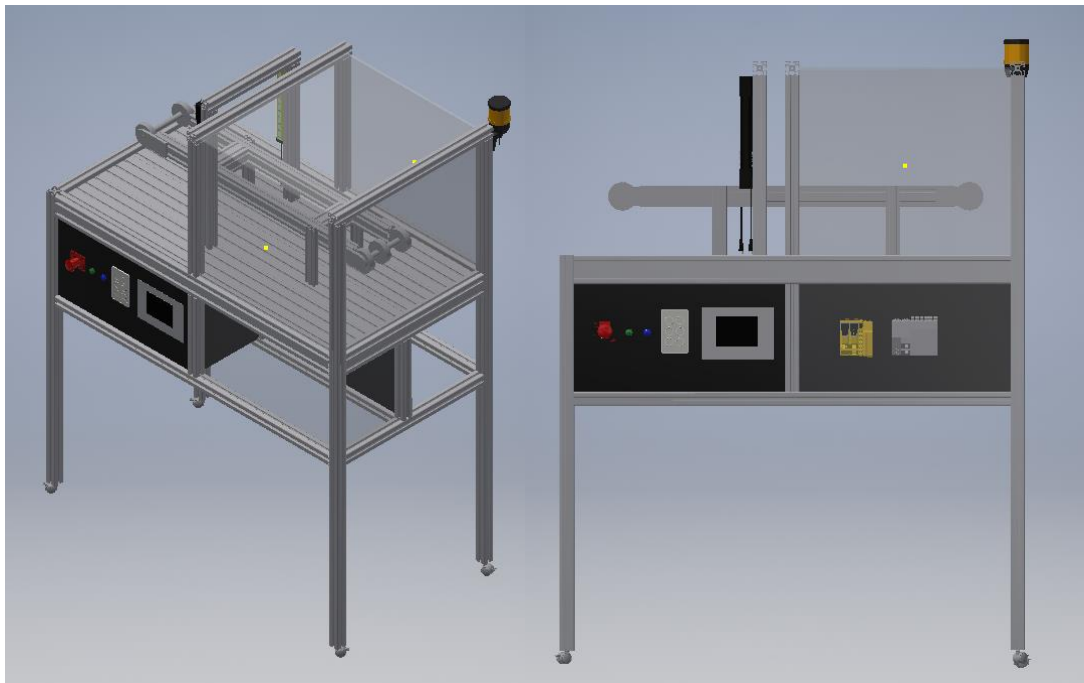


Figure 29 Final design of the safety demonstrator

4.3 Static Analysis of the structure

Part of the risk assessment is to be sure that the design of the structure is capable to hold up the weight of all the elements of the design, for that, the calculation of the maximum deformation is necessary.

In order to determine the deformation, stress and strain, a static analysis was performed in the Autodesk Inventor environment.

Considerations:

- Material: aluminium 6061.
- 4 point contacts with the ground (each leg of the structure) acting as a fixed constrain.
- A maximum force of 100 N is applied in each plane profile referring to the z-direction in the base coordinate system.

By simulating the forces applied in each of the plane profiles, the following displacement is obtained.

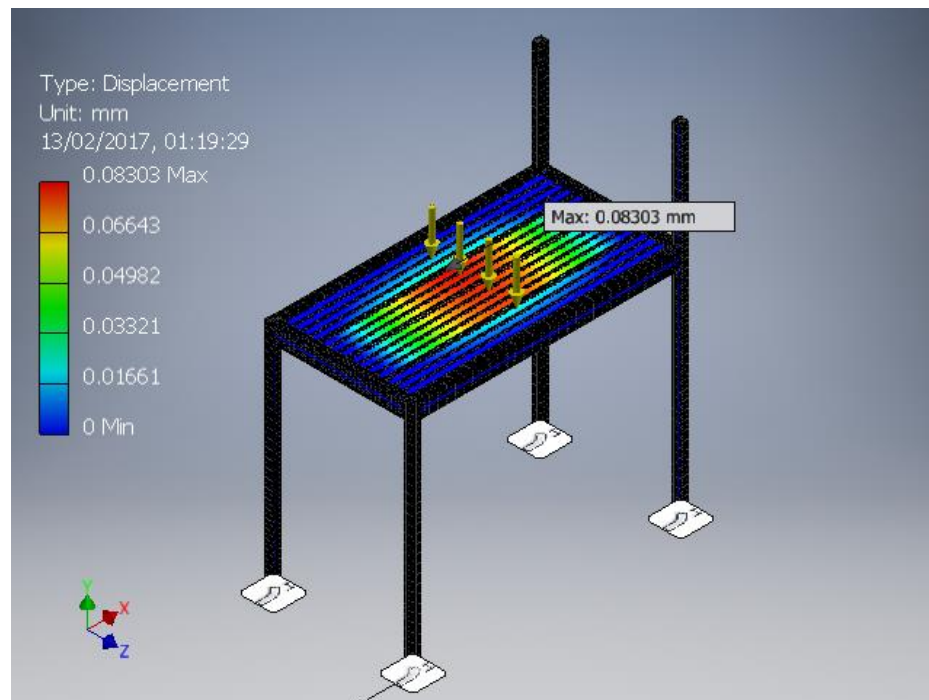


Figure 30 Displacement of the structure after load

☐ **Result Summary**

Name	Minimum	Maximum
Von Mises Stress	0.00000973612 MPa	2.11086 MPa
1st Principal Stress	-0.301633 MPa	2.74451 MPa
3rd Principal Stress	-1.70873 MPa	0.506298 MPa
Displacement	0 mm	0.0830338 mm
Safety Factor	15 ul	15 ul
Stress XX	-1.68523 MPa	2.68618 MPa
Stress XY	-0.608332 MPa	0.635742 MPa
Stress XZ	-0.818341 MPa	0.535081 MPa
Stress YY	-0.79691 MPa	0.813283 MPa
Stress YZ	-0.444931 MPa	0.417063 MPa
Stress ZZ	-0.688293 MPa	1.18768 MPa
X Displacement	-0.016193 mm	0.00554407 mm
Y Displacement	-0.0830332 mm	0.000316573 mm
Z Displacement	-0.00942233 mm	0.00899391 mm
Equivalent Strain	0.00000000141943 ul	0.0000287693 ul
1st Principal Strain	-0.00000302294 ul	0.0000334707 ul
3rd Principal Strain	-0.0000211328 ul	0.00000212017 ul
Strain XX	-0.0000207907 ul	0.0000323447 ul
Strain XY	-0.0000117428 ul	0.0000122719 ul
Strain XZ	-0.0000157967 ul	0.0000103289 ul
Strain YY	-0.0000115472 ul	0.0000114829 ul
Strain YZ	-0.00000858866 ul	0.0000080507 ul
Strain ZZ	-0.00000773184 ul	0.000014803 ul
Contact Pressure	0 MPa	18.5644 MPa
Contact Pressure X	-7.41806 MPa	10.9052 MPa
Contact Pressure Y	-13.9283 MPa	5.2806 MPa
Contact Pressure Z	-16.353 MPa	11.4363 MPa

Table 16 Result summary of the static analysis

The maximum displacement of .08303 mm is considered acceptable. The displacement is not significant, even applying a force larger than the force produced by the weight of all the elements of the demonstrator (conveyor belt, light curtain, safety zone structure). The structure of the demonstrator is strong enough to support all the elements and devices without suffering any significant deformation.

4.4 Safety distance for the light curtains

Once that the safety and the danger zone are defined, the designer should calculate the distance for the position of the light curtains.

The EN ISO 13855 defines the safety distance with the following formula:

$$S = (K * T) + C$$

Where:

S= safety distance in mm.

K= body/ part of the body speed in mm/s.

T= T1+T2

T1= the safety device's reaction time in sec.

T2=the machine's reaction time in sec.

C= Further distance in mm based upon the body's intrusion towards the risk area before the safety device has been activated.

The EN 13855 also defines some preferential distances:

$$S = (K * T) + 8(d - 14)$$

Where:

d=light curtain resolution in mm.

Since the demonstrator must deal with little objects, the safety light curtain was designed for finger protection and the times factors can be found in the manual of the devices; the following information is defined:

d=14 mm

K= 2000 mm/s (Hand speed)

T1= 3×10^{-3} sec.

T2= 18×10^{-3} sec.

Leading to a formula where the safety distance is:

$$S = \left[2000 \frac{mm}{s} (3 * 10^{-3} sec + 18 * 10^{-3} sec) \right] + 8(14mm - 14mm)$$

$$\mathbf{S = 36 mm}$$

Since the minimum safety distance is the 36 mm; for design proposes a safety distance of **50 mm** will be implemented in the final design.

4.5 Design and calculation for the safeguards

Before any calculation or analysis, the designer should confirm the right choice for the material and the type of safeguards, In accordance with EN 953 Annex A, the flow chart indicates the right choice of safeguards according to the danger and the operation of the machine:

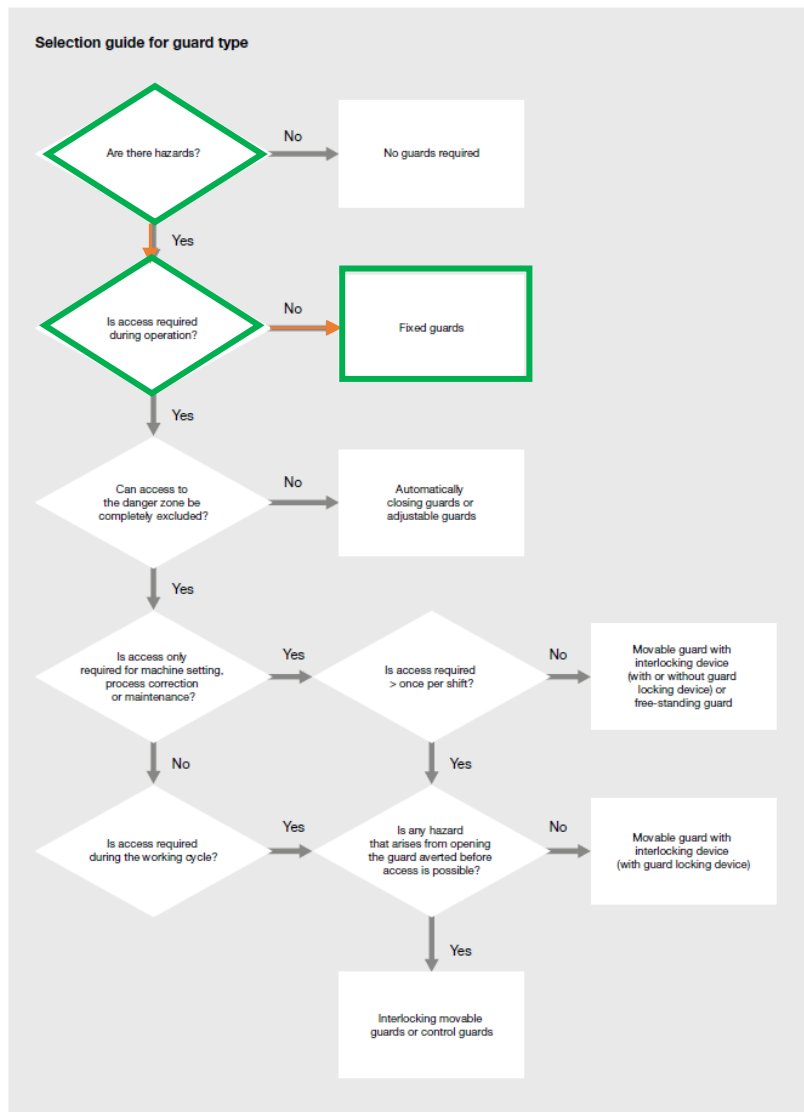


Figure 31 Selection of the type of safeguard [18].

Once that the type of safeguard is defined, the hazard identification for the installation of the safeguard is presented. By installing fixed guards, the designer must take into account that the guards must be fixed using systems that can be opened or removed only with tools. Where possible, guards must be incapable of remaining in place without their fixing.

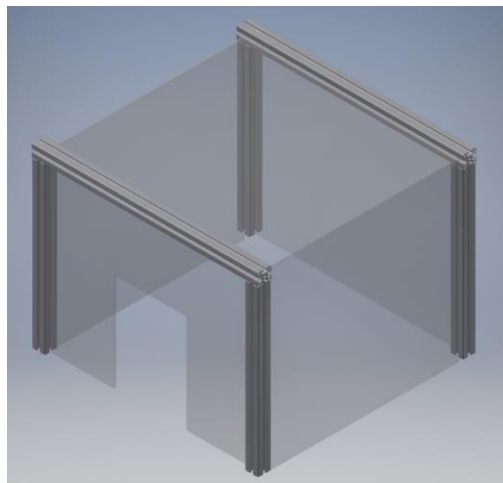


Figure 32 Design of the safeguards.

Hazard id		Hazard No: 1
Title	No safeguard around the danger zone of the conveyor	
Location	Top of the safety demonstrator	
Target	Fingers and hand extremities	
Activity	Automatic mode	
Task	Operation	
Function		
Type of hazard	Mechanical	
Description	The operator and the spectators of the safety demonstrator can reach the danger zone of the conveyor belt.	
Risk estimation and assessment		
Probability of occurrence 5	Frequency of event 4	
Degree of possible harm 4	Number of persons affected 2	
Hazard Rating Number (HRN): 160	Overall result: High	
Risk Reduction	Reference	
Install fixed safeguards around the danger zone. Access to the danger zone will be prevented by installing a pair of light curtains with a resolution of 14 mm for finger detection.		
Anticipated residual risk		
Probability of occurrence 1	Frequency of event 4	
Degree of possible harm 0.5	Number of persons affected 2	
Hazard Rating Number (HRN): 4	Overall result: Negligible	

Table 17 Hazard identification for the installation of safeguards.

Static analysis of the safeguard

Since the material of the safeguards is much more fragile than the material from the structure, a static analysis is important in order to know the limit of each of the plates of the safeguard. For the analysis a force of 200 N is used.

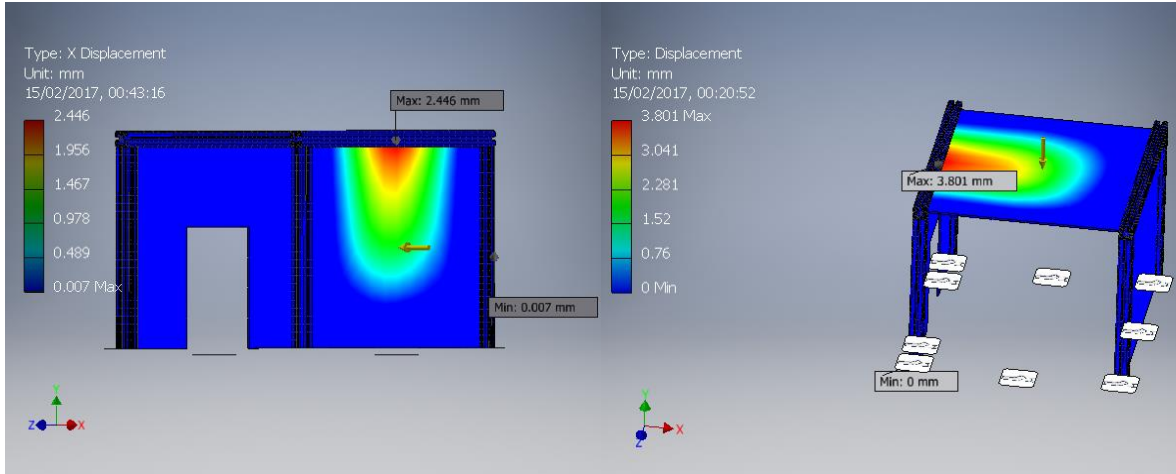


Figure 33 Displacement on the safeguards after load of 200 N

For this part a displacement of 3.8 mm is very significant, it is not recommended to apply a force of more than 120 N in order to maintain the integrity of the safeguard. The safeguard is designed to prevent the access of extremities to the danger zone and not for supporting heavy loads.

Result Summary

Name	Minimum	Maximum
Von Mises Stress	0.000735961 MPa	33.1071 MPa
1st Principal Stress	-15.015 MPa	55.7496 MPa
3rd Principal Stress	-41.2628 MPa	18.9166 MPa
Displacement	0 mm	3.80102 mm
Safety Factor	8.30637 ul	15 ul
Stress XX	-28.8274 MPa	21.4378 MPa
Stress XY	-13.7279 MPa	12.6814 MPa
Stress XZ	-4.31971 MPa	4.59296 MPa
Stress YY	-27.6681 MPa	53.9626 MPa
Stress YZ	-7.0872 MPa	10.565 MPa
Stress ZZ	-19.0279 MPa	27.7344 MPa
X Displacement	-0.0305878 mm	0.0526603 mm
Y Displacement	-3.80102 mm	0.0243677 mm
Z Displacement	-0.449623 mm	0.515044 mm
Equivalent Strain	0.000000467476 ul	0.00153137 ul
1st Principal Strain	-0.0000199955 ul	0.00163372 ul
3rd Principal Strain	-0.0009145 ul	0.0000155504 ul
Strain XX	-0.000221056 ul	0.000270837 ul
Strain XY	-0.000264995 ul	0.000244794 ul
Strain XZ	-0.000342724 ul	0.000487144 ul
Strain YY	-0.000249128 ul	0.00139919 ul
Strain YZ	-0.000136807 ul	0.000712548 ul
Strain ZZ	-0.000531077 ul	0.000566947 ul
Contact Pressure	0 MPa	61.1619 MPa
Contact Pressure X	-33.2356 MPa	35.159 MPa
Contact Pressure Y	-37.4012 MPa	49.7588 MPa
Contact Pressure Z	-51.7263 MPa	45.0521 MPa

Table 18 Displacement of the safeguards applying a force of 200 N

4.6 Safety-Related System

The integrated safety technology from B&R used in this project consists of the following components:

- openSAFETY
- SafeIO

4.6.1 openSAFETY

“B&R uses the technology of openSAFETY via POWERLINK for transferring safety relevant data. OpenSAFETY via POWERLINK is the first real-time Ethernet-base safety bus”. [19]

The purpose of the safety protocol is to ensure the integrity of transferred data. During the transfer, must not be repeated, lost or corrupted.

4.6.2 Enabling principles

There are two main enabling principles the “Direct” and the “Via SafeLOGIC”

- “Direct” enabling principle: “The output is portrayed as an unsafe digital output in the standard application. This mode makes it possible to operate the safe output with the standard application and the enabling of the safety controller are “TRUE”. [19]
- “Via SafeLOGIC” enabling principle: In this mode the SafeLOGIC controller is in charge of the output of the safety module.

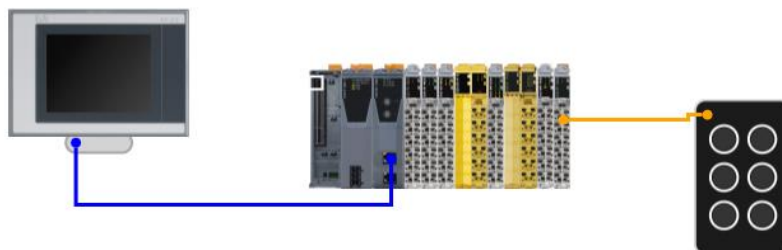


Figure 34 Connection of a "Direct" enabling principle on automation studio.

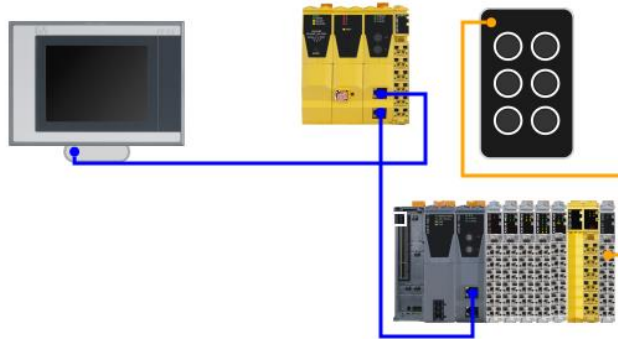


Figure 35 Connection of a "Via SafeLOGIC" enabling principle on automation studio.

For develop of this project a “Direct” enabling principle is used, this is due of two main reason:

- Compatibility problems with recent OS (Windows 10, 8, 7 and Vista) with the Safety Release version of the Module X20 SL8001 and the SafeDESIGNER software.
- The “Direct” enabling principle is suitable for the demonstration of a “Category 1” safety application, due to its simplicity.

Since the uses of the Safe DESIGNER software is no longer needed, the language of programing will remain entirely on the Structure Text language (ST).

4.7 SISTEMA validation process

Once all the elements, devices and safety measures are defined, the PL_r can be calculated by using the SISTEMA, in this section some key elements are showing, the full detail report can be consulted in the appendix.

Choosing the category

Since the risk assessment relies on the ISO 12100 (a type A standard), the safety function along with the safety devices and the safety measures taken, the category type 1 is suitable for the demonstration of the basic safety standards.

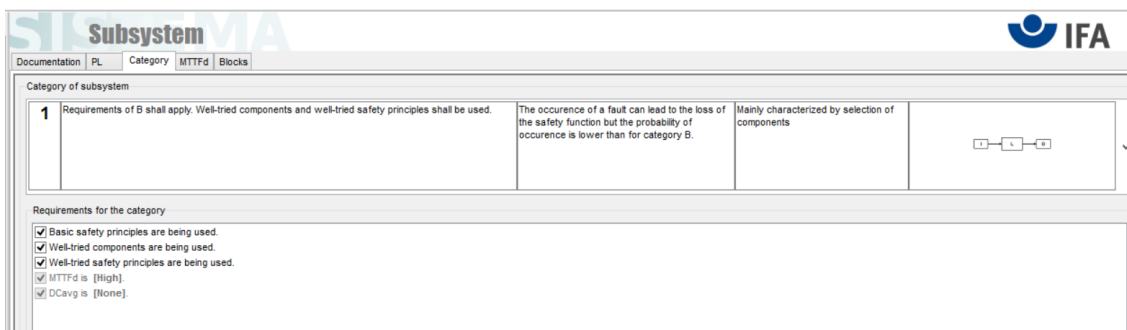


Figure 36 Category selected (SISTEMA tool)

Performance level required (PL_r)

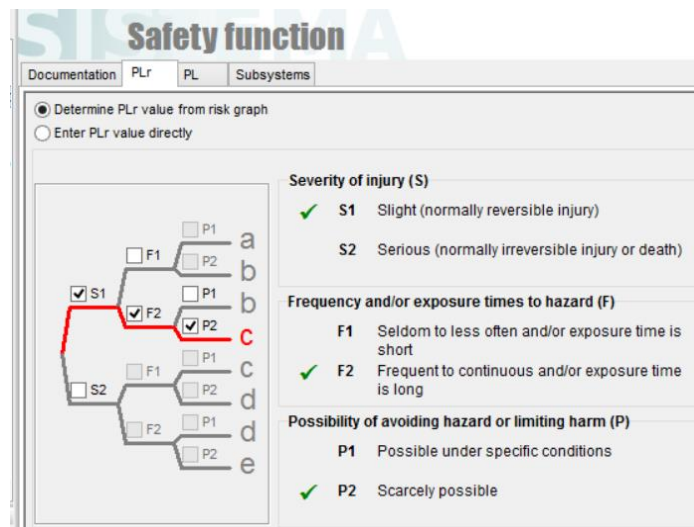


Figure 37 Level of PL required for the safety demonstrator.

Given the category, the safety elements and the safety functions, the demonstrator achieve a PL_c , the result can be checked by the status of the model,

Chapter 5 Conclusion and future work

5.1 Conclusions

In this thesis a design of a safety demonstrator was addressed as the main objective. The main contribution made during the development of this work is the validation of a structure capable to illustrate some of the basic safety functions, all these by following the recommendations dictated in ISO standards like the ISO 12100, ISO 13849-1 and EN 62061.

The knowledge presented in this thesis is transferable to any other safety application which can be expanded easily, this works acts as a solution for basic safety design. Overall, this thesis provides value information for students who are interested in the safety related work.

The complete construction of the demonstrator was not possible due to the delivery time of the light curtains and the plane aluminium profiles, however all the critical parts that involve these elements were simulated by software. This can be implemented as a future work along with the enhancement of the structure.

5.2 Future work

For oncoming works that can be done is the full construction and testing of the demonstrator. Also since the design is already planned for the addition of future sensor or modules, an easy modification of the structure will enable the enhancement of the safety measures, and even a change of the safety category is possible.

The upgrade of the SafeLogic module will resolve the compatibility problems, enabling the use of the “Via SafeLOGIC” principle and open a major of possibilities to implement more sensor or achieve a higher PL

References

- [1] ABB. (2011). Safety in control systems according to EN ISO 13849-1. 4-5.
- [2] B&R .(2016). *B&R Automation*. Retrieved from <https://www.br-automation.com/en/perfection-in-automation/>
- [3] Bhandari, V. B. (2010). *Design of machine elements*. New Delhi: McGraw-Hill.
- [4] Cross, N. (2000). *Engineering Design Methods, Strategies for Product Design*. England: WILEY.
- [5] European Association for injury Prevention and Safety Promotion (EuroSafe). (2013). *Injuries in the European Union*. Amsterdam.
- [6] European Association for injury Prevention and Safety Promotion (Eurosafe). (2014). *Injuries in the European Union*. Amsterdam.
- [7] European Combination for Standards. (2010). EN ISO 12100., (p. 96). Brussels.
- [8] European Combination for Standards. (2015). ISO 13849-1., (p. 86).
- [9] Health Survey for England. (2001). *Reducing risks, protecting people*.
- [10] IEC. (2016). *International Electrotechnical Commission Home Page*. Retrieved from <http://www.iec.ch/about/>
- [11] International Electrotechnical Commission. (2008). IEC/EN 62061., (p. 205).
- [12] Occupational Safety and Health Administration. (2011). *Laboratory Safety Guidance*. OSHA.
- [13] Rockwell Automation. (2013). *Functional safety in the process industry*. Milwaukee: Rockwell Automation.
- [14] Scheneider Electric. (n.d.). Comand and signaling units., (p. 58).
- [15] Schneider Electric. (2016). Safety legislation and Standards., (p. 9).
- [16] Siemens. (2016). Application Manual SIRIUS, Safety Integrated., (p. 194). Nürnberg, Germany.
- [17] Pilz. (2015). Pilz Guide to Machinery Safety. (p. 231).

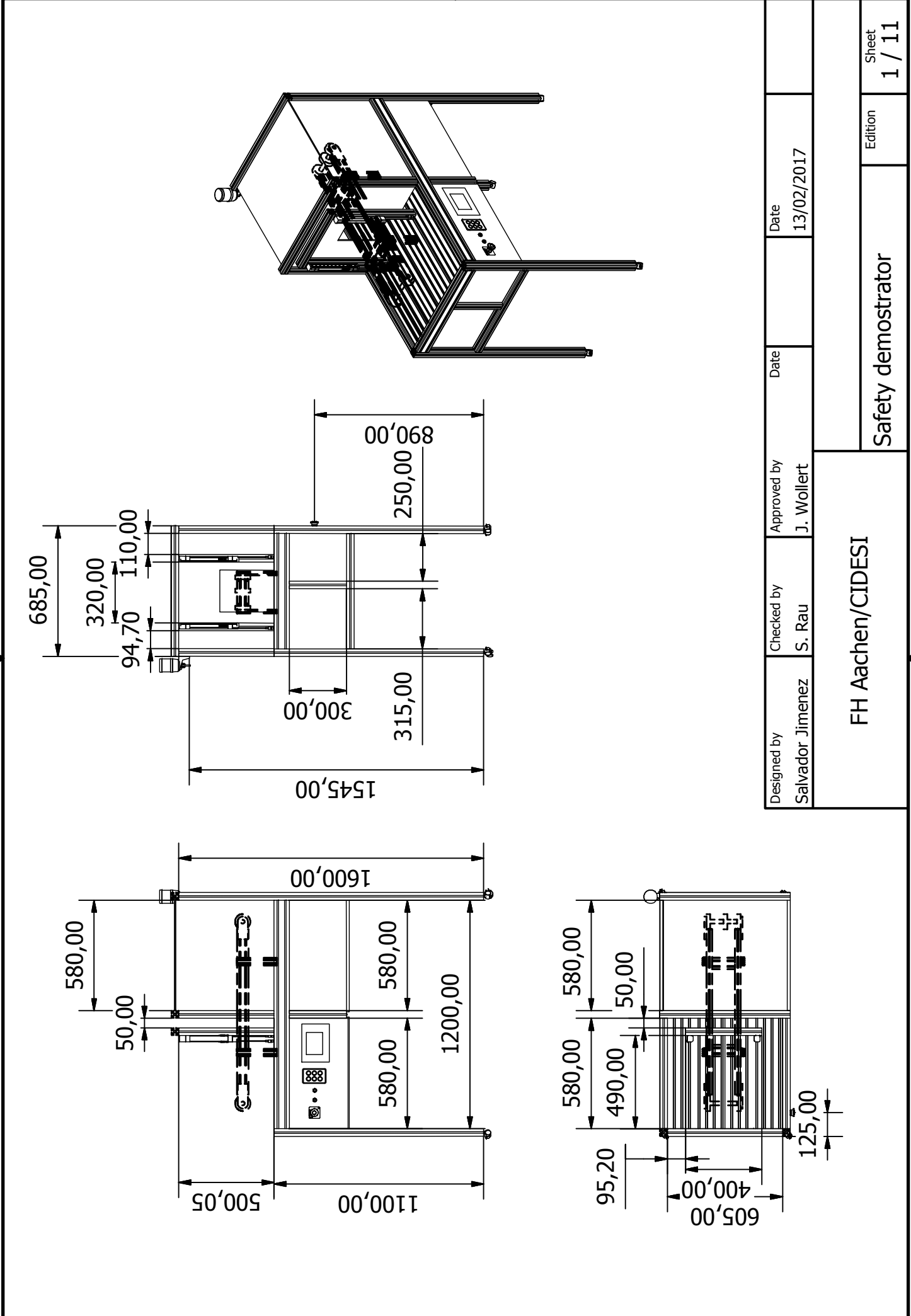
[18] Pilz. (2013). Pilz The Safety Compedium., (p.298). Ostfildern, Germany.

[19] B&R. (2014). Introduction to Integrated Safety. , (p. 36).

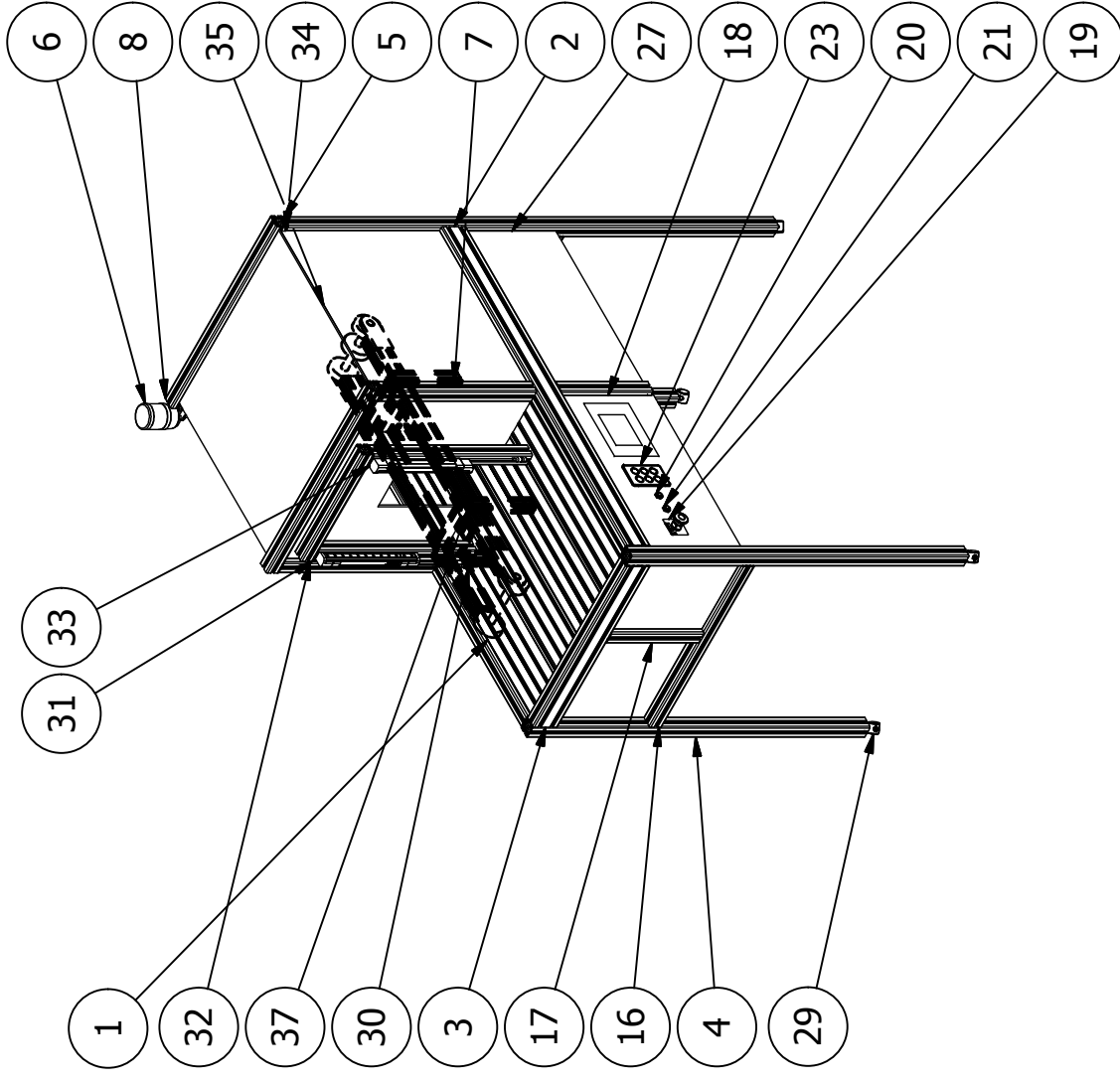
Appendix

Appendix A

CAD Drawings

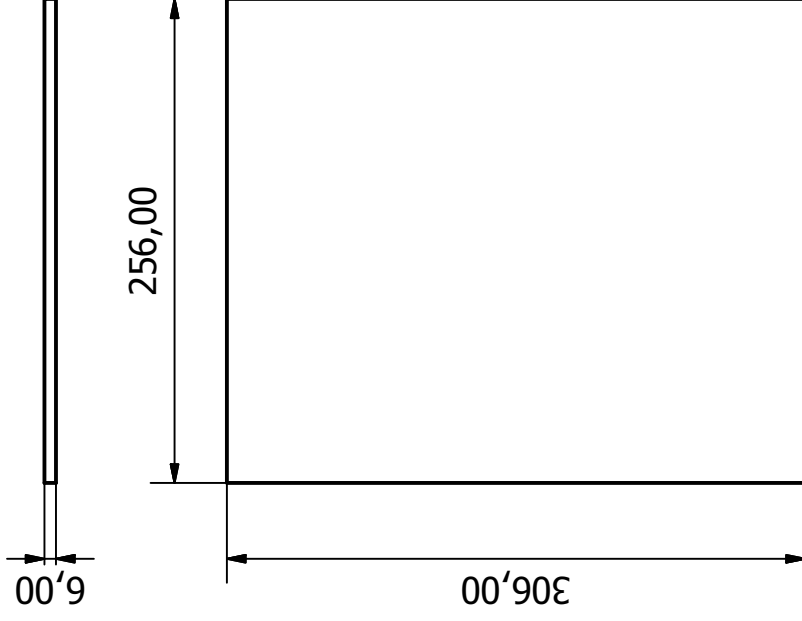


Designed by	Checked by	Approved by	Date
Salvador Jimenez	S. Rau	J. Wollert	13/02/2017
FH Aachen/CIDESI			Safety demonstrator
			Sheet 1 / 11



Designed by Salvador Jimenez	Checked by S. Rau	Approved by J. Wollert	Date 13/02/2017
FH Aachen/CIDESI		Safety demonstrator	
		Edition	Sheet 2 / 11

Acryl_middle



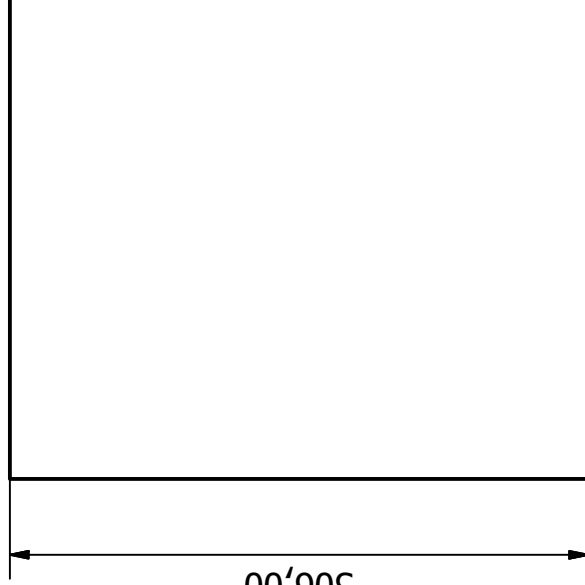
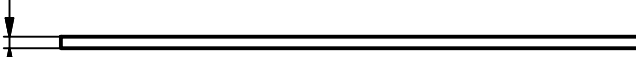
Designed by Salvador Jimenez	Checked by S. Rau	Approved by J. Wollert	Date	Date 13/02/2017
FH Aachen/CIDESI			Safety demonstrator	
			Edition	Sheet 3 / 11

middle_plastic_part

256,00

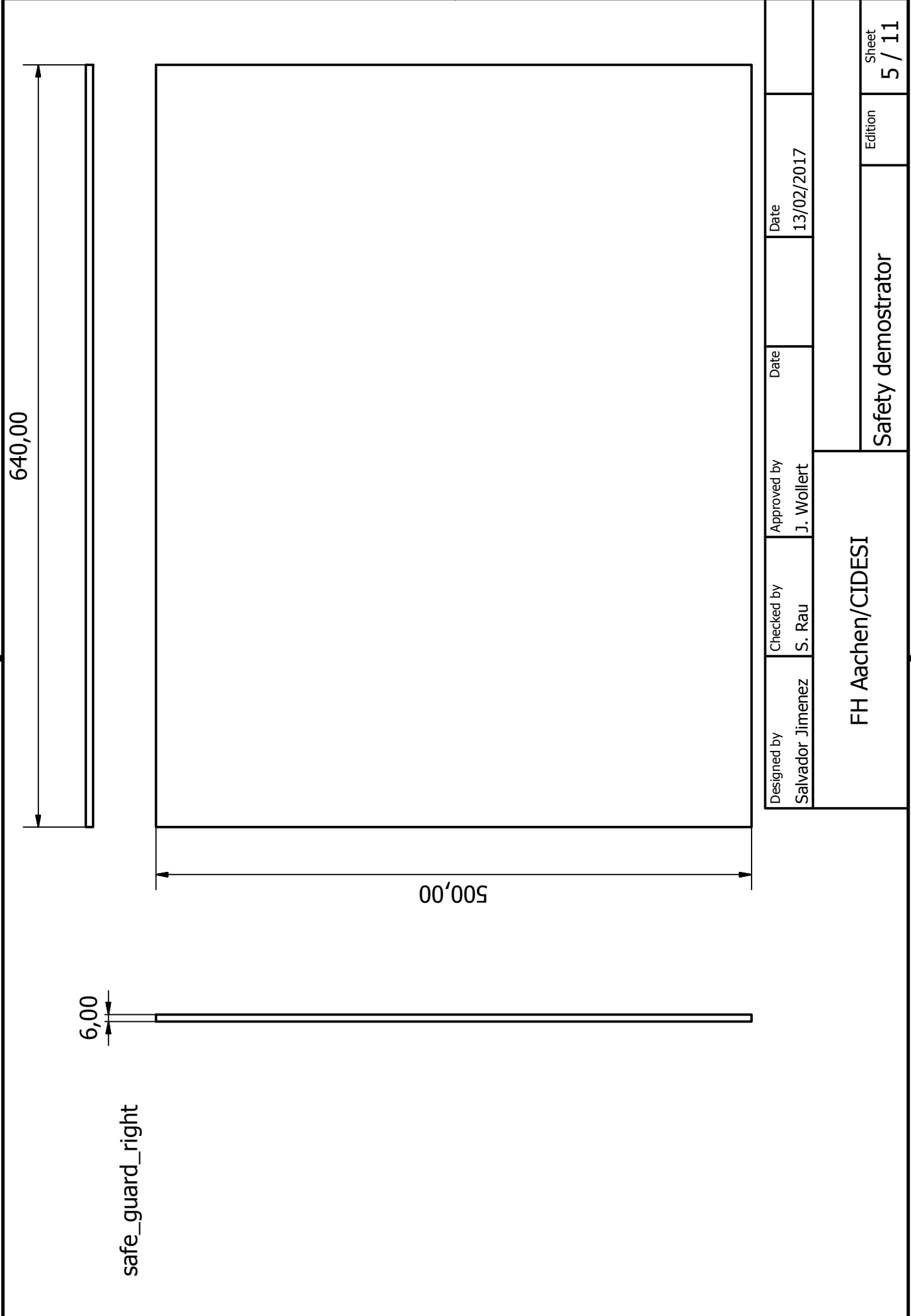


6,00



306,00

Designed by Salvador Jimenez	Checked by S. Rau	Approved by J. Wollert	Date	Date 13/02/2017
FH Aachen/CIDESI			Safety demonstrator	
			Edition	Sheet 4 / 11



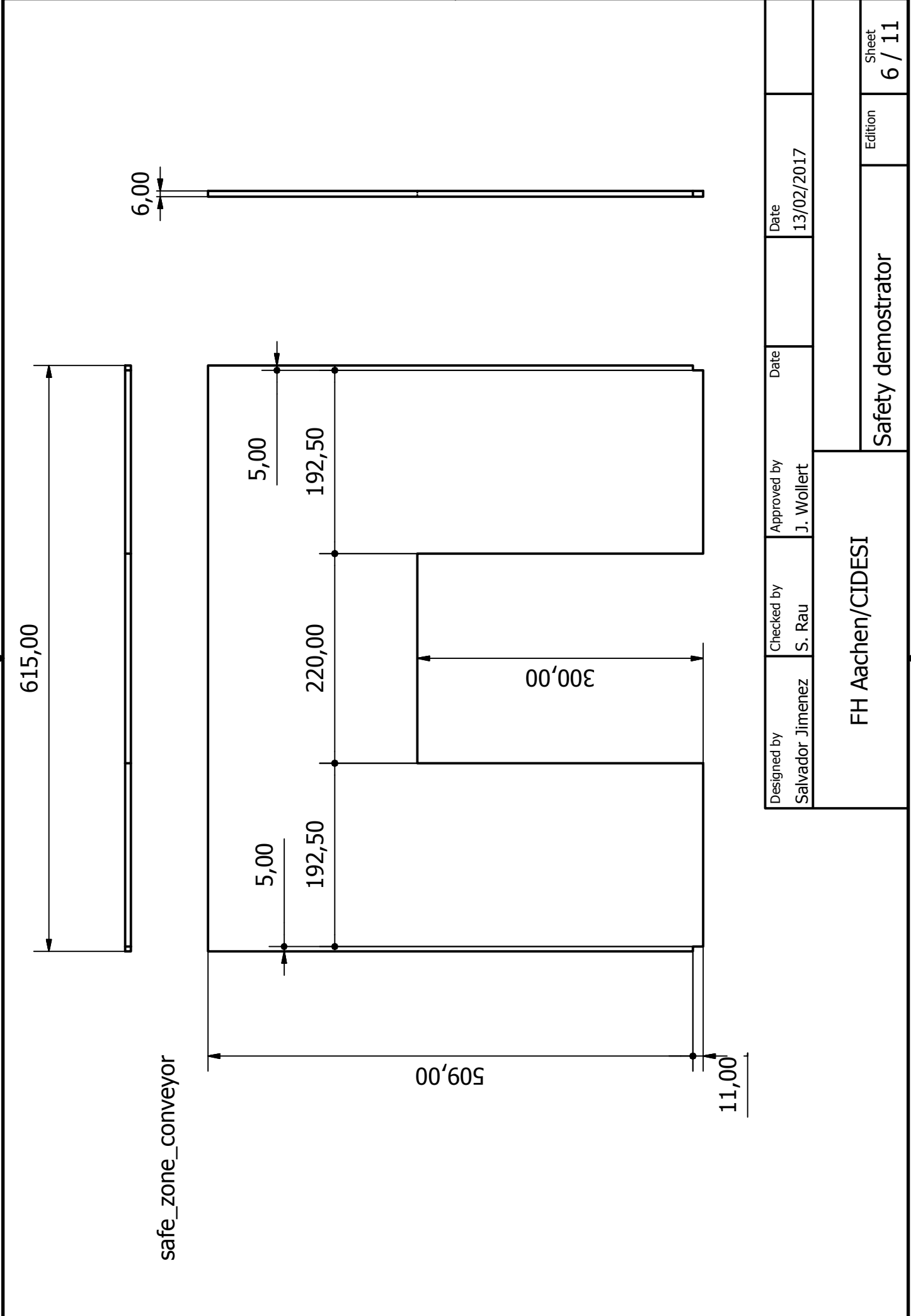
640,00

500,00

6,00

safe_guard_right

Designed by Salvador Jimenez	Checked by S. Rau	Approved by J. Wollert	Date 13/02/2017
FH Aachen/CIDESI			Safety demonstrator
			Edition 5 / 11
			Sheet 5 / 11



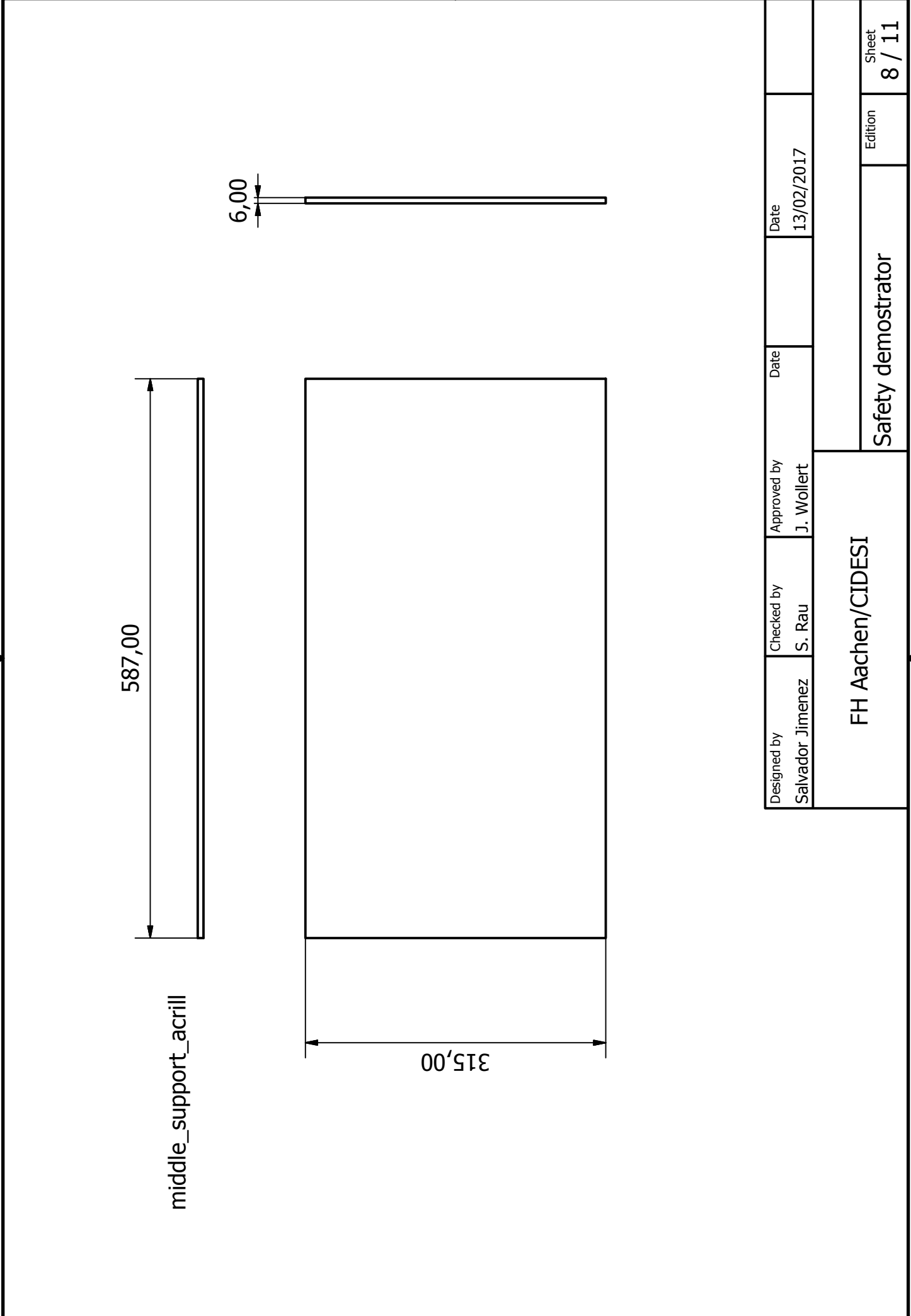
front_panel_acryl

580,00

300,00

6,00

Designed by Salvador Jimenez	Checked by S. Rau	Approved by J. Wollert	Date	Date 13/02/2017
FH Aachen/CIDESI			Safety demonstrator	
			Edition	Sheet 7 / 11



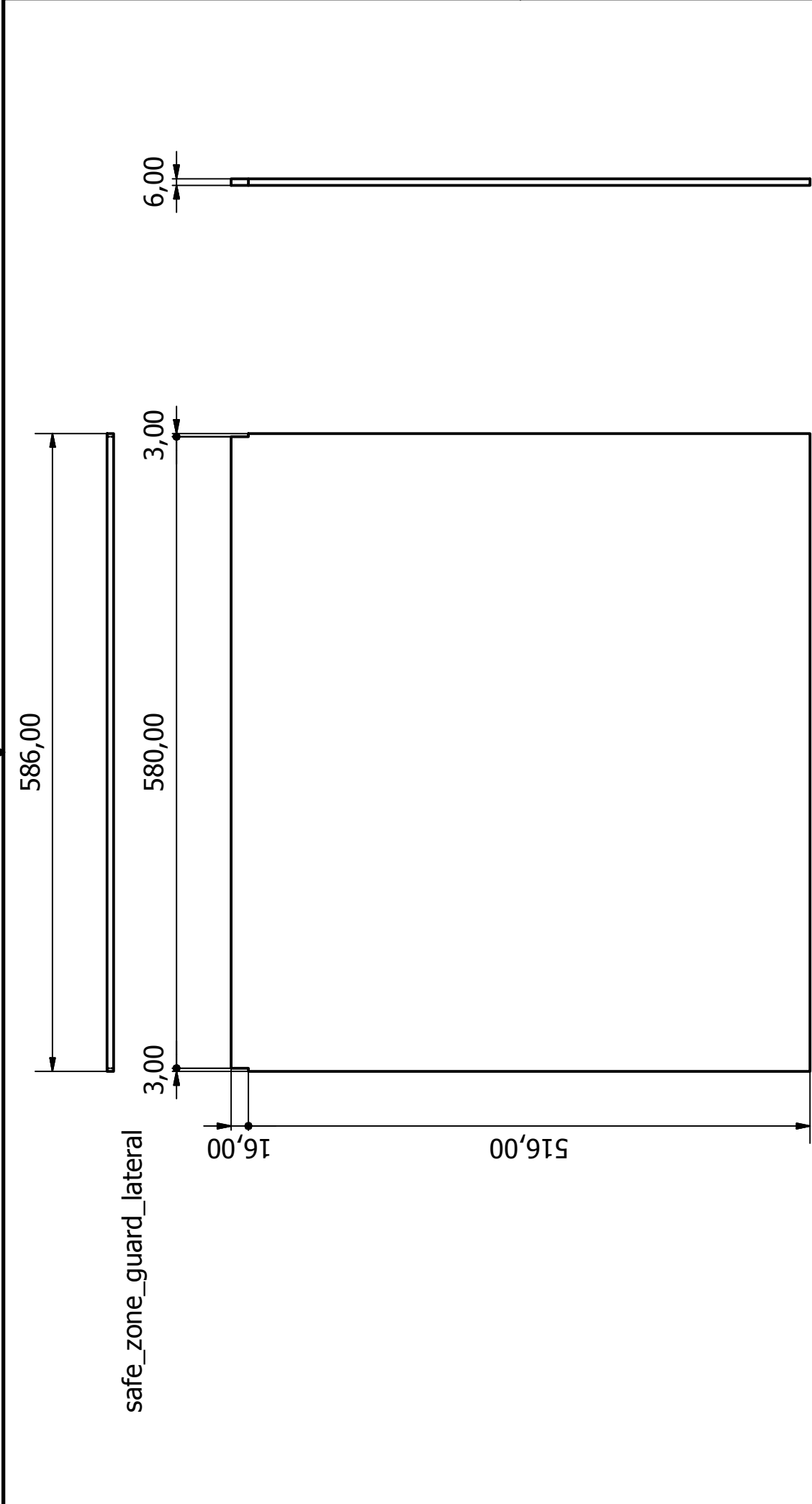
587,00

middle_support_acrill

315,00

6,00

Designed by Salvador Jimenez	Checked by S. Rau	Approved by J. Wollert	Date	Date 13/02/2017
FH Aachen/CIDESI			Safety demonstrator	
			Edition	Sheet 8 / 11



Designed by	Checked by	Approved by	Date
Salvador Jimenez	S. Rau	J. Wollert	13/02/2017
FH Aachen/CIDESI			
Safety demonstrator			Edition
			Sheet
			9 / 11

safe_guard_top

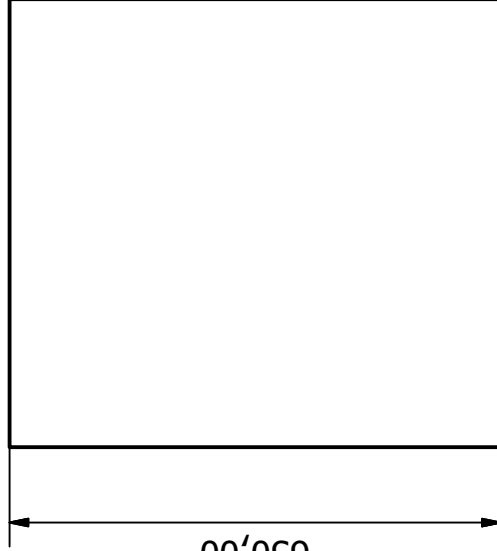
592,00



6,00



650,00



Designed by Salvador Jimenez	Checked by S. Rau	Approved by J. Wollert	Date	Date 13/02/2017
FH Aachen/CIDESI			Safety demonstrator	
			Edition	Sheet 10 / 11

PARTS LIST			PARTS LIST		
ITEM	QTY	PART NUMBER	ITEM	QTY	PART NUMBER
1	4	item_0046579_Plattenprofil_8_152x20_L=1200_1	23	1	4xp000_00-k64-c0
2	2	item_0002634_Profil_8_80x40_leicht_L=1200_3	24	1	safetymodules
3	2	item_0002634_Profil_8_80x40_leicht_L=605_2	25	1	education_modules
4	2	item_0002633_Profil_8_40x40_leicht_L=1100_1	26	2	middle_plastic_part
5	2	item_0002633_Profil_8_40x40_leicht_L=1600_2	27	1	front_panel_acryl
6	1	lamp	28	1	acryl_middle
7	2	item_0002633_Profil_8_40x40_leicht_L=500_1	29	4	Caster1.25in
8	2	item_0002633_Profil_8_40x40_leicht_L=685_3	30	1	C2C-SA0303XX10000lampsender
16	2	item_0002633_Profil_8_40x40_leicht_L=605_1	31	2	item_0002633_Profil_8_40x40_leicht_L=516_1
17	4	item_0002633_Profil_8_40x40_leicht_L=300_1	32	1	item_0002633_Profil_8_40x40_leicht_L=400_2 (1)
18	3	middle_support_acrill	33	1	C2C-EA0303XX10000lamprceiver
19	1	Emergency Stop Button - Assy	34	2	safe_zone_guard_lateral
20	1	reset_button	35	1	safe_guard_top
21	1	start_button	36	1	safe_guard_right
22	1	power_panel	37	1	safe_zone_conveyor

Designed by	Checked by	Approved by	Date
Salvador Jimenez	S. Rau	J. Wollert	13/02/2017

FH Aachen/CIDESI

Safety demonstrator

Edition

Sheet
11 / 11

Appendix B
SISTEMA Full Report

SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine



Project name: Demo_board

File date: 17/02/2017 03:43:58 Report date: 17/02/2017 Checksum: 317686a469bc1f69b2108f41a8c21400

PR Project name: Demo_board

Author:	Salvador
Dangerous point/machine:	
Documentation:	
Document:	
File name:	C:\Users\Salvador\Documents\SISTEMA\Projects\Demo_Board\Demo_board.ssm
Version of software:	1.1.9 build 2
Version of standard:	ISO 13849-1:2006, ISO 13849-1/Cor1:2009, EN ISO 13849-1:2006, EN ISO 13849-1:2008
Checksum:	317686a469bc1f69b2108f41a8c21400
Options:	<input checked="" type="checkbox"/> Use DC intermediate levels for calculation of PFH (more precise) <input type="checkbox"/> Raise the MTTFd-capping for Category 4 from 100 to 2500 years
Status:	green
Note:	There are no warnings listed for this project (or it's subordinate basic elements).

Contained safety functions

SF Name: Safety-related stop function initiated by E-stop

Required: PLr c

Reached: PL c

PFH [1/h]: 1.14E-6

Status: green



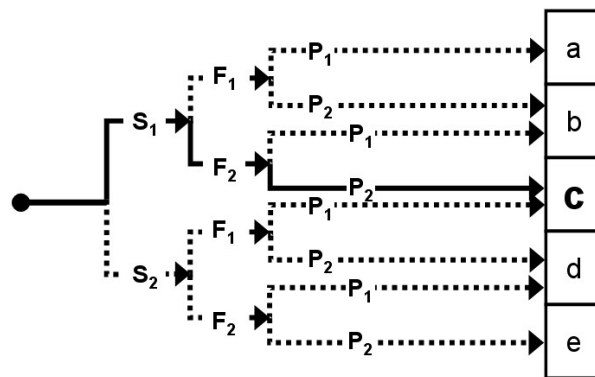
Project name: Demo_board

File date: 17/02/2017 03:43:58 Report date: 17/02/2017 Checksum: 317686a469bc1f69b2108f41a8c21400

SF Safety function: Safety-related stop function initiated by E-stop

Safety function type:	E-stop
Triggering event:	The E-stop is pressed
Reaction:	The dangerous movement will be stopped and unexpected start-up is prevented as long start button is press again
Safe state:	The dangerous movement is stopped (the electrical motor).
Documentation:	
Document:	
Reached PL:	c PFH [1/h]: 1.14E-6
PLr (by risk graph):	c
Severity of injury (S):	Slight (normally reversible) injury
Frequency / exposure times to hazard (F):	Frequent to continuous / exposure time is long
Possibility of avoiding (P):	Scarcely possible

Risk graph:



Status: green

Subsystems:

SB Name: OY001S

PL: c	PFH [1/h]: 1.14E-6
Cat.: 1	Mission time [a]: 20
DCavg [%]: not relevant	CCF Points: not relevant
MTTFd [a]: 100 (High)	

Documentation Subsystem

Documentation: The instructions are part of the unit. They contain information about the correct handling of the product. Read the operating instructions before use to familiarise yourself with operating conditions, installation and operation. Adhere to the safety instructions. Adhere to the specified ambient conditions.

Document: ..\ifm-electronic_operating_instructions\OY001S_OY010S_UK.pdf

Category Subsystem

Documentation/reasoning:

Source (e.g. standard) Category:



Project name: Demo_board

File date: 17/02/2017 03:43:58 Report date: 17/02/2017 Checksum: 317686a469bc1f69b2108f41a8c21400

SF Safety function: Safety-related stop function initiated by E-stop

File:

Requirements of the Category: Basic safety principles are being used. [fulfilled]
 Well-trying components are being used. [fulfilled]
 Well-trying safety principles are being used. [fulfilled]
 MTTFd is High. [fulfilled]
 DCavg is None. [not relevant]

Common cause failure Subsystem

CCF Measures:

Status / Messages Subsystem

Status: green

Channels / Test channels:

CH Name: Channel 1

MTTFd [a]: 6849.32

Blocks:

BL Name: **Emergency stop pushbutton ES11 (Release 2013-07)**

MTTFd [a]: 6849.32 (High) DC [%]: not relevant
 Mission time [a]: 20

Documentation Block

Documentation: Subject to errors and technical modifications. Only the data in the operating instruction of the respective product are binding.
 The stated values are only valid with the assumed cycles per year. An adjustment might be necessary.
 The data applies to the following product family:
 ES11 (surface mount version)

Document:

Status / Messages Block

Status: green

Elements:

EL Name: **mechanical part**

B10d [cycles]: 250000 nop [cycles/a]: 365
 T10d [a]: 684.93 MTTFd [a] (from B10d): 6849.32 (High)
 Mission time [a]: 20
 DC [%]: not relevant



Project name: Demo_board

File date: 17/02/2017 03:43:58 Report date: 17/02/2017 Checksum: 317686a469bc1f69b2108f41a8c21400

SF Safety function: Safety-related stop function initiated by E-stop

Documentation Element

Technology: mechanic

Documentation:

Document:

Diagnostic coverage Element

Documentation/reasoning:

Status / Messages Element

Status: green

Message [Status of Message]:

Elements:

EL Name: electrical part

MTTFd [a]: FE (High) Rate of dangerous failure [FIT]: 0

Mission time [a]: 20

DC [%]: not relevant

Documentation Element

Technology: electromechanic

Documentation:

Document:

Diagnostic coverage Element

Documentation/reasoning:

Status / Messages Element

Status: green

Message [Status of Message]:

Project name: Demo_board

File date: 17/02/2017 03:43:58 Report date: 17/02/2017 Checksum: 317686a469bc1f69b2108f41a8c21400

EXCLUSION OF LIABILITY

Care has been taken in production of the software SISTEMA, which corresponds to the state of the art. It is made available to users free of charge.

Die Software wurde gemäß dem Stand von Wissenschaft und Technik sorgfältig erstellt. Sie wird dem Nutzer unentgeltlich zur Verfügung gestellt.

Die Haftung des IFAs/ DGUV ist damit auf Vorsatz und grobe Fahrlässigkeit (§ 521 BGB) bzw. bei Sach- und Rechtsmängel auf arglistig verschwiegene Fehler beschränkt (523, 524 BGB).

The IFA undertakes to keep its website free of viruses; nevertheless, no guarantee can be given that the software and information provided are virus-free. The user is therefore advised to take appropriate security precautions and to use a virus scanner prior to downloading software, documentation or information.

CONTACT

Institute for Occupational Health and Safety of German Social Accident Insurance (IFA)
Division 5: Accident Prevention / Product Safety
Alte Heerstr. 111, 53757 Sankt Augustin
E-mail: sistema@dguv.de
www.dguv.de/ifa (Webcode e561582)

Date, signature of the revisor

Date, signature of the author