



Funktionales Sicherheitskonzept für eine industrielle Roboterstation

BACHELORARBEIT

zur Erlangung des akademischen Grades

Bachelor of Science

im Rahmen des Studiums

Technische Informatik

eingereicht von

Daniel Bigl

Matrikelnummer 01426652

an der Fakultät für Informatik

der Technischen Universität Wien

Betreuung: Ao.Univ.Prof. DI Dr. Wolfgang Kastner

Mitwirkung: Univ.Ass. DI (FH) Dieter Etz, MBA

Wien, 11. November 2020

Daniel Bigl

Wolfgang Kastner



Functional Safety Concept for an Industrial Robot Station

BACHELOR'S THESIS

submitted in partial fulfillment of the requirements for the degree of

Bachelor of Science

in

Computer Engineering

by

Daniel Bigl

Registration Number 01426652

to the Faculty of Informatics

at the TU Wien

Advisor: Ao.Univ.Prof. DI Dr. Wolfgang Kastner

Assistance: Univ.Ass. DI (FH) Dieter Etz, MBA

Vienna, 11th November, 2020

Daniel Bigl

Wolfgang Kastner

Erklärung zur Verfassung der Arbeit

Daniel Bigl
Karl-IIInerstraße 11
3830 Waidhofen/Thaya, Österreich

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 11. November 2020

Daniel Bigl

Dedication

This work is dedicated in loving
memory of my grandmother to

PhMr. Růžena Musilová

* 19.7.1928 † 19.10.2017

Konání dobra bylo poslání tvoje.

Kurzfassung

Die in Industrie 4.0 verwendeten Systeme sind keine einfachen Dampfmaschinen mehr. Sie sind hochkomplexe entwickelte, automatisierte Systeme teilweise bereits mit künstlicher Intelligenz ausgestattet. Die größten Probleme, welche solch komplexen Systeme verursachen, sind ihr hohes Risiko Menschen entweder direkt oder indirekt zu verletzen. Diese Arbeit beschäftigt sich mit diesen Problemen und erklärt, warum es wichtig ist, funktionale Sicherheit in solchen Systemen zu implementieren. Entsprechend werden auch die üblichen Normen und Methoden, welche für die Entwicklung eines Sicherheitskonzeptes verwendet werden, erläutert. Zusätzlich werden Sicherheitskomponenten und deren Kommunikation behandelt, um zu zeigen, wie die heutige Industrie funktionale Sicherheit in automatisierten Systemen implementiert. Abschließend wird ein funktionales Sicherheitskonzept für eine Roboterstation entwickelt und angewandt.

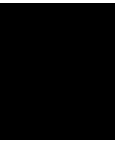
Abstract

In today's world, we not only live in a digital era, but our daily life is getting more and more complex and sophisticated every day. In industry, this development is taken up by the term 'Industry 4.0'. The systems that are used in industry are no longer simple steam engines, but they are also highly developed complex automation systems to some extent equipped with artificial intelligence. The biggest problems which such complex systems create constitute a high risk of damage to the health of people either directly or indirectly. This thesis deals with these problems and explains why it is important to build functional safety into such systems. According to this, the most important norms and methods used for designing safety concepts are discussed. Additionally, various safety devices and their connectivity are dealt with to demonstrate which components today's industry uses to deploy functional safety into automated systems. Finally, a functional safety design for a Robot Station is introduced and applied.

Contents

Dedication	vii
Kurzfassung	ix
Abstract	xi
Contents	xiii
1 Introduction	1
1.1 Motivation	1
1.2 Problem Statement	2
1.3 Aim of the Work	2
1.4 Structure	2
2 State of the Art	3
2.1 Commonly Used Safety Norms	3
2.1.1 IEC 61508	3
2.1.2 IEC 62061	5
2.1.3 EN ISO 13849	5
2.2 Legal Framework	6
2.2.1 European Legal Environment	6
2.2.2 Legal Environment in Austria	7
2.2.3 Legal Environment in U.S.	8
2.3 Risk Assessment	9
2.3.1 EN ISO 12100	9
2.3.2 Safety Integrity Level	10
2.3.3 Performance Level	10
2.3.4 Safety Function	12
2.4 Safety Devices	13
2.4.1 Detection and Ranging Solutions	13
2.4.2 Safety Switches	14
2.4.3 Safety Logic Devices	14
2.4.4 Light Curtain	15
2.4.5 Two-hand Control	16
	xiii

2.4.6	Pullback Devices	16
2.5	Safety Connectivity	17
2.5.1	Discrete Wiring Solutions	17
2.5.2	Specialities in Wiring	17
2.5.3	Ethernet Technologies	19
2.5.4	Challenges in Uniting Miscellaneous Cyber-physical Systems . . .	21
3	Safety Concept for an MPS Robot Station	23
3.1	Laboratory Setup	23
3.1.1	The Robot Station	23
3.1.2	The Computer Engineering Lab	23
3.1.3	Risks During Operation	24
3.2	Requirements	24
3.2.1	Austrian Legal Environment	24
3.3	Risk Assessment	27
3.3.1	Risk Assessment by Means of Performance Level (PL)	27
3.3.2	Safety Function	28
3.4	Safeguarding Devices	28
3.4.1	Active Safeguarding Devices	28
3.4.2	Passive Safeguarding Devices	31
3.5	Design & Implementation	33
4	Summary and future work	39
4.1	Summary	39
4.2	Future Work	40
	List of Figures	41
	List of Tables	43
	Acronyms	45
	Bibliography	47



Introduction

1.1 Motivation

Functional Safety (FS) has become a very important topic in the modern automation industry. Due to the development of highly complex automated systems, a need for competence, effective risk assessment, verification, and validation has come up. In Section 2.1.1, the IEC 61508 [IEC10], one of the most important and commonly used norms, is quoted. Since its publication in 1998, many companies and manufacturers have integrated FS into their project life-cycle as it has become rather a requirement than a recommendation. Also the proof and trip testing topic have become very important as many companies “[...] now use a more rational choice of proof test intervals” [Foo11]. Today, every operating robot or device comes along with a developed Functional Safety Concept (FSC) which guarantees that no damage to people’s health can occur neither directly nor indirectly through damage to property or environment.

There are already a lot of different norms that specify how an FSC has to be developed and realized. But all these regulations have in common that they only offer guidelines between which the FSC has to be developed. Every automation system has different requirements, which results in the need for designing individual safety concepts for each system.

The main focus of this thesis lies in the design and implementation of an FSC to an MPS Robot Station. Therefore, the process and the tools needed for designing a FSC have to be discussed. Furthermore, the different devices and their connectivity are also treated as they are an important part of a FSC.

1.2 Problem Statement

The Automation System Group operates a production line for teaching purposes which has recently been extended by a 6-axis-robot station. A robot is a machine that is capable of carrying out actions automatically, which poses a potential hazard for people. Therefore, to minimize the risk of injuries or damage to human health, it is absolutely essential to develop a FSC before operation.

1.3 Aim of the Work

The work aims to study various norms that are used to build functional safety into today's complex automated systems to get an idea of what is needed for designing a functional safety concept. Furthermore, various technologies and safety devices are considered to be able to make the best choice for the FSC of the MPS Robot Station. After having studied the state of the art and finished the design, the FSC is applied to the robot station.

1.4 Structure

In the beginning, some theoretical background is presented in Chapter 2. This chapter focuses on the state of the art including commonly used safety norms and the legal framework. Furthermore, it is stated how risk management is treated and which safety devices and safety connectivity can be used for implementing functional safety.

Afterward, in Chapter 3, the laboratory setup, the needed requirements, a risk assessment for the laboratory setup and possible solutions are discussed and a functional safety concept for the MPS robot station is designed and implemented as well.

To conclude, Chapter 4 presents a summary including the results of the chosen functional safety concept and gives an outlook for possible future work.

State of the Art

2.1 Commonly Used Safety Norms

Nowadays, there are a lot of different safety norms that are used voluntarily as well as of necessity by the industry to develop new products and to keep existing constructions in accordance with the legal environment. “Manufacturers and suppliers are engaged to enter a mutual Development Interface Agreement (DIA) which forces them to establish and document in detail the safety activities in the concept phase, the development phase, and the production phase” [Hel11]. Although all these safety-related activities are documented in detail and the manufacturer fulfilled all requirements, mistakes can happen. This mistakes can vary from small deviations from the requirements to huge differences of the predefined specifications which could even result in harm of life. In this case, there are laws based on national and European product liability law which refer to this problem. As the legal framework is also a very important part of developing new products - especially in safety-critical applications - it is discussed in more detail in Section 2.2.

In the following sections, only the most important and commonly used norms are briefly discussed to give a short overview. Figure 2.1 shows the fundamental structure of the mentioned norms but does not represent all needed and used norms at all. It more shows the importance of IEC 61508.

2.1.1 IEC 61508

One of the most important and commonly used norms in today’s industry is the IEC 61508 norm published by the International Electrotechnical Commission (IEC). It serves as a base norm to other application-specific norms. Its approach is to define procedures in the development of new products to guarantee that these products are developed by the state of art of technology to bring the risks of injury to humans and the environment

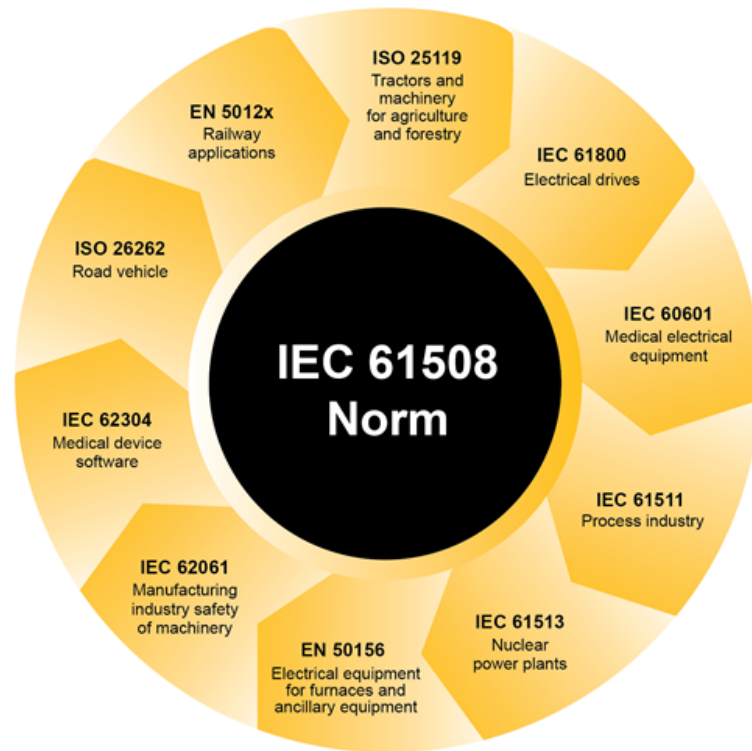


Figure 2.1: Structure of norms [Sin18]

to a minimum. It offers aspects that have to be considered at any point in the so-called product life cycle. That means that the manufacturer has to deal with these aspects from the very first step of the design process through the launch of the product to the taking out of service. Furthermore, the IEC 61508 introduces so-called Safety Integrity Levels (SIL) which are used for the categorization of various safety-related performances and are explained in more detail in Section 2.3. The IEC 61508 can be split into eight different parts where part 0 covers functional safety as it relates to the standard, parts 1-3 are the main sections and parts 4-7 provide supplementary material.

1. General Requirements: it covers general functional safety management, the requirements of the product life-cycle and “the need for competency criteria for people engaged in safety-related work [...]” [Ken11].
2. Requirements for electrical/electronic/programmable electronic safety-related systems: this part of the IEC 61508 deals more with the hardware than with the software aspects of the safety-related system. Requirements concerning the planning, validation, verification, fault tolerance and testing are defined here.

3. Software requirements: as the name already indicates this part deals with the different requirements concerning the design techniques to develop software.
4. Definitions and abbreviations
5. Examples of methods for the determination of safety-integrity levels: this part is subdivided into seven annexes which are more informative than normative. It covers “[...] the general concept of the need for risk reduction through to the allocation of safety requirements [...]” [Ken11], different methods for determining safety integrity levels and presents also alternative approaches.
6. Guidelines on the application of IEC 61508-2 and IEC 61508-3: in this part, some informative material on hardware failure probabilities-, common cause failure- and diagnostic coverage calculations are provided.
7. Overview of techniques and measures: this part “[...] is a reference guide to techniques and measures and is cross-referenced from other parts of the standard” [Ken11].

2.1.2 IEC 62061

Another important norm is the IEC 62061 [IEC05] which deals with the safety of machinery and is derived from the IEC 61508 as shown in Figure 2.1. It is more specific and the focus lies on functional safety of safety-related electrical, electronic and programmable electronic control systems. It provides requirements that are applicable to the system level design of complex and non-complex systems and devices. It concentrates on the application and cannot be used independently for the development of complex safety systems.

The IEC 62061 can be considered as a helpful addition to the evaluation of safety systems in the machinery industry. It more or less answers the question of how a control system that fulfills the requirements of a specific application can be built out of single devices. It only consists of one part and almost cannot be used without the IEC 61508. In contrast to the IEC 61508, it only deals with the aspects of the product life cycle that stand in relation to the allocation of safety requirements up to the validation of safety. Furthermore, it relies on the fact that the used programmable electronic components fulfill the specific requirements of the IEC 61508.

2.1.3 EN ISO 13849

Many devices are controlled by so-called control systems. The development of these comes along with the need for specified design principles. The ISO 13849 [ISO15] follows up with these safety-related design principles and is a successor of the EN 954 norm. Apart from electrical/electronic/programmable electronic safety-related systems, it also deals with the design principles of other control systems like fluid technology. Furthermore, it introduces a so-called Performance Level (PL) which is used for the categorization of

various safety-related performances and which is explained in more detail in Section 2.3. The ISO 13849 can be split mainly into the following parts:

1. Part 1: defines the general principles for the underlying design.
2. Part 2: describes the validation. This means that the safety functions of the safety-related components of the control system are evaluated including analysis and testing.

2.2 Legal Framework

Developing a new product has to be performed in accordance with the legal environment. On one hand, manufacturers are obliged to adhere to national and international laws to protect themselves from legal consequences in the case a specification-conforming product may be faulty and human health or environment is damaged. On the other hand, the user of the product has to be protected from harm. Thus, for better understanding, a short overview of the most important laws and directives in Europe and the United States is given in the following sections.

2.2.1 European Legal Environment

One of the most important documents forming the legal environment in relation to a standardized level of protection for accident prevention is the so-called European Machinery Directive 2006/42/EC [PoEU06]. However, since this directive is based on the European-Community-Treaty, it has no direct impact on member nations and has to be implemented into national laws by the individual member states. The fundamental importance of the European Machinery Directive 2006/42/EC can be derived from the number of member states which adopted large parts of this directive into their national law. Essentially, the European Machinery Directive 2006/42/EC applies to the following products:

- a) “machinery
- b) interchangeable equipment
- c) safety components
- d) lifting accessories
- e) chains, ropes and webbing
- f) removable mechanical transmission devices
- g) partly completed machinery” [PC06]

For being able to determine if the product that is developed fits one of these categories, definitions in more detail are given. Besides, the directive also lists products that are explicitly excluded from it or covered by others.

The European Machinery Directive has existed since 1989, which shows once more the importance of this document. Other substantiating reasons that show how important it is are:

- free movement of goods in Europe
- reduction of local regulations and detailed provisions
- reduction of technical barriers

Originally, it was known as Directive 89/392/EEC, then it was amended by Directives 91/386/EEC and 93/68/EEC. Directive 98/37/EC was created to consolidate the original Directive and its amendments before the latest version - the European Machinery Directive 2006/42/EC - was published in 2006.

2.2.2 Legal Environment in Austria

As Austria is part of the European Union, there are many directives and treaties published by the European Commission that come into effect. But as already mentioned in Section 2.2.1, these directives have no direct impact and have to be implemented into national laws by the individual member states. In Austria, there are mainly three big parts when it comes to legislation:

1. Administrative Law - this kind of law regulates the disciplinary actions before any damage to humans or the environment happens. Thus, this part of legislation includes regulations and laws such as the “Maschinen-Sicherheitsverordnung” [Msv10] that implements the Machinery Directive 2006/42/EC (mentioned in Section 2.2.1) into national law for the most parts. Of equal importance is the “ArbeitnehmerInnenschutzgesetz” [Asc19], which is another part of the administrative law in Austria. This law protects employees and ensures safe workplaces besides many other regulations. It is not possible to list all regulations and laws that are part of the administrative law, however, two more important regulations should be mentioned which are the “Gewerbeordnung” [Gew19] on one hand and the “Arbeitsmittelverordnung” [Amv19] on the other hand.
2. Criminal Law - this legislation part regulates the consequences of inflicted damage. In other words, it deals with the criminal law repercussions. The most important and biggest part of the criminal law is the “Strafgesetzbuch” [StG19] that deals with the legal punishments.

3. Civil Law - this law consisting mainly of the “Allgemeines bürgerliches Gesetzbuch” [Abg20] and the “Allgemeines Sozialversicherungsgesetz” [Asv19], resolves the question who is liable for the damage that happened. As this kind of law deals with compensation payments, the focus lies more on the financial aspect.

2.2.3 Legal Environment in U.S.

It is not surprising that the European Machinery Directive 2006/42/EC has no effect nor in the United States neither Canada. But there are numerous different norms, directives and legal regulations that are similar to those used in Europe although they conform to the national legal framework. In Northern America, machinery safety is ensured mainly by a mixture of product standards, fire codes, electrical codes, and national laws. All in all, there are four main organizations among others that deal with the topic of machinery safety. They are discussed in more detail in the following.

Occupational Safety & Health Administration (OSHA)

Every employer in the United States is obliged to ensure a safe workplace. Especially when it comes to an interaction between humans and machines, this topic gets even more important. As an official agency of the US Department of Employment, the Occupational Safety & Health Administration (OSHA) has to ensure safe workplaces by providing and enforcing different standards and directives. Every employer has to fulfill these requirements to guarantee that no human gets injured at work.

The OSHA-standards can be compared to the European directives as they act as government regulation. A difference is that the OSHA-standards refer more to a safe workplace and the employer, while European directives refer more to machine manufacturers.

American National Standards Institute (ANSI)

Among mandatory standards to which everybody has to comply, there is also some kind of voluntary directives. ANSI-standards are developed by private organizations that are not part of the government. Often the compulsory OSHA-standards make use of voluntary ANSI-standards so that they become mandatory, too.

Underwriters Laboratories (UL)

Requirements regarding electric devices and components are mainly developed and published by the Underwriters Laboratories (UL). These standards mostly deal with risks of fire and risks of electrocution. Many of them have become integrated into ANSI-standards or are even demanded by OSHA-standards. National and listed laboratories are obligated to verify the compliance of the UL-standards if they are demanded by an OSHA-standard. Compared to European standards, it can be stated, that the UL-standards often differ or are even contradicting to the European standards from IEC (International Electrotechnical Commission) or EN (European standards).

National Fire Protection Association (NFPA)

The National Fire Protection Association (NFPA) publishes the National Electrical Code (NEC) [NEC17] and the Electrical Standard for Industrial Machinery (ANSI/NFPA 79) [NFP18]. It is a fact that these standards are not mandatory but often used while constructing new buildings. However, in some states, the compliance of these standards is demanded and verified by local authorities.

2.3 Risk Assessment

Risks and hazards in a machine design that have the potential to cause harm, have to be detected. Therefore, a standardized process and different methods are needed in order to ensure that risk is assessed in a correct way and can be brought to a minimum.

2.3.1 EN ISO 12100

When it comes to risk assessment and risk reduction, the EN ISO 12100 [ISO10] is a very important standard that mainly defines important procedures concerning risk assessment for safety-related systems and safety-related parts of machinery and plant control systems. Risk assessment as a specific aspect of risk management gives design engineers general principles for the manufacture of safe machinery and describes the risk assessment procedures extensively. “The term machinery safety looks at the ability of a machine to fulfill its intended function(s) during its service life, whereby the risk has been sufficiently reduced.” [Mac19] The aim is to define basic hazards to help the engineers to identify relevant and significant hazards such as:

- Mechanical hazards
- Electrical hazards
- Thermal hazards
- Hazards generated by noise
- Hazards generated by vibration
- Hazards generated by radiation
- Hazards generated by materials and substances
- Hazards generated by the neglect of ergonomic principles in the design of machinery

among many other hazards that also can be important for the risk assessment of safety-related systems.

2.3.2 Safety Integrity Level

To assess the level of risk, so-called Safety Integrity Levels (SIL) were introduced. They are divided into four levels and serve as a measurement of performance required for a Safety Instrumented Function (SIF). These functions are realized by a safety circuit that consists of different utilities like sensors and actuators. If the risks in a process are assessed as small, the building safety circuit behind that process has a lower safety integrity level. Naturally, processes that are associated with high risk or hazard like the possible death of a human, are built by a high safety integrity level circuit.

For the determination of a SIL for a specific component, a look on the behavior during a failure has to be taken as well as the calculation of redundant structures. Additionally, the ratio between failures that occur certainly and failures that occur uncertainly has to be determined. The usage of these characteristics leads to the calculation of the probability of failure of the specific component. Together with the consideration of the life cycle process of the component, a SIL according to the norm's requirements can be determined.

Table 2.1 gives a brief overview of the different safety integrity levels. The first column represents the SIL whereby SIL4 represents the highest level of safety integrity and SIL1 the lowest level. The probability of failure on demand in the second column is used to determine the likelihood that a loop will fail when a demand is placed on it. The third column represents the risk reduction factor that indicates the probability of failure for an instrumented function. The risk reduction factor is the inverse of the required probability of failure, which is represented in years.

Safety Integrity Level	Probability of Failure on Demand	Risk Reduction Factor
SIL 4	0.001 % to 0.01%	100,000 to 10,000
SIL 3	0.01 % to 0.1 %	10,000 to 1,000
SIL 2	0.1 % to 1 %	1,000 to 100
SIL 1	1 % to 10 %	100 to 10

Table 2.1: Safety Integrity Levels [Sil18]

While manufacturers are allowed to judge their components with levels one and two, they are not allowed to do so with levels three and four. Therefore, an independent third party has to certify the component independently.

2.3.3 Performance Level

As already mentioned, the Performance Level (PL) is defined in the EN ISO 13849. Like the SIL, the PL is also used to assess the level of risk. It is divided into five levels that represent different, average probability values of hazardous failure of the system per hour.

A risk graph (as shown in Figure 2.2) is used to determine the required PL of the earlier specified SIF.

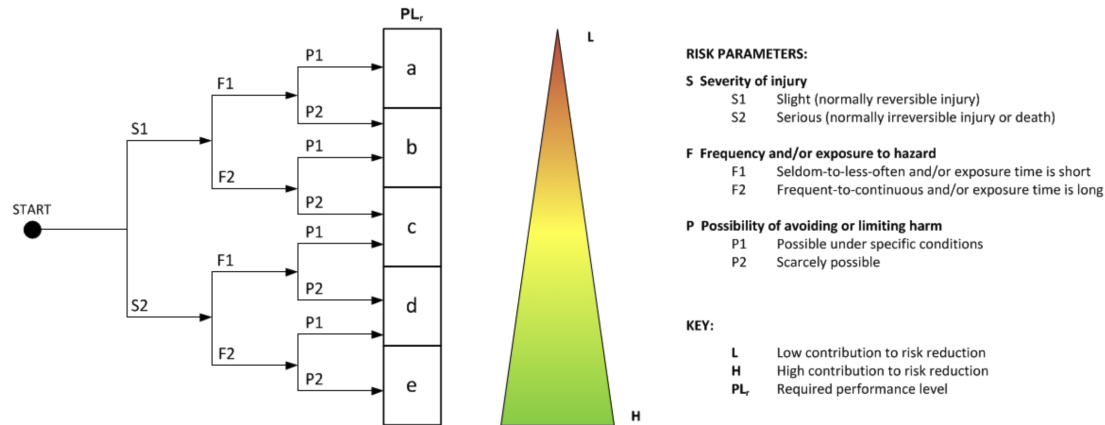


Figure 2.2: Performance Level Risk Graph [Ris14]

The process of determining the PL starts at the “start” node. The first step is to decide if the possible injury is a minor, reversible injury (S1) or a severe, irreversible injury including death (S2). The next step is to decide if the period of exposure to the hazard is rare to frequently (F1) or common to permanent (F2). Last but not least, the possibility of hazard avoidance (P1) or no possibility (P2) has to be determined. Having executed these steps results in a PL from “a” to “e” where “a” corresponds to a low contribution of the control function to the risk reduction and “e” corresponds to a high contribution to risk reduction. Attentive readers surely noticed that “there is clearly a correspondence between the SIL required according to the EN 62061 and the PL required according to EN ISO 13849-1”. [Rob] Table 2.2 shows that SIL3 in the third column is directly equivalent to PL_e in the first column, SIL2 is directly equivalent to PL_d and SIL1 is equivalent to PL_b-PL_c. The second column shows the probability of a dangerous failure per hour. The Safety Integrity Levels (SIL) as well as the Performance Level (PL) are two different but in some way also similar methods to assess the level of risk to eliminate possible hazards by design. “Both standards require the user to follow the same series of steps:

1. Assess the Risks
2. Allocate the Safety measures
3. Design Architecture
4. Validate” [Rob]

Performance Level (PL)	Average Probability of a dangerous failure per hour [1/h]	Safety Integrity Level (SIL)
a	$\geq 10^{-5}$ to $< 10^{-4}$	no special safety requirements
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$	1
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ to $< 10^{-6}$	2
e	$\geq 10^{-8}$ to $< 10^{-7}$	3

Table 2.2: Correspondence between SIL and PL [Rob]

2.3.4 Safety Function

Another important part of the risk assessment is a Safety Instrumented Function (SIF). Functional safety is not only achieved by determining the risks and hazards, but also by implementing some kind of automatic protection. Therefore, safety functions have to be established and their outcome has to be checked.

At the beginning of a design process, every developer has to go through a risk evaluation process as mentioned in the sections above. Then, different safety functions can be derived from this process. Afterwards, the solution of the safety function is “[...] checked and evaluated with hardware and [...] software components until the level of safety integrity specified in the risk assessment has been attained.” [Saf19] Figure 2.3 shows the main three steps that are necessary for a safety function. At the beginning, an input device measures some data for the logic component which checks whether the level of safety integrity has been reached. If so, an output device carries out an action, for example, a power-shut-off action.

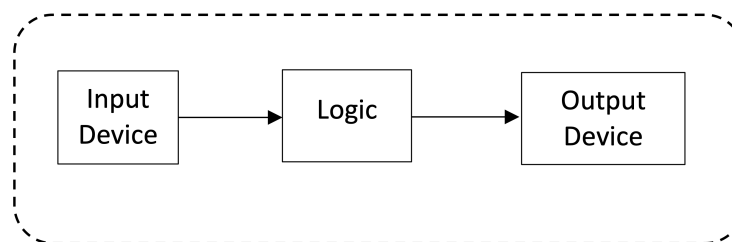


Figure 2.3: Example Safety Function

2.4 Safety Devices

Machine manufacturers have to apply to safety standards like the EN ISO 13849 and EN 62061 as already mentioned in the sections above. Conformity with these directives is achieved by qualitative observations and quantitative aspects whereby functional safety and the safety function play an important part.

For being able to develop a safety concept for a specific system, the needed safety devices have to be treated as they are a very important part of the FSC. Safety devices are a crucial part of the system as their main focus lies on safety. They implement some kind of safety connectivity (which will be discussed in Section 2.5) to guarantee that the communication between sensors and actuators is safe. This also implies that this hardware is always constructed redundantly to achieve a high level of safety. Today's modern industry offers a variety of different safety devices that can be used. Designing a FSC for a system comes along with heavy responsibility also in the decision which safety devices can be used as every specific application has different requirements. For example: think of a simple bench saw. There are a lot of different possibilities how risks and hazards can be minimized. One possibility would be to implement a sensor that checks whether a person is about to hurt themselves and stops the saw immediately. In this approach the sudden stop would result in damage to the saw, which can be very expensive in big industrial plants. Another solution would be to implement a sensor that moves the whole bench saw into a safety area if a person is about to get hurt. Despite this two mentioned approaches, it is maybe enough to stop the saw slowly so that the saw does not get damaged during the emergency stop. As attentive readers will have recognized, different safety-functions (see Section 2.3.4 for explanation) can be derived from the requirements of the application. Thus, there exist different ways how to make the application more safe. The specific use-case defines which approach is the best and which safety-function should be implemented.

In the following sections, only a few safety device technologies are quoted with a focus on the components that were bought for the laboratory of the Automation Systems Group at TU Wien. For the FSC of the MPS Robot Station, which will be also designed in this thesis, a mixture of already existing and needed components will probably be used.

2.4.1 Detection and Ranging Solutions

One important sector of the safety devices portfolio is the possibility of area protection, access protection or other different detection tasks like [...] anti-collision detection in ports, classification in traffic, detection in building automation or position evaluation in navigation [...] [Las18] by laser scanners. The market offers two- or more-dimension scanners which can be used either in indoor or outdoor applications. Apart from that, there are numerous other cases where this technology can be applied. Figure 2.4 illustrates a typical production line setting including a laser scanner. Thus, a safety-function that includes a laser scanner, a logic component and an actuator, is able to protect the operator from getting injured. The laser scanners can detect whether a person is getting close to

a “danger movement area” (yellow marked area in Figure 2.4). In this case, entering the warning field results in a controlled deceleration of the movement while entering the red section results in a complete stop of the process. One advantage of laser scanners is that the process does not have to be completely stopped when a person only gets close to a danger movement area in contrast to light curtains (explained in Section 2.4.4) where an emergency stop of the process is the most used solution. Another advantage is that the yellow area as well as the red area can be configured in accordance with the surrounding area. This is not possible when using light curtains.

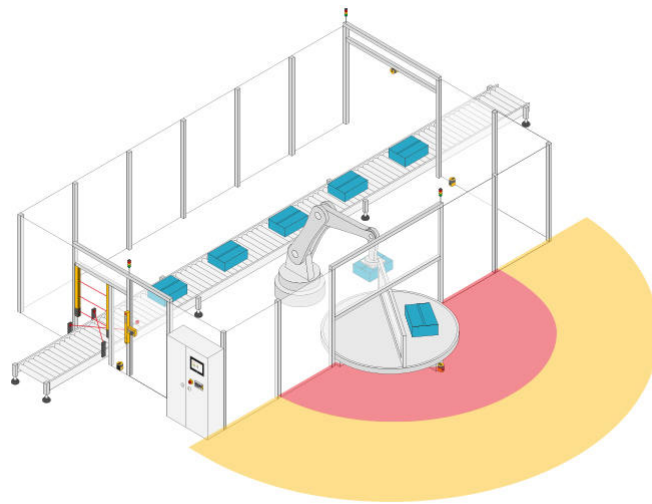


Figure 2.4: Production Line with Laser Scanner [Las19]

2.4.2 Safety Switches

“Safety switches are indispensable in any application where safety is required for people and machinery” [Las18]. In every safety-related system, there must be the possibility to perform a quick, easy and sudden stop. Furthermore, the manner of doing this has to be standardized so that it is obvious how the emergency stop can be performed as a situation where an emergency stop is required is most stressful and dangerous. In the industry, the most used switches are electric-mechanical, non-contact safety switches, safety locking devices, and safety command devices. All these devices have in common that it has to be ensured that connectivity to the application is present at any time. More about this topic will be discussed in Section 2.5.

2.4.3 Safety Logic Devices

For optimum interaction between humans and machine, it is necessary to focus on intelligent and intuitive machine design. To ensure safe communication, so-called

Programmable Logic Controllers (PLCs) and safety relays are needed. They connect safety laser scanners or safety switches with the system. These controller's and relay's advantages are modularity as well as optimum integration into automation processes. They are able to connect a variety of different safety sensors in compliance with the highest Performance Level (PL).

2.4.4 Light Curtain

Another popular way to increase the safety of devices is the installation of a light curtain (also known as light guards or light screens). A sender unit transmits pulses of infrared light beams to a receiver unit. Once there is an interruption of one of these light beams, the light curtain detects this interruption and forwards this information to a logic component which decides what the actuator should do. For example, the device is stopped immediately. When choosing this safety technology, considerations about the placement of the light curtain have to be made as well as a calculation of the right resolution of the curtain. Especially for point-of-operation¹ applications, it has to be ensured that the machine can be stopped before an injury occurs because people are working there close to the hazard. “Additionally, it is also important to consider the size and discreteness of the optical safety device. The device should be able to protect a worker from injury while also maintaining an ergonomic work-space.” [Aar16]

Concerning the resolution of the light curtain, it is important to know what exactly you want to protect. The higher the resolution is, the smaller the parts of a human body are which can be protected. Figure 2.5 shows that with a high resolution of about 14mm between the single light beams, fingers can be protected without a problem while a medium resolution of approximately 30mm may only protect small parts of a human body like hands, and a low resolution of 50mm to 90mm is only able to protect humans as a whole.

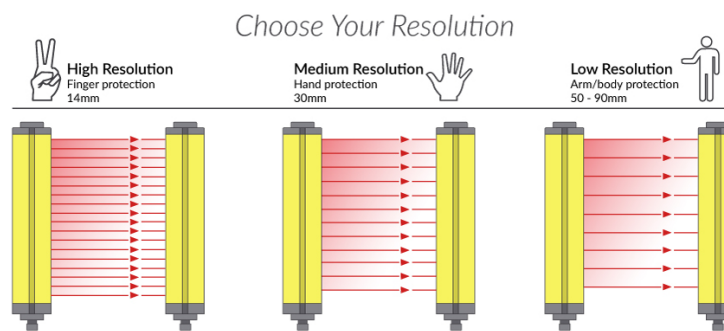


Figure 2.5: Resolutions of Light Curtains [MR19]

¹**Point-of-operation** is the area where the work is performed that is dangerous for the operator of the machine. Therefore, guarding this point-of-operation is critical to protect people from injury or accident.

2.4.5 Two-hand Control

Apart from safety devices in their meaning as physical objects, some methods increase the machinery safety a lot. A very simple method that can be used is the so-called two-hand control. It requires the operator of a machine to constantly press two independent control buttons in order to activate the machine (see Figure 2.6). A simple example showing the principle of a two-hand controlled system are press systems. The operator places the parts that should be pressed in the right position and is only able to activate the press with both hands by pressing the buttons on the two-hand control units. This results in a safe process where no or only very small risk of injury is ensured.

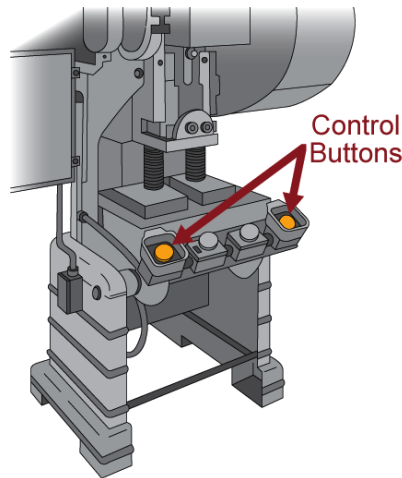


Figure 2.6: Two-hand Control [OSH18]

The design of the unit with the buttons guarantees that the buttons cannot be pressed with only one arm or other body parts. Depending on the surroundings of the device, the control buttons also can be placed in greater distance to the machine so that the user is not able to leave any part of his body in the safety-critical area during operation.

2.4.6 Pullback Devices

Another useful method for preventing damage to the user's health is the pullback method. Devices using the pullback method usually make use of cables that are attached to the operator's hands, wrists or arms as shown in Figure 2.7. When the machine is not running or activated, the user is allowed to access the point of operation. Once the machine starts its process, the pullback mechanism assures the pulling back of the hands from the dangerous area.

As already stated, the quoted safety devices and methods above are only a representation of a huge amount of devices available on the market. For the development of a FSC for a specific device, a variety of safety devices has to be taken into account and the advantages, as well as the disadvantages have to be discussed precisely.

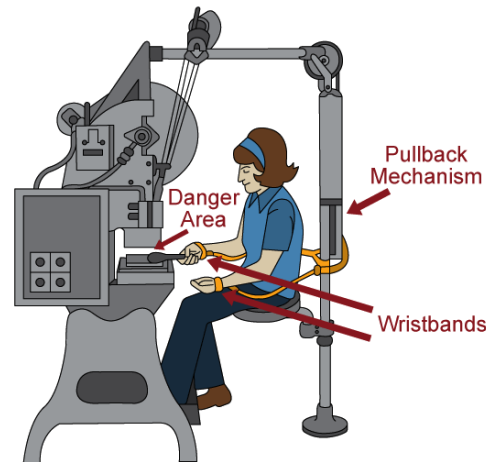


Figure 2.7: Pullback Device [OSH18]

2.5 Safety Connectivity

In this section, the connectivity in safety-critical systems and the different possibilities to ensure safe communication in such a system are discussed in more detail. In contrast to normal systems where safety is not as important as in systems where functional safety is a key issue, not only safety devices are required. The developer has to ensure that communication between all important parts of the system is guaranteed at any time. To achieve such a high level of safety, reliable communication systems are designed by using specially developed protocols and wiring solutions.

2.5.1 Discrete Wiring Solutions

When it comes to the decision which wiring solution is the best for a specific system, different requirements like safety, cost-effectiveness, diagnostics, flexibility, and wiring have to be considered. When connecting a low number of safety devices or connecting devices of different types, individual wiring is a commonly used method. The disadvantage of this method is the very high wiring complexity since every device needs its separate cable. This also limits flexibility as complex wiring makes it difficult to expand. If more devices have to be connected, there are various methods to do so although they mostly come along at high cost. For instance, the devices can be connected with monitored semiconductor outputs. The big advantage of this method is that it has a very high level of safety and immediate fault detection via test pulses of the monitored semiconductor outputs. This method also provides very good diagnostics.

2.5.2 Specialities in Wiring

As safety is a key issue in safety-critical systems, the wiring to safety components like safety switches or safety relays is just as special as many other things in this context.

The designer has to ensure that connectivity between sensors and actuators is given at any time. A loss of connection from an actuator to a sensor immediately has to result in the actuator's state switching from normal operation to a safe state. Therefore, every connection interruption has to be detected and managed properly. Furthermore, the developer has to ensure that all components of the system are correctly connected and that correct operation is not affected by electrical equipment that is connected to the circuit.

When it comes to wiring safety components, not only a broken cable has to be detected. Furthermore, a short-circuit has to be recognized as well. On one hand, it is important to protect safety components from failures that are caused by accidents but on the other hand also intentionally caused failures have to be avoided due to security reasons. The Output Signal Switching Device (OSSD) is a commonly used sensor interface that signals safety-related events reliably. The advantage of the OSSD is that it relies on two completely independent channels that possess the same output information from the device. Setting both lines to a specific voltage implies the idle signal. Periodically the lines are pulsed to 0V asynchronously to ensure that no short-circuit occurred. When both lines are set to 0V, the active signal is issued. Only one line carrying 0V for a duration longer than the test pulses signals an event. To sum up, it is important to know that safety components always have to be wired redundantly to detect broken cables as well as shortcuts in the circuit.

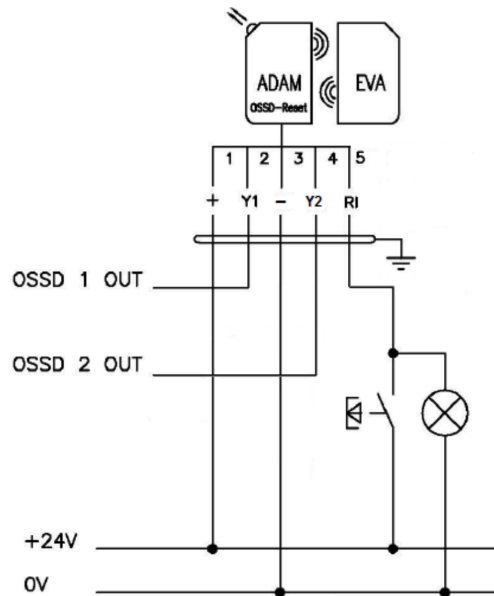


Figure 2.8: Redundant Wiring of Safety Components [Saf17]

For better illustration, Figure 2.8 shows a typical redundant wiring of a safety component. The OSSD 1 and OSSD 2 lines are outputs from a protective device to a safety relay.

As mentioned above, they possess the same output information from the device. The +24V line and 0V line represent the two different voltages that are used for signaling normal operation or an event. Additionally, this Output Signal Switching Device (OSSD) includes a reset light button that is connected to pin 5.

2.5.3 Ethernet Technologies

Ethernet technologies have become more and more important in recent years and are the technology of choice for many future applications. They come along with benefits like integration, flexibility, and decentralization. However, even if using Ethernet technologies, common principles for the transmission of safety-related messages are necessary. Therefore, the IEC 61784-3 [IEC17] was published to introduce standardized safe communication in accordance with the requirements of the IEC 61508. The IEC 61784-3 also recommends to use the so-called “Black Channel Principle” (explained in more detail in Section 2.5.3) to avoid typical message-transmitting errors like repetition of messages, loss of messages, insertion of messages (security reasons), incorrect order of messages, destruction of messages, delay of messages and many more. All protocols that are defined in the IEC 61784-3 use this principle.

Black Channel Principle

The design of safety-related systems has to be made according to norms like the IEC 61508 and IEC 61784. Using Ethernet technologies in these applications forces developers to use the black channel principle as it is based on the requirements for safe communication among participants within a distributed system. It guarantees that typical message-transmitting errors (listed in Section 2.5.3) are reliably detected.

The black channel principle integrates an additional safety communication protocol between the safety application and the “unsafe” default channel of communication (see Figure 2.10). This protocol fulfills the requirements of the used safety norms and detects and controls transmission errors of the underlying communication layers. This means that the integrity of the “unsafe” communication channel is checked constantly by a higher-level safe protocol.

Example of a Safety Protocol using the Black Channel Principle: PROFIsafe

PROFIsafe was one of the first communication standards following the IEC 61508 including standard as well as fail-safe communication. “From the very beginning, it was the intention of PROFIsafe to specify a comprehensive and efficient solution for both the safety device developer and the end-user” [PRO10]. The main method of transmitting messages is transmitting safety messages on the existing standard bus cables in coexistence with the standard messages (see Figure 2.9). Although the safety messages, as well as the standard messages are transmitted on the same bus cable, they have no impact on each other.

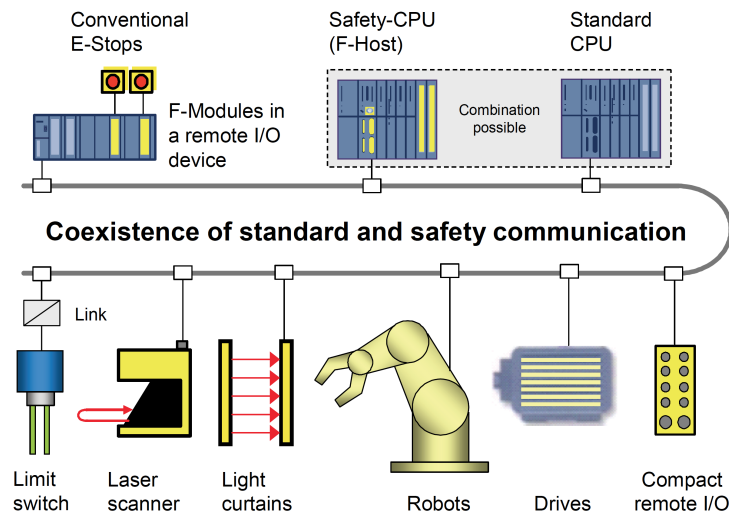


Figure 2.9: Single Channel Approach [PRO10]

This approach results in a reduction potential of needed wiring and the number of parts. It also allows the use of standard PLCs with integrated but logically separated safety processing. Also for users who prefer physical separation of the standard and safety communications, PROFIsafe is a good choice as neither the transmission rates nor the error detection mechanisms have any impact on the standard bus protocols. As shown in Figure 2.10, they are just “Black Channels” for PROFIsafe. The black channel principle is explained in Section 2.5.3.

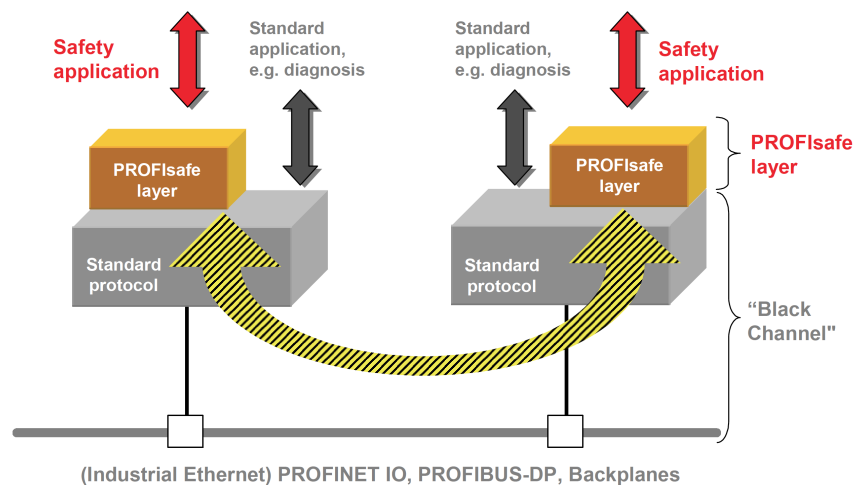


Figure 2.10: Black Channel Principle [PRO10]

Example of a Safety Protocol using Bus Technology with Industrial-Ethernet Wiring: openSAFETY

Another communication protocol for transmitting safety-related data is openSAFETY. Typical uses of this protocol are applications where safety-related data like alerts, triggered for example by the interruption of light beams of laser-scanners, are transmitted. openSAFETY allows transmitting safety-critical information without using an additional wire which is reserved only for this information. This is possible because the protocol uses bus technology with industrial Ethernet wiring. In contrast to other safety protocols that can be only used together with specific industrial Ethernet networks, openSAFETY can be used with numerous solutions theoretically. Unfortunately, the present situation is that openSAFETY can only be used in combination with POWERLINK ².

2.5.4 Challenges in Uniting Miscellaneous Cyber-physical Systems

As in many other sectors, also the automation and functional safety industry faces the big problem of different manufacturers. When it comes to the point of combining products from different manufacturers at the safety level, developers have to deal with many different problems. Although there are a lot of safety directives and norms, they only give direction to new concepts and innovations. In between, there is a “grey area” which can be used by the developers more or less innovatively, which results in inconsistency. Some typical challenges that have to be faced while uniting miscellaneous cyber-physical systems are:

- Various programming languages for the programmable logic controllers
- Additional experts for every specific system are needed
- Common communication protocols are needed and have to be supported by each machine
- Additional hardware for smooth communication is needed

In order to unite different machines from various manufacturers more easily, the IEC 61131 [IEC19] standard for PLCs was introduced by the International Electrotechnical Commission (IEC). This standard, as only one small step to a uniform, worldwide standard, deals with equipment requirements and tests, programming languages, user guidelines, communications and functional safety. Unfortunately, there are numerous implementations and versions that in the end often lead to a discrete wiring solution (see Section 2.5.1) in practice.

²**POWERLINK** is a real-time protocol for standard Ethernet. The main application purpose is the transmission of process data in the automation industry.

Safety Concept for an MPS Robot Station

In this chapter, the status quo is stated. It is explained which robot station is located at the university's laboratory and which risks for people and the environment come along with this station while operating. Furthermore, the legal environment which affects this experimental setup is discussed as well as the possible solutions for implementing a safety concept for this robot station.

3.1 Laboratory Setup

3.1.1 The Robot Station

The MPS Robot station for which a functional safety concept is designed and implemented is part of a manufacturing line (see Figure 3.1) which is located in the Computer Engineering Lab at TU Wien. The lab equipment is used to proof concept implementations when putting research into practice as well as for educational purposes. Precisely, the used robot station is manufactured by the FESTO company following the Machinery Directive 2006/42/EC in compliance with DIN EN 60204-1 and DIN EN ISO 12100. The used robot is a Mitsubishi robot RV-2FB. However, the main part is the Mitsubishi robot arm which is dealt with in this thesis, although the station itself consists of many more parts. Table 3.1 shows some technical data of the robot station.

3.1.2 The Computer Engineering Lab

For better illustration of the room situation, a spatial plan (see figure 3.2) of the computer engineering lab where the robot station is located is given in this subsection. The lab is located in room DEZE40 on the mezzanine floor and highlighted in blue. The given scale

Parameter	Specification
Power supply	230 V AC
Operating pressure	600 kPa (6 bar)
Maximum work-piece width	40 mm
Digital inputs	12
Digital outputs	5

Table 3.1: Technical Data of Robot Station

of 1:150 at the bottom of the figure indicates an approximate size of the room of more or less thirty-seven square meters. The existence of nine computer workplaces minimizes the place that can be used effectively, additionally which results in a higher potential risk of injury as well. A detailed plan of the lab is given in Section 3.5.

3.1.3 Risks During Operation

As shown in Figure 3.1, the manufacturing line is located in the middle of the room without any safety precautions. The room offers nine workplaces and can be entered by several authorized people simultaneously. The attentive reader will have noticed that the simultaneous stay of nine people or more in this small room results in a high potential risk of injury. Therefore, a functional safety concept has to be developed as otherwise, the robot station states a safety hazard for every user or human that enters the room while the station is in action. Due to the arm of the robot station moving around, people can get injured easily.

3.2 Requirements

3.2.1 Austrian Legal Environment

In Section 2.2, the legal framework for implementing functional safety into new products has already been discussed. For the implementation of a FSC for the robot station, the specific legal environment in Austria for this laboratory setup has to be taken into account as we are obliged to adhere to national as well as international laws. The main focus in this section will lie on the “Administrative Law” which was mentioned in Section 2.2.2 as this kind of law regulates the disciplinary actions *before* any damage to people or environment happens.

One very important regulation for this project is the “Maschinen-Sicherheitsverordnung” since its scope of application covers machines that are specially designed for research purposes and are located temporarily in laboratories. Thus, some of its requirements are stated in the following:

1. “§5.(1) The manufacturer or operator of the machine has prior to operation to ensure that

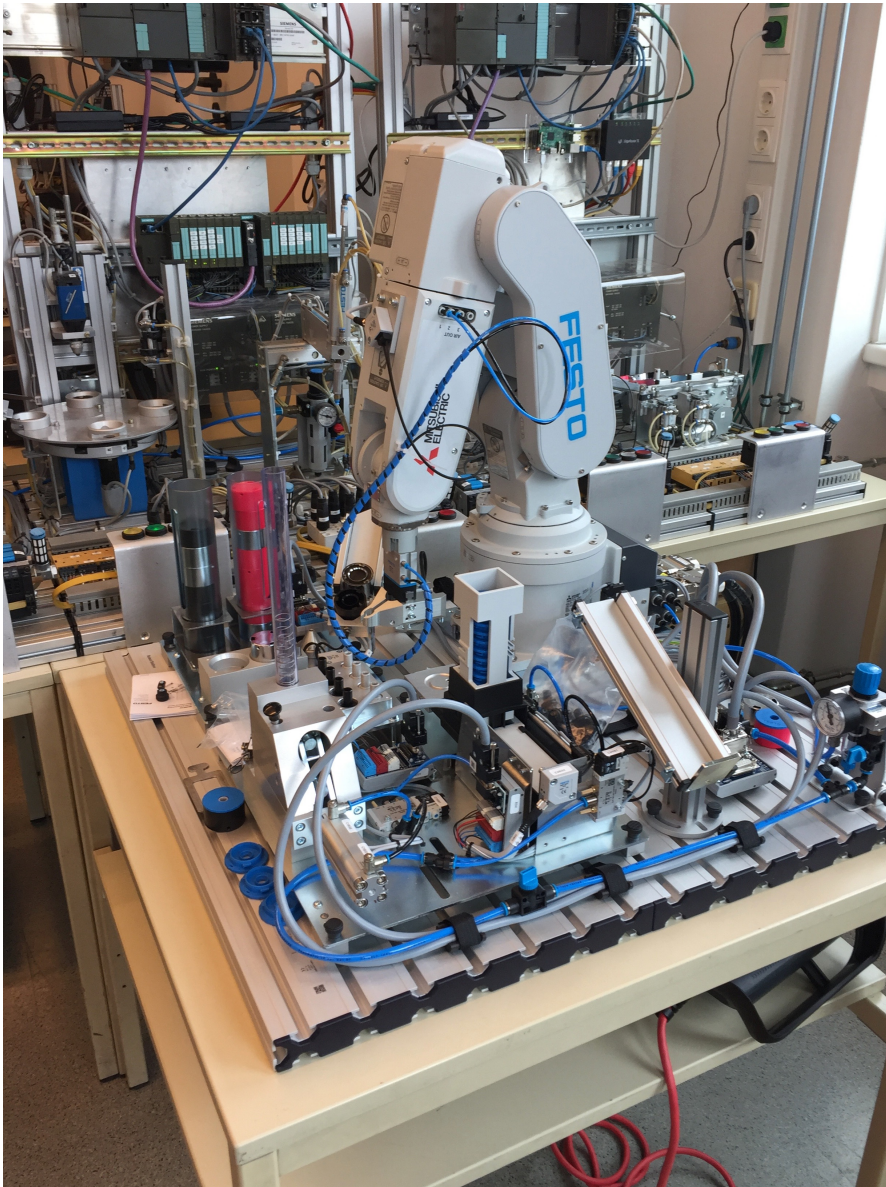


Figure 3.1: MPS Robot Station

- a) the machine complies to the safety and health requirements which are listed in annex I.
- b) the technical documents listed in annex VII section A are available.
- c) the necessary and important information like the operating instructions are available.
- d) the applicable conformity assessment procedures in accordance with §12 are performed.

3. SAFETY CONCEPT FOR AN MPS ROBOT STATION

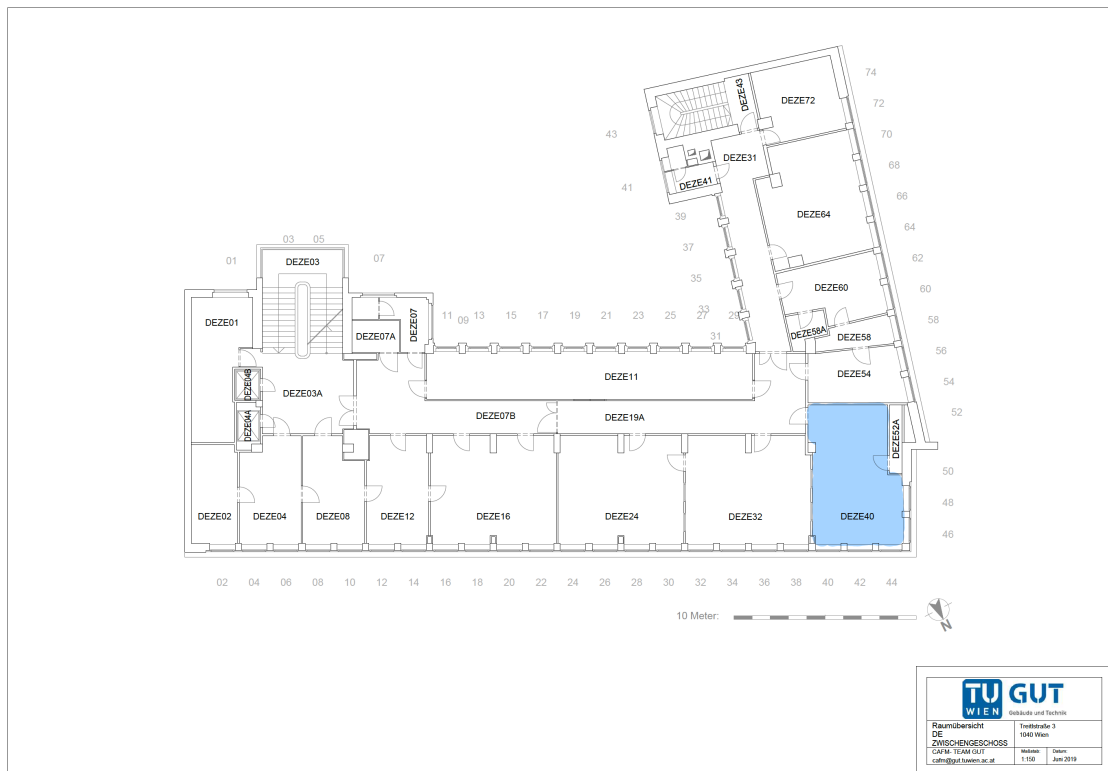


Figure 3.2: Spatial Plan of Computer Engineering Lab [Geb19]

- e) the EC declaration of conformity is issued according to annex II part 1 section A and attached to the machine.
 - f) the CE-label according to §16 is affixed to the machine.” [Msv10]
2. “Annex I, 1.1.2. Principles of implementing safety
 - b) The manufacturer or operator of the machine has to take action to set protections against risks which cannot be eliminated. Furthermore, he or she has to inform the users about the remaining risks due to incomplete effectiveness of the set protections; Indication of special needed education, training and safety equipment.” [Msv10]
 3. “Annex I, 1.2.4.3. Emergency Shutdown

Every machine has to be equipped with at least one emergency stop control device to avoid an immediate or occurring risk of injury.” [Msv10]
 4. “Annex I, 1.3.8. Protection against risks caused by moving parts

The protection device against risks caused by moving parts has to be chosen in accordance with the respective type of risk.” [Msv10]

The above-listed requirements are only a small part of all needed and considered requirements by different laws, regulations and directives. They should represent the most important points for this project that have to be taken into account and do not claim to be complete.

3.3 Risk Assessment

In this section, a risk assessment for the above-mentioned laboratory setup is done. As already stated in Section 2.3, the EN ISO 12100 is a very important standard when it comes to risk management and risk assessment. For being able to perform a risk assessment in accordance with the EN ISO 12100, potential risks caused by the robot station have to be identified and evaluated. According to the level of risk, actions for risk minimization have to be taken. Afterward, a re-evaluation in consideration of the appropriate measures is performed. Concerning risk minimization, the EN ISO 12100 describes mainly three steps to minimize the risk:

- Inherent safe design
- Technical protection measures
- User information (needed if risks remain despite inherent safe design and technical protection measures)

3.3.1 Risk Assessment by Means of Performance Level (PL)

To assess the level of risk of our laboratory setup, Performance Level (PL) which were presented and discussed in Section 2.3.3 are used. They are divided into five levels that represent different, average probability values of hazardous failure of the system per hour. According to the risk graph (as shown in Figure 2.2), the process of determining the PL starts at the “start” node and continues as follows:

1. **Decision between minor or severe injury:** as the hydraulic gripper arm of the robot station operates with relatively high pressures which result in high power, a person’s finger or hand can be injured irreversibly. This fact leads to the S2 edge in the risk graph.
2. **Decision between frequently or permanent exposure to the hazard:** the location of the robot station (more or less public space) and the fact that this robot station is used for scientific purposes results in common to permanent exposure to the hazard as the students or operators who work with this station are nearby and in still interaction with it. In the risk graph, this fact is represented by the F2 edge.
3. **Decision between possibility or no possibility of hazard avoidance:** as the lab can only be entered by people that study or work at TU Wien and this

access is checked by ID-cards, only people that have an educational background in safety-critical topics can enter the room. Additionally, they also get instructed before getting access to the room and this access only lasts for one semester. These points offer the possibility of hazard avoidance under specific conditions and are represented by the P1 edge in the risk graph.

4. **Resulting Performance Level (PL):** putting all the edges of the risk graph that were chosen above together, results in the PL “d”. This means that the contribution of the control function to the risk reduction is rather high. Furthermore, the average probability of a dangerous failure per hour that comes along with this PL is $\geq 10^{-7}$ to $< 10^{-6}$. Compared to Safety Integrity Levels (SIL), the PL “d” is equivalent to a SIL2.

3.3.2 Safety Function

When it comes to a risk evaluation process, safety functions are a key concept. As discussed in more detail in Section 2.3.4, safety functions are derived from those evaluation processes and afterward “[...] checked and evaluated with hardware and [...] software components until the level of safety integrity specified in the risk assessment has been attained.” [Saf19] In other words, “a safety function is a function of a machine whose failure can result in an immediate increase in risk. It [...] is a measure taken to reduce the likelihood of an unwanted event occurring and exposing a hazard.” [Saf10] Therefore, defining a safety function always includes the decision of what has to be done to reduce the risk.

In our case, the main hazard is the exposed robot arm of the robot station as it may cause severe injury during operation. Additionally, the operator is more or less permanent exposed to the hazard. Thus, the main focus of the safety function is to eliminate these risks.

Figure 3.3 shows the structure of the three safety functions that were derived from the requirements. In the beginning, a sensor measures data (e.g. distance from a person to the robot station or if an emergency stop button was pressed) and passes this information to the safety relay. The implemented logic of the safety relay then checks which level of safety integrity has been reached. Depending on this information, the robot controller performs some actions as decreasing movement speed of the robot station or performing an emergency stop. With having determined the required Performance Level (PL) in Section 2.3.3 and identified the safety functions in this section, the define-process of the safety functions is completed and the design-process can start.

3.4 Safeguarding Devices

3.4.1 Active Safeguarding Devices

In the previous sections and chapters, it has been shown that there are numerous approaches to implement functional safety and to design a functional safety concept.

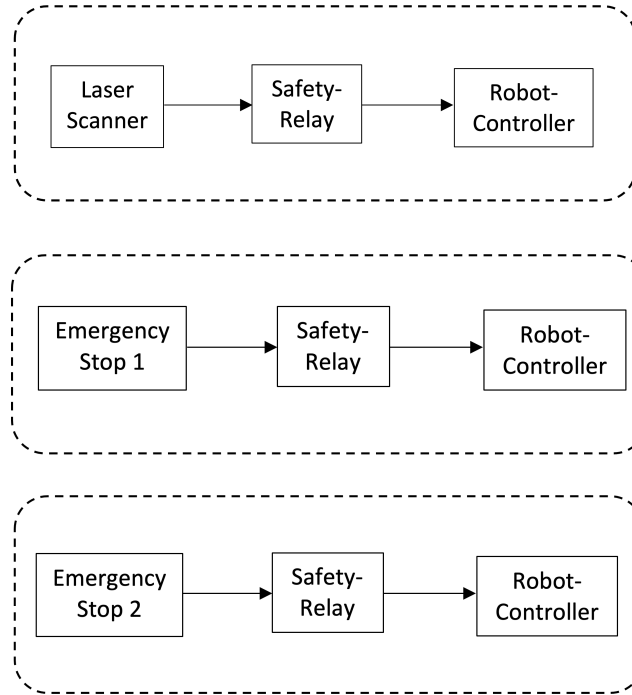


Figure 3.3: Structure of the Safety Functions

Depending on the result of a risk assessment, the right safety device can be chosen in accordance with the legal environment in order to design an FSC. In the following, some possible solutions are listed after all the important aspects for this specific project have been taken into account.

Laser Scanner

First of all, an attempt could be to place a laser scanner onto the existing robot station. Putting the scanner in the right position would result in the ability to slow down or stop the robot station before people enter the critical area where the arm of the robot station is moving. For better illustration, Figure 2.4 was quoted in Section 2.4.1. The biggest advantage of this solution is that the process does not have to be completely stopped when a person only gets close to the “danger movement area.” Only when the operator gets too close, the whole robot station is stopped immediately. Another positive aspect is that in our setup we would only need one laser scanner to monitor the whole critical area, which results in cost-effectiveness. As in many cases, it is always a trade-off between safety and usability. The robot station could have been also positioned behind a pallet cage or a perspex but this would have result in lower flexibility and maintainability. Table 3.2 shows some technical data of the laser scanner that was bought for the Computer Engineering Lab.

3. SAFETY CONCEPT FOR AN MPS ROBOT STATION


Picture	Parameter	Specification
	Operating range warning zone	40m
	Rotation time	30ms
	Selectable resolutions	70mm
	No. of safety zones simultaneous monitored	1
	No. of zones simultaneous monitoring	2
	No. of zone configurations	3
	Ambient temperature	0-50 °C

Table 3.2: Technical Data of Laser Scanner

Safety Relay

Information that is detected by sensors has to be transported somehow to a controller which carries out corresponding actions. Therefore, safety relays or safePLCs are needed as they collect the information from the sensors, evaluate it using the implemented logic and pass it on to an actuator. Additionally, they ensure safe communication between the sensors and the system at any time. The usage of a laser-scanner or an emergency stop button more or less implies the usage of a safety relay. Table 3.3 shows some technical data of the safety relay that was bought for the Computer Engineering Lab.


Picture	Parameter	Specification
	Number of configurable I/Os	8
	Number of digital inputs	12
	Positive switching 1-pole SC output	4
	Number of test pulse outputs	4
	Supply voltage (V)	24,0V
	Supply voltage type	DC
	Ambient temperature	0-60 °C

Table 3.3: Technical Data of Safety Relay

Light Curtain

Another approach could be the implementation of light curtains. They are just like laser scanners a popular way to increase the safety of devices as described in Section 2.4.4. If light curtains were applied to our robot station, injury of humans could be also avoided but this solution would come along with some disadvantages compared to laser scanners. First of all, light curtains either stop the machine once there is an interruption of a light beam or not. They are not able to monitor the critical area in the same way as laser scanners do. Thus, a deceleration of the process would only be possible if more light curtains at different distances to the point-of-operation were implemented. Since this solution in our setting is not possible due to too little space, light curtains are not the best solution for this FSC.

3.4.2 Passive Safeguarding Devices

In contrast to active safeguarding devices, there are also those which do not detect risks actively. A risk reducing action is only performed when it comes to a violation of defined rules (e.g. person touches the robot arm).

Delimitation & Barrier

The most simple way to reduce the risk of injury would be to cover the critical area with some kind of fence or a cage. The big advantage of these solutions is that usually, they are much cheaper than complex electric or electronic devices. Though, they are very impracticable because such barriers affect the workflow. Further, they have to be removed every single time when maintenance or repair come up. Thus, this solution is not the best for our FSC.

Cover Solutions

Another approach that was amongst others developed by the Blue Danube Robotics company is the use of covers. The idea is to cover those parts of a robot station that can injure a human with a “skin”. So the robot is able to detect collisions and triggers an emergency stop once a human or an object gets in touch with the skin. It is also possible to install different pads which make the so-called “Airskin” very flexible in use. Furthermore, it is easy to install and maintain - even by untrained operators. For better illustration, Figure 3.4 shows a picture of a covered robot arm. Unluckily, the “Airskin” is not available for our specific robot station which results in in-feasibility for our FSC.

Emergency Stop Button

As almost every safety-critical system contains emergency stop buttons, the usage of those is feasible in any case. The biggest advantage of emergency stop buttons is that they can also be operated or rather triggered by untrained personnel, children, old- or disabled people. Also, the worldwide identical look of a yellow plate or housing with a red



Figure 3.4: Airskin Cover [Rob18]

button makes this device familiar to numerous people. The functionality of emergency buttons was discussed in Section 2.4.2 and Section 2.5. Table 3.4 shows some technical data of the laser scanner that was bought for the Computer Engineering Lab. Finally, it should be mentioned that the positioning of an emergency stop button is very important and will be discussed in detail in Section 3.5.


Picture	Parameter	Specification
	Release type	rotational
	Actuator	pushbutton
	Self-monitored	yes
	Ambient temperature	-25-55 °C

Table 3.4: Technical Data of Emergency Stop Button

Signal Tower

Typically, industrial as well as other big plants come along with the installation of a signal tower for a specific part of the plant or the whole plant on its own. Using signal towers, the operator can check or verify the state of a system visually. Problems are detected easily and quickly which ensures rapid processing of the problem. Table 3.5 shows some

technical data of the signal tower that was bought for the Computer Engineering Lab.


Picture	Parameter	Specification
	Supply voltage (V)	24,0V
	Supply voltage type	DC
	Power consumption DC	5,0W
	Lamp	LED
	Ambient temperature	-20-50 °C

Table 3.5: Technical Data of Signal Tower

3.5 Design & Implementation

After having discussed the needed requirements, the laboratory setup and performed a risk assessment, the selected safety devices and the design for the FSC are briefly stated in this section. After comparison and consideration of numerous devices and opportunities including their advantages and disadvantages, a laser-scanner in combination with a safety-relay, a robot controller and emergency stop buttons will be used. Additionally, also a signal tower will be used in order to show the operator the state of the robot station.

For better illustration, a detailed plan of the Computer Engineering Lab is given in Figure 3.5. The attentive reader will recognize that the exact positioning of the used components is also indicated in the plan.

To minimize the risks of injury that were stated in the risk assessment in Section 3.3.1, the implementation of three safety-functions was realized. The first safety-function includes a scanner that is positioned approximately thirty centimeters above the ground at the corner of the robot station's desk and monitors the narrow space in front of the robot station at an angle of 275°. If a person enters the yellow marked area (see Figure 3.5) the robot controller decreases the robot station's operating speed. Entering the red marked area results in an emergency stop. As mentioned in Section 3.4.2, almost every safety-critical system contains emergency stop buttons. Thus, the two other implemented safety-functions include emergency stop buttons in order to have the possibility to perform an emergency stop by people who are not familiar with the robot station and its functionality. The emergency buttons can be easily identified due to their distinctive yellow case and red button. Triggering these buttons results in an immediate complete stop of the robot station. For better visualization of the robot station's state, a signal tower is positioned at the top of the production line (see Figure 3.5) so that it can be seen from every place in the room. It contains three colors whereby the color green indicates

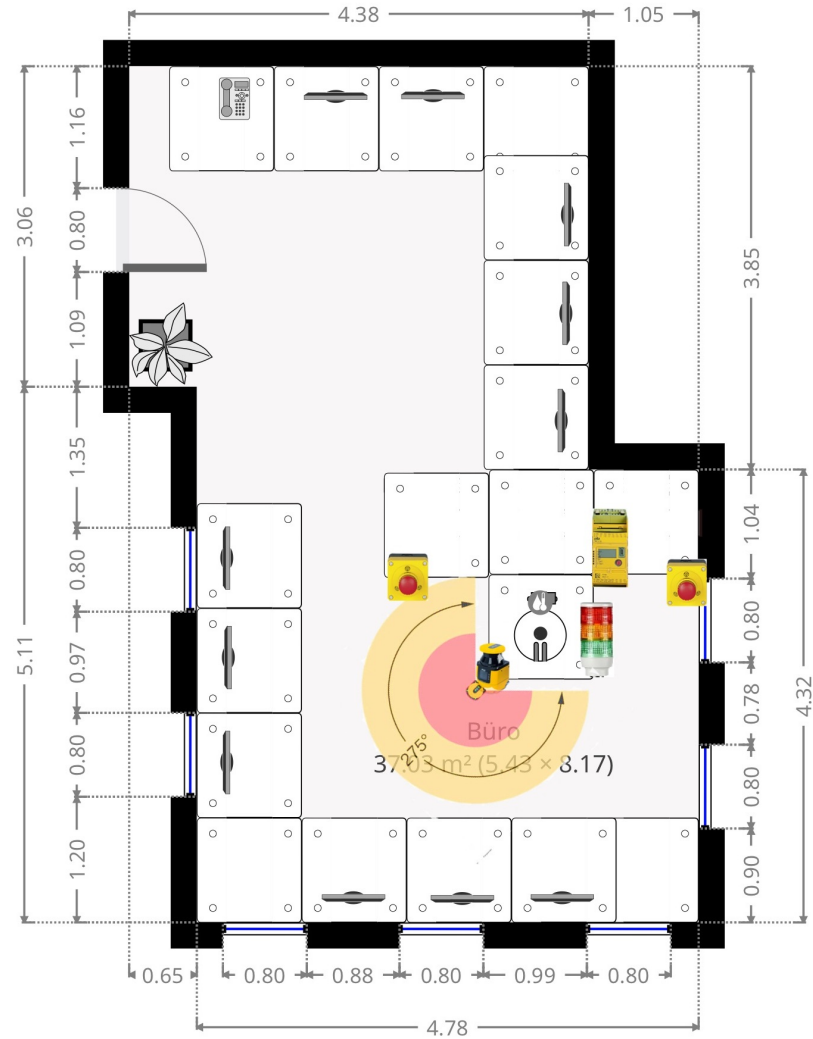


Figure 3.5: Computer Engineering Lab

normal operation of the robot station, the color yellow indicates a warning (someone is getting too close to the robot arm and the operating speed is reduced) and red indicates a stop of the process.

In Section 2.4.3 and 3.4.1, it was shown that safety relays are needed to ensure safe communication between safety sensors like a laser-scanner or an emergency button and the “brain” of a system which is often a controller. In Figure 3.3, the flow of information from the sensor to the safety relay which also includes logic that checks the safety-functions and to the robot controller can be seen. Since we use a laser-scanner and emergency stop buttons in our FSC, the need for a safety relay is given. For our design, we use a

safety relay with the technical data from table 3.3. In order to perform specific actions, also a controller is needed which controls the robot station. As shown in Figure 3.3 the robot-controller is the last part of the information flow and carries out actions that correspond to the sensor's measured data.

As the connection and the wiring of all the needed components is also of importance when it comes to correct and safe operation, it is briefly explained in Figure 3.6. It can be seen that all safety devices are connected redundantly to the safety relay as described in Section 2.5.2. The safety relay then checks if the connected safety components work properly and if a safe connection is ensured. In the case that any of the safety devices indicates a problem which should result in an emergency stop, the safety relay handles this information according to its implemented logic (will be explained in the following) and forwards the information about the emergency stop to the robot controller of the robot station. The robot controller then performs an emergency stop and reduces the operating speed of the robot station to zero. The state change of the robot station from normal operating mode to reduced operating speed mode or emergency stop is also indicated on the signal tower as explained above. Therefore, the signal tower is also connected directly to the safety relay. To perform a reset in order to switch the robot station back to normal operation mode after an emergency stop, a reset on the robot controller has to be performed by pushing a specific reset button. Additionally, also the reason that triggered such an emergency stop must be resolved (e.g. person has to leave the danger area). If the emergency stop was triggered by the detection of a broken cable of the redundant wiring of one of the safety devices, the device has to be replaced by a new and correct functioning one, before a reset can be performed.

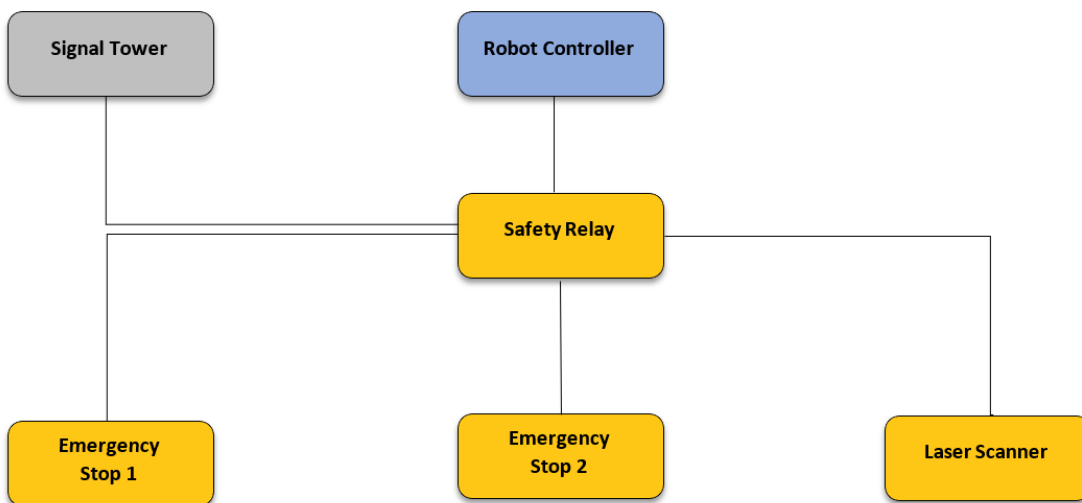


Figure 3.6: Connection of Safety Components, Safety Relay and Robot Controller

As described above, all the components that are important to ensure safe operation are

connected to the safety relay which forwards information to the robot controller on the ports O0 and O1 (see Figure 3.7). The ability of the safety relay to decide whether all components work properly or not is induced by some logic that is implemented and loaded on a chip card which is inserted into the safety relay. The advantage of this chip card is that in the case the safety-relay gets defect, the chip card only has to be inserted into a new safety-relay and the same configuration can be loaded and used. To create such a configuration, the PNOZmulti Configurator 10.11.0 from Pilz GmbH & Co. KG was used in order to implement the needed functionality of the used safety relay. Figure 3.7 shows a schematic block diagram of the used safety devices and the underlying logic. As can be seen, the first two blocks on the left side are the two installed emergency buttons. They are connected to the safety relay on pins IM0 and IM1 (respectively IM2 and IM3) via two different cables to ensure redundant wiring as described in Section 2.5. Thus, the safety relay is able to distinguish between a broken cable or an emergency stop that was really triggered by pressing the button (interrupt of both cables) - although both cases result in an emergency stop. Therefore, the internal logic of the emergency stop blocks is quite simple. The block checks whether both inputs (two cables of emergency stop button) are on high state. If so, no cable of the emergency button is broken and the button is not pressed. This means that the output of the block is on high state which indicates that the emergency button that is connected to this block works properly. The indication for a broken cable is given by one of the inputs being on low state while both inputs being on low state indicates a press of the emergency stop button. In both cases, the output of the block is low which results in an emergency stop of the robot station. The same logic also applies for the second emergency stop button. In the case the emergency stop was triggered intentionally, the robot controller only has to be reset and normal operation is ensured again whereby a broken cable of a safety device results in the exchange of this device before normal operation is possible again.

The next block indicates whether someone has entered the danger area. If so, again an emergency stop is triggered but this time automatically. The wiring is again done redundantly to the pins I4 and I5 of the safety relay. The logic of this block can be compared to the logic of the emergency stop buttons as high state on both inputs indicate that nobody has entered the danger area. In this case, the block output is on high state which results in normal operation of the robot station (assuming that the output of the emergency stop blocks is also high). Both inputs on a low state indicate that a person has entered the danger area and an emergency stop is triggered. Only one input on low state indicates a broken cable which also results in an emergency stop as correct functioning of the laser scanner cannot be ensured anymore. In this case, the laser scanner has to be exchanged before the robot station can be reset again. If the emergency stop was triggered by a person who entered the danger area, the robot controller can be reset after the person has left the danger area and the robot station functions normally again.

As the emergency stop buttons and the laser scanner detection in the danger area are safety-critical and all of them lead to an emergency stop, they are connected together by an “AND” block which is followed by a message block that triggers a message on the

safety-relay's display. In other words this means that the robot station is only moving if all emergency stop buttons are redundantly connected to the safety relay, no emergency stop button is pressed and the danger area is clear.

The last block on the left side indicates whether someone has entered the warning area. This event results in the activation of the yellow light on the signal tower and in a low state of the block's input which triggers also a low state on the output. As this feature is assessed as not safety-critical, the wiring this time is not done redundantly as mentioned above. Once the person who entered the warning area leaves this area again, the green light on the signal tower is illuminated again which indicates normal operation of the robot station. Also the input of the block is put on high again which also results in the output being in high state again.

The explained blocks of Figure 3.7 which are located on the left-hand side, are followed by logical blocks that implement a trivial logic for the correct output of the signal tower. The attentive reader will find them in the middle of figure 3.7. The green blocks on the right-hand side represent the corresponding output blocks for the three lights of the signal tower. The output for the red light is on port IM18 whereby the output for the yellow light is on port IM16 and the output for the green light is on port IM17.

The implementation of the safety relay as performed in this thesis, only allows the functionality of an emergency stop. The reduction of the robot arm's operating speed when someone enters the warning area, is indicated on the signal tower via the yellow light but the speed by now is not reduced. This is owed due to the fact that all the outputs of the safety relay are occupied as the signal tower is connected to it.

3. SAFETY CONCEPT FOR AN MPS ROBOT STATION

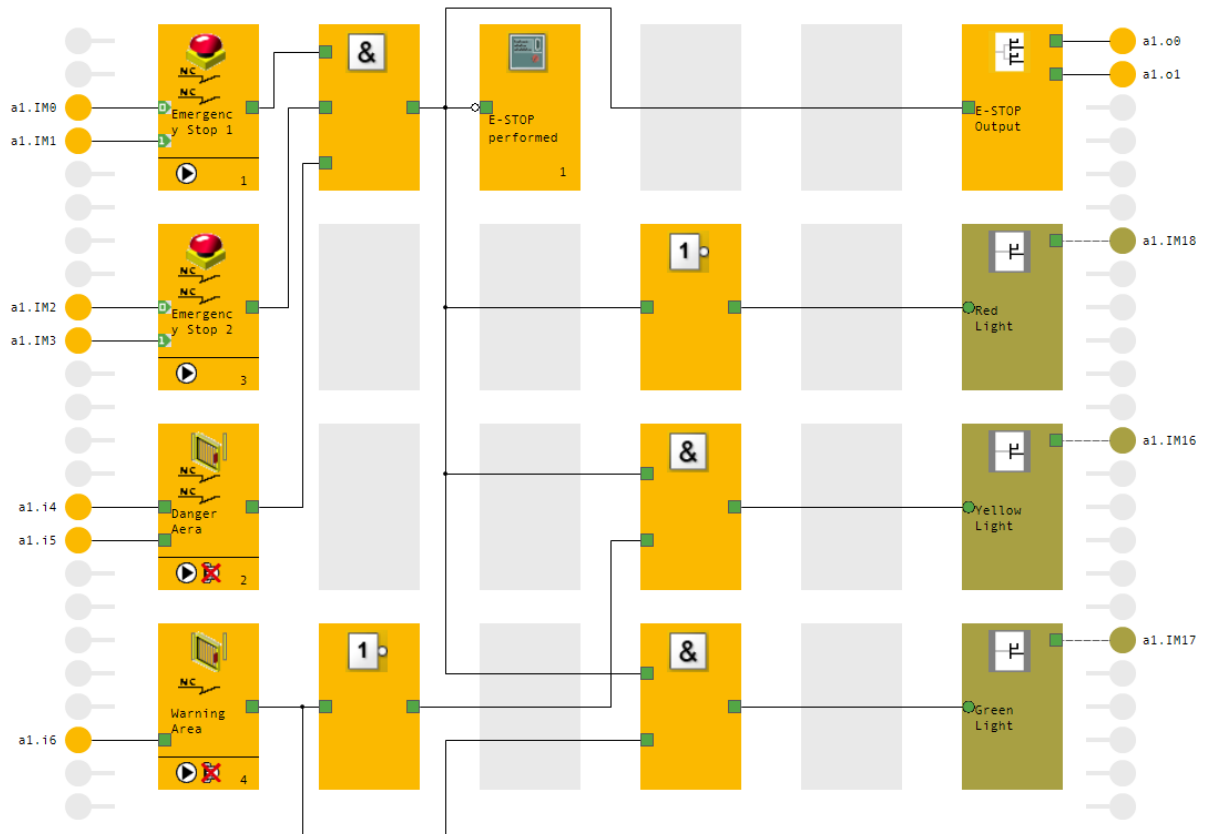


Figure 3.7: Implemented Configuration of Safety Relay

Summary and future work

4.1 Summary

In this thesis, a state of the art research concerning functional safety has been performed and afterwards a functional safety concept for a robot station has been designed and implemented. Therefore, the most important norms that come along with the design of a functional safety concept like IEC 61508, IEC 62061 and EN ISO 13849 have been studied and discussed. As the development of a new product always has to be performed in accordance with the legal framework, the European legal environment and the legal environment in Austria have been discussed as well as the legal environment in the United States.

After having defined the points that are needed for the design from a legal perspective, the next step was to take care about risk assessment. Risks and hazards in a machine design that have the potential to cause harm, have to be detected. Therefore, EN ISO 12100 standard has been stated and commonly used procedures and techniques for risk assessment and risk reduction have been presented. Furthermore, it has been stated how risk management is treated and which safety devices and safety connectivity can be used for implementing a functional safety concept.

In the last chapter of the thesis, the status quo has been stated first. The environment where the robot station is located has been explained and potential risks have been pointed out. Subsequent, the important sections of the Austrian legal environment that come into effect, have been discussed. The needed risk assessment has been performed by means of performance levels and three safety functions have been derived. Appropriately to the result of the risk assessment, also the decision on safety devices has been made.

According to the preliminary discussions, a functional safety concept for the MPS Robot Station has been designed, implemented and discussed in detail. With this newly created

concept, the functional safety of the robot station was increased. Thus, the risk of injury for people who operate the robot station has been reduced drastically.

4.2 Future Work

The designed functional safety concept only integrates the absolutely needed safety devices and standards. Therefore, in future work it would be interesting to improve the concept by adding even more functionality. As the reduction of the robot arm's operating speed is indicated on the signal tower but not performed yet, it would be interesting to implement this feature. Therefore, the signal tower control would need to be outsourced from the safety relay to the robot controller. In this case, more outputs of the safety relay would become free and the signal that indicates the speed reduction could be forwarded to the robot station. Since safety is a very important topic when it comes to saving human lives or reducing the risk of injury, the industry offers a lot of possibilities and devices how safety can be improved.

Another interesting idea would be to extend the functional safety concept to the whole production line in which the robot station represents only a small part.

List of Figures

2.1	Structure of norms [Sin18]	4
2.2	Performance Level Risk Graph [Ris14]	11
2.3	Example Safety Function	12
2.4	Production Line with Laser Scanner [Las19]	14
2.5	Resolutions of Light Curtains [MR19]	15
2.6	Two-hand Control [OSH18]	16
2.7	Pullback Device [OSH18]	17
2.8	Redundant Wiring of Safety Components [Saf17]	18
2.9	Single Channel Approach [PRO10]	20
2.10	Black Channel Principle [PRO10]	20
3.1	MPS Robot Station	25
3.2	Spatial Plan of Computer Engineering Lab [Geb19]	26
3.3	Structure of the Safety Functions	29
3.4	Airskin Cover [Rob18]	32
3.5	Computer Engineering Lab	34
3.6	Connection of Safety Components, Safety Relay and Robot Controller	35
3.7	Implemented Configuration of Safety Relay	38

List of Tables

2.1	Safety Integrity Levels [Sil18]	10
2.2	Correspondence between SIL and PL [Rob]	12
3.1	Technical Data of Robot Station	24
3.2	Technical Data of Laser Scanner	30
3.3	Technical Data of Safety Relay	30
3.4	Technical Data of Emergency Stop Button	32
3.5	Technical Data of Signal Tower	33

Acronyms

DIA Development Interface Agreement. 3

FS Functional Safety. 1

FSC Functional Safety Concept. 1, 2, 13, 16, 24, 29, 31, 33, 34

IEC International Electrotechnical Commission. 3, 21

OSSD Output Signal Switching Device. 18, 19

PL Performance Level. xiv, 5, 10–12, 15, 27, 28, 43

PLC Programmable Logic Controller. 15, 20, 21

SIF Safety Instrumented Function. 10–12

SIL Safety Integrity Levels. 4, 10–12, 28, 43

Bibliography

- [Aar16] Aaron Woytke, Aaron Schulke. Light curtain or safety laser scanner? How to choose an optical safety device. SICK AG, 2016.
- [Abg20] Allgemeines bürgerliches Gesetzbuch für die gesammten deutschen Erbländer der Österreichischen Monarchie. Bundesrecht, 2020.
- [Amv19] Arbeitsmittelverordnung - AM-VO. Bundesrecht, 2019.
- [Asc19] Arbeitnehmerinnenschutzgesetz – ASchG. Bundesrecht, 2019.
- [Asv19] Allgemeines Sozialversicherungsgesetz – ASVG. Bundesrecht, 2019.
- [Foo11] Gulland W. G., Foord A. G., editor. *Ten years of IEC 61508; Has it made any difference?*, volume 156 of *Hazards XXII*. IChemE, 2011.
- [Geb19] TU Wien - Gebäude und Technik. Raumübersicht DE, 2019.
- [Gew19] Gewerbeordnung 1994 - GewO 1994. Bundesrecht, 2019.
- [Hel11] Dr. Ekkehard Helmig. Functional safety – dealing with independency, legal framework conditions and liability issues. SGS TÜV Saar, 2011.
- [IEC05] Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems. International Electrotechnical Commission, 2005.
- [IEC10] Functional safety of electrical/electronic/programmable electronic safety-related systems. International Electrotechnical Commission, 2010.
- [IEC17] Industrial communication networks - Profiles - Part 3: Functional safety field-buses - General rules and profile definitions. International Electrotechnical Commission, 2017.
- [IEC19] Programmable controllers. International Electrotechnical Commission, 2019.
- [ISO10] Safety of machinery - general principles for design - risk assessment and risk reduction. Austrian Standards International, 2010.

- [ISO15] Safety of machinery – safety-related parts of control systems. International Electrotechnical Commission, 2015.
- [Ken11] David J. Smith, Kenneth G.L. Simpson. *Safety critical systems handbook : a straightforward guide to functional safety : IEC 61508 (2010 edition) and related standards, including process IEC 61511, machinery IEC 62061 and ISO 13849*. Butterworth-Heinemann, 2011.
- [Las18] Product portfolio. https://www.sick.com/at/en/c/PRODUCT_ROOT, 06.12.2018.
- [Las19] Sicherheits-Laserscanner PSENscan. <https://www.pilz.com/de-DE/eshop/00106002197131/PSENscan-Sicherheits-Laserscanner>, 19.09.2019.
- [Mac19] EN ISO 12100 - Principles for the manufacture of safe machinery. <https://www.pilz.com/en-DE/knowhow/law-standards-norms/iso-standards/mechanic-construction/en-iso-12100>, 09.09.2019.
- [MR19] Maria Martinez-Rodriguez. Safety light curtains: One way to safeguard your machines. <https://trimantec.com/safety-light-curtains-q-a/>, 24.04.2019.
- [Msv10] Maschinen-Sicherheitsverordnung 2010 – MSV 2010. Bundesrecht, 2010.
- [NEC17] National electrical code. National Fire Protection Association, 2017.
- [NFP18] Electrical standard for industrial machinery. National Fire Protection Association, 2018.
- [OSH18] OSHAcademy. Introduction to machine guarding. *Course 726*, 2018.
- [PC06] The European Parliament and Council. European Machinery Directive 2006/42/EC 42, 2006.
- [PoEU06] European Parliament and Council of European Union. Directive 2006/42/ec of the european parliament and of the council, 2006.
- [PRO10] Profisafe system description – safety technology and application. PROFIBUS Nutzerorganisation, 2010.
- [Ris14] Decoding ranking systems related to industrial safety. SICK AG, 2014.
- [Rob] Stewart Robinson. SIL or PL? What is the difference? TÜV SÜD Product Service.
- [Rob18] Blue Danube Robotics, 2018.
- [Saf10] Safety and functional safety - A general guide. ABB, 2010.

- [Saf17] ABB Jokab Safety. Eden OSSD Coded non-contact safety sensor. ABB AG, 2017.
- [Saf19] Application of the Safety Standards EN ISO 13849-1 and EN 62061. <https://www.industry.siemens.com/topics/global/en/safety-integrated/machine-safety/safety-standards/tabcards/pages/safety-standards.aspx>, 19.09.2019.
- [Sil18] Overview of safety integrity level. <https://instrumentationtools.com/overview-of-safety-integrity-level/>, 13.11.2018.
- [Sin18] Jatinder (JP) Singh. IEC 61508 diagram. <http://www.latticesemi.com/en/Blog/2018/02/02/00/07/ImportanceofFunctionalSafety>, 06.02.2018.
- [StG19] Strafgesetzbuch – StGB. Bundesrecht, 2019.