Heikki Ihainen

Machine safety: Risk assessment and safety design

Type of the work Thesis
Spring 2019
School of Technology
Automation Engineering

SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree programme: Automation Engineering

Specialisation: Electrical Automation

Author: Heikki Ihainen

Title of thesis: Machine Safety: Risk Assessment and Safety Design

Supervisor: Niko Ristimäki

Year: 2019 Number of pages: 40

The purpose of this thesis was to provide fully functioning safety applications for machine builders. These safety applications were aimed to be used by the Machine Safety marketing team of Schneider Electric.

The theory part concentrated on the basic knowledge of machine safety. Some of the most common components used in this thesis were handled. Also the basic terms and values of safety were explained.

The practical part studied five different machines from are the perspective of their performance in normal operation. The risks of the machines were defined and explained how their safety functions are working. In the case of one safety function the whole calculation was studied. In this thesis safety modules and modular safety controller were used as processing devices in the applications.

Keywords: machine safety, safety, application

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikan yksikkö

Tutkinto-ohjelma: Automaatiotekniikka

Suuntautumisvaihtoehto: Sähköautomaatio

Tekijä: Heikki Ihainen

Työn nimi: Machine Safety: Risk Assessment and Safety Design

Ohjaaja: Niko Ristimäki

Vuosi: 2019 Sivumäärä: 40

Opinnäytetyön tarkoituksena oli luoda toimivia valmiita turvaratkaisuja koneenrakentajille. Nämä turvaratkaisut suunniteltiin käytettäviksi Schneider Electricin Machine Safety Marketing tiimin myynnin tukena.

Teoriaosuudessa keskityttiin kertomaan yleisesti koneturvasta, siihen liittyvistä termeistä ja arvoista. Tässä osuudessa käytiin läpi myös koneturvaan liittyviä yleisimpiä komponentteja joita opinnäytetyössä käytettiin.

Käytännön osuudessa tehtiin riskienarviointi jokaisen opinnäytetyöhön tehdyn koneturvaratkaisun osalta sekä esiteltiin hieman tarkemmin yhden turvafunktion turvalaskelmat. Turvaratkaisuissa keskityttiin käyttämään prosessointiyksikkönä turvamoduuleja sekä modulaarista turvakontrolleria.

Avainsanat: koneturva, turvallisuus, applikaatio

TABLE OF CONTENTS

Terms and Abbreviations

CCF	**Common Cause Failure**
DCavg	**average Diagnostic Coverage**
EN	**European standards**
IEC	**International Electrotechnical Comission**
ISO	**International Organization for Standardization**
MTTFd	**Mean Time To dangerous Failure**
PFHd	**Probability of dangerous Failure per Hour**
PL	**Performance Level**
PLr	**Required Performance Level**
SIL	**Safety Integrity Level**
SILr	**Required Safety Integrity Level**
SS1	**Stop category 1**
STO	**Safe Torque Off**

Tables, Figures and Pictures

1 Introduction

Schneider Electric Automation GmbH is a multinational company which is a part of Schneider Electric that has revenue of 24.7 billion Euros and employs over 142000 people worldwide. The headquarters of Schneider Electric is located in Paris, France and it is listed in Paris Stock Exchange. (Schneider Electric a.)

The company was established in 1836 by Adolphe and Eugene Schneider. First it concentrated on heavy industry railroads, shipbuilding and steel. After the First World War Schneider Electric started to expand to electricity business which is the core business of the company now-adays. (Schneider Electric 2005.)

This thesis was made in Marktheidenfeld, Germany where is Schneider Electric Automation GmbH headquarters of Machine Solutions and System Consistency. In Marktheidenfeld there are working approximately 400 people from over 26 countries. (Schneider Electric b.)

1.1 Background

This thesis was made to help Machine Safety Marketing team to show how capable products safety module and Modular Safety controller are for machine builders.

Machine safety is a growing part in the more and more automated world and in many work environments people need to work with different kind of machines and thus the machine safety factor becomes really important in work safety. In this written part the risk evaluation is in the largest role of the thesis because if that part of the machine building is done poorly, the machine can easily became hazardous for the machine user or someone who needs to work closely with the machine.

In this thesis five different applications were built in machine safety kind of view using all the safety related components and tested by inserting different kinds of risks to the applications, collecting the data and then making safety calculations with Sistema calculation tool.

2 Machine safety

A machine builder is responsible for the safety of the machine. The machine builder needs to make a risk assessment for the machine and to examine all the standards and safety criteria which concern the machine and then follow them when building the machine. The risk assessment includes determining every risk that a machine could possibly cause, seriousness and probability of each risk. The risk assessment is done with every interest group which are working with the machine. In this section different safety principles are explained. (Schneider Electric 2009.)

In the graphic below the evaluation process that need to be done with every machine which is built. First thing is to determine limits of the machine and how it moves. Then all the risks needs to be identified that the machine causes. Next risks are estimated how often they occur and evaluated how severe they are. Last the machine is evaluated if it is safe enough to use or if it needs more risk reduction. Risk reduction is made with safety related components, limiting the zone where operator can enter. (Schneider Electric 2009.)

2.1 Basic principles

The general principles of machine safety are given in the standard EN ISO 12100. It gives a basis for the set of standards which are divided in to three types.

Type-A standards are about the general principles, designs and concepts of machinery.

Type-B standards have been divided into two subtypes: B1 is about certain safety aspects for example safety distances or noise. B2 include standards for different kind of safety devices, for example emergency stops or two-hand control.

Type-C standards are made for particular machinery like grinding machines or hydraulic presses. (Schneider Electric 2009.)

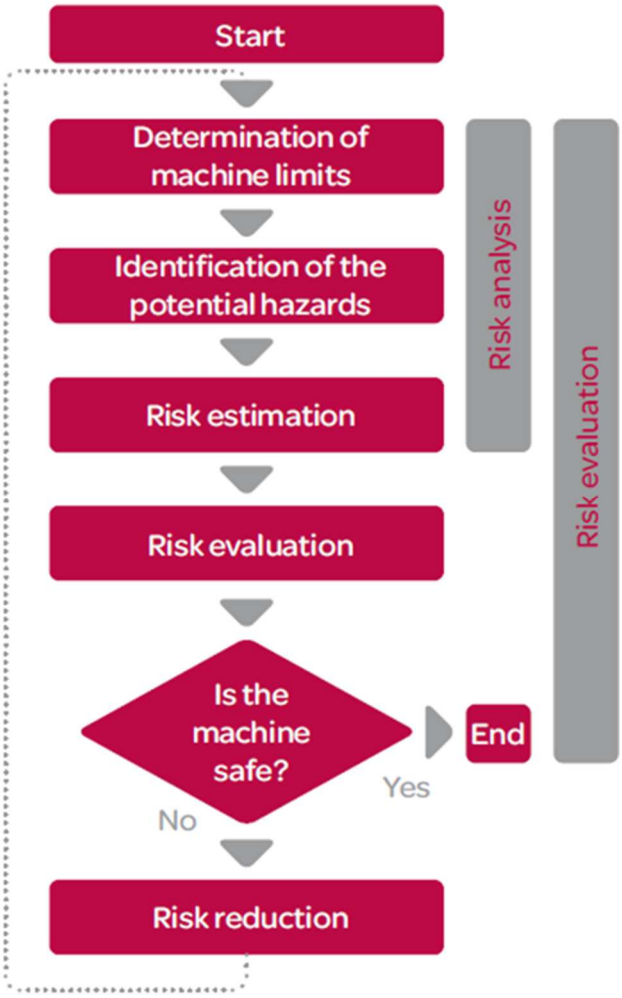


Figure 1 Risk evaluation (Schneider Electric 2009).

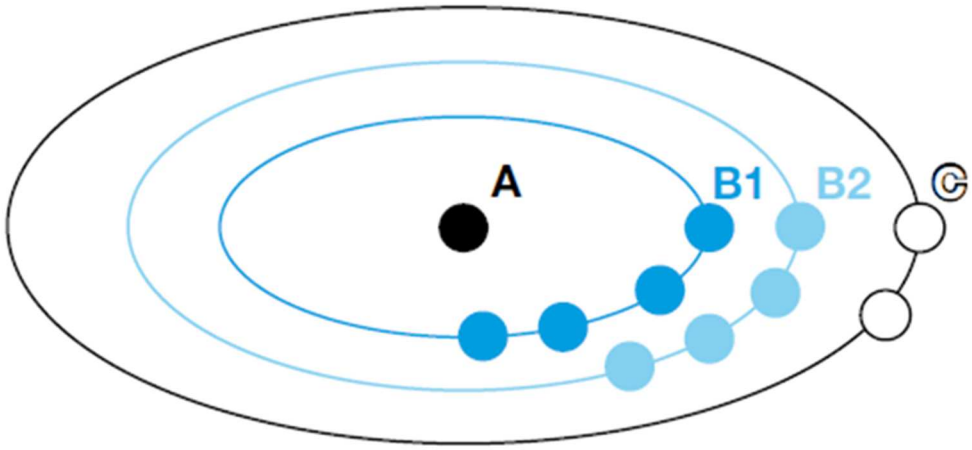


Figure 2 EN ISO 12100 standard types (Schneider Electric 2009).

2.2 Functional safety

Before functional safety, there was the standard EN 954-1 which was replaced by EN ISO 13849-1. This standard is a combination of Mean Time To Dangerous Failure (MTTFd), Diagnostic Coverage (DCavg) and architecture categories which determine performance Level (PL) of safety functions. Then there is a standard EN IEC 62061. It describes safety on three different Safety Integrity Levels (SIL). Levels are defined by the Probability of a dangerous Failure per Hour (PFH_D). The table below show how the two standards are related to each other. (Schneider Electric 2009).

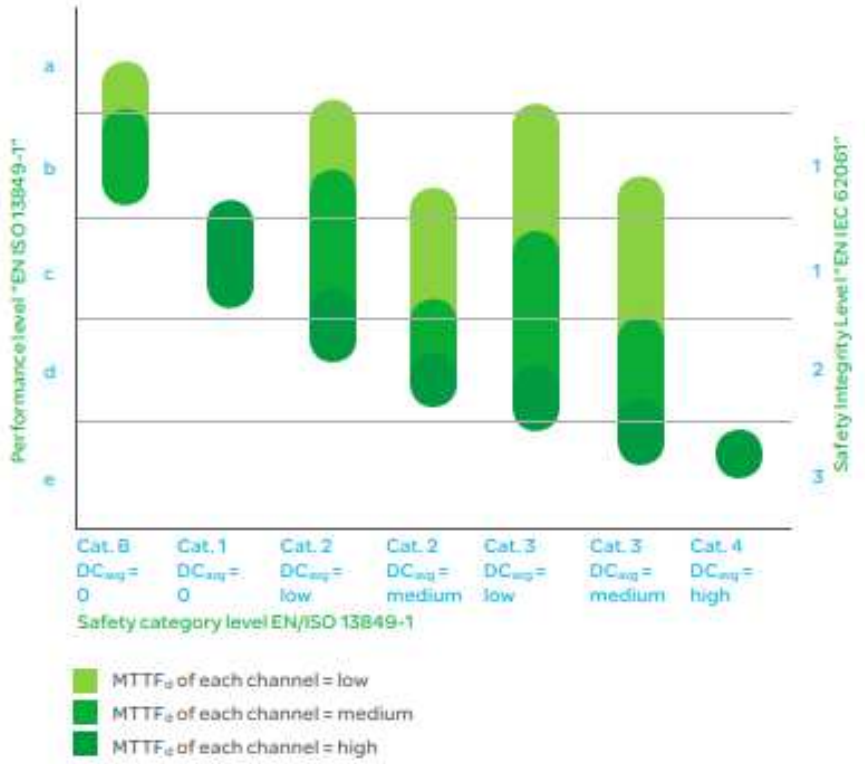


Figure 1 Comparison of PL and SIL (Schneider Electric 2009).

In EN ISO 13849-1 to attain different categories certain $MTTF_d$ and DC_{avg} values are required. For category B, $MTTF_d$ has to be between 3 to 29 years, CCF is not considered and DC_{avg} can be under 60%. Category B does not require any particular safety features. Next category 1 requires well-tried components to be used, CCF is not considered, $MTTF_d$ has to be 30 to 100 years but the DC_{avg} can still be under 60%. In categories 2 and 3, $MTTF_d$ can be 3 to 100 years which is lower than in category 1 because at these levels the DC_{avg} needs to be 60-98% and safety functions must be checked at suitable intervals also CCF is considered and have to be over 65 points. In category 3 safety functions have to be built so one fault

happening in the safety function does not cause loss of the safety function for example if one contactor is malfunctioning there is still second one to ensure that the function works. In category 4, $MTTF_d$ has to be 30 to 100 years, DC_{avg} 99 to 100%, CCF is considered and is has to be over 65 points and also safety functions have to be monitored so that every fault is detected before the loss of the safety function. Below is a table which is used to calculate CCF. (Siirilä 2008, 296-303).

Table 1.Common Cause Failure score table (EN ISO 13849-1).

Table F.1 — Scoring process and quantification of measures against CCF

No.	Measure against CCF	Score
1	**Separation/ Segregation**	
	Physical separation between signal paths, for example: — separation in wiring/piping; — detection of short circuits and open circuits in cables by dynamic test; — separate shielding for the signal path of each channel; — sufficient clearances and creepage distances on printed-circuit boards.	15
2	**Diversity**	
	Different technologies/design or physical principles are used, for example: — first channel electronic or programmable electronic and second channel electromechanical hardwired, — different initiation of safety function for each channel (e.g. position, pressure, temperature), and/or digital and analog measurement of variables (e.g. distance, pressure or temperature) and/or Components of different manufactures.	20
3	**Design/application/experience**	
3.1	Protection against over-voltage, over-pressure, over-current, over-temperature, etc.	15
3.2	Components used are well-tried.	5
4	**Assessment/analysis**	
	For each part of safety related parts of control system a failure mode and effect analysis has been carried out and its results taken into account to avoid common-cause-failures in the design.	5
5	**Competence/training**	
	Training of designers to understand the causes and consequences of common cause failures.	5
6	**Environmental**	
6.1	For electrical/electronic systems, prevention of contamination and electromagnetic disturbances (EMC) to protect against common cause failures in accordance with appropriate standards (e.g. IEC 61326-3-1). Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers' requirements concerning purity of the pressure medium. NOTE For combined fluidic and electric systems, both aspects should be considered.	25
6.2	Other influences Consideration of the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards).	10
	Total	**[max. achievable 100]**

Total score	**Measures for avoiding CCF[a]**
65 or better	Meets the requirements
Less than 65	Process failed ⇒ choose additional measures

[a] Where technological measures are not relevant, points attached to this column can be considered in the comprehensive calculation.

2.3 Emergency stop and stop categories

For emergency stop there is a standard ISO 13850:2015, which is a B2-type standard. Emergency stop is needed in almost every machine. The main reason why machines need

an emergency stop is if the normal stop function is not easily reachable for the operator using the machine. Emergency stop needs to be always red and the surroundings yellow. For emergency stop two stop categories can be used stop category 0 or stop category 1. (EN ISO 13850.)

Stop category 0 STO is the most common stop category. When safety function is enabled energy is switched off from the actuator and it freewheels to stop.(EN ISO 13850.)

Stop category 1, SS1. This category is most commonly used in devices with high inertia. When stop function is enabled the drive which controls the actuator starts ramp down by drive slowing down the machine in a controlled manner. After standing still the drive changes to STO. (EN ISO 13850.)

3 Input devices

Input devices in case of machine safety mean devices which prevent the machine user or other persons from getting hurt or getting killed by the machine or devices that are used for stopping the machine when hazardous event occurs. For many devices, there is a particular standard for example for two-hand control devices there is EN 574. (Schneider Electric 2009.)

3.1 Emergency stop pushbutton

Emergency stop pushbutton cuts the contact when pushed and the device always needs to lock to stop position where machine is being stopped and the machine should not start when the emergency stops is returned to normal the state. Still it should be possible to run the machine manually so that the possible victim can be saved quickly. (Siirilä 2008, 206-218.)

Figure 2 Emergency stop pushbutton XALK178 (Schneider Electric c).

Emergency rope pull switch is a different kind of emergency stop but the basic principles are the same. Rope pull switch is operated with rope which is located near the machine that is attached to switch that will cut contact from the circuit and cause emergency stop. (Siirilä, 2008.)

Figure 3. Emergency rope pull switch XY2CEDA296

3.2 Interlocking guard with a shaped actuator

For interlocking guards there is a type B2 standard ISO 14119:2013 which states the principles of the design and selection of the interlocking devices with guards. Interlocking guards are built for preventing access to hazardous area temporarily and they are used with machines which take a long time to stop. Unlocking guard can be controlled by timer that controls opening the interlock automatically or with manual opening function. (EN ISO 14119.)

The interlocking guard with a shaped actuator has two parts, shaped actuator which is inserted to the interlock which changes the state of the device. Actuator can also be locked so that the guard can not be opened by mistake. (Schneider Electric 2009).

Figure 4 Interlocking guard XCSLE2525312 (Telemecanique Sensors)

3.3 Magnetic switch

Magnetic switch is a same kind of device like an interlocking guard without the locking guard. The function of the magnetic switch is to detect un-authorized access to hazardous area preventing dangerous events. (Telemecanique Sensors.)

In a magnetic switch there is an actuator part which has moving contacts or solid-state relays. The state of the actuator is changed by a magnetic part which is moved closer to the actuator or removed from the actuator. (Telemecanique Sensors.)

Figure 5. Coded magnetic switch XCSDMP5012

3.4 Enabling device

Enabling devices are used in machines where it is necessary to observe the operation close to the moving parts which might cause dangerous situation. Normally enabling switches are used for maintenance and machine setup. (Schneider Electric 2009.)

3.5 Enabling switch

Enabling switch is normally a device which is operated by one hand and has a 3-stage pushbutton. A machine is allowed to run only in the middle stage when the switch is pressed but not squeezed till the end and if squeezed till the end (3-stage) switch need to be released in order to make it run again in the middle stage. (Schneider Electric 2009.)

3.6 Two hand control

Two hand controls are used for the machines where machine operator need to stay away from the moving machine. The two hand control can be used by only using two hands. The standard EN 574+A1 states the functional aspects for two-hand control devices. (Schneider Electric 2009.)

3.7 Speed monitoring

Speed monitoring is used to ensure the working speed of machine. If speed is not in set limits the speed monitoring device detects it. In this thesis safe limited speed it means that machine is allowed to work in slow speed even machine user can enter the working area. Speed monitoring is carried out normally with speed monitoring modules. (Schneider Electric. 2015b.)

4 Processing devices

Processing devices are devices which are monitoring signals from input devices and then controlling output devices with the given parameters. In this thesis three different kind of processing device has been dealt with. (Schneider Electric 2009.)

4.1 Safety Modules

Safety modules are safety processing devices which control one safety function, for example emergency stop or light curtain. Some modules can be used for many different safety functions but only one at a time. Modules are simple and don not require any programming. If necessary they are configured by wiring or potentiometer. (Schneider Electric 2015a.)

4.2 Modular Safety Controller

Modular Safety Controller is a controlling device for multiple safety functions. The Modular Safety Controller which is used in this thesis can work as a standalone with 8 safety inputs and 2 two-channel safety outputs. This can be expanded to 128 inputs and 16 safety outputs with expansion modules. There is also safe speed monitoring modules the controller and one is used on application in this thesis. The Modular Safety Controller can be connected with other modules by a bus or up to six islands by safe expansion bus. For the communication between a PLC and a controller it is possible to use non-safe communication modules. (Schneider Electric 2015b.)

4.3 Safety PLC

Safety PLC is made for more complex systems with multiple safety functions and safety stop categories. In normal a PLC, voltage is coming straight from the source that cannot be monitored by the PLC if a short circuit occurs. Also in a safety PLC outputs are monitored and there are two different outputs used for the same device to ensure the power to be cut off. In a normal PLC outputs are working independently without monitoring. In a normal PLC there

only one microprocessor which executes the commands, but in a safety PLC there is another one which is monitoring the other processor. (Schneider Electric 2017.)

5 Output devices

Output devices execute the stop function which is controlled by a processing unit. Normally output devices are contactors, servo drives, frequency converters or safe-torque-off starters. (Schneider Electric e.)

5.1 Contactor

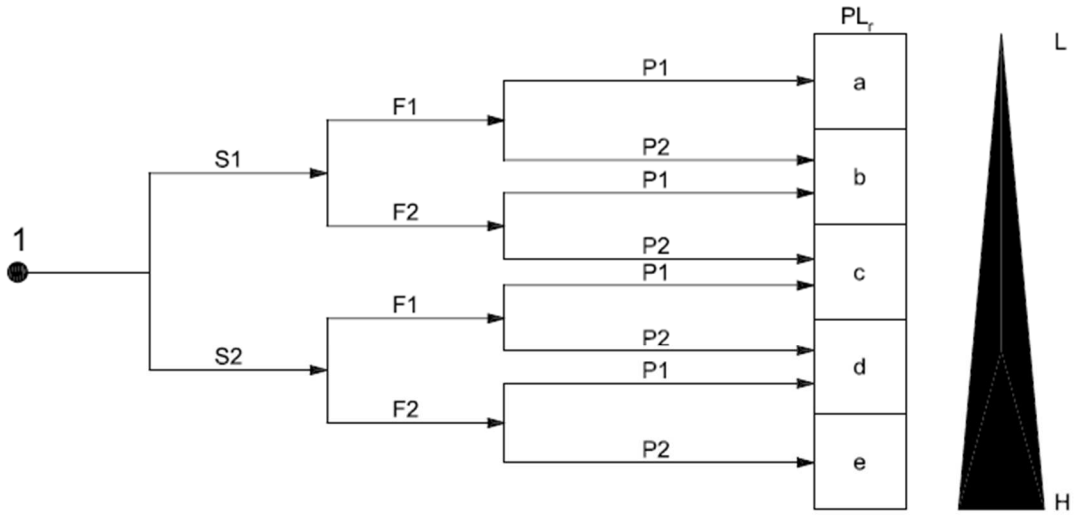
Contactor is used as an output device in safety applications where the STO function is needed. Feedback can be also achieved by using contactors outputs. In a safety function one or more contactors can be used for cutting power off the machine. Contactor works by cutting the power off after voltage has been removed from its coil by a processing device. The safety functions which are used in this thesis are made with mirror contacts which means that if any main contact is closed, no auxiliary normally closed contact is allowed to be closed if it is closed it means that the contactor is dead. (Schneider Electric d.)

5.2 Servo drive and safety module

Servo drives are used as output devices in applications which require a controlled stop function for example SS1. The servo drive controls and monitors the speed, velocity and torque of servo motors. Some servo drives need a safety module or a card to fulfill the safety standards. An executed safety function gives a signal to the safety module/card which then gives the command to the servo drive to execute the right stop function. The servo drive which was used in this thesis had to have safety module attached to fulfill the requirements of achieving the SS1 stop category. There was also an encoder in the servo motor which gives the drive information on how the servo is running. (Schneider Electric 2015c.)

6 Safety calculations

In this thesis all the calculations were made with a Sistema safety calculation tool. First to calculate safety you have to determine the PL_r. To determine it you have to identify the risks of the machine and then define their severity and frequency and the possibility of avoiding the hazard. After this you will get the PL_r to fulfill. (EN ISO 13849-1.)



Key

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

Risk parameters:

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

Figure 6 Performance level estimation (EN ISO 13849-1.)

To calculate $MTTF_D$ the number of operations needs to be calculated with the following formula

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600\ s/h}{t_{cycle}}$$

h_{op} is the mean operation time of the machine, in hours per day.

d_{op} is the mean operation time of the machine, in days per year.

t_{cycle} is the cycle time how often the safety function is triggered, in seconds

$$MTTF_D = \frac{B_{10D}}{0{,}1 \times n_{op}}$$

B_{10d} is how many times a component can be used before 10 percent of the components will fail dangerously, this value is stated by the manufacturer. (EN ISO 13849-1.)

SISTEMA is the toll which was used in this thesis to make the safety calculations. SISTEMA is an abbreviation of Safety Integrity Software Tool for Evaluation to Machine Applications. SISTEMA is a calculation tool which can be used to calculate the performance level of the safety function. German Institute for Occupational Safety and Health of the German Social Accident Insurance, IFA is the publisher of this software.

Many of the largest electrical component builders release their own SISTEMA libraries which include their components and all the information needed to calculate the performance level for the complete safety function.

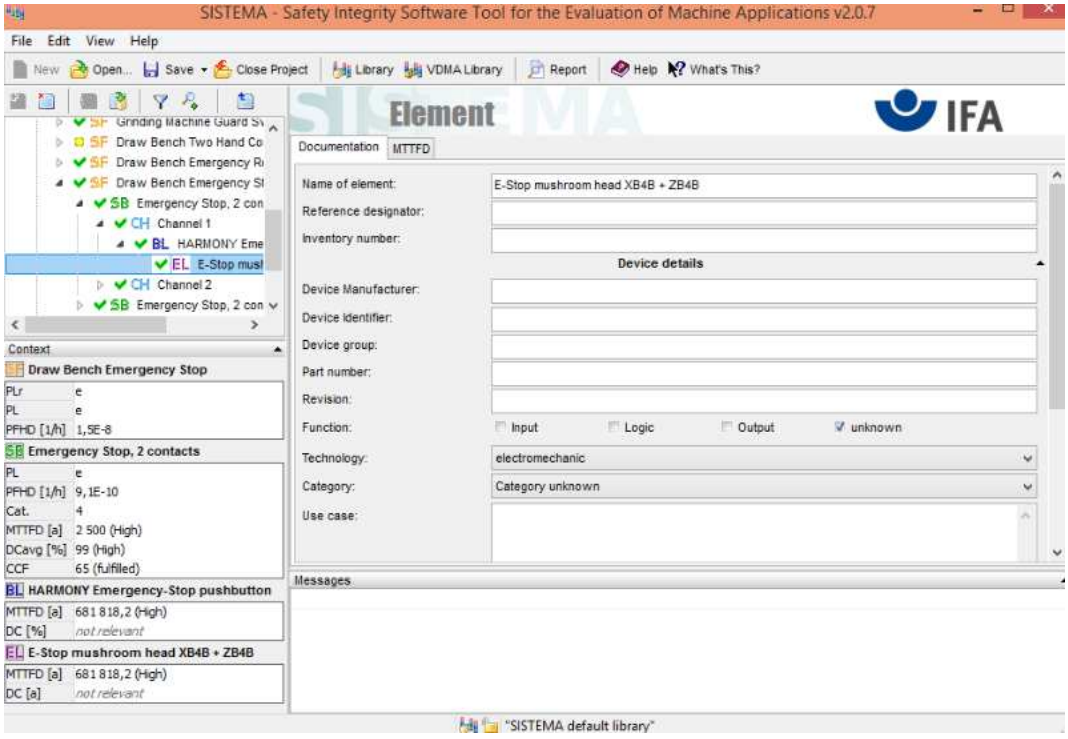


Figure 7. Sistema calculation tool

7 Safety functions

This part explains how all the machines which are picked for this thesis, work and how machine safety requirements are defined for the machines. The safety calculation is explained in the draw bench application.

7.1 Continuous fryer

A continuous fryer is an industrial deep fryer which is used to prepare different kind of food at an industrial level for example potato chips. The machine contain a conveyor that transfers food through heated oil to the next processing station, an oil tank and an oil cleaner that extracts pieces of food out of the oil so the produced food stays homogenous. (Heat and Control 2018.)

7.1.1 Normal operation

Machine is on and hood is down conveyor is running and oil is heated up. Product is in example chicken nuggets that are fed to beginning of the conveyor and then it transfers product through the oil to the end of machine where products are going to another conveyor.

7.1.2 Safety in Normal operation

In the continuous fryer guard switch is connected to the hood (Q3 and Q4), opening the guard shuts down the power from the conveyor (Q1 and Q2) and heating element (Q5) and the machine goes to Safe Torque Off (STO) state, but still leaves the power for the hood lifting mechanism. After lowering the hood and closing the guard switch machine can be started again after pressing the reset. Pressing emergency stop execute STO function which cuts power from the machine.

7.1.3 Determining requirements

Safety functions need to fulfill at least PL c and SIL 1. Also there is a standard EN 1672 Food processing machinery which machine need to fulfill standard does not include machine safety.

Table 2. Assessment of the risks concerning the fryer with the PLr determination for each risk.

Hazard	Origin of hazard	Possible effects	Examples of injury	Required PL & SIL
Mechanical	Conveyor	Trapping, Friction, Drawing-in	Crush injuries, fractures	PLr c SILr 1
Other	Oil	Burning	Burns	PLr c SILr 1
Electrical	Electrical equipment	Poorly maintained equipment, failure in isolation	Electric shock, burns, death	PLr c SILr 1

7.2 Grinding machine

Grinding machine that is focused on this thesis is three axes grinding station where all axles are inside the machine covered by door which is monitored by safety interlock switch. Grinding machines can be used to handle many different kind of materials from metal to wood. In this example the servo drive is quite small so material which is machined by this setup has to be soft.

7.2.1 Normal operation

Operator opens the door while pressing door opening button and workpiece is fastened inside the machine. Door is closed and machine is started. When the program is stopped, door can be opened again and the product is removed from the machine.

7.2.2 Safety in Normal operation

In grinding machine, there is guard switch connected to the protective door which is locked while machine is running and door can be opened only while machine is stopped by pushing the door opening button which opens the door (E1).

In grinding machine, there is also one emergency stop pushbutton at the control panel which executes STO function (Q1 and Q2) after being pressed.

Machine can be driven door open with safety limited speed when enabling switch is activated.

7.2.3 Determining requirements

Machine need to fulfill the requirements of Performance Level c (PL c) according to ISO 13849-1 and Safety Integrity Level 1(SIL1) according to IEC 62061. Machine needs to also fulfill Type C standard ISO 16089:2015 for stationary grinding machines.

Machine is designed to belong to group 2 in accordance to EN ISO 16089 which means that the machine is manually controlled with limited numerical control. Mandatory mode of safe operations is 0 (MSO 0) and I selected to use voluntarily also 1 (MSO 1), because in the application there is movable guards and a possibility to run the machine with safe speed in according to ISO 16089.

Table 3. Assessment of the risks concerning the grinding machine with the PLr determination for each risk..

Hazard	Origin of hazard	Possible effects	Examples of injury	Required PL & SIL
Mechanical	Approach of a moving element to a fixed part	Crushing	Crush injuries	PLr c SILr 1
Mechanical	Cutting parts	Cutting severing	Cut injuries	PLr c SILr 1
Electrical	Electrical equipment	Poorly maintained equipment, failure in isolation	Electric shock, burns, death	PLr c SILr 1

7.3 Meat dicer

Meat dicer is a machine which is used in food industry to cut or dice meat. Machine has a chute where the meat is placed and a press which controls the size of the diced meat by the movement speed. Meat is diced by rotating blades which are under protective cover. (Treif 2012.)

7.3.1 Normal operation

Operator opens chute where he inserts the meat which is going to be diced, then he closes the chute and then press starts pressing the meat against the slicer which dices the meat next the diced meat drops to conveyor and then the conveyor moves the meat to container. Press goes back to the state where it started. When H1 illuminates and indicates that chute can be opened.

7.3.2 Safety in Normal operation

In Meat dicing machine, there is coded magnetic switch in the chute which prevents machine from running while press is moving if operator opens the chute while press is moving modular safety controller is executing Safe Torque Off (STO), after closing the coded magnetic switch (chute) machine starts automatically from where it was before the STO function. There is a light which illuminates when the press is stopped to the back position and chute can be opened.

On the guard door, which is covering the meat dicing blade is guard switch with interlock, so the door can be opened only while machine is stopped and can be re started only after resetting the guard switch when the door is closed.

In the Machine, there is also one emergency stop which when pressed executes the STO function

7.3.3 Determining requirements

Machine need to fulfill the requirements of Performance Level c (PL c) according to ISO 13849-1 and Safety Integrity Level 1(SIL1) according to IEC 62061. Meat dicer needs to also fulfill Type C standard ISO 16089:2015 for stationary grinding machines. EN 1974:1998+A1:2009 which gives more detailed information about food processing machinery for slicing machines and for machinery safety and hygiene requirements. In EN 1974:1998+A1:2009 is stated that machine should achieve PL c accordance to EN ISO 13849-1:2008 and maximum stopping time should not exceed four seconds.

Table 4. Assessment of the risks concerning the meat dicer with the PLr determination for each risk.

Hazard	Origin of hazard	Possible effects	Examples of injury	Required PL & SIL
Mechanical	Conveyor	Trapping, Friction, Drawing-in	Crush injuries, fractures	PLr c SILr 1
Mechanical	Press	Getting crushed	Crush injuries	PLr c SILr 1
Mechanical	Dicing blade	Getting cut	Cut wounds	PLr c SILr 1
Electrical	Electrical equipment	Poorly maintained equipment, failure in isolation	Electric shock, burns, death	PLr c SILr 1

7.4 Rotation molding machine

Rotation molding machine is a device designed to create large plastic objects with heating the mold by gas burner and rotating the mold so the molten plastic sticks evenly to the mold. After melting and sticking to the molds surface the axle which rotates the mold is moved to the cooling chamber where the mold is cooled by water spray. Last step the axle moves out of the chamber to in front of the machine where machine operator can remove the ready product from the mold and adding a new plastic powder to the mold.

7.4.1 Normal operation

Operator adds plastic to the rotating axle and closes the mold. Then operator goes to enabling switch and drives the axle to the oven and after axle is inside the oven and the door is closed enabling switch can be released. Then the axle is spinning and melting the plastic to the mold. Next the axle goes to the cooling room and after that door of the cooling room is opened and operator drives the axle out in front of the machine.

7.4.2 Safety in Normal operation

A limit switch is triggered when a rotating axle is in the area where the operator works, operator needs to drive it with an enabling switch. If the enabling switch is pushed to the bottom or released Safe Torque Off (STO) is executed. STO cuts power off from the axle. When the limit switch is at normal state again, the machine starts to run automatically after the reset button has been pressed.

When the emergency stop is pressed, the STO function is executed shutting down the power from the machine including the doors and the heating element

7.4.3 Determining requirements

Rotation molding machine need to fulfill the requirements of Performance Level e (PL e) according to ISO 13849-1 and Safety Integrity Level 3(SIL3) according to IEC 62061.

Table 5. Assessment of the risks concerning the rotation molding machine with the PLr determination for each risk.

Hazard	Origin of hazard	Possible effects	Examples of injury	Required PL & SIL
Mechanical	Door	Trapping, getting crushed, Drawing-in	Crush injuries, fractures	PLr e SILr 3
Mechanical	Axle	Getting crushed, getting hit	Crush injuries	PLr e SILr 3
Other	Oven	Getting burned	burns	PLr d SILr 2
Electrical	Electrical equipment	Poorly maintained equipment, failure in isolation	Electric shock, burns, death	PLr c SILr 1

7.5 Draw bench

Draw bench is a tool used for cold working metal. The machine basically just draws metal rod through a die which then changes the rod to a wanted shape and size. These machines can be run with a motor in the thesis a motor powered machine was considered.

7.5.1 Normal operation

An operator or an automatic system feeds the metal to the draw bench and then the gripper grips the metal and a draw trolley starts drawing lit through the die. When end of the metal piece is coming close the drawer stops if the operator does not use the two-hand control. When the two-hand control is pressed, metal is fully drawn out of the die, released from the gripper and moved to the next phase. After this the draw trolley is returned to the die end.

7.5.2 Safety in Normal operation

In a draw bench there is two-hand control which needs to be pressed before the drawn piece of metal is in the end to prevent the operator from being too close to the metal which might spring and hit the operator. Two-hand control has an effect only on the drawing motor.

A rope of rope pull switch is set to the whole length of the machine to the edge where the operator locates. The rope pull switch executes the STO function for the whole machine. In the Machine, there is also emergency stop which executes the STO function when pressed.

7.5.3 Determining requirements

In the draw bench there is a lot of hazardous components near the area where the operator of the machine works. Draw benches safety functions need to fulfill at least PL e and SIL 3.

Table 6. Assessment of the risks concerning the draw bench with the PLr determination for each risk.

Hazard	**Origin of hazard**	**Possible effects**	**Examples of injury**	**Required PL & SIL**
Mechanical	Drawing mechanism	Trapping, Friction, Drawing-in	Crush injuries, fractures	PLr e SILr 3
Mechanical	Product released from drawing trolley	Crushing, Impact	Crush injuries	PLr c SILr 1
Electrical	Electrical equipment	Poorly maintained equipment, failure in isolation	Electric shock, burns, death	PLr c SILr 1

8 Calculating safety function for draw bench

The safety function which is calculated here is an emergency stop pushbutton for a draw bench application. It was picked as an example because it is quite common safety function.

8.1 Devices used

The whole application contains all the devices but for this safety function we only need to emergency stop pushbutton, a modular safety controller, an input module and contactors. The rest of the devices will not have an effect on the calculation so those are not considered.

These devices were picked from Schneider Electrics Sistema libraries and added under one safety function.

Table 7. Devices used for the safety function

Item	Product	Description	Quantity
1	XALK178F	Harmony, Emergency Stop pushbutton	2
2	XY2CEDA296	Telemecanique, Emergency rope pull switch	1
3	XY2SB71	Telemecanique, Safety two-hand control	1
4	XCSM3902L1	Telemecanique, Limit Switch	1
5	XPSMCMCP0802	Preventa, Modular Safety Controller	1
6	XPSMCMDI1600	Preventa, Input module	1
7	XB4BVB6	Harmony, Reset pushbutton	1
8	2LC1D09BD	TeSys, 3-phase contactor	2

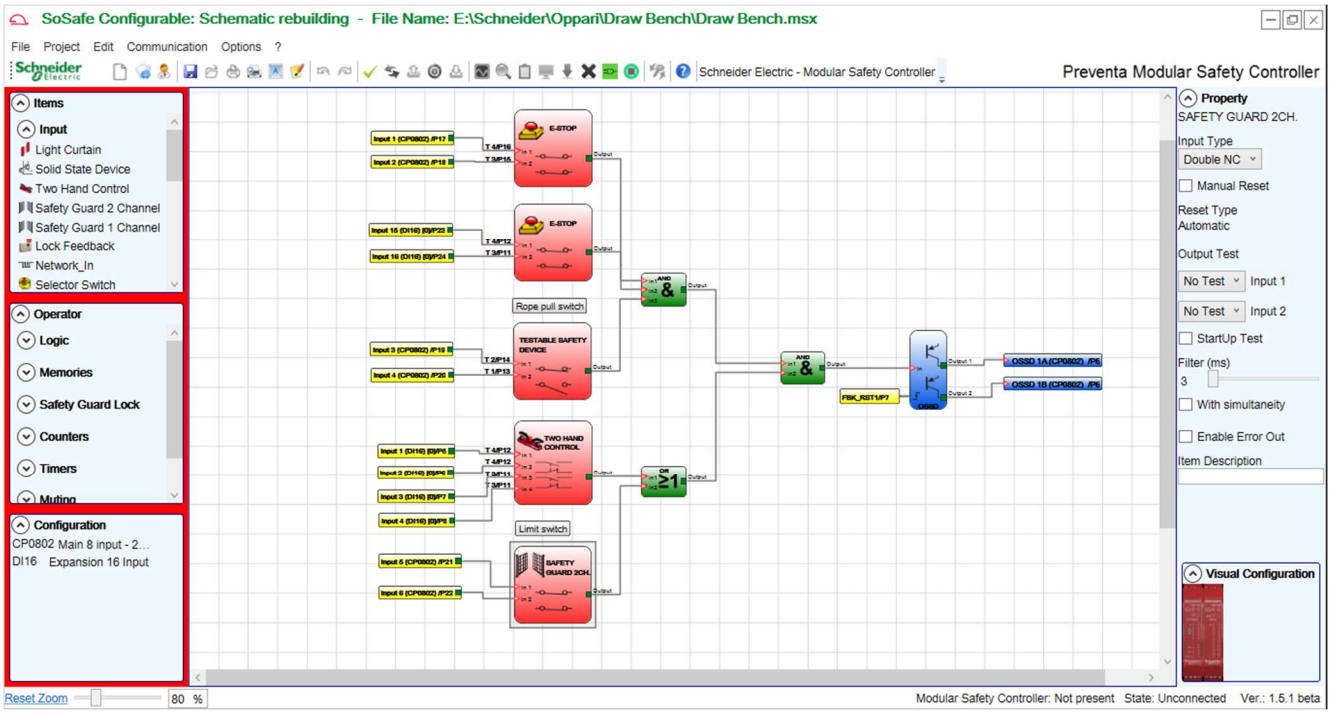


Figure 8. SoSafe Configurable program for the Draw bench application

8.2 Calculation

As in every safety calculation the cycle time is estimated in this function. It is estimated that the emergency stop pushbutton is pressed every 432000 seconds which is every 10th day when operating 12 hours per day this makes 22 times per year when working the estimated 220 days in a year.

This cycle time and the B10D of the device are fed to Sistema which calculates the number of operations. This must be done for each device and both of the channels.

Cycle Time	432000
Number of hours' operation per day (h)	12
Number of days' operation per year	220
Number of operations per year (n_{op})	22

Figure 9. Operations per year

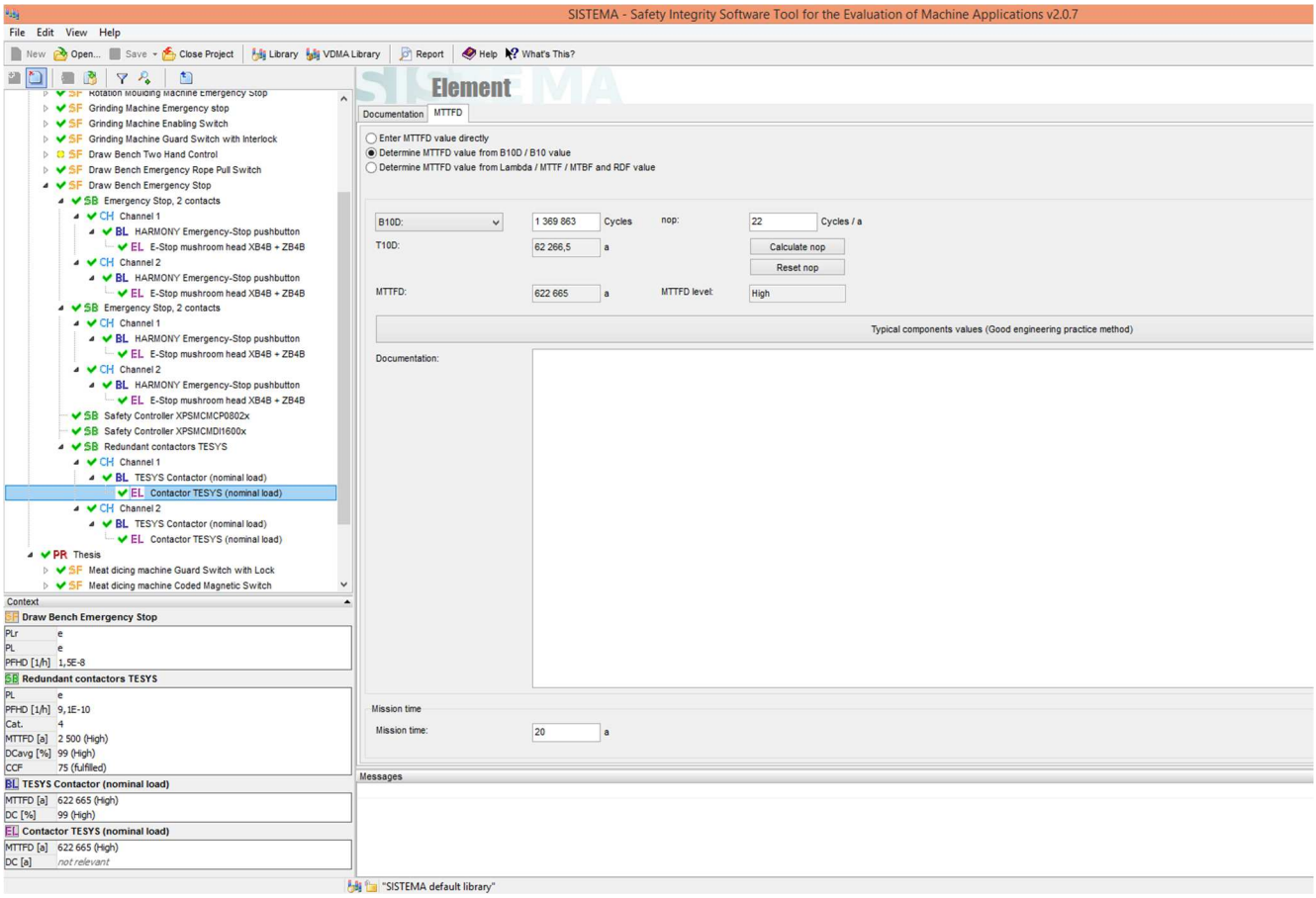


Figure 10. Inserting cycles per year to Sistema

The values which are counted for the safety calculations are given by the manufacturer in this case by Schneider Electric. For the modular safety controller and the input expansion module SoSafe programmable software calculates the combined values for the devices.

Preventa Modular Safety Controller Schneider Electric

```
Project Report generated by SoSafe Configurable Ver.: 1.5.1 beta

Project Name: Schematic rebuilding
User: Modular Safety Controller
Company: Schneider Electric
Date: 21.1.2019 19:47:38
Schematic CRC: 5207H

Modular Safety Controller: Configuration
Module CP0802 (Configured Firmware version: FW >= 3.0)
Module DI16 Node 0 (Minimum Required Firmware version: 0.1)
Updating from Memory card Disabled: True
Cycle Time (ms) = 3,316

Modular Safety Controller: Safety Information
PFHd (according to IEC 61508): 1,18E-008 (1/h)
MTTFd (according to EN ISO 13849-1): 208 years
DCavg (according to EN ISO 13849-1): 99.00 %
```

Figure 11. Values given by the SoSafe Configurable for the Modular safety controller setup.

Table 8. Safety calculation result

Safety Level Calculation - Emergency stop		Values	
		Channel 1	Channel 2
Acquire Information (Input) XALK	B_{10} (operations)	300 000	300 000
	%dangerous failure	20	20
	B_{10D} (operations)	1500 000	1500 000
	T_{10D} (years)	68 181,8	68 181,8
	$MTTF_D$ (years)	681 818,2	681 818,2
	$MTTF_D$ resulting (years)	2500	2500
	PFH_D resulting (1/h)	9,06E-10	9,06E-10
	DC (%)	99	99
Modular Safety Controller XPSMCMCP0802	B_{10} (operations)	not relevant	not relevant
	%dangerous failure	not relevant	not relevant
	B_{10D} (operations)	not relevant	not relevant
	T_{10D} (years)	20,8	20,8
	$MTTF_D$ (years)	208	208
	$MTTF_D$ resulting (years)	208	208
	PFH_D resulting (1/h)	1,18E-08	1,18E-08
	DC (%)	99	99
Expansion module XPSMCMDI1600	B_{10} (operations)	not relevant	not relevant
	%dangerous failure	not relevant	not relevant
	B_{10D} (operations)	not relevant	not relevant
	T_{10D} (years)	not relevant	not relevant
	$MTTF_D$ (years)	not relevant	not relevant
	$MTTF_D$ resulting (years)	not relevant	not relevant
	PFH_D resulting (1/h)	not relevant	not relevant
	DC (%)	not relevant	not relevant
Stop the Machine Devices (Output) LC1 (lowload)	B_{10} (operations)	1000 000	1000 000
	%dangerous failure	73	73
	B_{10D} (operations)	1369 863	1369 863
	T_{10D} (years)	62 266,5	62 266,5
	$MTTF_D$ (years)	622 655	622 655
	$MTTF_D$ resulting (years)	2500	2500
	PFH_D resulting (1/h)	9,06E-10	9,06E-10
	DC (%)	99	99
Safety Function (Result)	$MTTF_D$	156,1	
	DC_{avg}	99 (high)	
	PFH_D resulting (1/h)	1,54E-08	
	PL attained	e	
	SIL attained	3	

The calculation result has been achieved with SISTEMA software. As stated before in chapter 7.5.3 draw bench need to achieve at least PL e and SIL 3. Safety function achieves it.

9 Summary

The aim of this thesis was to provide safety functions for different kind of machines. In total five different applications were built paying attention to the machine safety. These safety functions will work as tool for the marketing team how wide and flexible Schneider electrics product range is.

In the theory part machine standards were studied more closely. How those are in order by A-, B- and C-type. How to achieve the required SIL or PL and how those two compare. Stop categories and different kind of safety devices and devices involved with machine safety. The devices which were picked for this part are devices which have been used in the safety functions created in this thesis. Calculations and different variables are looked closer.

In the practical part the five picked devices were explained how they work normally and how it works when paying attention to safety. Risks were assessed and the PLr was estimated for each risk. This is the most important part of making a safety function because if the risks have not been properly assessed some hazardous working cycles can be left unnoticed. That is why this part of the practical part is the longest. The last thing in the practical part was the calculation of one safety function with the Sistema calculation tool.

This thesis made me to see the importance of machine safety. Machine safety will make the workplace safer to workers and this way it also provides faster and more efficient work flow when the workers can only focus on production as all the hazards have been already taken into account.

BIBLIOGRAPHY

EN 574+A1. 2008 [Standard]. Safety of machinery – Two-hand control devices – Functional aspects – Principles for design.

EN ISO 13849-1. 2008 [Standard]. Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design.

EN ISO 13850. 2007 [Standard]. Safety of machinery – Emergency stop – Principles for design.

Heat and Control. 2018 [Web page]. Heat and Control inc. [Ref 13 April 2018]. Available at: http://www.heatandcontrol.com/eqmain.asp?eqid=1

ISO 14119. 2013 [Standard]. Safety of machinery – Interlocking devices associated with guards – Principles for design and selection.

Stoker Concast. Undated. Draw bench. [Web page]. Stoker Concast Pvt. Ltd. [Ref. 13 April 2018]. Available at: http://www.stokerconcast.com/draw-bench.html

Schneider Electric. Undated a. [Web page]. Schneider Electric GmbH. [Ref. 27 March 2018]. Available at: https://www.schneider-electric.com/en/about-us/company-profile/

Schneider Electric. Undated b. Eine Erfolgsgeschichte für Deine Ausbildnung. [Web page]. Schneider Electric GmbH. [Ref. 27 March 2018]. Available at: https://www.schneider-electric.de/de/about-us/careers/vocational-training/marktheidenfeld/

Schneider Electric. Undated c. XALK178. [Photograph]. Schneider Electric GmbH. [Ref. 29 March 2018] Available at: https://www.schneider-electric.com/en/product/XALK178/yellow-station---1-red-mushroom-head-pushbutton-%C3%B840-turn-to-release-1nc/?range=660-harmony-xald%2C-xalk&node=166481931-control-stations

Schneider Electric. Undated d. Does Schneider Electric offer 'safety contactors'?. [Web page]. Schneider Electric GmbH. [Ref. 12 April 2018] Available at: https://www.schneider-electric.co.uk/en/faqs/FA136111/

Schneider Electric. Undated e. Schneider Electric reliability value Libraries. [SISTEMA library]. Schneider Electric GmbH. [Ref. 12 April 2018] Available at: https://www.schneider-electric.com/en/download/document/Reliability_values/

Schneider Electric. 2005. Schneider Electric, 170 years of history [Online publication]. Schneider Electric GmbH. [Ref. 27 March 2018]. Available at: https://www.schneider-electric.co.cr/documents/empresa/se_history_brands_march2005.pdf

Schneider Electric. November 2009. Safe Machinery Handbook. [Online publication]. [Ref. 28 March 2018]. Available at: http://www2.schneider-electric.com/documents/original-equipment-manufacturers/en/shared/safety-handbook-v3.pdf

Schneider Electric. 2015a. The Preventa XPS Modules Customer Presentation. [PowerPoint-presentation]. Schneider Electric GmbH. [Ref. 10 April2018]. Available at: Only for internal use.

Schneider Electric. 2015b. The Preventa XPSMCM Modular Safety Controllers Customer Presentation. [PowerPoint-presentation]. Schneider Electric GmbH. [Ref. 10 April 2018]. Available : Only for internal use.

Schneider Electric. 2015c. Machine Solutions Training Lexium 32 Safety Engineering with eSM Module. [PowerPoint-presentation]. Schneider Electric GmbH. [Ref. 12 April 2018]. Available : Only for internal use.

Schneider Electric. 2017. 01 Machine Safety_May_2017. [PowerPoint-presentation]. Schneider Electric [Ref. 10 April 2018]. Available : Only for internal use.

Siirilä, T. 2008 Koneturvallisuus 1: EU-määräysten mukainen koneiden turvallisuus. 2nd ed. Keuruu: Otavan Kirjapaino Oy.

Telemecanique Sensors. Undated. XCSLE2525312. [Photograph]. [Ref. 29 March 2018] Available at: http://www.tesensors.com/global/en/product/safety-switches/preventa-xcs-ref/?conf=sensors&el_typ=product&range_id=616&prd_id=XCSLE2525312&scp_id=WW_en

Telemecanique Sensors. Undated. Safety switches Preventa XCS Catalogue. [Online publication]. [Ref. 29 March 2018] Available at: https://download.schneider-electric.com/files?p_File_Id=38182522