

Alexi Pullinen

Machine Safety Design

per application

Thesis

Spring 2017

Seinäjoki UAS, School of Technology

Automation Engineering



SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree Programme: Automation Engineering

Specialisation: Machine Automation

Author: Aleksi Pullinen

Title of thesis: Machine safety design –per application

Supervisor: Jorma Mettälä

Year: 2017

Number of pages: 54

Number of appendices: 3

The purpose of this thesis was to create machine safety designs for machine builders and sales persons. The thesis was made for Schneider Electric Automation GmbH Marketing Safety team, and the results will be beneficial for their work.

The theory part is about the safety devices, which have been used in the architectures designed in this thesis. Standards and safety calculations are a big part of designing new machine safety systems and thus, they were shown and explained widely in the thesis. SISTEMA software has been explained by showing a little calculation example.

The practical part consists of three different architecture examples of three different machine types: a palletiser, a wrapping machine and a bending press. Their operation principles have been described and it has been explained how the designed safety architecture operates. Possible hazards have been introduced, and examples of safety devices have been listed.

.

Keywords: machine safety, SISTEMA, muting, palletizing

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikan yksikkö

Tutkinto-ohjelma: Automaatiotekniikka

Suuntautumisvaihtoehto: Koneautomaatio

Tekijä: Aleks Pullinen

Työn nimi: Koneturvallisuuden suunnittelu kolmelle eri tuotantokoneelle

Ohjaaja: Jorma Mettälä

Vuosi: 2017

Sivumäärä: 54

Liitteiden lukumäärä: 3

Tämän opinnäytetyön tarkoitus oli luoda koneturvallisuusmalleja koneentekijöille ja myyntihenkilöstölle. Opinnäytetyö tehtiin Schneider Electric Automaatio GmbH:n markkinointi tiimille ja tuloksia tullaan hyödyntämään heidän työssään.

Teoria osuus koostuu turvallisuuslaitteista, joita on käytetty suunnitelluissa malleissa. Standardit ja turvallisuuslaskelmat ovat suuressa osassa suunnittelussa turvallisuusjärjestelmää ja nämä asiat on esitetty opinnäytetyössä laajasti. SISTEMA ohjelmaa on esitetty tekemällä laskelmaesimerkki.

Käytännön osuus koostuu turvallisuusarkkitehtuurin suunnittelusta kolmeen eri koneeseen: lavaaja, pakkauskone ja hydraulinen prässä. Tekstissä esitellään koneiden ja turvallisuuslaitteiden toimintaa. Myös mahdolliset tapaturmat on tuotu esiin ja esimerkkilaitteistot on listattu.

.

Asiasanat: koneturvallisuus, SISTEMA, passivointi, lavaaja

TABLE OF CONTENTS

| | |
|---|-----------|
| Thesis abstract..... | 2 |
| Opinnäytetyön tiivistelmä..... | 3 |
| TABLE OF CONTENTS | 4 |
| Terms and Abbreviations..... | 7 |
| Tables, Figures and Pictures..... | 8 |
| 1 INTRODUCTION | 11 |
| 1.1 Schneider Electric | 11 |
| 1.2 Background..... | 12 |
| 1.3 Structure of the research..... | 12 |
| 2 MACHINE SAFETY..... | 14 |
| 2.1 General information about machine safety..... | 14 |
| 2.2 Machine safety standards | 14 |
| 2.3 Risk assessment..... | 15 |
| 2.4 Categories..... | 16 |
| 2.5 Stop Categories | 17 |
| 2.6 Muting function..... | 17 |
| 3 SAFETY COMPONENTS..... | 19 |
| 3.1 Acquire information | 19 |
| 3.1.1 Emergency stop..... | 19 |
| 3.1.2 Light curtain | 20 |
| 3.1.3 Magnetic safety switch..... | 20 |
| 3.1.4 Photo-electric sensors | 21 |
| 3.1.5 Enabling switch..... | 22 |
| 3.2 Monitoring & processing..... | 22 |
| 3.2.1 Safety modules | 23 |
| 3.2.2 Configurable safety controllers | 23 |
| 3.2.3 Schneider Electric XPSMCM | 24 |
| 3.2.4 SoSafe Configurable software | 24 |
| 3.3 Contactors..... | 25 |

| | | |
|----------|---|-----------|
| 4 | PALLETIZING MACHINE WITH AN AUTOMATIC PALLET DISPENSER | 27 |
| 4.1 | Normal operation mode..... | 27 |
| 4.1.1 | Safety on the normal operation mode | 28 |
| 4.2 | Maintenance mode..... | 29 |
| 4.2.1 | Safety on maintenance mode | 29 |
| 4.3 | Hazards according to EN 415-4:1997 | 29 |
| 4.3.1 | Hazards on normal operation mode..... | 30 |
| 4.3.2 | Hazards on maintenance mode | 30 |
| 4.4 | Architecture | 31 |
| 4.5 | List of needed safety devices | 31 |
| 5 | WRAPPING MACHINE | 32 |
| 5.1 | Normal operation mode..... | 32 |
| 5.1.1 | Safety on normal operation mode | 32 |
| 5.2 | Maintenance mode..... | 33 |
| 5.2.1 | Safety on maintenance mode | 33 |
| 5.3 | Hazards according to EN 415-6:2013 | 34 |
| 5.3.1 | Hazards on normal operation mode..... | 34 |
| 5.3.2 | Hazards on maintenance mode | 34 |
| 5.4 | Architecture | 35 |
| 5.5 | List of materials | 35 |
| 6 | BENDING PRESS | 37 |
| 6.1 | Operation principle | 37 |
| 6.2 | Safety..... | 38 |
| 6.3 | Hazards according EN 12622 | 38 |
| 6.4 | Architecture | 38 |
| 6.5 | List of materials..... | 39 |
| 7 | SAFETY DATA | 40 |
| 7.1 | Safety Integrity Level (SIL) & Performance Level (PL)..... | 40 |
| 7.2 | SISTEMA | 41 |
| 7.2.1 | Creating SISTEMA calculations | 41 |
| 7.3 | Safety calculations | 48 |
| 8 | SUMMARY..... | 51 |

| | |
|-------------------|----|
| BIBLIOGRAPHY..... | 52 |
| APPENDICES | 54 |
| APPENDIX 1 | 1 |
| APPENDIX 2..... | 2 |
| APPENDIX 3..... | 3 |

Terms and Abbreviations

| | |
|-------------------------|--|
| DC_{avg} | average Diagnostic Coverage |
| IFA | Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung |
| IEC | International Electrotechnical Commission |
| ISO | International Standard Organisation |
| MTTF_d | Mean Time To a dangerous Failure |
| PFH_d | Probability of a dangerous Failure per Hour |
| PL | Performance Level |
| PL_r | Required Performance Level |
| SIL | Safety Integrity Level |
| SIL_r | Required Safety Integrity Level |

Tables, Figures and Pictures

| | |
|--|----|
| Table 1 Table of relevant hazards on normal operation mode | 30 |
| Table 2 Table of relevant hazards on maintenance mode | 30 |
| Table 3 Table of needed safety devices | 31 |
| Table 4 Table of relevant hazards on normal operation mode | 34 |
| Table 5 Table of relevant hazards on maintenance mode | 35 |
| Table 6 Table of needed safety devices | 36 |
| Table 7 Table of relevant hazards..... | 38 |
| Table 8 Table of needed safety devices | 39 |
| Table 9 Relations between PL, SIL, PFHD and MTTFd (Siirilä T 2009 147) | 40 |
| Table 10 Table of referred values | 49 |
| Table 11 Safety level calculation..... | 50 |
| | |
| Figure 1. Logo of Schneider Electric. (Schneider Electric [Referred 9.2.2016]) | 11 |
| Figure 2. Schneider Electric Automation GmbH Headquarters in Marktheidenfeld. (Schneider Electric [Referred 9.3.2016]) | 11 |
| Figure 3 Structure of A B & C standards (Schneider 2009) | 15 |
| Figure 4 A muting with two crossed beams (Telemecanique [Referred 07.02.2017]) | 18 |
| Figure 5 A sequential muting with four sensors (Telemecanique [Referred 07.02.2017])..... | 18 |

| | |
|---|----|
| Figure 6 Schneider Electric Emergency stop button. (Schneider Electric [Referred 9.2.2016])..... | 19 |
| Figure 7 A Telemecanique light curtain..... | 20 |
| Figure 8 A coded magnetic safety switch (Schneider Electric [Referred 30.11.2016]) | 21 |
| Figure 9 Telemecanique photo-electric sensors (Telemecanique 2014)..... | 21 |
| Figure 10 Enabling switch (Schneider Electric 2009)..... | 22 |
| Figure 11 Schneider Electric XPSBAE safety module (Schneider Electric [Referred 30.11.2016])..... | 23 |
| Figure 12 Schneider Electric XPSMCMCP0802 safety controller (Schneider Electric [Referred 30.11.2016])..... | 24 |
| Figure 13 Schneider Electric SoSafe Configurable software (Schneider Electric 2015)..... | 25 |
| Figure 14 Mirror Contact (Schneider Electric [Referred 1.11.2016]) | 26 |
| Figure 15 Columbia FL1000-SW Palletizer (Columbia 2015) | 27 |
| Figure 16 Ring machine | 32 |
| Figure 17 Cincinnati bending press..... | 37 |
| Figure 18 Adding the library | 41 |
| Figure 19 Adding local library..... | 42 |
| Figure 20 Choosing libraries from the hard disk..... | 42 |
| Figure 21 Creating a new project | 43 |
| Figure 22 The project tree..... | 43 |
| Figure 23 Safety functions | 44 |

| | |
|--|----|
| Figure 24 Overview of safety function | 44 |
| Figure 25 PLr Tab | 45 |
| Figure 26 The subsystems..... | 45 |
| Figure 27 Subsystem from the library | 46 |
| Figure 28 Project tree | 47 |
| Figure 29 Elements..... | 47 |
| Figure 30 Calculating the number of operations | 48 |

1 INTRODUCTION

1.1 Schneider Electric

Schneider Electric is a European multinational corporation. They are specializing in energy management, automation management and delivering innovative solutions to customers. In 1836 Schneider brothers took over the Creusot foundries. Two years later, they created Schneider & Cie. Starting from its roots in the iron and steel industry, heavy machinery, and shipbuilding, it moved into electricity and automation management. Nowadays Schneider Electric employs 170 000 people in more than 100 countries. In 2014, the revenue was 24.9 billion euros. (Schneider Electric [Referred 9.2.2016].) Schneider Electric Automation GmbH headquarters are located in Marktheidenfeld. Figure 1 below shows the logo of Schneider Electric and Figure 2 the headquarters of Schneider Electric in Marktheidenfeld.



Figure 1. Logo of Schneider Electric. (Schneider Electric [Referred 9.2.2016])



Figure 2. Schneider Electric Automation GmbH Headquarters in Marktheidenfeld. (Schneider Electric [Referred 9.3.2016])

1.2 Background

The purpose of this thesis is to create a safety design tool for Schneider Electric Automation GmbH. Their sales persons have faced problems when explaining safety functions and safety equipment that machine builders need. With an unambiguous safety design tool, sales persons have proper knowledge about machine safety, and it is easier to convince customers that they need this specified application. With the help of this thesis, the sales persons do not have to contact marketing team in every case. The main goal is to get the customers understand what kind of safety related possibilities they have with their machines and which standards they require.

1.3 Structure of the research

The first section contains an introduction to the thesis, including a company profile, background and structure of the research.

The second section contains the theory part concerning machine safety, safety standards and safety components. In this section, the muting function is explained, which is crucial for the applications performed in this thesis.

In the third section, most common safety components are explained. The components have been divided into inputs, processing and outputs.

After the third section the chosen machine types and machine safety applications for them are introduced. The possible hazards for each machine according to the applicable standards are shown in respective subsections. The safety devices needed in this section are also shown in the tables. At the end of this part the required Performance Level (PL) and Safety Integrity Level (SIL) are decided.

The fifth section is about safety data and safety calculations using the SISTEMA software tool. In this part, only one example is shown and other calculations can be found in the appendices.

The last section contains the summary of the thesis. In this section there is discussion on how well the goals were reached.

2 MACHINE SAFETY

This section contains general information about machine safety and safety machinery standards. The three types of standards are briefly introduced. In the end of the section, the muting function is discussed.

2.1 General information about machine safety

Safety is very important in machine automation and human life is the most important value in a company. Lack of safety can increase insurance premiums and injuries may give a negative image to the company (Schneider Electric 2015.)

Machines usually have moving parts, sharp edges and hot surfaces, which can cause severe workplace injuries. Machine safety with e.g. safeguards can prevent many injuries (NIOSH 2014). Machine safety must be taken into account at all the stages in the life of a machine: design, manufacture, installation, adjustment, operation, maintenance and eventual scrapping (Schneider Electric 2009).

2.2 Machine safety standards

The EU Machinery Directive is a European law, and defines the machines which are considered dangerous. The purpose is to guarantee a minimum safety level for machinery and equipment sold within the EU market. The directive allows the free circulation of machinery within the European Union and guarantees high level of protection for EU workers and citizens.

In the past European manufacturers have designed safety-related parts of the machines' control systems in accordance with the standard EN 954-1. This standard, however, does not cover the components of the safety devices and therefore, was not good enough to ensure a safe machine. Nowadays manufacturers can design their machines according to EN ISO 13849 for Performance Level (PL) and EN/IEC 62061 for Safety Integrity Level (SIL). EN ISO 13849 standard gives safety requirements relating to principles for the design and integration of safety related parts of

control systems. Standard EN/IEC 62061 gives rules for the integration of sub-systems designed in accordance with EN/ISO 13849. Non-European countries have their own directives and standards but almost all their standards are based on European Standards. (Schneider Electric 2015.)

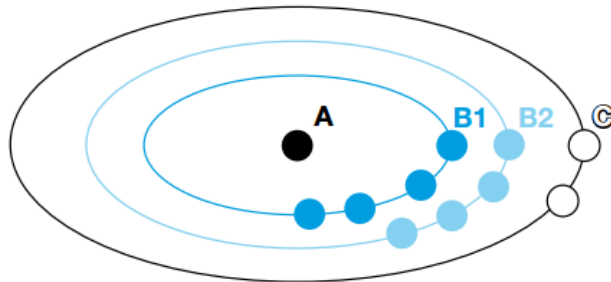


Figure 3 Structure of A B & C standards
(Schneider 2009)

There are three different types of standards for the Safety of machinery: A, B & C standards. Figure 3 above shows the structure of the standards.

Type A standards are basic safety standards, giving basic concepts and guidelines for design. These standards can be applied to all machinery. Type B standards are dealing with one safety aspect or one type of safeguard. Type C standards are machine safety standards and are relevant in this research. Type C standards are used in the detailed safety requirements of a particular machine or a group of machines. (Schneider Electric 2009.)

2.3 Risk assessment

Machine builder has to ensure that risk assessment is done when starting to build the machine. There are various methods to make risk assessment but in every method, severity of the potential harm and probability of occurrence is evaluated. These features are considered to define a level of risk, which is the evaluated to define whether the risk reduction objectives haven been achieved. Type-C standards examine deeper into details as they apply to specific machine group (Sick [Referred 10.02.2017].)

2.4 Categories

Categories are the basic parameters used to achieve a specific PL. They state the required behaviour of safety-related part of a control system in respect of its resistance to faults on the design considerations (SFS-EN ISO 13849-1/AC 2009.)

In category B components must be chosen so, that they endure specific conditions. The range of $MTTF_d$ must be from 3 to 29 years (Siirilä 2009, 143).

In category 1 proven safety principles and well tried components have to be used. Category 1 has greater reliability, but still loss of safety function is possible. The range of $MTTF_d$ must be from 30 to 100 years. The devices in this category are single channel devices (Siirilä 2009, 143-144.)

In category 2 the requirements are the same as in category B and well-tried safety principles have to be used. In addition, it has to endure checking safety function when the machine is starting and before a dangerous situation occurs. The category requires checking the safety device's proper operation at least 100 times more than need of the safety device. The range of $MTTF_d$ must be from three to 100 years and DC_{avg} from 60 to 98 percentages. The CCF must be low. The devices in this category are single channel devices (Siirilä 2009, 144.)

In category 3 the requirements of category B and well-tried safety principles have to be used. The control system has to be able to perform the safety function (e.g. stop the machine) even though there is some failure. In addition, majority of failures have to be revealed. The range of $MTTF_d$ has to be from three to 100 years and DC_{avg} at least from 60 to 98 percentages. The CCF must be low. The devices in this category are two channel devices, the second channel is for fault exposing. (Siirilä 2009, 144.)

In category 4 the same requirements of category B and well-tried safety principles have to be used. The control system has to be able to perform the safety function even though there is some failure. The control system has to be able to expose all failures in a system, so accumulation is not possible in category 4. The range of $MTTF_d$ has to be from 30 to 100 years and DC_{avg} from 99 to 100 percentages. The

CCF must be low. The devices in this category are two channel devices, the second channel is for fault exposing (Siirilä 2009, 144.)

2.5 Stop Categories

There are three stop categories in machine safety. Stop categories indicate how the machine stops for example in case of emergency.

Stop Category 0 stops the machine by switching the electrical current off immediately. Stop Category 1 is a controlled stop with power available to the machine actuators to achieve the stop and then switching the current off when the stop has been achieved. Stop Category 2 is a controlled stop with power left available to the machine actuators. Stop Category 2 does not cut the energy supply. (Schneider Electric 2015.)

2.6 Muting function

Muting is a feature of certain configurations of electro sensitive protective devices, which are positioned at the entry and exit points of pallet loads and empty pallets so that they are muted while loads enter and exit the machine. The control system and device employed for muting shall be of the same category and type respectively as specified for the associated electro sensitive protective device.

There are a few conditions that shall be met when muting electro sensitive protective devices. Muting shall only occur during a time in the operating cycle when safety is obtained by alternative means, for example when a loaded pallet is obstructing the access to the danger zone. Muting should be fully automatic, i.e., independent from the operator intervention. Mute initiation shall not rely on a single electrical signal. Mute initiation shall not rely entirely on software signals. Mute signals, which occur in an incorrect sequence, shall neither allow a muted condition nor cause the machine to stop. The safety function of the electro sensitive protective device shall be re-instated immediately following passage of the recognised component through the detection field (DIN EN 415-4 1997.) Figure 4 below shows a muting with two

crossed beams and Figure 5 below shows a sequential arrangement muting with four sensors.

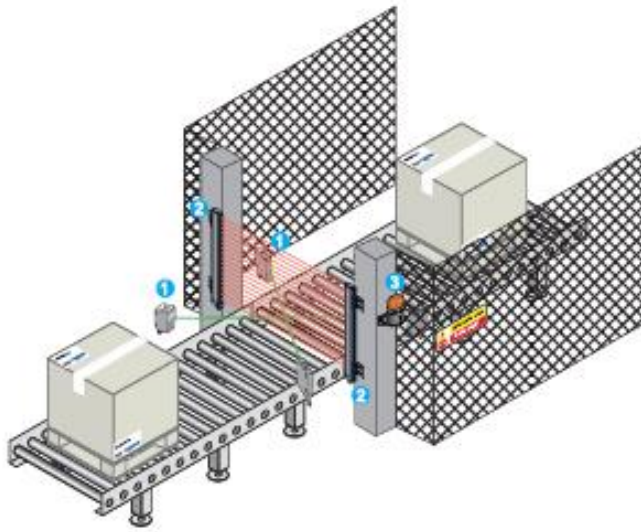
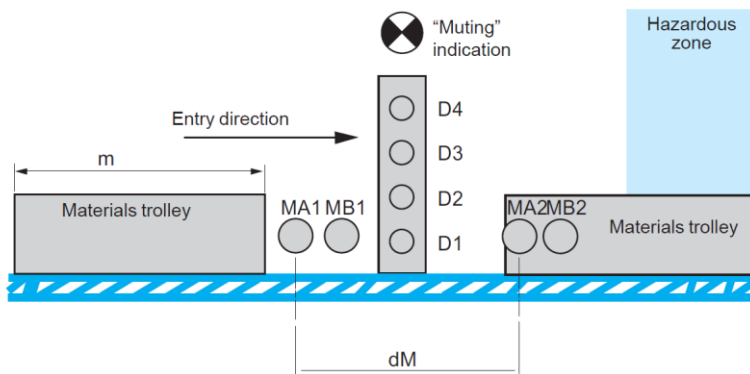


Figure 4 A muting with two crossed beams (Telemecanique [Referred 07.02.2017])



*D1, D2, D3, D4: monitoring photo-electric sensors.
 MA1, MB1, MA2, MB2: "muting" photo-electric sensors.
 m = trolley length (including material)
 dM = distance between MA1, MB1 and MA2, MB2.*

Figure 5 A sequential muting with four sensors (Telemecanique [Referred 07.02.2017])

3 SAFETY COMPONENTS

Safety components within safety-related control systems are designed to prevent mechanical accidents and attain safety in machines. Control systems that obtain safety must be designed to minimize the possibility of danger even if there is a malfunction in an interlock device (Omron [Referred 07.02.2017].)

3.1 Acquire information

Different kind of safety components, which acquire information, are based on different physical principles. Some components are better than others for certain type of applications, even if they have the same working principle. These aspects have to be noticed when reducing the risks. A few of the many safety components are introduced below. (Siirilä T 2008 226).

3.1.1 Emergency stop

E-stops are used to stop the machine if someone is in danger. Emergency stop should be initiated by a single human action when the normal stopping function is deficient. All E-stop buttons should be red with a yellow housing or collar. (Schneider Electric [Referred 30.03.2016]). Emergency stop is not truly a safety function, rather it is an additional safety procedure, but every machine there should be an emergency stop (Siirilä T 2008 280.)



Figure 6 Schneider Electric Emergency stop button. (Schneider Electric [Referred 9.2.2016])

3.1.2 Light curtain

A light curtain has infrared light transmitters and light recognizing receivers. If a human body, a hand or some other obstacle cuts off the light beam, the receiver notices a beam or several cut and sends a signal to the control system. The light curtain has to be installed so far from the danger zone that the machine's movement has time to stop before the person enters the danger zone. (Siirilä 2008, 240-241). Figure 6 below shows a Telemecanique light curtain.



Figure 7 A Telemecanique light curtain

3.1.3 Magnetic safety switch

Magnetic safety switches are typically used to monitor the position of the guards of a machine. The switch consists of two parts, a sensor and a counter-magnetic actuator. Magnetic safety switches are easy to install and they provide high level of safety. Although they provide a low coding and thus are relatively easy to misuse. (Allen-Bradley. 2016.) Figure 7 show a coded magnetic safety switch.



Figure 8 A coded magnetic safety switch (Schneider Electric [Referred 30.11.2016])

3.1.4 Photo-electric sensors

A photo-electric sensor are built of a light beam transmitter (light-emitting diode) and a light-sensitive receiver (photo-transistor). The light-emitting diode emits light when electric current flows through it. The light can be visible or invisible. Detection occurs if an object enters the detection zone and the receiver does not get a signal from the transmitter (Telemecanique 2014.) Figure 9 below shows four different photo-electric sensors.



Figure 9 Telemecanique photo-electric sensors (Telemecanique 2014)

3.1.5 Enabling switch

Enabling switch is designed to operate only in one position. Thus, other positions are designed to cause a stop condition. Enabling switch is used where e.g. safety guarding is not possible. Enabling switch is often used in a manual mode, when the operator has to make some maintenance work or adjustment for the machine. It has to be located so that when the operator is using the machine, he or she should not be in the hazardous area (Schneider 2009.) Figure 10 below shows an enabling switch.



Figure 10 Enabling switch
(Schneider Electric 2009)

3.2 Monitoring & processing

The signals from input devices are usually monitored using safety modules, safety controllers or even safety PLCs, which are used to run the outputs like contactors. The choice of the monitoring unit will depend on many factors: the number of functions, cost, complexity of the safety functions and the amount of cabling (Schneider Electric 2009). Machine builders have to evaluate all these aspects. The safety modules and controllers are used in this research, safety PLCs are typically used in big and very complex applications.

3.2.1 Safety modules

Safety modules implement safety functions and will work to reduce the risk to an acceptable level. When an error occurs, the safety modules initiates a safe and reliable response to a machine. Each safety module monitors a specific function. There are also safety modules on the markets, which can do several safety functions, but only one at the time. Safety modules are a simple and efficient way to provide safety. They provide protection for both the operator and the machine (Galco [Referred 31.03.2016].) Figure 11 below shows a Schneider Electric safety module.



Figure 11 Schneider Electric XPSBAE safety module (Schneider Electric [Referred 30.11.2016])

3.2.2 Configurable safety controllers

Configurable safety controllers can provide all the safety functions but they usually need a software to configure. Safety controller is one option for a safety module, when a machine or application needs more complex configuration or many safety inputs.

3.2.3 Schneider Electric XPSMCM

XPSMCM product offer includes the total of 19 different modules: a controller, a safe mixed I/O expansion module, safe input expansion modules, safe output expansion modules, safe relay output modules, safe speed monitoring modules, safe communication modules and non-safe communication modules.

The safety controller can be used as a standalone device, or it can be connected with maximum 14 safe expansion modules. The maximum number of safety inputs is 128, 16 safety outputs and 26 status outputs. The modules can be attached together with a backplane expansion connector. The configuring of the controller, has to be done by the SoSafe Configurable software. The controller is connected to a PC by a mini-USB cable. The safety system realized including XPSMCM can reach the category 4 and the PL e by conforming to the requirements of EN/IEC 13849-1. Figure 12 below shows a Schneider Electric XPSMCM safety controller.



Figure 12 Schneider Electric XPSMCMCP0802 safety controller (Schneider Electric [Referred 30.11.2016])

3.2.4 SoSafe Configurable software

The SoSafe Configurable application software is used to configure a logic connection between the inputs, processing and outputs of the XPSMCM Modular Safety

Controller system and the components of the application being developed. The controller and its input or output modules form a functional safety system for monitoring and controlling the connected safety components. Figure 13 shows a screenshot of the SoSafe Configurable software.

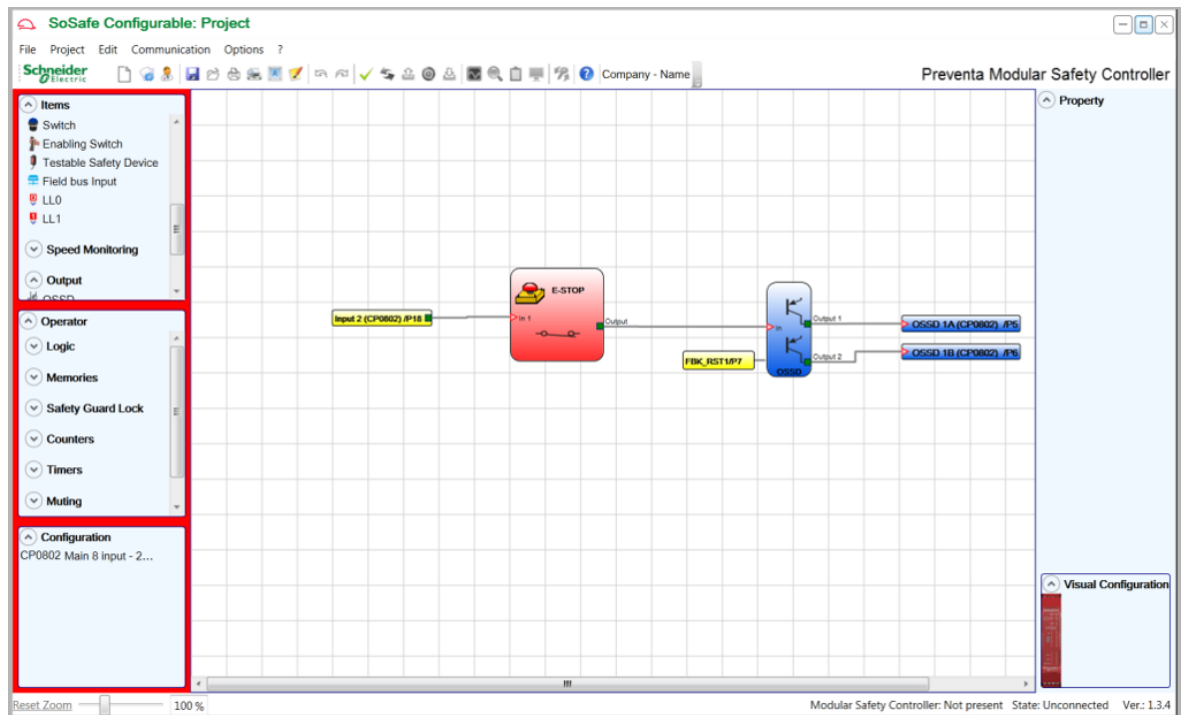


Figure 13 Schneider Electric SoSafe Configurable software (Schneider Electric 2015)

3.3 Contactors

In machine safety, contactors with mirror contacts are used. The essence of the mirror contact function is that normally an open auxiliary contact on a contactor will not close when one of the power contacts are closed and thus cannot close the feedback loop circuitry to a safety module or a safety controller. The mirror contact feature is a mechanical link between the auxiliary contacts and the power contacts of a contactor. (Schneider Electric [Referred 1.11.2016]). Figure 14 below shows how a mirror contact is made.

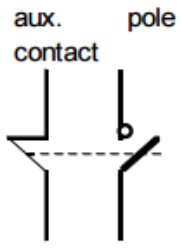


Figure 14 Mirror Contact (Schneider Electric [Referred 1.11.2016])

4 PALLETIZING MACHINE WITH AN AUTOMATIC PALLET DISPENSER

There are many different kinds of packaging machines. For liquids, groceries, consumer goods, just to mention a few. In this thesis, when studying the parcel packaging machines and wrapping machines the focus is on the packaging area. The palletizing machine has to have two different operation modes: normal and the maintenance mode. Figure 15 below shows an example of a palletizing machine.



Figure 15 Columbia FL1000-SW Palletizer (Columbia 2015)

4.1 Normal operation mode

The operator feeds packaged products to the palletizer's own conveyor. A pallet dispenser feeds the pallets from the bottom of the stack. On that pallet, the machine will stack the products. When the pallet is full, the conveyor moves the pallet out of the machine and the operator takes it with a forklift to the storage room or for further operations. The operator also brings the empty pallets to the pallet dispenser when needed. The machine has an automatic mode and a manual mode, selected by using a selector switch. The normal operation mode requires one or two operators, depending on the working speed.

4.1.1 Safety on the normal operation mode

The pallet dispenser has a hand detection light curtain (max distance between beams 30mm) and photoelectric sensors for the muting function. Two photoelectric sensors with the muting function, allow the light curtain's detection function to be temporarily inhibited without triggering the stop function, while the operator is transporting new pallets to the dispenser. Interruption of the light curtain detection zone causes the dispenser's and the palletizer's outputs to go off. The dispenser has one emergency stop pushbutton and one enabling switch for the maintenance mode.

The palletizer has a body detection light curtain (max distance between beams 300mm) and four photoelectric sensors for the muting function. Passing the light curtain's detection zone causes all the safety outputs, except for the exit conveyor, to open. The muting function is enabled by the means of photoelectric sensors. Muting allows the light curtain's detection function to be temporarily inhibited without triggering the stop function. During the muting time interval, material can be transported through the hazardous area. The palletizer is enclosed by a fixed guard with one access door. Opening of the protective guard is detected by the means of a coded magnetic switch. Opening causes the safety system to stop the whole machine. The palletizer has one emergency stop pushbutton and one enabling switch for the maintenance mode. Emergency stop will open all the safety outputs.

The exit conveyor has a body protection light curtain with two photoelectric sensors. The operation of the light curtain can be temporarily inhibited, while the operator is picking a stacked pallet.

For the pallet dispenser and palletizer, there are separate selector switches, so the operator can run the machines separately in the maintenance mode.

4.2 Maintenance mode

Maintenance mode is mainly used for maintenance and adjusting situations. When maintenance mode is used, the machine operates on slow speed and is operated by enabling switch. In maintenance mode, guard monitoring safety inputs are not in use. Situations where maintenance mode is needed are for example during adjusting the palletizer due to packages of different sizes, maintenance and releasing jammed products or pallets.

4.2.1 Safety on maintenance mode

Adjusting and maintenance often require machine movement while accessing the hazardous parts, so reduced speed is required. Access to hazardous zone must be enabled by selector switch "maintenance mode" and movement has to be enabled by enabling switch.

4.3 Hazards according to EN 415-4:1997

The EN 415-4:1997 (Safety of packaging machines Part 4: Palletizers and depalletizers) standard specifies the safety requirements for the design, manufacture and information for safe use of palletizers and depalletizers. These safety requirements apply to automatic and semi-automatic (de)palletizers. They take into account the hazards which may occur during setting, commissioning and decommissioning, adjustment, use according to the information given by the manufacturer, maintenance and cleaning. This standard is used to define possible hazards of palletizer (DIN EN 415-4:1997).

4.3.1 Hazards on normal operation mode

Standard EN 415-4:1997 gives typical hazards, which can occur while using the machine on normal operation mode. Table 1 below shows types of hazard, sources of hazard, possible effects, possible injuries and what level of PL & SIL is required regarding risk assessment.

Table 1 Table of relevant hazards on normal operation mode

| Hazard | Origin of hazard | Possible effects | Examples of injury | Required PL & SIL |
|------------|----------------------|---|----------------------------------|-------------------|
| Mechanical | Conveyor | Trapping, Friction, Drawing-in | Crush injuries, fractures | PLr d SILr 2 |
| Mechanical | Pallet movement | Pallet falling | Crush injuries | PLr d SILr 2 |
| Mechanical | Pallet movement | Load falling | Crush injuries | PLr b SILr 1 |
| Mechanical | Machine movement | Getting hit or crushed | Crush injuries, fractures, death | PLr e SILr 3 |
| Electrical | Electrical equipment | Poorly maintained equipment, failure in isolation | Electric shock, burns, death | PLr e SILr 3 |

4.3.2 Hazards on maintenance mode

Standard EN 415-4:1997 does not show specified hazards for maintenance. The hazards shown on Table 2 are based on own thinking.

Table 2 Table of relevant hazards on maintenance mode

| Hazard | Origin of hazard | Possible effects | Examples of injury | Required PL & SIL |
|-------------|-----------------------|-------------------------------------|-------------------------|-------------------|
| Maintenance | Adjusting machine | Bad posture | Bad back, neck problems | PLr b SILr 1 |
| Maintenance | Product getting stuck | Bad posture, using excessive effort | Bad back, neck problems | PLr b SILr 1 |

4.4 Architecture

Manufacturers can design their machines according to EN ISO 13849 for Performance Level (PL) and IEC 62061 for Safety Integrity Level (SIL). For the palletizing machine, there is the C-Type standard EN 415-4. This standard specifies detailed safety requirements for a palletizing machine. Risk assessment shows that this machine requires PL e & SIL 3, so the processing unit has to reach PL e.

The best solution for this application is to use safety controller. With one-function modules, wiring could be a problem, because of the large amount of inputs. Safety PLC would be too complex to configure and it is not necessary in this application. A controller with three expansion modules is the optimal solution and it can reach to PL e.

Outputs can be for example contactors or drives. In this example application only contactors are used.

4.5 List of needed safety devices

In this application, only Schneider Electric products are used. These components were chosen based on the behavior described on chapter 4.1.1. All needed safety devices are listed on Table 3 below.

Table 3 Table of needed safety devices

| Product | Description | Qty |
|-----------------|---------------------------------------|-----|
| XPSMCMCP0802 | Safety controller | 1 |
| XPSMCMDI1600 | Safe input expansion module 16 inputs | 1 |
| XPSMCMMX0802 | Safe mixed I/O expansion module | 1 |
| XPSMCMDI0800 | Safe input expansion module 8 inputs | 1 |
| XUSxxxxx | Light curtain | 3 |
| XCSDMCxxxx | Coded magnetic switch | 1 |
| OsiSense XU | Photo-electric sensors | 8 |
| Preventa XY2AU1 | Enabling switch | 2 |
| Harmony XALK | Emergency stop push button | 2 |
| LC1D09BD | Tesys Contactor | 3 |

5 WRAPPING MACHINE

Like in packaging machines, there are also many variations in pallet wrapping machines, for example hooding machines, stretch wrapping machines and shrink wrapping machines. A stretch film pallet wrapping machine with a ring is chosen in this application. In this machine, a film carriage moves circularly around the stationary product (see Figure 16) and wraps the pallet by moving from top to bottom of the load.

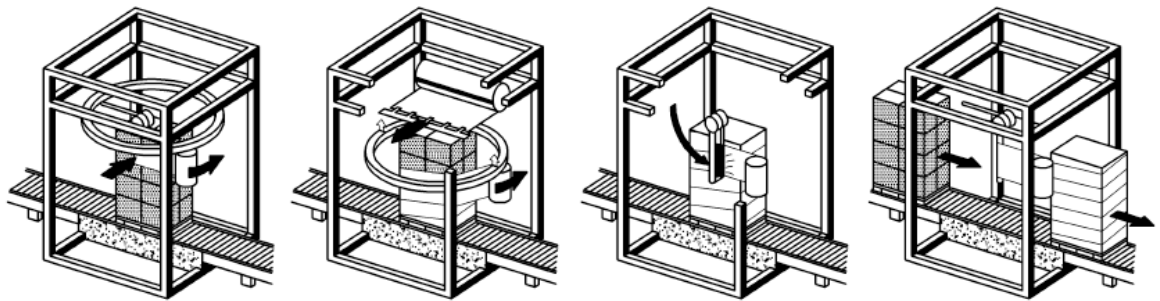


Figure 16 Ring machine

5.1 Normal operation mode

The operator in the wrapping machine brings the products with a forklift to the wrapping machine's own conveyor. A rotating and vertically moving plastic wrap roll wraps the product. After this, the pallet moves to the endpoint, from where the operator takes it off with the forklift and puts it in the storage room. The conveyor will not transport a new product until the previous product is picked up from the conveyor end.

5.1.1 Safety on normal operation mode

In the front panel of the stretch wrapping machine there is a body detection light curtain (max distance between beams 300mm) and photoelectric sensors for muting. Muting function is enabled by means of four photoelectric sensors, which allow

the light curtain's detection function to be temporary inhibited without triggering the safe operating stop.

Exit conveyor has a body protection light curtain with two photoelectric sensors located diagonally on each side of the conveyor. The light curtain can be temporarily inhibited, while the operator picks up the wrapped product.

Wrapping machine has enclosure by fixed guard with one access door. Opening protective guard is detected by means of the coded magnetic switch. Opening causes the safe operating stop to whole machine.

The machine has one emergency stop button and one enabling switch for maintenance mode. The machine has a selector switch, which is used for choosing normal operation mode or maintenance mode.

5.2 Maintenance mode

Maintenance mode is mainly used for maintenance and adjusting situations. When maintenance mode is used, the machine operates on slow speed and is operated by enabling switch. In maintenance mode, safety inputs are not in use. Situations where maintenance mode is needed are for example adjusting the wrapping machine for different plastic wrap rolls, changing a new roll and maintenance.

5.2.1 Safety on maintenance mode

Adjusting and maintenance often require machine movement with reduced speed. Movement has to be enabled by enabling switch. Guard monitoring safety inputs are not in use in maintenance mode.

5.3 Hazards according to EN 415-6:2013

The EN 415-6:2013 is a standard for pallet wrapping machines. This standard deals with safety requirements for machine design, construction, installation, commissioning, operation, adjustment, maintenance and cleaning of pallet wrapping machines (DIN EN 415-6 2013).

5.3.1 Hazards on normal operation mode

The standard EN 415-6:2013 shows typical hazards regarding the use of the machine on normal operation mode. Table 4 below shows types of hazard, sources of hazard, possible effects, possible injuries and estimated PL & SIL regarding risk assessment.

Table 4 Table of relevant hazards on normal operation mode

| Hazard type | Origin of hazard | Possible effects | Examples of injury | Estimated PL & SIL |
|-------------|----------------------|---|----------------------------------|--------------------|
| Mechanical | Conveyors | Friction, Drawing-in | Crush injuries, fractures | PL d SIL 2 |
| Mechanical | Pallet movement | Pallet falling | Crush injuries | PL d SIL 2 |
| Mechanical | Pallet movement | Load falling | Crush injuries | PL b SIL 1 |
| Mechanical | Machine movement | Getting hit or crushed | Crush injuries, fractures, death | PL e SIL 3 |
| Electrical | Electrical equipment | Poorly maintained equipment, failure in isolation | Electric shock, burns, death | PL e SIL 3 |

5.3.2 Hazards on maintenance mode

Table 5 below shows the most likely hazards, which can most likely occur while using the machine on maintenance mode. Hazards are listed by using own thinking.

Table 5 Table of relevant hazards on maintenance mode

| Hazard | Origin of hazard | Possible effects | Examples of injury | Estimated PL & SIL |
|-------------|----------------------------------|-------------------------------------|-------------------------|--------------------|
| Maintenance | Adjusting machine | Bad posture | Bad back, neck problems | PL b SIL 1 |
| Maintenance | Loading new roll of plastic wrap | Bad posture, using excessive effort | Bad back, neck problems | PL b SIL 1 |

5.4 Architecture

Manufacturers can design their machines according EN ISO 13849 for Performance Level (PL) and IEC 62061 for Safety Integrity Level (SIL). For the wrapping machine, there is the C-Type standard EN 415-6. This standard specifies detailed safety requirements for a wrapping machine. Risk assessment shows this machine requires PL e & SIL 3, so processing unit has to reach PL e.

The best solution for this application is to use a safety controller. With one-function modules wiring could be a problem, because of the large amount of inputs. Safety PLC would be too complex to configure, it is expensive, and it is not necessary in this application. A controller with an expansion module is the optimal solution, and can reach to PL e. Outputs can be for example contactors or drives. Only contactors are used in this example application.

5.5 List of materials

Table 6 below shows what safety devices are needed in this application. Only Schneider Electric products are used in this application.

Table 6 Table of needed safety devices

| Product | Description | Qty |
|-----------------------|-----------------------------|------------|
| Preventa XPSMCMCP0802 | Safety controller | 1 |
| Preventa XPSMCMDI1600 | Safe input expansion module | 1 |
| XUSL4E | Light curtains | 2 |
| XCSDMP | Coded magnetic switch | 1 |
| OsiSense XU | Muting sensors | 6 |
| Preventa XY2AU1 | Enabling switch | 1 |
| Harmony XALK | Emergency Stop push button | 1 |
| LC1D09BD | Tesys Contactor | 1 |

6 BENDING PRESS

Bending presses are machines used to bend sheet metal. The machine typically has two parts, the upper and the lower part. The upper part holds the tooling and a punch, which has a V shape to it. The lower part has a matching shape, called the *die*. These two parts are pressed towards each other so they force a metal sheet between them to bend. On the market, there are a few types of bending presses: mechanical, pneumatic, hydraulic and servo-electric, divided by the means of applying force (SheetMetal.me 2015). Figure 17 below shows a Cincinnati hydraulic bending press.



Figure 17 Cincinnati bending press

6.1 Operation principle

The operator chooses the applicable *die* for the work piece and puts it on the working bench. The bending press is operated with a 2-hand control station. The press bends the metal sheet to desired shape. At the end of the cycle press goes up and the operator can remove the bended metal sheet from the *die*.

6.2 Safety

The 2-hand control station is designed to help control the location of the operator's hands outside the hazardous area while the machine is operating. Both actuators must be activated synchronously to make the outputs to activate. If one of two pushbuttons is released, outputs go down until both pushbuttons are released and pressed again synchronously.

6.3 Hazards according EN 12622

According to EN 12622 there are some hazards when using the bending press. Table 7 below shows types of hazard, sources of hazard, possible effects, possible injuries and estimated PL & SIL regarding risk assessment.

Table 7 Table of relevant hazards

| Hazard | Origin of hazard | Possible effects | Examples of injury | Estimated PL & SIL |
|------------|------------------|---------------------------------------|-----------------------------------|--------------------|
| Mechanical | Machine movement | Crushing, Cuts, Amputation, Death | Crushing, Cuts, Amputation, Death | PL e SIL 3 |
| Mechanical | Sharp edges | Material causes cuts | Cuts | PL c SIL 1 |
| Mechanical | Die | Parts dropping | Crushing | PL c SIL 1 |
| Mechanical | Moving parts | Maintenance, Impact from moving parts | Bruising, Fractures | PL c SIL 1 |

6.4 Architecture

Manufacturers can design their machines according EN ISO 13849 for Performance Level (PL) and IEC 62061 for Safety Integrity Level (SIL). For the bending press, there is the C-Type standard EN 12622. This standard specifies detailed safety requirements for a machine. Risk assessment shows that this machine requires PL e & SIL 3, so processing unit has to reach PL e & SIL 3.

The best solution for this application is to use one-function modules, because there are only three different inputs. There is no need for software configuration, and wiring is easy with standard inputs. Modules can reach required PL and SIL. In this application, outputs are contactors.

6.5 List of materials

Table 8 below shows what safety devices is needed for this application. Only Schneider Electric products are used in this application.

Table 8 Table of needed safety devices

| Product | Description | Qty |
|----------------|------------------------------|------------|
| XPSBAE | 2-Hand control safety module | 1 |
| XPSAFL | Safety light curtain module | 1 |
| XUSL4E | Light curtain | 1 |
| XYS2SB | 2-Hand control station | 1 |
| XCSDMC | Coded Magnetic Switch | 1 |
| XPSDMB | Coded Magnetic Switch module | 1 |
| LC1D09BD | Tesys Contactor | 1 |

7 SAFETY DATA

This section describes performance level (PL) and safety integrity level (SIL) and how they are related in safety calculations. Second part of this section shows how to create safety calculations using SISTEMA software tool. In the end of section, safety calculation formulas can be found and values that are used in this research.

7.1 Safety Integrity Level (SIL) & Performance Level (PL)

The SIL certification is a tool for measuring the amount of risk reduction provided by a Safety Instrumented Function. It determines the acceptable failure rate of an individual device. The SIL has four different levels: Level 1 is the lowest and level 4 is the highest level of safety. Level 1...3 is applicable for machines and level 4 only for possible mass destruction causing process plants like e.g. nuclear power plants, oil refineries or big chemical plants (SOR [Referred 13.12.2016]). Regarding the EN 13849 standard, safety-related parts to perform a safety function is expressed through the determination of the performance level (SFS-EN ISO 13849-1/AC). Table 9 below shows relations between PL, SIL, PFHD and MTTF_d.

Table 9 Relations between PL, SIL, PFHD and MTTF_d (Siirilä T 2009 147)

| Safety Integrity Level (SIL) (IEC 61508-1) | Performance Level (PL) (EN ISO 13849-1) | Probability of a dangerous failure per hour (PFH _d) | Mean time to dangerous failure (MTTF _d) |
|---|--|---|---|
| - | a | $10^{-5} \dots 10^{-4}$ | 1 ... 10 |
| 1 | b | $3 * 10^{-6} \dots 10^{-5}$ | 10 ... 40 |
| 1 | c | $3 * 10^{-6} \dots 3 * 10^{-5}$ | 40 ... 100 |
| 2 | d | $10^{-7} \dots 10^{-6}$ | 100 ... 1000 |
| 3 | e | $10^{-8} \dots 10^{-7}$ | 1000 ... 10 000 |

7.2 SISTEMA

The IFA has created a safety integrity software tool for the evaluation of machine applications called SISTEMA. This tool enables you to model the structure of the safety-related control components based on the designed architectures. It also provides automated calculation of the reliability values with various levels of detail, including that of the attained Performance Level (PL). Many machine automation component manufacturing companies use SISTEMA and have created their own libraries to SISTEMA, as Schneider Electric has done. In this research, all calculations are made with SISTEMA.

7.2.1 Creating SISTEMA calculations

The SISTEMA software tool can be downloaded from IFA's website. There are also the SISTEMA libraries of many automation component manufacturers, which can be downloaded to personal use.

When making safety calculations with SISTEMA, I first added Schneider Electric SISTEMA libraries to the system by clicking "Library". Libraries include Schneider Electric products and their data, which are used in the calculations. Adding the library is shown in Figure 18.

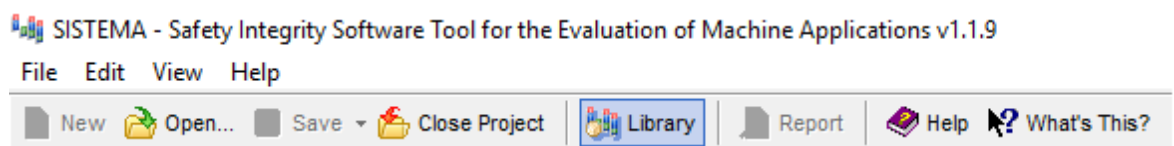


Figure 18 Adding the library

Then by clicking “Add local library” local libraries could be selected from local folder structure, as shown in Figure 19.

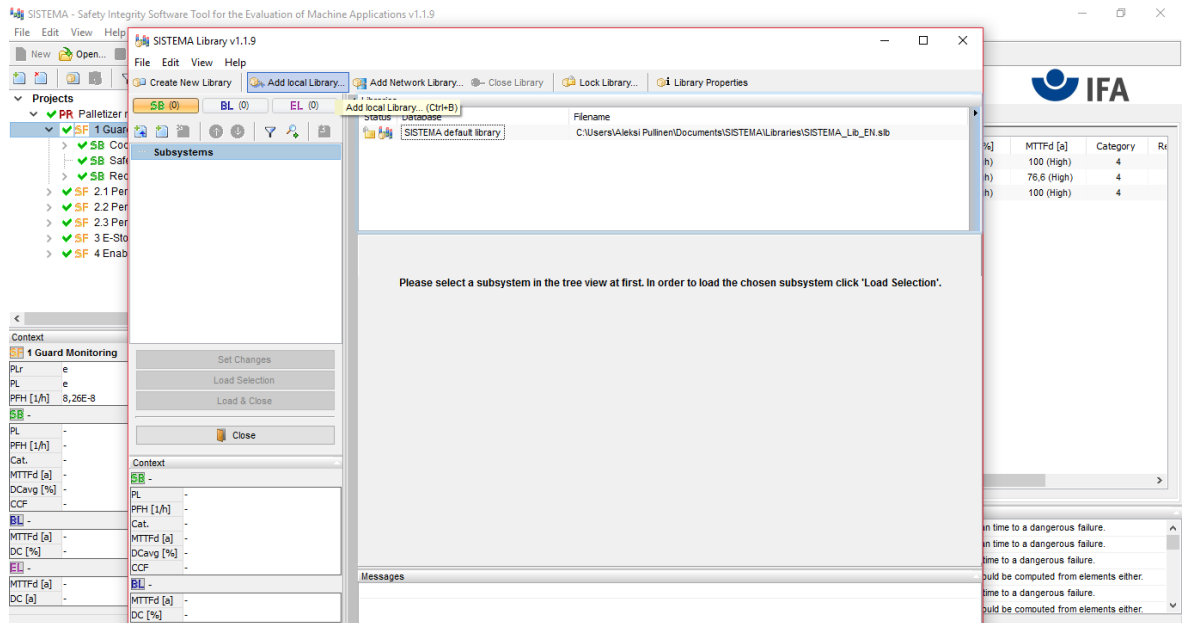


Figure 19 Adding local library

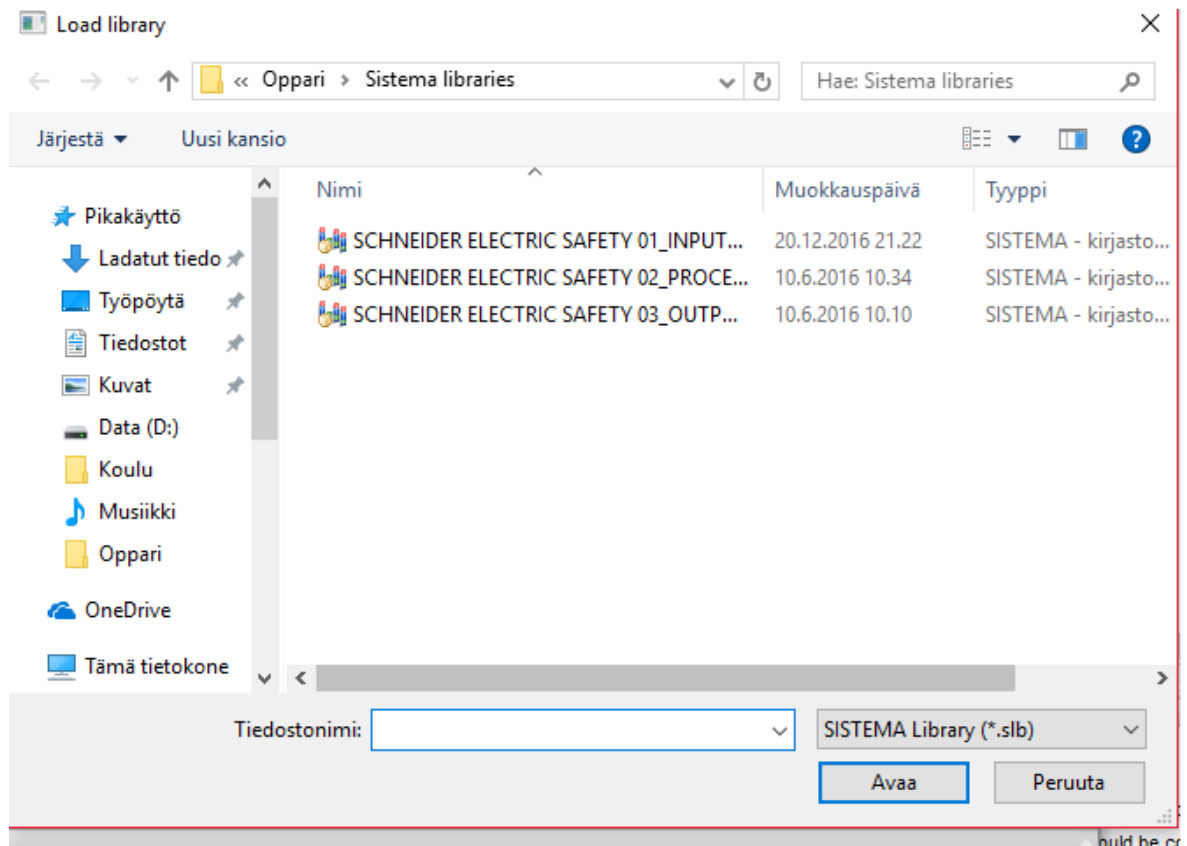


Figure 20 Choosing libraries from the hard disk

Schneider Electric libraries are divided to input-, processing- and output libraries as can be noted in Figure 20 above. Each one has to be chosen individually. Now Schneider Electric component libraries have been included to Sistema user library and can be used in the calculations. Now a new project with Schneider Electric products can be created by clicking “New” button on up left as shown in Figure 21 below.

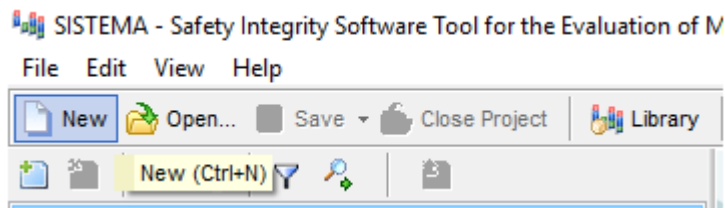


Figure 21 Creating a new project

Then the software creates a new project on the project tree on the left side and a window pops up as shown in Figure 22 below.

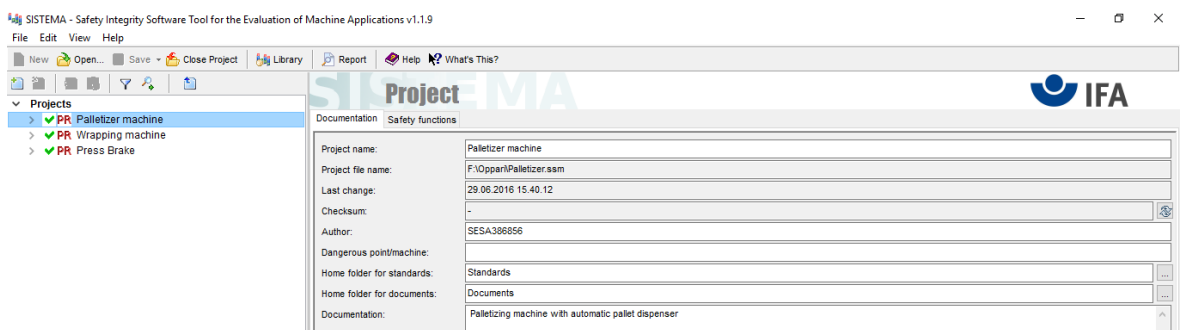
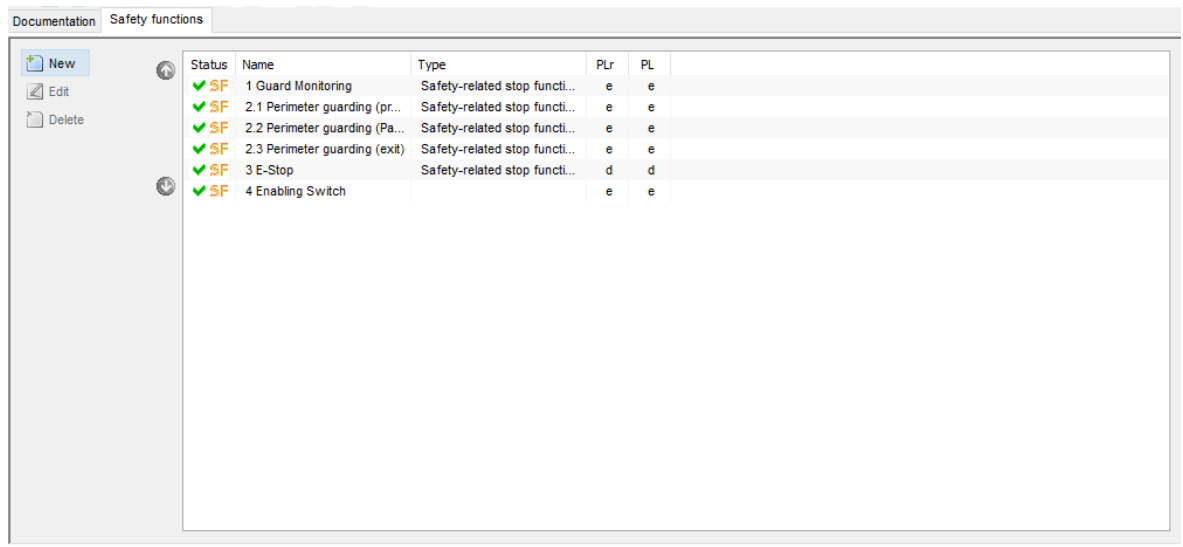


Figure 22 The project tree

Here the project can be named and other documentation regarding the project can be added. The other tab on this window is “Safety Functions”. In Figure 23 below the safety functions are already created.

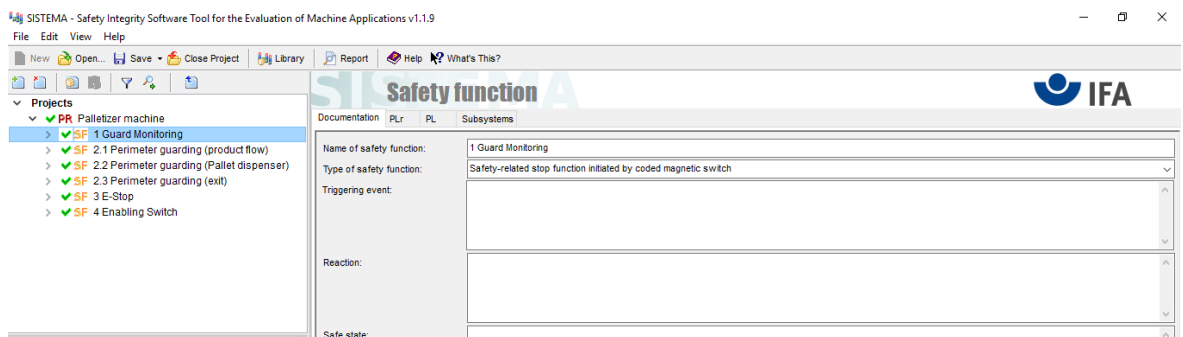


| Status | Name | Type | PLr | PL |
|--------|-------------------------------|-------------------------------|-----|----|
| ✓ SF | 1 Guard Monitoring | Safety-related stop functi... | e | e |
| ✓ SF | 2.1 Perimeter guarding (pr... | Safety-related stop functi... | e | e |
| ✓ SF | 2.2 Perimeter guarding (Pa... | Safety-related stop functi... | e | e |
| ✓ SF | 2.3 Perimeter guarding (exit) | Safety-related stop functi... | e | e |
| ✓ SF | 3 E-Stop | Safety-related stop functi... | d | d |
| ✓ SF | 4 Enabling Switch | | e | e |

Figure 23 Safety functions

On Safety functions tab new safety functions can be added to the project. Depending on how machine safety works, it is recommended to divide the complete safety of the machine to various safety functions.

After clicking “New” button on left side, the software gives a window where the safety function can be created. All created safety functions appear on the list and under the created project on the project tree on the left side, as shown in Figure 24 below.



SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications v1.1.9

File Edit View Help

New Open... Save Close Project Library Report Help What's This?

Projects

- PR Palletizer machine
 - ✓ SF 1 Guard Monitoring
 - ✓ SF 2.1 Perimeter guarding (product flow)
 - ✓ SF 2.2 Perimeter guarding (Pallet dispenser)
 - ✓ SF 2.3 Perimeter guarding (exit)
 - ✓ SF 3 E-Stop
 - ✓ SF 4 Enabling Switch

Safety function

Documentation PLr PL Subsystems

Name of safety function: 1 Guard Monitoring

Type of safety function: Safety-related stop function initiated by coded magnetic switch

Triggering event:

Reaction:

Safe state:

Figure 24 Overview of safety function

On documentation tab the safety function can be named and described more precisely. On the next tab, “PLr”, the required Performance Level has to be determined. It can be done either by risk graph as shown in Figure 25, or by entering the PLr value directly. In this calculation risk graph was used. The user has to define severity

of injury, frequency and/or exposure times to hazard and the possibility of avoiding hazard.

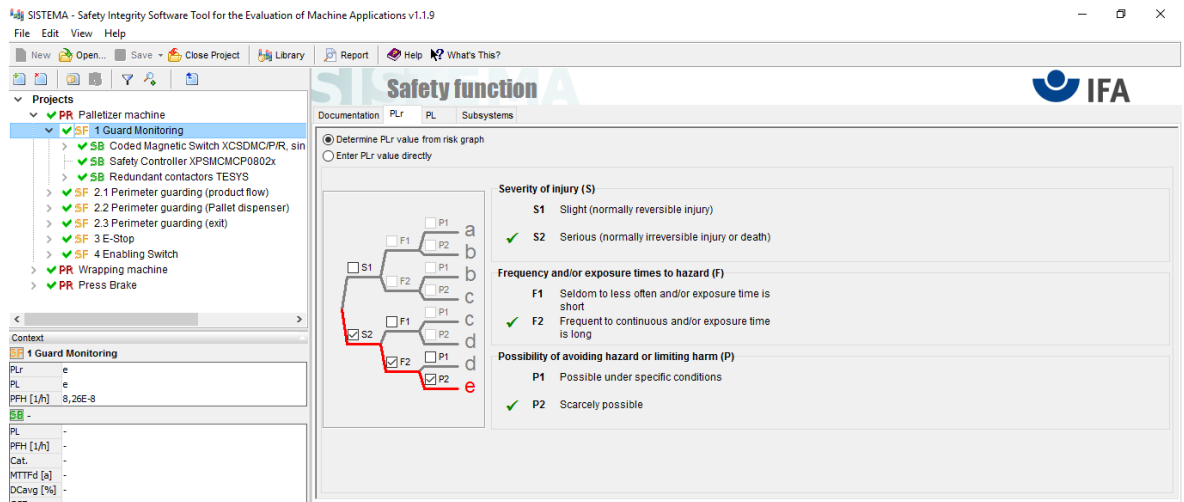


Figure 25 PLr Tab

The PL tab shows that PL has to be determined from the subsystems, which are defined next. The subsystems are shown in Figure 26 below.

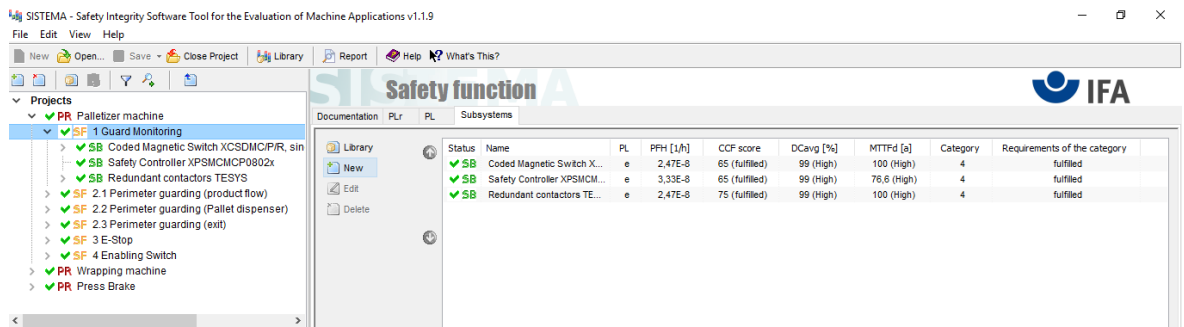


Figure 26 The subsystems

The subsystems used in this thesis can be found directly from the Schneider Electric SISTEMA libraries, which were added in the beginning. By clicking the “Library” button above the “New” button the libraries open and subsystems can be added to the safety function. Figure 27 below shows the subsystems.

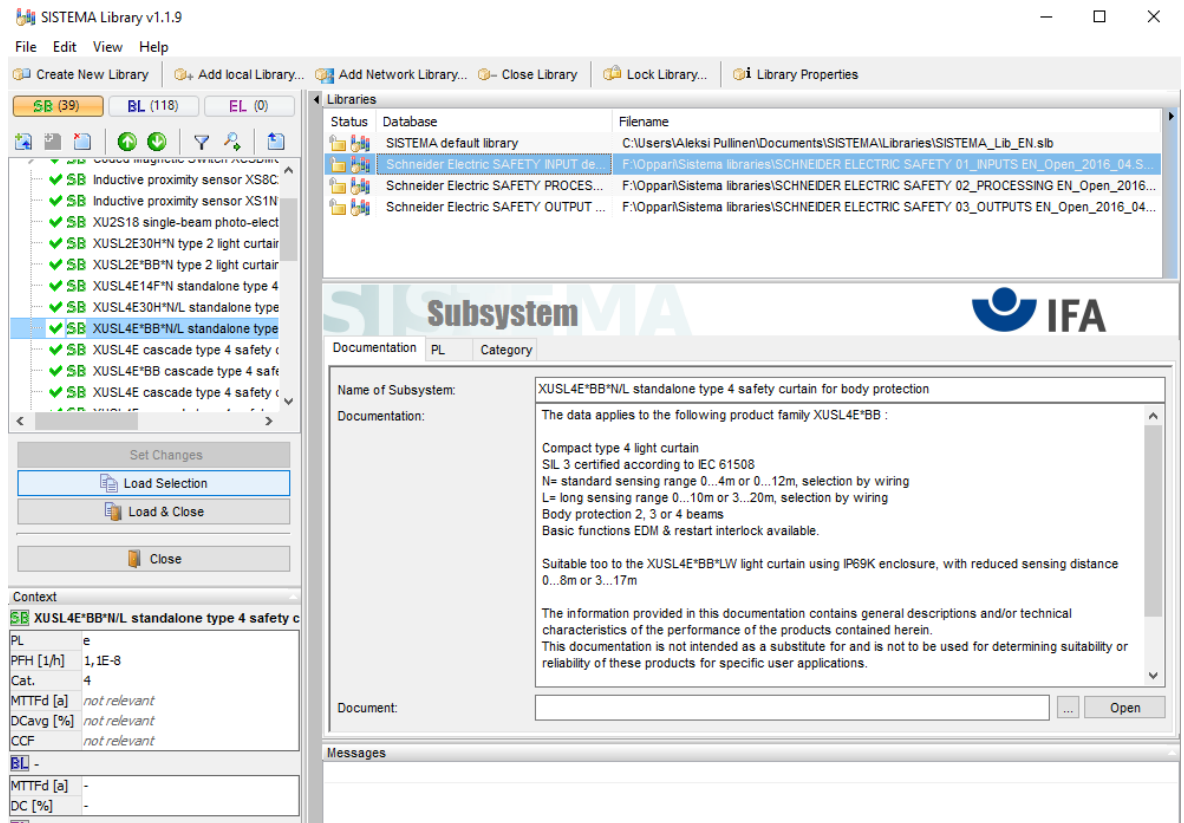


Figure 27 Subsystem from the library

After choosing the wanted subsystem and clicking “Load Selection”, the software adds a subsystem to the safety function. Like this, other Inputs, processing, and output subsystems are added to the project and they appear on the left side of the project tree, under the safety function.

This example is performed by using a light curtain as an input, a safety controller as a processing device and contactors as output. The values of these devices are included in the libraries.

After choosing the contactors from the output library, some values have to be determined. Under the contactor subsystem, there are channels 1 and 2 (see Figure 28). In this safety function the channels are the same but values have to be given to both channels.

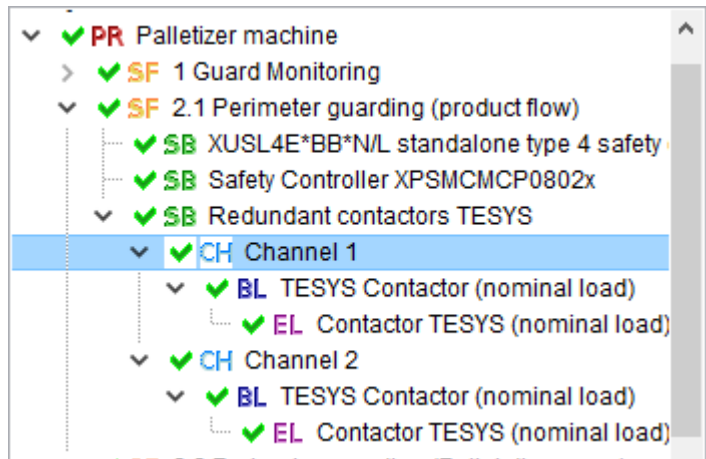


Figure 28 Project tree

Under both channels, there are blocks and under the blocks there are elements as shown in Figure 29 below.

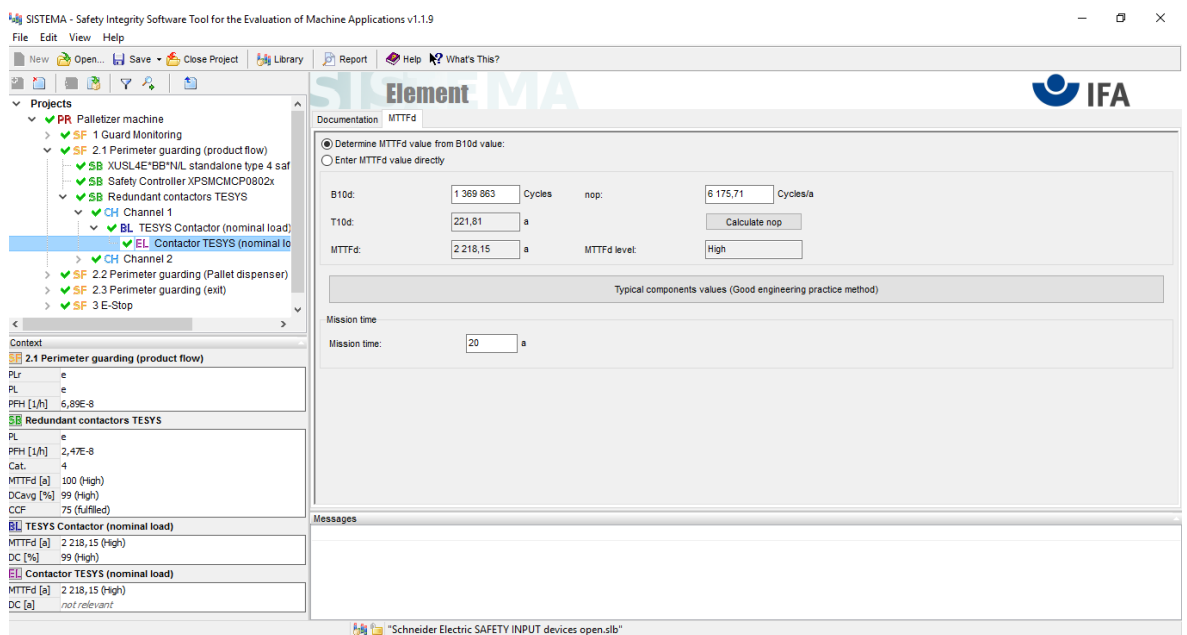


Figure 29 Elements

In the element section, on the $MTTF_d$ tab, the number of operations has to be calculated (n_{op}). By clicking “Calculate nop” a new window opens as shown in Figure 30 below.

The screenshot shows a dialog box titled "Nop" with a close button (X) in the top right corner. On the left side, there is a mathematical formula: $n_{op} = \frac{d_{op} \times h_{op} \times 3600 \text{ s/h}}{t_{cycle}}$. To the right of the formula are three input fields: "d_op:" with a dropdown menu set to "Days", "h_op:" with a dropdown menu set to "Hours", and "t_cycle:" with a dropdown menu set to "Seconds". At the top right of the dialog is a "Delete" button. At the bottom are "Cancel" and "Ok" buttons.

Figure 30 Calculating the number of operations

In this window the software calculates the number of operations when the user gives the required values. These values can be seen in table 10. The software shows to the user if the safety function is acceptable by a green checkmark. A red X is given if the safety function is not acceptable. In that case the values have to be changed to attain the required PLr.

When the “Report” up in the middle is clicked, the software prints a report of the project. For more information, see Appendix 1.

7.3 Safety calculations

A required performance level (PLr) must be specified for each intended safety function. The performance level (PL) attained by the control system must be validated by verifying whether it is greater than or equal to the PLr.

Manufacturers determine B_{10d} value for the components. B_{10d} value is the number of cycles performed until 10 % of the components will fail dangerously. With B_{10d} and n_{op} , the mean number of annual operations, $MTTF_d$ for components can be calculated as

$$MTTF_d = \frac{B_{10d}}{0,1 * n_{op}} \quad (1)$$

where

$$n_{op} = \frac{d_{op} * h_{op} * 3600 \text{ s/h}}{t_{cycle}} \quad (2)$$

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

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

t_{cycle} is the mean time between two cycles of the component in seconds per cycle. (SFS-EN ISO 13849-1/AC 2009).

This is the palletizer perimeter guarding on product flow. The subsystem solution is explained briefly below.

The number of operations (n_{op}), 6176 is calculated so that there are 220 working days per year, the machine will operate 12 hours per day and the cycle time is 1438 seconds.

Table 10 Table of referred values

| | |
|--|------|
| Cycle Time | 1538 |
| Number of hours' operation per day (h) | 12 |
| Number of days' operation per year | 220 |
| Number of operations per year (n_{op}) | 6176 |

Table 11 Safety level calculation

| Safety Level Calculation | | Values |
|--|-------------------------------------|----------|
| Acquire Information (Input) XUSL4E | PL | e |
| | Category | 4 |
| | PFH _D resulting (1/h) | 1,1E-8 |
| Monitoring and Processing (Logic) XPSMCMCP0802 | PL | e |
| | Category | 4 |
| | PFH _D resulting (1/h) | 3,33E-8 |
| Stop the Machine Devices (Output) LC1 (nominal load) | PL | e |
| | Category | 4 |
| | MTTF _d (years) | 2 218,15 |
| | DC (%) | 99 |
| | CCF | 75 |
| | PFH _D resulting (1/h) | 2,47E-8 |
| Safety Function (Result) | PL attained | e |
| | PFH _D resulting (1/h) | 6,89E-8 |

Mean time to dangerous failure (MTTF_d) values exceeding 100 years will be limited to this value to avoid overstating the component reliability in comparison with the other notable influencing variables, such as the architecture or testing.

A PFH_d value of 1.1×10^{-8} has been stated for a body protection light curtain. For a safety controller XPSMCMCP0802 3.33×10^{-8} has been stated. These values come directly from the safety device data and have been certified by a notified body.

For the contactor, the B₁₀ value corresponds under a nominal load to an electrical lifetime of 1 369 863 switching cycles.

Measures against common cause failures must attain at least 65 points.

The safety related control system corresponds to category 4 with high MTTF_d. The complete functional safety system results in average probability of dangerous failure (PFH_d) of 6.89×10^{-8} . This corresponds to PL e and SIL 3.

8 SUMMARY

The goal of this thesis was to make machine safety architectures for a palletizer with an automatic dispenser, a wrapping machine and a bending press. The machine safety architectures for these three machines can be used as examples for machine builders. For each machine, safety architecture was planned by using Schneider Electric catalogue.

In the theory part machine safety standards were explained and also the muting function was as it was a crucial function when planning the palletiser or the wrapping machine. In this thesis standard EN 13849 and C type standards EN 415-4, EN 415-6 and EN 12622 were used and followed. A big part of the theory concentrated on different kinds of safety devices and their working principles. It is important for machine builders to know which kind of opportunities they have and how they can solve the issue with safety devices.

The practical part consisted of performing risk assessment regarding possible hazards, figuring out safe machine operation, designing the architecture, choosing applicable safety devices and calculating safety performance. Also wiring diagrams were planned and drawn for each machine, but they were not shown in this thesis. For the palletiser and the wrapping machine also a program with SoSafe Configurable was made. This thesis benefits the marketing safety team, when dealing with machine builders.

BIBLIOGRAPHY

- Allen-Bradley. 2016. Safety Function: Light Curtain with Muting (Two Sensor L-type) and Configurable Safety Relay. [Online publication]. Rockwell Automation Inc. [Referred 25.10.2016]. Available: http://literature.rockwellautomation.com/idc/groups/literature/documents/at/safety-at136_-en-p.pdf
- Allen-Bradley. 2016. Protective Measures and Complementary Equipment. [www-document]. Rockwell Automation Inc. [Referred 1.11.2016]. Available: <http://www.ab.com/en/epub/catalogs/3377539/5866177/3378076/7131359/Non-Contact-Interlock-Switches.html>
- Columbia. 2015. FL1000-SW. [Online publication]. Columbia Palletizers. [Referred 30.11.2016]. Available: <http://www.palletizing.com/products/floor-level-palletizers/fl1000-sw>
- DIN EN 415-4. 1997. Safety of packaging machines- Part 4: Palletisers and depalletisers. Berlin: Deutsches Institut für Normung.
- DIN EN 415-6. 2013. Safety of packaging machines- Part 4: Pallet wrapping machines; English version EN 415-6:2013, English translation of DIN EN 415-6:2013-09. Berlin: Deutsches Institut für Normung.
- Galco. No data available. Safety Relays – Where and How They Work. [www-document]. Galco. [Referred 31.03.2016]. Available: <http://www.galco.com/comp/prod/saftrela.htm>
- NIOSH. 2014. Machine Safety. [www-document]. The National Institute for Occupational Safety and Health. [Referred 23.03.2016]. Available: <http://www.cdc.gov/niosh/topics/machine/>
- Omron. No data available. Technical Support – Safety Components. [www-document]. Omron. [Referred 07.02.2017]. Available: https://www.ia.omron.com/support/guide/3/safety_components.html
- Schneider Electric. No data available. Company profile. [www-document]. Schneider Electric. [Referred 9.2.2016]. Available: <http://www2.schneider-electric.com/sites/corporate/en/group/profile/history/schneider-electric-history.page>
- Schneider Electric. No data available. Schneider Electric products page. [www-document]. Schneider Electric. [Referred 30.03.2016]. Available: <http://www.schneider-electric.com/ww/en/>
- Schneider Electric. No data available. Schneider Electric products page. [www-document]. Schneider Electric. [Referred 30.11.2016]. Available: <http://www.schneider-electric.com/ww/en/>

- Schneider Electric. 2009. Safe Machine Handbook. [Online publication]. Schneider Electric. [Referred 24.2.2016]. Available: <http://www2.schneider-electric.com/documents/original-equipment-manufacturers/en/shared/safety-handbook-v3.pdf>
- Schneider Electric. 2015. 01 Machine Safety General Presentation Safety_Aug_2015_Short_UK. [PowerPoint-presentation]. Schneider Electric [Referred 01.03.2016]. Available: Only for internal use
- Schneider Electric. No data available. Mechanically linked contacts and Mirror contacts. [Online publication]. Schneider Electric. [Referred 1.11.2016] Available: http://www2.schneider-electric.com/resources/sites/SCHNEIDER_ELECTRIC/content/live/FAQS/212000/FA212124/en_US/R018_mechanically_linked_contacts_and_mirror_contacts.pdf
- SFS-EN ISO 13849-1/AC. 2009. Safety of machinery- Safety-related parts of control systems- Part 1: General principles for design (ISO 13849-1:2006). Helsinki: Finnish Standards Association.
- SheetMetal.me. 2015. Brake Press. [www-document]. SheetMetal.me. [Referred 8.11.2016]. Available: <http://sheetmetal.me/tooling-terminology/brake-press/>
- Sick. No data available. The Risk Assessment Process. [Online publication]. Sick. [Referred 10.02.2017]. Available: <https://www.sick.com/medias/SICK-White-Paper-Part-2-Risk-Assessment-Final.pdf?context=bWFzdGVyfHJvb3R8NDUyNTM0fGFwcGxpY2F0aW9uL3BkZnx-oMDYvaGNhLzg5MDIxOTg4MjA4OTQucGRmfDU1YjU-xMGFIZmRiNjVjZDA0MDAyNmEyZDkzMzM5ZjJhNTRhMjdjNDZjOD-RkN2JhMTMyMWYxNDY0NDM1NmU3NjM>
- Siirilä, T. 2008. Koneturvallisuus, EU-määräysten mukainen koneiden turvallisuus. 2th renewed edition. Helsinki: Inspecta Koulutus Oy.
- Siirilä T. 2009. Koneturvallisuus, Ohjausjärjestelmät ja turvalaitteet. 2th renewed edition. Helsinki: Inspecta Koulutus Oy
- SOR. No data available. Safety Integrity Level, Quick Guide. [Online publication]. SORINC. [Referred 13.12.2016]. Available: <http://www.sorinc.com/assets/images/uploads/2012/09/sil-quick-guide-1528.pdf>
- Telemecanique. 2014. Photo-electric sensors OsiSense XU. [Online publication]. Telemecanique. [Referred 1.11.2016]. Available: http://download.schneider-electric.com/files?p_Doc_Ref=DIA4ED2140904EN
- Telemecanique. No data available. Safety light curtains Preventa XUSL. [Online publication]. Telemecanique.[Referred 07.02.2017]. Available: http://download.schneider-electric.com/files?p_File_Id=1676503334

APPENDICES

APPENDIX 1 Palletizer machine SISTEMA overview

APPENDIX 2 Wrapping machine SISTEMA overview

APPENDIX 3 Bending press SISTEMA overview

APPENDIX 1

SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine



Projectname: Palletizemachine

File date: 29.06.2016 15.40.12 Report date: 13.12.2016 Checksum: 392325f5e294b39793ab7445463f2171

PR Projectname: Palletizemachine

| | |
|-------------------------|--|
| Author: | SESA388856 |
| Dangerouspoint/machine: | |
| Documentation: | Palletizing machine with automatic pallet dispenser |
| Document: | |
| Filename: | F:\Oppari\Palletizer.ssm |
| Versionofsoftware: | 1.1.9 build 2 |
| Versionofstandard: | ISO 13849-1:2006, ISO 13849-1/Cor1:2009, EN ISO 13849-1:2006, EN ISO 13849-1:2008 |
| Checksum: | 392325f5e294b39793ab7445463f2171 |
| Options: | <input checked="" type="checkbox"/> Use DC intermediate levels for calculation of PFH (more precise) <input type="checkbox"/> Raise the MTTFd-capping for Category 4 from 100 to 2500 years |
| Status: | green |
| Note: | There are no warnings listed for this project (or it's subordinate basic elements). |

Containedsafetyfunctions

| | | | | |
|--|-----------------|---------------|-------------------|---------------|
| SF Name: 1 Guard Monitoring | Required: PLr e | Reached: PL e | PFH[1/h]: 8,26E-8 | Status: green |
| SF Name: 2.1 Perimeterguarding (productflow) | Required: PLr e | Reached: PL e | PFH[1/h]: 6,89E-8 | Status: green |
| SF Name: 2.2 Perimeterguarding (Palletdispenser) | Required: PLr e | Reached: PL e | PFH[1/h]: 6,89E-8 | Status: green |
| SF Name: 2.3 Perimeterguarding (exit) | Required: PLr e | Reached: PL e | PFH[1/h]: 6,89E-8 | Status: green |
| SF Name: 3 E-Stop | Required: PLr d | Reached: PL d | PFH[1/h]: 1,07E-7 | Status: green |
| SF Name: 4 EnablingSwitch | Required: PLr e | Reached: PL e | PFH[1/h]: 8,26E-8 | Status: green |

APPENDIX 2

SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine



Projectname: Wrappingmachine

File date: 29.06.2016 20.20.22 Report date: 13.12.2016 Checksum: 06266e97086f38b95cf78a999c901314

PR Projectname: Wrapping machine

| | |
|-------------------------|--|
| Author: | SESA386856 |
| Dangerouspoint/machine: | |
| Documentation: | |
| Document: | |
| Filename: | F:\OppariWrappingmachine.ssm |
| Versionofsoftware: | 1.1.9 build 2 |
| Versionofstandard: | ISO 13849-1:2006, ISO 13849-1/Cor1:2009, EN ISO 13849-1:2006, EN ISO 13849-1:2008 |
| Checksum: | 06266e97086f38b95cf78a999c901314 |
| Options: | <input checked="" type="checkbox"/> Use DC intermediate levels for calculation of PFH (more precise) <input type="checkbox"/> Raise the MTTFd-capping for Category 4 from 100 to 2500 years |
| Status: | green |
| Note: | There are no warnings listed for this project (or it's subordinate basic elements). |

Containedsafetyfunctions

| | | | | |
|--|-----------------|---------------|-------------------|---------------|
| SF Name: 1 Guard Monitoring | Required: PLr e | Reached: PL e | PFH[1/h]: 8,26E-8 | Status: green |
| SF Name: 2.1 Perimeterguarding(frontopening) | Required: PLr e | Reached: PL e | PFH[1/h]: 6,89E-8 | Status: green |
| SF Name: 2.2 Perimeterguarding(exit) | Required: PLr e | Reached: PL e | PFH[1/h]: 6,89E-8 | Status: green |
| SF Name: 3 E-Stop | Required: PLr e | Reached: PL e | PFH[1/h]: 8,26E-8 | Status: green |
| SF Name: 4 EnablingSwitch | Required: PLr e | Reached: PL e | PFH[1/h]: 8,26E-8 | Status: green |

APPENDIX 3

SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine



Projectname: Press Brake

File date: 13.12.2016 18.10.18 Report date: 13.12.2016 Checksum: 531ea47f7748e6c66b04e42842ddc5c1

PR Projectname: Press Brake

| | |
|-------------------------|--|
| Author: | SESA388856 |
| Dangerouspoint/machine: | |
| Documentation: | |
| Document: | |
| Filename: | F:\Oppari\PressBrake\PressBrake.ssm |
| Versionofsoftware: | 1.1.9 build 2 |
| Versionofstandard: | ISO 13849-1:2008, ISO 13849-1/Cor1:2009, EN ISO 13849-1:2008, EN ISO 13849-1:2008 |
| Checksum: | 531ea47f7748e6c66b04e42842ddc5c1 |
| Options: | <input checked="" type="checkbox"/> Use DC intermediate levels for calculation of PFH (more precise) <input type="checkbox"/> Raise the MTTFd-capping for Category 4 from 100 to 2500 years |
| Status: | green |
| Note: | There are no warnings listed for this project (or it's subordinate basic elements). |

Containedsafetyfunctions

| | | | | |
|--------------------------------------|-----------------|---------------|------------------|---------------|
| SF Name: Guard Monitoring (backdoor) | Required: PLr e | Reached: PL e | PFH[1/h]:5,32E-8 | Status: green |
| SF Name: LightCurtain | Required: PLr e | Reached: PL e | PFH[1/h]:4,13E-8 | Status: green |
| SF Name: 2-HandControl | Required: PLr e | Reached: PL e | PFH[1/h]:8,24E-8 | Status: green |