Janne Niinisalo

Machine Safety Architecture Designer Application

Thesis
Spring 2017
SeAMK 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: Machine Automation

Author: Janne Niinisalo

Title of thesis: Machine Safety Architecture Designer Application

Supervisor: Petteri Mäkelä

Year: 2017 Number of pages: 40

This thesis was based on an idea about a software, which would help Schneider Electric Automation's safety team and their customers. The purpose of the software is to help in designing and understanding the machine safety.

At first, there is an introduction to machine safety in general, including legislation, risk assessment of machines and a preview into common safety components, mainly provided by Schneider Electric Automation. This is followed by the software requirements specification. This chapter contains also an introduction to the software itself. At the end there is a summary and conclusions concerning the whole work process.

Keywords: machine safety, software, application

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikan yksikkö

Tutkinto-ohjelma: Automaatiotekniikka

Suuntautumisvaihtoehto: Koneautomaatio

Tekijä: Janne Niinisalo

Työn nimi: Machine Safety Architecture Designer Application

Ohjaaja: Petteri Mäkelä

Vuosi: 2017 Sivumäärä: 40

Tämä opinnäytetyö perustui ideaan ohjelmasta, joka helpottaisi Schneider Electric Automationin koneturvallisuusosaston työntekijöitä vähentämällä heidän työmääräänsä. Myös heidän asiakkaansa hyötyisivät ohjelmasta, kykenemällä valitsemaan komponentit sekä suunnittelemaan turva-arkkitehtuurin omaan laitteistoonsa.

Opinnäytetyönä tehdyn ohjelman tarkoitus on auttaa suunnittelemaan ja ymmärtämään koneturvallisuutta ja koneturva-arkkitehtuureja. Ensiksi työssä käydään läpi koneturvallisuutta yleisesti. Tämä osuus käsittelee lainsäädäntöä, riskien arviointia sekä yleisiä koneturvakomponentteja.

Koneturvallisuusosiota seuraa sovelluksen vaatimusmäärittely. Kappale sisältää myös sovelluksen kuvauksen ja esittelyn. Viimeisessä luvussa on pohdintaa sekä yhteenveto koko projektista, sisältäen ajatuksia haasteista ja ongelmista projektin aikana.

Asiasanat: koneturvallisuus, ohjelmisto, applikaatio

TABLE OF CONTENTS

Terms and Abbreviations

a, b, c, d, e	Denotation of performance levels.
B10d	Number of cycles until 10% of the components fail dangerously (for pneumatic, hydraulic and electromechanical components).
Cat.	Category.
DC	Diagnostic coverage.
ISO	International Organization for Standardization
MTTF	Mean time to failure.
MTTFd	Mean time to dangerous failure.
PL	Performance level.
PLC	Programmable logic controller.
PLr	Required performance level.
S, S1, S2	Severity of injury.
SCS	Safety Chain Solution
SIL	Safety integrity level.
VDMA	**V**erband **D**eutscher **M**aschinen- und **A**nlagenbau - Mechanical Engineering Industry Association

Tables, Figures and Pictures

1 INTRODUCTION

The work has been done for Schneider Electric Automation GmbH. The topic of this thesis was to create an application based on the safety concept. With the application a user can create a complete safety architecture via any entry point. The created architecture can be linked to a smart selector, which associates the customer's architecture to the most similar Safety Chain Solution and helps the customer to generate the bill of materials as well.

The purpose of this thesis work is to facilitate the communication between a customer and the Safety Automation marketing team of Schneider Electric Automation. With the application the customer can independently create a safety architecture and find out the bill of materials. This reduces the workload of the Safety team. The application also helps the customer to better understand the safety architectures and the meaning and importance of machine safety in general.

1.1 Objective of the work

The main purpose of this thesis is to get a free of charge distributable tool for customers to make a quick first evaluation of how they can build safety architectures using Schneider Electric products. Another aim is to decrease the workload of the safety team. When the customer creates the wanted safety architecture with the application, there is no more need for the safety team to first find out about the customer's necessities. This also cuts off the need from the safety team personnel to solve the certain details of the customers safety architecture. However, the safety team or sales person have to check the compatibilities of the components.

1.2 Structure of the work

Chapter 2 starts with the introduction to machine safety and machine automation. It also contains previews of the basic safety components including input, processing and output devices, provided by Schneider Electric Automation.

In chapter 3, there is brief software requirements specification about the application made during the practical part of this thesis. As well there is described the functionality and usage of the application.

At the end, there is a summary. It contains thoughts about the whole project. This includes thoughts about the difficulties and problems and as well solutions during the project.

1.3 Schneider Electric

Schneider Electric was founded in 1836 in France. It is a global specialist in energy management and automation. Over 160 000 employees in over 100 countries are helping customers to use and manage energy and processes safely, reliably, efficiently and sustainably. From the simplicity of switches to complex operational systems, Schneider Electrics technology, software and services improve the way of the customers manage and automate their operations. In 2015, the full year revenue was 26.6 billion Euros. (Schneider Electric 2016.)

Schneider Electric Automation GmbH is a fully owned daughter company of Schneider Electric. It is the original equipment manufacturer line of business under the Industry business unit of Schneider Electric. The headquarters are located in Marktheidenfeld, Germany. There are over 400 employees representing over 26 nationalities at the office. (Schneider Electric 2016.)

Figure 1 Logo of Schneider Electric. (Schneider Electric 2016. [Referred 15.11.2016]).

2 MACHINE SAFETY

This chapter contains general information about machine safety. It includes an introduction to the main standards about safety of machinery and explanations of the terms used in definitions of the safety of machines. At the end, there is information on the safety components provided by Schneider Electric Automation GmbH.

2.1 General information about machine safety

The purpose of machine safety is to minimize the risks and dangers of the machines and systems to make them safe to use for the operator and other personnel e.g. in maintenance or cleaning. Another aim was to minimise the damage caused to property. In the past, machine safety was not considered so important in industry, but nowadays it is greatly increasing its importance. It is one of the main topics when designing new automation systems. As well, old machines and factories are being updated with safety functions at a growing extent.

Well designed and implemented machine safety will normally drastically reduce the accidents and close calls at factory. This leads to significant decrease in a company’s healthcare expenses. As a side effect, employees may also be happier to work, when they know that their job is safe, which typically leads to increased productivity.

2.1.1 Law and legislation

Requirements for the new machines within European Union are based on directives. The machinery directives set the minimum requirements, but all the countries have freedom to extend the level of requirements. There have also been aims to unify the supervision of the machine safety within the whole region. If, for instance, some machine is discovered to be against the statutes and thus it is forbidden to sell it in some country, the information of the prohibition will be sent to

other countries in the economic region. Consequently the machine will be prohibited within the whole European economic region.

2.1.2 Machine safety standards

IEC 61508 is the only A-type standard for machine safety, which defines the structure of A-, B-, and C-types of standards. This structure has been copied to most machine safety standards.

The standard ISO 13849-1: Safety of machinery, has copied the structure from IEC 61508, so that there are three different groups.

- **Type A standards** are basic safety standards. They give the basic concepts, principles for designing, and general aspects that can be applied to all machinery.
- **Type B standards** are generic safety standards. They deal with one safety aspect or one type of safeguard that can be used across a wide range of machinery:
    - Type B1 standards are for particular safety aspects e.g. noise, surface temperature or safety distances.
    - Type B2 standards are for safeguards e.g. two-hand controls, pressure sensitive devices or guards.
- **Type C standards** deal with detailed safety requirements for a particular machine or group of machines, e.g. gantry cranes or bread cutting machines.

Figure 2 shows graphically the cohesion of the standards mentioned above (Schneider Electric 2009, 7).

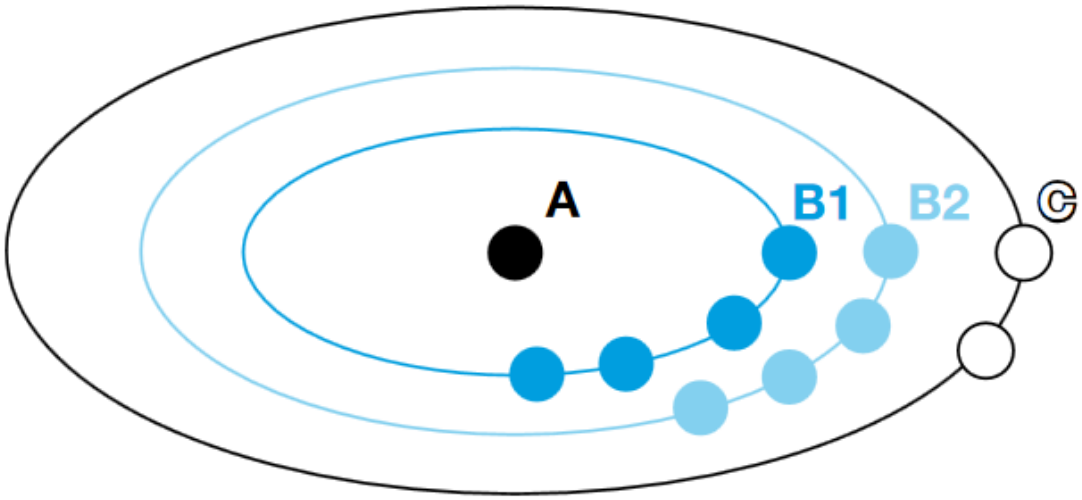

Figure 2. European standards for the Safety of machinery form. (Schneider Electric 2009, 7).

2.2 Machine's risk assessment

Risk assessment is the complete procedure of determining risks in machinery, containing:

- evaluation if the object is a machine
- study if the machine is on the dangerous machines list of the Machinery Directive
- study of the applicable standards
- risk evaluation
- possible risk reduction
- new evaluation on residue risk, if the risk reduction is done
- either a certification or a self-declaration depending on the device category in the Machinery Directive, if remaining risk is below the acceptable level.

Machine's risks and dangers are determined with a risk evaluation. Risks and dangers can be for instance spinning or moving blades or sprockets. There are

several techniques for making risk evaluation. It depends on the machine which kind of technique is used. In the chart below (Figure 3), there can be seen a common way to determine the risks of machine.

In the Figure 3 there is described the common procedure of risk evaluation. Risk evaluation is a repeating process. During this process limits of the machinery are being determined, including usage of the machinery and moderately predictable misuse of the machinery. Then comes detection of possible risks generated by the machinery and associated dangers. After possible risks have been detected there is estimation of level of the risk, taking into account the severity and probability of possible injury determining the magnitude of the risk, to define if the risk has to be reduced. And last removal of dangers or reducing the risk associated to dangers as effectively as possible.

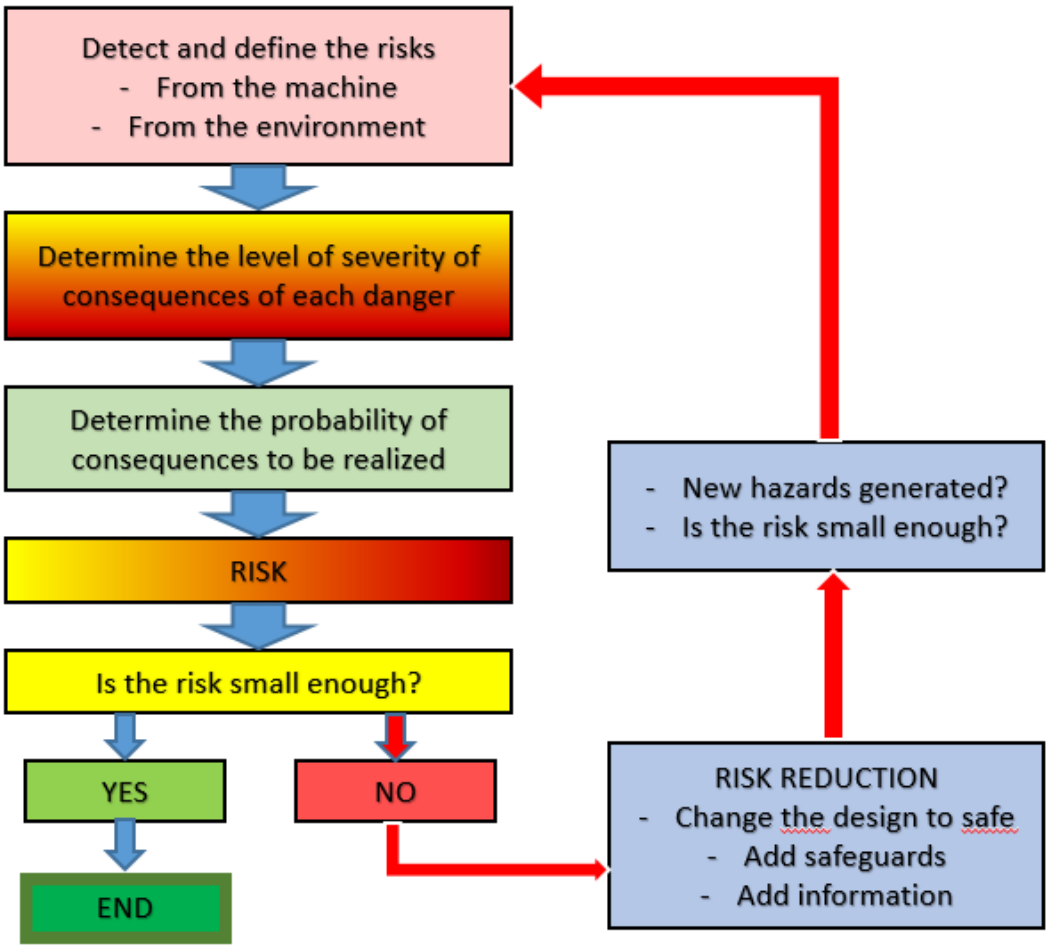

Figure 3. Common risk evaluation process. Own picture.

2.3 Machine safety terms

The safety of the machine is defined by various different terms. These terms define the safety level of the machine from different aspects and with different requirements. Although, they measure different values, some of them are essentially linked together.

2.3.1 Stop categories

Stop categories are a part of safety motion functions defined in a specific standard for the purpose and there are around 25 of them. The safety categories define the way the machine and its actuators have to be stopped in case one or more safety devices sends the stopping signal.

The stop functions of the stop category 0, stop category 1, and/or stop category 2 shall be provided by the risk assessment and the functional requirements of the machine. These functions provide different ways to stop the machine.

Stop category 0 (STO): Figure 4 (Schneider Electric 2015.) shows that the power is cut off from the machine, when the stop signal is given. Stopping is done by an immediate removal of the power from the machine actuators. This is a so called uncontrolled stop; stopping of the machine motion by removing the electrical power.

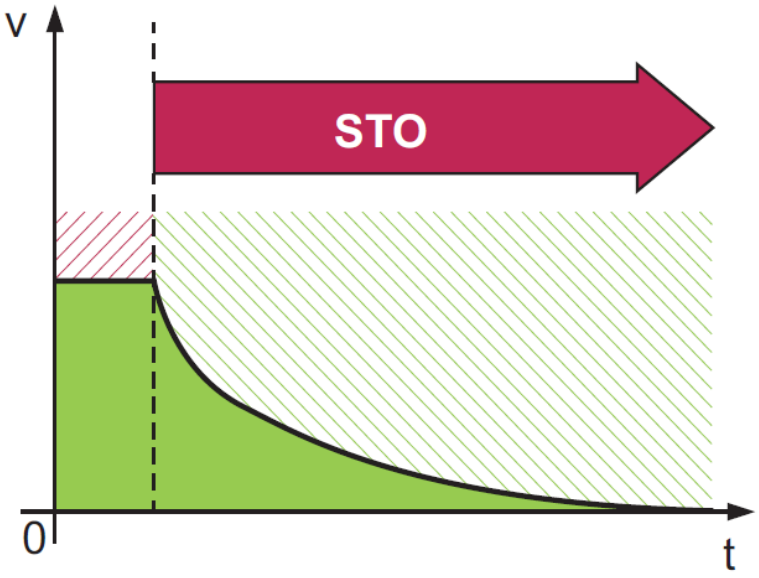

Figure 4. STO: SafeTorque Off. (Schneider Electric 2015.)

Stop category 1 (SS1): Figure 5 (Schneider Electric 2015.) shows, that machine and/or its actuators are being stopped with electrical power. Electrical power is removed after the machine has stopped. This is a controlled stop with power

available to the machine actuators to achieve the stop and when the stop is completed, the power is removed.

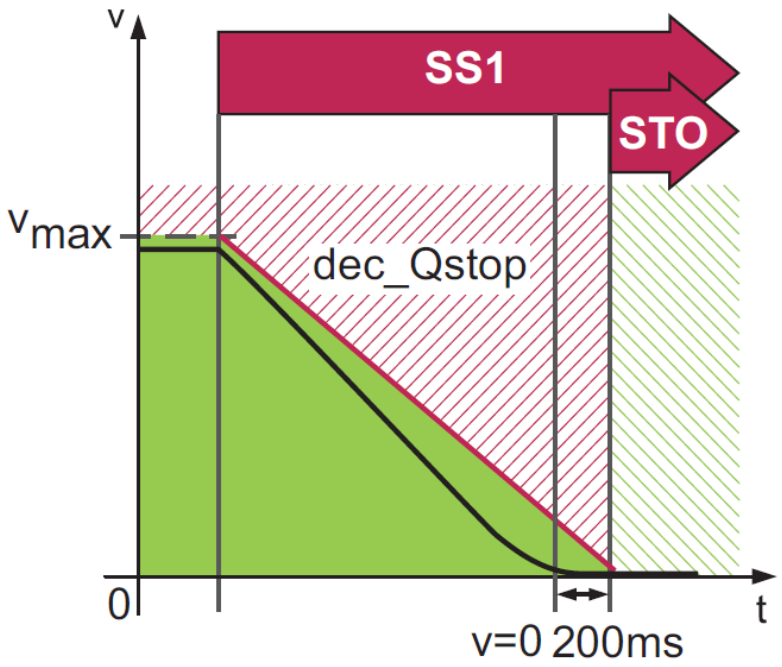

Figure 5. Stop category 1 visualization. (Schneider Electric 2015.)

Stop category 2 (SS2): Figure 6 (Schneider Electric 2015.) shows a controlled stop with power left to the machine actuators. The actuators are kept in constant position with electrical power after the actuators have stopped.

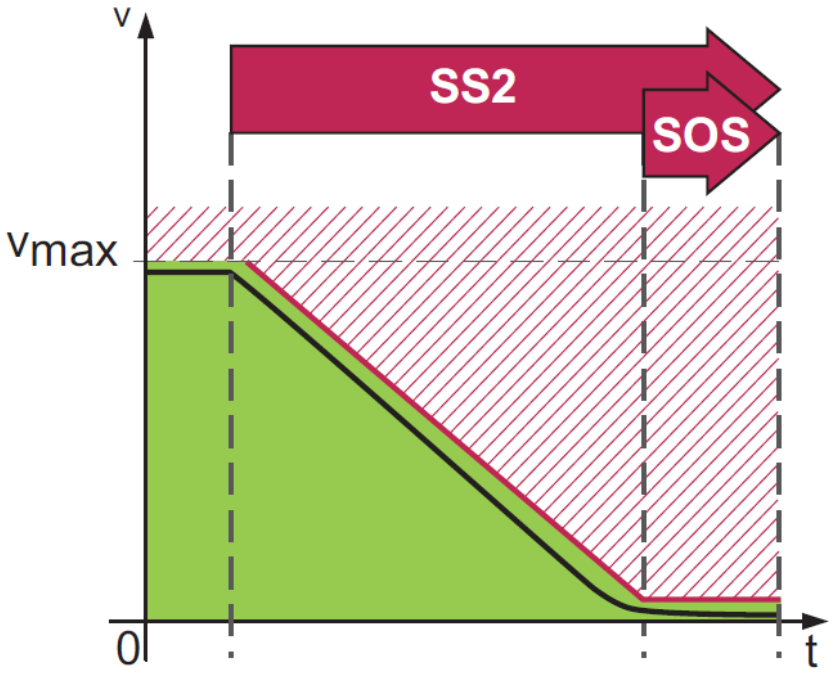

Figure 6. Stop category 2 visualization. (Schneider Electric 2015.)

2.3.2 Speed monitoring

Safety-limited speed function prevents a motor from exceeding the specified speed limit. When the function is initiated a machine starts to decelerate to the defined safe speed, within the defined time. When the machine gets to the safe speed, the function will monitor the speed, so it stays below the safe limit.

Safe maximum speed function provides a safe output signal to indicate if the motor speed is below a defined limit or not. This function is an optional function to limit the maximum speed and monitor it.

Safe direction function prevents the motor from moving to wrong direction.

Vertical position monitoring is used with elevators. When the cabin is at a landing point, doors opened, some lifts automatically correct their level in relation to the landing point in order to compensate any differences generated by medication of the load in the cabin. The positioning of the cabin is in relation with the landing, and it is detected by two limit switches. It is also possible to use magnetic sensors with reed contact.

Safe operating stop (SOS) function prevents the motor from deviating more than pre-defined amount from the stopping position. The drive gives energy to the motor for it to be able to resist external forces. This function is often used in together with the Safe Stop 2 function, where the machine movement decreases down to zero speed then the Safe Operating Stop is enabled.

2.4 Safety components

Machine safety is built with safety components. Those components can be roughly divided to three categories: input devices, processing devices and output devices. Typically there are also devices which can perform (at least partially) parallel in two of the categories e.g. input and processing devices or processing and output devices. Devices in each category has their own purpose and functionality in machine safety. Usually safety components can be noticed by the red colour in it, excluding output devices. The main colour of the whole component is red, or alternatively some parts of it are red. In some cases, output devices might be also partly red.

2.4.1 Acquire information

Input devices work as the sense of touch, vision and hearing of the system. With these devices, system knows what is happening within it. Things like errors, defects and faults in the devices of the system are being monitored. But most importantly, the safety of the operator and other personnel e.g. maintenance or cleaning, is being monitored.

Emergency stop is very common safety input device. E-Stop pushbutton is shown in Figure 7 (Schneider Electric 2016). The function E-stop can be initiated also by a trip wire switch. In case, when user is in danger to get hurt, user or another person can press emergency stop button. This action will cut the power from the machine and perform a safe stop.

For the Emergency stop function, either Stop Category 0 or Stop Category 1 is chosen, according to the risk assessment results of the machine.

Figure 7. Emergency stop pushbutton by Schneider Electric. (Schneider Electric 2016.)

Guard monitoring with electromechanical switch, shown in Figure 8 (Schneider Electric 2016). On many potentially dangerous machines, the operator must be kept at a distance from hazardous area during operation, but needs to take action when the machine is stopped to for example position a part, remove a product or adjust a tool. An effective protection is to install a guard which, based on the type of installation, will cut off the power from the actuator i.e. motor, if the user tries to open it during the machine operation. In all cases, it must be taken care, that re-start action cannot be run until the guard is closed. Depending on the required level of protection, the system will contain two conventional limit switches, or a combination of protected, actuator operated guard switches to prevent tampering.

Figure 8. Metal safety switch without guard locking. (Schneider Electric 2016.)

Guard monitoring with guard locking device is shown in the Figure 9 (Schneider Electric 2016). This type of guard is necessary for potentially dangerous machines, with high inertia. This means long run-down time. The guard is locked with spring actuated bolt. The guard can be opened, if the machine is completely standing still, by solenoid working against the spring and actuating to open position.

Figure 9. Metal safety switch with guard locking. (Schneider Electric 2016)

Coded magnetic switch in Figure 10 (Schneider Electric 2016.) **and system** in Figure 11 (Schneider Electric 2016.) are non-contact solutions and are often used in industrial machines, fitted with a door or guards. Typically coded magnetic switches are low or medium coded, so they are relatively easy to misuse by the personnel. It is particularly suitable for machines, which are under frequent washing or splashing of liquids. It is also often used on small machines with a single guard for self-contained systems. Depending on the model of the guard, sensing distance can be between 5 and 10 mm. The reed contacts used for the coded magnetic switches cannot withstand short circuits and the switches always incorporate a resistor in series. Therefore, their operation can only be guaranteed with a proper processing module.

Figure 10. Coded magnetic switch. (Schneider Electric 2016.)

Figure 11. Coded magnetic system. (Schneider Electric 2016.)

RFID safety sensors are high coded contactless system that consists of a microprocessor-controlled switch and a transducer. As being high-coded, it is practically impossible for personnel to misuse the sensors in purpose. The basic applications are for monitoring the position of movable safety guards such as robotic work cells, assembly lines, mobile equipment and packaging machines.

Perimeter guarding with light curtains is shown in Figure 12 (Schneider Electric 2016)**.** Safety light curtains are electro-sensitive systems designed to protect users working in the immediate presence of the machine. The dangerous movements of the machine are stopped when the light beam is broken. The machine must be designed so that it is not possible to have access to hazardous area without breaking the light beam of the light curtain. In addition, the movement have to be stopped, independent of the entry speed of the operator, when entering to the hazardous area. The safety distance **S**, defined by the standard, takes into account the speed at which a user can cross the safety zone to reach the hazardous area.

Figure 12. Safety light curtain. (Schneider Electric 2016.)

Perimeter guarding with safety mat is shown in Figure 13 (Bircher. 2016)**.** Safety mats are used to detect the user walking or standing on the mat, or to detect objects falling onto the mat. Any detection on the mat will initiate stopping of the

machine. Restart action can be done manually or automatically, depending on the configuration of the machine. In general, some mats are used to cover the safety zone.

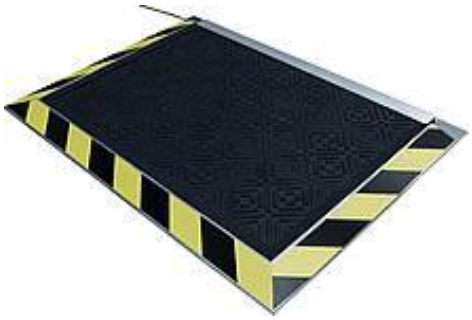

Figure 13. Safety mat. (Bircher. 2016.)

Enabling movement with two-hand control station is shown in Figure 14 (Schneider Electric 2016)**.** Two-hand control stations require simultaneous operation with both hands in order to start and maintain operation of the machine. Therefore, it provides protection especially for the operator.

Figure 14. Two-hand control station. (Schneider Electric 2016.)

Enabling movement with enabling switch is shown in Figure 15 (Schneider Electric 2016)**.** Enabling switch allows the operator to carry out a maintenance,

adjustment or programming operations in the hazardous area of the machines, when certain required conditions are met. Usually this requires also running the machine at reduced speed, which is often set by the user using selector switch with key locking or equivalent.

The operating principle of the enabling switch is: Position 0: contact open (control operator at rest), Position 1: contact closed (control operator presses the switch to normal enabling position) and Position 2: contact open (control operator presses the switch all the way to the bottom). When the switch is pressed to position 1, it must return to position 0, if released. The switch must change from position 1 to position 2, if user presses the switch harder. When the switch is released from position 2 to position 0, the switch contact must pass position 1 without closing.

Figure 15. Enabling switch. (Schneider Electric 2016.)

Speed monitoring devices, such as encoders and residual voltage for zero speed are used to detect the stop condition of the electric motors. The most common applications include: providing the unlock signal for interlocked guard monitoring devices, controlling rotation direction signals for reversing motors and engaging locking brakes after motor has come to a standstill.

2.4.2 Monitor and processing

The signals from the safety input components are commonly monitored and processed by using safety modules, safety controllers or safety PLCs. These devices will make decisions based on the input signals, and then drive output devices, such as contactors. Safety monitoring devices are divided to those three groups (modules, controllers, PLCs), according to the intelligence and the amount of programmable features in the device.

The choosing of the processing device depends on many factors, such as number of necessary safety inputs/outputs, cost, complexity of required safety functions themselves, need and number of necessary cabling and the physical size of the safety architecture in the system.

Safety modules are the simplest and cheapest safety processing devices. An example picture of safety module is shown in Figure 16 (Schneider Electric 2016). Safety modules are non-programmable devices, with few input and output ports. Some modules might have parameters which user can set as they like.

Figure 16. Example of Schneider Electric safety module. (Schneider Electric 2016.)

Safety controllers have usually more input and output ports than modules. Example picture of Schneider Electric modular safety controller is shown in Figure 17 (Schneider Electric 2016). They are also more expensive. Controllers have quite

much intelligence in them, and they can be parameterized, instead of being programmed. That means, they have hardcoded base-configuration blocks, which user can combine to function together partly freely, partly in defined organisation. Nevertheless, the variety of parameters and their combinations that user can configure, is quite wide. Parametrization is relatively easy and fast, at least compared to programmable PLCs.

Figure 17. Example of Schneider Electric modular safety controller. (Schneider Electric 2016.)

Safety PLCs, programmable logic controllers, are the most expensive processing devices. They are powerful and fully programmable devices with huge variety of functions. Amount of input and output ports can be increased to control hundreds of devices. The programming is relatively difficult and requires a lot of knowledge. Example device is shown in Figure 18 (Schneider Electric 2016).

Figure 18. Example of Schneider Electric safety PLC. (Schneider Electric 2016.)

2.4.3 Stop the machine

Output devices will execute the actions decided by processing devices. Processing devices sends the signal to output device to slow down or directly shut down the machine.

Most common output devices, which are connected to safety processing devices, are **contactors**. With contactors, it is possible to control many kinds of different devices and functionalities. For instance, in conveyors, contactors are used to control the current for a motor, that runs the conveyor. Figure 19 (Schneider Electric 2016.) shows contactor with red safety cover provided by Schneider Electric.

Figure 19. Schneider Electric contactor with red safety cover. (Schneider Electric 2016.)

Variable speed drives and **motion control devices** are also common devices connected to safety processing devices. They are used to control electrical motors with advanced way e.g. digitally over fieldbus. This means for instance that the speed and direction of rotation of the motor can be set by the user to fit in each situation. Safety processing device will give a permission or prevent the drive or motion control device to drive the motor. Figure 20 (Schneider Electric 2016.) shows example of variable speed drive provided by Schneider Electric. Figure 21 (Schneider Electric 2016.) shows example of motion servo drive provided by Schneider Electric.

Figure 20. ATV340 variable speed drive by Schneider Electric. (Schneider Electric 2016.)

Figure 21. LXM62 by Schneider Electric. (Schneider Electric 2016.)

Rotary switch disconnectors: for equipment isolation from the electrical supply and for emergency stop by direct interruption of the power supply. Therefore e.g. maintenance or cleaning is safe to perform.

In addition, besides actual output actuators, there might be additional equipment connected to processing devices. Good example of that kind of units are **warning lights** and **alarms**. Example of modular tower light by Schneider Electric can be

seen in Figure 22 (Schneider Electric 2016.). These kind of units are not actual safety devices. They are meant to increase the safety without actually increasing the safety level of the machine itself. With these lights and alarms, user can visually see and/or hear, when the machine is in safe state, or alternatively in dangerous state depending on the configuration of the lights and alarms.

Figure 22. Modular tower light by Schneider Electric. (Schneider Electric 2016.)

2.5 VDMA

VDMA (Verband Deutscher Maschinen- und Anlagenbau, Mechanical Engineering Industry Association) is an association that represents over 3200 mainly medium-sized equipment manufacturers in the capital goods industry. It is the largest industry association in Europe.

VDMA's membership covers the whole process chain, including for instance production, manufacturing, drive-train and automation engineering, software and product related services. (VDMA. 2017).

VDMA 66413 is a Universal data format for safety-related values of components or parts of control systems. It is a common base for the exchange of information.

The standards about machine safety are harmonized under the Machinery Directive 2006/42/EC. They require assessments and calculations regarding the probability of dangerous failure and systematic aspects of a machine’s safety functions.

Device manufacturers have to create characteristic value libraries for their safety devices in a “universal data format” (VDMA qualified XML document). Calculation tool (supplier) provides a way for importing libraries in a database format. The characteristic values are prepared for display and selection within the tool. Machine manufacturers use the characteristic value libraries provided by the device manufacturer to update the values within the calculation tool. Requirements of the universal data format:

Machine manufacturers need to take care, that

- the characteristic values from all device manufacturers have to be available for every calculation tool
- characteristic values have to be transparent for users in terms of content
- understandable, additional information for the users is available
- ability to read and edit the library using standard PC software
- ability to reuse sets of characteristic values without additional software

Device manufacturers

- provide the characteristic values once in a single electronic format, which can be in all calculation tools.
- minimize the work in providing the values.
- tool suppliers are responsible for the method used to import the calculation tool. The device manufacturer do not need to check the import results for being correctly processed.
- characteristic values have to be provided to all machine manufacturers in one standard format, as a characteristic value library.

In addition, the database format has to meet the requirements of the calculation tool. Examples of calculation tools: SISTEMA, Safety Evaluation Tool and PAScal. (VDMA. 2012)

3 SOFTWARE REQUIREMENTS AND IMPLEMENTATION

In this chapter there is given a brief software requirements specification about the application which was created during of this thesis project. This chapter contains also an introduction to the application. The purpose of the software is to help the customer of Schneider Electric Automation, to visually design and understand the machine safety architecture of their machinery.

3.1 Functionality

The main functionality of the application is that the user can create a complete safety architecture via any entry point (input, processing or output). Designing happens by dragging icons from the drop-down menus on the left side of the application window, and dropping them to the white based, dot gridded designing area in the middle of the window. Information on getting the component icons is given later in chapter 3.2.1 Before designing. The icons have been divided in to three groups. Red based icons are input devices, blue based icons are processing devices and green based icons are output devices.

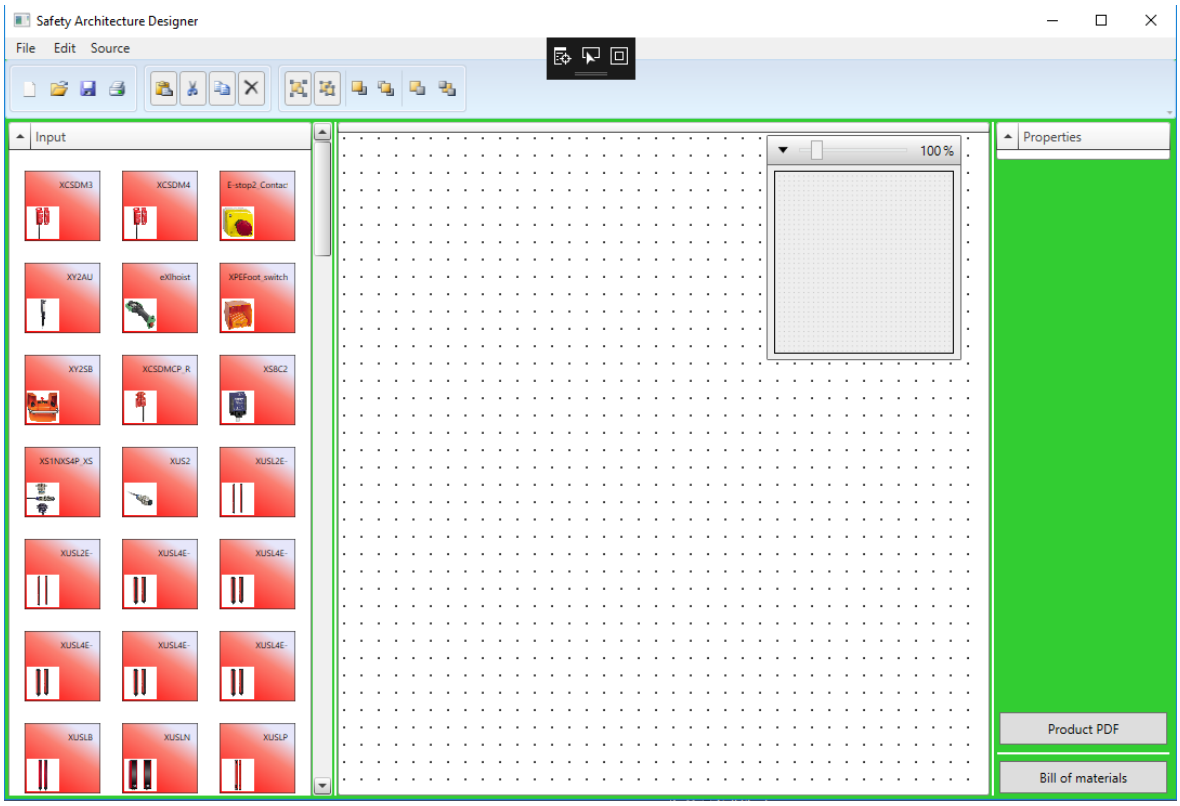

Figure 23. Main window, Schneider Electric Automation's VDMA library loaded. Screenshot.

The icons dragged into the designing area, can be linked to each other with lines. These lines show which devices are connected together. For instance, emergency stop can be linked to some kind of a processing device, for example, an e-stop module.

Designing area can be widened, therefore it will not limit the size of the architecture. It will automatically get wider, when the user drags an icon outside the designing area. The designing area can be zoomed as well. The zoom limits are from 25% up to 400%. There is also a zoombox fitted in a drop-down menu in the upper right corner of the designing area. There the whole architecture can be seen in a smaller box.

When the wanted safety architecture has been designed, it can be linked to a selector. This selector associates the user's safety architecture to the most similar Safety Chain Solution. In addition, it helps the user to generate a bill of materials needed for the certain safety architecture.

The user can open the product PDFs of the component which the user is interested in. In the PDF files, there is detailed information on the component.

3.1.1 Before designing

Before the user can begin creating the architecture they want, there must be a VDMA qualified XML document loaded in to the application. More information on this document is given later in chapter 3.5 Information content. When the document has been successfully loaded to the application, all safety related components from the manufacturer whose VDMA library has been loaded, are available for the user to design the architecture. Components can be seen as icons on the left side of the window, inside three different drop-down menus. There can be multiple libraries loaded into the application, in case the user wants to use components from different manufacturers.

3.1.2 During the designing

When all the wanted VDMA libraries have been loaded in to the application, the user can begin the designing of the architecture. All the available safety components are divided into three groups listed on the left side of the window: inputs, processing and outputs. From those lists, the user can drag and drop the wanted components to the designing area in the middle of the window.

The user has a possibility to open an instruction sheet in a PDF format for any component to get more information about the component.

3.1.3 After the designing

When the user has completely designed the desired architecture, it can be linked to a selector. This selector finds the most similar Safety Chain Solution and presents it to the user. In addition, the user can print out a bill of materials needed for their architecture.

When the wanted architecture has been designed and the bill of materials is saved and/or printed, the user can send the information about the architecture straight to the salespersons of the manufacturer. In that situation, the salespersons only needs to check through the list of materials, and make sure that all the components are compatible with each other. When everything has been checked, the offer concerning the architecture can be made.

3.2 Users

This application is mainly meant for the customers of Schneider Electric Automation. Another group of users is the sales personnel of Schneider Electric Automation. They can use the application, for instance, when introducing different safety architectures and combinations to customers or colleagues. As well, they can review the architectures made by the customers.

3.3 Assumptions & dependencies

Because the application is made for the Microsoft Windows operating system, the user needs to have a Windows operating system on their PC. The user is expected to have at least basic knowledge about machine safety. In addition, the user needs to have a VDMA library, provided by Schneider Electric Automation or some other safety component manufacturer.

At least one VDMA library must be loaded in to the application successfully, before any safety architecture designing can be started.

3.4 Information content

The main sources of information in the application are the VDMA libraries provided by the safety component manufacturers. These documents can be obtained from the manufacturers in some common archive format, such as RAR or ZIP. The ar-

chived file contains the VDMA library in an XML format and folders for the product PDF documents and images of the products in a PNG format.

VDMA qualified XML document contains all necessary information about the components, such as Performance Level and Safety Integrity Level. In the library, components are also defined by their type, like input, processing or output. In some cases, a certain component can be either a processing device or an output device, depending on the configuration.

The users should always use the latest component lists (VDMA libraries) provided by the manufacturers. By doing so, they always have the updated offers from the manufacturers.

3.5 Further development

By the time, Schneider Electric Automation will add more SCS’s in their offer. These complete Safety Chain Solutions should be added to the application, to make sure that the user has the possibility to choose the most similar SCS compared to their own safety architecture.

4 SUMMARY

This thesis introduces the common devices and methods of machine safety used in industrial applications. The information was gathered from the experience gained during the internship and thesis work periods at Schneider Electric Automation, and from the documentation of Schneider Electric Automation's safety team.

Programming language C# was decided to be used as the implementation language over the others like Python or C/C++, because it provides easy-to-use implementation and developing methods. The created application is not a large software and, therefore, it does not require the powerfulness and performance advantages, which C/C++ would have given. In addition, the development of graphical user interfaces and other graphical things are relatively faster in C# than in C/C++. The requirement of the Windows operating system is also a great reason for choosing C#.

The biggest issues with the implementation were the graphical problems with the UI. Some functions were surprisingly complicated to implement, and support from Schneider Electrics Microsoft team was needed to be able to solve the problems.

The aim was this project would help the customers when creating or upgrading safety into their machinery and also the Schneider Electric sales personnel when giving their proposals to customers. Additionally, this project may give ideas, on how different technologies can be used to help and ease daily work.

BIBLIOGRAPHY

Bircher. 2016. [www-page]. Bircher Reglomat. Available: http://reglomat.bircher.com/us/products/safety-mats/

Schneider Electric. 2009. Safe Machinery Handbook. [Online publication]. Rueil-Malmaison Cedex. [Referred 15.11.2016]. Available: http://www.schneider-electric.fi/documents/original-equipment-manufacturers/pdf/Machine-safety-guide.pdf

Schneider Electric. 2015. Machine Struxure – Preventa solutions for efficient machine safety. [PDF-publication]. Schneider Electric Industries SAS, France. [Ref. 10.1.2017]. Available: For internal use only.

Schneider Electric. 2016. [www-page]. Schneider Electric SE. Available: http://www.schneider-electric.com/ww/en/

VDMA. 2012. [PDF-document]. VDMA Specification. Available: https://ea.vdma.org/documents/266693/2951892/VDMA66413%20Abstract_en_Chap4.pdf/03245a3c-493e-4ed2-8a7e-ea93db6b38bf

VDMA. 2017. [www-page]. VDMA – Who We Are. [Ref. 15.02.2017]. Available: http://www.vdma.org/viewer/-/article/render/14957036