Kalle Jaatinen

Machine safety design and risk assessment with PacDrive3 system

Thesis
Spring 2018
Seinäjoki UAS, 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: Electric Automation

Author: Kalle Jaatinen

Title of thesis: Machine safety design and risk assessment by using PacDrive3 system.

Supervisor: Ismo Tupamäki

Year: 2018 Number of pages: 47 Number of appendices: 3

In this thesis PacDrive3 automation solution by Schneider Electric Automation GmbH is examined for usage on machine safety design for selected machines: robotic palletizer and labelling machine.

The theory is introducing PacDrive3 system and its features. In this part the basics of machine safety, machine standards and used devices are explained.

Designed safety architectures and functional behaviour were the main parts of the practical part of the thesis.

Keywords: machine safety, PacDrive3, safety equipment, Sistema

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikan yksikkö

Tutkinto-ohjelma: Automaatiotekniikka

Suuntautumisvaihtoehto: Sähköautomaatio

Tekijä: Kalle Jaatinen

Työn nimi: Koneturvasuunnittelu ja riskien arviointi PacDrive3-järjestelmää käyttäen

Ohjaaja: Ismo Tupamäki

Vuosi: 2018 Sivumäärä: 47 Liitteiden lukumäärä: 3

Tässä opinnäytetyössä on tarkasteltu Schneider Electric Automation GmbH-yrityksen PacDrive3-järjestelmää ja sen soveltamista valittujen laitteiden turvasuunnittelussa.

Teoriaosuudessa on esitelty PacDrive3-järjestelmä ja sen omaisuudet. Osuudessa pureudutaan myös koneturvallisuuden peruskäsitteisiin, standardeihin sekä laitteistoon.

Työn käytännönosuus pitää sisällään turva-arkkitehtuurien suunnittelun ja toiminnallisen testauksen käyttäen PacDrive3-järjestelmää sekä yhtiön koneturvatuotteita.

Asiasanat: koneturva, PacDrive3, turvalaitteet, Sistema

TABLE OF CONTENTS

Terms and Abbreviations

CCF	Common-Cause Failure
DC	Diagnostic Coverage
IEC	International Electrotechnical Commission
IFA	Institut für Arbeitsschutz
ISO	International Organization for Standardization
LMC	Logic Motion Controller
MTTFd	Mean Time to Dangerous Failure
PL	Performance Level
SIL	Safety Integrity Level
Sistema	Safety Integrity Software Tool for the Evaluation of Machine Applications
SLC	Safety Logic Controller
SLS	Safe Limited Speed
SMS	Safe Maximum Speed
SOS	Safe Operating Stop
SRCF	Safety Related Control Function
SS1	Safe Stop 1
SS2	Safe Stop 2
STO	Safe Torque Off
VDW	Verein Deutscher Werkzeugmaschinenfabriken e.V.

ZVEI	Zentral-verband Elektrotechnik- und Elektroindustrie e. V.

Tables, Figures and Pictures

1 Introduction

Schneider Electric Automation GmbH is a part of the Schneider Electric Group which is the global specialist in the fields of energy management and automation. The revenue of the company is around 25 billion euros and it's over 150 000 employees are working in over 100 countries. Schneider Electric is offering to its customer's products from a simple switch to whole operational systems, software and services which help customers to manage and automate their operations. (Schneider Electric [Referred 21.2.2018].)

Figure 1. Factory site in Marktheidenfeld

The site of this thesis work is located in Marktheidenfeld, Bavaria, Germany and is headquarter of the Schneider Electric Automation GmbH's Machine Solutions and System Consistency divisions. The headquarters develops and also produces hardware and software products for automation solutions and plant construction. On the Marktheidenfeld site there are working about 400 employees from over 26 countries. (Schneider Electric [Referred 21.2.2018].)

1.1 Background and structure of thesis

This thesis is made to help sales persons in their work with PacDrive3 embedded safety. The thesis considers necessary aspects of safety design for selected example machines. With correct safety calculations, architecture, safety functions and implemented safety devices it is easier for the sales personnel to explain the need of machines safety requirements and show the capabilities of Schneider Electric products.

The first part is introducing the company, machine safety and the background of this thesis. The second part goes deeper in to the machine safety, explaining the theory and standards behind safety calculation and common safety functions. In the third part PacDrive3 automation solution is introduced from the safety point of view. This part contains also some references to the topics of the second part. The used example machines are introduced in the fourth part. This part contains safety calculations, operational descriptions of the machines and the used safety architectures.

2 Machine Safety

This chapter introduces the basic terms of machine safety. To plan safety, subjects like SIL, PL, stop categories, speed monitoring and the basics of international standards and Sistema calculations need to be understood.

2.1 Why Safety?

The purpose of machine safety is to keep machines safe for the user and prevent unnecessary machine stop downs/ breakdowns. In addition to the moral obligation to avoid harming anyone, there are laws that require machines to be safe, and sound economic reasons for avoiding accidents. Safety must be considered through the whole life cycle of a machine: all the way from design, manufacturing, installation, adjustment, operation, maintenance to scrapping in the end. Even though a machine’s life consists of many phases, still 60 % of machine accidents occur during installation, adjustment and maintenance. The reason for this seems to be that these phases are not considered deeply enough in design and risk analysis. (Schneider Electric 2009.)

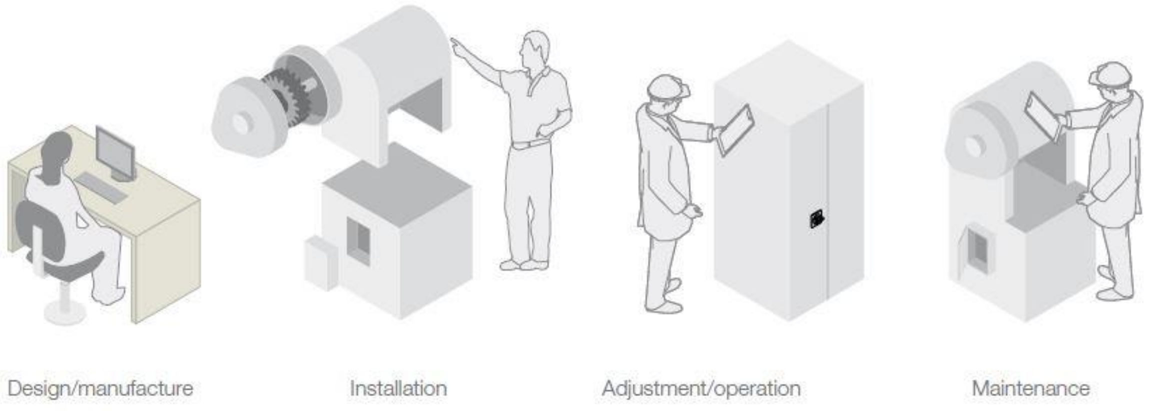


Figure 2. Life cycle of a machine (Schneider Electric 2009)

The requirements for the safety and protection of machinery have changed more and more with the increasing use of automation. In the past safety devices were seen as a nuisance and were often not used. Nowadays well developed protective devices are integrated into to the work process. Safety is not slowing down production anymore, but in many cases it is rather improving productivity. (SICK 2015.)

2.2 Standards

European Union's machine directive is a European law which defines machines considered dangerous and guarantees a minimum level of safety for machines and equipment's sold. The European Union standards include requirements, principles and means to achieve the Machinery Directive demands. Non- European

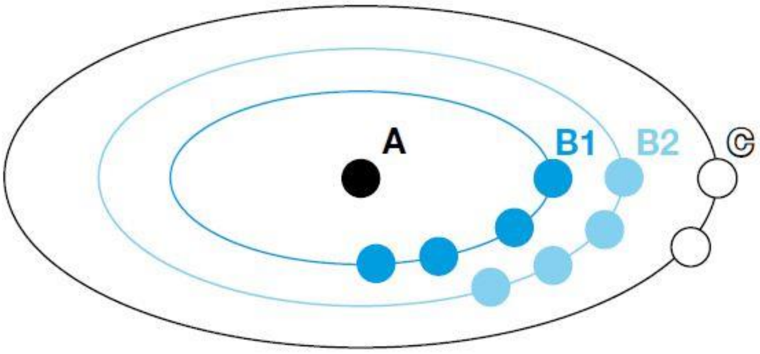


Figure 3. Standard types (Schneider Electric 2009)

countries have their own directives and standards, most of those are based on European standards. (Schneider Electric 2009.)

Standards are divided into three types. Type A standard is a basic safety standard EN ISO 12100 which gives the basic concepts, principles for design and general aspects needed to achieve the goals of the machine directive. The Second type, Type B standards are also called generic safety standards and are divided into Type B1 for particular safety aspect (e.g. safety distances) and to Type B2 for safeguards (e.g. two-hand controls). The last main type of standards is Type C which provides detailed safety requirements for a particular machine or a group of machines. An example of a Type C standard can be EN ISO 10218-1 Robots for industrial environments - Safety requirements - Part 1: Robot. If a machine is having a specific Type C standard it will be the guiding standard. (Schneider Electric 2009.)

2.3 Current main standards

Currently there are two main standards for machine safety which act as a guideline for how to design safety devices. IEC 62061:2005 – Functional safety of safety-related electrical, electronic and programmable electronic control system, is factoring safety integrity requirements of each SRCF by terms of SIL. (Robotic Industries Association [Referred 22.02.2018].)

The second, ISO 13849-1:2015 - Safety related part of the control system -- Part 1: General principles for design and ISO 13849-2:2012 - Safety related part of the control system -- Part 2: Validation. These standards are using similar methods to address machine safety. This standard is approaching safety by using performance levels on a five level scale. These levels are a combination of old safety categories by standard EN 954-1, MTTFd, DC and CCF. When designing machine safety the designer can use one of these two standards. (Robotic Industries Association [Referred 22.02.2018].)

2.4 Safety Categories & Performance Levels and Safety Integrity Level

Like said earlier, categories are defined as a five level scale, which goes in the following way from lowest to highest: B, 1, 2, 3, 4. Category B is a simple circuit with a possible loss of the safety function if an event of a fault is effecting the circuit. Category 1 requires that a control system is built by using well tried and tested components and a proven safety principle. It has greater reliability but still a loss of safety function is possible when a fault occurs. In category 2 requirements are tighter as the safety functions must be tested at suitable intervals. Fault detection in each test prevents undetected faults of the control system but it does not ensure the safety function. Category 3 requires that a single fault does not cause a loss of a safety function and that the fault shall be detected when it occurs. This means that the architecture is redundant, in the other words dual channel. In case of a fault a safety function is ensured, except in a case where the system is facing an accumulation of faults. The highest category 4 requires the same features as all other categories together and on top of those an accumulation of faults must not cause a loss of safety function. In case of faults category 4 control system always ensures safety functions. (Schneider Electric 2014.)

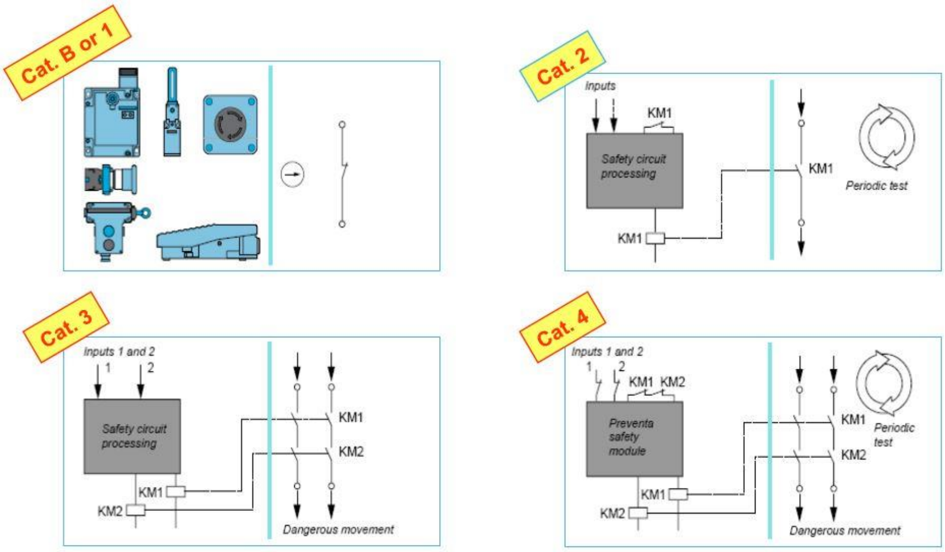
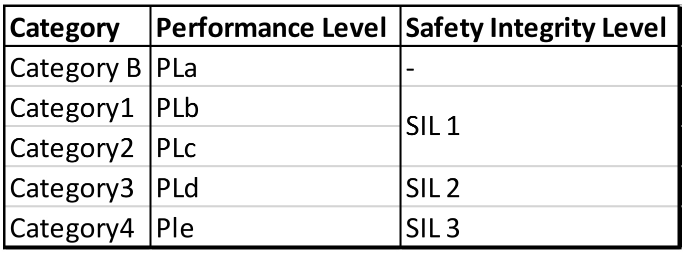


Figure 4. Categories in a graphical form (Schneider Electric 2016b)

Like said in chapter 2.3 the performance level (PL) is basically improved safety categories with added features. Because categories are based on basic electromechanical devices only, they need to face more features to answer the needs of modern control systems with all kind of technologies like pneumatics, fluids and hydraulics, not only electrics anymore. Even though both, PL and categories are using a 5 level scale they cannot be directly converted to each other because PL needs more calculation and information than the old categories. (Schneider Electric 2016b.)

Table 1. Relation between the categories PL and SIL (Schneider Electric 2016b)



Category	Performance Level	Safety Integrity Level
Category B	PLa	-
Category1	PLb	SIL 1
Category2	PLc	
Category3	PLd	SIL 2
Category4	Ple	SIL 3

Safety integrity level (SIL) requires that the probability of dangerous failures per hour values are within certain limits to achieve the SIL levels. Safety integrity by IEC 62061 also requires that each SRCF must be specified in terms of SIL. (Robot industries association 2015). Performance level and safety integrity level are compared and converted between each other by using the following table. (Schneider Electric 2016b).

Table 2. Relation between PL, SIL and PFHd (Schneider Electric 2016b)

PL	SIL	PFH_D - Probability of Dangerous Failures per Hour (1/h)
a	No correspondence	$\geq 10^{-5} < 10^{-4}$
b	1	$\geq 3x10^{-6} < 10^{-5}$
c	1	$\geq 10^{-6} < 3x10^{-6}$
d	2	$\geq 10^{-7} < 10^{-6}$
e	3	$\geq 10^{-8} < 10^{-7}$

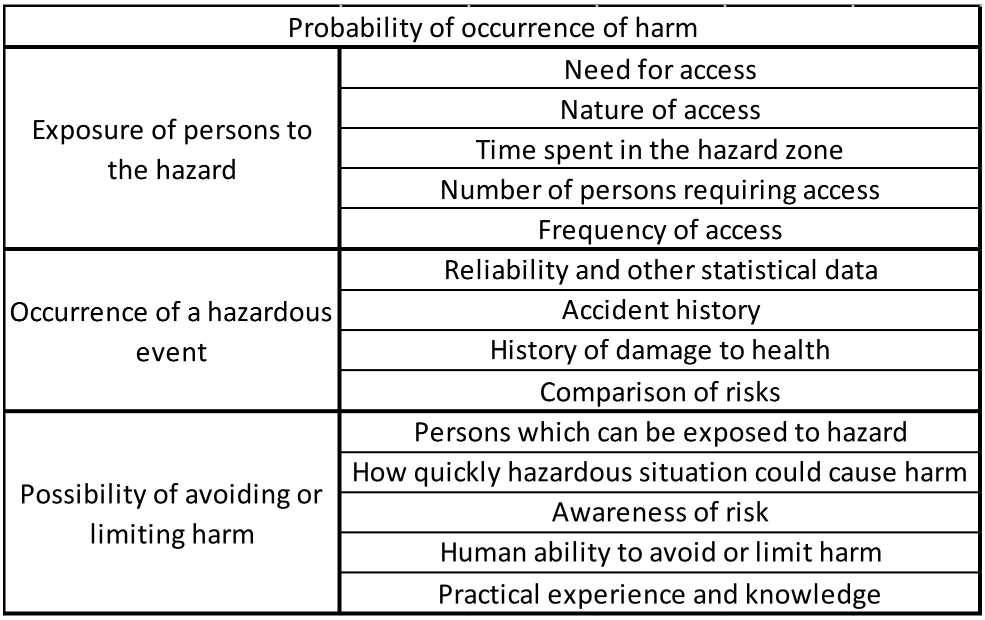
2.5 Sistema

Sistema is free safety level calculation software provided by IFA. The idea of SISTEMA is to offer a safety evaluation platform for safety-related machine controls. The system is using the context of ISO 13849-1 standard which determines the requirements and guidance needed to design and integrate safety-related parts of control systems. With Sistema tool a user is able to model the safety-related components of the architecture and get calculated safety categories and values. Sistema is using relevant parameters such as PL, CCF, MTTFd and DCavg which are entered to the calculation software. Each parameter change is immediately calculated and its impact to the whole system can be seen right away. (Sistema [Referred 09.03.2018].)

2.6 Risk assessment

The definition of risk assessment is determined in type-A standard ISO 12100, where a risk is explained by using the following elements. The first element is the severity of harm when hazard is happening. This element can be divided into two areas: severity of injury and extent of harm. Severity can be expressed with a scale from a slight injury to death. The extent of harm is giving information on how many people can be affected to the injuries, for example from one person to several persons. The second element is the probability of occurrence which can be divided into three areas: Exposure of a person to the hazard, the occurrence of a hazardous event and the possibility to avoid or limit the harm. All these features can be divided in different parameters which are demonstrated in following table. The risk itself can be seen as a function of two elements demonstrated in figure 5. (EN ISO 12100:2010)

Table 3. Derived from ISO 12100



Probability of occurrence of harm	
Exposure of persons to the hazard	Need for access
	Nature of access
	Time spent in the hazard zone
	Number of persons requiring access
	Frequency of access
Occurrence of a hazardous event	Reliability and other statistical data
	Accident history
	History of damage to health
	Comparison of risks
Possibility of avoiding or limiting harm	Persons which can be exposed to hazard
	How quickly hazardous situation could cause harm
	Awareness of risk
	Human ability to avoid or limit harm
	Practical experience and knowledge

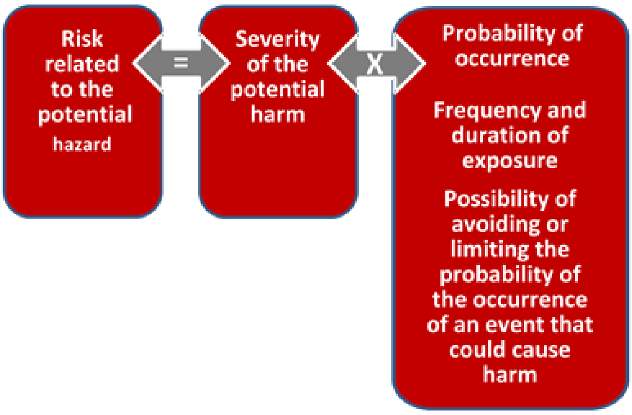

Risk related to the potential hazard
=
Severity of the potential harm
X
Probability of occurrence
Frequency and duration of exposure
Possibility of avoiding or limiting the probability of the occurrence of an event that could cause harm

Figure 5. Risk as a function of elements (Schneider Electric 2016b)

2.7 Stop Category 0

In each of the following chapters is determined how a machine should behave when it is stopped to fulfil the selected or required category.

Stop Category 0 is the most common motion safety function and it can be found from almost all drives as a standard. The safety function in Stop Category 0 is STO – Safe Torque Off. Removing the power that generates torque from machine actuators ensures the stopping of a machine. This uncontrolled stop allows machine to freewheel until standstill is reached. STO ensures that no torque that could generate energy can affect the motor and so prevents unintended starting. (Schneider Electric 2017.)

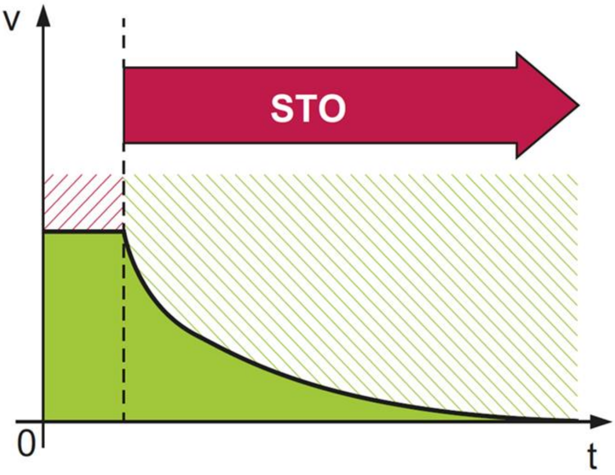


Figure 6. Safe Torque Off (Schneider Electric 2017)

2.8 Stop Category 1

Stop Category 1 is very common in machines which require stopping movement with high inertia or when the control off machine stopping is required to avoid mechanical collision. The safety function in Stop Category 1 is SS1 – Safe Stop 1. This function causes the motor a rapid but controlled rundown by keeping the electrical power available for machine actuators and switches the motor to a torque free mode (STO) after the standstill conditions are met. (Schneider Electric 2017.)

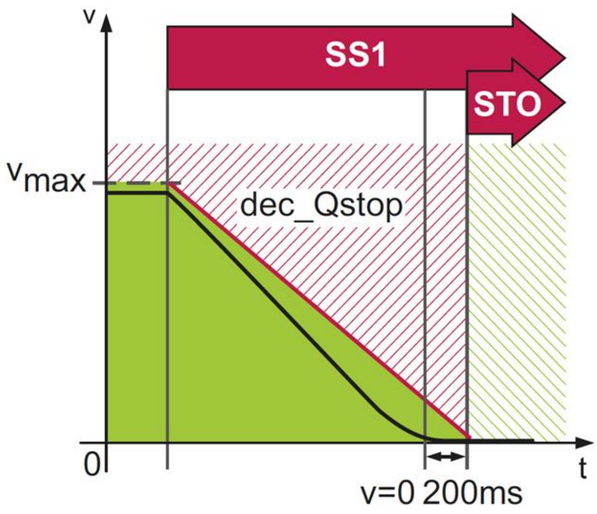


Figure 7. Safe Stop 1 (Schneider Electric 2017)

2.9 Stop Category 2

Stop Category 2, final stop function is basically more advanced version of Stop Category 1 and doesn’t differ greatly from it. Safety function in Stop Category 2 is SS2 – Safe Stop 2. This function causes motor rapid and controlled rundown and achieves standstill like SS1. Instead of activating STO when standstill conditions are met is SOS function activated. SOS – Safe Operating Stop is a counterpart for STO-based standstill, when STO cuts all of the power, which can affect the motor, the SOS function enables even full torque to be used to maintain standstill. This standstill state is monitored and in controlling software is determined tolerance within motor can have movement. (Schneider Electric 2017.)

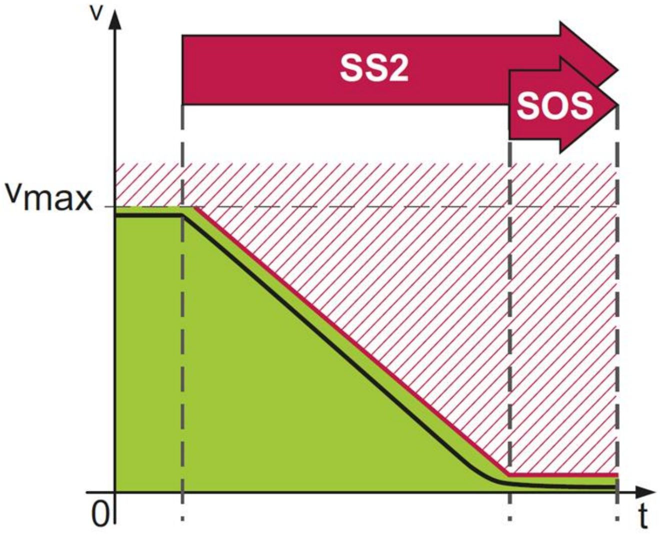


Figure 8. Safe Stop 2 (Schneider Electric 2017)

2.10 Safe Limited Speed

Speed monitoring safety function (SLS) working principle is to assure that speed of the drive doesn’t violate determined limit speed. When SLS is activated control of drive starts to decelerate to achieve limited speed, safety device is monitoring the speed. If preset safety speed is not reached during monitoring time or if speed will exceed the limit, the safety device will activate fallback safety function such as SS1 or STO. (Schneider Electric 2017.)

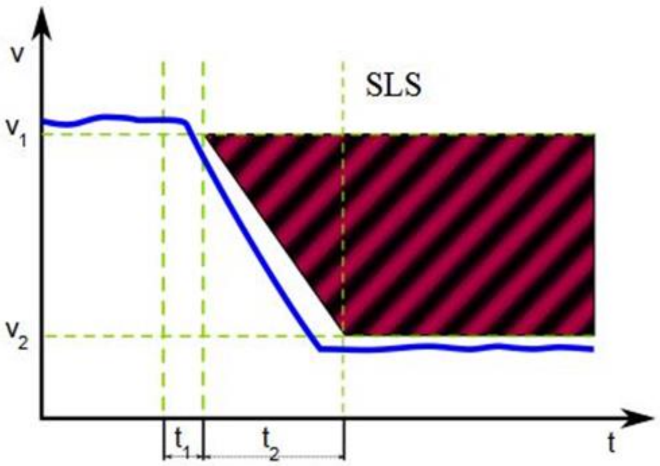


Figure 9. Safe Limited Speed (Schneider Electric 2017)

3 PacDrive3

PacDrive (Programmable Automation Controller and Drive) is Schneider Electric automation solution for high performance machines not only motion oriented but also automation oriented. With complete automation system from controllers to input modules and servo drives with embedded safety under same Sercos III communication PacDrive3 offers flexible automation solution with large variety of models that can reduce time to market. (Schneider 2017b). PacDrive3 embedded safety location in the markets is demonstrated in figure 10. The PacDrive3 solution is introduced below.

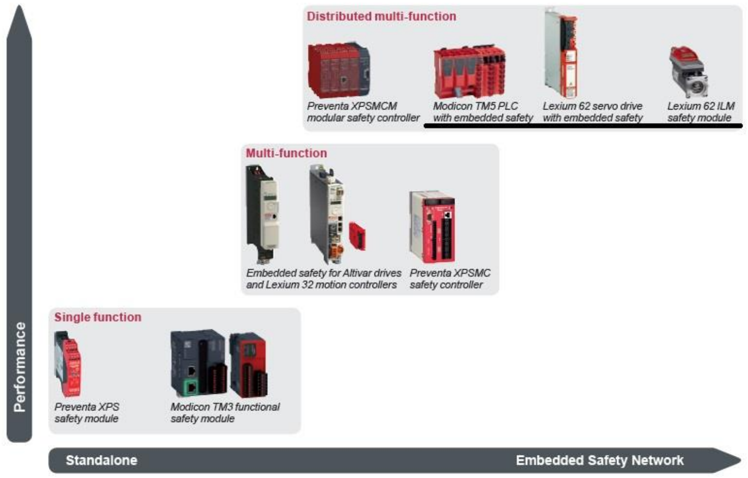
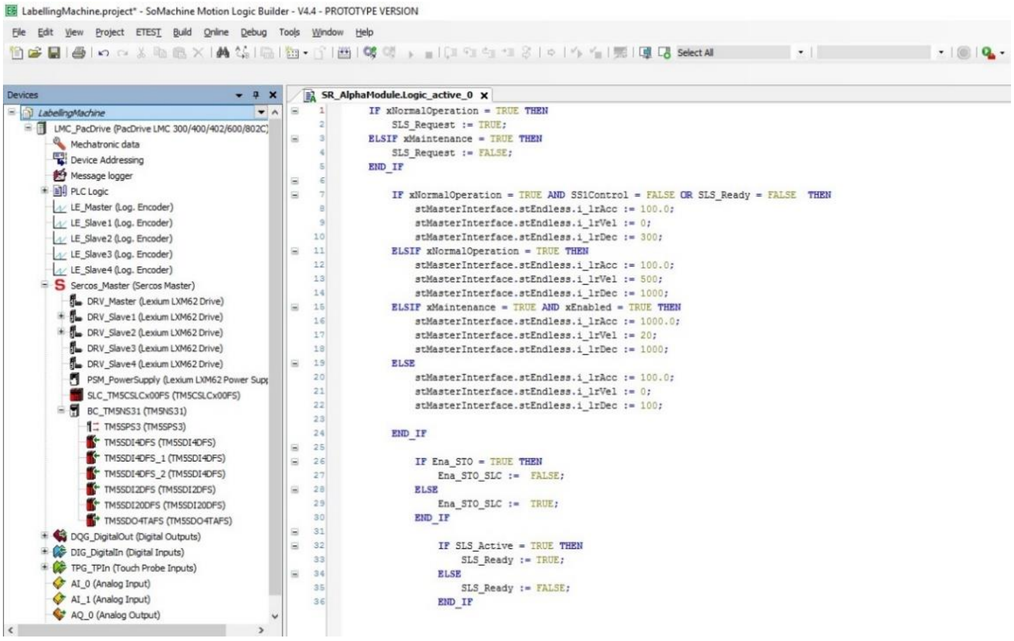

Distributed multi-function
Preventa XPSMCM modular safety controller
Modicon TM5 PLC with embedded safety
Lexium 62 servo drive with embedded safety
Lexium 62 ILM safety module
Multi-function
Embedded safety for Altivar drives and Lexium 32 motion controllers
Preventa XPSMC safety controller
Single function
Preventa XPS safety module
Modicon TM3 functional safety module
Performance
Standalone
Embedded Safety Network

Figure 10. Embedded safety positioning in markets (Schneider Electric 2018)

3.1 SoMachine Motion

SoMachine Motion is Schneider Electric software for developing, configuring and commissioning PacDrive 3 -system. SoMachine is creating one project file which contains all engineering tools provided. Logic builder is a tool for programming PacDrive controllers, by using IEC 61131-1 comforting programming languages such as LD, ST, FBD. Motion builder is a tool for motion design and sizing of motion related devices like motors, gearboxes, drives. Software contains also built in HMI configuration software Vijeo designer which contains, to mention some, along with other features graphical editor, object animation and simulator. (Schneider Electric 2016.)


LabellingMachine.project* - SoMachine Motion Logic Builder - V4.4 - PROTOTYPE VERSION
File
Edit
View
Project
ETEST
Build
Online
Debug
Tools
Window
Help
Select All
Devices
LabellingMachine
LMC_PacDrive (PacDrive LMC 300/400/402/600/802C)
Mechatronic data
Device Addressing
Message logger
PLC Logic
LE_Master (Log. Encoder)
LE_Slave1 (Log. Encoder)
LE_Slave2 (Log. Encoder)
LE_Slave3 (Log. Encoder)
LE_Slave4 (Log. Encoder)
Sercos_Master (Sercos Master)
DRV_Master (Lexium LXM62 Drive)
DRV_Slave1 (Lexium LXM62 Drive)
DRV_Slave2 (Lexium LXM62 Drive)
DRV_Slave3 (Lexium LXM62 Drive)
DRV_Slave4 (Lexium LXM62 Drive)
PSM_PowerSupply (Lexium LXM62 Power Supp
SLC_TM5CSLCx00FS (TM5CSLCx00FS)
BC_TM5NS31 (TM5NS31)
TM5SPS3 (TM5SPS3)
TM5SDI4DFS (TM5SDI4DFS)
TM5SDI4DFS_1 (TM5SDI4DFS)
TM5SDI4DFS_2 (TM5SDI4DFS)
TM5SDI2DFS (TM5SDI2DFS)
TM5SDI20DFS (TM5SDI20DFS)
TM5SDO4TAFS (TM5SDO4TAFS)
DQG_DigitalOut (Digital Outputs)
DIG_DigitalIn (Digital Inputs)
TPG_TPIn (Touch Probe Inputs)
AI_0 (Analog Input)
AI_1 (Analog Input)
AQ_0 (Analog Output)
SR_AlphaModule.Logic_active_0

```
IF xNormalOperation = TRUE THEN
    SLS_Request := TRUE;
ELSIF xMaintenance = TRUE THEN
    SLS_Request := FALSE;
END_IF

    IF xNormalOperation = TRUE AND SS1Control = FALSE OR SLS_Ready = FALSE  THEN
        stMasterInterface.stEndless.i_lrAcc := 100.0;
        stMasterInterface.stEndless.i_lrVel := 0;
        stMasterInterface.stEndless.i_lrDec := 300;
    ELSIF xNormalOperation = TRUE THEN
        stMasterInterface.stEndless.i_lrAcc := 100.0;
        stMasterInterface.stEndless.i_lrVel := 500;
        stMasterInterface.stEndless.i_lrDec := 1000;
    ELSIF xMaintenance = TRUE AND xEnabled = TRUE THEN
        stMasterInterface.stEndless.i_lrAcc := 1000.0;
        stMasterInterface.stEndless.i_lrVel := 20;
        stMasterInterface.stEndless.i_lrDec := 1000;
    ELSE
        stMasterInterface.stEndless.i_lrAcc := 100.0;
        stMasterInterface.stEndless.i_lrVel := 0;
        stMasterInterface.stEndless.i_lrDec := 100;

    END_IF

        IF Ena_STO = TRUE THEN
            Ena_STO_SLC :=  FALSE;
        ELSE
            Ena_STO_SLC :=  TRUE;
        END_IF

            IF SLS_Active = TRUE THEN
                SLS_Ready := TRUE;
            ELSE
                SLS_Ready := FALSE;
            END_IF
```

Figure 11. SoMachine Motion Logic Builder

3.1.1 SoSafe Programmable add-on

Safety systems of PacDrive3 are programmed using SoSafe Programmable safety add-on. Software is embedded to the SoMachine Motion environment and each hardware component is defined there as a part of whole system. The application program and configuration of safety hardware is made in SoSafe Programmable. (Schneider Electric [Referred 02.03.2018].)

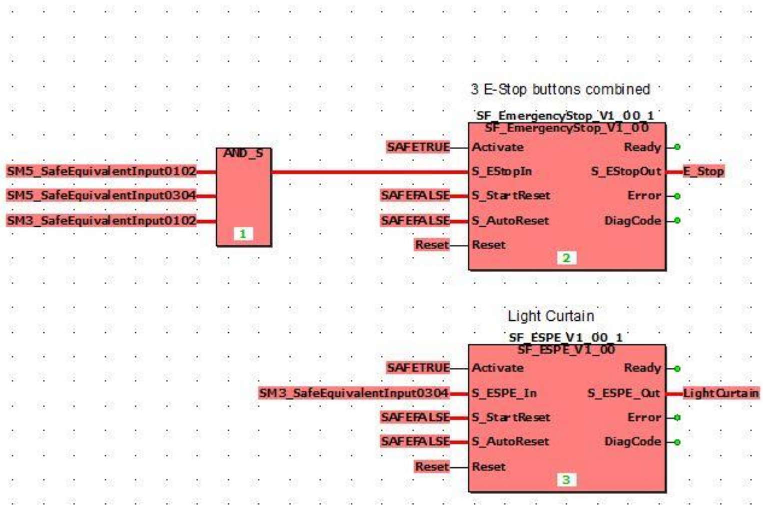


Figure 12. Part of SoSafe Programmable application program

3.2 Sercos

The Sercos (SErial Real-time COmmunication System) is one of the leading bus systems in industrial application already over 25 years. Origin of Sercos takes place to the mid-1980s when industrial consortium supported by VDW and ZVEI created first generation digital drive interface. First it was used mainly in advanced machine tool applications, following years it came worldwide accepted and used in all kind of servo-driven applications. (Sercos 2018.)

In 1999 second generation of Sercos was launched. Data transmission rates were increased and service channel for the transmission of asynchronous data was extended. This new technology has been available since 2001, while downward compatibility to the first generation was maintained. (Sercos 2018.)

Nowadays Sercos is standard bus for many branches, especially in highly dynamic servo applications with many axes like printing machines, packaging machines and multi-axis machine tools. (Sercos 2018.)

3.2.1 Basic Topologies

Sercos network has always a master device and at least one slave device. Typically devices are used in line or in ring topology. For this reason Sercos devices are containing two communication ports, which are used to connect devices to previous and to next device of topology. (Sercos 2018.)

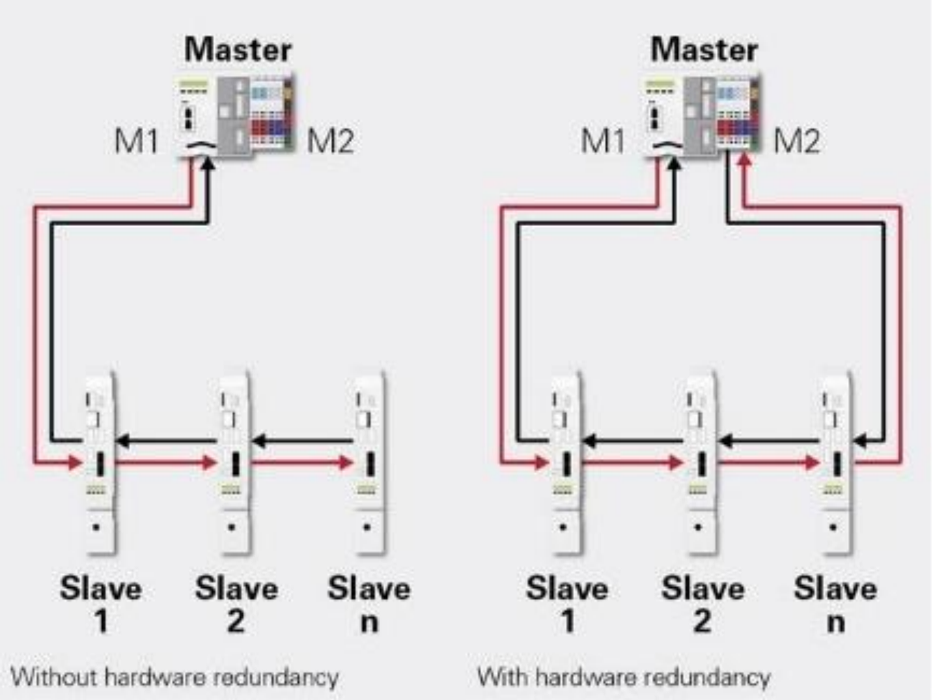


Figure 13. Line and Ring topologies (Sercos 2018)

In line topology sercos devices are connected in line after the master device. Data telegrams are running through the slave devices and are looped back from last device. Every device is analysing data from both directions, this guarantees data reachability for all the devices despite the order they are placed in. This way all the devices are integrated to the network. (Sercos 2018.)

Ring topology has same working principle and features than line topology with one extra benefit. Adding one more cable to network between last device and the master device forms a ring. This topology provides redundancy for network, which means additional safety for communication. If one cable breaks between devices the network will not lose the synchronization or communication. (Sercos 2018.)

3.2.2 Advantages

Sercos allows decentralized, unlimited real-time communication and intelligent automation structures with cross communication between all devices. Indirect communication between slaves bypassing the master device would compromise synchronous movements, e.g. corrupting robotic axes or slowing reaction times of machines. Thou Sercos slaves can communicate via cross communication directly with minimum communication dead times, this opens ability for unlimited real-time communication and intelligent machine structures. Controller to controller communication uses same principle when communicating to each other's. (Sercos 2018.)

All data is always processed in two directions despite of used topology. This gives an advantage of minimal delay even with longer cycle times. All real-time data is synchronized in every point of network. Data processing in easy, efficient and flexibly in individual network nodes. Diagnostics and monitoring of network are carried out as a result. (Sercos 2018.)

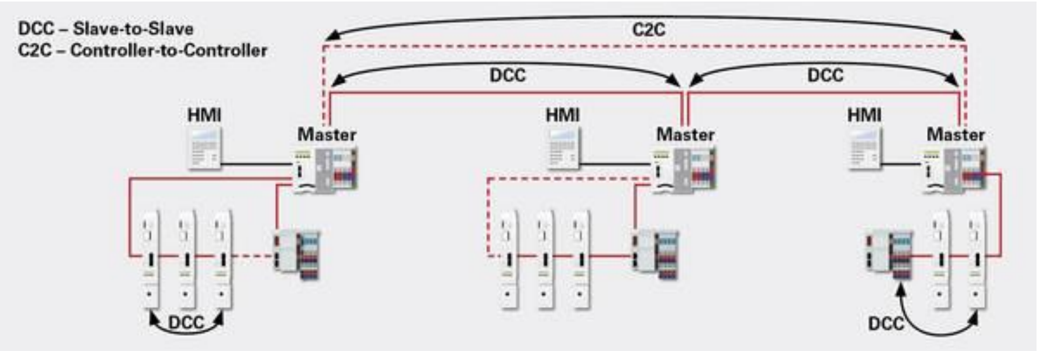


Figure 14. Cross communication between slaves and controllers (Sercos 2018)

Key benefits of Sercos for PacDrive: Universal, fully integrated for drive, fieldbus and safety communication. Media redundancy reduces probability of failure and keeps communication reliable. Powerful network keeps update rate minimal even with high amount of servo axes. Cost-effective Sercos doesn’t need hubs or switches. (Sercos 2018.)

3.3 Integrated system approach

PacDrive3 digital system architecture is based to the concept of a centralized controller. Single controller performs all control functions from Cartesian and robotic motion to temperature regulation and machine logic, by using IEC 61131-3-compliant machine program. This is the main principle to create modular machines. (Schneider Electric 2015.)

Figure 15. PacDrive3 related products (2017c)

PacDrive3 offers single controller solution for motion, PLC logic and for communication. All calculations of all axis positions are made in controller which allows change from real to the virtual axes on the fly. Motion testing and simulation is possible to perform without connecting servo drives or motors. Configuration of modular machine is made easy as possible. Controller recognizes all modules connected to it and is able to active or deactivate them automatically based upon the modules connected to the machine. (Schneider Electric 2015.)

3.3.1 Logic Motion Controller

Large variety of PacDrive LMC controllers makes possible to cover wide range of applications, from small application with a few servo axes to complex high-performance system up to 130 synchronized axes. Factors such as number of axes, data transmission volumes and range of robotic elements determines best controller for application. (Schneider Electric 2017b)

Figure 16. LMC Eco and LMC Pro/Pro2 (Schneider Electric 2017b)

All controller series share the same identical Schneider Electric Logic Motion Runtime software. Programming tool for LMC controllers is Schneider Electric SoMachine Motion software, which is used to develop, configure and commission the whole PacDrive system. Depending of the controller model, the controllers are equipped with integrated digital and analog I/Os. Standard and high-speed IOs are also included to the controllers for fast response of sensor inputs e.g. motion-relevant signals. Safety IOs can be added to the system with Sercos bus coupler and modular TM5 and TM7 I/O solution. (Schneider Electric 2017b)

3.3.2 Lexium servo system

Lexium servo system contains different drive systems and servo motors. Drive systems from stand-alone to integrated or detached are designed to meet with all kind of requirements of machine builders from small number of axes to modular machines and cabinetless automation. PacDrive3 automation solution contains four servo systems. Stand-alone solution Lexium 52, multi-axis solution Lexium 62, integrated drive solution Lexium 62 ILM and detached drive solution Lexium 62 ILD. All of these servo drive solutions are fully software-compatible and they can be implemented side by side in mixed configuration. (Schneider Electric 2017c)

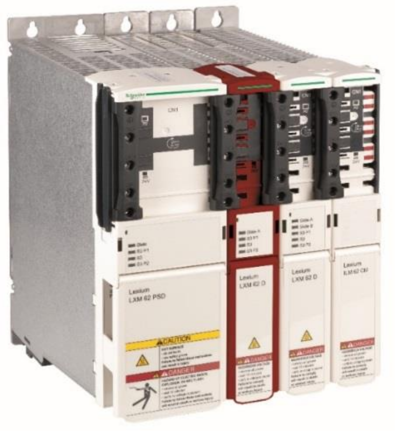


Figure 17. Lexium 62 power supply and drives (Schneider Electric 2017e)

3.3.3 TM5/TM7 I/O system

Modicon TM5 series is IP20-rated modular I/O system which provides flexible and scalable configuration for expansions and distributed islands with direct communication between controller and TM5 slices. Family contains digital input and output modules, analogue modules, power distribution modules and communication modules. (Schneider Electric 2014.) Safety versions of TM5 modules are coloured red.

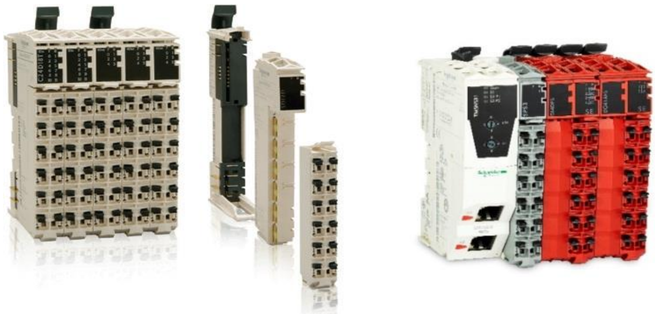


Figure 18. TM5 non-safety and safety modules. (Schneider Electric [Referred 6.7.2017])

Modicon TM7 series of IP67-rated I/O blocks to achieve concept of “Flexible machine Control” by offering possibility to mount devices outside of electrical cabinet directly on installation. The protection of IP-class guarantees functional control of machines and processes even in the harshest environments which contains water, oil, dust, etc. Family contains digital input and output modules, analogue modules, power distribution modules and communication modules. (Schneider Electric 2014.) Safety versions of TM7 modules are coloured red.

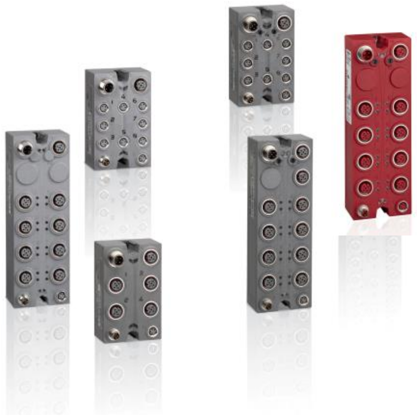


Figure 19. TM7 slices (Schneider Electric [Referred 6.7.2017])

3.4 Embedded Safety and SLC

PacDrive3 embedded safety is orientated to motion centric and distributed machines which requires safety using one fieldbus, this is made by adding safety PLC, safety I/O slices and safety drives to the system. Embedded safety offer for PD3 is certified to fulfil EN ISO 13849-1 PL e Category 4, and EN/IEC 62061 SIL 3. Safety related devices are managed by Modicon safety logic controller which communicates with systems master controller. Following figure demonstrates how normal and safety-related devices are working in same network. (Schneider Electric 2018.)

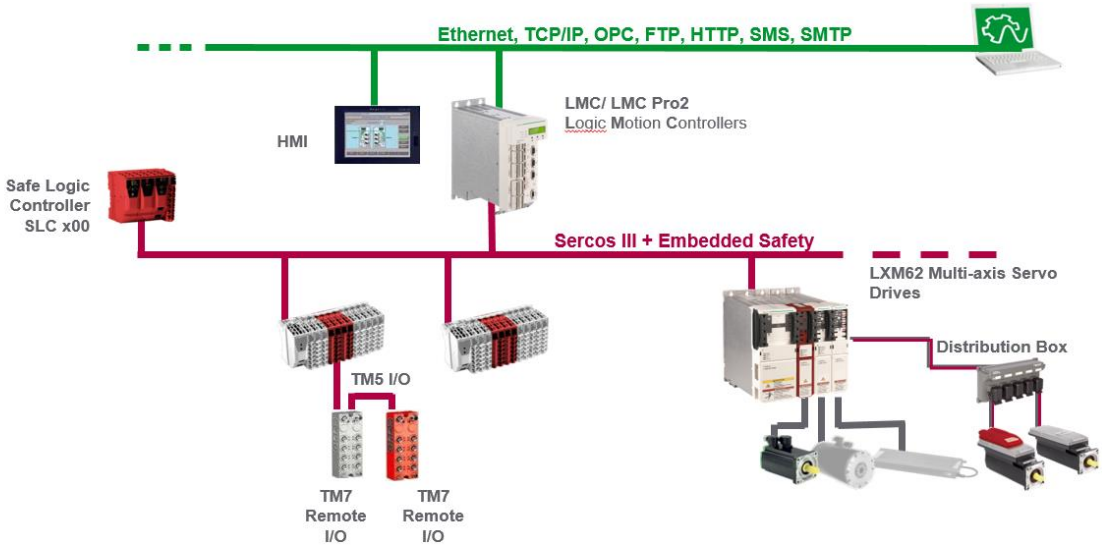


Figure 20. PacDrive3 embedded safety architecture (Schneider Electric [Referred 2.3.2018])

Safety logic controller is performing all safety-related task made in SoSafe Programmable. SLC is communicating with LMC master controller by Sercos network, controllers are capable to exchange configured variables between each other’s in both directions. Therefore it is possible to use variables provided by safety I/Os or SLC as a part of machines main control application program. The maximum number of safety I/O modules connected to one SLC controller is one hundred. (Schneider Electric 2017d.)

Figure 21. Modicon Safety logic controller (Schneider Electric [Referred 6.7.2017])

4 Robotic palletizing & Labelling Machine

The practical part was started by investigating the possible machines which would be suitable for this thesis work. After the suitable machines where chosen the actual work was started. In the beginning the first step was to get understanding on how the selected machines are working. This learning process was accomplished by using all available material from the machine manufacturers. The material contained pictures, product brochures and introduction videos which were analysed carefully to get enough understanding. The second step was to recognize the possible sources of hazards. At this point the first standards were also looked to see which kind of hazards these machines could cause. After the hazards had been identified it was a natural step to continue studying how frequent and severe they could be and how they could be properly reduced. When the decisions on the safety functions and devices had been made the actual work of programming and testing the safety application was started.

The first application study of this thesis was robotic palletizing. Automated palletizing can be referred to as an industrial robotic palletizing system which performs the application automatically.

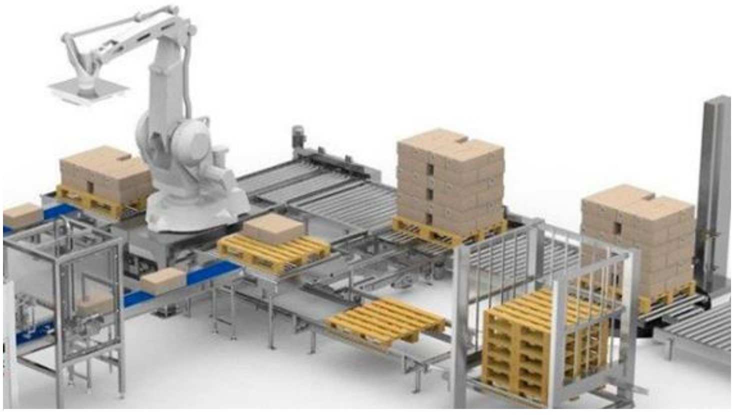


Figure 22. ULMA palletizing system (ULMA packaging [Referred 13.3.2018])

The second application study of this thesis was the labelling machine. The chosen labelling machine uses a tubular sleeve created inside the machine from roll fed labels film stock.

Figure 23. Sacmi labelling machine (Sacmi [Referred 13.3.2018])

4.1 Automatic operation modes and safety in them

In automatic operation modes is described behaviour of machines during automatic drive which are determined by using all possible information provided by manufacturers. Typical information sources for this kind of studies are datasheets, functional descriptions and videos.

4.1.1 Palletizing robot

Palletizing robot station is fed by one or multiple conveyor lines with packed products ready to be moved to the pallets. A pallet dispenser is delivering an empty pallet for the station when needed. Full pallets are moved with a conveyor system to the wrapping machine which prepares the pallets for transportation. Full pallets are moved with a conveyor system to the wrapping machine which prepares the pallets for transportation.

Palletizing robots are typically placed inside of monitored guards with locked guard doors. Product input and output are guarded by light curtains with a muting function which allows the material to enter and exit the robot operational area. Detected interruption of light curtains will cause a protective stop of the system. The system contains also multiple Emergency Stop pushbuttons, which are located at each control station that can affect the robot’s motion. All operation modes are also monitored with the Safe Maximum Speed which prevents the user from misusing the machine by setting a too high operating speed.

4.1.2 Labelling machine

Labelling machine is fed with filled and capped bottles or cans by a conveyer system. Machine made labels are attached to bottles in a carousel. The machine itself does not need an operator to use the machine when labelling is started. When the label roll is empty a new one needs to be attached to the machine. The operation modes are controlled by a selector switch and an enabling switch.

The machine is covered with safety glass or plastics, the parts with opening possibilities are guarded with door switches and interlocks. Opening of these guards during normal operation will cause a safe stop of machine. A light curtain is placed into the roll infeed module of the machine. The machine contains E-Stop push buttons which are located around the machine. The activation of the E-Stop will cause an immediate stop of the machine. All operation modes are also monitored with the Safe Maximum Speed which prevents the user from misusing the machine by setting a too high operating speed.

4.2 Manual modes and safety in them

Selecting a manual mode from the selector switch causes the machine to stop movement but does not activate any stop function. It is possible to drive the machine with a slow speed using the enabling device. This is a typical way to use the enabling switch and can be applied to all kind of machines.

Manual mode is a monitored slow speed operation mode for manual driving and configuration procedures controlled by selector switch and enabling switch, where the machine user can safely run the machine after changed configurations or during maintenance.

4.3 Safety in manual mode

Slow movement of manual mode is controlled by using an enabling switch. In this mode the machine operator can enter the restricted space of the machine by opening locked or monitored guards. The safety outputs, except for the emergency stop and enabling switch in the emergency position, are not used.

If the enabling switch is pressed until the panic position the STO safety-function will be activated and the robot's movement stopped. Also the release of the switch will cause the stopping of the machine's movements but without the activation of the safety function. The working principle of the 3-stage enabling switch is introduced in Figure 24.

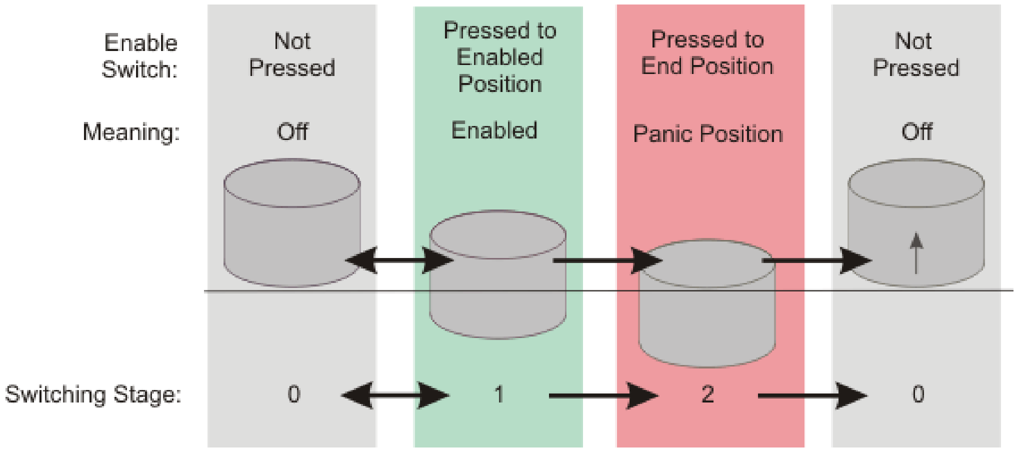


Figure 24. Working principle of an enabling switch (Schneider Electric [Referred 5.7.2017])

4.4 Hazards of robotics

In the table below are listed some of the possible hazards of robotic systems. The C-type standard ISO 10218-1 for robots and robotic devices – safety requirements for industrial robots provides a list of significant hazards for robots and robot systems. The list in the table is derived from standard ISO 12100.

Table 4. Hazards of robotics

Hazard Type	**Origin**	**Risk**	**Injury**
Mechanical	Movement of a robot arm, rotational move of any axis, unintended movement of jigs or a gripper.	Drawing in, entanglement, impact, stabbing.	Wounds, crushes, fractures, burn, death.
Electrical	Contact with exposed parts or connections, confusion of various voltages on system.	Equipment failure, arc flash, electrocution.	Burns, projection of molten particles, electric shock, death.
Others	Cables, hoses, poorly designed teach pendant or enabling devices.	Falling, slipping, stripping, fatigue, unhealthy postures when repeating move.	Fractures, bruises, bad back.

4.5 Hazards of system for labelling machine

Labelling machine doesn’t have specific c-type standard to determine hazard types and origins for machine. In this case the basic safety standard ISO 121100 is used. The list in the table is derived from standard ISO 12100.

Table 5. Hazards of machinery

Hazard Type	**Origin**	**Risk**	**Injury**	**Labelling Machine**
Mechanical	Rotating parts	Drawing in, Entanglement	Crushes, Fractures, Burn, Death	Carousel, In- and outfeed starwheels, Sleeve unit
Mechanical	Linear Moving parts	Impact, Crushing, Severing, Drawing in	Crushes, Fractures, Death	Conveyor, Sleeve application
Mechanical	Sharp edges, moving or stationary	Cutting, Puncturing	Wounds	
Electrical	Machine Electrics	Equipment failure, bad condition of equipment	Burns, Electric Shock, Death	
Other	Cables or Hoses	Falling, Slipping, Stripping	Fractures, Bruises	

4.6 Example architecture

This chapter presents an architecture example for a robotic palletizer from the machine safety point of view. Figure 25 demonstrates the connections between devices using Sercos III communication and safety input device connections to TM5 safety modules. The numbered device clusters in the figure are points where the scalability of the system for the used machine needs to be taken into account. This means that the variety and number of devices connected to I/O modules, servo drives and servo motors is adapted to answer the needs of the currently used machine.

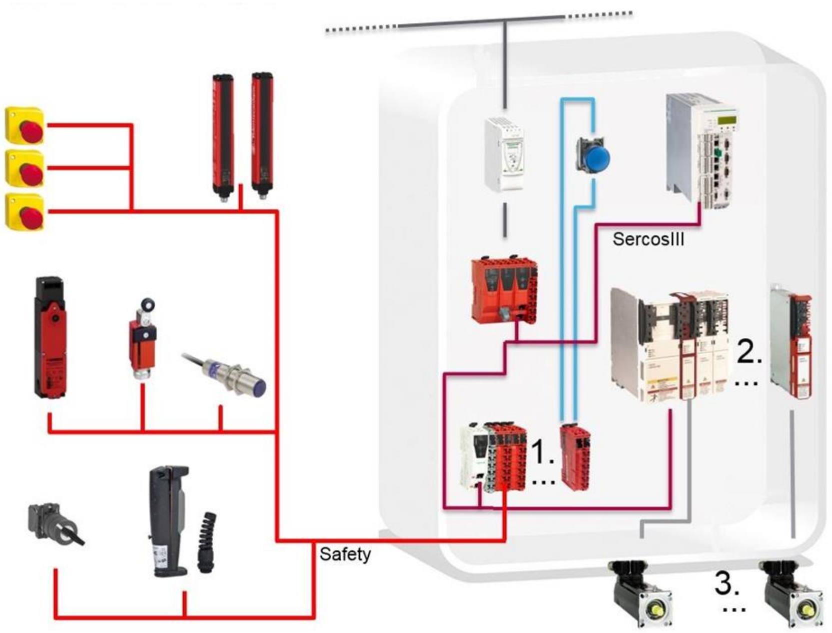


Figure 25. Possible architecture layout

The performance of each safety function is specified by using SIL (Safety Integrity Level) and PL (Performance Level), which are determined in standards EN/IEC 62061 and EN/ISO 13849-1. The basic concepts, general principles and risk assessment are described in EN/ISO 12100, which is the basic standard for machinery. The Safety Category is estimated by means of risk assessment.

Safety level calculations are made by using Sistema Safety Integrity tool which shows that certain points of machine operations require PLr-level PLe and SIL-level SIL 3. The used products, wirings and controlling software must also reach these levels.

The machine’s complexity makes it well suitable for the PacDrive3 system which can control and monitor large number of drives, safety-related equipment and safety-related functions. In this example application the Lexium62 double drive and servo motors are used as an output to simulate the machine’s operation states.

Functional tests and fault simulations were run and documented to designed and built safety application programs. The equipment and devices used in the test and partial data from the tests are presented in the appendixes.

4.7 Summary of Safety functions

The used safety functions in the safety application programs were selected according to the standards. If no specific standard instructions were found for the particular machine type the functions were selected according to the needs of a corresponding machine. For robotics there is a c-type standard ISO 10218 which states the protective stop of a robot in the following way.

> At least one protective stop function shall be a stop category 0 or 1, as described in IEC 60204-1. The robot may have an additional protective stop function using stop category 2 as described in IEC 60204-1 that does not result in drive power being removed but does require monitoring of the standstill condition after the robot stops. Any unintended motion of the robot in the monitored standstill condition or detected failure of the protective stop function shall result in a category 0 stop in accordance with IEC 60204-1.(ISO 10218-1:2011, 11)

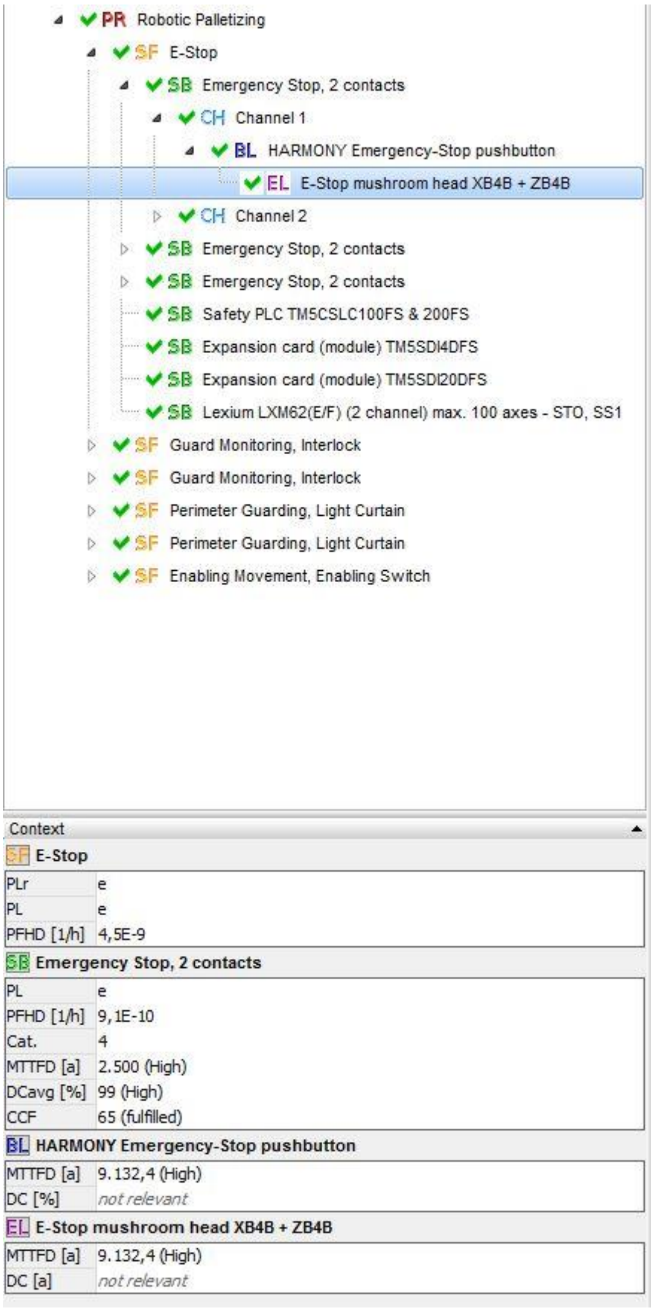
The safety application program of the robotic palletizer therefore contains the stop categories 0 and 1. In this case the optional stop category 2 is not used.

The labelling machine does not have the c-type standard which usually would refer which kind of stop functions are needed. For this reason safety functions are selected by evaluating the needs of a machine. Safety application of labelling machine contains the stop categories 0 and 1.

The used safety functions in these two machine applications are emergency stop, guard monitoring, movement enabling, speed monitoring and perimeter guarding. Detailed information on these functions can be found from the Sistema safety calculation project and safety data files, which are not shown in this thesis.

4.8 Safety data

Machine safety related safety data calculations were made by using the Sistema calculation software with the Schneider Electric device libraries. All safety functions used in the safety applications are confirmed to fulfill the determined performance and safety integrity levels. Sistema project files has been done but not shown in this thesis completely. See figures below for the information of one safety function.



- ✓ PR Robotic Palletizing
  - ✓ SF E-Stop
    - ✓ SB Emergency Stop, 2 contacts
      - ✓ CH Channel 1
        - ✓ BL HARMONY Emergency-Stop pushbutton
          - ✓ EL E-Stop mushroom head XB4B + ZB4B
      - ✓ CH Channel 2
    - ✓ SB Emergency Stop, 2 contacts
    - ✓ SB Emergency Stop, 2 contacts
    - ✓ SB Safety PLC TM5CSLC100FS & 200FS
    - ✓ SB Expansion card (module) TM5SDI4DFS
    - ✓ SB Expansion card (module) TM5SDI20DFS
    - ✓ SB Lexium LXM62(E/F) (2 channel) max. 100 axes - STO, SS1
  - ✓ SF Guard Monitoring, Interlock
  - ✓ SF Guard Monitoring, Interlock
  - ✓ SF Perimeter Guarding, Light Curtain
  - ✓ SF Perimeter Guarding, Light Curtain
  - ✓ SF Enabling Movement, Enabling Switch

Context

SF **E-Stop**

PLr	e
PL	e
PFHD [1/h]	4,5E-9

SB **Emergency Stop, 2 contacts**

PL	e
PFHD [1/h]	9,1E-10
Cat.	4
MTTFD [a]	2.500 (High)
DCavg [%]	99 (High)
CCF	65 (fulfilled)

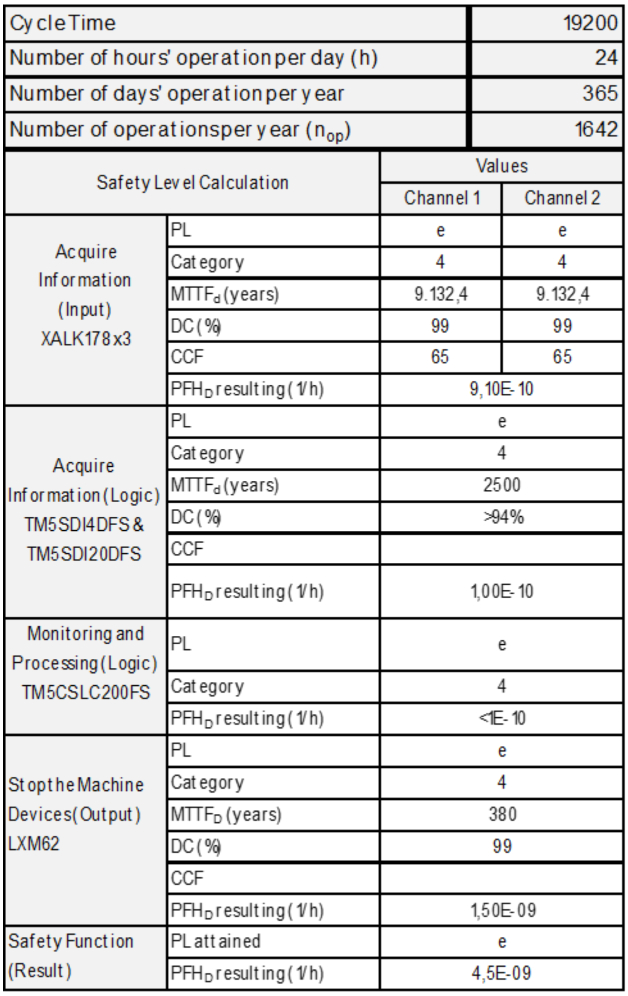
BL **HARMONY Emergency-Stop pushbutton**

MTTFD [a]	9.132,4 (High)
DC [%]	*not relevant*

EL **E-Stop mushroom head XB4B + ZB4B**

MTTFD [a]	9.132,4 (High)
DC [a]	*not relevant*

Figure 26. Emergency stop safety function



Cycle Time	19200
Number of hours' operation per day (h)	24
Number of days' operation per year	365
Number of operations per year (n_{op})	1642

Safety Level Calculation		Values	
		Channel 1	Channel 2
Acquire Information (Input) XALK178x3	PL	e	e
	Category	4	4
	$MTTF_d$ (years)	9.132,4	9.132,4
	DC (%)	99	99
	CCF	65	65
	PFH_D resulting (1/h)	9,10E-10	
Acquire Information (Logic) TM5SDI4DFS & TM5SDI20DFS	PL	e	
	Category	4	
	$MTTF_d$ (years)	2500	
	DC (%)	>94%	
	CCF		
	PFH_D resulting (1/h)	1,00E-10	
Monitoring and Processing (Logic) TM5CSLC200FS	PL	e	
	Category	4	
	PFH_D resulting (1/h)	<1E-10	
Stop the Machine Devices (Output) LXM62	PL	e	
	Category	4	
	$MTTF_D$ (years)	380	
	DC (%)	99	
	CCF		
	PFH_D resulting (1/h)	1,50E-09	
Safety Function (Result)	PL attained	e	
	PFH_D resulting (1/h)	4,5E-09	

Figure 27. Safety data of emergency stop

5 Summary

The aim of his thesis was to produce machine safety design examples for the Schneider Electric PacDrive3 automation system. The designs were made for two selected machines which were a labelling machine and a robotic palletizer.

The theory part introduced some of the key features of machine safety. Standards, categories and performance levels were in the main positions of machine safety. The safe limited speed function was also introduced as it is used in both application programs. Introduction to PacDrive3 automation system forms the main part of the theory to give understanding of how big but still flexible the system is.

In the practical part machines were introduced and their operation modes were explained. The safety features used in the machines were explained with functional descriptions of the machines. This part contained also hazard tables derived from the a-type ISO 12100 and c-type ISO 10218-1 standards. Partial safety data information was also introduced. Wiring diagrams for all connections between devices were also drawn but they were not shown in this thesis. The safety application program was made by using the SoMachine Motion with the SoSafe Programmable safety add-on. The functional test and fault simulations for architectures were run and documented but, like wirings, they are not shown in this thesis.

BIBLIOGRAPHY

IFA. No date available. Software: Sistema. [www-document]. IFA. [Referred 09.03.2018]. Available: http://www.dguv.de/ifa/praxishilfen/practical-solutions-machine-safety/software-sistema/index.jsp

EN ISO 10218-1. 2011. Robots and robotic devices – Safety requirements for industrial robots. International organization for standardization.

NF EN ISO 12100-2. 2010. Safety of machinery – General principles for design – Risk assessment and risk reduction. Afnor.

Robotic Industries Association. No date available. Safety Categories, Performance Levels and SILs for Machine Safety Control Systems. [Online publication]. Robotic Industries Association. [Referred 22.02.2018]. ble: https://www.robotics.org/filesDownload.cfm?dl4=2_Understanding%20Safety%20Categories%2C%20Performance%20Levels%20and%20SILs%20for%20Machine%20Safety%20Control%20Systems.pdf

Sacmi. No date available. Product profile. [www-document]. Sacmi. [Referred 13.3.2018]. Available: http://www.sacmi.com/en-US/Products-and-Services/Beverage-Packaging-machines-producer/Business-Units/Labelling/FORMSLEEVE-Labellers.aspx?idc=62427&ln=en-US

Schneider Electric. 2009. Safe Machinery Handbook. [Online publication]. Schneider Electric [Referred 16.06.2017]. Available: https://www.schneider-electric.fi/documents/original-equipment-manufacturers/pdf/Machine-safety-guide.pdf

Schneider Electric. 2014a. 03 Machine Safety Principles training v3. [PowerPoint-presentation]. Schneider Electric [Referred 02.03.2018]. Available: Only for internal use

Schneider Electric. 2014b . Modicon TM5/TM7 Flexible System. [Online publication]. Schneider Electric [Referred 18.09.2017]. Available: https://www.schneider-electric.us/en/download/document/EIO0000000426/

Schneider Electric. 2015. PacDrive 3 automation solution. [Online publication]. Schneider Electric [Referred 18.09.2017]. Available: http://electroautomatica.ru/img/documentation/MKTED2120601EN_3.pdf

Schneider Electric. 2016a. SoMachine Motion Software. [Online publication]. Schneider Electric [Referred 18.09.2017]. Available: https://www.schneider-electric.com/en/download/document/DIA7ED2160302EN/

Schneider Electric. 2016b. Implementation Guide for Safety Functions. [Worddocument]. Schneider Electric [Referred 02.03.2018]. Available: Only for internal use

Schneider Electric. 2017a. 01 Machine_Safety_May_2017. [PowerPoint-presentation]. Schneider Electric [Referred 05.02.2018]. Available: Only for internal use

Schneider Electric. 2017b. PacDrive3 automation solution, PacDrive LMC motion controllers. [Online publication]. Schneider Electric [Referred 16.09.2017]. Available: https://www.schneider-electric.us/en/download/document/DIA7ED2160303EN/

Schneider Electric. 2017c. PacDrive3 General Presentation. [Online publication]. Schneider Electric [Referred 16.09.2017]. Available: https://www.schneider-electric.com/en/download/document/DIA3ED2160301EN/

Schneider Electric. 2017d. Modicon TM5 Safety Logic Controller SLC100/200 FS, Hardware Guide. [Online publication]. Schneider Electric [Referred 16.09.2017]. Available: https://www.schneider-electric.us/en/download/document/EIO0000000889/

Schneider Electric. 2017e. PacDrive3 automation solution, Lexium 62 multi-axis drive system. [Online publication]. Schneider Electric [Referred 16.09.2017]. Available: https://www.schneider-electric.co.uk/en/download/document/DIA7ED2160305EN/

Schneider Electric. 2018. Safety Modicon TM5 & TM7Safety logic controller and safety I/O module. [Online publication]. Schneider Electric [Referred 16.06.2017]. Available: https://www.schneider-electric.us/en/download/document/DIA3ED2160309EN/

Schneider Electric. No date available. Embedded safety PLC Technical presentation V2.1. [PowerPoint-presentation]. Schneider Electric [Referred 02.03.2018]. Available: Only for internal use

Schneider Electric. No date available. SF_EnableSwitch_SE. [User Guide]. Schneider Electric [Referred 5.7.2017]. Available: Only for internal use

Schneider Electric. No date available. Schneider Electric product picture database. Schneider Electric [Referred 6.7.2017]. Available: Only for internal use

Schneider Electric. No date available. Company profile. [www-document]. Schneider Electric. [Referred 21.2.2018]. Available: https://www.schneider-electric.de/de/about-us/careers/vocational-training/marktheidenfeld/

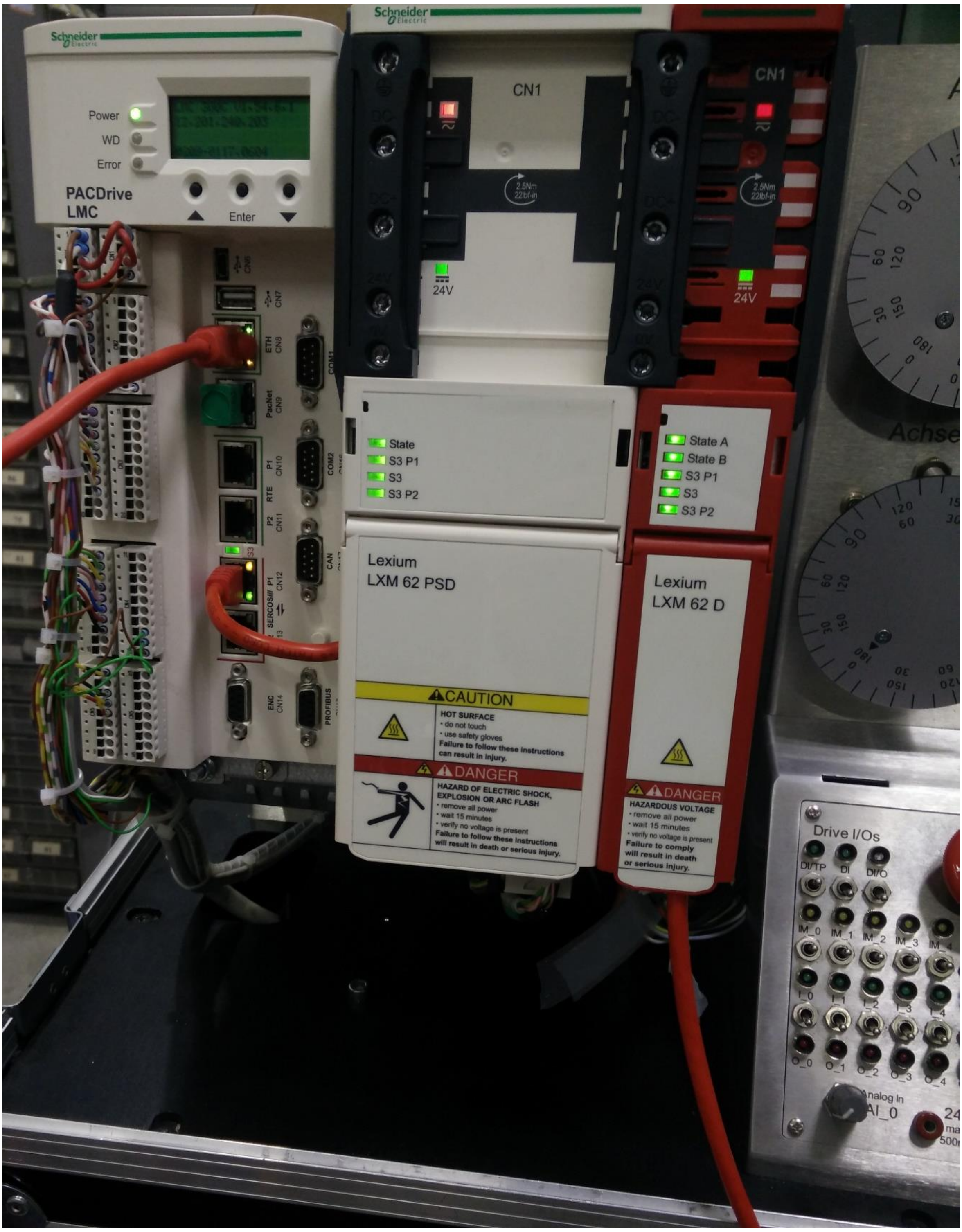
Sercos. 2018. Sercos Technology. [www-document]. Sercos. [Referred 10.01.2018]. Available: https://www.sercos.org/technology/

Sick. 2015. Guide for Safe Machinery. [Online publication]. Sick [Referred 16.03.2017]. Available: https://www.sick.com/media/docs/8/78/678/Special_information_Guide_for_Safe_Machinery_en_IM0014678.PDF

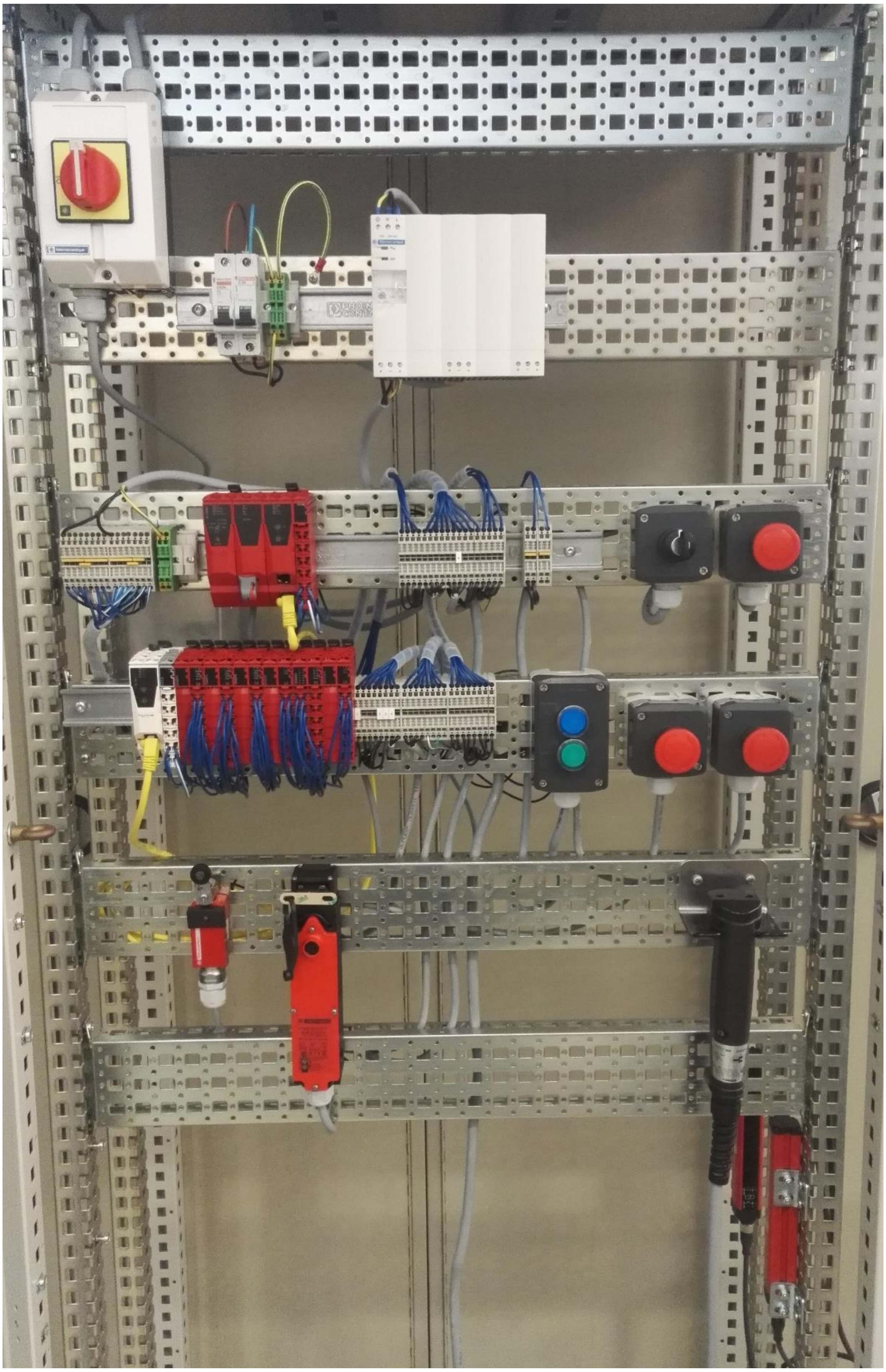
ULMA packaging. No date available. Product profile. [www-document]. ULMA packaging. [Referred 13.3.2018]. Available: http://www.ulmapackaging.com/packaging-machines/integral-solution/palletizing-systems

APPENDICES

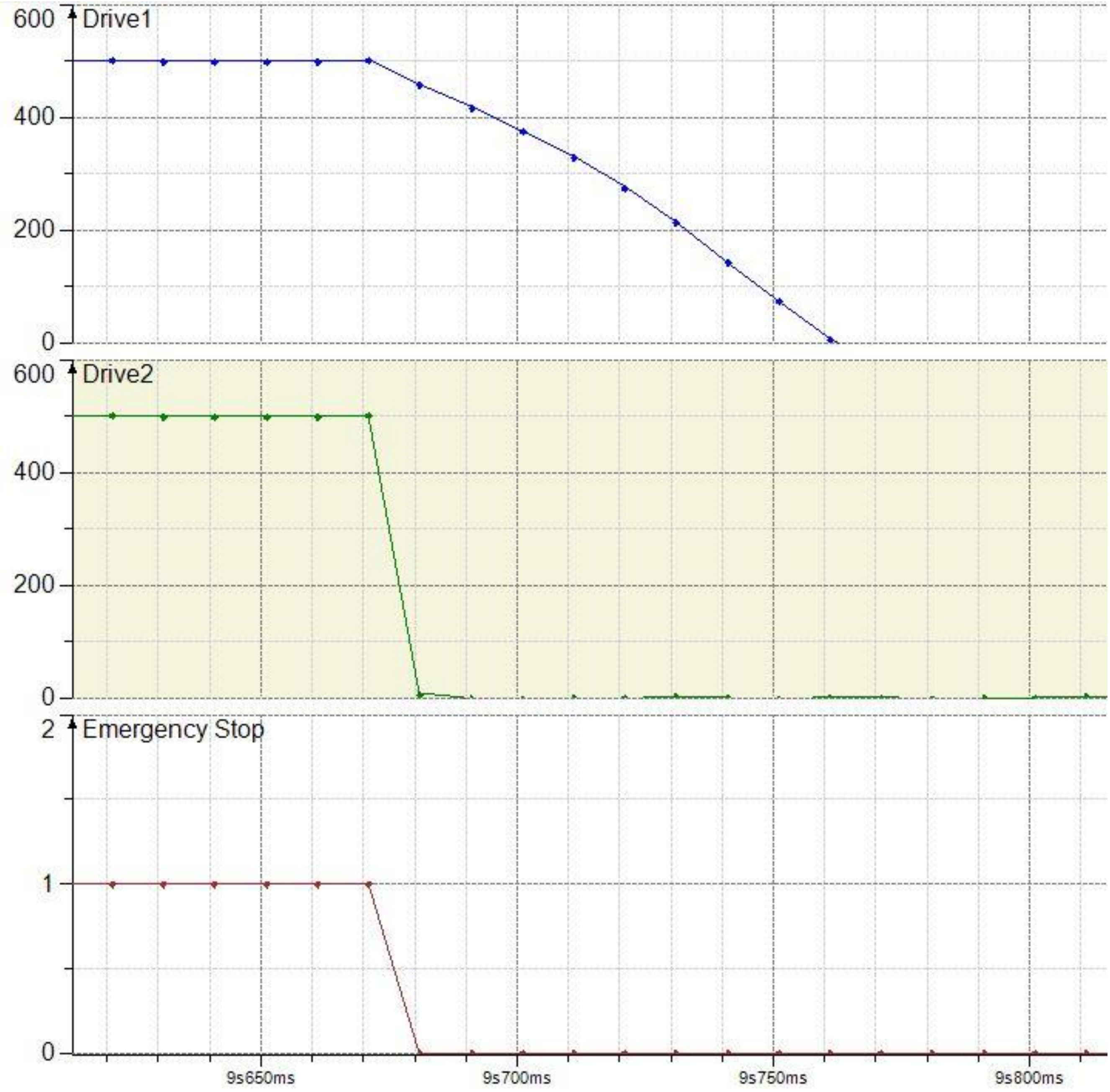
APPENDIX 1


Schneider Electric
Power
WD
Error
PACDrive LMC
Enter
CN1
24V
State
S3 P1
S3
S3 P2
State A
State B
Lexium LXM 62 PSD
Lexium LXM 62 D
CAUTION
DANGER
Drive I/Os
Achse

APPENDIX 2



APPENDIX 3


600
400
200
0
Drive1
600
400
200
0
Drive2
2
1
0
Emergency Stop
9s650ms
9s700ms
9s750ms
9s800ms