Ostwestfalen-Lippe University of Applied Sciences

Department of Electrical Engineering and Technical Informatics

bachelor thesis

of the Lord

Philip Kleen

Matr. No.: 1524 4088

according to the bachelor's examination regulations for the electrical engineering course in the version published on October 26, 2011

(Announcement sheet of the university 2011/No.29).

Topic: Implementation of a concept for functional safety (safety) for a versatile assembly system using SafetyBridge technology

1st examiner: Prof. Dr.-Ing. Juergen Jasperneite

2nd examiner: Prof. Dr.-Ing. Rolf Hausdorfer

The report consists of 51 pages.

Explanation

I declare that I have completed this bachelor's degree independently. I did not use any sources or resources other than those specified.

The copy and appendices are included on CD-ROM.

Lemgo, 11/18/2015

_____

Philip Kleen

Hochschule Ostwestfalen-Lippe
University of Applied Sciences

Department of Electrical Engineering and Technical Informatics

Implementation of a concept for functional safety (safety) for a versatile mounting system using the SafetyBridge technology

from

Philip Kleen

November 2015

summary

In this bachelor thesis, the safety concept from the study work is implemented with the SafetyBridge technology (SBT) from Phoenix Contact. The existing versatile assembly system of the smartFactoryOWL consists of three system components: the smart transfer system, a laser engraving machine and a robot assembly machine. These three machines will be equipped with the SBT-V3 to enable communication for the exchange of safety-related data between the three Ma

build rails. The safety function of the cross-machine emergency stop is set up via these communication links . With sensors on the machines and an extensive evaluation in the safety control of the transfer system, an expectation of the number of required emergency stop signals is built up. This is confirmed by the machine operator. The safety-related components were integrated into the standard controls.

When implementing the safety concept, eight machines should be considered: the integration environment and seven possible machine modules that can be integrated. This requirement could not be met. On the one hand, the SBT was not powerful enough for the concept created and, on the other hand, no adequate user specifications could be created. For these reasons, the implementation was limited to three possible machine modules for integration. With this restriction, an emergency stop function could be implemented across all integrated machine modules without restricting the versatility of the assembly system. In addition, the existing safety functions of the machine modules were checked and supplemented. Possible requirements for future security concepts and controls emerged during implementation. Similar challenges arose, for which solutions are already being sought in standard automation technology.

Table of Contents

List of Figures

glossary

CE mark

The machine manufacturer must affix a CE mark to the machine that is placed on the market . [1, p. 380]

CE marking

Necessary certification from the machine manufacturer that the machine meets all relevant regulations of the Machinery Directive and can therefore be placed on the market. The CE mark certifies this to the user. [1, p. 380]

CE conformity, declaration of conformity

Procedure with which it is declared that the machine placed on the market corresponds to the basic safety and health requirements of the MD. The CE marking can only be issued with the declaration of conformity. [1, p. 390]

CEN

Stands for Comité Européen de Normalization and is the European committee for standardization.

CENELEC

Stands for Comité Européen de Normalization Électrotechnique and is the European committee for electrotechnical standardization.

European standard (EN)

Marking of a standard that it is harmonized under an EU directive or was developed by CENELEC or CEN.

Machinery Directive (MRL)

Directive 2006/42/EC of the European Parliament and of the Council of May 17, 2006 on machinery and amending Directive 95/16/EC (recast). The directive applies to machines and, among other things, defines the relevant basic safety and health requirements in Annex I (agreement between the EU member states who undertake to convert these into national law). [1]

NAMUR

NAMUR is an international association of users of automation technology in the process industry. [2]

Performance Level (PL)

Discrete level that specifies the ability of safety-related parts of a controller to perform a safety function under foreseeable conditions: from PL a (highest probability of failure) to PL e (lowest probability of failure). [3]

Safety Integrity Level (SIL)

Discrete level (one of three possible) for defining the requirements for the safety integrity of the safety-related control functions, which is assigned to the SRECS , with safety integrity level 3 representing the highest safety integrity level and safety integrity level 1 representing the lowest safety integrity level. [4]

Safety Related Electrical Control System (SRECS)

en: safety-related electrical control systems
Safety-related electrical control system of a machine, the failure of which leads to an immediate increase in risk. [4, p. 14]

smartFactoryOWL

The SmartFactoryOWL addresses the most important fields of action of the intelligent factory, such as adaptability, resource efficiency and human-machine interaction . Intelligent technical systems play a prominent role here.

Located on the campus of the Ostwestfalen-Lippe University of Applied Sciences in Lemgo, in the middle of one of the most important mechanical engineering regions in Germany, the SmartFactoryOWL is at the same time a practice-oriented test and demonstration platform for the scientists and engineers of the participating research institutions and industrial companies as well as a learning environment for students of the engineering disciplines. [5]

Programmable Logic Controller (PLC)

en: Programmable Logic Controller (PLC)
A programmable logic controller is a device used to control or
Used to control a machine or system and programmed on a digital basis

becomes.

List of abbreviations

BCD	Binary Coded Decimal
Ministry of Labor and Social Affairs	Federal Ministry of Labour and Social Affairs
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
DIN	German Institute for Standardization
dip	Dual in-line package
EN	European Standard
HMI	human-machine interfaces
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
MRL	machine guideline
NAMUR	standard working group for measurement and control technology technology in the chemical industry
OPC UA	Open Platform Communication – Unified Architec door
OSI	Open Systems Interconnection
OWL	Ostwestfalen-Lippe
pl	performance level
PROFINET	PROcess FIELD NETwork
RFID	Radio Frequency IDentification

SBT SafetyBridge technology
SIL safety integrity level
PLC programmable logic controller

UDP User Datagram Protocol

1 Introduction

1.1 Motivation and goal setting

The versatile assembly system of the smartFactoryOWL meets the requirements of the fourth industrial revolution. Individual, independent machines are brought into an integration environment. A system for the assembly of various products is created. The previous study work showed that a uniform functional safety concept had to be found for this system design. In the study work, standards were analyzed in relation to a modular machine design in accordance with the NAMUR recommendation *NE 148 .* Such plant concepts are intended to create production plants that can be used in a variety of ways. For this purpose, a single machine makes the completion of a work step available as a service. By exchanging individual work steps in the form of machines or interchangeable equipment, individual and different products can be manufactured. In addition to determining applicable standards, the focus was on analyzing the technological possibilities of a consistent emergency stop concept. Setting up safety-related, certified machine-to-machine communication is a possible solution for implementing a consistent emergency stop that meets the requirements of such a system concept . This can be made possible via a corresponding P2P connection.

In the student research project, various technologies from different manufacturers were compared, with the result that it is only possible with considerable effort to develop a mechanism that enables reliable, secure machine-to-machine communication . The existing assembly system must be equipped with functional safety technology that is established on the market. In comparison, the SafetyBridge technology (SBT) from Phoenix Contact, among other things, was able to meet the decisive requirements. The decisive factor was above all the fact that SBT components had already been installed in the machines.

A modular and global emergency stop is to be implemented with the SBT-V3 . A machine module that has already been taken into account is connected to the transfer system at a designated location and put into operation. Adding and removing is to be made possible by functional safety without stopping the entire system. A manageable and conscious procedure must be found when adding and removing machine modules in the assembly system. Only the required technological procedure is considered. In order to fulfill the risk-reducing measures from the risk assessment according to *DIN EN ISO 12100 ,* safe sensors and actuators must be selected and put into operation

men. Risk assessment considerations such as:

a permissible point in time for a change to the system or ensuring that only machines are integrated that correspond to the permissible machine type (classification) at the respective point in time.

1.2 Outline

In Chapter 2, State of the Art, the current implementation of the emergency stop and the risk-reducing measures on the machines are explained. It is assumed that the versatile assembly system is known. This has already been explained in the thesis . The state of the art of the machine modules, the smart transfer system and the standards and guidelines are considered. The SBT is discussed below. Chapter 3 formulates the requirements that must be met in order to achieve the goal of creating a functionally safe, versatile assembly system.
The concept of the modular emergency stop to be implemented and its implementation is described in Chapter 4 below. The non-secure implementation in the PC-WORX programming environment is also discussed. A partial validation in Chapter 6 checks whether the requirements from Chapter 3 are met. For this purpose, the guaranteed response time is determined. Finally, in Chapter 6.6, there follows an outlook on future requirements for safety-related products and possible improvements in the control-related implementation of the safety concept.

2 State of the art

This chapter explains the state of the art of the smart transfer system, the machine modules and the SafetyBridge technology (SBT). In the previous study work, several possible safety concepts and associated control- technical solutions for the versatile assembly system were presented. The Phoenix Contact concept is based on the SBT and is to be integrated into the versatile assembly system. Each machine module is an independent machine with its own programmable logic controller (PLC). The machine modules are supplied with electricity, compressed air and information via defined interfaces. This can be used to connect the machine modules to the transfer system as interchangeable equipment . The definition of the term security was already explained in the study paper, see [6, p. 3]. In this bachelor thesis is also with *sure* resp . *Safety* refers to the reference to functional safety.

2.1 Smart transfer system

Depending on how it is viewed, the smart transfer system can be used as an integration environment *DIN EN ISO 11161* or as a basic machine according to the Machinery Directive (MRL) . The smart transfer system is an extended slide system. It was expanded in such a way that on the one hand it provides integration stations with a supply connection and on the other hand the production information is transported directly with the product via an RFID tag in the slide . At the integration places , machine modules can be added to the system as integratable machines or as interchangeable equipment . Furthermore, another communication path is available through the provision of an Ethernet interface in the supply connection. This can be a possible interface for networking functional safety. Due to this property, the transfer system provides more functions than the originally intended product transport. The automation takes place via a central control for the entire transfer system. This prepares the sensors and actuators and makes them available to the integrated machine modules via a software interface . However, the smart transfer system is currently unable to provide any reliable answers to the following functional safety questions:

- How are the machines arranged?
- Which machines are integrated?
- What dangers can the integrated machine modules pose?
- How many machines are currently integrated?

• When may the machine be added or removed from the process? • When must which integrated machine be transferred to a safe state?

Some of the questions can already be answered by standard automation technology. Answering the questions and the functions described above make the transfer system a bit more intelligent. It represents the basic machine of the versatile assembly system. A non-intelligent transfer system only offers the possibility of workpiece transport using a static object carrier. This includes the organization of transport via stoppers and indexing. During the risk assessment, it was noticed that the smart transfer system only has an emergency stop switch on the control cabinet. A magnetic actuator from Schmersal is already attached to the workpiece carriers to determine the correct positioning in connected machine modules. There is no additional protective measure on the transfer system.

The lack of an emergency stop switch was particularly noticeable on the transfer belt assembly for product removal and at the integration station for manual assembly steps.

2.2 Robot assembly machine

On the assembly machine with a robot, access to the protected area for the robot is not monitored. The separating protective device is prepared for quick dismantling and can be removed during operation. Dismantling is not a suitable access to set up the robot, see risk assessment of the machine.
It is also possible to reach into the protected area by reaching underneath. Furthermore , there is access to the protected area when no magazine is used. The presence of a magazine is not queried. In this context, it should be noted that there is no device that allows operation without an engaged magazine. A limitation of the working area and the manual control operation with the manual control device is monitored via the Kuga control. The release for automatic operation is set via the already installed SafetyBridge-V2 and the evaluation of a local emergency stop switch is taken over. According to the user *standard DIN EN ISO 10218-2 ,* there is no clear selection of the operating mode. There must be manual and automatic operation. The machine module does not have any safety-related sensors to determine whether it has been introduced into an integration environment. A manual user selection via a corresponding operating mode is also not available.

2.3 Engraving Machine

This machine can engrave a product using a laser beam
will. The laser unit is controlled by its own controller. This provides an interface for safety locks, via which the laser beam can be safely switched off or a shutter can be closed in an emergency. The shutter securely closes the laser beam so that it does not necessarily have to be switched off. The secure magnetic sensor from Schmersal checks that the laser cabin is correctly closed by the workpiece carrier. In addition, an emergency stop switch is evaluated via the already installed SafetyBridge-V2 and integrated into the emergency stop circuit of the laser. Access to the laser cabin is not suitable for maintenance work. A possible opening of the laser cabin by unscrewing side elements of the housing is not monitored. When engraving different materials, sparks may fly or vapors may be generated. It must be ensured that no materials are used that could cause flying sparks, as the vapors are extracted with a filter system. The proper operation of this system is not monitored. The machine can be operated in a manual or automatic mode. One
there is no clear selection of operating modes. Further details can be found in the risk assessment of the machine. This machine module has neither a sensor system for the formation of secure information nor a manual option for specifying the place of use and can therefore not check the selection of an associated operating mode. For this reason, it is not possible to distinguish whether the machine module is operated as interchangeable equipment or an integrable machine on a compatible system or as a single machine. This means that non-corresponding functional safety functions cannot be selected.

2.4 The SafetyBridge system

The SBT from Phoenix Contact is a secure, proprietary system that works together with various standard PLCs and exchanges safety-related data using the black channel principle via standardized bus systems and components.

> " The SafetyBridge technology from Phoenix Contact is ideal for all safety applications in which conventional safety relays are too inflexible, parallel wiring proves to be too costly due to the expansion of the safety circuits, or the use of a safe bus system in conjunction with a safe controller is ruled out for cost reasons as an economical solution.” [7, p. A-1]

A conventional implementation of the emergency stop would have been possible with safety relays, but this parallel wiring would have proved to be very complex due to the smart transfer system. Another point is that some of the modular inline system from Phoenix Contact is already installed in the machines. The SafetyBridge hardware is installed by adding it to the existing Inline stations. This means that no special installation guidelines need to be observed when installing the modules, apart from the standard guidelines for inline technology . [7, p. A-1] The SafetyBridge system has a modular structure and can be adapted to the requirements. At least one so-called logic module is required. In addition to eight safe outputs, this provides safe logic and is therefore the safety controller. Such a module is called an island . The expansion modules are assigned to this logic module via addressing . These are called satellites. Before the SafetyBridge modules are lined up, they must be addressed via DIP switches. Transmission speed, address (island number) and satellite number are set. The procedure can be found in the user manual. [7]

The inputs and outputs are parameterized using the supplied SAFECONF programming environment. Safe blocks and functions are available for evaluating safety devices. Binary data can be exchanged between the standard controller and the safety logic. In this way, an individual status query and an acknowledgment can be made via the standard programmable logic controller (PLC) or the enabling principle for functions and outputs can be implemented. A status of all safe inputs and outputs and diagnostic data can be read out with the standard controller. The functions configured in SAFECONF are executed on the SafetyBridge logic module . An island can be expanded with 16 additional modules, the so-called satellites. Different digital input and output modules can be combined.

The SBT relies on a standard controller from Phoenix Contact, Rockwell Automation, Siemens, Schneider Electric or a CODESYS-based controller that organizes the data transfer between the logic modules and the satellites. The logic module must be added to the implementation of the standard controller using the available function blocks from the Phoenix Contact library . The application created in SAFECONF can be exported in the required format and loaded onto the logic module as a function block or as a binary file.

2.4.1 SAFECONF programming environment

SAFECONF is the free programming environment that is included or can be downloaded for TriSafe and SafetyBridge, products from Phoenix Contact. The required safety functions can be created and exported using this programming environment. The following safe modules are available for implementation: anti and equivalent, contactor monitoring, 3-stage enabling switch, emergency stop evaluation, evaluation of isolating and non-contact protective devices, 5-way operating mode selector switch, muting modules for light barriers, reset and two-hand evaluation -Control units. The blocks can be linked with safety-related and standard logic. The following functions are available for this: TRUE and FALSE, AND and OR, comparison of two signals for inequality or equality, trigger on rising or falling edge, SR and RS function, switch-on and switch-off delay, pulse generation, negation, exclusive Or and linking of a safe and non -safe signal according to the enabling principle. The networks can be designed clearly using connectors. A signal from a connector can only be used after it has been written in the further course of implementation. In addition, 16 safe and 32 non-safe inputs and outputs are available for exchanging binary signals with other controllers.

2.4.2 Structure of the cross communication

With the SBT-V3 , the logic modules (islands) can exchange 32 signals with each other, 16 binary input signals and 16 output signals. To do this, the logic modules in a SAFECONF project of a higher-level logic module must be added as a slave in the hardware structure and the address of the slave island must be parameterized. A hierarchical or flat topology can arise. These two variants can be combined with each other. The structure of the standard network is initially not from Be interpretation. When determining shutdown times, the network structure and utilization are decisive. In the Phoenix Contact documentation, the only requirement for the network is that it must be deterministic. This requirement is discussed further in Chapter 3.4 . A watchdog time for the safety-related communication connection must be defined in the parameterization of a slave logic module. The Phoenix Contact Competence Center Safety found out that the transmission time of the safe communication connection to the slave logic module is measured by a toggle bit, which is sent from the logic module to the satellite and from there back to the logic module. Therefore, the watchdog time of the connection must b

be like the transmission and processing time of the standard and security components involved. As mentioned at the beginning, the secure cross-communication is exchanged through the existing infrastructure according to the black channel principle via the standard components, see Chapter 2.4.3. A maximum of 31 SafetyBridge logic modules (islands) can be installed in a system. A maximum of 16 additional satellites can be connected to an island. In addition to the expansion modules, this also includes logic modules that are added as slaves to the hardware configuration in the higher-level SAFECONF project . As a result, the number of possible cross-connections to other islands depends on the number of modules already present. Via function blocks for standard
controls, the SBT is integrated into the implementation of the standard control.
Secure cross-communication with high availability can only occur if the communication connection between the standard controllers exists and if it has a deterministic property.

Determination of the guaranteed switch-off *time (tG)*

The guaranteed switch-off time of the SBT consists of a processing *time (tIN)* at the input terminal, a transmission *time (tFW D_IN)* from the satellite to the logic module, a processing *time (tOUT_LP SDO)* from the logic module itself, and the configured transmission times *(tFW D_SLb)* to other logic modules together. If the signal is passed on via logic modules, the processing *times (tOUT_LP SDOa) add up.* The signal must still be passed on from a logic module to a satellite with output terminals . The time is taken into account with *(tFW D_OUT).* The time *(tOUT)* is required to set the output. Equation (1) for determining the guaranteed switch-off *time (tG)* of the SBT results for a signal course over x logic modules .

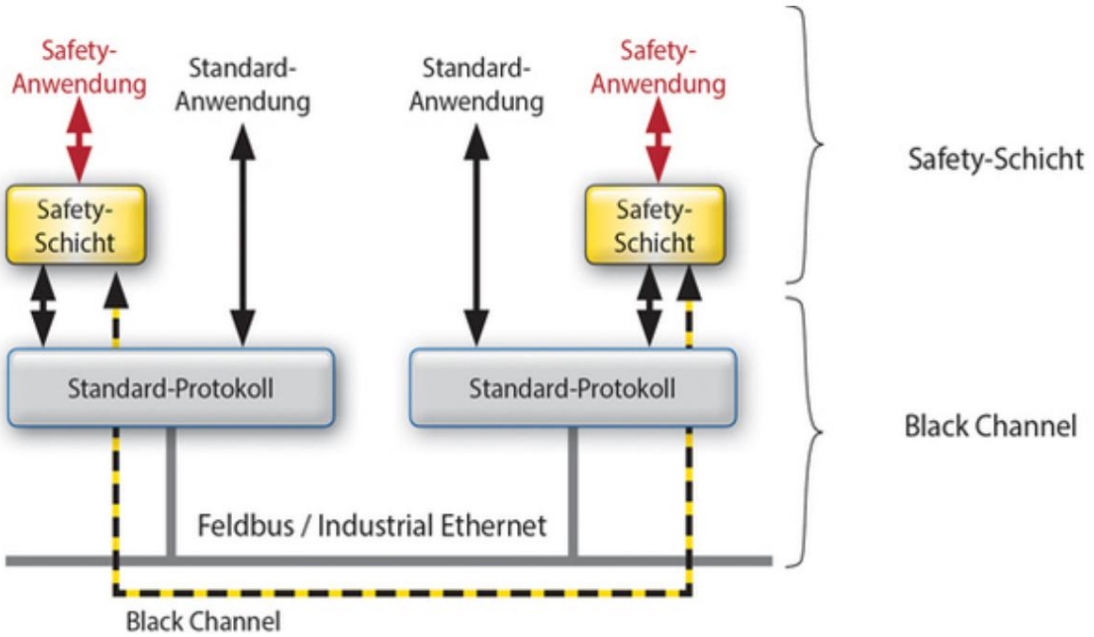
$$tG = tIN + tFW\ D\_IN + x\ tOUT\_LP\ SDO + \sum_{n=1}^{x} tFW\ D\_SLn + tFW\ D\_OUT + tOUT \quad (1)$$

2.4.3 Black Channel Principle

The black channel principle encapsulates the part for executing a safety function from the standard functions. Applied to a communication system, this means that all the hardware components, protocols and services previously required for networking automation components are combined as a communication channel that is not further specified . When analyzing contexts, a similar principle is used, which makes certain contexts easier to view

summarized as a *black box* . With the black channel principle, all layers of the OSI reference model are combined and a *safety layer* (a security communication layer) is inserted above them. The protocol that represents this layer must meet the requirements of *IEC 61784-3* and comply with the required measures to ensure the required transmission quality. “This principle has been worked out together with certifiers such as TÜV, has been scientifically examined and is well secured. In this way, an additional safety layer above the black channel turns a standard fieldbus or a standard Industrial Ethernet solution into a system with which data for functional safety can be reliably transmitted." [8]

The opposite of the black channel principle would be the white channel principle. The entire communication path is considered a secure system and must meet the requirements of *IEC 61508* . [9]



Source: [8]

Figure 1: With the black channel principle, the security function acts as its own *Safety layer* on the actual transmission medium

2.5 Networking of the machines

A deterministic network is required in Section 3.4. For better understanding, this terminology is specified in more detail below. Starting from a general definition

of determinism from the dictionary, this is transferred to machine-level networking.
In this context, some facts are briefly explained as a basis.

> "Teaching, conception of the causal [pre]determination of all events or action"

Transferred to a network technology, the definition can be understood as follows : The behavior of the network can be determined in particular for future events.
This applies above all to the temporal behavior of the technology used. The *Ethernet* medium used according to IEEE 802.3x initially does not have this property .
One reason for this is that the bus is accessed using the random and non-deterministic Carrier Sense Multiple Access/Collision Detection (CSMA/CD) method according to IEEE 802.3 . Corrupted data is detected via a checksum from the User Datagram Protocol (UDP) and consequently discarded. Only correctly transmitted data is processed further, which is to be understood as data consistency. Due to the cyclic sending of the data, there is no need to send it again in the event of an error. A confirmed service could result in outdated process data being transmitted. With the UDP in combination with the Internet Protocol (IP) or through the use of PROFINET , the Ethernet medium can also achieve soft real-time capability in addition to data consistency . There is a difference between the two protocols UDP/ IP and PROFINET-RT . A monitoring time and update time for the process data is specified for PROFINET-RT . The length of the process data is specified and cannot be changed during runtime. To make the Ethernet-based network more determinable
it is helpful to know and take into account the physical structure and possible changes to it. By using managed switches, an Ethernet-based bus protocol such as PROFINET can be preferred. Fluctuations in the transit time of data packets are further reduced and the transmission time

hold becomes more predictable. With these aids can be used in an Ethernet-based network
a determinism with predictable tolerances arise. Further steps like Mes
Calculation of transmission and processing times between the network participants
Time synchronization enable hard real-time requirements over an Ethernet-based Network.

2.6 Standards and Guidelines

In the study work, it turned out with the interpretation paper [10] from the Federal Ministry of Labor and Social Affairs (BMAS) on the subject of the totality of machines that the versatile assembly system does not form a totality of machines. precondition

is that there is no production-related and safety-related connection.
An exception is a higher-level evaluation unit for evaluating the emergency stop.
Furthermore, the system was considered as an integrated production system according to *DIN EN ISO 11161 .* [11] The machines suitable for integration were also considered machine modules in the TÜV Süd position paper. [12]
CE conformity can also be proven through direct compliance with the Machinery Directive. This applies not only to machines, but also to interchangeable equipment, which is defined as follows in Article 2b) of MRL 2006/42/EC:

> "[...]a device which the operator of a machine or tractor, after it has been put into service, attaches to it himself in order to change or extend its function, provided that this equipment is not a tool" [13, Article 2b)]

This description applies to the machines that are added to or removed from the smart transfer system. For this reason, a machine module can also be understood and treated as interchangeable equipment. "There is no requirement that interchangeable equipment meets the definition of machinery." [14] According to Article 2 of the MD, interchangeable equipment is machinery in a broader sense of the Directive. This is therefore to be regarded as a separate product. " Within the scope of the safety and health requirements according to Annex I of the Machinery Directive, the manufacturer must not only consider the equipment itself, but also its interaction with the basic machine." [14]

The interchangeable equipment is also intended to be operated individually. This results in another type of machine that must be evaluated again with the Machinery Directive or with harmonized standards. Due to the different possible uses, there are different functionalities and a diverse intended use. The safety and health requirements may change. This can result in a different conformity assessment procedure. The machines considered in this bachelor thesis, in the narrower and broader sense of the MD, do not represent compliance with the machines described in Annex IV. This is decisive for the following requirements (see 3.5).

3 requirements

In this chapter, the findings from Chapter 2 are formulated with measurable criteria for requirements. With the help of this, a concept is then developed and implemented in Chapter 4 . The concept to be created must meet the relevant requirements from the harmonized standards *ISO 12100, ISO 13849, ISO 13850 .* Depending on how it works, a machine module can be viewed differently . There are different descriptions of the intended use. Each mode of operation represents its own operating mode. For each machine module, there must be an automatic and a manual mode in each operating mode. A machine module is to be regarded as an independent machine, so it must also function individually without being integrated into a system and without increased risk. A separate operating mode must be provided for this. Furthermore, the machine can be operated on a compatible system (integration environment). The machine module is to be regarded as an integrable machine according to *ISO 11161* or as interchangeable equipment according to the MD.

One of the two viewing types is to be selected and another operating mode provided for this on the machine module.

3.1 Smart transfer system

In the section on the state of the art, it was already established that there are no additional protective measures on the transfer system, so these must be retrofitted with additional emergency stop switches on the conveyors of the transfer system. Emergency stop switches for the

install additional protection. In the study work was under Berück

After reviewing the current set of rules, it was determined that their activation results in the shutdown of the entire transfer system and all machine modules connected to it.

In *DIN EN ISO 13850 ,* no statement has been made about a response time. However, it can be seen that the emergency stop function must be available and functional at all times . In this bachelor thesis, a worst-case reaction time or guaranteed switch-off *time (tG)* of the SBT of less than 350 ms is specified as a measure of adequate availability .

In order to be able to build up expectations, the smart transfer system must be able to reliably recognize at all times how many machine modules have been placed in the intended places. This requirement is sufficient to fulfill the goals set in this bachelor thesis . For further security requirements, it may also be necessary to answer the other questions from Chapter 2.1. This is when capturing

of connected machines should be taken into account if possible. The information obtained about the number of integrated machines must be checked for plausibility using additional signals and inputs. Adding and removing machines must be a conscious act.

3.2 Robot assembly machine

The activation and deactivation of safety devices depends on the function and thus the selected operating mode. In order to make the selection of the operating mode plausible, safe sensors must be used to determine whether this module can actually be in individual operation. The addition to or removal from the transfer system must be consciously triggered by the machine operator. Another requirement for this machine module is that it can process the emergency stop signal from the smart transfer system in a safety-relevant manner. In the study work it was already determined that access to the protected area can be realized with a door switch based on the four-step model. [6, p. 37] Access in four stages is described in the standard *DIN EN ISO 14119:2014-03 .* The door switch must therefore have process and position monitoring. For this reason, the response time of the local safety controller is not important. The safety control must be at least PL d certified with a Category 3 or SIL 2 structure; further performance requirements are described in *DIN EN ISO 10218-2* in Section 5.2. [15, p. 17] The operating mode may only be selected by a specific group of people. The risk-reducing protective measures of the risk assessment, which are evaluated via a safety PLC , must be implemented. The safety interface X11 of the Kuka robot control is to be evaluated and controlled according to the selected operating mode .

It must be ensured that the robot arm cannot exceed the protected area in the event of an error. For the largest possible working space for the robot, the separating protective measure must be designed in such a way that it cannot be penetrated by the robot.

3.3 Engraving Machine

As with the robot assembly machine, the deactivation and activation of safety devices is related to the selected operating mode; Therefore, the selected operating mode must also be verified on this machine with additional safe sensors. Adding and removing from the transfer system must be a conscious act. The machine must be able to process the emergency stop signal from the smart transfer system.
The study work assumes a worst-case reaction time of the controller of 50 ms,

in order to be able to switch off the laser beam in good time in the event of an error. [6, p. 39] The risk-reducing protective measures of the risk assessment must be implemented, which must be evaluated by a safety PLC . This results in the individual requirements, such as ensuring that engraving can only take place if the extraction system is working properly. Further points can be the entrances to the machine or the laser cabin. Access must be monitored and suitable for the tasks at hand.

3.4 SafetyBridge Technology Requirements

“The SafetyBridge system makes no special demands on the standard controller.

However, it must be able to fulfill the following tasks:
Network:

- Deterministic network

Steering:

- Fast enough to meet response time expectations • Memory must be large enough to hold the configuration and parameter data set to be able to save
- Ensuring data consistency over 24 words." [7, A 2.2]

These requirements have been taken from the SafetyBridge manual and specified in more detail with the state of the art from chapter 2.5 on page 9. The maximum network structure of the versatile mounting system must be estimated and specified.
The adaptability of the mounting system must be taken into account. A monitoring time for safe cross-communication must be determined. In the case of the standard controllers already installed, it can be assumed that they can already meet the requirements. The islands of the SBT must be uniquely addressed. Island numbers are assigned via DIP switches. An addressing concept to be created should prevent several machine modules with the same island number being integrated .

3.5 Normative Requirements

The description of exchangeable equipment found in MRL 2006/42/EG under Article 2b) applies to a machine module, also known as an integrable machine. In the *interchangeable equipment* operating mode , a machine module is to be understood as a machine in the broader sense of the Machinery Directive. Therefore, the machine modules the relevant obligations of the Machinery Directive both in this operating mode and in individual operation

fulfill. In both cases, the basic health and safety requirements must be met. In the case of interchangeable equipment, not only the equipment itself must be considered, but also the interaction with the basic machine . In this bachelor thesis, the machine modules are considered as integratable machines according to *DIN EN ISO 11161 .* The risk-reducing measures of the previous risk assessment according to *DIN EN ISO 12100 must be* implemented. Within the framework of this bachelor thesis, the risk-reducing measures are mainly to be implemented in a control-related context. When designing the modular emergency stop, the harmonized standards *DIN EN ISO 13850* and *DIN EN ISO 11161* apply

fulfill. In this way, the conformity procedure can be simplified.

4 concept

In this chapter, a concept is created that meets the requirements of Chapter 3. The SafetyBridge technology (SBT) selected in the study work is taken into account. The focus of this concept lies in the control technology implementation of a safety concept for a modular system design, which is tested using the versatile assembly system of the SmartFactoryOWL.

4.1 Functionality of the safety devices

Assuming that the controllers start up without errors and are in the expected operating states, the start-up on the smart transfer system must first be acknowledged. After that, each machine has to be acknowledged individually and then the automated production process has to be started. A separate acknowledgment on the integrated machines prevents the automatic restart of the machine module.
If it can be ensured that there is no risk from an automatic restart, there is no need for a renewed acknowledgment. This must be taken into account accordingly in the standard implementation. The production starts with the last step, starting the belts from the transfer system. The main steps are shown as a program flow chart in Figure 2.

By selecting *Add machine ,* the plausibility links are changed and a machine can be brought into the integration environment without stopping production . A reasonable period of time is available for this process. The setup of the cross-communications is then automatically triggered and the change in the plausibility links is reset. A machine is logged off at the machine in question. The plausibility links are changed again for a fixed period of time . In the event of an error, the system goes into the associated safe state.

The emergency stop on the remaining machine modules that can be integrated remains active and is not bypassed. According to *DIN EN ISO 13850:2014-06* Section 4.3.7, activated emergency stop switches must be recognizable. This comes with an illuminated emergency stop button too consider.
The release for production, which can only be granted in proper operation, takes place in every machine. In integrated operation, a crucial condition is the presence of the emergency stop signal from the other machines. This signal is transmitted via the SafetyBridge's safety-related cross-communication. Errors are acknowledged on the affected machine module. The acknowledgment is requested when the acknowledgment button lights up. The acknowledgment button is pressed

distributed in a safety-related manner to the integrated machine modules via the integration environment . In this way, the absence of the external emergency stop signal can be acknowledged.

4.2 Structure of the hardware

Each machine module is adapted with a SafetyBridge Technology V3 logic module . The logic modules are hierarchically subordinated to the logic module by the transfer system. Binary signals are exchanged and processed between the safety-related logic modules using safety-related cross-communication.
The master logic for the transfer system is addressed as island 31. The logic modules of the machine modules are addressed in sequence from one to seven.
This addressing scheme should be continued when expanding the collection of compatible machines so that double addressing can be ruled out.

4.3 Cross Communication

After the time allotted for adding a machine has expired, the safety-related cross-communication between master and slaves is reactivated. The logic module integrated as a slave transmits a sign of life with the first bit of cross communication, also known as a live bit. The integrated machine also receives such a live bit from the master via the first bit. The state of the emergency stop is passed on and received with the second bit . This applies to the machine modules and the transfer system. Through an evaluation in the higher-level logic, the status of the emergency stop is evaluated by all machines and returned to them.

Since this is a certified transmission, no additional bit is needed for verification. In the event of an error, this drops out and the machines go into a safe state. The third bit transmits the log-off signal of the respective machine module.
This changes the plausibility links on the master for a certain period of time. This allows a machine to be removed without having to stop all production on the system. If the emergency stop is actuated on another machine , the system is nevertheless placed in a safe state. By changing the plausibility links, not all emergency stop signals will be ignored.

Interruption of the cross communication

The availability of the cross communication is continuously monitored within the SBT and must not exceed the configured safety time (F watchdog time). If this is exceeded, all transmitted signals of the cross communication are switched off.

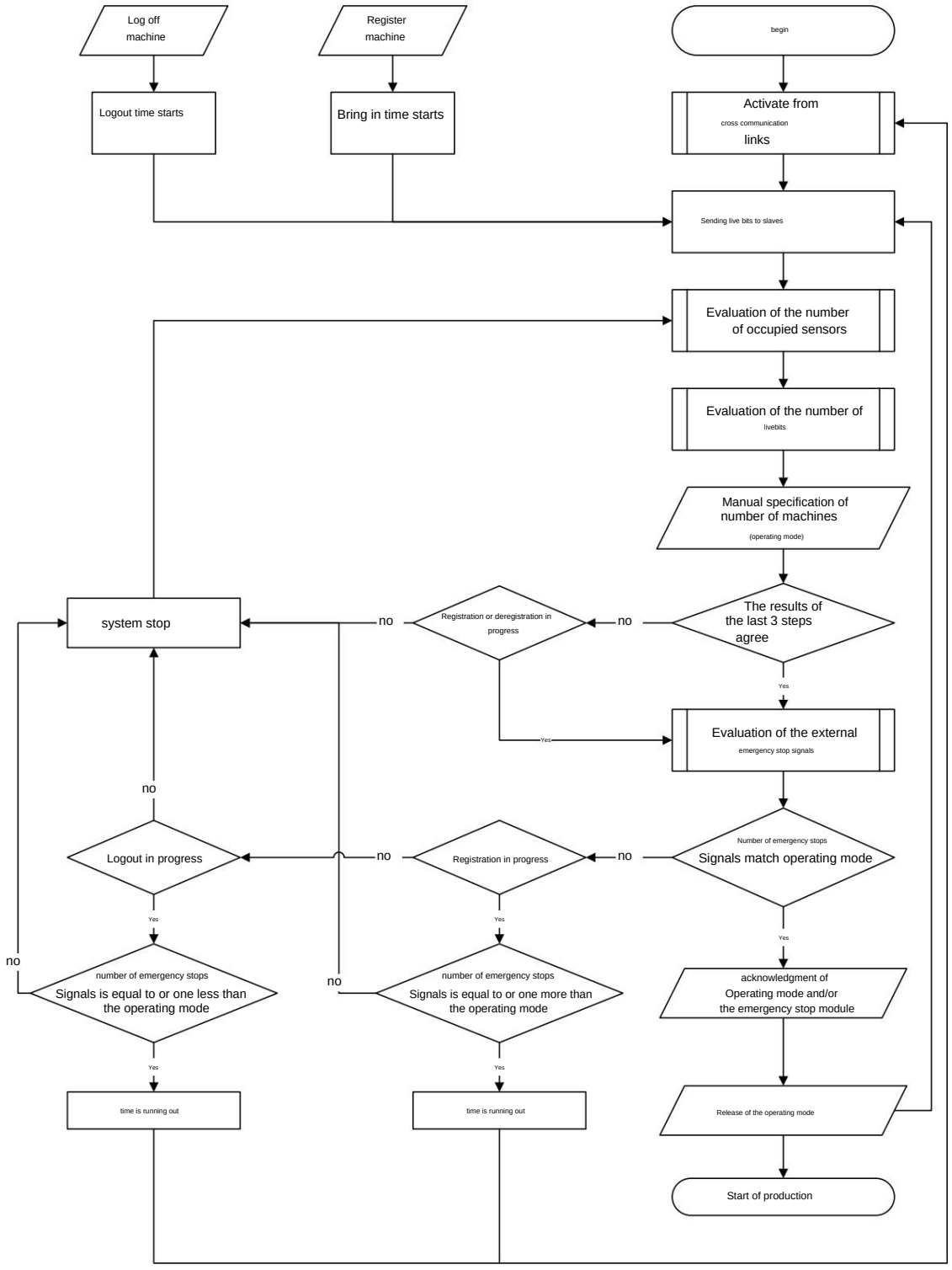


Figure 2: Program flow chart of the safety controller in the transfer system (master)

The emergency stop signal and live bit drop out and a communication error can be evaluated between the two machines. The connection can be reestablished through a conscious action on the transfer system. Since the emergency stop signal drops out, the procedure after activating the connection is the same as when pressing an emergency stop switch.

4.4 Plausibility check

With the help of safe magnetic sensors in the locks at the integration places, the higher-level logic module of the transfer system evaluates how many places are occupied. To check, the number of connected machines is determined based on the evaluation of the live bits. If these two determined numbers match the number specified by the machine operator, this can be assumed to be plausible and the selected operating mode can be activated.
The number of connected machines has now been determined three times. In this way, a plausible expectation can be established, which can be used to decide how many emergency stop signals are to be received from the integrated machine modules. These are exchanged via the cross communication of the SBT. If the number of emergency stop signals does not match what is expected, the emergency stop signal to the slaves is switched off and the machine modules go into the stored safe state. While a machine is being logged on or off, the plausibility check is carried out by an internal signal

changed for a period of time. The number of live bits and emergency stop may vary

Only change signals by one signal, otherwise the entire assembly system will be put in a safe state. If the determined numbers do not match, the system cannot be put into operation. The establishment of the connection is triggered again by pressing and holding the acknowledgment button on the transfer system.

A further plausibility check is carried out in each machine module. As already mentioned, the machine module receives a live bit from the higher-level logic module.
A secure magnetic sensor on the machine module is used to query whether the machine is connected to another. The evaluation of the magnetic sensor and live bit takes place in the logic module of the respective machine module. The appropriate operating mode can be selected using a key switch. If the three signals live bit, sensor and operating mode match, manual or automated operation can be started in the selected operating mode .

4.5 Other Features

Behavior of the emergency stop

The activation of an emergency stop is processed by the SafetyBridge island of the respective machine with the result that the machine is immediately and safely stopped. As a result, the second bit of the cross communication falls. The evaluation in the master controller detects the absence and triggers a safe standstill on the connected machines by removing the second bit of the cross-communication. After the error has been corrected, the error is also acknowledged on the triggering machine. If the correct operating mode is still selected, the production release can be regained by pressing the acknowledgment button several times. This is passed on to the connected machine modules using cross communication via the transfer system. Thus, an automatic restart is conceivable from a control point of view. This could possibly result in hazards. If there is a machine module on the transfer system that is not in the associated operating mode, a

emergency stop.

triggering of safety devices

The triggering of safety devices, such as when a protected area is violated, does not stop the entire system. Only the affected machine is stopped. This behavior is to be seen in connection with the upstream and downstream processes. The processes are partially decoupled on the versatile assembly system, since up to 10 kg can be accumulated on an assembly from the transfer system. Another possibility is that if the machine stops locally and the machine is therefore not available, the product carriers are transported past it. This is a function that cannot be performed in a safety-related manner, but must be considered in the safety concept. For this behavior, the standard controller evaluates and further processes the status of the local safety controller accordingly. If the automated production process stops at a single machine module, the same situation arises as described above and must be resolved accordingly.

4.6 Test setup

A test setup must be set up to familiarize yourself with how the SBT works. This is intended to simulate the smart transfer system and two machine modules. In addition

controls can be mounted on a mounting grid as follows. An RFC 470 PN is already installed in the transfer system of the mounting system and can also be used on the mounting grid . Two Inline stations are to be created with two PROFINET bus couplers. One represents an emergency stop on a module from the transfer belt and consists of a safe input module with eight inputs. The other is later installed in the control cabinet and consists of a SafetyBridge logic module and two safe input modules. The design of the two machine modules to be simulated is identical in terms of control technology on the test setup and each consists of an ILC 330 PN PLC, a logic module and two safe input modules, each with eight inputs. For operation, control bottles are to be mounted on the test setup using plug connections.

The power supply for the controls is provided via this plug connection. In this way , removing or attaching the control bottle can simulate removing or adding machine modules. The versatile assembly system can be visualized with the help of a process simulation circuit board. In addition to three LEDs for the status of the associated machine, DIP switches must also be provided, with which various sensors can be simulated. The test setup was planned using an EPLAN engineering tool by creating the associated circuit diagram for the wiring and the layout plan for the assembly. Figure 3 shows a photo of the test setup.

Figure 3: right: transfer system; top left: machine module 1; bottom left: machine module 2

5 implementation

This chapter describes the implementation of the concept from chapter 4. Challenges that arose when creating safety functions are also addressed. The safety functions were implemented using the free and associated SAFECONF programming environment. As already described in Chapter 2.4 , the SafetyBridge technology (SBT) has been integrated into the Phoenix Contact controllers using the *SBT_V3_V1_00* library.

5.1 SafetyBridge in a PC WORX project

The library *SBT_V3_V1_00* was downloaded from the Phoenix Contact homepage , opened with PC-Work and compiled. In the next step, the PC-WORX projects were expanded to include the functions of the SBT. The central Operate block has been taken from the SafetyBridge library mentioned above. For this and for all other blocks from the library, variables with the documented Da

created. The name was chosen to be the same as the input or output designations of the function block, supplemented with an index of the island number. After activating this block, the status can be evaluated by the logic module. A few special features that must be taken into account when creating the variables are discussed below. The specification of the island number should not change at runtime and has been created as a constant. All blocks of the SafetyBridge library are integrated into an exchange structure.

The variables *arrSBTOnlCntrlBuf* and *arrSBTOnlValBuf* at the inputs and outputs of the Operate block must be created globally and written to the process data directory (PDD). This is done when creating the variable by selecting the appropriate option. This means that the online values of the safety controller can later be displayed in SafeProg. The output *arr_wSBTdiagCode* can be evaluated with the library *block SBT_V3_DiagCode_V1_00 .* This means that the status of each individual SafetyBridge satellite can be read out. If a satellite requires an acknowledgment, this is done via the library *block SBT_V3_arrAckBuff_V1_00,* which is connected to the *arrAckBuff input* of the Operate block. There is also an operator acknowledgment with which certain hardware errors, such as a communication error in the cross connection, can be acknowledged. The 32 non-secure bits are exchanged in each double word. For better handling , it is advantageous to create a function block that splits the respective double word into individual bits or combines the 32 bits into a double word. Is in the

If the approval is activated for safe parameterization of the SafetyBridge output, this can be supplied via the *arr_wOutData input* of the Operate block. This variable is an array of data type word with 17 entries. A word is assigned to each possible satellite . In the applicable word, the appropriate bit for the one output from the one particular satellite must be set. For simplification, appropriate function blocks must be created that write the required bit to the appropriate position.
The direct consent via the hardware can lead to errors if the output controls a safety relay and the correct functioning is monitored by this.

The output of the module for relay monitoring is set and expects the control signal for monitoring according to the set tolerance time. This does not happen because the output was not set in the peripherals/hardware if there was no consent.

5.2 Structure of the cross communication

To set up cross communication, the CrossComm block uses an array of
Exchange structures created. This block has the maximum number of

Specify SafetyBridge islands. The number is important when multiple islands are managed by one controller. An element of the array must be assigned to each logic module on its associated Operate module. The safety-related cross-communication between the logic modules that are operated by a controller is established.
The versatile assembly system consists of individual complete machines. For this reason, each logic module is linked to a different Inline controller from Phoenix Contact . The cross communication that has already been created is not sufficient for this and the project of the standard controller must be expanded with the *DataExch* library module .
An instance is to be inserted in the master control for each island and to be hung in the same exchange structure as the operate block of the master logic module.
The DataExch block outputs the data to be sent and provides an input for the received data. The data exchange between the controls had to be created, this was taken from a sample project from Phoenix Contact.
In the test setup, it was noticeable that the secure cross-communication was repeatedly interrupted. As a result, the application for sending and receiving via the IP blocks was improved as follows. The standard controller, on which a SafetyBridge logic module is operated as a slave, always sends the exchange structure of the cross communication after it has been received. This prevents the two tasks involved, which are executed on different controllers, from diverging and therefore resulting in longer transmission times than the monitoring time set in the safety application. Unfortunately, this approach led

not to the desired success; Phoenix Contact Support was contacted. This behavior is evaluated in Chapter 6.3.
Another option is to integrate the standard PLC as a device in the PROFINET bus from the transfer system and to pass on the data from the DataExch module via the process data . A function block was then created that writes and reads out the SafetyBridge data at a defined point in the PROFINET process data. For comparison, the communication between the controllers was set up via the PROFINET bus and via UDP/IP. Finally, pay attention to the following special feature of the DataExch block:

No island number needs to be specified on the instance of the DataExch block that is intended for a slave logic module. The SafetyBridge exchange structure must be an element of the array that has not yet been used and not the element that is specified on the Operate block or other blocks. It should be clarified again that the DataExch instance working on the master controller must have the same element of the exchange structure as the associated Operate block of the Master SafetyBridge island.

5.3 Plausibility check

As explained in chapter 4.3, the master safety logic module sends a TRUE directly to all slaves via the first bit of the cross communication. Conversely, a slave always outputs a TRUE signal via the first bit. These binary signals can be used to evaluate how many controllers are on the transfer system.
The only operation for sending or receiving successfully is the correct operation of the SafetyBridge logic modules including the cross communication. For this reason , this signal is called the live bit. If no emergency stop is actuated, a TRUE signal is exchanged in the same way. The evaluation in the master recognizes the absence of an emergency signal and sets the emergency signal for all subordinate safety controls to a FALSE signal. The binary emergency stop signals are evaluated with a gate made up of AND, OR and NOT functions. Each application can be understood as a Boolean algebra. Evaluating a signal out of seven possible ones is given in Eq. 2 shown. For further illustration, the evaluation of two out of seven possible signals in Eq. 3 shown. Each term of the OR gate represents its own small logic gate. The magnetic sensors in the locks at the integration stations of the transfer system are actuated when a machine is approached and are routed to inputs of the safety control. The live bits, the emergency stop signals and the magnetic sensors are evaluated with the gates that have been created using Boolean algebra. With the available safe building blocks

no such counting function can be created. Initially, only three machines and thus possible signals were assumed for testing. For example, Figure 4 shows a gate that outputs a TRUE signal when exactly one of the three possible signals is present.

In the safety control of the machine modules, the evaluation is much easier. If the machine module is integrated in the integration environment, the magnetic sensor is actuated. This is evaluated by the safety controller of the machine module. The operating mode selector switch is linked to the signal from the magnetic sensor and the live bit and routed to the module for operating mode selection. If all three signals (operations) do not occur, individual operation is selected. Otherwise it is an error case that is tolerated for the duration of adding machine modules to the integration environment. The emergency stop switches and the external emergency stop signal are monitored via the associated blocks. The protective devices on the respective machine module are routed to the SafetyBridge module of the respective machine and are monitored by it using the corresponding modules. If there is no error, the production release is approved and passed on to other controls via a safety relay, such as the laser controller or the Kuka control.

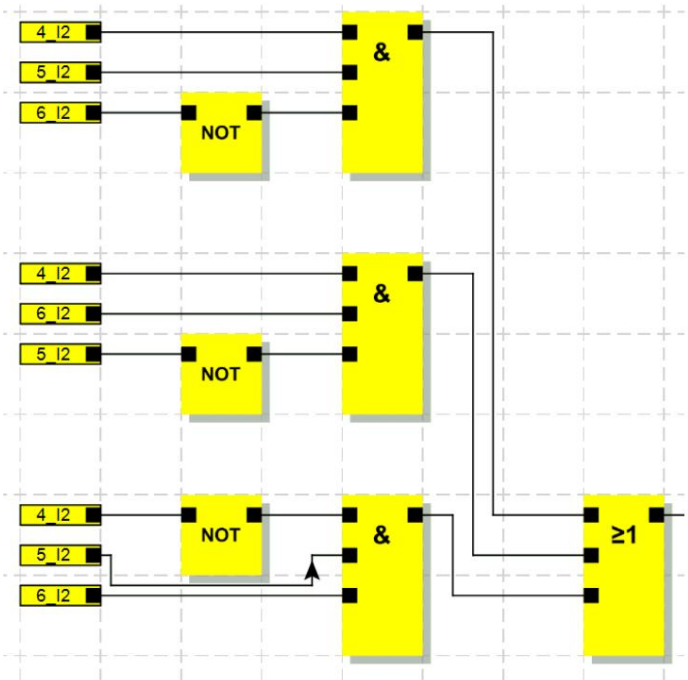


Figure 4: Gate to evaluate exactly one of three possible signals

$$Q1 = ABCDEF\,G + ABCDEF\,G + ABCDEF\,G + \ldots \quad (2)$$

$$Q2 = ABC\,D\,E\,F\,G + ABC\,D\,E\,F\,G + AB\,CD\,E\,F\,G + AB\,C\,DE\,F\,G + AB\,C\,D\,EF\,G + AB\,C\,DE\,F\,G + A\,BCD\,E\,F\,G + A\,BC\,DE\,F\,G + A\,BC\,D\,EF\,G + A\,BC\,D\,E\,FG + A\,B\,CDE\,F\,G + A\,B\,CD\,EF\,G + A\,B\,CD\,E\,FG + A\,B\,C\,DEF\,G + A\,B\,C\,DEF\,G + A\,B\,C\,D\,EFG \quad (3)$$

Further processing of the information obtained

The following description of the implementation refers to the SafetyBridge logic module on the transfer system, the master for all connected machine modules. First, the number of machine modules used is determined. The number of connected machines is specified by the operator via an operating mode selector switch. This is led to safe inputs and forwards the number of safe inputs. After the signal has been evaluated, the specified number is linked to the determined number of actuated magnetic sensors and routed to the module for operating mode selection. Initially, only four different presets are possible. In the next steps we will use the created gates to count the number of live bits and emergency stop

signals detected. After the number of emergency stop signals has been determined, they are checked for plausibility with the selected operating mode. If the information matches, the *emergency stop signals ok* connector becomes true. Finally, if no emergency stop is actuated on the transfer system itself, the second bits of the cross-communications are set. The evaluation of the emergency stop signals has been expanded with additional plausibility checks for logging on and off machine modules, see Figure 2.
Finally, all the information obtained is summarized. If these match, the release is set. If the numbers of live bits, activated magnetic sensors and the operator specification match, these are plausible states.
If this is not the case, the release can be retained by setting a sign-on or sign-off signal. If an error is detected in the emergency stop circuit, it will still come to a standstill. The information is further evaluated for diagnosis so that an error in the cross-communication can be diagnosed. In the event of an error, the integration environment and the machine modules connected to it are placed in a safe state and multiple acknowledgments are required after the error has been rectified.

5.4 Installation in the mounting system

Many challenges arose during installation in the mounting system. The decisive factor was that the transfer system and the existing machine modules were not expanded to the declared degree of automation. The following points had to be improved first. The special features of the creation of safety functions that stood out in the machine modules are then discussed.

- The transfer belt assemblies had to be adapted so that the downsized integration environment could be expanded again.
- Due to design reasons, the robot assembly module was no longer able to assemble Lego figures as intended. The control functions had to be adjusted to make the robot compatible with the integration environment again. The robot had to be trained for the new functions. These had to be made known as assembly steps in the integration environment and written on the RFID tag for a product as required construction plan steps
  will.
- The blueprint steps were not, as explained, after completion on the RFID
  Day noted accordingly, but generally marked as done. As a result, after the manual workstation, the products were completely finished according to the information on the RFID tag, the product memory.
- Adjustments to the control projects were only possible with additional effort, since the current project files could not be found.

robot assembly machine

There is a block in SAFECONF for the required access monitoring. In addition to two-channel feedback from the process guard locking, this expects position monitoring. The required position monitoring could not be reliably determined with the intended product ; a new one was appointed. In addition, the block requires reliable information that the protected process is not currently causing any danger . In this application, a secure signal is required that states that
the robot stands securely and the restart is prevented. This one won't have that
hardware interface output. The following solution was found. Access is requested by the machine operator. After the program has finished, the robot is stopped by the standard controller. Then the request of the operator in the

Security control approved. After a safety time has elapsed, standstill monitoring of the robot is activated via a safety relay via the safety interface of the Kuka controller . This relay is monitored by the safety controller.

The switching of the relay is evaluated as a safe shutdown of the process, since the monitoring is directed to the block for access monitoring. Access to the protected area is possible without errors.

6 evaluation

In this chapter, the requirements from Chapter 3 are compared and evaluated with the results of the implemented concept from Chapter 4. The bachelor thesis is completed with the outlook, which gives starting points for future improvements.

6.1 Implementation of the concept

The required range of functions could be implemented with restrictions. The conceptual functionality when adding and removing machines could be achieved and fulfilled. To determine the number of signals, many AND and OR functions had to be combined to form logic gates. Dimensioning these gates for seven possible machines in the future turned out to be more time-consuming than previously assumed.

The graphic implementation option can be operated intuitively and the sensors could be evaluated quickly with existing modules. As the configuration of the functions progressed, they increasingly lost clarity; an implementation in a high-level language was not available. The gates could not be combined as functions or function blocks. It was therefore not possible to improve the clarity of the program. The subdivision into so-called *networks* could not significantly improve this. The safe memory of the SafetyBridge logic is 30 kbytes and is not sufficient for a project of the required size with seven possible machine modules. So that there is a conscious action when adding and removing machine modules, the machine operator specifies the number of machine modules inserted via a toggle switch. Only one toggle switch with eight switch positions could be found, four of which actuate one switching element each. The switch position is evaluated via the safe module for operating mode selection. The block is designed for up to five different operating modes, so that zero to four machines can be switched on or evaluated by the block.

The selection of toggle switches with more switch positions that can be evaluated is limited. The switch position is often announced via a binary or BCD code and must be evaluated accordingly. Another solution had to be found for the requirement of being able to integrate seven possible machines at the same time.
A possible solution would be to default to a restricted selection of a Human Machine Interface (HMI) panel. After changing the number of integrated machines, an acknowledgment must be made. This ensures that changing the number of integrated machine modules results in a conscious action.

In summary, the following reasons can be established that prevent seven possible machine modules from being taken into account.

- Restricted user specification: a maximum of three integrated machines can be specified.
- Complex to create logic links for the evaluation.
- SAFECONF project exceeds the memory of the logic module.
- A maximum of three possible machine modules could be in the SAFECONF project be taken into account.

For these reasons, the number of possible machine modules was limited to three when implementing the safety concept.
According to the *ISO 13849-2* standard, the measures required in the risk assessment must be validated in a documented manner. This has happened in part with this bachelor thesis, since measures from the risk assessment have been incorporated into the requirements in Chapter 3 . The result of the implementation is recorded in Chapter 6.4. With the subsequent cross communication, it was possible to create a modular emergency stop function networked via Ethernet.

6.2 Detection of safe sensors in the field

The SBT does not offer the option of evaluating or bundling sensors directly in the field and transferring them to the control cabinet in a safety-related manner. Parallel wiring through the transfer system to the control cabinet is necessary. In addition to the increased effort involved in adapting the entire connector system of the transfer system, this approach is also no longer up to date. For faster and preliminary implementation, PROFINET bus couplers from Phoenix Contact for the Inline system were attached to the transfer belts with safety-relevant sensors. A SafetyBridge satellite with eight safe inputs was added to each bus coupler, which is evaluated by the island 31 logic module in the control cabinet of the transfer system. With this solution, the sensors could be safely evaluated in the field and safely transmitted via Ethernet for further processing. The disadvantage of this solution is that the bus couplers and the inline modules are not intended for installation in the field. An installation in a housing that is mounted on a transfer belt assembly would be a possible solution. For this reason, this is a temporary solution.

6.3 Cross Communication

The SBT-V3 supports safety-related communication between logic modules. Communication can be carried out using various Ethernet-based protocols and bus technologies . In the test setup, a network connection was first set up between the standard controllers via the Internet Protocol (IP) and the SafetyBridge exchange structure was exchanged via UDP. Cross communication between the safety controllers was successfully established. A high availability of the system could not be achieved initially. The availability could be increased through application-related improvements in the PC-WORX projects of the two controllers, but the result was not yet satisfactory. As can be seen in figure 5, peaks in transmission time occur again and again. These exceed the configured monitoring time and the safety-related connection is terminated.

As a result, a safe stop is initiated on the transfer system and on all connected machine modules. This is associated with a production stop. The simultaneous absence of a live bit and the external emergency stop signal can be diagnosed as a communication error in the configuration of the master.

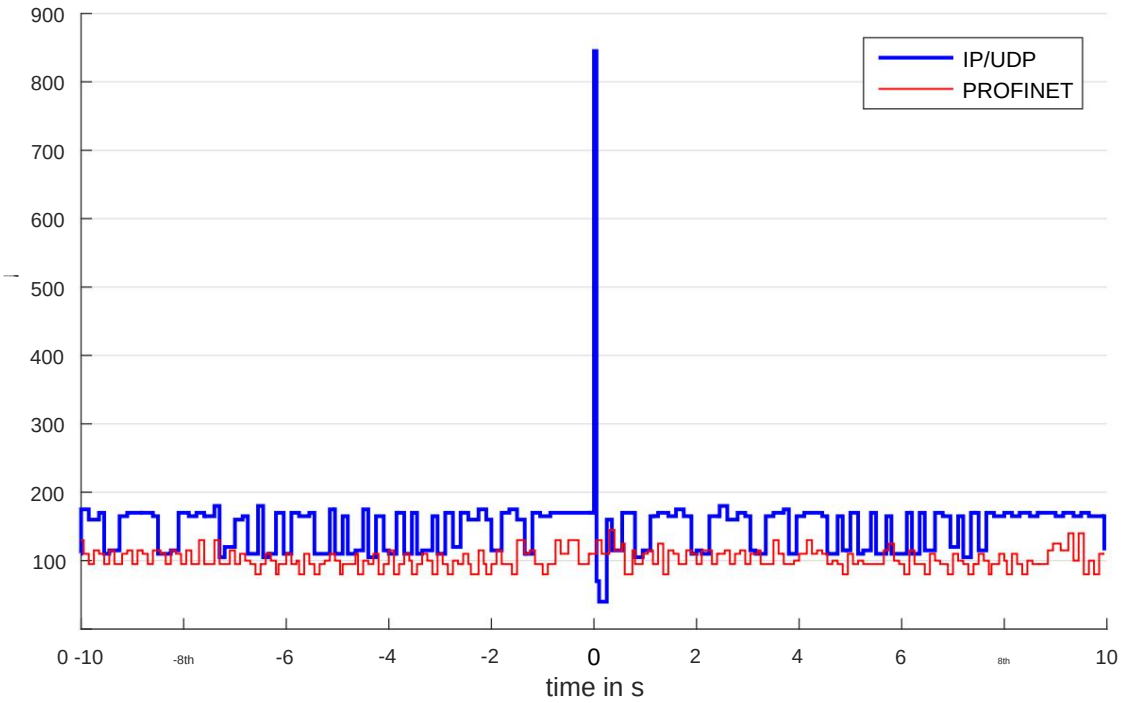


Figure 5: Course of the transmission time between two SafetyBridge logic modules

Some of the differences between UDP/IP and PROFINET have already been explained in Chapter 2.5. These differences can already be an explanation for the randomly occurring peaks in the UDP/IP transmission. If the safety bridge cross communication is exchanged via the PROFINET process data, there are no noticeable peaks in the transmission time, see Figure 5. It can also be seen that the transmission time is shorter via PROFINET and, in contrast to UDP/IP, there are fewer differences in the difference of transmission time. Thus, the transmission behavior can be understood as more deterministic and better meets the requirements of the SBT. The availability and transmission time could be further improved with this measure.

A possible explanation for the occurrence of the peaks can be found in the performance of the controls used. The established communication connections must be processed by the controllers. This is organized by the operating system of the controller. The data is written from a communication interface to a memory (stack). This is processed by the operating system with different priorities. Only the manufacturer knows exactly how the ProConOS operating system works . He was contacted for troubleshooting and was able to confirm the findings described above, but not in the processing period of the

Solve bachelor thesis.

These findings were transferred to the versatile assembly system and the controllers of the possible machine modules were integrated as devices in the PROFINET structure of the integration environment. This measure restricts the requirement to be able to introduce a machine module with compatible interfaces without further adjustments to the integration environment. During commissioning, it turned out that the monitoring times between the island and the satellites and to the slave islands that were parameterized in the test setup could not be achieved.

The following findings could be determined during the analysis of the possible causes.

- The maximum update time of the PROFINET process data is 16 ms.
- Significantly more network components and participants than in the test setup.
- Large runtime differences from 1 ms to 1500 ms when sending ping commands.
- Occasional bus coupler failures due to bus errors. The maximum permissible process data update time is 192 ms. After that, the lack of current process data is evaluated as a bus error.

Based on these findings, the responsible persons of the production network Consultation held on how to minimize the differences in transmission time

be able. The findings could be confirmed, but a timely solution could not be found. The above findings are not related to the transmission of functional safety data, so an error in the application of the SBT can be ruled out. In addition, the SBT was successfully put into operation in the test setup. It is obvious that the production network does not fulfill the required properties such as determinism. As a result, the availability of the versatile assembly system decreases. The fact that the standardized components of the production network must meet the requirements of functional safety is due to the black channel principle, see Chapter 2.4.3. A more in-depth analysis of the production network to meet the requirements is not part of the functional safety and thus exceeds the scope of this bachelor thesis. A production network with the required properties is assumed to be fundamental.

According to the Machinery Directive (MRL), the emergency stop considered here is an additional safety device that was designed according to *DIN EN ISO 13850 .*

The required guaranteed switch -off *time tG* of 350 ms could not be achieved for the versatile assembly system. In order to achieve adequate availability , the configured monitoring times between the logic modules had to be adjusted to 400 ms and the satellites in the field of the transfer system to 200 ms. The monitoring times for the satellites that are installed on the same Inline station as the associated logic module were parameterized individually. This adjustment can be made because *DIN EN ISO 13850* does not specify a switch-off time and the process does not require a time-critical, cross-machine switch-off.

Analysis of transmission times

The course of the transmission times was recorded using the TransTime block from the SBT library. This enabled a transmission time to be set that leads to an improvement in availability. Figure 6 shows an excerpt from a continuous recording of the transmission times between the safety controller of the transfer system and the associated satellites. The following conclusions can be drawn from the course of the transmission times: Satellites one and ten are installed side by side in an inline station. in the

SAFECONF project, on the other hand, these are not configured next to each other, but as satellites in positions one and ten. There is a similar trend over time in Fig. 6

with a certain offset in the transmission time. A reason for this behavior can possibly be found in the internal functioning of the SBT or the associated library blocks in the PC WORX project.

Satellites two, three and four, each with a bus coupler, are distributed on transfer band assemblies. In comparison to the other curves, a more frequent change in the transmission time can be observed. Individual peaks in the transmission time can also be observed, which do not exceed 150 ms in this section. With a parameterization of the F watchdog time of 150 ms, however, it was found that the availability of the system was reduced. Reasons for the peaks in the transmission time can be a fluctuating network load. A parallel recording of all network traffic could provide a more accurate explanation. This evaluation of the standardized network components exceeds the scope of this bachelor thesis, see above. A basic requirement for the SBT was a deterministic network. The occurrence of the spikes shows that this requirement is not sufficiently met.

The transmission time of the cross communication between two logic modules on different controllers is significantly higher. Seen per unit of time, this does not change that frequently. The difference in transmission times has the highest magnitude. The topology of the transfer system, which has a line topology of switches, should be mentioned again at this point for evaluation purposes. The machine module with the robot is integrated into the transfer belt assembly with satellite four. Both branch off from the last switch in the line topology. For this reason, the difference in transmission speeds between the island of the machine module in slave mode and satellite four cannot be explained solely in the network. A reason can be found in the different realization of the data exchange. The satellite on the bus coupler is integrated with the process data assignment via a variable that is made available by a library block of the SBT . For the slave island , the SBT exchange structure is extracted using the DataExch function block. This Exchange structure is then written to the PROFINET process data, which comprises 32 bytes. Reverse processing is performed on the slave island side.
This background can explain the increased transmission time compared to satellite.

Finally, it should be noted that on the Inline stations that were set up with an ILC controller , the internal transmission speed could only be set to 500 kbaud because of an already installed module . Comparisons with the test setup have shown that the transmission time can be improved by around 20 ms if the internal transmission speed of the Inline station can be configured to 2 Mbaud .

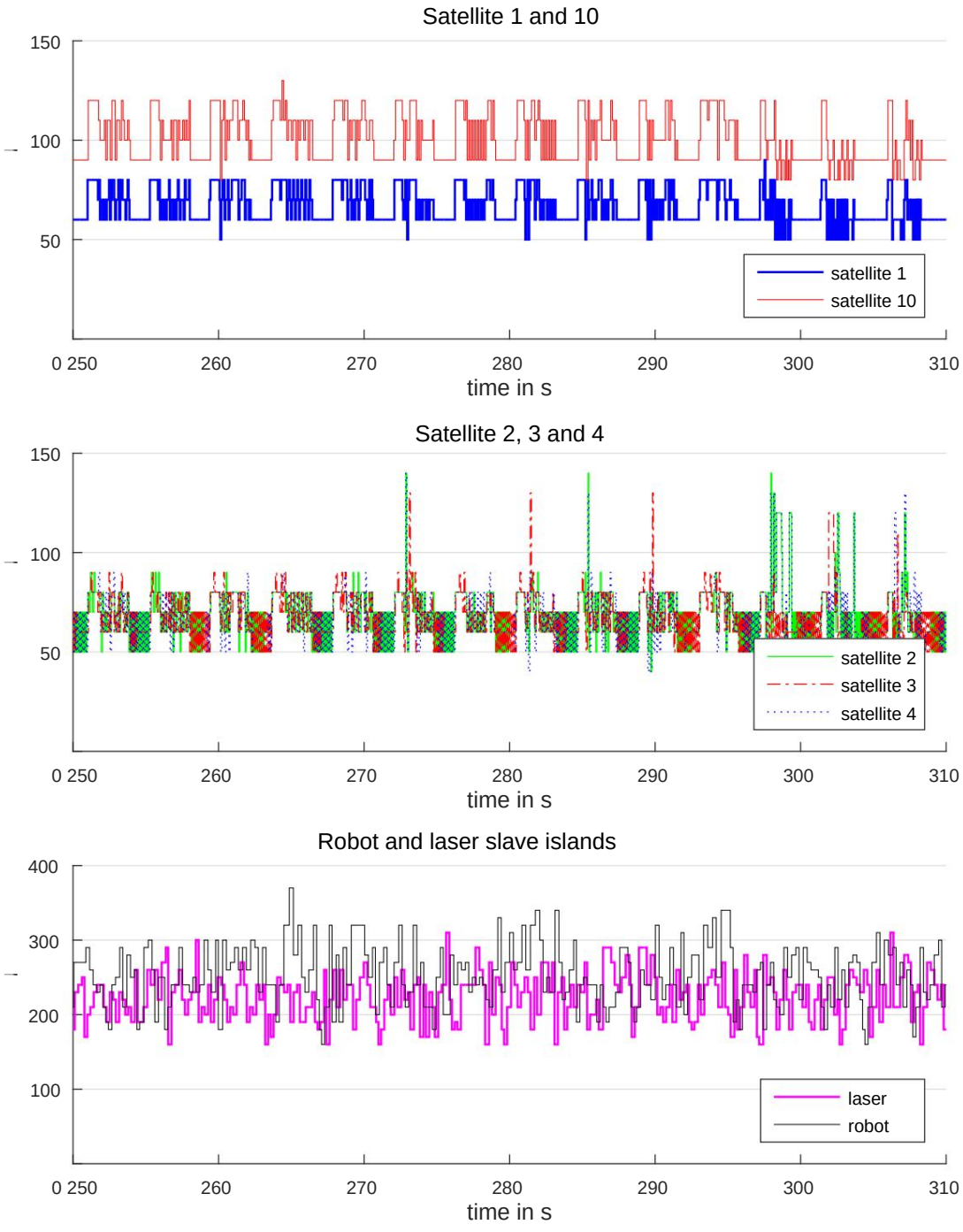


Figure 6: Excerpt from a continuous recording of the transmission time between the SafetyBridge logic modules

6.4 Safety functions of the machine modules

In this section, the individual control functions of the machine modules are checked. To determine compliance, these are checked against the requirements from the risk assessments. In the following , the functions that could not be fulfilled are discussed in particular. As a result, a new risk assessment or a further iteration step of the assessment is necessary.

6.4.1 Smart transfer system

The control of the smart transfer system was successfully expanded to include the SafetyBridge hardware . Due to the existing automation components and their wiring/ structure, some actuators cannot be switched off in a safety-related manner, or switching them off is not a practicable solution. The most important point is stopping the transfer belts. Their control is explained in more detail for a better understanding . Each transfer belt assembly has a frequency converter that is controlled via Profibus. For this reason, the release or controlled stopping of the conveyor belt cannot be carried out in a safety-related manner. Stopping via the standardized control is possible in the event of an emergency stop, but is not sufficient. Another measure for safe shutdown would be the safety-related shutdown of the power supply. This means switching off the energy distribution of the entire smart transfer system and consequently of the integrated machine modules. This switch-off is not practicable, as it means a generator failure for the machine modules and thus a time-consuming restart.

The compressed air was switched off in a safety-related manner. Switching off the compressed air must be taken into account in the safety concepts of the machine modules that can be integrated, so that there is no risk, for example, of tools being released.

Determination of the guaranteed switch-off time

Finally, the guaranteed switch-off *time (tG)* for a machine- spanning emergency stop that is processed by the transfer system should be determined. The guaranteed switch-off time for the safety function is made up of the longest processing time of the safe inputs involved in the safety function and the switch-off time of the safe output involved (single or two-channel). [7, A 9.2] As in Eq. (5) , the guaranteed switch-off time is made up of many factors, which are briefly described below. Starting with the processing time of the input *(tIN),* which

according to Eq. (4) consists of a parameterized filter time *(tF ilter)* and a constant firmware runtime *(tFW),* the associated satellite must transmit this information to the island. For this transfer, an F watchdog time *(tFW D_IN)* was parameterized in the SAFECONF project, which may be used as a maximum. Otherwise the SafetyBridge system goes into a safe state. The associated satellites are evaluated by the logic module of machine module 2. 15 ms *(tOUT_LP SDO2)* are constantly required for this. With the help of cross communication, the emergency stop signal is passed on to the higher-level island 31, to the transfer system. An additional F watchdog time *(tFW D_SL2) was* specified for this transmission . The island 31 in the transfer system requires a maximum of the time *(tOUT_LP* SDO31) for further processing. At this point, the emergency stop is triggered both on the transfer system itself and on the integrated machine modules. This is done again with the help of cross communication and requires the parameterized F watchdog time *(tFW D_SL3) to island 3 at most.* Island 3 in the robot assembly cell requires the maximum time *(tOUT_LP SDO3)* for further processing. Similar to the processing of the input signal, there is also a parameterized F watchdog time *(tFW D_OUT)* for transmission to the satellite and a switch-off time for the output *(tOUT) .* If the exits from the island are used, these two times are omitted and are

therefore to be taken as zero.

This time must be supplemented by the worst-case reaction times of the sensors *(tS)* and actuators *(tA)* and the *stopping time (tST OP)* of the machine in order to obtain the total maximum required switch-off time of the safety *function (tSF).* The requirement for the maximum switch-off time is met if it is less than the required one. For an emergency stop signal, no absolute time is required by standards. 350 ms is required here as an acceptable guaranteed switch-off time. According to the result of Eq. (5) are not complied with.

$$tIN = tF\ ilter + tFW \tag{4}$$

$$\text{tin} = 3ms + 0.25\text{ms}$$

$$\text{tin} = 3.25ms$$

$$tG = tIN + tFW\ D\_IN + tOUT\_LP\ SDO2 + tFW\ D\_SL2 + tOUT\_LP\ SDO31 + tFW\ D\_SL3 + tOUT\_LP\ SDO3 + tFW\ D\_OUT + tOUT \tag{5}$$

$$tG = (3,25 + 150 + 15 + 400 + 15 + 400 + 15 + 0 + 0)\ \text{ms}$$

$$tG = 998.25ms\ \_$$

6.4.2 Robot assembly machine

The required operating modes were successfully installed on the robot assembly machine. The Kuka controller is influenced in a safety-related manner via the hardware interface X11, since safety-related data cannot be exchanged between PROFIsafe and the SBT.

When restoring the compatibility between the smart transfer system and this machine module, it turned out that this machine module can no longer be used in connection with the intended material store. For this reason , the separating protective device for the protected area of the robot must be redesigned.
During the risk assessment in advance, access to the protected area was already determined to be unsuitable for all tasks. This should be changed by a door with process guard locking. Adjusting the access constructively is not part of this bachelor thesis. Access in four levels has already been taken into account in the configuration of the safety functions, see Chapter 5.4. With the help of the solution created there and a safety switch with position and process monitoring, safe access can be made possible after the installation of a door.

The robot's tool sucks in the workpiece using negative pressure, which is generated with compressed air. In the event of an error, the compressed air is switched off and the workpiece falls down. With the intended products, this does not result in any further danger to people, machines or the environment.

6.4.3 Engraving machine

The required operating modes were successfully installed on the engraving machine. However , the safety-related monitoring of the suction was not successful. It could not be ensured that laser processing is only possible with proper operation of the extraction system. This is due to the lack of safe feedback contacts for the suction .

When checking the safety functions, it became apparent that the laser controller was not working as expected. A safety switch detects that the processing area has been closed by a workpiece carrier. Only then is it permissible to open the shutter. Instead of opening, however, an error message appeared that the laser diode was consuming too much current. This message is not comprehensible because the diode was not switched off, but the shutter should be opened again. The manufacturer was contacted and says there is a known problem that could perhaps be fixed with an update. So that the machi

ne can continue to be operated, the previous status has been restored. The shutter remains impermissibly, regardless of the closed processing area, ge
opens.

Determination of the maximum required switch-off time *(tSF)*

In this section, the maximum required switch-off time *(tSF)* is determined, which is required to detect the error until the shutter closes. The laser processing cabin must be closed during the engraving process with a laser beam through the slide. A magnetic safety switch is installed to check whether the lifted specimen slide closes the cabin correctly. The associated actuator is attached to the slide. This switch requires a maximum response time *(tS)* of 30 ms until the outputs have switched. [16]

For evaluation, the input was parameterized with a filter time *(tF ilter)* of 3 ms.
The firmware from the associated satellite requires the time *(tFW).* [17] The satellite is located at the same inline station as the associated island 2 (logic module), which is required for the evaluation. An F watchdog time *(tFW D_IN)* was configured for communication between these two Inline modules. The logic itself needs the time *(tOUT_LP* SDO2) for processing. The output to be switched is on the logic module, so there is no further F watchdog time *(tFW D_OUT)* for transmission to a satellite, as is the reaction time of the output *(tOUT).*

The safety circuit for the shutter provided by the laser controller must be closed potential-free so that the shutter releases the laser diode. For this purpose, a safety relay with feedback was connected to the output of the SafetyBridge logic module (island 2) . The maximum time to drop out *(tA)* is 20 ms. [18] The safety circuits of the laser controller are not safety-related and are not specified in more detail.
The manufacturer informed us that a maximum switch-off time of 200 ms *(tST OP)* should be assumed.

This relationship for determining the maximum switch-off time required is set out in *Equation* (6) and leads to the result *tSF* = 368.25 ms. A time of *tSF* = 280 ms was required. Of this, 50 ms was reserved for the SafetyBridge system and the safety relay. This time obviously cannot be met. Consequently, the depth that the slide dips into the laser processing booth has to be recalculated , see [6, p. 40].

$$tSF = tS + tF\ ilter + tFW + tFW\ D\_IN + tOUT\_LP\ SDO2 + tFW\ D\_OUT + tOUT + tA + tST\ OP \quad (6)$$

tSF = (30 + 3 + *0,* 25 + 100 + 15 + 0 + 0 + 20 + 200) ms

$tSF = 368.25ms$ _

6.5 Conclusion

With the SafetyBridge technology (SBT), the safety concept for a versatile assembly system could be implemented. A system size with seven possible machine modules was required . Due to the performance, this requirement had to be limited to three possible machine modules. The extensive plausibility check of signals to build up an expectation requires more memory than the logic module can offer. The decisive factor was the lack of a module with the following function. A number of signals are routed to the block and the number of TRUE signals is output as a result. The result of the determined number can be output via an output of the block. With this solution, there is no need to introduce an integer data type and the use of several self- assembled logic gates could have been avoided. An alternative would have been an extended operator specification, which specifies with the switch position which machine module is integrated at which integration station. This project is limited by the number of switch positions or the implemented safety functions limit the adaptability of the mounting system.

The worst-case reaction times and guaranteed switch-off times required and assumed in the safety concept could not be achieved with the SBT. This is partly due to the existing production network and partly to the technology itself. This can be determined by comparing equations (5) and (6).

When implementing the safety concept, differences in the functionality of the versatile assembly system and some of the installed safety-relevant components were noticed. The following two points are given as examples. The assembly system could not be expanded with the robot assembly machine in the manner described, according to the plug-and-work principle . The intended functionality of the robot assembly machine could not be executed and a decision for a new application was not made. The safety function that controls the laser's shutter could not be fully determined. Although the laser controller has safety interlocks that can be actuated, these are not certified.

For this reason, the safety function could not be fully determined.

The basic machine or the smart transfer system has been expanded with a safety controller and can now offer the service of exchanging safety-relevant data between the integrated machine modules via the safety controller. By selectively bridging safety functions, the assembly system can be changed without stopping production.

6.6 Outlook

The implementation of the SBT has shown that this technology is only suitable for the security concept under consideration to a limited extent. The number of machines that can be integrated can be increased, for example, by using PROFIsafe. Some of the built-in components can still be used. The SBT is to be expanded for future requirements. This can be done using other safe modules . A possible module is already described in Chapter 6.5, others may result from the future requirements described below. It is uncertain what the safety concepts for a modular system construction according to NE 148 Module Variant II might look like in the future. TÜV Süd presents one approach with its position paper. [12] It remains to be seen that the set of rules must be adapted to future modular plant construction by taking this more into account. It is not yet possible to say what new requirements will arise as a result. Based on our own experiences with the versatile SmartFactoryOWL assembly system , the following points turned out to be possible improvements and solutions .

- Institutions with an influence on standardization committees (eg VDMA, TÜV) must find safety concepts for modular mechanical engineering with autonomous machines .

- Manufacturers of functional safety hardware and software must comply with their
  Offer products simple generic solutions.

- Like products from standard applications, safety-relevant sensors must grow in terms of functionality and become more intelligent, see practical example 1.

- The use of a uniform manufacturer-independent protocol for the transmission of safety-related data, such as OpenSafety, is required.

- A certified mechanism for the automatic detection of additional safety controls must be found, which enables an exchange of safety-related data, see HIMA as an example.

- Information on hazards should be stored in the safety controls.
  With this information, the safety controller can determine whether the monitored machine module in combination with the other machine modules in may go into operation without an increased risk arising. In this context , the use of a classification of the machine modules makes sense. [12]

- A standardized exchange of specified information must take place via uniform function blocks, similar to OPC-UA for standard applications.

HIMA offers the already certified HICore processor. That's what it's all about
is a safety system-on-chip solution. With this hardware and the associated programming environment, it is possible to develop a product that could meet the above-mentioned requirements for future safety controls. This chip can be used, for example, to develop a safety controller for processing fewer digital signals . As is usual today, this controller can be modularly expanded. In addition to processing some digital signals, the focus should be on automatically establishing a direct connection to the next safety controller. A machine-to-machine communication is created that can be used for the exchange of safety-relevant data. An algorithm, which may be implemented in the hardware, ensures that the safety controller automatically integrates itself correctly into the existing network. This can include the transmission of a unique identification number and the specification of parameters (classification of the machine) for integration into the modular machine system. If controllers are already available, the controller is supplied with information from the others.
With information from the existing controls, the expectations can be adjusted . The number of required emergency stop signals can result from this expectation. Furthermore, functions must be taken into account that make it possible to identify the upstream and downstream machine modules and to put their processes in a safe state. The safety controller to be developed with the HICore should have a standardized interface for exchanging safety-related data between machines
Offer. This standardized interface has yet to be created.

Practical example 1

The implemented safety concept was limited to answering the question of how many machine modules are integrated. The answers to the other questions, see Chapter 2.1, page 3, were not followed up any further. The idea was pursued of simultaneously determining, in a safety-related manner, which machine module was inserted at which integration point, at the same time as determining the number of inserted machine modules. To answer, the use of RFID magnetic switches was considered and found that this is not possible. The RFID code from the actuator, which is read and processed by the sensor, is not output by the sensor for further processing.
At present, only manipulation protection can be achieved through the use of RFID magnetic switches

increased and only the information of the correct actuation can be obtained. For this statement, the product portfolio of the companies ABB, Schmersal, Pilz and Sick was analyzed and some products were tested. In order to better answer the question considered above, the sensors must be more diverse, for example by determining and outputting the identification number in a safety-related manner. The simple binary sensor is no longer sufficient. This has already been recognized for standard applications and a possible solution has been developed with the IO-Link concept . There are currently no plans to use the IO-Link approach for the transmission of safety-relevant data. [19]

Elsewhere you can read that a working group has been set up for this topic and that the first results can be expected in two to three years. [20]

Another approach to answering other safety-related questions, see page 3, is to include standardized automation technology. The residual risk of incorrect answers must be minimized and determined using certain methods, such as redundancy, so that they can be used for security-related functions . In addition to a coherent and well-documented security concept, this procedure means verification and certification by an external certifier.

This approach usually represents a one-off solution and cannot be generically transferred to machines with a similar modular structure.

In addition to the manufacturers considered in the study, the company Pilz now also offers another option for implementing safety functions for a versatile mounting system . At the time of the study work, no statement or solution for the versatile mounting system could be obtained from the company Pilz . In the meantime, this can be justified by the participation in the SmartFactory KL research project . According to product information and sales inquiries, it should be possible to meet the requirements of Industry 4.0 with the PSS 4000 controller.

This is made possible by a multi-master concept. [21]

Example HIMA

As part of the study work, an automation concept for functional safety from the company HIMA was also presented. [6, p. 57] In this concept, a safety-related machine-to-machine communication could be set up using the diverse implementation options of the controller offered. This would make it possible to dispense with a higher-level controller. The controller offers a wide range of functions and represented the highest costs in comparison. In addition, the estimated implementation effort was comparatively high. According to the current findings of this bachelor thesis, the use of the HIMatrix F30 03 and the concept developed by HIMA can be further revised

follow. The functions to be implemented can not only be used in the versatile assembly system, but can also continue to be used in other modular systems with controllers from HIMA. In the following paragraph, an ideal product is conceived, which is influenced by one's own experiences and ideas.

literature

[1] Patrick Gehlen. *Functional safety of machines and systems: Implementation of the European Machinery Directive in practice.* Siemens. Erlangen: Publicis Publ, 2010. isbn: 978-3-89578-366-1.

[2] NAMUR – interest group for automation technology in the process industry *NAMUR home page.* Published by NAMUR – interest group for automation technology in the process industry eV 2015. url: http://www.namur.net/ (visited 01/24/2015).

[3] German Institute for Standardization. *Safety of machines - Safety-related parts of controls - Safety of machines - Safety-related parts of controls - Part 1: General design principles.* Beuth Verlag GmbH. DIN EN ISO 13849-1:2008-12. Berlin, 2008.

[4] German Institute for Standardization. *Safety of machines - Functional safety of safety-related electrical, electronic and programmable electronic control systems.* Beuth Verlag GmbH. DIN EN 62061 (VDE 0113-50):2013-09. Berlin, 2013.

[5] Fraunhofer Application Center Industrial Automation. *SmartFactoryOWL.* Published by Fraunhofer Application Center Industrial Automation. 2014. url: http://www. smartfactory-owl.de/index.php/de/smartfactory (visited on January 26, 2015).

[6] Philip Kleen. »Creation of a concept for functional safety (safety) for a versatile assembly system, comparison of possible solutions«. 2015

[7] PHOENIX CONTACT, ed. *Inline module with integrated safety logic and safe digital outputs: UM DE IB IL 24 LPSDO 8 V3-PAC: User Manual.* 2992035. 3 Apr 2013.

[8] Michael Volz. Published by WEKA Fachmedien GmbH. 2014. url: http : / / www . elektroniknet.de/ automation/sonsiges/artikel/114773/1/.

[9] Michael Volz. Published by the DKE conference on IEC 61508 in Darmstadt. 2009. url: https:// www.dke.de/de/Wirueberuns/MitteilungendenDKEGeschaeftstelle/ documents / vde % 20dke % 20 - %20tagung % 20zu % 20iec % 2061508 % 20 _ %20pr % C3 % A4sentation%20safetyrelated%20bussysteme. pdf.

[10] Federal Ministry of Labor and Social Affairs. *Interpretation paper on the subject of " The entirety of machines".* Ed. from the 2011 issue of Makrolog ?__blob= publicationFile (visited 2015-08-24).

[11] German Institute for Standardization. *Safety of machinery - Integrated manufacturing systems - Essential requirements.* Beuth Verlag GmbH. DIN EN ISO 11161:2010-10. Berlin, 2010.

[12] Holger Allmang. »Industry 4.0 - Modular certification for dynamically configurable industrial systems«. Receive position paper in personal conversation; TÜV SÜD Product Service GmbH-01.05.2105. 2015

[13] the European Parliament and the Council of the European Union. *Machinery Directive; Directive 2006/42/EC.* Publication in the Official Journal. 2006

[14] Hans Dipl.Ing. Easter man. *Interchangeable equipment.* Edited by MBT Mechters heimer GbR. 2015. url: http : //www.maschinen guidelines.de/machine guidelines/neue- mrl- 2006- 42-eg/werbungbereich/auswechselbare-ausruestungen/ (visited on August 24, 2015).

[15] German Institute for Standardization. *Industrial robots - Safety requirements - Part 2: Robot system and integration.* Beuth Verlag GmbH. DIN EN ISO 10218-2:2012-06. Berlin, 2011.

[16] KA Schmersal GmbH & Co. KG, ed. *data sheet - CSS 8-180-2P+DE-LST.* German. Nov 12, 2015.

[17] PHOENIX CONTACT, published *user manual. UM DE IB IL 24 PSDI 8-PAC.* German. 2910444. June 25, 2013.

[18] PHOENIX CONTACT, ed. *PSR-. . . -24UC/ URM4/5X1/2X2/ B. safety relay for contact expansion.* German. 100517_en_02. May 12, 2014.

[19] TMG Technology and Engineering GmbH. *FAQs. Is it possible to transmit safety- related data, such as emergency stop commands, via IO-Link?* German. 2015. url: http://www.io-link.com/de/FAQ/FAQs.php?thisID=9#Frage10 (visited 11/08/2015).

[20] Joachim Lorenz. *PROFINEWS 116. IO-Link is on its way!* PNO. May 2014. url: http://www.profibus.com/newsroom/profinews-newsletter/profinews-2014-v2/profinews-116-io-link-is-on-its-way (visited on November 8, 2015).

[21] Pilz GmbH & Co. KG. *Industry 4.0. Answers to the questions of the future.* German. Web code 83549. 2015. url: https://www.pilz.com/de-INT/company/industry40 (visited on November 9, 2015).

Attachment: Contents of the CD-ROM

- Bachelor's thesis_Kleen_Print.pdf: Print template used
- Bachelor's thesis_Kleen.pdf: digital copy
- Wiring plan test setup.pdf: Circuit and assembly plan for the test setup
- Pictures
- digital sources
- SAFECONF project files