18. AALE Konferenz
Pforzheim, 09.03.-11.03.2022

Decentralized safety architecture for cyber-physical production systems

C. Faller[1] , A. Schwoll [1]

Summary

In the context of the paper, a research work is shown to implement a networked decentralized safety architecture that replaces the central architecture. Thus, the safety system fits better into the rest of the automation structure. On the one hand, this is done by a clearer hardware structure, as there is now one safety controller per decentralized unit, which, analogous to the distributed automation system, communicates with the other stations via an Ethernet-based bus system, thus greatly reducing the wiring and commissioning effort. On the other hand, the decentralized processing allows a local shutdown of the safety-relevant components and an escalation of the emergency shutdown to other areas, depending on the emergency stop situation. This means that in the event of a safety-critical situation, the shutdown is reduced to what is necessary from a safety point of view, which increases system availability.

Keywords

Industry 4.0, cyber-physical production systems, safety technology

1 Introduction

In order to enable an Industry 4.0 research infrastructure on the one hand and a practical training of students as well as a further training opportunity for employees of regional SMEs in the key region Velbert/Heiligenhaus on the other hand, an Industry 4.0 learning factory was launched on the Campus Velbert / Heiligenhaus (CVH) of the Bochum University of Applied Sciences, which represents a holistic image of a production company. The learning factory consists of a holistic model of a manufacturing company, from the ERP (or enterprise) level to the automation level. The represented process includes a raw parts warehouse, a testing facility, an assembly cell with robot, a shipping robot, connected with corresponding conveyor technology. The individual stations of the production plant each comprise a PLC, which is the heart of the decentralized automation. However, contrary to the plant's decentralized automation concept, the previous safety architecture consisted of a central safety PLC that can shut down the plant centrally. In the context of the paper, a research work is shown to implement a networked decentralized safety architecture that replaces the central architecture. Thus, the safety system fits better into the rest of the automation structure. On the one hand, this is done by a clearer hardware structure, as there is now one safety controller per decentralized unit, which, analogous to the distributed automation system, communicates with the other stations via an Ethernet-based bus system, thus greatly reducing the wiring and commissioning effort. On the other hand, the decentralized processing allows a local shutdown of the safety-relevant components and an escalation of the emergency shutdown to other areas, depending on the emergency stop situation. This means that in the event of a safety-critical situation, the shutdown is reduced to what is necessary from a safety point of view, which increases system availability.

[1] Bochum University of Applied Sciences

2 Initial situation in the CVH learning factory

As a research environment, and in order to provide practical training for students on the one hand and further training for employees of regional SMEs on the other, an Industry 4.0 learning factory was set up on the Velbert / Heiligenhaus campus (CVH) of Bochum University of Applied Sciences, which represents a holistic image of a production operation [1].

The learning factory consists of a holistic model of a manufacturing company, from the ERP level - pot floor - to the field level - the shop floor. SAP is the ERP system, the MES from MPDV, SCADA and energy monitoring from Schneider Electric are available. A transfer line from Festo Didaktik is available as a realistic production environment. This is originally from the year 2000 and is successively migrated in student projects to a contemporary automation technology with current PLCs (Siemens S7-1500, Beckhoff CX5120, Schneider-Electric M340) HMIs and communication systems (ProfiNet, ModbusTCP, EtherCat, OPC-UA). The depicted process includes a raw parts warehouse, a testing facility, an assembly cell with robot, a shipping robot, connected with corresponding conveyor technology. A CNC control (Siemens 840 D sl) for a (simulated) prefabrication completes the process. By integrating the plant into visualization systems, MES, ERP and simulation tools, the physical plant is mapped virtually throughout and thus represents a cyber-physical production system [2].

For the students, the contents of the learning factory are used in the courses of study Fundamentals of Automation, Specialization in Automation, Industrial Management (Bachelor) and IT Systems in Production and Automation (Master). Since the dual students are already working in projects at the regional SMEs, the knowledge acquired in this way is transferred directly to the regional companies. In addition to the practice-oriented use in the named lectures, the partner companies in the entrepreneur network "The Key Region" are offered the possibility of further training in the areas of automation technology, industrial communication technology and energy efficiency in the learning factory.

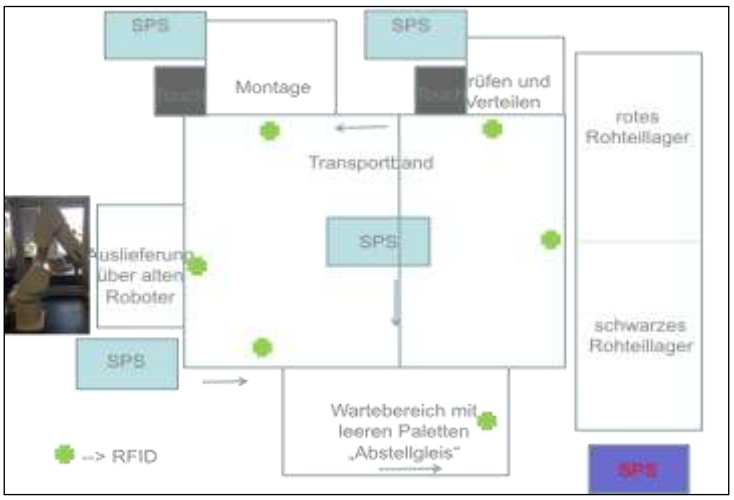


Figure 1: Structure of the CVH Learning Factory

The plant described above has a modular structure. There is no hierarchical communication but a flat architecture in which the individual plant components communicate with each other via OPC-UA and exchange the required information. Since many of the PLCs only have an OPC server, the data is orchestrated by a Node-Red application [3].

Only the safety architecture is still centralized. The information from the individual stations and safety devices is combined and evaluated in a programmable safety relay. In the event that the safe state must be assumed, the corresponding outputs are set by the relay and drives are switched off or pneumatic actuators are depressurized. This architectural principle contradicts the decentralized approach of non-safe automation systems since there is no flexibility with respect to the safe state of the plant [4]. No matter in which area the emergency stop occurs, the consequence is always the same. In order to be able to make a more individual fault assessment here, a decentralized concept was developed in which an individual safety assessment and thus individual shutdowns are possible.

3 Risk assessment of the installation

The safety of a machine cannot be designed arbitrarily, but a designer is obliged to deal with the defined machine guideline and to design the system on the basis of the guideline. The aim of the Machinery Directive is to minimize the risk to people and the immediate environment by means of measures and constructive technical equipment. The protection of people and the environment is to be standardized to the same extent in all countries by means of international common guidelines. At the same time, distortion of competition due to differing safety requirements in the machinery trade is to be avoided. The new revised Machinery Directive 2006/42/EC, the first version of which was issued in 1989, came into force in 2009 [5].

The dangerous situations in different active life phases of the plant would be summarized as:

- Risk of impact due to uncontrolled movements of the bearing system
- Crushing of limbs by pneumatically driven machine parts
- Gripping robots can perform unpredictable movements due to incorrectly entered coordinates and thus endanger their environment.
- Moving merchandise supports or the belt itself can pinch or pull in limbs, long hair, or items of clothing.

To prevent these situations, an appropriate safety system in the form of emergency stop switches, door monitoring sensor and a light barrier is required. From here on, the safety functions are implemented by means of a control system. For this reason, the DIN ISO 13849 standard is used as described in the fundamentals. The risk assessment according to DIN ISO 13849 shows that the required performance level of the safety solution for this type of hazard corresponds to the PL d classification.

After the activation of an emergency stop element, the emergency stop program is triggered. Due to the fact that all emergency stop elements are interconnected and have equal functionality, the entire system is safely shut down. The following steps would then be to completely clear the emergency situation and reset the emergency stop switches to their default settings. However, the system must not be immediately integrated into normal operation. An integration that is not carried out consciously can lead to dangerous situations. An example of this is the light barrier. If the light barrier is triggered and the line of sight between the transmitter and receiver is re-established, the system must not be reintegrated into normal operation immediately afterwards. It is not clear whether the emergency situation has been completely eliminated. The light barrier is not able to determine in which direction the person has left the light beam. For this reason, there may still be persons in the danger zone. For this reason, every emergency stop that is triggered must be acknowledged by pressing a release button after the fault has been rectified, whereupon the system can be resumed in normal operation. The risk assessment according to DIN ISO 13849 shows that the required performance level of the safety solution for this type of hazard corresponds to the PLr a classification. The low classification is justified as follows. Even if an acknowledgement button sticks or fails completely, the system cannot be started. A

short positive edge is necessary for an acknowledgement; if the signal is positive for more than one second, no acknowledgement process is started. Without an acknowledgement option, the system can be accidentally reset to normal operation after resetting the emergency stop switch and thus harm persons who may still be in the danger zone.

4 Conception and realization

The goal is to convert the entire plant to the new decentralized safety solution. It must be designed in such a way that a single emergency stop safely shuts down and switches off all hazardous components of the plant.

IP67 IO modules from Turck are used as safety components. As decentralized intelligence, these enable the implementation of a safety application for the respective station of the plant. Via the ProfiNet interface, they allow communication with a higher-level controller, which should be safety-oriented (Siemens F-CPU). By means of the superordinate control it is possible to send safety-related messages to the other decentralized intelligences, so that these, if necessary for the occurred state, the respective local safe state can be assumed. In the future, it is planned to be able to do without the higher-level controller for cross-communication between the decentralized intelligences. Currently you need the following elements for the realized application:

- Hardware
  - Turck safety module TBPN-1L-FDIO-2IOL
  - Emergency stop switch
  - Acknowledge button
  - SIMATIC ET200SP with F-CPU 1512SP F-1PN

- Software
  - Turck Service Tool V3.2.2
  - Turck Safety Configurator V3.2.2.3
  - Siemens TIA Portal V16 + license for the F-modules

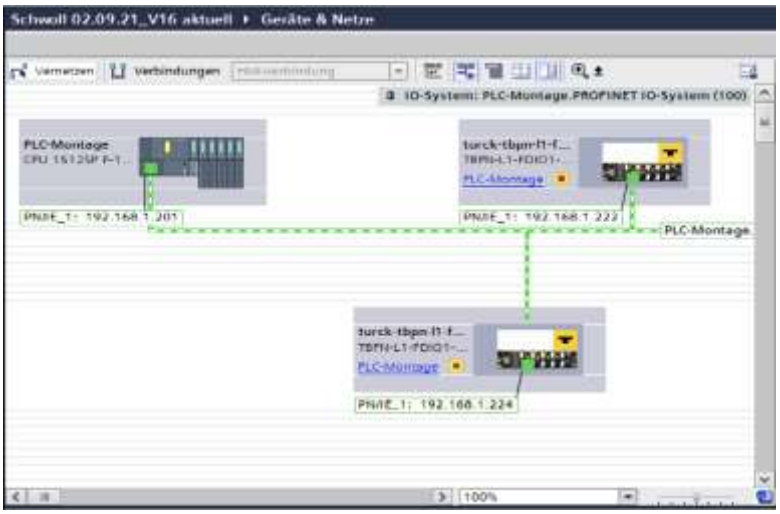


Figure 2: SIEMENS TIA Portal with higher-level and decentralized controls

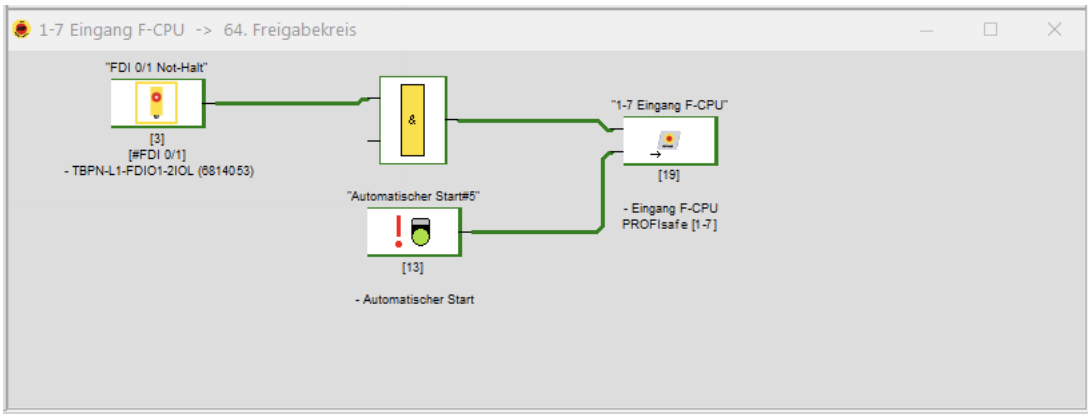


Figure 3: Decentralized application in the TURCK system

The F-CPU and the I/O modules are connected to each other via the central Ethernet switch of the system. For the recognition of the I/O modules in the network, each module requires its own IP address. This address can be identified and, if necessary, reassigned using the "Service Tool V 3.2.2" software developed by Turck. The safety program of the I/O modules is created using "Turck Safety Configurator V3.2.2.3" and transferred to the modules. During the initial setup of an I/O module, the Turck software first creates a standard configuration of the inputs and outputs. This configuration is then adapted to the situation and requirements. The aim of the initial setup is to control the defined safe outputs of all I/O modules via a safe input of an I/O module and to switch them on and off safely. For the linking of two I/O modules, it is still necessary to implement this via a higher-level controller. The Siemens TIA Portal has the possibility to connect the I/O modules from Turck with the F-CPU. For the integration, the TIA Portal requires a GSDML file of the Turck modules. This file contains all the relevant information required for the configuration and signal transmission of the devices. After this GSDML file has been entered in the TIA Portal, the I/O modules are available in the selection and can be integrated into the F-CPU.

Figure 4 shows a program flow chart for controlling the I/O module outputs. This program flow chart only roughly describes the overview of the structure. This structure can be applied to one, two or all I/O modules in the system. If the system is started up and the system is ready to start, the reintegration of all I/O modules must first be carried out. This condition ensures a monitored start. This is done via an input bit of any I/O module in the system, which must be set briefly by a pushbutton. This in turn activates an output bit of the F-CPU for all I/O modules. A monitoring module in the Turck configuration therefore enables the outputs and normal operation is now active. Normal operation can be disturbed by three different causes. One is a faulty emergency stop switch. This can be triggered, for example, by a defective NC contact, line break or cross-circuit of the adjacent contacts. On the other hand, by an error in the communication between the I/O modules and the F-CPU.

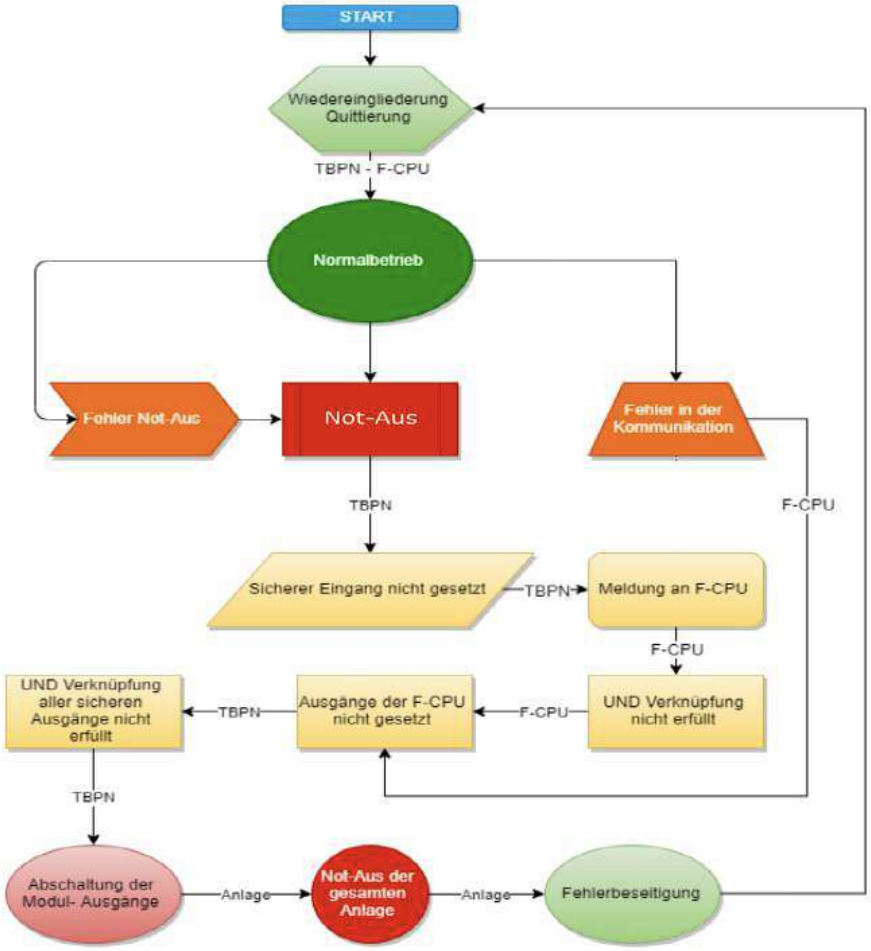


Figure 4: Structure of the safety application

This can be caused, for example, by a break in the Ethernet line, faulty communication protocols, exceeding the monitoring time or a power failure of the individual I/O modules.

As a rule, however, normal operation is interrupted by an emergency stop switch. If an emergency stop is actuated, a normally closed contact opens. The I/O module registers an input that is not set and immediately reports the new status to the F-CPU via ProfiNet. In the F-CPU, a simple program is written, which controls all input signals of the I/O modules that are linked with an AND function block. If all emergency stop switches are deactivated, the AND operation is fulfilled, and the bits of the F-CPU outputs are set. Otherwise, one or more bits are set to 0, depending on how many emergency stop elements have been activated. In case of the latter, it results in the AND operation not being satisfied, and the F-CPU outputs being disabled. Consequently, the linkage of the internally written program of the I/O modules is not fulfilled. The logic operation consists of the output bit of the F-CPU and the input signal of the connected emergency stop switch. The result is the shutdown of all module outputs and thus all connected actuators whose F-CPU bit has not been set. After the cause has been located and eliminated, the outputs of the I/O modules can be acknowledged, and the actuators reintegrated. The local architecture for the bearing station is shown in Figure 5.

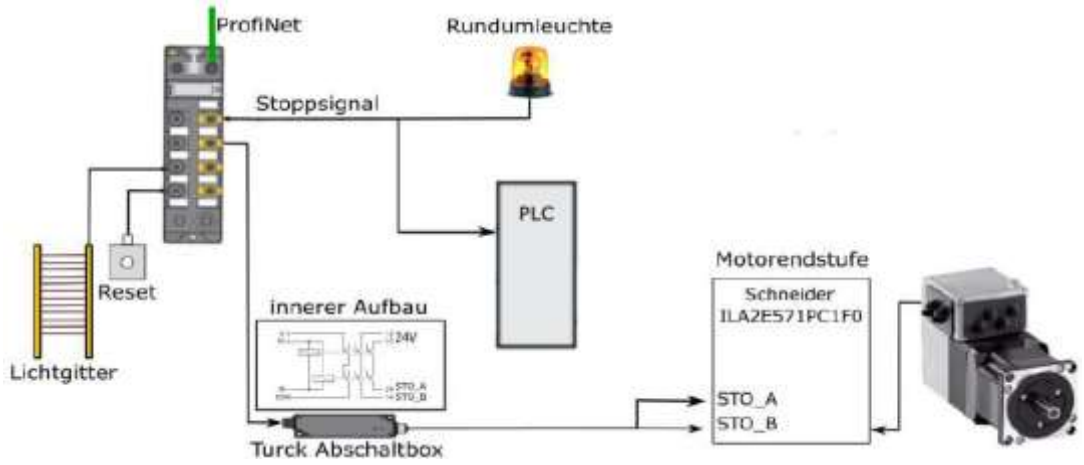


Figure 5: Decentralized safety architecture

5 Validation

The SISTEMA Safety of Machine Controls software wizard provides assistance in validating and evaluating the safety of control systems within the scope of DIN EN ISO 13849-1. The tool extracts safety-related characteristic values of the control parts from the manufacturer's VDMA files on the basis of the standard certification and calculates reliability values at various levels of detail, including the performance level (PL) achieved. The created sub-system is compiled, and the entire parameterization of the complete system is displayed. The result can then be printed out as a report for documentation.

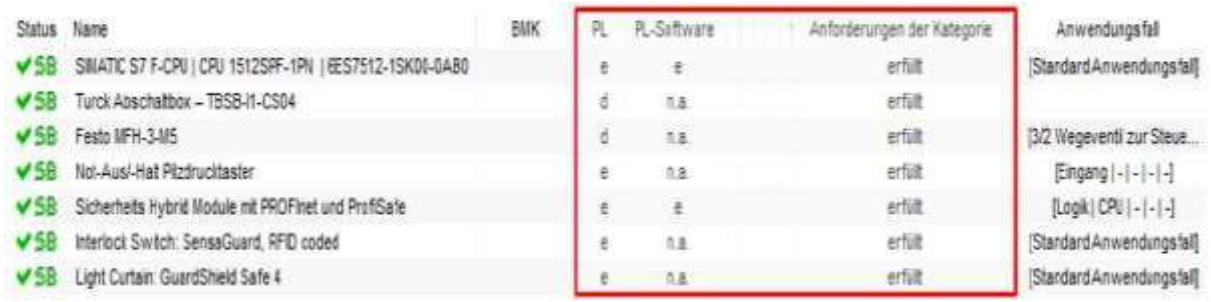
The aim is to safely shut down the entire system after activation of any emergency stop element. For this reason, all emergency stop elements are combined into one sub-system. However, a total of two sub-systems are required. The first sub-system is responsible for the emergency stop of the entire system. This consists of a total of seven system components:

- SPS SIMATIC S7 F-CPU
- Turck safety hybrid modules
- Door monitoring Interlock Switch: SensaGuard
- Light Curtain: GuardShield Safe 4
- 2 channel emergency stop/stop push button latching
- Turck switch-off box - TBSB-I1-CS04
- MFH-3-M5 Pressure valve

As can be seen from the chapter on risk assessment, the required performance level for the emergency stop system has been assigned to level d. The achieved performance level must at least correspond to this level. The performance level achieved must at least correspond to this level. After entering all system components for the emergency stop in the Sistema tool, a positive result is obtained, which is satisfactory for the required level d. All components meet PL level d, i.e., the required performance level for the emergency stop system. All components meet PL level d, the second highest safety level. These components for the safe emergency stop can therefore be used without any loss of safety.

The second subsystem is necessary for acknowledging the system for reintegration after a restart or an emergency stop situation. It essentially consists of three components. On the one hand the acknowledgement button itself and on the other hand the ProfiSafe truck safety module. For the networking of all Turck modules the SIMATIC S7 F-CPU is required. If the three components are entered into the

SISTEMA Assistant and considered as a single sub-system, the result is satisfactory. All components meet at least the required level PL a. For this reason, the system can be used in this form without hesitation.



Status	Name	BMK	PL	PL-Software	Anforderungen der Kategorie	Anwendungsfall
✔SB	SIMATIC S7 F-CPU | CPU 1512SPF-1PN | 6ES7512-1SK00-0AB0		e	e	erfüllt	[Standard Anwendungsfall]
✔SB	Turck Abschaltbox – TBSB-I1-CS04		d	n.a.	erfüllt	
✔SB	Festo MFH-3-M5		d	n.a.	erfüllt	[3/2 Wegeventil zur Steue...
✔SB	Not-Aus/-Halt Pilzdrucktaster		e	n.a.	erfüllt	[Eingang | - | - | - | -]
✔SB	Sicherheits Hybrid Module mit PROFInet und ProfiSafe		e	e	erfüllt	[Logik | CPU | - | - | -]
✔SB	Interlock Switch: SensaGuard, RFID coded		e	n.a.	erfüllt	[Standard Anwendungsfall]
✔SB	Light Curtain: GuardShield Safe 4		e	n.a.	erfüllt	[Standard Anwendungsfall]

Figure 6: Validation with SISTEMA software

6 Conclusion

The goals defined in the task, to develop a safe modular safety solution and to integrate it into the existing laboratory facility of the university, were achieved. The facility now has a modern decentralized emergency stop system. With regard to the risk analysis carried out and the subsequent evaluation performed with the aid of the SISTEMA software, the emergency stop system achieves the PL d classification, which corresponds to the second highest classification according to EN ISO 13849. Due to decentralization, the amount of wiring required has been reduced many times over. In addition, the wiring structure has become clearer, making it easier to locate and eliminate faults and to adapt the system to new requirements. The safety application can now be further modularized in a targeted manner, so that shutdowns in the event of a critical state are minimized. This increases the overall availability of the system.

7 Literature

[1] Faller, C., Feldmüller, D.: Industry 4.0 Learning factories for regional SMEs; Procedia CIRP; Volume 32, Pages 88-92 (2015), 5th Conference on Learning Factories, Edited by Dieter Kreimeier, ISSN: 2212-8271

[2] Bildstein, A.; Seidelmann, J.: Industrie 4.0-Readiness: Migration zur Industrie 4.0-Fertigung, in: Bauernhansl, T; ten Hompel, M; Vogel-Heuer, B.(Eds.): Industrie 4.0 in Produktion, Automatisierung und Logistik, Springer Vieweg, Wiesbaden 2014, ISBN: 978-3658046811

[3] Faller, C.; et. al.: Control-System-Algorithm implemented with NodeRed and OPC-UA, 14th International Conference of Accomplishments in Mechanical ands Industrial Engineering, Mai 2019, Banja-Luka, Bosnien und Herzegowina (Tagungsband), ISBN 978-99938-39-84-2

[4] Sergej Japs, Harald Anacker, Roman Dumitrescu: SAVE: Security & safety by model-based systems engineering on the example of automotive industry, Procedia CIRP, Volume 100, 2021, Pages 187-192, ISSN 2212-8271, https://doi.org/10.1016/j.procir.2021.05.053.

[5] Bundesministerium für Arbeit und Soziales: Produktsicherheitsgesetz, 9. ProdSV (Maschinenverordnung) Interpretationspapier zum Thema "Wesentliche Veränderung von Maschinen" (Bek. des BMAS vom 09.04.2015 – IIIb5-39607-3 – im GMBl 2015, Nr. 10, S. 183-186)