Safety Integrity Evaluation of Safety Function

Peter Ždánsky, Jozef Balák, Karol Rástočný
Department of Control and Information Systems
University of Žilina, Faculty of Electrical Engineering
Žilina, Slovak Republic
peter.zdansky@fel.uniza.sk, jozef.balak@fel.uniza.sk, karol.rastocny@fel.uniza.sk

***Abstract* – For a possibility of using the safety relevant system in practice, it is necessary to prove, that safety requirements, which are defined based on results of risk analysis, are fulfilled. Part of proving the safety of safety relevant system is also quantitative evaluation of safety integrity of the hardware which is involved in the safety functions realization. Objective of the paper is to compare different ways of the quantitative hardware safety integrity evaluation. For a specific technological process are identified hazards, their consequences and from them resulting safety functions. For each defined safety function is, by three different procedures, calculated the probability of dangerous failure per hour. At the end of the paper are stated reasons of results mismatch, which were obtained using different approaches.**

Keywords- safety function; safety integrity; safety related system; sPLC; IEC 61 508; Markov Chain; validation

I. INTRODUCTION (HEADING 1)

If a device, machine or process may in some way endanger assets that are within its scope, it is necessary to identify the hazards, their consequences and subsequently to calculate (estimate) the risk. If this risk is higher than acceptable risk, then it is necessary to apply reasonable measures for the risk reduction. In case of technical measures are defined the safety functions (SFs), whose task is to minimize the hazards occurrence and/or minimize the hazards consequences so, that residual risk is lower or equal to the tolerable risk. Safety functions are performed by the safety relevant system (SRS) [21].

From each SF is required to achieve a certain safety integrity level. Safety integrity of the SRS is according to [1] defined as probability of safety relevant system to satisfactorily perform the required SFs under all specified conditions and within the specified time interval.

Safety integrity consists of three parts [1]:

- Systematic safety integrity – part of the safety integrity of the SRS related to systematic failures in a dangerous mode of failure;
- Software safety integrity – part of the safety integrity of the SRS related to systematic failures in a dangerous mode of failure, that are attributable to software
- Hardware safety integrity – part of the safety integrity of the SRS related to random hardware failures in a dangerous mode of failure.

Generally, safety integrity associated with systematic failures is considered to be an incalculable part of safety integrity. Evaluation of this part of the safety integrity is realized by qualitative methods, whose goal is to prove, that adequate measures have been applied to prevent systematic failures.

Standard [1] requires the quantitate evaluation of requirements fulfilment for the safety integrity, which is related to the random hardware failures. For evaluation is possible to use one method (e.g. failure mode and effects analysis (FMEA) [3], reliability block diagram method (RBD) [4], fault tree analysis (FTA) [5], Markov chains (MC) [6]) or a combination of methods.

If the SF operates in the high demand mode of operation or in continuous mode of operation, then the achieved safety integrity level (SIL) against random failures is determined based on calculated value of the probability of dangerous failure per hour $PFH_D(t)$ of the SF [1].

In general, calculation of $PFH_D(t)$ can be realized by one of these approaches:

- By using the relations and procedures stated in [7]. In [7] for individual architectures of the SF (1oo1, 1oo2, 1oo2D, 2oo2, ...) are defined simplified relations, which are valid under certain assumptions. These assumptions are related to the technical and operational properties of the SRS (or its subsystems), which performs the given SF.
- By using a certified tool specifically designed for this purpose, such a tool Safety Evaluation Tool from company Siemens [8]. This tool simplifies the application of the relations and procedures stated in [7].
- By using the mathematical-graphical model, that is specially designed for a given SF with respect to all the major factors influencing its hardware safety integrity, such as in [2], [18], [19].

In this paper, all three approaches of the safety integrity evaluation of the SFs are used with goal to compare results calculated by each of them.

II. SAFETY FUNCTIONS AND THEIR REALIZATION

Let us consider a technological cell (hereinafter referred to as cell), in which machining the workpiece takes place (Fig. 1). This cell, together with other cells, is part of production line and one production step is realized in it. After execution of all prescribed operations in previous cell is workpiece moved into

ISBN 978-80-261-0722-4,

considered cell. In this considered cell are executed all the prescribed operations and consequently a workpiece is moved into next cell for further processing.

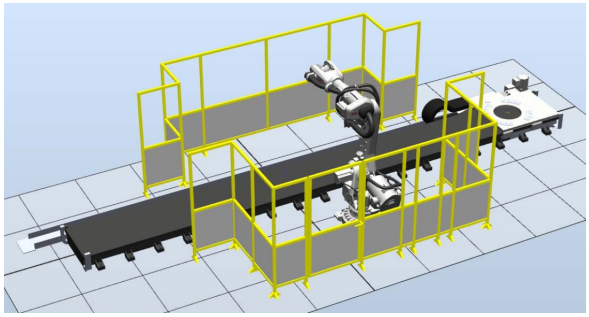


Figure 1. Technological cell

In the considered cell is machining of workpiece realized using an industrial robot. Considering, that in working area of the robot (dangerous zone) when performing the prescribed operations, an injury of a person, who is in this dangerous zone, can happen, dangerous zone is fenced (passive mechanical protection). For possibility of workpieces transfer between cells, two holes are created in the fence. The first hole serves to transfer the workpiece from previous cell into the considered cell. The workpiece is transferred from considered cell into next cell through the second hole. The workpiece transfer is performed by automated cart. The access of the maintenance staff to the fenced dangerous zone is made possible through the doors located in one of the fencing walls.

A. The hazards identification and safety functions definition

The following hazards have been identified during the risk analysis of the considered technological process:

- Movement the robot arm even after a person (maintenance) enters the cell (dangerous zone) through the door.
- Movement of the robot arm even after a person enters the cell (dangerous zone) through the hole intended to transfer the workpiece from the previous cell.
- Movement of the robot arm even after a person enters the cell (dangerous zone) through the hole intended to transfer the workpiece into the next cell.

Each of the identified hazards can lead to serious injury or death of a person in the dangerous area. These SFs were defined for elimination of the identified hazards:

- Safety function SF1 – stop the operations execution and disconnection of the robot from power source when opening the side door.
- Safety function SF2 – stop the operations execution and disconnection of the robot from power source upon entry of a person into the cell through the hole intended to transfer the workpiece from the previous cell.
- Safety function SF3 – stop the operations execution and disconnection of the robot from power source upon entry of a person into the cell through the hole intended to transfer the workpiece into the next cell
- Safety function SF4 – stop the operations execution and disconnection of the robot from power source after pressing the emergency stop button. It is reaction of personnel to other unspecified hazards.

For the above mentioned SFs, that operate in continuous mode, based on the estimated risk associated with individual hazards, the required safety integrity levels were determined. For the SF1 is required SIL2, for the SF2, SF3 and SF4 is required SIL3.

B. The safety related system design

The Fig. 2 shows block scheme of the SRS, that realizes safety functions SF1 to SF4. It consists of the sensor subsystem, the logic subsystem and the final element subsystem. Block Equipment Under Control (EUC) represents the controlled device, i.e. in case of considered cell, it is industrial robot. The SRS realizes only the SFs. Control functions of the robot are realized by the independent standard control system (not safety relevant), that does not subject to safety analysis and therefore is not part of the paper.

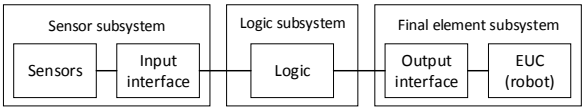


Figure 2. Block scheme of the SRS

The SRS is realized based on safety PLC (sPLC). Safety analysis concerns only those part of the sPLC, whose incorrect function can cause the dangerous failure of the SF. Used modules have dual-channel architecture and fail-safe property. These are the modules:

- Processor unit (F-CPU) Simatic CPU 1512SP F-1 PN (6ES7512-1SK01-0AB0) [9].
- Digital input module (F-DI) Simatic F-DI 8x24VDC HF (6ES7136-6BA00-0CA0) [10].
- Digital output module (F-DO) Simatic F-DQ 4x24VDC/2A PM HF (6ES7136-6DB00-0CA0) [11].

Task of SF1 to SF4 is to react to threatening danger so, that they ensure the robot disconnection from power source, therefore the final element subsystem will participate in realization of all the SFs. The robot is disconnected from power source by a pair of 3-pole contactors K1, K2 of type Sirius 3RT1026-1BB40 [12], whose contacts are connected in series for the required SIL achievement (architecture 1oo2). Contactor K1 is controlled by left channel of the F-DO module and contactor K2 is controlled by right channel of the F-DO module (Fig. 3). The digital output module is not connected directly to F-CPU, but connection is realized through communication module Simatic IM 155-6 PN ST (6ES7155-6AU00-0BN0) using the communication interface PROFINET [13]. Safety communication is ensured by PROFIsafe protocol.

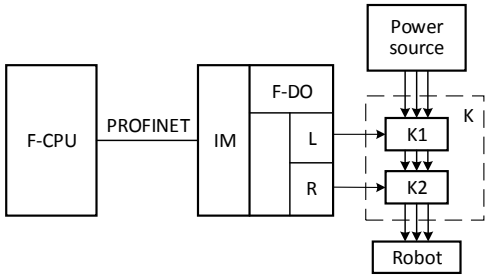
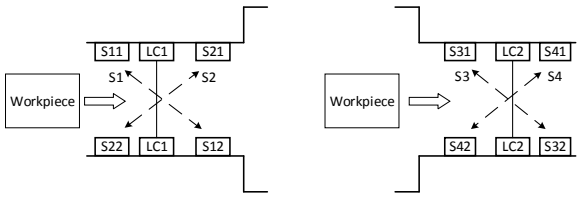


Figure 3. Principle of connection of the final elements block

The sensors subsystem provides information from the technological process, that is relevant for the SFs performance. Sensors are connected to the F-DI modules, that communicate with F-CPU trough the communication module Simatic IM 155-6 PN ST [13] and communication interface PROFINET.

The open door detection is provided by contact-free safety door switch (DS) of type Sirius 3SE6315-1BB02 [14]. DS has dual-channel architecture and for safe detection of the door opening is enough to use one DS.

Realization of the SF2 requires to distinguish between a situation, when workpiece enters the cell and a situation, when a person enters the cell. For this purpose, the light curtain (LC) of type Simatic FS400 from 3RG78 44 series [15], which has SIL 3 and two blocks of polarized retroreflective sensors S1, S2, is used. Each block of optical sensors consists of a sensor pair (S1 - S11, S12; S2 - S21, S22) of type IFM O5P502 (O5P-FNKG /US100) [16]. This kind of solution allows to achieve the required SIL, to use the Muting function [15] and distinguish a person from a workpiece. Condition of distinguishing a person from a workpiece is appropriate layout of these sensors considering the light curtain. The Muting function is realized by 2-sensor connection of type T (Fig. 4.a). A similar solution is also used for realization of the safety function SF3 (Fig. 4.b).



a) SF2 b) SF3

Figure 4. Principle of the sensor connection for the SF2 and SF3

Part of realization of the SF4 is emergency stop button (E-STOP) of type Sirius 3SB3500-1AA20 [17], which has dual-channel architecture.

Manufacturers, for individual components, that participate in the SFs realization, either give directly the value PFH_D (for electronic elements), or give parameters (B_{10}, ...), based on which the value PFH_D can be calculated, if a number of operation cycles of given element per year is known (for electromechanical elements). In calculations of PFH_D for individual SFs the following values are considered:

- Door sensor (Sirius 3SE6315-1BB02): $PFH_D^{DS} = 2{,}7.10^{-10}$ h^{-1}.
- Polarized retroreflective optical sensor (IFM O5P502 (O5P-FNKG/US100)): $PFH_D^{Si} = 1{,}30.10^{-7}$ h^{-1}, where $i = 1,2,3,4$.
- Light curtain (Simatic FS400 from 3RG78 44 series): $PFH_D^{LC1} = PFH_D^{LC2} = 2{,}67.10^{-8}$ h^{-1}.
- Emergency stop button (Sirius 3SB3500-1AA20): $PFH_D^{ESTOP} = 6{,}84.10^{-9}$ h^{-1} .
- Contactor (Sirius 3RT10261BB40): $PFH_D^{K1} = PFH_D^{K2} = PFH_D^{K12} = 1{,}3.10^{-7}$ h^{-1}.
- Digital input module (Simatic F-DI 8x24VDC HF): $PFH_D^{DI} = 1.10^{-9}$ h^{-1}.
- Digital output module (Simatic F-DQ 4x24VDC/2A PM HF (6ES7136-6DB00-0CA0)): $PFH_D^{DO} = 1.10^{-9}$ h^{-1}.
- Logic unit (Simatic CPU 1512SP F-1 PN (6ES7512-1SK01-0AB0)): $PFH_D^{CPU} = 2.10^{-9}$ h^{-1} (including the PROFIsafe).

Communication safety on the basis of PROFIsafe protocol (including transmission components) has individual safety assessment. The intensity of the dangerous falsification of transmitted message (about 1.10^{-9} h^{-1}) is negligible in comparison to the required SIL for individual SFs and therefore it is not considered further [20].

Overall realization of the SRS is shown in Fig. 5.

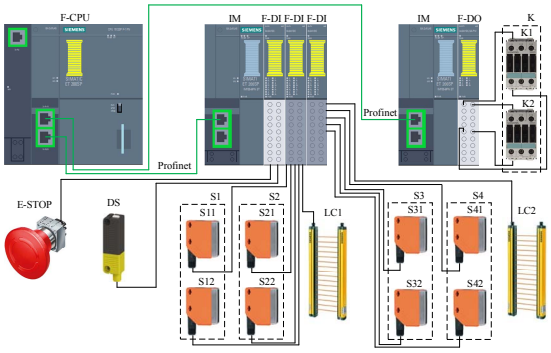


Figure 5. Technical solution of the SRS

C. *Assignment of safety functions to individual part of the SRS*

For each SF is necessary to determine, which parts of the SRS participate in SF realizations. This is shown in Fig. 6.

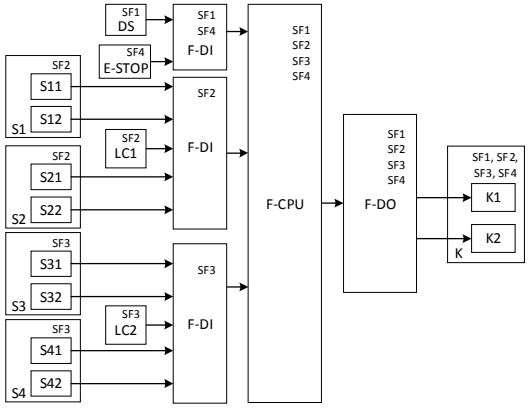


Figure 6. Assignment of safety functions to individual part of the SRS

III. CALCULATION OF THE DANGEROUS FAILURE RATE OF THE SAFETY FUNCTION SF1

The paper presents the calculation of the dangerous failure rate of the safety function SF1 by three different approaches. In all three cases, the same assumptions are made. The same approach was applied in calculation of PFH_D for the SF2, SF3 and SF4.

A. Calculation using the mathematical-graphical model

The Fig. 7 shows Continuous-Time Markov Chain (CTMC), which describes transition of the safety function SF1 from the no-failure, safe state (state 1) into the state, which corresponds to the dangerous failure of the SF1 (state 3). The state 2 represents the situation, when contactor K1 or K2 has the potentially dangerous failure.

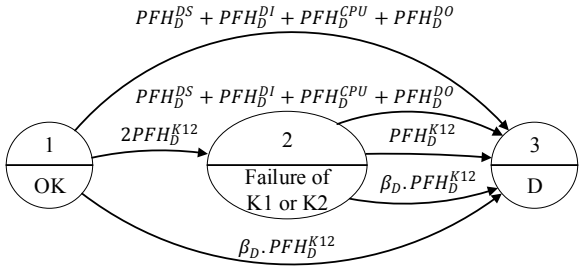


Figure 7. CTMC of the safety function SF1

The intensity of the state 3 occurrence corresponds to the dangerous failure rate of the SF1. From CTMC in Fig. 7 can be deduced, that

$$PFH_D^{SF1} = PFH_D^{DS} + PFH_D^{DI} + PFH_D^{CPU} + PFH_D^{DO} + \beta_D.PFH_D^{K12} + \frac{2.PFH_D^{K12}\left(e^{-PFH_D^{K12}.t} - e^{-2.PFH_D^{K12}.t}\right)}{2e^{-PFH_D^{K12}.t} - e^{-2.PFH_D^{K12}.t}}, \quad (1)$$

where PFH_D^{DS} is the probability of dangerous failure per hour of the door sensor, PFH_D^{DI} is the probability of dangerous failure per hour of the digital input module, PFH_D^{CPU} is the probability of dangerous failure per hour of the processor unit, PFH_D^{DO} is the probability of dangerous failure per hour of the digital output module, PFH_D^{K12} is the probability of dangerous failure per hour of the contactor and β_D is the proportion of the contactor detectable failures with common cause.

Based on recommendations [7], technical parameters of contactor, realization of the SRS and operational properties of the SRS, it was determined, that $\beta_D = 0.05$ and the proof test interval $T_1 = 8\,760$ h (proof test is perfect). After using these values in (1), it can be calculated, that $PFH_D^{SF1} = 1{,}107.10^{-8}$ h^{-1} (maximum value).

Since the standard [7] considers the mean value of the probability of dangerous failure per hour, for calculation of this value the equation (2) was used with result $PFH_{D\_mean}^{SF1} = 1.092 * 10^{-8}$ h^{-1}.

$$PFH_{D\_mean}^{SF1} = \frac{1}{T_1}\int_0^{T_1} PFH_D^{SF1}dt \quad (2)$$

B. Calculation according to IEC EN 61508-6

In [7] the block diagrams for different SF architectures and related relations for calculation of observed parameters are stated. The block diagram of the safety function SF1 is shown in Fig. 8.

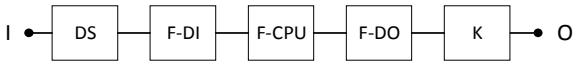


Figure 8. RBD of the safety function SF1

The block diagram consists of serial connection of the elements, that participate in the SF1 realization (dangerous failure of any element causes the dangerous failure of the SF1), therefore the probability of dangerous failure per hour of the SF1 is calculated as:

$$PFH_D^{SF1} = PFH_D^{DS} + PFH_D^{DI} + PFH_D^{CPU} + PFH_D^{DO} + PFH_D^{K}. \quad (3)$$

Because of serial connection of the contactors K1, K2 contacts in circuit of the robot power source, the dangerous failure of the SF1 due to the contactors failure can be described by the block diagram (Fig. 9), that in [7] corresponds to architecture 1oo2. Block CCF in Fig. 9 represents the common cause failures of the contactors K1 and K2.

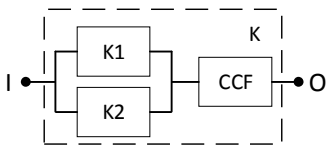


Figure 9. RBD of the robot contactors pair

According to [7] the probability of dangerous failure per hour for the group of components connected in architecture 1oo2, considering identical channels and continuous mode of operation, is calculated as

$$PFH_D^{1oo2} = 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} + \beta_D\lambda_{DD} + \beta\lambda_{DU}, \quad (4)$$

where PFH_D^{1oo2} is the probability of dangerous failure per hour for the group of components connected in architecture 1oo2, λ_{DD} is the dangerous detectable failures rate, λ_{DU} is the dangerous undetectable failures rate, β is the proportion of undetectable failures with common cause, β_D is the proportion of detectable failures with common cause and t_{CE} is the channel equivalent mean downtime. The following relations are related to (4):

$$\lambda_{DU} = \lambda_D(1-DC), \lambda_{DD} = \lambda_D.DC, \quad t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR, \quad (5)$$

where λ_D is the channel dangerous failure rate, DC is the diagnostic coverage, T_1 is the proof test interval and $MTTR$ is the mean time to recovery.

Based on recommendations [7], technical parameters of contactor, realization of the SRS and operational properties of the SRS, individual parameters were determined as follows: $MTTR = 8$ h, $DC = 1$, $\beta_D = 0.05$, $\beta = 2.\beta_D = 0.1$, $T_1 = 8\,760$ h (proof test is perfect). After using these values in (4) and (5), it can be calculated, that $PFH_D^K = PFH_D^{1oo2} = 6.501 * 10^{-9}$ h^{-1}.

Then, from (3) can be calculated, that $PFH_D^{FS1} = 1.078.10^{-8}$ h^{-1}.

C. Calculation using the Safety Evaluation Tool

The Fig. 10 shows basic output information provided by the Safety Evaluation Tool, that is related to the SF1. Using this tool, it was calculated, that $PFH_D^{FS1} = 1{,}16425.10^{-8}$ h^{-1}.

1.1. Safety function SF - Door

Name:	SF - Door
Last editor:	Balák, Jozef
Inspector:	
Last edit date:	February 21, 2018 4:40:37 PM GMT
Status:	open
Version:	1.0
Operation mode:	continuous mode
Description:	
Required SIL:	SIL 2
Achieved SIL:	SIL 3
Achieved PFHD:	1.0770 E-08

Details of the subsystems see annex (pages 8, 9)

Figure 10. Basic information from the Safety Evaluation Tool for the SF1

IV. Results Comparison

The Tab. 1 and Tab. 2 contain calculated values of the PFH_D and corresponding achieved SIL for individual SFs.

For all the safety functions (SF1 to SF4) were calculated the values of the PFH_D, which correspond SIL3, what is in accordance with the defined requirements for SF2, SF3, SF4. For the SF1 was required the SIL2 and achieved the SIL3. It is not in contradiction with safety, but there is scope for using components with worse safety properties, if it would lead to the reduction of the SRS price.

The Tab. 1 and Tab. 2 show, that values of the PFH_D calculated by different approaches are approximately the same and differences are negligible. Existing differences are caused by the fact, that each of used methods uses certain simplifications with the aim to resulting relations are easier to use in practice.

Using the Safety Evaluation Tool and procedures stated in [7] has certain limitations. It is possible to use them only if architecture of evaluated SF and technical and operational properties of the SRS, that realizes given SF, are in compliance with assumptions stated in [7]. Conversely, the method of the PFH_D calculation based on CTMC has universal use, but it is computationally demanding. Also, the probability of mistake when model creating is increasing in complex solutions of the SF.

TABLE I. Calculated probability of dangerous failure per hour (part 1)

Calculation method	SF1		SF2	
	PFH_D [h^{-1}]	SIL	PFH_D [h^{-1}]	SIL
Safety Evaluation Tool	$1.077 * 10^{-8}$	3	$5.020 * 10^{-8}$	3
IEC EN 61508	$1.078 * 10^{-8}$	3	$5.153 * 10^{-8}$	3
CTMC	$1.092 * 10^{-8}$	3	$5.064 * 10^{-8}$	3

TABLE II. Calculated probability of dangerous failure per hour (part 2)

Calculation method	SF3		SF4	
	PFH_D [h^{-1}]	SIL	PFH_D [h^{-1}]	SIL
Safety Evaluation Tool	$5.020 * 10^{-8}$	3	$1.734 * 10^{-8}$	3
IEC EN 61508	$5.153 * 10^{-8}$	3	$1.734 * 10^{-8}$	3
CTMC	$5.064 * 10^{-8}$	3	$1.749 * 10^{-8}$	3

Acknowledgment

This paper has been supported by the Educational Grant Agency of the Slovak Republic (KEGA) Number: 034ŽU-4/2016: Implementation of modern technologies focusing on control using the safety PLC into education.

References

[1] IEC EN 61508-1: "Functional safety of electrical/electronic/programmable electronic safety-related systems", 2010.

[2] Rástočný K., Ždánsky J., Hrbček J., "Influence of architecture and diagnostic to the safety integrity of SRECS output part", in International conference of Applied electronics (AE), 2015, pp. 297-301, ISBN: 978-80-261-0386-8.

[3] IEC 60812: "Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)", 2006.

[4] IEC 61078: "Analysis techniques for dependability - Reliability block diagram and boolean methods", 2016.

[5] IEC 61025: "Fault tree analysis", 2006.

[6] IEC 61165: "Application of Markov techniques", 2006.

[7] IEC EN 61508-6: "Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3", 2010.

[8] Siemens.com, "Safety Evaluation Tool", 2018. [Online]. Available: https://www.industry.siemens.com/topics/global/en/safety-integrated/machine-safety/safety-evaluation-tool/Pages/default.aspx. [Accessed: 14-Feb-2018].

[9] Siemens, "Data sheet 6ES7512-1SK01-0AB0", 2018. [Online]. Available: https://mall.industry.siemens.com/tedservices/DatasheetService/DatasheetService?control=%3C%3Fxml+version%3D%221.0%22+encoding%3D%22UTF-8%22%3F%3E%3Cpdf_generator_control%3E%3Cmode%3EPDF%3C%2Fmode%3E%3Cpdmsystem%3EPMD%3C%2Fpdmsystem%3E%3Ctemplate_selection+mlfb%3D%226ES75121SK010AB0%22+system%3D%22PRODIS%22%2F%3E%3Clanguage%3Een%3C%2Flanguage%3E%3Ccaller%3E

Mall%3C%2Fcaller%3E%3C%2Fpdf_generator_control%3E. [Accessed: 14-Feb-2018].

[10] Siemens, "Simatic ET 200SP Digital input modul F-DI 8x24VDC HF (6ES7136-6BA00-0CA0). Manual", 2013. [Online]. Available: https://industry.siemens.com/dl/files/499/78589499/att_878784/v1/et200sp_f-di_8x24vdc_hf_manual_en-US_en-US.pdf. [Accessed: 14-Feb-2018].

[11] Siemens, "Simatic ET 200SP Digital output modul F-DQ 4x24VDC/2A PM HF (6ES7136-6DB00-0CA0). Manual", 2013. [Online]. Available: https://support.industry.siemens.com/cs/attachments/78645789/et200sp_f-dq_4x24vdc_2a_pm_hf_manual_en-US_en-US.pdf. [Accessed: 14-Feb-2018].

[12] Siemens, "Data sheet 3RT1026-1BB40", 2018. [Online]. Available: https://support.industry.siemens.com/tedservices/DatasheetService/DatasheetService?format=pdf&mlfbs=3RT1026-1BB40&language=en&caller=SIOS. [Accessed: 14-Feb-2018].

[13] Siemens, "Simatic ET 200SP IM 155-6 PN ST interface module (6ES7155-6AU01-0BN0). Manual", 2017. [Online]. Available: https://support.industry.siemens.com/cs/attachments/59768173/et200sp_im_155_6_pn_st_manual_en-US_en-US.pdf. [Accessed: 14-Feb-2018].

[14] Siemens, "Industrial controls. Detecting devices. Sirius RFID safety switch. Configuration manual", 2013. [Online], Available: https://support.industry.siemens.com/cs/attachments/52233535/Configuration_Manual_Safety_Switch_3SE6_en-US.pdf. [Accessed: 14-Feb-2018].

[15] Siemens, "SIMATIC Safety Integrated for Factory Automation. Light curtain SIMATIC FS400 with muting in F-CPU in category 4 according to EN 954-1: 1996 (with evaluation according to EN 62061 and EN ISO 13849-1: 2006)", 2007. [Online]. Available: https://cache.industry.siemens.com/dl/files/201/21331201/att_15594/v1/21331201_as_fe_i_005_v20_en_lcurtain.pdf. [Accessed: 14-Feb-2018].

[16] Ifm.com, "O5P502 (O5P-FNKG/US100). Photoelectric senzors", 2007. [Online]. Available: https://www.ifm.com/au/en/product/O5P502. [Accessed: 14-Feb-2018].

[17] Siemens, "Data sheet 3SB3500-1AA20", 2017. [Online]. Available: https://mall.industry.siemens.com/tedservices/DatasheetService/DatasheetService?control=%3C%3Fxml+version%3D%221.0%22+encoding%3D%22UTF-8%22%3F%3E%3Cpdf_generator_control%3E%3Cmode%3EPDF%3C%2Fmode%3E%3Cpdmsystem%3EPMD%3C%2Fpdmsystem%3E%3Ctemplate_selection+mlfb%3D%223SB3500-1AA20%22+system%3D%22PRODIS%22%2F%3E%3Clanguage%3Een%3C%2Flanguage%3E%3Ccaller%3EMall%3C%2Fcaller%3E%3C%2Fpdf_generator_control%3E. [Accessed: 14-Feb-2018].

[18] Ilavský J., Rástočný K., "Considerations of the recovery in 2-out-of-3 safety-related control system", in 11th IFAC/IEEE International Conference on Programmable Devices and Embedded Systems (PDeS). MAY 23-25, 2012, Brno, Czech Republic. DOI: 10.3182/20120523-3-CZ-3015.00032.

[19] Rástočný K., Franeková M., Zolotová I., Rástočný K. Jr., "Quantitative assessment of safety integrity level of message transmission between safety-related equipment", in: The journal Computing and Informatics, Volume 33, pp. 1001-1026 (2014). ISSN: 1335-9150.

[20] Siemens, "Safety integrated. Overview of safety-related parameters for Siemens components in accordance with ISO 13849-1 and IEC 62061", 2017. [Online]. Available: https://www.industry.siemens.nl/topics/nl/nl/safety-integrated/machineveiligheid/Documents/SIEMENS-producten_PFHd_SIL_PL_B10-waarden%20(EN).pdf. [Accessed: 14-Feb-2018].

[21] Rausand M., Reliability of safety-critical systems: Theory and applications. Wiley, 2014. ISBN 978-1-118-11272-4.