The Output Circuit Solution of the Safety PLC for a Larger Number of Output Points

Juraj Ždánsky
University of Žilina, Faculty of Electrical Engineering and Information Technology
Department of Control and Information Systems
Univezitná 8215/1, 010 26 Žilina, Slovak Republic
juraj.zdansky@uniza.sk

Karol Rástočný
University of Žilina, Faculty of Electrical Engineering and Information Technology
Department of Control and Information Systems
Univezitná 8215/1, 010 26 Žilina, Slovak Republic
karol.rastocny@uniza.sk

Jozef Hrbček
University of Žilina, Faculty of Electrical Engineering and Information Technology
Department of Control and Information Systems
Univezitná 8215/1, 010 26 Žilina, Slovak Republic
jozef.hrbcek@uniza.sk

***Abstract*— Safety PLCs (Programmable Logic Controllers) are commonly a part of the Safety Related Control System (SRCS), especially in industrial applications. In most cases, the controlled devices cannot be connected directly to the safety PLC outputs, but they require an output circuit consisting of relays or contactors. The paper deals with the solution of the output circuit for a larger number of controlled devices and analyzes the influence of selected factors (especially the switching frequency of the used relays) on the Safety Integrity Level (SIL) of the output circuit.**

Keywords*— *safety PLC, SRCS, relay, contactor, SIL

I. INTRODUCTION

Standards dealing with the functional safety of safety-related control systems (SRCSs), e.g. [1], [2], [3], are based on the general assumption that the SRCS consists of an input part, a logic part, and an output part (output circuit). Before putting such a system into operation, proof must be provided that the safety integrity requirements are met. The safety integrity assessment must be performed separately for each safety function (SF) performed by the SRCS.

According to the standard EN61508 [1] the safety integrity is created of systematic safety integrity, software safety integrity and hardware safety integrity (HW-SI)

Problems related to ensuring the systematic and software safety integrity of SRCS are not analyzed in this paper. This topic is dealt with in more detail, e.g. [4], [5]. HW-SI is affected by random hardware failures, and for SF, which is implemented by electronic SRCS, the proof must be provided by the quantitative analysis.

The SRCS input part consists of sensors that provide input information for the logical part of the system. In this paper, it is assumed that the logical part is provided by the safety PLC.

In the realization of common control functions, the output circuit is primarily realizing a power matching of the outputs of the control system and the controlled device. In addition to power matching, SFs safety integrity requirements must be considered when designing the output circuit, in which realization the output part participates, or other requirements.

The paper deals with some variants for the solution of the output circuit and the influence of these solutions on HW-SI realized by SFs. The paper considers the basic connection of the output circuit (the output circuit may contain other supporting elements). It is assumed that the safe state of the SF is achieved by disconnecting the equipment under control (EUC), in the control of which the SF participates (in general, one SF participates in the control of several EUCs).

II. CONTROL OF ONE EUC BY ONE SF

In Fig. 1. the SRCS logic consists of a safety PLC and the output part is a circuit composed of relays. The relay contacts control the EUC. Two-channel control of the EUC is required if SF should be implemented with a high level of safety integrity (SIL 3 or SIL 4), for example the use of two relays having main contacts connected in series with the EUC (safe state of the EUC is enforced by disconnecting its power supply). Since this is a relay for which the manufacturer does not guarantee a permanent opening of the main contact in the event of a relay failure (permanent closing due to a failure is not excluded), it is necessary to check the correct operation of the relay. Checking is possible with the auxiliary contacts of the relay. In order for such a check to be acceptable from a safety point of view, the auxiliary contacts must be mechanically linked to the main contacts (the definition of mechanically linked contacts is in [6]) and must be designed as a mirror contact (according to [7]). Auxiliary contacts are connected in feedback and their status is evaluated by the safety PLC.

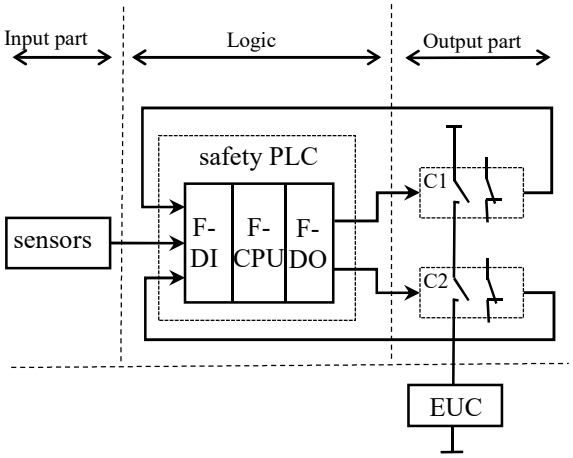

Fig. 1. Output circuit - control of one EUC

A complete test of the fault-free state of the relay is performed by an application program in such a way that the application program sends the command to change the state of the relay (also for changing the state of its contacts) and

2021 International Conference on Applied Electronics (AE) | 978-80-261-0973-0/21/$31.00 ©2021 10.23919/AE51540.2021.9542910

ISBN 978-80-261-0973-0, © University of West Bohemia, 2021

checks whether the state of the relay contacts corresponds to the command. The safety PLC sends the command to permanently interrupt the excitation of both relays if a mismatch is detected between the required and detected state of the contacts of both relays.

In Fig. 1 there is not a complete connection of the output circuit, but only those elements are shown that are important for the evaluation of HW-SI (they affect HW-SI).

Let the SRCS in Fig. 1 implements one SF. Then the quantitative analysis of the HW-SI safety function can be realized by analyzing each of its parts separately and the resulting SF dangerous failure rate is given by the relation (it is a serial arrangement of the parts of the SRCS):

$$\lambda_{DSF}(t) = \lambda_{DI}(t) + \lambda_{DsPLC}(t) + \lambda_{DO}(t), \quad (1)$$

where $\lambda_{DSF}(t)$ is the dangerous failure rate of SF, $\lambda_{DI}(t)$ is the dangerous failure rate of the input part, $\lambda_{DsPLC}(t)$ is the dangerous failure rate of the safety PLC and $\lambda_{DO}(t)$ is the dangerous failure rate of the output part.

The input part dangerous failure rate depends on the sensors used and the way they are connected to the safety PLC.

The safety PLC dangerous failure rate can be determined on the basis of the manufacturer's catalog data and the number of modules used (only those modules that have an impact on the HW-SI are taken into the account).

$$\lambda_{DsPLC} = \lambda_{CPU} + k \cdot \lambda_I + l \cdot \lambda_O, \quad (2)$$

where λ_{CPU} is the processor unit dangerous failure rate, λ_I is the input module dangerous failure rate, λ_O is the output module dangerous failure rate, k is the input modules number, l is the output modules number (Note: Some manufacturers also provide certain values usable for calculating the dangerous failure rate per one input, resp. output).

The output part dangerous failure rate can be expressed by the relation

$$\lambda_{DO}(t) = \frac{\frac{P_{DO}(t)}{dt}}{1-P_{DO}(t)}, \quad (3)$$

where $P_{DO}(t)$ is the probability of dangerous failures of the output part.

$$P_{DO}(t) = P_{R1}(t) \cdot P_{R2}(t), \quad (4)$$

where $P_{R1}(t)$, resp. $P_{R2}(t)$ is the probability of failure of relay R1, resp. R2.

Since the relay is an electromechanical element, so the failure distribution of this element is approximated in the calculations by an exponential distribution, which is in accordance with [3]. Then the relay failure rate can be determined based on the operating load by the equation:

$$\lambda_R = \frac{3 \cdot d_{OP} \cdot h_{OP}}{73 \cdot t_C \cdot B_{10D}}, \quad (5)$$

where d_{OP} is the number of operating days per year, h_{OP} is the number of operating hours per day, t_C is the time between two times switching the contact of relay in seconds and B_{10D} is the relay parameter specified by the manufacturer (expresses the number of relay cycles at prescribed load during which 10% of tested relays fails dangerously). Under the above assumptions λ_R expresses the relay dangerous failure rate in [h^{-1}].

Then

$$P_{R1}(t) = 1 - e^{-\lambda_{R1} \cdot t}$$
$$P_{R2}(t) = 1 - e^{-\lambda_{R2} \cdot t} \quad (6)$$

If it is valid that $\lambda . t \ll 1$ then it can be derived from (3), (4) and (6) that:

$$\lambda_{DO}(t) = 2 \cdot \lambda_{R1} \cdot \lambda_{R2} \cdot t,$$
$$t = t_D + t_N, \quad (7)$$

where t_D is the time of the failure state detection (it means a time that elapses between two relay state changes, i.e. the time interval between the commands to pull and release the relay armature) and t_N is the time of failure state negation (the reaction of the logic in the case of failure state detection - actuation the EUC to the safe state).

If the SRCS logic consists of a safety PLC and the output part consists of a relay (the negation time is a maximum of a few seconds), then it is usually true that $t_D \gg t_N$ and therefore it is sufficient consider only the time of failure state detection. The time t_N can be determined based on the safety PLC response time . This problematics id described in more detail in [8] and [9].

If the change of relay state is not repeated with a regular time interval, then a pessimistic approach must be chosen and the longest time between two changes of relay state must be considered. Alternatively, it is possible to implement a test procedure into the application program in order to trigger a relay state change at an appropriate time and evaluate this change. The maximum time between two changes of relay state is given by the tolerable dangerous state rate of the output circuit, i.e.

$$t_D \leq \frac{\lambda_{DOT}}{2 \cdot \lambda_{R1} \cdot \lambda_{R2}}, \quad (8)$$

where λ_{DOT} is the output circuit tolerable dangerous failure rate, which depends on the required SIL of the safety function.

III. CONTROL OF ONE EUC BY SEVERAL SFS

Control of one EUC by several SFs is a very frequent requirement that occurs in control of an industrial or transport process. This problem is solving in the safety PLC application software. The individual SFs then work with a different set of sensors in the input part but with the same output part. The output circuit is realized by a pair of relays, as describe the part II. of this paper.

IV. CONTROL OF SEVERAL EUCS BY ONE SF

If one SF controls two or more EUCs, the following principal solutions are possible:

- each EUC is controlled by a separate pair of relays;
- each EUC is controlled by one individual relay and one relay common for all EUCs;
- a combination of the first and second solutions.

A. EUC control by a separate pair of relays

Such a solution (Fig. 2) is required when each EUC has different power requirements. In essence, this is a multiple application of the output circuit connection in Fig. 1.

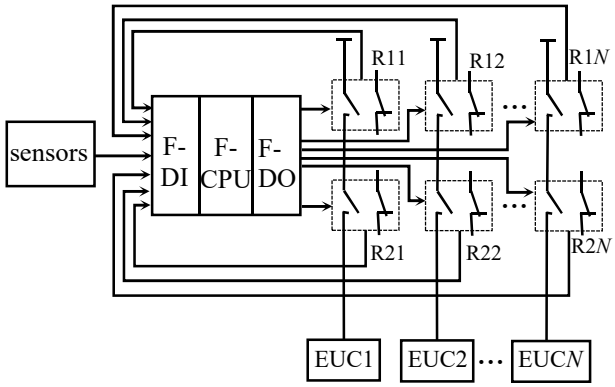

Fig. 2. Output circuit – control of several EUCs

Since all the relays connected in the output circuit participate on the realization of one SF, the inability to disconnect any EUCs from the power supply will cause a dangerous SF failure. Therefore, when calculating the SF dangerous failure rate, the entire connection of the output circuit must be considered. If it is valid that $\lambda_{Rji} \cdot t \ll 1$, where $j = 1, 2$ *and* $i = 1,2, \dots, N$, then

$$\lambda_{DO}(t) = 2 \cdot \lambda_{R11} \cdot \lambda_{R21} \cdot t_1 + 2 \cdot \lambda_{R12} \cdot \lambda_{R22} \cdot t_2 + \cdots + 2 \cdot \lambda_{R1N} \cdot \lambda_{R2N} \cdot t_N, \quad (9)$$

where N is the number of EUCs and t_i is the time of failure state detection and negation for the $i-$ th pair of relays.

If the times $t_1, t_2, \dots, t_N$ are not the same, the pessimistic assumption can be used

$$t_R = \max(t_1, t_2, \dots, t_N), \quad (10)$$

or the mean value can be used (a more optimistic approach).

The requirement for the output circuit failure detection time follows from (8)

$$t_R \le t_D \le \frac{\lambda_{DOT}}{2 \cdot (\lambda_{R11} \cdot \lambda_{R21} + \cdots + \lambda_{R1N} \cdot \lambda_{R2N})}. \quad (11)$$

If $\lambda_{R11} = \lambda_{R21} = \lambda_{R12} = \lambda_{R22} = \cdots = \lambda_{R1N} = \lambda_{R2N} = \lambda_R$, then it is possible to adjust (11) as follows:

$$t_R \le t_D \le \frac{\lambda_{DOT}}{2 \cdot N \cdot \lambda_R^2}. \quad (12)$$

In order for condition (11) to apply, the time of failure detection and negation for the individual relay pairs must be adjusted accordingly. During designing the output circuit it is necessary to proceed in such a procedure that the requirement for t_R is determining at first and consecutively adjust the times $t_1, t_2, \dots, t_N$ accordingly.

The failure rate of the SF is given by relation (1).

B. Output circuit with common relay for controlling EUCs

If the EUCs do not require galvanic isolation, it is possible to use the output circuit according to Fig. 3. If the number of controlled EUCs is N, then the number of relays of output circuit is $N + 1$, unlike the circuit in Fig. 2, where the number of relays is $2N$.

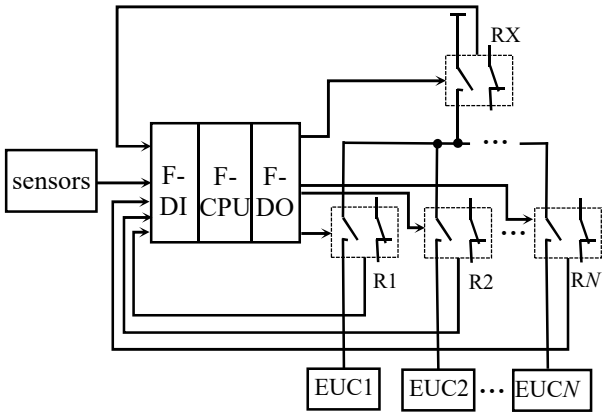

Fig. 3. Simplified connection of the output circuit – control of several EUCs by a common relay

In the fault tree (Fig. 4) the top event V is defined as an output circuit dangerous failure, i.e. connecting the EUC to the power supply at the time, when the command to disconnect is sending. The individual basic events correspond to the effect of the failure state of the given relay.

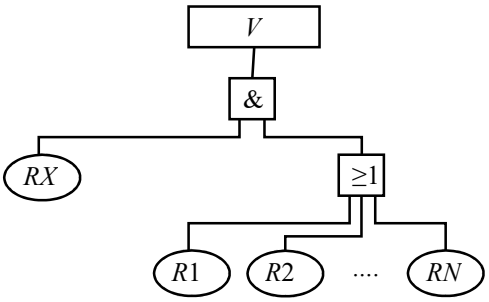

Fig. 4. Fault tree for connection of the output circuit according to Fig. 3

The logic function describing the fault tree in Fig. 4 is given by the equation:

$$V = RX \cdot (R1 + R2 + \cdots + RN), \quad (13)$$

where Ri is the basic event corresponding to the fault state of the relay Ri, where $i = X, 1, 2, \dots, N$.

If it is valid that $\lambda_{Ri} \cdot t \ll 1$, where $i = X, 1, 2, \dots, N$, then based on (13) it can be deduced that

$$\lambda_{DO}(t) = \lambda_{RX} \cdot [\lambda_{R1} \cdot (t_X + t_1) + \lambda_{RX} \cdot \lambda_{R2} \cdot (t_X + t_2) + \cdots + \lambda_{RX} \cdot \lambda_{RN} \cdot (t_X + t_N)], \quad (14)$$

where t_X is the failure state detection and negation time (the time between two switching-off of the relay contacts) RX and t_i is the failure state detection and negation time (the time between two times switching the contact of the relay) of relay Ri.

If it is valid that $\lambda_{R1} = \lambda_{R2} = \cdots = \lambda_{RN} = \lambda_R$ and $t_1 = t_2 = \cdots = t_N = t_R$, then the equation (14) can be modified as follows

$$\lambda_{DO}(t) = N \cdot \lambda_{RX} \cdot \lambda_R \cdot (t_X + t_R). \quad (15)$$

If the times $t_1, t_2, \dots, t_N$ are not the same, a pessimistic assumption can be used

$$t_R = \max(t_1, t_2, \dots, t_N), \quad (16)$$

or the mean value can be used (a more optimistic approach).

Then, a requirement for the failure state detection time of the output circuit fulfills an inequality

$$(t_X + t_R) \leq t_{DT} \leq \frac{\lambda_{DOT}}{N \cdot \lambda_{RX} \cdot \lambda_R}. \quad (17)$$

V. CASE STUDY

Tab. 1 shows the parts of the SRCS realizing the safety function and their characteristic parameters related to safety.

TABLE I. THE PARAMETERS OF THE SRCS PARTS THAT REALIZE THE SAFETY FUNCTION

SRCS parts	**Parameters**
input part	λ_{DI}=1.10^{-10} h^{-1}
safety PLC	
F-CPU 1516F-3PN/DP	λ_{CPU}=1.10^{-9} h^{-1}
F-DI 16x24VDC	λ_I=1,00.10^{-9} h^{-1}
F-DO 8x24VDC/2APPM	λ_O=2,00.10^{-9} h^{-1}
relay LC1D09BD	B10d=1369863 cycles with nominal load conforming to EN/ISO 13849-1

Assume that the SRCS is in operation 260 days a year (working days), 8 hours a day. Under these conditions, Fig. 5 shows the curves of the dangerous failure rate of the SRCS output part depending on the time between two times switching the contact of the relay. The curves were created in the MS excel program based on the relations (5), (9) and (14).

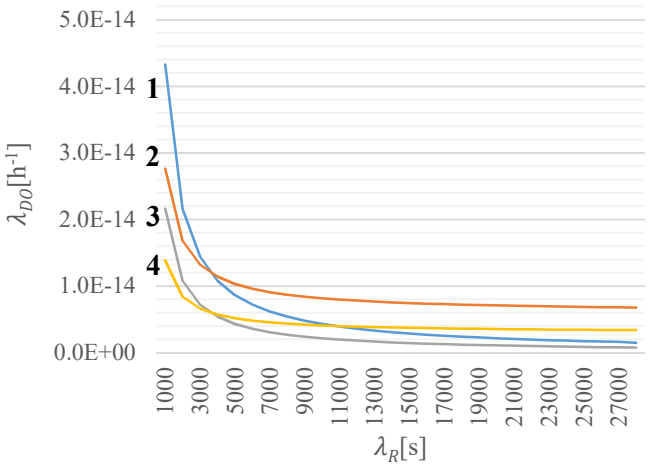

Fig. 5. The dangerous failure rate of the SRCS output part

The curves take into account the fact that the time between two switching-on of the relay contacts affects the output circuit dangerous failure rate through two factors:

- affects the failure rate of the relay (relation (5));
- affects the failure state detection of the relay (relation (9) and (14)).

Curves 1 and 3 show the dangerous failure rate of the output circuit connected according to Fig. 2 and curves 2 and 4 show the dangerous failure rates of the output circuit connected according to Fig. 3. Curves 1 and 2 are for 10 controlled EUCs (N = 10) and curves 3 and 4 are for 20 controlled EUCs (N = 20). Curves 2 and 4 use the parameter 1hour as the time between two switching-off of the relay contacts RX (t_X= 3 600 s).

From the comparison of courses 1 and 3, resp. 2 and 4, the influence of the number of controlled EUCs on the dangerous failure rate of the output circuit is obvious. These results are evaluated in more detail in the following chapter.

Tab. 2 shows the SF dangerous failure rate using the connection according to Fig. 2 and Fig. 3, for different times between two switching-off of the relay contacts and the different numbers of controlled EUCs.

TABLE II. THE SF DANGEROUS FAILURE RATE FOR VARIOUS PARAMETERS

Circuit	Number of controlled EUCs	times between switching off of the relay	Dangerous failure rate λ_{DSF}
according to Fig. 2	10	t_R= 60 s	7,41.10^{-9} h^{-1}
according to Fig. 2	20	t_R= 60 s	1,37.10^{-8} h^{-1}
according to Fig. 3	10	t_R= 60 s t_x = 3600 s	4,60.10^{-9} h^{-1}
according to Fig. 3	20	t_R= 60 s t_x = 3600 s	7,73.10^{-9} h^{-1}

VI. EVALUATION OF RESULTS AND DISCUSSION

In the circuit according to Fig. 2, a pair of relays controlling one EUC operates with the same time between two switching-off of the relay contacts. In the circuit according to Fig. 3, the RX relay can operate in two modes. In the first mode, it will switch-on the relay contacts on request to energize any of the EUCs from N. In other words, it will energize simultaneously with any of the relays Ri ($i = 1, 2, \dots, N$). In the second mode, the relay will be permanently energized and switched-off only if the feedback evaluates the fault state of whichever relays Ri ($i = 1, 2, \dots, N$).

In the first case, the time t_X cannot be determined unambiguously, because it would be necessary to know the exact time regularities of the switching of the relay Ri ($i = 1, 2, \dots, N$). This is practically impossible. If simultaneous switching of several relays could be ruled out, then it is valid that $t_R > t_X$. However, if this cannot be ruled out, we must assume that relay RX is permanently switched-on during the control of N EUCs because the switching-on of the relays Ri ($i = 1, 2, \dots, N$) overlap in time mutually. In this case, the first mode is the same as the second mode.

The mode of operation of the RX relay will depend on the controlled process. Based on this, the times t_X and t_R can also be determined. In a sense, there are two conflicting requirements. The test time of the relay impacts the achieved safety level (that's why it is appropriate to change its state as often as possible), but from the life of the system point of view, it is suitable that the relay is not switched often (more frequent switching leads to increase its failure rate- relation (5)). Depending on the type of operation and the mode of operation of the relay, it may be switched-off for example at the beginning of a work shift. If the character of the controlled process is such that the time between switching the RX relay cannot be guaranteed, then the time t_X must be identified with the expected life of the system (t_X= 20 years).

From the curves, in Fig. 5 it can be seen that if $t_R < t_X$, the output part according to the Fig. 2 has a higher dangerous failure rate. However, if $t_R > t_X$, then, on the contrary, the output part dangerous failure rate according to Fig. 3 is worse than the connection according to Fig. 2.

In general, it can be assumed that applications in which are valid that $t_R < t_X$, will be more frequently realized than applications in which $t_X < t_R$, because with the increasing number of controlled EUCs, the time in which the RX relay could be switched decreases.

For the elements used in the case study is valid that from the safety point of view, the output circuit has an almost negligible effect on the SF dangerous failure rate. The failure rate of the output circuit is an order of magnitude lower than the input part dangerous failure rate and also the of logic. However, this only applies to the given relay and its application parameters. Improving the SF dangerous failure rate connection according to Fig. 3 in comparison with the connection according to Fig. 2 (Table 2) is mainly due to the smaller number of inputs and outputs used. The reason for this is that the smaller number of relays in the simplified connection of the output circuit (Fig. 3) also requires a smaller number of necessary inputs and outputs (with the same number of controlled EUCs).

VII. CONCLUSION

The paper deals in more detail only with the output part of the SRCS composed of relays and analyzes in more detail the case when one SF controls the EUCs. The safety of the realized safety function also affects the other parts of the SRCS, which are dealt with in more detail in other papers, e.g. [10], [11], [12], [13].

Increasing the number of relays in the output circuit has an adverse influence on the required failure state detection time of the output circuit (relation (10)). Ultimately, this can also have an adverse influence on the operation (need to change the state of the relay more often). Before such a solution is approached, it must be verified based on a risk analysis whether more than one SF can be used to control the EUCs. The failure of each SF is then evaluated separately, and for different SFs there may be a different requirement for the failure state detection time.

These procedures, stated in previous chapters, can be applied even if the output circuit will be realized by the electronic elements.

When selecting a specific output circuit, as well as the entire SRCS architecture, other required features must be also taken into account (especially availability, maintainability, and last but not least, also price). More detailed information about these properties can be found e.g. in [13], [14].

ACKNOWLEDGMENT

This work has been supported by the Educational Grant Agency of the Slovak Republic (KEGA) Number 008ŽU-4/2019: Modernization and expansion of educational possibilities in the field of safe controlling of industrial processes using the safety PLC.

REFERENCES

[1] EN 61508, “Functional safety of electrical/ electronic/programmable electronic safety-related systems,” 2010.

[2] EN 62061, “ Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems,“ 2016.

[3] EN ISO 13849, “Safety of machinery. Safety-related parts of control systems,” 2012.

[4] K. Rástočný, J. Ždánsky and, J. Hrbček, “The problems related to realization of safety function with SIL4 using PLC,” Proceedings of the 30th International Conference on Cybernetics and Informatics, Velke Karlovice, Czech Republic, 29 January 2020 through 1 February 2020, ISBN 978-1-7281-4380-4, 2020

[5] K. Rástočný, J. Ždánsky and J. Hrbček, “Using a safety PLC to Implement the Safety Function,” ASTES Journal, ISSN 2415-6698, Volume 6, Issue 1, p. 1072-1078, 2021.

[6] EN 60947-5-1, “Low-voltage switchgear and controlgear. Part 5-1: Control circuit devices and switching elements . Electromechanical control circuit devices,” 2020.

[7] EN 60947-4-1, “Low-voltage switchgear and controlgear.Part 4-1:Contactors and motor-starters.Electromechanical contactors and starters,” 2018.

[8] J. Ždánsky, K. Rástočný, “Influence of safety PLC parameters to response time of safety functions,” Proceedings of international conference applied electronics, Pilsen, Czech Republic, ISBN 978-80-261-0166-6, ISSN 1803-7232, pp. 327-330, 2013.

[9] J. Ždánsky, J. Valigurský and M. Medvedík, “Influence of architecture and parameters of SRCS on Safety function response time,” In: ELEKTRO 2020 conference proceedings, ISBN 978-1-7281-7541-6, p. 1-5, 2020.

[10] J. Ždánsky, K. Rástočný and M. Medvedík, “Safety of two-channel connection of sensors to safety PLC”, In: ELEKTRO 2020 conference proceedings, ISBN 978-1-7281-7541-6, p. 1-5, 2020.

[11] J. Ždánsky, K. Rástočný and J. Hrbček, “Influence of architecture and diagnostic to the safety integrity of SRECS output part,” Proceedings of international conference Applied Electronics, Pilsen, Czech Republic, ISBN 978-80-261-0385-1, ISSN 1803-7232, pp. 297-301, 2015.

[12] P.Cuninka, P. Zavacky and M. Stremy, “Influence of Architecture on Reliability and Safety of the SRCS with Safety PLC,” Proceedings of 2nd International Conference on Mathematics and Computers in Sciences and in Industry, Sliema, Malta, ISBN: 978-147998673-6, p. 225-230, 2015.

[13] H. Ahangari, F. Atik, Y.I. Ozkok, S.O. Ata, O. Ozturk, “Analysis of design parameters in safety-critical computers,” In Journal IEEE Transactions on Emerging Topics in Computing, Volume 8, Issue 3, ISSN 2168-6750, p. 712-723, 2020.

[14] J. Koziorek, A. Gavlas, J. Konecny, M. Mikolajek, R. Kraut, P Walder, “Automated control system design with model-based commissioning,” In International Journal of Circuits, Systems and Signal Processing, Volume 13, 2019, Publisher: North Atlantic University Union NAUN, ISSN:1998-4464, p. 6-12, 2019.