ACTA TEHNICA CORVINIENSIS – Bulletin of Engineering
Tome VIII [2015] Fascicule 1 [January – March]
ISSN: 2067 – 3809

[1.] Juraj ŽDÁNSKY, [2.] Karol RÁSTOČNÝ

INFLUENCE OF REDUNDANCY ON SAFETY INTEGRITY OF SRCS WITH SAFETY PLC

[1-2.] Department of Control and Information Systems, University of Žilina, Faculty of Electrical Engineering, Žilina, SLOVAKIA

Abstract: PLCs produced at present have incomparably wider range of application options than PLCs produced in the past. One of the options where the using of PLC has not yet been common is the safety-critical processes control. PLCs used for this purpose form a special category of PLCs and are known as safety PLCs. Safety PLCs (Programmable Logic Controller) are one of the appropriate tools for implementation of safety-related control system (SRCS). Their modular construction allows implementation not only control systems of defined safety integrity level (SIL), but even redundant control systems with defined availability. The contribution considers influence of redundant architectures on safety integrity of SRCS with safety PLC.
Keywords: SRCS, safety PLC, safety integrity level, probability of failure state, redundancy

INTRODUCTION

PLCs produced at present have incomparably wider range of application options than PLCs produced in the past. As an example of the PLC application options expansion can be mentioned [1], [2], [3]. One of the options where the using of PLC has not yet been common is the safety-critical processes control. PLCs used for this purpose form a special category of PLCs and are known as safety PLCs.

Attribute of safety PLC is after failure transition with defined probability into pre-defined safe state (it's an attribute marked as fail-safe). For all commercially available safety PLCs, safe state is considered as state in which output is disconnected - state without power (logical level 0 in output). This attribute is related to safety PLC, not to SRCS which also includes a safety PLC. Safety PLCs are primarily used for the implementation of SRCS at process level, therefore sensors and actuators must also be considered as a part of SRCS[4].The basic parts of safety PLC consist of sensors, F-I module/modules (Fail-safe Input module), F-CPU (Fail-safe Central Processing Unit), F-DO module/modules (Fail-safe Digital Output module) and actuators (Figure 1.).Due to the safety functions implemented by SRCS for example contactors can be used instead of actuators, as it's considered in this contribution.

By combining the different architectures of the input part, the logic and the output part, a wide range of architectures of SRCS with safety PLC can be achieved. The contribution is more detailed about the output part architectures of SRCS with safety PLC. Influence of some input part architectures on the reliable and safety properties of SRCS is given for example in [5].

The fundamental difference in manufactures attitude to ensuring required availability and safety of safety PLC is that some manufacturers observe these properties separately (they offer PLC with increased availability and safety PLC with increased safety) and some manufactures offer safety PLC with modular architecture, which allows synchronously observing of availability and safety increasing of created SRCS.

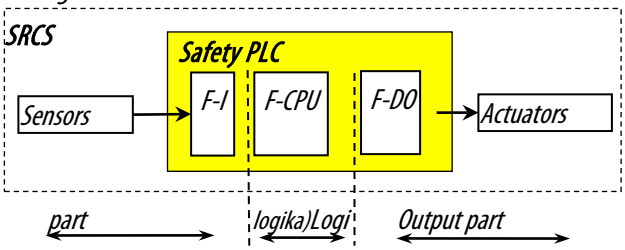

Figure 1. Basic parts of SRCS with safety PLC

As the achievement of required safety properties, as well as the achievement of required availability is implemented by appropriate application of redundancy. Literature relating to the SRCS with safety PLC often says about using of redundancy only in the context of increasing availability. This specificity is due to the fact that the redundancy associated with increasing safety properties is mainly applied in the modules of the safety PLC and therefore from user viewpoint it's "invisible" redundancy. Conversely, the redundancy associated with increasing availability is from the user viewpoint "visible", because it's implemented by using number of modules the same type.

From this viewpoint SRCS with safety PLC can be divided to:

- ✓ SRCS with safety PLC without redundancy;
- ✓ SRCS with safety PLC with redundancy.

In this understanding, objective of redundancy of SRCS with safety PLC is enhancing its reliable properties (in relation to the availability of SRCS). This doesn't automatically lead to an increase of its safety integrity. The contribution refers the interdependencies between the influence of redundancy of SRCS with safety PLC on safety integrity (expressed through the dangerous failure rate) and on the probability of failure state of SRCS with safety PLC.

© copyright Faculty of Engineering - Hunedoara, University POLITEHNICA Timisoara

EVALUATION OF RELIABILITY AND SAFETY INTEGRITY OF SRCS WITH SAFETY PLC

If we want to observe the redundancy influence on reliable and safety properties of a system, it's necessary to establish indicators by which we will evaluate reliability and safety integrity. In this contribution the observed properties are evaluated considering consequences of the random hardware failure. The software evaluation isn't object of this contribution (software evaluation is based on qualitative methods).

In the next section of this contribution let's assume that:

- ✓ *individual considered parts of SRCS are independent of each other in the meaning that an occurrence of failure in one part of SRCS doesn't affect the probability of failure in other part of SRCS;*
- ✓ *SRCS implement one safety function and thus SIL SRCS correspond to the SIL of the safety function.*

Then the probability of SRCS failure state (decomposed according to Figure 1) can be expressed by term:

$$P(t) = P_I(t) + P_L(t) + P_O(t) - P_I(t).P_L(t) - P_I(t).P_O(t) - P_L(t).P_O(t) + P_I(t).P_L(t).P_O(t)$$

where $P_I(t)$, $P_L(t)$ and $P_O(t)$ are probabilities of failure state of the input part, the logic and the output part of SRCS.

The safety integrity level for SRCS is expressed by the dangerous failures rate per hour and the function [6]. The dangerous failures rate for SRCS according to Figure 1 can be expressed by term:

$$\lambda_H(t) = \lambda_{HI}(t) + \lambda_{HL}(t) + \lambda_{HO}(t)$$

where $\lambda_{HI}(t)$, $\lambda_{HL}(t)$ and $\lambda_{HO}(t)$ are dangerous failures rates of the input part, the logic and the output part of SRCS.

THE OUTPUT PART OF SRCS WITH SAFETY PLC WITHOUT REDUNDANCY

In the above given output part architectures, we consider one controlled value. Implementation of specific safety function may require more controlled values and therefore a greater number of F-DO modules and actuators. Analysis of reliable and safety properties of the output part of SRCS with safety PLC must cover all actuators and F-DO modules that are involved in the implementation of the safety function.

Connection with one actuator

Connection of the output part with one actuator (Figure 2) may be used if the F-DO module and also the connected actuator comply the required SIL.

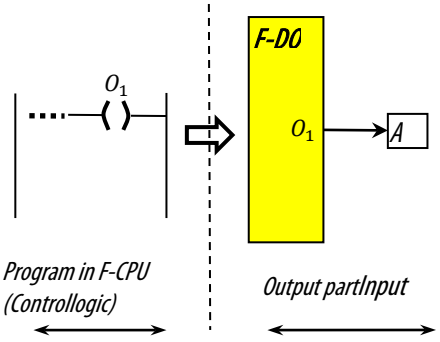

Figure 2. *Connection of the output part with one actuator*

For the probability of failure state of the output part of SRCS with one actuator (Figure 2) is valid:

$$P_O^{1A}(t) = 1 - \big(1 - P_A(t)\big)\big(1 - P_{DO}(t)\big)$$

where $P_A(t)$ is the probability of failure state of actuator A and $P_{DO}(t)$ is the probability of failure state of F-DO module.

For dangerous failures rate of the output part of SRCS with one actuator (Figure 2) is valid:

$$\lambda_{HO}^{1A}(t) = \lambda_{HA}(t) + \lambda_{HDO}$$

where $\lambda_{HA}(t)$ is the dangerous failures rate of actuator A and λ_{HDO} is the dangerous failures rate of F-DO module.

Connection with two actuators

Connection with two actuators (Figure 3) may be used if actuator with the required SIL isn't available. This connection doesn't impose special requirements on the safety properties of actuators and presumes safe disconnection of controlled object RO from the power source (due to the serial actuators connection).

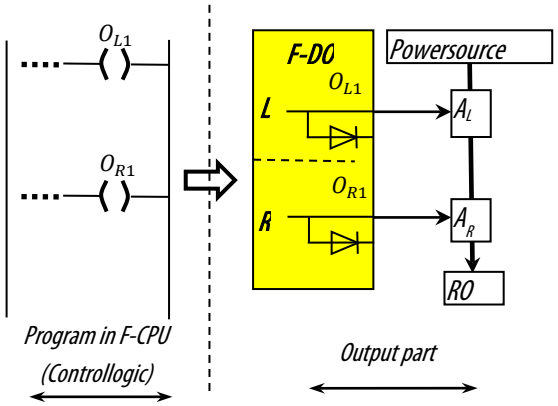

Figure 3. *Connection of the output part with twoactuators*

For the probability of failure state of the output part of SRCS with two actuators (Figure 3) is valid:

$$P_O^{2A}(t) = 1 - \big(1 - P_{AL}(t)\big)\big(1 - P_{AR}(t)\big)\big(1 - P_{DO}(t)\big)$$

where $P_{AL}(t)$, respectively $P_{AR}(t)$ is the probability of failure state of actuator A_L, respectively A_R and $P_{DO}(t)$ is the probability of failure state of F-DO module.

For the dangerous failure rate of the output part of SRCS with two actuators (Figure 3) is valid:

$$\lambda_{HO}^{2A}(t) = \frac{\frac{dP_{HA}(t)}{dt}}{1 - P_{HA}(t)} + \lambda_{HDO}$$

where $P_{HA}(t)$ is the probability of dangerous failure of actuators pair A_L and A_R, λ_{HDO} is the dangerous failures rate of F-DO module.

The probability of dangerous failure of actuators pair A_L and A_R can be expressed by term:

$$P_{HA}(t) \le P_{AL}(t).P_{AR}(t)$$

The probability value $P_{HA}(t)$ depends on the detection time with the failure negation time of actuators (the failure negation time is due to the failure detection time generally negligible).The failure detection of actuators can be implemented by functional or test diagnostics (the actuators diagnostics isn't shown in pictures in this contribution).For the implementation of functional diagnostics is possible to consider the failure detection time as the maximum time between operational commands for changing of actuators state. For the implementation of the test diagnosis is possible to consider the failure detection time as the maximum time between the executions of test procedures.

For considerations in the next section of this contribution is valid:

- *the failure detection time with the failure negation time is t_{0A};*
- *the random failures rates of actuators are constant (exponential distribution of the failures occurrence).*

Then the probability of dangerous failure of actuators pair A_L and A_R can be expressed by term:

$$P_{HA}(t_{0A}) \leq \left(1 - e^{-\lambda_{AL}.t_{0A}}\right).\left(1 - e^{-\lambda_{AR}.t_{0A}}\right)$$

where λ_{AL}, respectively λ_{AR} is the random failures rate of actuatorA_L, respectively A_R.

If $\lambda.t \ll 1$, so the dangerous failures rate of actuators pairA_L and A_R can be determined by term:

$$\lambda_{HALR}(t_{0A}) \cong 2.\lambda_{AL}.\lambda_{AR}.t_{0A}$$

The dangerous failures rate of the output part of SRCS with two actuators can be determined by term:

$$\lambda_{HO}^{2A}(t_{0A}) \leq \lambda_{HDO} + \lambda_{HALR}(t_{0A})$$

where λ_{HDO} is the dangerous failures rate of F-DO module.

THE OUTPUT PART OF SRCS WITH SAFETY PLC WITH REDUNDANCY

Redundancy at actuators level

If the safety properties of actuators are significantly worse than the safety properties of F-DO module it's appropriate to apply redundancy at actuators level. The actuators control must be solved in the application program. The principle of actuators control is shown in Figure 4.

For the probability of failure state of the output part of SRCS with redundancy at actuators level (Figure 4.) is valid:

$$P_O^{RA}(t) = 1 - \left(1 - P_{A1}(t).P_{A2}(t)\right)\left(1 - P_{DO}(t)\right)$$

Where $P_{A1}(t)$ is the probability of failure state of actuators pairA_{L1} and A_{R1} and $P_{A2}(t)$ is the probability of failure state of actuators pairA_{L2} and A_{R2} and $P_{DO}(t)$ is the probability of failure state of F-DO module.

The probability of failure state of actuators pairA_{L1} and A_{R1} can be expressed by term:

$$P_{A1}(t) = 1 - \left(1 - P_{AL1}(t)\right)\left(1 - P_{AR1}(t)\right)$$

where $P_{AL1}(t)$, respectively $P_{AR1}(t)$ is the probability of failure state of actuator A_{L1}, respectively A_{R1}.

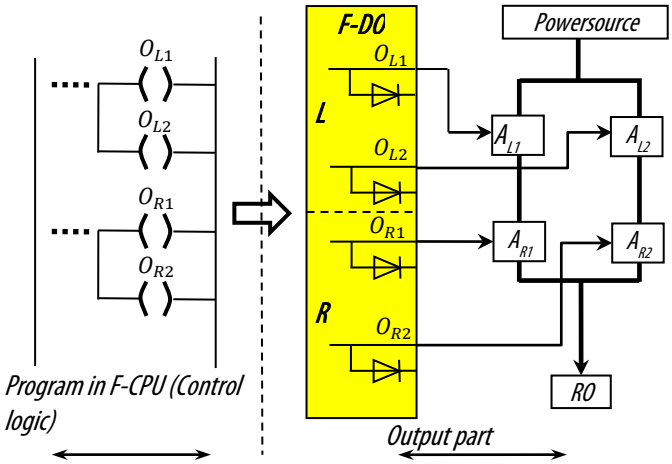

Figure 4. *Connection of the output part with redundancy at actuators level*

The probability of failure state of actuators pair A_{L2} and A_{R2} can be expressed by term:

$$P_{A2}(t) = 1 - \left(1 - P_{AL2}(t)\right)\left(1 - P_{AR2}(t)\right)$$

where $P_{AL2}(t)$, respectively $P_{AR2}(t)$ is the probability of failure state of actuatorA_{L2}, respectively A_{R2}.

For the dangerous failures rate of the output part of SRCS with redundancy at actuators level (Figure 4) is valid:

$$\lambda_{HO}^{RA}(t_{0A}) \leq 2.\lambda_{AL1}.\lambda_{AR1}.t_{0A} + 2.\lambda_{AL2}.\lambda_{AR2}.t_{0A} + \lambda_{HDO}$$

where λ_{AL1}, λ_{AR1}, λ_{AL2} and λ_{AR2} are random failures rates of actuators A_{L1}, A_{R1}, A_{L2} and A_{R2}.

Redundancy at F-DO modules level

Redundancy at F-DO modules level can be implemented (Figure 5) but requires the application of additional measures. Objective of these measures is to prevent short circuit of outputs of modulesF-DO1 and F-DO2 (by two outputs it's necessary to control one actuator).In assessing the reliable and safety properties of the output part with redundancy at F-DO modules level it's necessary to analyse the influence of the implemented measures. There is in Figure 5 preventing the short circuit realized by the separating diodes.

There are also F-DO modules that have measures to prevent the short circuits implemented by internal circuits of the module. In this case there is no need to deal with the analysis of the safety of these measures.

It's necessary to set the redundancy at F-DO modules level by using the F-DO modules parameters (not every type of safety PLC supports this type of connection). Then a user accesses the modules pair F-DO1 and F-DO2 as in the case of one module.

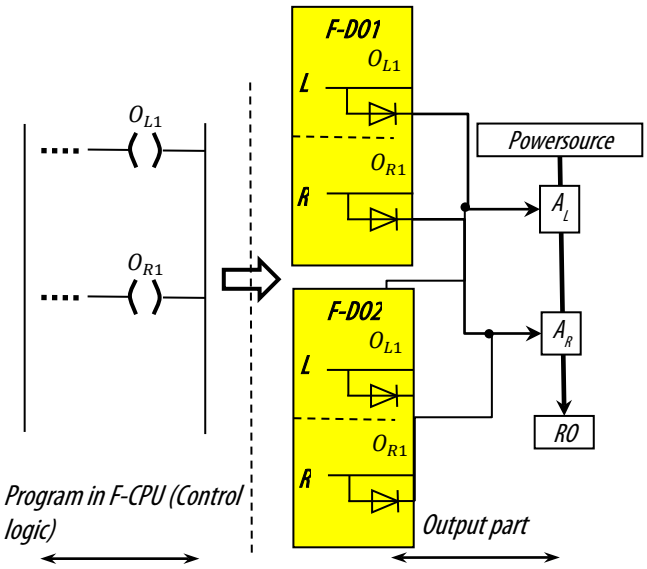

Figure 5. *Connection of the output part with redundancy at F-DO modules level*

The probability of failure state of the output part of SRCS with redundancy at F-DO modules level (Figure 5.) can be expressed by term (assuming that measures to prevent short circuits are realized by internal circuits of the module):

$$P_O^{RM}(t) = 1 - \left(1 - P_{AL}(t)\right)\left(1 - P_{AR}(t)\right)\left(1 - P_{DO1}(t).P_{DO2}(t)\right)$$

where $P_{AL}(t)$, respectively $P_{AR}(t)$ is the probability of failure state of actuator A_L, respectively A_R and $P_{DO1}(t)$, respectively

$P_{DO2}(t)$ *is the probability of failure state of the module F-DO1, respectively F-DO2.*

The dangerous failures rate of the output part of SRCS with redundancy at F-DO modules level (Figure 5.) can be expressed by term:

$$\lambda_{HO}^{RM}(t_{0A}) \leq 2.\ \lambda_{AL}.\lambda_{AR}.t_{0A} + \lambda_{HDO1} + \lambda_{HDO2}$$

where λ_{HDO1}*, respectively* λ_{HDO2} *is the dangerous failures rate of the module F-DO1, respectively F-DO2.*

Redundancy at actuators and F-DO modules level

If the reliable properties of the actuators pair A_L *and* A_R *aren't sufficient and reliable properties of F-DO module also aren't sufficient, the connection according to Figure 6 can be used.*

For the probability of failure state of the output part of SRCS with redundancy at actuators and F-DO modules level (Figure 6.) is valid:

$$P_O^{RAM}(t) = P_{O1}^{2A}(t).P_{O2}^{2A}(t)$$

where $P_{O1}^{2A}(t)$ *is the probability of failure state of the first channel (components F-DO1,* A_{L1} *and* A_{R1}*) and* $P_{O2}^{2A}(t)$ *is the probability of failure state of the second channel(components F-DO2,* A_{L2} *and* A_{R2}*).* $P_{O1}^{2A}(t)$ *and* $P_{O2}^{2A}(t)$ *can be determined by term (5).*

The dangerous failures rate of the output part of SRCS with redundancy at actuators and F-DO modules level (Figure 6) can be expressed by term:

$$\lambda_{HO}^{RSM}(t_{0A}) \leq 2.\lambda_{AL1}.\lambda_{AR1}.t_{0A}$$
$$+2.\lambda_{AL2}.\lambda_{AR2}.t_{0A} + \lambda_{HDO1} + \lambda_{HDO2}$$

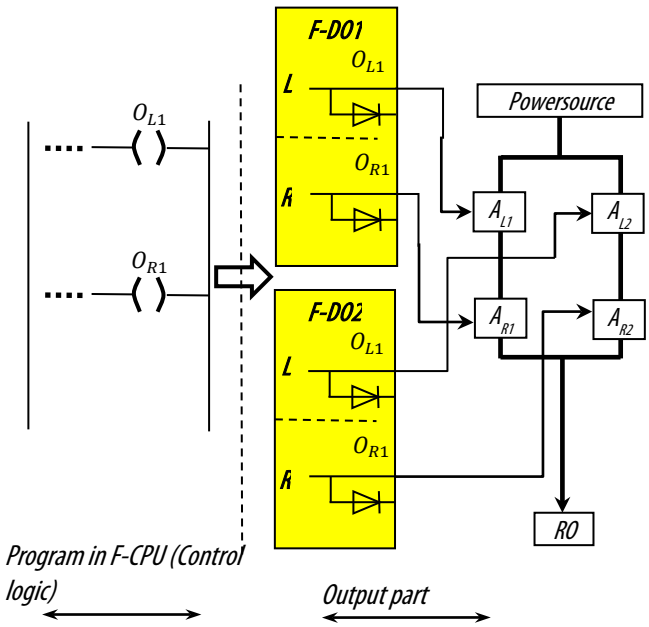

Figure 6. *Connection of the output part with redundancy at actuators and F-DO modules level*

THE PROPERTIES COMPARISON OF INDIVIDUAL ARCHITECTURES

Curves comparing the architectures of the output parts of SRCS with safety PLC are shown in Figure 7 and Figure 8. And are built for SRCS with safety PLC Simatic (reliable parameters of components of Simatic system can be found in [7] and safety parameters are part of the technical documentation of individual modules). Estimated random failures rate of actuators is 5.10^{-6} h^{-1}.

For both images applies the curves numbering according to Table 1.

Table 1. *Curves numbering in Figure 7 and Figure 8*

Curve number	Corresponding architecture
1	Connection of the output part with twoactuators (Figure 3); terms (5) and (10).
2	Connection of the output part with redundancy at actuators level (Figure 4); terms (11) and (14).
3	Connection of the output part with redundancy at F-DO modules level (Figure 5); terms (15) and (16).
4	Connection of the output part with redundancy at actuators and F-DO modules level (Figure 6); terms (17) and (18).

The graph in Figure 7 shows curves of the probability of failure state of the output parts of SRCS with safety PLC. From these curves the influence of redundancy on the probability of failure state of individual architectures of the output part of SRCS with safety PLC is obvious.

There are in Figure 8.curves of the dangerous failures rates of the output parts of SRCS with safety PLC depending on the failure detection time with the failure negation time of the actuator(t_{0A}*).*

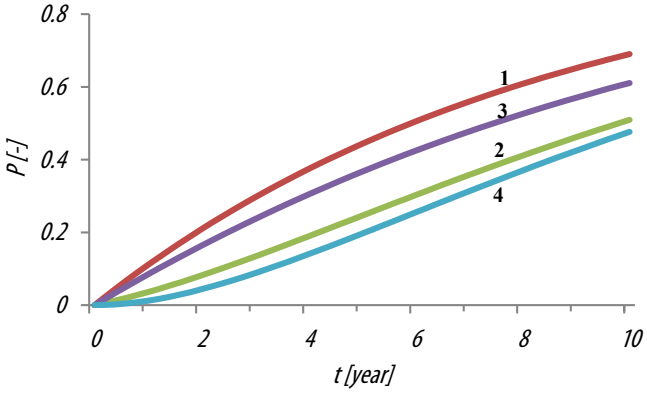

Figure 7. *The probability of failure state of the output parts of SRCS*

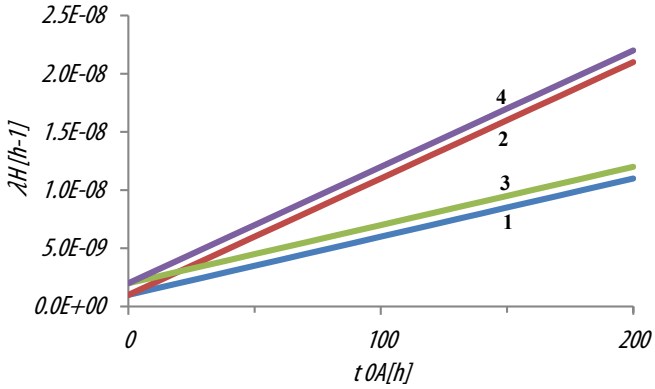

Figure 8. *The dangerous failures rate of the output partsof SRCS*

From the graphs in Figure 7 and Figure 8 can be seen that by influence of using the redundancy we can achieve an improvement of the reliability (reducing the probability of failure state) but it also leads to deterioration of safety integrity (increase of the dangerous failures rate).This is caused by influencing the safety of the output part of SRCS with redundancy by parts forming the reserve.

There isn't in graphs in Figure 7 and Figure 8 curve corresponding to the architecture of the output part with one actuator (Figure 2). It's because this architecture requires an actuator satisfying the required SIL. Such an actuator has different parameters (the probability of

failure state and dangerous failures rate) as actuators used in other architectures and therefore a comparison of such architecture with the other architectures loses its meaning.

CONCLUSION

Reliable and safety properties of SRCS with safety PLC can be influenced by the choice of an appropriate SRCS architecture. Choice of architecture shouldn't be based only on observing one property because its improvement doesn't automatically mean improvement of other properties. Architecture should be chosen so as to fulfil the minimum required level of all observed properties.

Acknowledgment

This paper was supported by the scientific grant agency VEGA, grant No. VEGA-1/0388/12 "Quantitative safety integrity level evaluation of control systems in railway application".

References

[1] *T. Skulavik, M. Kopček, A. Kopčeková, "Fuzzy Control of Robotic Arm Implemented in PLC",IEEE 9th International Conference on Computational Cybernetics 2013, pp. 45-49, ISBN 978-1-4799-0061-9, Tihany, Hungary, 2013.*

[2] *J. Hrbček,V. Šimák, "Implementation of Multi-dimensional Model Predictive Control for Critical Process with Stochastic Behavior", chapter in: Advanced Model Predictive Control, p.109-124, InTech, Tao Zheng (Ed.), ISBN 978-953-307-298-2, 2011.*

[3] *M. Kopček, G. Križanová, "Models used for PID controller and PLC programming teaching", Process Control 2008 : Proceedings of the 8th International Scientific-Technical Conference. Kouty nad Desnou, Czech Republic, June 9-12, 2008. - Pardubice : University of Pardubice, ISBN 978-80-7395-077-4, 2008.*

[4] *K. Rástočný, J. Ždánsky, "Riadiace systémy so safety PLC", EDIS - vydavateľstvo ŽU, Žilina, ISBN 978-80-554-0681-7, 2013.*

[5] *J. Ždánsky, P. Nagy, "Influence of the Control System Structure with Safety PLC on its Reliability and Safety", Proceedings of the 9th international conference ELEKTRO 2012, Rajecké Teplice, IEEE Catalog Number: CFP1248S-ART, p. TA4_25, ISBN 978-1-4673-1178-6, 2012*

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

[7] *MTBF_2009-04.xls. Available at http://www.nwe.siemens.com/denmark/ internet/dk/industry/information/Software_vejledninger/Documents/MTBF_2009-04.xls.*

ACTA Technica CORVINIENSIS
BULLETIN OF ENGINEERING
ISSN:2067-3809

copyright ©
University POLITEHNICA Timisoara, Faculty of Engineering Hunedoara,
5, Revolutiei, 331128, Hunedoara, ROMANIA
http://acta.fih.upt.ro