TRENDS IN CONTROL AREA OF PLC RELIABILITY AND SAFETY PARAMETERS

J. Ždánsky[1], J. Hrbček[2], J. Zelenka[3]

[1] Katedra riadiacich a informačných systémov, Elektrotechnická fakulta, Žilinská univerzita, Veľký diel, 010 26 Žilina, tel.: +421 513 3342, mail: juraj.zdansky@fel.uniza.sk
[2] Katedra riadiacich a informačných systémov, Elektrotechnická fakulta, Žilinská univerzita, Veľký diel, 010 26 Žilina, tel.: +421 513 3354, mail: jozef.hrbcek@fel.uniza.sk
[3] Katedra riadiacich a informačných systémov, Elektrotechnická fakulta, Žilinská univerzita, Veľký diel, 010 26 Žilina, tel.: +421 513 3334, mail: jan.zelenka@fel.uniza.sk

Summary: Extension of the PLC application possibilities is closely related to increase of reliability and safety parameters. If the requirement of reliability and safety parameters will be suitable, the PLC could by implemented to specific applications such the safety-related processes control. The goal of this article is to show the way which producers are approaching to increase PLC`s reliability and safety parameters. The second goal is to analyze these parameters for range of present choice and describe the possibility how the reliability and safety parameters can be affected.

1. INTRODUCTION

One of the appropriate tools to realize automatic control are the programmable logic controllers (PLC) with their circuit and technological solution. The characteristic attributes of PLC are: programmability, ability for reconfiguration, robustness and quickness. Because of these characteristics of PLCs, they are becoming favorite devices for various problems solution. Nowadays a wide assortment of PLC is accessible by many various manufacturers. Their application possibility, comfort by programming and tuning makes from PLC the tools to by incomparable with any previous other (the beginning of development of PLC). Nowadays the main trends belong to increase the reliability and safety parameters of PLC.

The basic differences between provider's approaches are:

- some providers pay attention to reliability and safety parameters separately (they offer PLC with enhanced safety and enhanced reliability parameters).
- others providers offers the PLC with modular structure which allows pay attention to booth enhanced safety and enhanced reliability parameters as well.

2. RELIABILITY PARAMETERS OF PLC

By ordinary control processes (not safety critical) the requirement to specific application can lead to enhanced safety parameters of control system. The suitable parameter for qualitative expression of reliability can be control system availability. Availability is probability that system occur in the state to be able perform a desired function by given requirement and in any moment or given time interval provided that required maintenance tool are at their disposal [1]. PLC that fulfils the conditions for minimum level of availability can be chosen according to availability model of PLC.

If we deal with common PLC then availability can by represent by Markovov diagram according to Fig.1. Diagram consists of failure-free state of PLC (state 1) and failure state of PLC (state 2). Transition rate from state 1 to state 2 matches with fault intensity of PLC - λ. Transition rate (from state 2 to state 1) matches with renewal intensity of PLC after failure - γ.

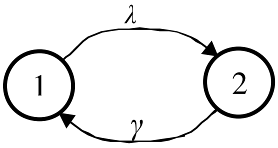

Fig. 1. Markovov diagram represents availability PLC without redundancy

Availability (according to Fig.1.) is probability that system occur in the state 1. Equation for computation of this probability can be deduced from differential equations, with which can we describe Markovov diagram on Fig. 1. For this probability computation from differential equations is deduced formula that can be the Markovov diagram on Fig. 1. described.

$$p_1(t) = 1 - \frac{\lambda}{\gamma + \lambda}\left(1 - e^{-(\gamma+\lambda)t}\right). \qquad (1)$$

Failure intensity of PLC can be computed from equation:

$$\lambda = \sum_{i=1}^{n} \lambda_i \ , \qquad (2)$$

where λ_i is failure intensity of i's module and n is quantity of modules which PLC is compound.
PLC renewal intensity after failure is:

$$\gamma = \frac{1}{MDT}, \qquad (3)$$

where the MDT (Mean Down Time) is mean time of unworkable state of PLC.

Availability is the time related value which in time t→∞ is equal to so-called availability coefficient A^K . It's a deal, that

$$A^K = \lim_{t\to\infty}\left(1-\frac{\lambda}{\gamma+\lambda}\left(1-e^{-(\gamma+\lambda)t}\right)\right)=\frac{\gamma}{\gamma+\lambda}. \qquad (4)$$

In general we can for arbitrary system specify the availability coefficient from data from real process according to the equation:

$$A^K = \frac{MUT}{MUT+MDT}, \qquad (5)$$

where the MUT (Mean Up Time) is mean time of useable state of PLC and the MDT (Mean Down Time) is mean time of unworkable state of PLC. If the availability of common PLC is convenient for requirement of given application, it is necessary to implement the redundancy to control system. It can be realize using two PLC and their mutual cooperation to be able replace the failure PLC by the second PLC. On the Fig. 2. and Fig. 3. are represent two most often used PLC structure with witch can be enhanced the availability of control system.

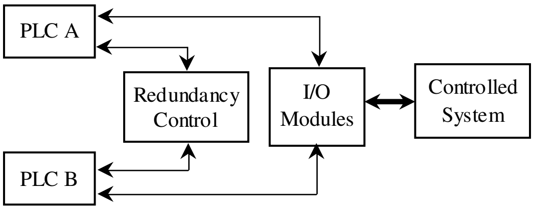

Fig. 2. Redundancy control principle by co-operative modules.

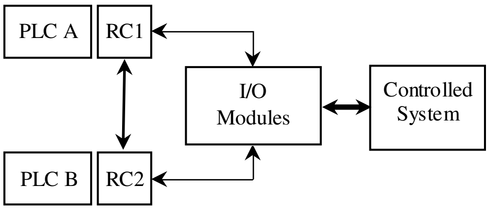

Fig. 3. Redundancy control principle by independent modules.

Function of circuit on the Fig. 2. is controlled by the redundancy control block. Working principle rests in that, that input-output modules are in failure-free state controlled by PLC A and after failure of PLC A, the PLC B takes his function. By this solution is created the space for PLC A restoration. Company Teco a.s use this technique to combine their PLC [2]. Another one possibility how to control cooperation of two PLC to achieve enhanced availability is on the Fig. 3. In this case for coordination the PLC A and PLC B are used two autonomous modules (RC1 and RC2). Company Allen Bradley use this technique [3]. To compute the availability structure, according to Fig. 2. we can deduce a following equations:

- Availability of redundancy system controlled by co-operative module:

$$A_{CM}(t)=\left(1-\left(1-A_{PLC_A}(t)\right)\left(1-A_{PLC_B}(t)\right)\right).A_{RC}(t).A_{IO}(t), \qquad (6)$$

where $A_{PLC_A}(t)$ and $A_{PLC_B}(t)$ are availability of PLC A and PLC B, $A_{RC}(t)$ is a redundancy control module availability and $A_{IO}(t)$ is availability of input-output modules. Availability of separate components we can determine according to the term (1).

- Availability of redundancy system controlled by independent module:

$$A_{IM}(t)=\left(1-\left(1-A_{PLC_A}(t)A_{RC1}(t)\right)\left(1-A_{PLC_B}(t)A_{RC2}(t)\right)\right).A_{IO}(t) \qquad (7)$$

On the Fig. 4. and Fig. 5. are the characteristics of availability of these structure for comparison. The characteristics on Fig. 4. are made by hypothesis that redundancy control modules failure intensity λ_{RC} is significant equal that failure intensity PLC λ_{PLC}.

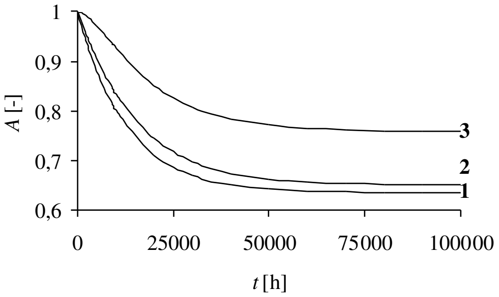

Fig. 4. Availability for λ_{RC}= λ_{PLC}=2.10^{-5} h^{-1}

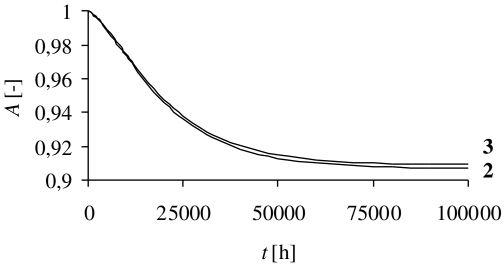

Fig. 5. Availability for $\lambda_{RC} << \lambda_{PLC}$ (λ_{RC}=2.10^{-7} h^{-1}; λ_{PLC}=2.10^{-5} h^{-1})

The characteristics No. 1 represent availability of control system without redundancy. His availability is lower then any of all characteristics. The characteristics No. 2 represents availability of redundancy control system with cooperation by mutual module (Fig. 2.) and the characteristics No. 3 represents availability of redundancy control system with cooperation by two independent modules (Fig. 3.). From the characteristics is evident that in both case redundancy add to availability of control system. But the availability increase significantly according to wiring on Fig. 3. (Redundancy control principle by independent modules). It's so because of by the redundancy control principle by independent modules (Fig. 2.)

is this module from the availability side the feeblest place. More perfectly solution of this wiring we can achieve by decreasing failure intensity of redundancy modules in comparison to PLC. This example is shown on Fig. 5. (failure intensity of control system modules is of two dimension lower as failure intensity of PLC).

3. PLC SAFETY PARAMETERS

By control the safety-critical system, the choice of appropriate control system is a bit complicated as the choice of control system by common processes, possibly the processes with higher safety requirement. Typical example is safety-critical control with continuous running. In this case the control must be working after failure of control system too (failure of control system wont be endanger safety of controlled system – it is primary safety) and in most cases after control system failure the human take over control task. The human mistake can lead to safety threat of control system (secondary safety). For this reason is safety depend not only on safety parameters of control system (express as dangerous failure intensity) but also depends on their reliability parameters. That's why to say about so-called RAMS (*Reliability, Availability, Maintability, Safety*) parameters. To achieve the required safety level it is necessary choose the control system structure to fulfil the minimum values of mentions parameters. PLC providers offer so-called safety PLC to control safety-critical processes. Safety PLC are designated for common use. Trouble of their application to control safety-critical processes related to individuality review of safety level. Using the safety PLC not guaranteed safety of control system in complexly. With suitable models we can choose from providers offer suitable structure of PLC to make easily the implementation of safety-critical control system.

3.1 PRESENT STATE IN SAFETY PLC AREA

Technical safety of PLC reaches the producers by various precautions. The collective goal of these precautions is to reach required value (satisfactory low) of dangerous failure rate. Dangerous failure rate values for required safety integrity level (SIL 1 to SIL 4) are defined in [4]. For lower safety integrity level is the simples possibility use the standard PLC without redundancy. Standard PLC for using in safety critical application for integrity level SIL 1 and SIL 2 offer for example Allen Bradley Company. This solution assumes application of modules which failure rate is satisfy low (the catalogue of modules by Allen Bradley Company, suitable for this purpose is in document [5].

To achieve the higher security level as SIL 2 is necessary use a redundancy. Producers apply the redundancy to PLC by various ways. From the customer's side is the simplest solution this which safety PLC present as its compact entirety with minimum choices of configuration. This solution is suitable only for special-purpose application. The typical example is Simotion Safety Unit (unit for press control) by Siemens Company [6].

By the growing universality of safety PLC the variants of use is growing too (various structure) and many configurable parameters of PLC are added. The choice of structure and parameters tuning can significantly affect to safety integrity level of PLC. Optimal attribute setting similarly as PLC structure choice can be realized on a basis of model. Effect of variable parameters of PLC to safety of control system can be suitably shown on the method of connection and data evaluation by sensors and actuators to control system.

3.2 CONNECTION OF SENSORS AND ACTUARORS

It is necessary to pay attention for choice of sensors and their connection and setting methods and setting of related parameters because by producer's statement (see [5]) is 90 per cent of dangerous failure made by sensors failure and actuators and only 10 per cent is produced by failure of PLC. Multi-channel connections of sensors are suitable for mostly of before mentioned safety integrity levels. On Fig. 6. is shown two-channel sensors connection. The input module is divided into left and right part. Every value is scanning by two sensors, at which each sensor is evaluate separately. If the information from both sensors is the same, the resultant information is considered to be right. Probability of dangerous failure of this case of sensors connection will be:

$$N_i = N_{S_{Li}}.N_{S_{Ri}}\,, \tag{8}$$

where $N_{S_{Li}}$ is probability of i-th sensor dangerous failure connected to left channel and $N_{S_{Ri}}$ is probability of dangerous failure of i-th sensor connected to right channel. If we suppose exponential distribution of sensors failure occurrence we can the equation (8) modify as follows:

$$N_i = (1 - e^{-\lambda^N_{SLi}.t_p})(1 - e^{-\lambda^N_{SRi}.t_p})\,, \tag{9}$$

where λ^N_{SLi} a λ^N_{SRi} is dangerous failure rate of sensors connected to left channel and right channel and t_p is permitted time of reciprocal mismatch between both channels (this time is one of tunable safety PLC parameters). Mentioned way of sensors connection and theirs suitable evaluate we can achieve relatively good safety parameters. This way makes worse the availability because availability of sensors pair will by:

$$A_i = A_{S_{Li}}.A_{S_{Ri}}\,, \tag{10}$$

where $A_{S_{Li}}$ is availability of i-th sensors connected to left channel and $A_{S_{Ri}}$ is availability of i-th sensors connected to right channel.

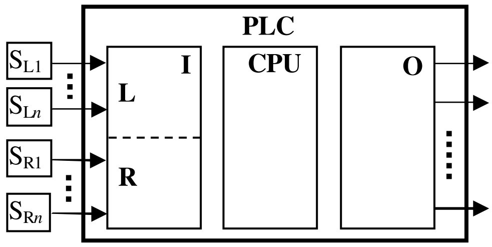

Fig. 6. Two-channel sensors connection

On the assumption of exponential distribution of sensors failure occurrence we can the equation (10) modify as follows:

$$A_i = e^{-(\lambda_{SLi}+\lambda_{SRi})t_p}, \tag{11}$$

where λ_{SLi} and λ_{SRi} is failure rate of i-th sensor connected to left and right channel. If sensors availability in this connection not satisfy the specify requirements, we can use the complicated PLC structure, in which each value will be measured by fourth sensors. By fault of one pair sensors measurement will be realize by second pair of sensors. This structure is convenient for higher reliabilities requirement. Availability of this sensors connection will be:

$$A_i = 1-(1-A_i^1)(1-A_i^2), \tag{12}$$

where A_i^1 and A_i^2 is availability of first and second pair of sensors. This availability can be computed from equation (10) or (11).

On Fig. 7. are represent the characteristics of probability of dangerous failure of pair sensors (characteristic No. 2; connection according to Fig. 6.) and probability of one sensor dangerous failure (characteristic No. 1; standard connection of sensor). From the characteristics is evident that two channels connection lead to reduction probability of sensors dangerous failure.

The characteristics are time-dependent. By regarding to exponential distribution attribute (characteristics are made on the assumption of exponential distribution of sensors failure occurrence) we can the maximum of dangerous failure affected by allowed time-discrepancy setting (t_p).

Similar ways lead to achieve the required reliability and safety parameters of actuators, or by autonomous control system.

Dangerous failure rate of separate components of control system effect to dangerous failure rate of whole control system we can formulate by:

$$\begin{aligned}N &= N_{SN}+N_{CS}+N_{AC}-N_{SN}N_{CS}-N_{SN}N_{AC}-\\&-N_{CS}N_{AC}+N_{SN}N_{CS}N_{AC}\end{aligned} \tag{13}$$

where N_{SN}, N_{CS} and N_{AC} are probability of dangerous failure of sensors parts, control system and actuators.

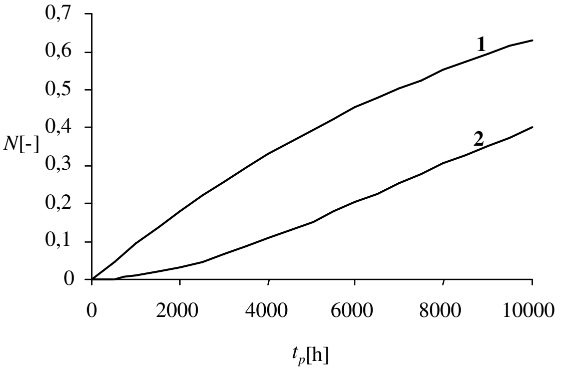

Fig. 7. Probability of dangerous failure by different sensors connections

4. CONCLUSION

To reaching the reliability and safety parameters of control system related not only by fulfillment of control system implementation criteria but also by investment to devices and maintenance of control system. Therefore is appropriate to be the choice of control system optimal by regarding to required reliability and safety parameters. This can be obtainable by appropriate models.

It is necessary not forget that achievement of the required safety integrity level is related to ensure of functional safety. By the PLC based control systems isn't problem with functional safety and it can be based on the finite automata theory [7].

This work has been supported by the scientific grant agency VEGA, grant No. VEGA-1/0040/08 "Mathematic-graphical modelling of safety attributes of safety-critical control systems".

LITERATÚRA

[1] STN IEC 50 191: Medzinárodný elektrotechnický slovník. Kapitola 191: Spoľahlivosť a akosť služieb. 1993

[2] http://www.tecomat.com

[3] http://www.ab.com

[4] STN EN 61 508: *Funkčná bezpečnosť elektrických / elektronických / programovateľných elektronických bezpečnostných systémov.* 2002

[5] Publikácia: 1756-RM001E-EN-P - November 2006, Dostupné na www.ab.com/manuals

[6] http://www.siemens.com

[7] RÁSTOČNÝ, K., ŽDÁNSKY, J.: *Použitie konečného automatu pri programovaní PLC.* In: Advances in Electrical and Electronic Engineering, No. 1 Vol. 3/2004, ŽU v Žiline, s. 45 - 49, ISSN 1336-1376