THE CHOICE OF THE APPROPRIATE STRUCTURE OF THE CONTROL SYSTEM WITH RESPECT TO THE REQUIRED AVAILABILITY AND SAFETY

Juraj Ždánsky[1], **Jozef Hrbček**[2]

Nowadays, the programmable logic controllers (PLCs) are often in the role of control systems. They are used primarily for control of technological processes, but the exception is neither the utilization in transport. As an example can be mentioned systems of rail safety technique: system MODEST from the company 1Signální, ELEKSA system from Siemens, the system SPA 4 from Bombardier Corporate.

The PLC producers continually improve their properties. The aim of the producers is to extend their application possibilities. Therefore there can be found in the offers of PLC producers PLC with attribute fail-safe, eventually fault-tolerant.

PLCs are modular systems, so their availability and safety depends on the chosen structure of control system. The choice of structure is appropriate to base on the modeling of monitored properties. Another reason to create a suitable model, eventually models, is that the certificate of producer about reached level of safety PLC says nothing about the application of PLC. The correct model must also take into account the application individualities (e.g. the way of sensors connecting, actuators, etc.).

The article compares the availability and safety of various structures of control systems based on PLC on the ground of created models.

Key words: control system, safety, availability

1 Introduction

Nowadays, the programmable logic controllers (PLCs) are often in the role of control systems. They are used primarily for control of technological processes, but the exception is neither the utilization in transport. As an example can be mentioned systems of rail safety technique: system MODEST from the company 1Signální, ELEKSA system from Siemens, the system SPA 4 from Bombardier Corporate, etc.

The PLC producers improve their properties continually. The aim of the producers is to extend their application possibilities. Therefore there can be found in the offers of PLC producers PLC with attribute fail-safe, eventually fault-tolerant (e.g. [www.automation.siemens.com], [www.ab.com], [www.meau.com]). In the first case, it concerns PLC for control of safety critical processes and in the second case it concerns PLC for control of processes that require high availability. In both cases the monitored characteristic is achieved by appropriate application of redundancy. Regarding the fact that

[1] Ing. Juraj Ždánsky, PhD., Department of Control and Information Systems, Faculty of Electrical Engineering, University of Žilina, Univerzitná 8215/1, SK-010 26 Žilina, Slovakia, E-mail: juraj.zdansky@fel.uniza.sk

[2] Ing. Jozef Hrbček, PhD., Department of Control and Information Systems, Faculty of Electrical Engineering, University of Žilina, Univerzitná 8215/1, SK-010 26 Žilina, Slovakia, E-mail: jozef.hrbcek@fel.uniza.sk

PLC is the modular system, the user influences the usage of redundancy by the choice of system structure, too and then also reliability and safety characteristics of the control system. Manuals of the producers offer an overview of the various structures of control systems. The plenty of solutions often leads the user to the question, what is the basis on which we proceed the selection of an optimal control system structure. If we added to the monitored characteristics even the price of control system, the user is placed to the relatively complex problem. Regarding the reliability and safety of control system it is necessary to choose the optimal structure on the grounds of modeling of reliability and safety characteristics of structures in compliance with requirements of a given application.

In this article we will focus on different structures of control systems with PLC, which can be built up from commercially available modules. For each structure we will analyze the probability of failure and the probability of dangerous failure of control system. The probability of failure is one of the main factors influencing the availability of control system and the probability of dangerous failure reflects the reached level of safety. The mutual comparison of results shows positives and negatives of concrete structure in regard to the monitored characteristics. In developed models there are not taken into consideration sensors and actuators because of simplicity. Their number will be high dependent on the chosen application. The way of sensors and actuators connecting, and the influence of setting of related parameters to the safety is described in [1] in more details.

2 The basic structure of control system with safety PLC

To the basic structures offered by producers with the aim of safety increase of control system belongs the structure in the Fig.1. It is a one-channel structure, which consists of modules designed for safety PLC. This structure is composed of a processor (CPU), communication bus, communication module (K), input (I) and output (O) module.

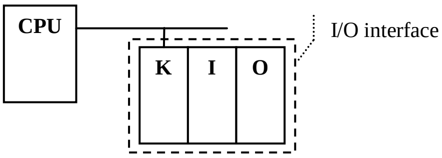

Fig. 1: The basic structure of safety PLC

In this case, the redundancy is applied inside the modules and the user sets only application-dependent parameters of modules. Regarding the serial control of the modules of this structure, the dangerous failure of control system can be caused by dangerous failure of any module of the structure. It is given by:

$$\begin{aligned} N_{CS}(t) = {} & N_{CPU}(t) + N_B(t) + N_{IO}(t) - N_{CPU}(t)N_B(t) - N_B(t)N_{IO}(t) - \\ & - N_{CPU}(t)N_{IO}(t) + N_{CPU}(t)N_B(t)N_{IO}(t) \end{aligned} \quad (1)$$

where $N_{CPU}(t)$, $N_B(t)$ and $N_{IO}(t)$ are probabilities of dangerous failure of processor parts, communication bus and I/O interface.

The probability of dangerous failure of part i can be calculated with assuming the exponential dividing of failures probability, according to the equation:

$$N_i(t) = 1 - e^{-t\sum_{j=1}^{n}\lambda_j^N} \quad (2)$$

where λ_j^N is intensity of dangerous failures of j-th module and n is the number of modules of i-th part of the structure. With regard to the fact that it concerns PLC determinated for control of safety critical applications, data about intensities of dangerous failures of modules are available in producers catalogues.

The common feature of all on the market available safety PLC is that they are certified by producers for maximal SIL 3 (Safety Integrity Level [2]). This fact is particularly influenced by the current market requirements.

The failure probability of such structure can be expressed similarly:

$$P_{CS}(t) = P_{CPU}(t) + P_B(t) + P_{IO}(t) - P_{CPU}(t)P_B(t) - P_B(t)P_{IO}(t) - P_{CPU}(t)P_{IO}(t) + \\ + P_{CPU}(t)P_B(t)P_{IO}(t) \qquad (3)$$

where $P_{CPU}(t)$, $P_B(t)$ and $P_{IO}(t)$ are failure probabilities of processor parts, communication bus and I/O interface.

The probability of failure of *i*-th part can be calculated with preconditions the exponential division of failures probability according to relation:

$$P_i(t) = 1 - e^{-t\sum_{j=1}^{n}\lambda_j} \qquad (4)$$

where λ_j is intensity of failures of *j*-th module and *n* is the number of modules of *i*-th part of the structure.

If the parameters of the mentioned basic structure are not sufficient for a given application, it is necessary to use more complex structures of control systems. These structures are offered by producers in order to increase the availability of control system. However, by their building there may be used modules of safety PLC in order to create the structure conforming to the reliability and safety requirements of a given application. But it is necessary to regard the fact that by increasing of availability would not come to the safety degrease of control system. The following parts of the article focus on this problem.

3 The more complex structure of control systems

For more complex structures of control systems, the redundancy is applied at the level of modules. In the simplest case, there can be used redundancy of some module, eventually of some part of control system. If necessary there can be proposed such structure that each component in it will be redundant. The impact of such solutions to the probability of failure and dangerous failure is described in the following parts of the article.

3.1 Partially redundant control system

The most common case of partially redundant control system is the control system in the Fig. 2. In this case, the processors are redundant (CPU 1 a CPU 2), and I/O interface is connected to the communication bus through the communication module. Such a structure is displayed in the Fig. 2. It concerns the hot backup of processor and this structure is able to mask the failure of one processor.

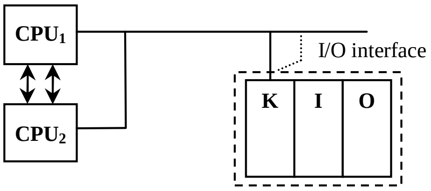

Fig. 2: The structure of control system with redundancy at the level of CPU

In the Fig. 3 there is a block diagram of no-failure operation of control system in the Fig. 2. From this block diagram it is possible to derive that for the calculating of failure probability of this structure can be used equation (3), and for the failure probability of processor is valid:

$$P_{CPU}(t)=P_{CPU_1}(t).P_{CPU_2}(t) \tag{5}$$

where $P_{CPU_1}(t)$ and $P_{CPU_2}(t)$ are probabilities of processors failures from the Fig. 2.

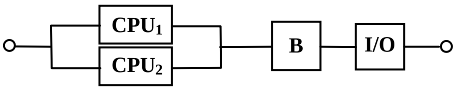

Fig. 3: Block diagram of no-failure operation of control system in the Fig. 2

The structure safety in the Fig. 2 is dependent on the way of mutual cooperation of processors. If the producer does not guarantee whether the processor not participating in control (generating the hot back-up) can influence the controlled process in the dangerous way, then it is necessary to proceed to the creation of model pessimistically. This approach assumes that a dangerous failure of any processor causes a dangerous failure of control system. The model created on the ground of this assumption is in the Fig. 4.

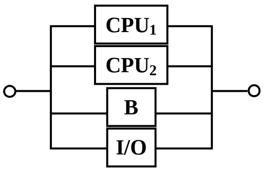

Fig. 4: Block diagram of safety of control system in the Fig. 2

The probability of dangerous failure of the structure in the Fig. 2 can be expressed by equation:

$$N_{CS}(t)=1-(1-N_{CPU_1}(t))(1-N_{CPU_2}(t))(1-N_B(t))(1-N_{IO}(t)). \tag{6}$$

3.2 Completely redundant control system

An example of control system, in which each module of control system is backed-up, is displayed in the Fig. 5. Such a structure can mask the failure of one from a pair of mutually redundant modules. However, it is not possible to consider the current failure of one element of each pair, because for example the failure of the first processor (CPU1) excludes the use of the first communication bus.

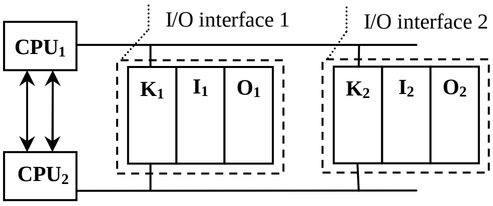

Fig. 5: The structure of completely redundant control system

The influence of particular elements used in the structure in the Fig. 5 on no-failure operation of control system represents the block diagram in the Fig. 6.

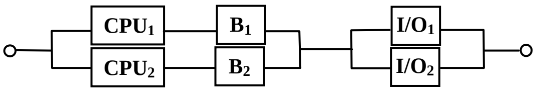

Fig. 6: Block diagram of no-failure operation of control system in the Fig. 5

From the block diagram in the Fig. 6 can be derived the relation for calculation of failure probability of control system:

$$P_{CS}(t)=1-(1-(1-(1-P_{CPU_1}(t)).(1-P_{B_1}(t))).(1-(1-P_{CPU_2}(t)).(1-P_{B_2}(t)))).$$
$$(1-P_{IO_1}(t)P_{IO_2}(t)) \tag{7}$$
$$.$$

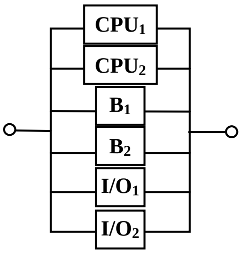

Fig. 7: Block diagram of safety of control system in the Fig. 5

The probability of dangerous failure can be derived from the block diagram in the Fig. 7. To have comparable results, this block diagram is built-up on the same assumption as the block diagram in the Fig. 4. Therefore we will use the pessimistic assumption that the dangerous failure of the part creating back-up may also cause a dangerous failure of control system.

It is given by:

$$N_{CS}(t)=1-(1-N_{CPU_1}(t))(1-N_{CPU_2}(t))(1-N_{B_1}(t))(1-N_{B_2}(t))(1-N_{IO_1}(t))(1-N_{IO_2}(t)) \qquad (8)$$

4 Comparison of reliability and safety characteristics of individual structures

In previous parts of the article we introduced various structures of control systems and derived equation for calculation of probability of failure and dangerous failure of mentioned control systems. In this part of the article we compare the time courses of probability of failure and dangerous failure of mentioned structures in order to point out on the influence of change in the structure on the mentioned characteristics. Intensities of failures and dangerous failures of particular modules are taken from the documents [3], [4] a [5].

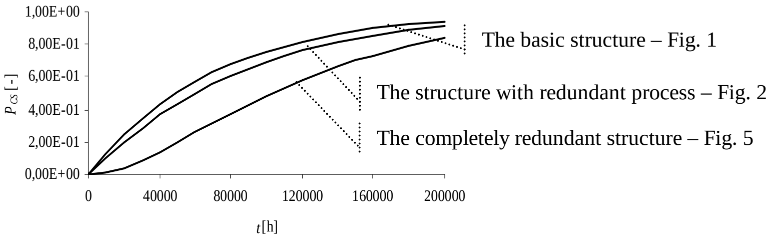

Fig. 8: The time dependence of failure probability

In the Fig. 8 there are time courses of failure probability of control systems introduced in the Fig. 1, Fig. 2 and Fig. 5 (the basic structure, the structure with redundant processor and the completely redundant structure). From these courses it is obvious that failure probability of control system is decreasing using the redundancy.

It should be noted, that the processes of probabilities of dangerous failure are in reverse order. Then the structure that has better characteristics regarding the availability is worse regarding the safety characteristics. This is due to the assumption that the safety is also influenced by parts creating the back-up. Improving of availability for a price of worsening in safety would be possible to achieve by more complex structure of control system (e.g. structure 2z3). More complex structures, however, are not usually offered by producers. In some cases, however, it would be possible to achieve them by appropriate connection and additional application software.

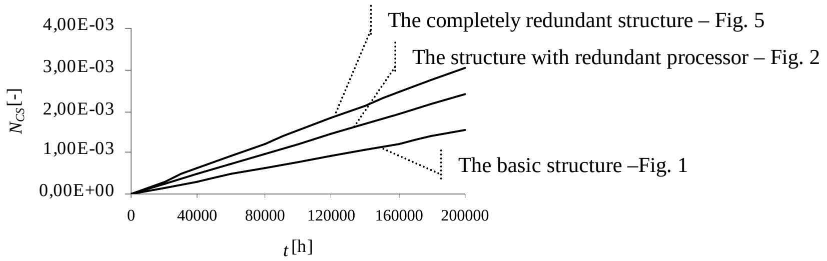

Fig. 1: The time dependence of dangerous failure probability

5 Conclusion

Choosing the appropriate structure of control system is becoming the more demanding when we monitor the more characteristics during its choice. The article points out to the problem that improving of one characteristic does not automatically mean the improving of other characteristics. If it concerns the control system determinated for control of safety critical process, steps must be taken to avoid the worsening of safety by the influence of improvement of other characteristics of control system.

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

Reference literature

1. ŽDÁNSKY, J.: Modeling of safety characteristics of control system with safety PLC, MOSATT 2009, ISBN 978-80-970202-0-0, p. 303-308
2. EN 61 508: *Functional safety of electrical/electronic/programmable electronic safety-related systems.* 1998
3. System Manual: Safety Engineering in SIMATIC S7, http://support.automation.siemens.com
4. Installation and Operating Manual: Automation system Fail-safe signal modules, http://support.automation.siemens.com
5. MTBF_2009-04.xls, http://www.nwe.siemens.com/denmark/internet/dk/industry/information/Software_vejledninger/Documents/MTBF_2009-04.xls