PARAMETERS EVALUATION OF PLC DEPENDABILITY AND SAFETY

J. Ždánsky, K. Rástočný

Department of Control and Information Systems, Faculty of Electrical Engineering,
University of Žilina, Univerzitná 1, 010 26 Žilina

Summary This paper is focused on evaluation of dependability and safety parameters of PLC (Programmable Logic Controller). Achievement of requested level of these parameters is an application assumption for using PLC in control of safety critical processes. Evaluation of these parameters can be made on the base of suitable model and it can be influenced by system architecture when necessary.

1. INTRODUCTION

Wide range of programmable logic controllers (PLC) from various manufacturers is available at present market. Application area is very large and gradually getting to use it in control of safety critical processes in industry area and traffic.

The trend in PLC area converges to modular solutions, so customer is able to define the PLC final architecture based on both, function requirements and requirements on control system availability and safety, too [1]. Proper using of redundancy in the system can positively influence availability and safety. Improper using of redundancy in system should increase availability (for example failure masking) but it can decrease safety and vice versa [2]. So that, such architecture must be chosen (typically variant solutions are available), which attributes are mostly approaching the global optimum regarding to monitored decision criteria (minimum availability requirements, minimum safety requirements, cost requirements, time requirements, etc.). It is suitable to choose optimum architecture based on RAMS (Reliability, Availability, Maintainability, Safety) system parameters modelling.

2. MODELING OF RELIABILITY AND SAFETY PARAMETERS OF PLC

Various methods (also methods that were initially developed only for analysis of system reliability indicators – RBD [3], FTA [4], FMEA [5], Markov model [6], etc.) could be successfully applied in analysis of system RAMS parameters. Use of suitable method or combination of methods depends on concrete analysis case. For example, methods of RBD, FTA, and FMEA have disadvantage in that they don't make possible to build one universal model for all RAMS parameters. Usually, there is a need to make equivalent model for each necessary RAMS parameter, which for given architecture and followed parameter enables to estimate only local optimum. Model that complex describes systems' RAMS parameters should be created on the base of Markov processes or Petri nets. Skills confirm that best result can be achieved by using of various analysis methods combination.

In practice, some in principle varying approaches are using for stochastic models analysis. The difference is in results accuracy, application abilities and calculation severity. These approaches include:

- simulation; stochastic model is imitated by simulator, which simulates time, spend in individual states; accuracy of results depends on simulation time, which designates limit for practical application;
- numerical solution; accuracy of results depends on proper choice of calculation method and numeric accuracy of calculation method; it is necessary to use suitable software tools (for example BQR reliability engineering [7], RELEX software [8], ITEM software [9], etc.); the number of model states is the limiting factor to calculation severity;
- analytical solution; state properties are expressed in form of entire equations that involve model parameters; it is most exact solution, but it is a difficult solution for more complicated models.

In general, PLC consists of these modules:

- chassis;
- power supply;
- processor module;
- input module;
- output module.

If we consider PLC as a subsystem (logic) of control system, than it is necessary to take into account sensor (sensors) and actuator (actuators) of model development.

PLC is an electronic system, so we can assume that its individual parts, from which individual modules are realized of, will have exponential distribution of random failure occurrence. For serial element connection is characteristic that if elements have constant value of failure rate, than whole scheme has constant value of failure rate. This assumption can be accepted, even though the reality is a little bit different (serial-parallel reliability model is usually used for individual modules), because:

$$\lambda_M \le \sum_{i=1}^{n} \lambda_i \ , \qquad (1)$$

λ_M is failure rate of module; λ_i is failure rate of i-th element (for example list value); n is the number of elements.

From practical point of view, this simplification is a big advantage (it is concerned as a more pessimistic assumption) because by quantitative analysis of RAMS parameters, analytical solution is simpler (for example we can work with homogeneous Markov process). Basically, it is an approximation of real distribution function of failure $F_r(t)$ by exponential distribution function $F_t(t)$ (Fig. 1.), and it's a bargain that:

$$F_r(t) \le F_t(t) \text{, for } t \ge 0 . \qquad (2)$$

This simplification can be usually used only at lowest system level. Using it on higher system level can lead to differences between calculated and real value.

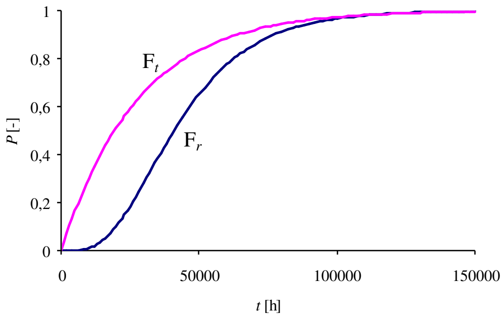

Fig. 1. Approximation of distribution function

3. COMPARISON OF DEPENDABILITY AND SAFETY PARAMETERS FOR CONCRETE PLC ARCHITECTURES

We will follow two concrete schemes of PLC that are recommended by manufacturer in document [10]. Both PLC schemes have equivalent functional facilities, but different dependability and safety parameters. In both cases, I/O interfaces are controlled by processor module of ControlLogix system through ControlNet bus. They are usually used if in the cases of control failure there is no danger or only claims of minimum after-effects are possible. Therefore, using of these schemes is not characteristic for control of safety critical processes.

Single-channel scheme of PLC (architecture 1 out of 1; Fig. 2.) is designated for using in the standard cases without special dependability and safety requirements. PLC scheme consists of control logic (power supply, processor module, communication module), bus and remote input-output interface (power supply, communication module, input modules, output modules).

In this case, serial block diagram (Fig. 3.) can be applied for description of standard PLC dependability (single-channel scheme of PLC).

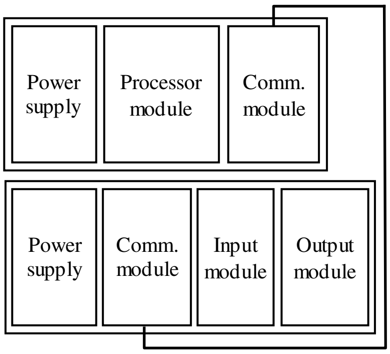

Fig. 2. Single-channel PLC architecture

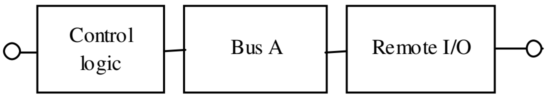

Fig. 3. Block diagram of single-channel PLC scheme dependability

Two-channel scheme of PLC (architecture 1 out of 2; Fig. 4.) is designated for use in applications that require higher dependability level of control system. For this case, manufacturer provides modules that ensure control of multiple channels cooperation in the system. PLC consists of three subsystems; control logic, bus, and input-output interface. Control logic consists of two independent channels, which functionality is evaluated through using of control system redundancy modules. These modules are coupled one to each other by optical communication channel. Control logic works as a 1 out of 2 two-channel system. Similarly, communication with input and output modules is performed over ControlNet, which consists of two equivalent buses. If one channel fails, communication is performed over second channel. Scheme of two-channel PLC is developed to be comparative to single-channel scheme from the function point of view.

Unified model is not possible to use for analysis of RAMS parameters of multi-channel system (for example for safety PLC or if some modules are doubled). For such analysis must be created specific model depending on redundancy type and application case, although model development could be done according to unified algorithm.

According to functionality of PLC scheme (Fig. 4.) we can say that the PLC will be in operation if in operation is at least one of control logic channels, at least one of communication channels, and input-output system interface.

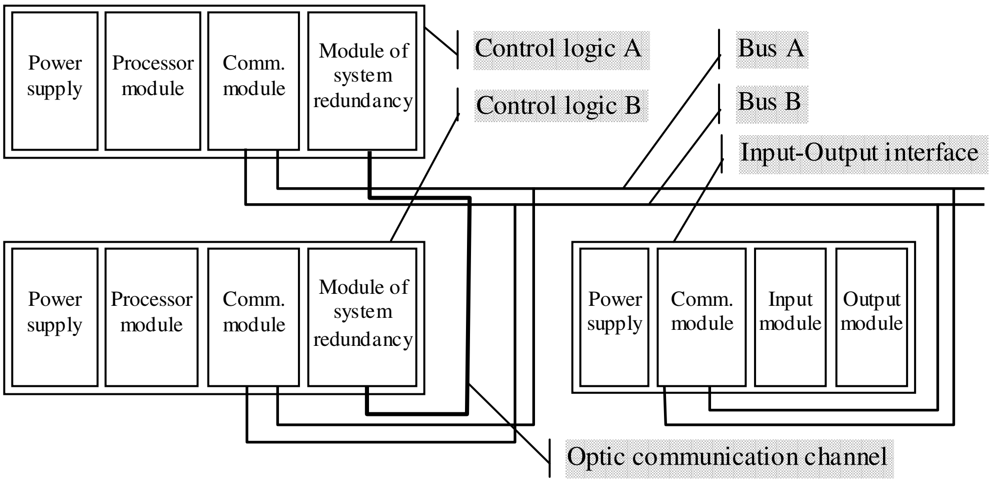

Fig. 4. Two-channel PLC architecture

To describe the reliability of scheme at Fig. 4., block diagram at Fig. 5. can be used.

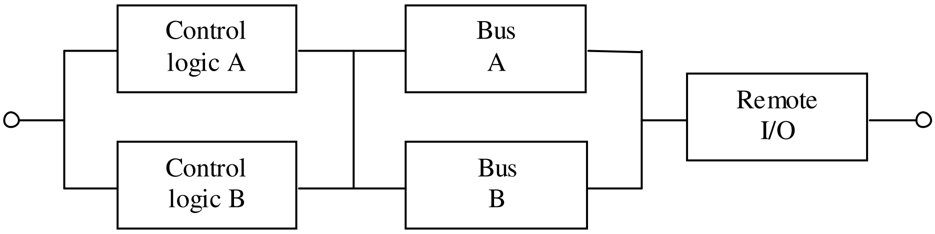

Fig. 5. Block diagram of two-channel PLC scheme reliability

If we want to describe not only the failure rate of individual modules but also the effect of reparation to the reliability, we must combine RBD method with another method of analysis (for example Markov model). Each block of diagram (Fig. 3. or Fig. 5.) is described by Markov model according to Fig. 6. Diagram includes no-failure state of block (state 1) and failure state of block (state 2). Transition rate from state 1 to state 2 is equivalent to failure rate of block; Transition rate from state 2 to state 1 is equivalent to reparation rate of block after each failure.

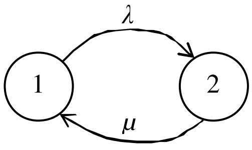

Fig. 6. Markov diagram of block

Probability of non-failure operation of block (probability that block state equals to state 1) can be calculated by equation

$$p_1(t)=1-\frac{\lambda}{\mu+\lambda}\left(1-e^{-(\mu+\lambda)t}\right), \tag{3}$$

where λ is failure rate of block and μ is repair rate of block.

Probability of non-failure operation of control system with single-channel architecture

$$R_{1oo1}=1-\frac{\lambda_{1oo1}}{\mu_{1oo1}+\lambda_{1oo1}}\left(1-e^{-(\mu_{1oo1}+\lambda_{1oo1})t}\right). \tag{4}$$

Failure rate of PLC with single-channel architecture

$$\lambda_{1oo1}=\lambda_{CL}+\lambda_{B}+\lambda_{IO}, \tag{5}$$

where λ_{CL} is failure rate of control logic, λ_B is failure rate of bus and λ_{IO} is failure rate of input-output interface.

Repair rate of PLC with single-channel architecture

$$\mu_{1z1}=\frac{1}{MDT}, \tag{6}$$

where *MDT* (mean down time) is mean time of PLC failure state.

Based on block diagram (Fig. 5.) probability of reliability of PLC with two-channel architecture (Fig. 4.) could be calculated by following equation

$$R_{1oo2}=\left(2.R_{CL}-R_{CL}^2\right)\left(2.R_B-R_B^2\right)R_{IO}, \tag{7}$$

where R_{CL}, R_B, R_{IO} are probabilities of reliability of individual blocks of diagram (Fig. 3. and Fig. 5.), which are calculated by equation (3).

Probability failure state curves (state 2; fig. 6.) of single and two-channel PLC for different repair rate values are displayed on Fig. 7. and Fig. 8.

Considered modules failure rate values that were use for calculation are listed in document [10].

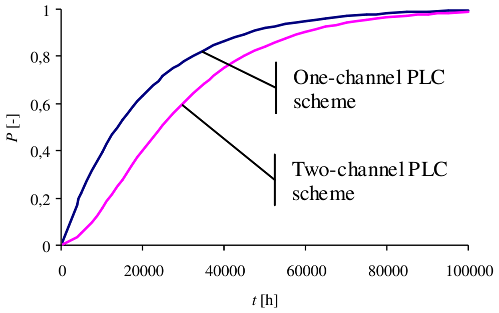

Fig. 7. Probability of failure of single-channel and two-channel PLC schemes without reparation (μ=0 h^{-1})

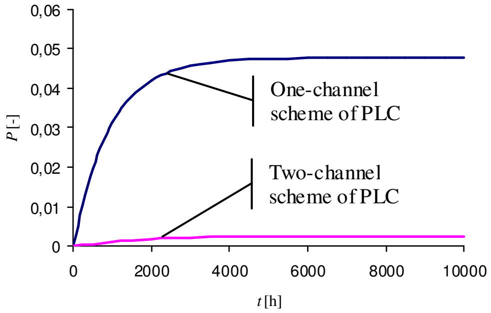

Fig. 8. Failure state probability of single-channel and two-channel PLC scheme with reparation (μ=0,001 h^{-1})

4. CONCLUSION

Similar considerations can be also done to safety requirements. To analyse safety requirements we have to know also:

- definition of dangerous state of control system;
- coefficient of diagnostic coverage of failure for individual blocks of system;
- coefficient that indicate proportion between non-dangerous failure rate (occurrence of safety failure doesn't influence safety of control system) and dangerous failure rate of individual system blocks.

In this case, PLC with one-channel architecture has better properties than PLC with two-channel architecture.

This work has been supported by the Agency for science and technical support by financial support no. APVV - 20 - P00705.

REFERENCES:

[1] STN EN 61508: *Funkčná bezpečnosť elektrických / elektronických / programovateľných elektronických bezpečnostných systémov*. 2002

[2] ZAHRADNÍK, J., RÁSTOČNÝ, K., KUNHARD, M.: *Bezpečnosť železničných zabezpečovacích systémov.* EDIS – vydavateľstvo ŽU, 2004, ISBN 80-8070-296-9

[3] STN EN 61078: *Metódy analýzy spoľahlivosti. Metóda blokového diagramu spoľahlivosti*. 2001

[4] STN IEC 1025: *Analýza stromu poruchových stavov*. 1995

[5] STN IEC 60812: *Metódy analýzy spoľahlivosti. Postup analýzy spôsobu a dôsledku porúch (FMEA)*. 1992

[6] ČSN IEC 165: *Použití Markovových metod.* 1995

[7] www.bqr.com

[8] www.relexsoftware.de

[9] www.itemuk.com

[10] www.ab.com/manuals (publication 1756-RM001D-EN-P)