RELIABILITY OF NETWORKED CONTROL SYSTEM USING THE NETWORK RECONFIGURATION STRATEGY

Ján SARNOVSKÝ, Ján LIGUŠ
Department of Cybernetics and Artificial Intelligence, Faculty of Electrical Engineering and Informatics,
Technical University of Košice, Letná 9, 042 00 Košice, Slovak Republic, tel.: +421 55 602 2508,
e-mail: jan.sarnovsky@tuke.sk, jan.ligus@tuke.sk

ABSTRACT

This paper presents results of modelling and analysis of Network Control Systems (NCS) using the reconfiguration strategies in case of individual networks faults. In general the NCS as all systems follows its mission which should be accomplished with guarantee. The system mission can be disturbed or interrupted by failures which occur with some probability. A primary requirement in order to benefit from network reconfigurations is to prepare some reconfiguration mechanisms which are executed just after the network failure, when the communication of some of the components has to be retransmitted through other non-failed networks. The implementation of a suitable reconfiguration strategy allows significant improvement of the dependability attributes and parameters.

Keywords: *network control system, reconfiguration, reliability, control topologies, coloured Petri Nets, Monte Carlo simulation*

1. INTRODUCTION

Networked control systems are complex control structures with various types of dependencies among constituting subsystems. Several new phenomena such as random delays or problematic of asynchronism appear among the subsystems communicating through the network, which are not solved by using the classical control theory. Because of the complexity of NCS, different dependencies appear which have influence to the final system behaviour; the ignorance of the inter-subsystem influences could lead to a non-presumed system behaviour. The complexity of the NCS is also an advantage due to the existence of distributed processing which allow the decision algorithms to be implemented onto several processing units. Mentioned approach is based on control system design where some additional redundant components are considered, in concrete networks. This hardware approach which is represented by using the redundant components will be considered further. The method used for the evaluation of the reliability as well as MTTF dependability parameter is Monte Carlo Simulation.

2. NETWORKED CONTROL SYSTEMS

The definition of networked control systems (NCS) is formulated as follows: „A networked control system is one type of distributed control system where sensors, actuators and controllers are interconnected by communication networks“. As we can see from the definition of networked control system (Fig. 1), the network is a very important part of the control structure. Thus, it is realized the exchange of all the required control data needed to hold the system's states between the required limits, through the network. The implementation of a network into the control loop has several advantages as lower cabling price in comparison with the analogue connection, easier installation and maintenance, easy diagnostics of system, increasing of control architecture flexibility, increasing of system reconfiguration etc. But this network interconnection has also some disadvantages as communication constraints, dependability of control from network faults, asynchronous elements of control, unpredictable network faults etc.

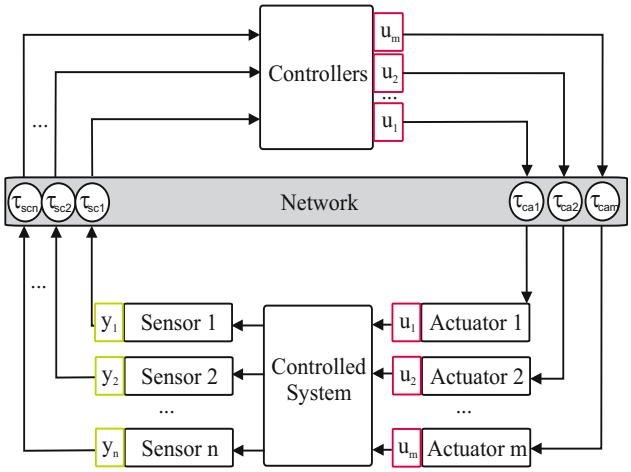

Fig. 1 The block diagram of the complex NCS

Thanks to decreasing the level of complexity of interconnections among components more effective diagnostic and maintenance could be considered in comparison with the same control system realized in conventional (centralized) fashion.

On the other side, NCS brings new phenomena which are not described by classical control theory. One of the main problems of NCS is random delay caused by the network which could destabilize the controlled system.

There are other parameters related to network which have a direct influence on the stability or instability of the system:

- network bit rate,
- type of communication protocol,
- sample period of each of the nodes connected to the network (sensors, controllers, actuators – Fig. 1),
- number of connected nodes.

ISSN 1335-8243 (print) © 2011 FEI TUKE
www.aei.tuke.sk

ISSN 1338-3957 (online)
www.versita.com/aei

The mentioned parameters as well as others should be taken into account when a NCS is designed and realized for using in industrial applications. Several problems will be described in further text.

In conventional control systems (centralized control systems) measuring, computing and actuating are strictly sequential. However, in NCS these three functions could be achieved in parallel. This feature brings problem of synchronization of all nodes connected to the network.

All the problems which could appear in NCS have an influence not only to the stability but also to other parameters for the quality of control (QoC) [1] as well as parameters and attributes of the system dependability.

3. DEPENDABILITY OF THE SYSTEM

There are defined attributes and parameters associated to the dependability as well as Safety Integrity Levels (SIL) in the following subchapters.

3.1. Definition of dependability attributes and parameters

The term dependability, according to IEC 61069-5, is a general term which covers the concepts of availability and credibility which covers reliability, maintainability, integrity and security term.

A short definition of the dependability mentioned in [2] is as follows:

"The dependability is an ability of the system to perform properly."

There are presented four basic attributes (Availability, Reliability, Security, Safety) in [3] and in addition presents other three attributes (Maintainability, Integrity, Credibility). In summary there is one additional attribute (Safety).

The *reliability* as first attribute of the dependability is defined as follows [4]:

"The *Reliability* $R(t)$ of the system is the probability that a system is up and running correctly during the time interval $<0, t>$". $R(t) = P$[*system will not failed during the time interval* $<0, t>$]

The second attribute is the *Availability* of the system $A(t)$ defined as the probability that a system is up and running correctly at time t. $A(t) = P$[*system will not failed at time t*].

The average availability of the system within the time interval $<t_1, t_2>$ is defined as:

$$\overline{A}(t_1, t_2) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} A(t)dt \tag{1}$$

The complement to availability is the unavailability which is defined as: $U(t) = P$[*system will failed at time t*], and holds

$$A(t) + U(t) = 1 \tag{2}$$

The maintainability $M(t)$ is defined as a probability that the system will be restored within a specified period of time t. $M(t) = P$[*system will be repaired during time t*]

In order to measure the attributes defined previously, specialists in dependability have defined some parameters: for example Mean Time To Failure (*MTTF)* and Mean Time To Repair (*MTTR)*.

MTTF is defined as:

$$MTTF = \int_0^{\infty} R(t)dt \tag{3}$$

where $R(t)$ is the reliability of the system.

MTTR is defined as:

$$MTTR = \int_0^{\infty} [1 - M(t)]dt \tag{4}$$

For completeness, further are provided the definitions of density of probability of failures and failure rate (FR) [1]. The density of probability of failures $f(t)$ is given by:

$$f(t) = -\frac{dR(t)}{dt} \tag{5}$$

and the failure rate $r(t)$ (abbreviation FR) by:

$$r(t) = \frac{f(t)}{R(t)} \tag{6}$$

Other definitions of the concepts and terminology related to system dependability are presented in mentioned IEC standards.

3.2. SIL levels

Through the attribute of the dependability, we could divide the systems into several categories described by International standards IEC 61508 and IEC 61511 which represent Safety Integrity Levels. According to above mentioned standards the SIL is:

"The key design parameter specifying the amount of risk reduction that the safety equipment is required to achieve for a particular function in question."

There are four levels divided by value Probability of Failure on Demand (PFD) or Frequency of Dangerous Failure per Hour (FDFH). All levels and values of PFD and FDFH are introduced in Table 1.

Except other terms, standard IEC 61511 defines safety instrumented function (SIF) as an action which provides the controlled process or component in a safe state. These actions are realized in different modes of SIL assignment. Based on different types of values (PFD, FDFH), we can divide SIL assignment into two modes [5]:

- Demand mode (Low-demand) of operation – demands to activate safety instrumented function (SIF) are infrequent compared to the rest of the SIF.
- Continuous mode (High-demand) – demands are placed on the SIF much more frequently.

The first mentioned mode is most common in process industries. Based on average PFD value we can determine the SIL by using the followed formula:

$$SIL = -\log_{10}\left(PFD_{avg}\right) \tag{7}$$

The second one is more common in the machine industry and avionics. As we can see, in this mode the SIL

category is described by the number of dangerous failures per hour. The value represented by SIL 1 supposes approximately one dangerous failure every ten years.

In common Distributed Control System (DCS), there are different subsystems or group of subsystems with several levels of SIL. Then, the SIL of the entire DCS has a value equal to the SIL of the smallest level: this is done under the assumption that there is no redundancy.

Table 1 Safety integrity levels and corresponding PFD and FDFH [5]

Safety Integrity Level (SIL)	Average PFD Range	FDFH Range
4	$10^{-4} \rightarrow 10^{-5}$	$10^{-8} \rightarrow 10^{-9}$
3	$10^{-3} \rightarrow 10^{-4}$	$10^{-7} \rightarrow 10^{-8}$
2	$10^{-2} \rightarrow 10^{-3}$	$10^{-6} \rightarrow 10^{-7}$
1	$10^{-1} \rightarrow 10^{-2}$	$10^{-5} \rightarrow 10^{-6}$

In the next chapter there are described the coloured Petri Nets and the Monte Carlo simulation, because of its usage for the reconfiguration strategies simulations.

4. COLOURED PETRI NETS AND MONTE CARLO SIMULATION

4.1. Coloured Petri Nets (CPN)

All the simulations results mentioned below are the outputs of the coloured Petri Nets simulations. CPN is the hierarchical coloured Petri net that belongs to group of high – level Petri nets. CPN are modelled in the CPN Tools, which is interactive computer java application for performing modelling and simulation with CPN, which works under OS Linux as well as under OS Windows.

4.2. Monte Carlo Simulation (MCS)

In order to obtain relevant results from multiple simulations it is necessary use some appropriate method. Monte Carlo simulation is very useful statistical method which provides evaluating of dependability parameters and attributes.

The principle of this method is to simulate several times a scenario in order to get statistically representative results. The exactness of this method depends on the duration of each simulation and on the number of provided simulations [5]. The number of simulation to obtain the results with precision ε can be given by:

$$n = \left(\frac{u_{\alpha/2}}{\varepsilon} \right)^2 \tag{8}$$

where $\alpha = 0.1$ and $u_{\alpha/2} = 1.645$. Mentioned constants are table values.

In addition there are several methods which allow computing the error of MCS during the simulations.

In [4] is described the method of the static modeling which is one of the Monte Carlo methods. The procedure of dependability parameters computation by using this method can be summarized in the few following points:

1. Computing the random values of the time to repair and time to failure.
2. Computed random values are processed by preparing algorithms to compute time to failure and time to repair of the system.
3. The first and second simulation steps are repeated *n*-times.
4. The output values obtained in each 2nd step are used to compute required parameters of the system.

Error of the mentioned method is given by:

$$\varepsilon = \frac{3\sigma(X)}{\sqrt{n}} \tag{9}$$

where X is random variable, $\sigma(X)$ is the standard deviation and n is the number of provided simulations.

In order to increase the exactness as obtain smaller standard deviation holds followed formula

$$n_1 = 2^i * n \tag{10}$$

where n_1 is number of simulation to reduce standard deviation *i-th* times. Thus, decreasing the standard deviation to half value is necessary provide $2^2 * n$ simulations, hence holds

$$\varepsilon_1 = \frac{\varepsilon}{2} = \frac{\sigma(X)}{\sqrt{n_1}} = \frac{1}{2}\frac{\sigma(X)}{\sqrt{n}}, \text{ for } i = 2 \tag{11}$$

5. DESCRIPTION OF THE NCS RECONFIGURATIN STRATEGY

5.1. Modelled NCS

Suppose the cascade control system without network shown in Fig. 2. Its networked topology is shown in Fig. 3.

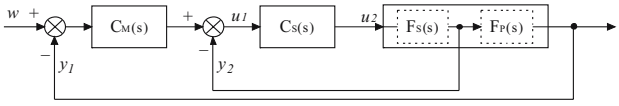

Fig. 2 Cascade control system scheme

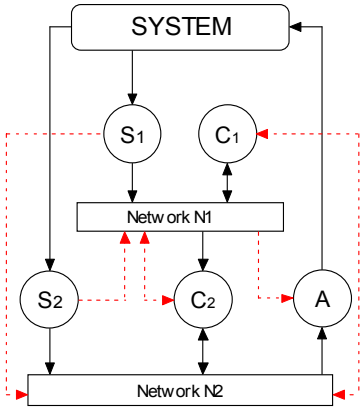

Fig. 3 Network topology of the cascade NCS components

The system is composed of five main components (Sensor S_1, S_2, controllers C_1, C_2 and actuator A) and two networks [6]. The communication flow among

components is determined by its cascade control structure. Thus, sensor S_1 sends a measured value to the controller C_1 (Master), the controller C_2 (Slave) receives the values from the sensor S_2 as well as the controller C_1 in order to compute an actuating value for the actuator A. Both networks transmit required data - network N_1 transmit data from S_1 to C_1 and from C_1 to C_2 such as network N_2 from S_2 to C_2 and from C_2 to A. Thus both networks are active and allocated during the system mission. However, when NCS reconfiguration of components is considered the system is not already composed of independent components. Depending on the performance parameters of the used hardware equipment in the control loop, a specific influence on the system reliability should be taken into account. A primary requirement in order to benefit from network reconfiguration is to prepare some reconfiguration mechanism which is executed just after the network failure, when the communication of some of the components has to be retransmitted through other non-failed networks. This kind of spares represents another type of redundant components, which are not primary determined as redundant, but they are able to replace some other subsystems, if it is urgently required. This type of redundancy is referred as *shared redundancy* [6] or quasi-redundancy [7]. *Quasi-redundant* component is not considered as a primary redundant component such as the active or the passive redundant components. The reconfiguration mechanism should take into account all important physical parameters of the network such as bit rate, maximal number of connected components, etc. From a physical point of view, it is necessary that all potentially reconfigured components should be connected to both (all) networks which are considered as quasi-redundant. As it is shown in Fig. 3 the components S_1, S_2, C_1, C_2, A have to be connected in both networks if the shared redundancy can be applied on this networked control structure.

5.2. Simulation scenarios

Presented studies and results take into account spontaneous loading of the quasi-redundant subsystem S_k just after the subsystem S_n. At first we can suppose that, even if the network capacity is insufficient, the communication will run for a short time interval which allows switch the system into the safe mode. A second approach is to solve the problem of the insufficient bit rate by a controlled reconfiguration mechanism.

The first approach could be hazardous because the mentioned short interval could have randomly long duration whereas it can disallow a guarantee that the system will have enough time in order to remain in the safe mode. On the other hand, the controlled reconfiguration can specify a time interval which can be taken into account in order to protect the system against the damage.

Hence in further text several different scenarios are studied in order to propose a reconfiguration strategy which minimizes the reliability reduction of the shared redundant components. Studied scenarios are as follows:

- Step change of the failure rate (6) up to a specified value for a time interval.
- Gradually increased failure rate during a specified time interval until the maximal value of the failure rate.
- Periodically failure rate increasing and decreasing between its nominal and maximal values.

In the case of the first scenario, the failure rate of the quasi-redundant subsystem is increased by step up to the maximal value whereas after a specified time interval the loading of the components is eliminated and the failure rate is returned to its nominal value. This controlled loading of the subsystem is periodically repeated until the system failure.

The next situation which is studied is the gradual increasing of the failure rate until specified value. When the maximal limit is obtained then the failure rate decreases down to the nominal value of the failure rate for a defined time.

The last mentioned scenario supposes a continuous load increasing and decreasing with a defined periodicity similarly like sine or cosine functions. The two different approaches are compared. In the first, the step subsystem loading is supposed whereas loading is continuously decreased down to a limit which is characterized by the nominal failure rate (cosine function). The second one supposes continuously loading up to the high limit of the failure rate, then the loading is continuously decreased down to the value of the nominal failure rate. As it was already mentioned, all changes of the failure rate of the quasi-redundant subsystems are periodical until the system failure.

Finally, the results of all the mentioned scenarios are compared in order to propose the best strategy for reconfiguration of the NCS based on the principle of the load control.

5.3. Evaluation of simulations

In further study the presumptions are based on the example of two shared networks (subsystems N1 and N2). As was mentioned two supposed scenarios were simulated where the failure rate (FR) is periodically changed following these behaviours [6]:

- Step change - rectangle curve (Fig. 4b, c and 5b) – Scenario I.
- Gradual increasing and step reduction (Fig. 4d and 5c) – Scenario II.
- Gradual increasing and decreasing – sine and cosine functions (Fig. 6b) – Scenario III.

The periodicity of all the simulated scenarios is ten time units. This time interval is chosen due to its sufficient length in order to demonstrate all scenarios. Following the simulated scenario the FR of the components are increased within the interval. Thus, the maximal decrease factor d_R is 0.005 (as equivalent to single FR change) what represents increasing the load of the network which increases the probability of the failure of the network five times.

The FR curve which corresponds to the studied scenario is defined by two parameters which specify the time interval T_i when the network load increases and the time interval T_n when the network load is nominal (nominal FR $\lambda_n = 10^{-3}$). Depending on the simulated

scenario the FR increases gradually or by step during the time interval T_i. The time intervals T_i and T_n have to be determined based on the parameters of the controlled system such as dynamics, etc.

Fig. 4a shows the comparison of the reliability curves for two different scenarios - step change (Fig. 4b, c) and gradual increasing (Fig. 4d) of the FR. As we can see the scenario shown in figure 4c supposes the increasing of the network loading up to the maximal limit (λ_{max} = 6.10^{-3}) during nine time units and for one T_u the network load decreases back to the nominal value (λ_n = 10^{-3}). This scenario covers the situation when the control network fails and the components connected to this network immediately start transmitting the required data through a non-failed network. After a specified number of the sampling periods (time units) several nodes are excluded from the communication in order to decrease the failure rate to the nominal value. This communication blocking some of the nodes is held during the time interval T_n.

In order to develop the mentioned behaviour of component communication through the network, it is necessary to implement the approach of the network scheduling technique to guarantee the minimum level of the quality of service (QoS). In further text and figures two different situations are considered:

- The communication of all components actually connected to the non-failed network has a longer duration than the time of blocking of some of the components ($T_i > T_n$).
- Opposite to the first case.

Thus, in the first situation, the network failure rate is higher for a longer time interval than the nominal FR. In the second case, the network loading is increased for a shorter time interval in comparison with the time when the network is normally loaded (nominal FR).

Fig. 4 shows the two considered scenarios which suppose step and gradual change of the failure rate up to the maximal limit (λ_{max} = 6.10^{-3}) for nine time units. For the step FR change, we can use the equivalent example when the newly connected nodes to the network starts sending the data immediately and it causes the step change of the network loading up to a limit which corresponds to a failure rate level λ_{max} = 6.10^{-3}. After nine time units several components stop the communication in order to decrease the network load and reduce the FR to the nominal value (λ_n = 10^{-3}). After one time when this communication interruption continues the scenario is repeated until the system failure. Thus, time intervals ratio T_i/T_n is 9/1. As in previously presented figures with reliability curves, there are shown highest and lowest reliability values which are equivalent to a system with classical active redundant systems (top long-dashed curve – MTTF = 1503T_u) and system without redundancy (bottom long-dashed curve – MTTF = 498T_u).

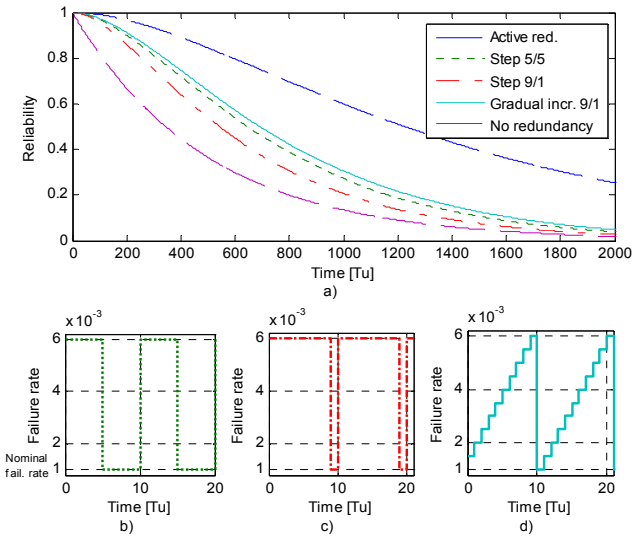

Fig. 4 a) Comparison of the Scenario I and Scenario II of the subsystem loading, b) step FR change with time ratio T_i/T_n = 9/1 (Scenario I.), c) step FR change - T_i/T_n = 5/5 (Scenario I.), d) gradual FR increasing T_i/T_n = 9/1 (Scenario II.)

Table 3 System life time by following scenarios shown in Fig. 5

FR change	Step change 2/8	Gradual incr.2/8	Gradual incr. 3/7
MTTF [T_u]	995 T_u	1070 T_u	998 T_u

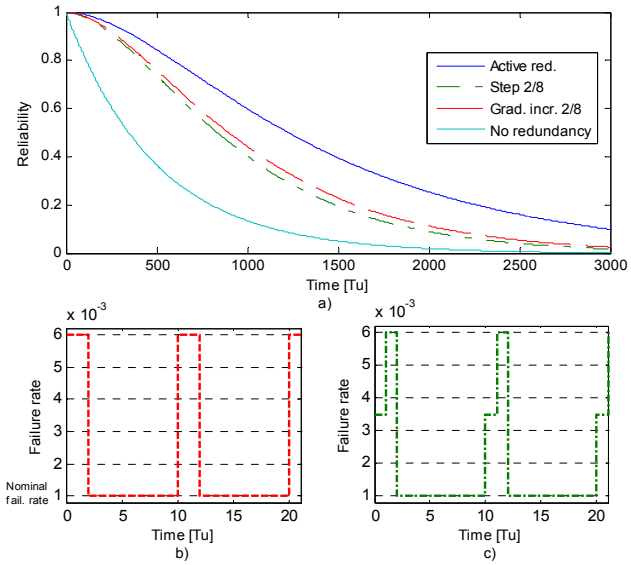

Fig. 5 a) Comparison of two different scenarios of the subsystem loading, b) step FR change with time ratio T_i/T_n = 2/8 (Scenario I.), c) gradual FR increasing T_i/T_n = 2/8 (Scenario II.)

Table 2 System life time by following scenarios shown in Fig. 4

FR change	Step change 5/5	Step change 9/1	Gradual incr. 9/1
MTTF [T_u]	783 T_u	678 T_u	833 T_u

Table 4 System life time by following scenarios shown in Fig. 6

FR change	Sine λ_{max} = 6.10^{-3}	Cosine λ_{max} = 6.10^{-3}	Sine λ_{max} = 10^{-2}	Cosine λ_{max} = 10^{-2}
MTTF [T_u]	737.9 T_u	737.32 T_u	513.3 T_u	514.5 T_u

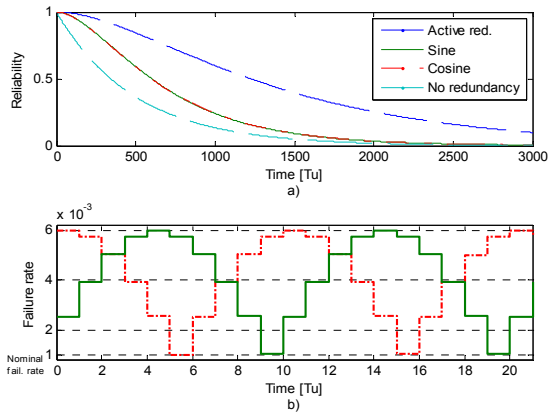

Fig. 6 Gradual increasing and decreasing scenario – following sine and cosine behaviour (Scenario III.)

6. RESULTS

As we can see from presented results the best way in order to prolong the life time of the system is to control the increasing of the network load gradually until the maximal level and then decrease the FR down to the nominal FR for a several time units defined by parameters of the controlled system. The life time is characterized by a MTTF parameter whereas percentage extension of the life time of the non redundant subsystems is presented.

The network reconfiguration approach can significantly increase the reliability and extend the life time of the system as well. Several strategies are compared and evaluated for different cases of the system abilities (consideration of nodes' priority, etc.).

7. CONCLUSIONS

The NCS network reconfiguration approach can significantly increase the reliability and extend the life time of the system as well. However this advantage can be additionally improved in order to obtain better reliability results when a suitable reconfiguration strategy is used. The paper focused on the reconfiguration strategy of the NCS. The implementation of a suitable reconfiguration strategy allows significantly improving of the dependability attributes and parameters.

ACKNOWLEDGMENTS

This work is the result of the project implementation: Center of Information and Communication Technologies for Knowledge Systems (ITMS project code: 26220120020) supported by the Research & Development Operational Program funded by the ERDF (100%).

REFERENCES

[1] BARLOW, R., E. – PROSCHAN, F.: "Statistical Theory of Reliability and Life Testing – Probability models", McArdle Press, Inc., Silver Spring, 1981.

[2] KRINGS, A. W.: Fault-Tolerant Systems, CS449/ 549, 2005.

[3] LAPRIE, J. C.: Dependability: Basic Concepts and Terminology, Springer Verlag Wien-New York, Vol. 5, 1992.

[4] STARÝ, I.: Spolehlivost systému (in Chzech), Vydavatelství ČVUT, Praha, ISBN 80-01-01756-7, 1998.

[5] MARSHAL, E. – SCHARPF, E.: Safety Integrity Level Selection – Systematic Methods Including Layer of Protection Analysis, ISA – The Instrumentation, Systems, and Automation Society, ISBN 1-55617-777-1, 2002.

[6] GALDUN, J.: Dependability Analysis of Networked Control Systems with Consideration of Shared Redundant Subsystems, Doctoral dissertation, Košice, 2008.

[7] WYSOCKI, J. – DEBOUK, R. – NOURI, K.: "Shared Redundancy as a Means of Producing Reliable Mission Critical Systems", 2004 Annual Symposium – RAMS – Reliability and Maintainability, pp. 376–381, 2004.

Received October 4, 2010, accepted April 11, 2011

BIOGRAPHIES

Ján Sarnovský was born on 28.3.1945. He graduated MSc. degree in Technical Cybernetics on the Faculty of Electrical Engineering of the Slovak Technical University Bratislava in 1968. He defended his dissertation thesis in the field of Automatization and Control in 1980 at the same University; his thesis title was "Control of Large Scale Systems Using Hybrid Computer Systems". Since 1969 he is working at Faculty of Electrical Engineering and Informatics Technical University in Košice as a Associate Assistant, since 1980 as Associate Professor and since 1993 as a Professor. Since 1985 he is working as a tutor with the Department of Cybernetics and Artificial Intelligence. His scientific research is focusing on the large scale systems and multiagent systems in control of the large scale systems. He is an author lots of scientific articles and the contributions published in the journals and international conference proceedings. He is also an author of some monographs.

Ján Liguš was born on 8.3.1969. He graduated MSc. degree in Control Technics and Automation on the Faculty of Electrical Engineering and Informatics of the Technical University of Košice in 1992. He defended his dissertation thesis in the field of Automation and Control in 2001 at the same University; his thesis title was "Hierarchical decision in the control of the complex systems". Since 1996 he is working at Faculty of Electrical Engineering and Informatics Technical University in Košice as a Lecturer. His research interests Distributed Control Systems as a complex cybernetic systems, including the design of information and control systems for large-scale technological complexes optimalized regarding the hardware, software and communication structures, hierarchical approaches to classical (hierarchical PID controllers) and non-classical – networked controllers, modern (fuzzy, neural, fuzzy-neural, neural-fuzzy-inductive) control algorithms, decomposition of fuzzy rules, hierarchical fuzzy systems, fuzzy-inductive reasoning methodology, fuzzy-bayesian inference in decision algorithms.