Reliability Analysis of Electronic Protection Systems Using Optical Links

Mirosław Siergiejczyk[1] and Adam Rosiński[2]

[1] Warsaw University of Technology, Faculty of Transport, Department
Telecommunication in Transport, ul. Koszykowa 75, 00-662 Warsaw, Poland
e-mail: msi@it.pw.edu.pl
[2] Warsaw University of Technology, Faculty of Transport, Department
Telecommunication in Transport, ul. Koszykowa 75, 00-662 Warsaw, Poland
e-mail: adro@it.pw.edu.pl

Abstract. Theory of the systems reliability is particularly applicable to electronic protection systems (alarm systems), which due to their specific character of use, should be characterised by the high level of reliability. The devices and electronic units applied in the wide range in those systems, the microprocessor systems in particular, require a new perspective on the reliability and the safety of the systems. The paper presents a reliability analysis of the electronic protection systems using optical links.

1 Introduction

Electronic protection systems realize the service safety assurance while travelling, which is one of the services that are realized by telematics transport systems [14,15]. This service can be realized by the systems installed at: airport, railway stations, logistic centres, trans-shipping terminals as well as by the systems installed in the mobile objects (e.g. vehicles). Suitability assurance is the essential condition of their correct operation.

The group of electronic protection system includes as follows:

- Intruder alarm system,
- Access Control System,
- Closed Circuit TeleVision,
- Fire Alarm System,
- External Terrains Protection System.

Protection resulting from operation of the systems can be provided by the following features:

- signalisation of health condition and personal danger,
- signalisation of environmental dangers,
- against-theft,
- vehicles location systems.

W. Zamojski et al. (Eds.): Dependable Computer Systems, AISC 97, pp. 193–203.
springerlink.com

The intruder alarm system will be introduced in the following part of my paper, but similar issues can also be found in other electronic safety systems.

The European Standard EN 50131-1:2006 "Alarm Systems – Intrusion and Hold-up Systems – Part 1: System Requirements", which has also the status of the Polish Standard PN-EN 50131-1:2009 "Alarm Systems – Intrusion and Hold-up Systems – System Requirements" contains a list of definitions and abbreviations that are then used in subsequent chapters of this standard [5]. Among them there are definitions, such as:

- alarm system – electric installation, responsible for manual or automatic detection of the presence of danger,
- control and indicating equipment – a device for data receiving, processing, controlling, imaging, and further transmission thereof.

Alarm control panels are specialised devices that are meant to:

- receive information signals (analogue and/or digital) from various devices,
- process in accordance with a pre-programmed settings (of the installer and/or the manufacturer)
- control by specifying the appropriate output signals,
- provide imaging of events that occur on the respective devices of the anti-burglary system,
- transmit data to other systems (such as e.g. Alarm Receiving Centre, abbreviated ARC).

PN-EN 50131-1:2009 „Alarm Systems – Intrusion and Hold-up Systems – Part 1: System Requirements" defines the class of protection that the intruder alarm systems should meet. They are as follows:

- grade 1: low risk (it is assumed that the intruder has minimum knowledge about the alarm system and possesses easily accessible tools of the limited choice),
- grade 2: low-to-medium risk (it is assumed that the intruder has a minimum knowledge of the alarm system and has a widely available tools and portable devices such as digital multimeter),
- grade 3: medium-to-high risk (it is assumed that the intruder knows the alarm system entirely and has a complex set of powerful tools and portable electronic equipment),
- grade 4: high risk (applicable whenever safety has priority over all other factors. It is assumed that the intruder has the ability or resources to plan a burglary in detail and has a set of any equipment, including measures to replace the key of an electronic alarm system).

Having specified what class of the protection the intruder alarm system has to fulfil, there are selected devices that meet those requirements. The standard obviously refers to what units have to be applied. Therefore, there are various solution designs of the alarm control panel. They can fulfil the requirements of a specific class of protection, but they also differ among themselves depending on their manufacturer.

As it has already been mentioned, the alarm control panel is the „heart" of the intruder alarm system. Data is sent about the condition of individual supervisory lines (e.g. detectors), exit lines (e.g. load outputs) or a specific one introduced by the user or a maintenance guy (and earlier during the installation of the system). Information can directly be sent to the plate of the main alarm control panel, depending on the type of alarm control panel or also to modules, realising definite functions (e.g. expanding input, expanding output, interfaces of printers, etc.). Information between alarm control panel and individual modules is sent digitally using the transmission format that is mostly applied at present RS-232 or RS-485 or another one (very often elaborated by the manufacturer) [6,9]. There are also solutions of the burglary-signalling systems where transmission bus can combine:

- intra-several alarm control panels (they operate in the so-called annulus),
- control (e.g. the keyboard steering),
- alarm control panels with the supervisory and management centre as well as the managing of the integrated safety system.

The intruder alarm system can be divided into three principal groups:

- concentrated systems,
- distracted systems,
- mixed systems

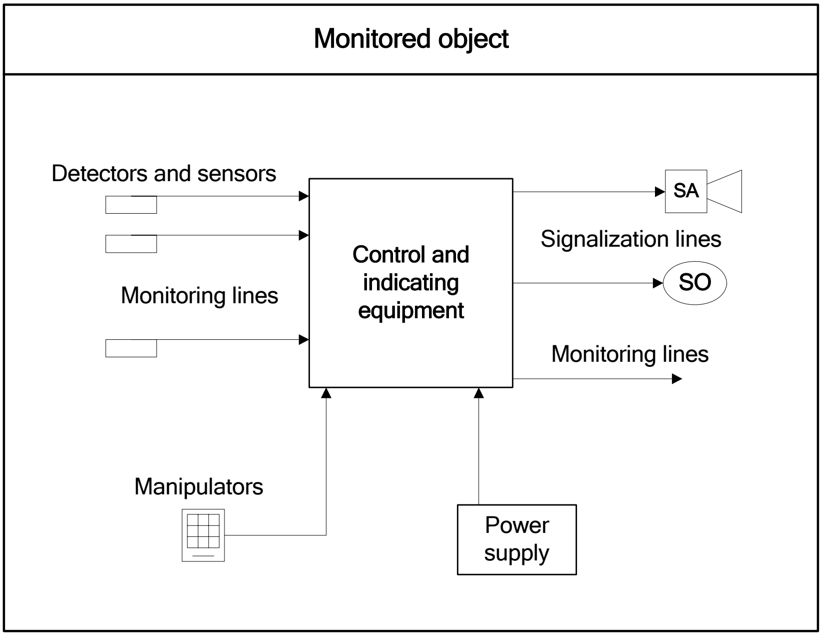

Fig. 1 Intruder alarm system with concentrated structure, where: SA – audio signalling device, SO – optical signalling device

The concentrated structures envisage connection of all the monitored lines and output lines (monitoring and signalising) to the alarm exchange (Fig. 1.).

In the widespread objects requiring a big number of monitoring lines and a big number of control zones, the systems basing on the microprocessor digital exchanges with the concentrated structure are not applicable. Therefore, there systems with dissipated or mixed structure must be used. A characteristics for the dissipated structure is decentralisation of the alarm exchange, basing on the use of transmission buses that are connected to the respective modules (input, output, power) as well as the use of transmission buses to connect the separate concentrated exchanges among themselves and thus creating the system with a dissipated structure. The mixed structure combines characteristics of both described here structures, and it means that the monitoring lines are connected both to the alarm exchange and to the expanding modules.

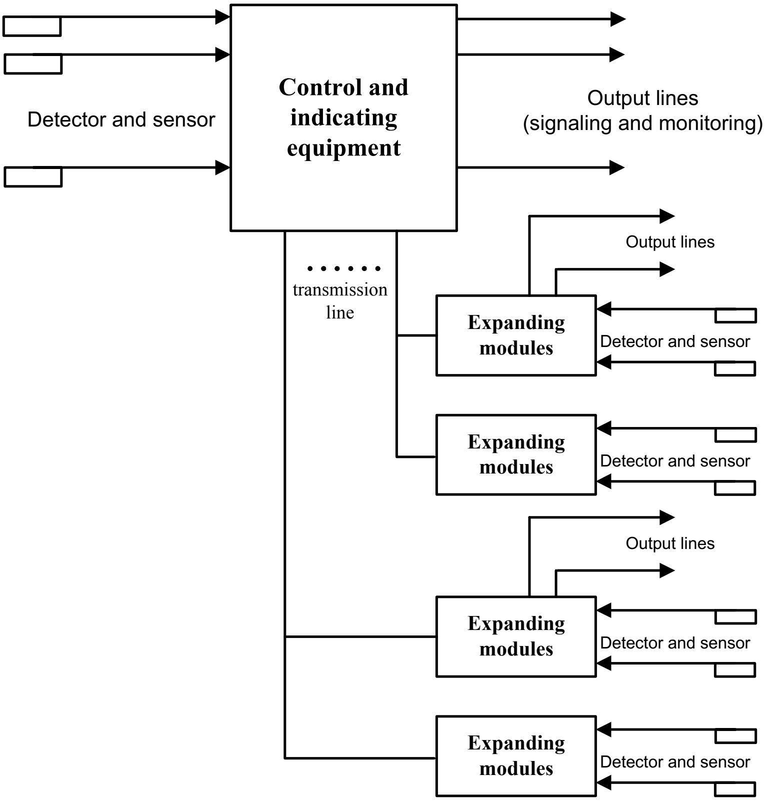

Fig. 2 Intruder alarm system – mixed systems

Figure 2 presents the mixed alarm system with the distracted character where own (switch boards) entries of the supervisory lines are used. The system where concentrated systems are connected by the RS-232 or RS-485 lines (or others, but enabling data transmission between respective alarms and controls in the concentrated version, thus creating the intruder alarm system in the mixed version) can also be treated as the mixed alarm system.

The questions of reliability, exploitation and electromagnetic compatibility in the electronic safety systems are particularly essential, especially if they are they applied in domain of transport. There is very limited number of publication which present this issue [3,4,10]. However they do not take into account the reliability analysis of electronic safety systems in which the optical transmission was applied. That is why it seems necessary to consider such solutions as well.

2 Analysis of Electronic Protection Systems Using Optical Links

Electronic protection system has a defined reliability structure: serial, mixed or parallel. In general, it is presented in Fig. 3. Such a structure is often applicable in large and extensive objects. The reliability analysis of this type of structures is presented in many scientific papers [1,8,11,12,16,17].

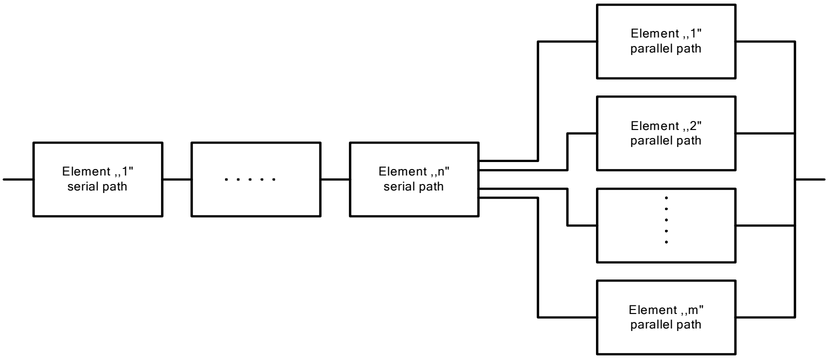
Element „1" serial path
.....
Element „n" serial path
Element „1" parallel path
Element „2" parallel path
.....
Element „m" parallel path

Fig. 3 Structural reliability flow chart of electronic protection system

Due to a specific characteristics of the protected objects (e.g. airports, railway stations, logistic bases), as those buildings are very often located on a large area and simultaneously they have a huge enough surface, there is a need to design the Intruder Alarm Systems which shall enable placement of component units in the protected rooms and adjacent terrains. Using the conventional line solutions in which transmission lines are applied (e.g. modules, manipulators) to the transmission of electric signals is not sufficient because of the guaranteed quality of the data transmission in the function of distance among the units of the system. Electromagnetic disturbances that may occur are the next essential issue. That is why the transmission measure, namely the optical fibre, started to be applicable.

Data transmission requires conversion of electrical signals into optical (fibre-optic transmitter) and vice versa (fibre-optic receiver) [6] - Figure 4. Since data transfer information in the electronic security system busses is normally bi-directional, so the fibre optic converter system should include both the transmitting and the receiving system. Therefore, two optical fibres are necessary to ensure data transmission between the two converters.

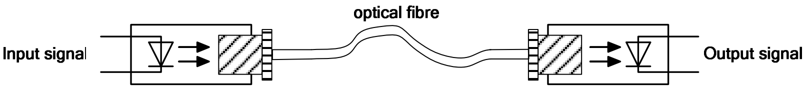

Fig. 4 Optical fibre link for signal transmission

The advantages of fibre optic transmission between devices forming the Intruder Alarm System include inter alia [13]:

- high resistance of communication to interferences,
- no generation of electromagnetic interference,
- lack of sensitivity to the phenomenon of stray currents (this is particularly important in the railway environment where in close proximity to each other there may be a small capacities of say milliwatts (telecommunication signals) and large capacities of say megawatts (electric locomotives),
- high bandwidth fibre enables the connection of further devices,
- galvanic isolation of devices.

By modelling the single optical bus transmission lines applying the serial structure, the readiness should be considered of such component units as: amplifiers, cables, regenerators, etc. (Fig. 5) [7].

Let us assume the following indications of the value of the readiness coefficients: transponder K_{gtrans}, regenerator K_{greg}, amplifier K_{gwzm}. Analysing the process of the exploitation of the optical link, we can distinguish the following states of efficiency:

- s_0 – the state of the correct execution of the function of transmission,
- s_1 – the state in which the functions of the broadcast realisation are not executable.

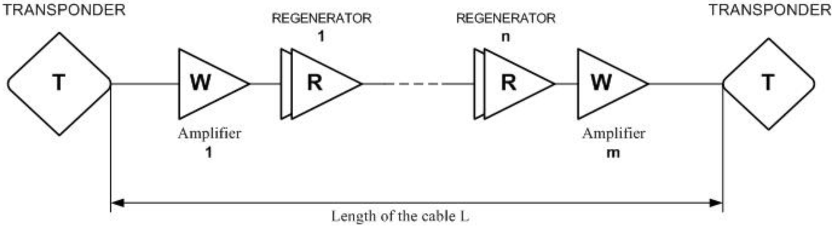

Fig. 5 Structure of a single optical transmission line

The matrix of transitions probabilities between the distinguished states takes the form of:

$$\mathbf{P} = \begin{bmatrix} 1-\lambda_k & \lambda_k \\ \mu_k & 1-\mu_k \end{bmatrix} \tag{1}$$

Accepting the solid intensity of damages λ for individual units of the optical link and the solid intensity of the service μ, we can determine a stationary value of the readiness coefficient of optical amplifier, regenerator, and transponder in the form of:

$$\mathrm{K}_{\mathrm{g\ trans}} = \mathrm{K}_{\mathrm{g\ reg}} = \mathrm{K}_{\mathrm{g\ wzm}} = \mathrm{P}_0 = \frac{\mu_\mathrm{k}}{\mu_\mathrm{k} + \lambda_\mathrm{k}} \tag{2}$$

where index *k* means parameters of time distribution of proper operation and repair time respectively for optical amplifier, regenerator, and transponder, respectively.

Components such as fibre optic cables also have a significant impact at operational readiness of the entire optical link. The optical cables readiness can be counted using the *CC Cable Cut* parameter, which expresses the average length of the cable that breaks once during the whole year (8760 [h]). Coefficient *CC is expressed* in kilometres, meanwhile the value of the parameter *MTBF*$_K$ *(Mean Time Between Failure)* for the cable whose length is *L*, is defined in hours and has a form of [2]:

$$MTBF_K(L) = \frac{CC \cdot 8760}{L} \tag{3}$$

The value of the readiness coefficient for the optical cable can be written in the form of:

$$K_{gK} = P_0 = \frac{MTBF_K}{MTBF_K + MTTR_K} \tag{4}$$

where: *MTTR*$_K$ - is the optical cable repair time.

3 Analysis of Practical Application Reliability of Electronic Protection Systems Using Optical Links

Figure 6 shows a diagram of the Intruder Alarm System with mixed structure, which has been designed and implemented using a microprocessor alarm control panel INTEGRA.

The hereto presented system belongs to the group of mixed systems, i.e. part of monitoring lines (e.g. PIR detector, magnetic sensor, alarm box) is connected by radio channels with a special module of wireless devices. The module is connected to the mainboard of the alarm control panel via the wired transmission bus. Also, some

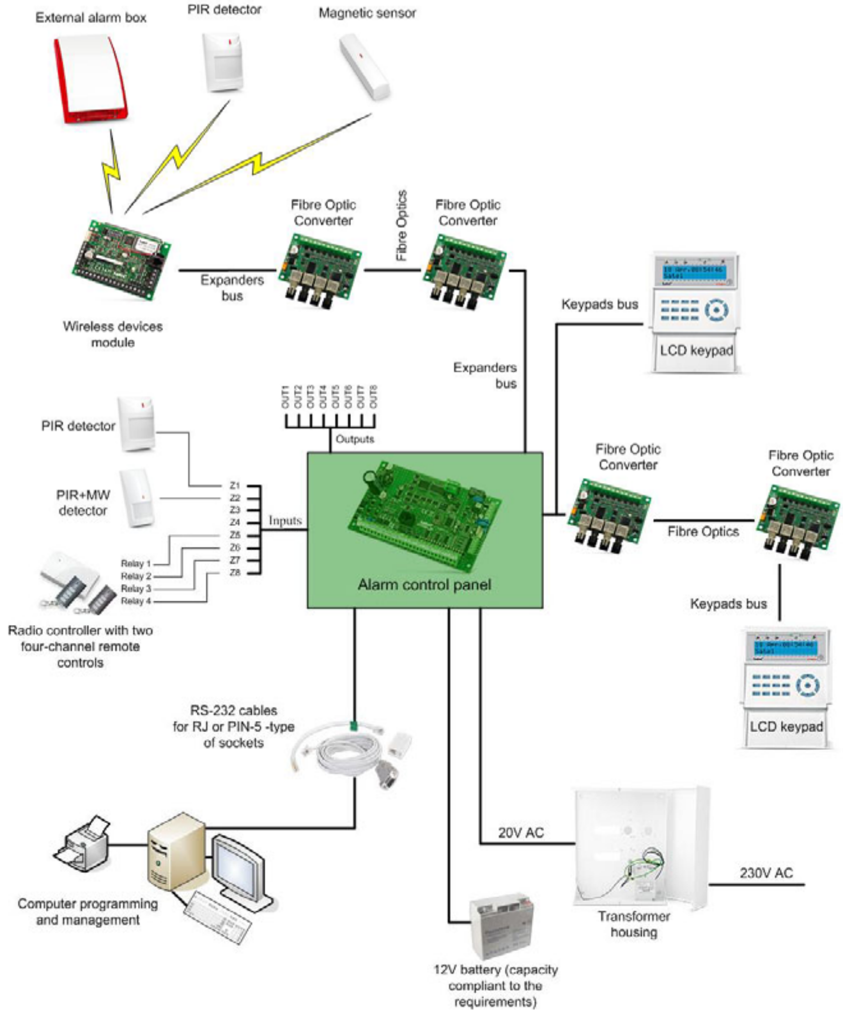

Fig. 6 The intruder alarm system of dispersed structure (with applied fibre optic converters)

of the detectors are linked to the mainboard via a conventional monitoring wired-lines. The entire system is programmable and controllable by a computer (using appropriate software) linked to the mainboard of the alarm control panel via RS-232 interface. The system is also operable through LCD keypads. One of them is directly connected to the mainboard of the alarm control panel via conventional wired bus keypads. The second one is also connected to the keypads bus, but using the fibre optic converters between which data transmission takes place through the transmission medium, namely the fibre-optic cable. There are neither amplifiers nor regenerators used in the hereto applied solution.

The following values have been adopted in the analysed system:

- research time – 1 year:

$$\mathrm{t_b} = 8760[h]$$

- reliability of fibre-optic converter:

$$\mathrm{R_{ks}}(t_b) = 0{,}99$$

- intensity of repairs of fibre-optic converter (it corresponds to the repair time equal to 12 [h]):

$$\mu_{\mathrm{ks}} = 0{,}08333\left[\frac{1}{h}\right]$$

- repair time of fiber-optic cable:

$$MTTR_{\mathrm{K}} = 24[h]$$

- fiber-optic cable intersection parameter:

$$CC = 4[km]$$

- length of fibre-optic cable:

$$L = 2[km]$$

Knowing the value of reliability $\mathrm{R_{ks}}(t_b)$, we may estimate the intensity of fibre-optic converter damages λ_{ks}. The following relationship can be used for the exponential distribution:

$$\mathrm{R_{ks}}(\mathrm{t_B}) = \mathrm{e}^{-\lambda_{\mathrm{ks}}\mathrm{t_B}} \text{ for } t \geq 0$$

therefore:

$$\lambda_{\mathrm{ks}} = -\frac{\ln \mathrm{R_{ks}}(\mathrm{t_B})}{\mathrm{t_B}}$$

For $\mathrm{t_b} = 8760[h]$ and $\mathrm{R_{ks}}(t_b) = 0{,}99$ we receive:

$$\lambda_{\mathrm{ks}} = -\frac{\ln \mathrm{R_{ks}}(\mathrm{t_B})}{\mathrm{t_B}} = -\frac{\ln 0{,}99}{8760} = \frac{0{,}01}{8760} = 1{,}147298 \cdot 10^{-6}\left[\frac{1}{\mathrm{h}}\right]$$

Knowing the value of λ_{ks}, the expected operation time between successive damages is calculable:

$$E(T)=\frac{1}{\lambda_{ks}}=871612[h]$$

Fibre-optic converter readiness index can be determined from the following dependence (2):

$$K_{g\,ks}=\frac{\mu_{ks}}{\mu_{ks}+\lambda_{ks}}=\frac{0{,}08333}{0{,}08333+1{,}147298\cdot 10^{-6}}=0{,}999986$$

The readiness index of the fibre-optic link can be determined from the dependence (3 and 4):

$$MTBF_K(L)=\frac{CC\cdot 8760}{L}=\frac{4\cdot 8760}{2}=17520[h]$$

$$K_{gK}=\frac{MTBF_K}{MTBF_K+MTTR_K}=\frac{17520}{17520+24}=0{,}998632$$

The readiness index of the entire single fibre-optic link is:

$$K_g=K_{gks}\cdot K_{gK}\cdot K_{gks}=0{,}999986\cdot 0{,}998632\cdot 0{,}999986=0{,}998604$$

4 Conclusions

Not only the stage of the threat effecting from an object, designed according to the currently binding standards and recipes, but also a possibility to use modern solutions in the area of safety engineering should be considered when designing an electronic safety protection system (it has been presented in the Report on Exemplary Intruder Alarm System). The example is a possibility to utilize optical units as elements assuring data transmission between the alarm control panel and the modules. This increases the level of the guaranteed quality of data transmission in the function of distance between elements of the system, as also it protects the transmitted information against electromagnetic disturbances that may occur.

The paper presents methodology for analysing reliability of those electronic protection systems where optical links have been applied. This type of the consideration are particularly important in the event when this type of technical solutions are applied to the protection of objects about the strategic meaning for the country (e.g. airports, railway stations, atomic power stations) and its defence (e.g. military base). The results obtained from the reliability analysis can be used while designing of the system in order to assure the suitable values of the reliability coefficients. There is also a possibility to use the methodology hereto presented to analyse the already existing systems in order to qualify the influence that modernisation of the system units has on their reliability.

References

[1] Będkowski, L., Dąbrowski, T.: The basis of exploitation, part II: The basis of exploational reliability. Wojskowa Akademia Techniczna, Warsaw (2006)

[2] Chołda, P., Jajszczyk, A.: Assessment of availability in telecommunication networks. Telecommunication Review and Telecommunication News. No. 2-3/2003. Publication by Sigma NOT, Warsaw (2003)

[3] Dyduch, J., Paś, J.: Exploitation of the transport systems of supervision on the extensive railway area. In: VII The National Conference: the Technical Diagnostics of Devices and Systems – DIAG 2009, Ustroń (2009)

[4] Dyduch, J., Paś, J.: Electromagnetic environment on the railway and its influence on the systems of the safety. Transport and Communication (1)2009)

[5] European Standard EN 50131-1:2006. Alarm Systems – Intrusion and Hold-up Systems – Part 1: System Requirements. Brussels: European Committee for Electrotechnical Standardization CENELEC

[6] Haykin, S.: Telecommunication systems, vol. I & II. WKiŁ, Warsaw (2004)

[7] Horowitz, P., Hill, W.: The art of electronics, vol. I & II. WKiŁ, Warsaw (2006)

[8] Jaźwiński, J., Ważyńska-Fiok, K.: System safety. PWN, Warsaw (1993)

[9] Norman, T.: Integrated security systems design. Butterworth Heinemann, Butterworths (2007)

[10] Paś, J., Dyduch, J.: Influence of the electromagnetic disturbances on the transport systems of safety. Measurements Automation Robotics (9,10) (2009)

[11] Rosiński, A.: Reliability analysis of the electronic protection systems with mixed – three branches reliability structure. In: Proc. International Conference European Safety and Reliability (ESREL 2009), Prague, Czech Republic, pp. 1637–1641 (2009)

[12] Rosiński, A.: Design of the electronic protection systems with utilization of the method of analysis of reliability structures. In: Proc. Nineteenth International Conference On Systems Engineering (ICSEng 2008), Las Vegas, USA, pp. 421–426 (2008)

[13] Siergiejczyk, M., Gago, S.: A Concept of Monitoring and Supervising System in Railway Junction. In: Sixth International Scientific & Technical Conference LOGITRANS 2009, Szczyrk (2009)

[14] Siergiejczyk, M.: Maintenance Effectiveness of Transport Telematics Systems. Transport Series, vol. (67). Scientific Works of the Warsaw University of Technology, Warsaw (2009)

[15] Wawrzyński, W., Siergiejczyk, M., et al.: Final Report on Grant KBN 5T12C 066 25. Methods for Using Telematic Measures to Support Realisation of Transport Tasks, Supervisor: Associate Professor Ph.D. D.Sc. W. Wawrzyński, Warsaw (2007)

[16] Ważyńska-Fiok, K., Jaźwiński, J.: Reliability of technical systems. PWN, Warsaw (1990)

[17] Zamojski, W. (ed.): Reliability and Maintenance of Systems. Publisher of Wroclaw University of Technology, Wroclaw (1981)