DIAGNOSTYKA, 2017, Vol. 18, No. 4

ISSN 1641-6414
e-ISSN 2449-5220

ANALYSIS OF EXPLOITATION PROCESS IN THE ASPECT OF READINESS OF ELECTRONIC PROTECTION SYSTEMS

Jarosław ŁUKASIAK[1], Adam ROSIŃSKI[2]

[1] Warsaw Military University of Technology Faculty of Electronic
00-908 Warsaw, gen. S. Kaliskiego 2, jaroslaw.lukasiak@wat.edu.pl
[2] Warsaw University of Technology Faculty of Transport
00-662 Warsaw, Koszykowa 75, adro@wt.pw.edu.pl

Abstract

This paper presented issues concerning the operation process of electronic safety systems. The particular attention was paid to the issues related to periodic inspections and rationalisation of the readiness index value. The analysis of current reliability and operation models allowed to conclude that a thesis, which also takes into account information obtained from diagnostic subsystems, is right. This approach made it possible to develop a graph of relationships in the system including diagnostic information.

Keywords: operation, periodic inspections, diagnostics

ANALIZA PROCESU EKSPLOATACJI W ASPEKCIE GOTOWOŚCI ELEKTRONICZNYCH SYSTEMÓW OCHRONY

Streszczenie

W artykule przedstawiono zagadnienia związane z procesem eksploatacji elektronicznych systemów zabezpieczeń. Zwrócono szczególną uwagę na kwestie związane z przeglądami okresowymi i racjonalizacją wartości wskaźnika gotowości. Analiza dotychczasowych modeli niezawodnościowo-eksploatacyjnych pozwoliła stwierdzić, iż słuszna jest teza by uwzględnić także informacje otrzymane z podsystemów diagnostycznych. Takie podejście umożliwiło opracowanie grafu relacji w systemie z uwzględnieniem informacji diagnostycznych.

Słowa kluczowe: eksploatacja, przeglądy okresowe, diagnostyka

1. INTRODUCTION

The composition of electronic safety systems, depending on a type of detected hazards, includes the following systems:

- intrusion detection system (SSWiN),
- fire alarm system (SSP),
- access control system (SKD) [22],
- video surveillance (CCTV) [5,6],
- protection of external sites.

The protection resulting from operation of these systems can be supplemented by the following systems:

- health condition and personal threat alarm,
- environmental threat alarm,
- anti-theft system,
- voice alarm systems,
- car protection against burglary and theft.

One of the most important elements of the electronic safety systems includes alarm transmission systems. They constitute devices and telecommunication networks used for transferring information on the condition of one or more alarm systems to one or more alarm receiving centres.

European standard EN 50131-1:2006 "Alarm systems – Intrusion and hold-up systems – Part 1: System requirements", which at the same time, has the status of the Polish standard PN-EN 50131-1:2009 "Alarm systems – Intrusion and hold-up systems - System requirements", contains indications related to the system's failure. It provides definitions and abbreviations, among others:

- state of failure: the alarm system state which prevents normal functioning of the intrusion detection alarm system or its part,
- failure signal/message: information produced as a result of failure.

The above-mentioned definitions specify the condition, in which the intrusion detection system does not completely meet the imposed requirements to provide the protection of persons and property. This condition is unacceptable from the perspective of a user of the system. However, it is not possible to eliminate it from the operation states, which can occur in real working conditions. Therefore, it is important to use the diagnostic subsystems, which make it possible to obtain information on the states of complete usability, partial usability and unfitness, in which the intrusion detection system may occur. Thus, it is possible to take reasonable action (as to the time and its scope) for the occurred situation. Such an approach allows, in case of failure to the system, to take appropriate measures in order to remove the failure, and thus, to restore the system's state of usability. At the same time, a person carrying out the repair has a facilitated task of searching for the place of failure, and also gains knowledge, to a certain extent (depending on the applied diagnostic subsystem), on the type and scope of failure.

Electronic safety systems operate in variable operation conditions [7,13,14]. Their correct operation is dependent not only on the reliability of individual components comprising the system [1], but also on the periodic inspections adopted for implementation [15]. There are publications, in which the issues related to rationalisation of the operation process, also taking into account the electromagnetic interference, were presented [4,8,10,16,21]. The authors of this paper also discussed all sorts of models of the electronic devices' operation process in their articles. It allowed, among others, to develop a method for maximising the readiness index by optimising the performance of periodic inspections [11]. Despite the obtained positive results of the method verification, it would be appropriate to continue its further modification in order to take into account the diagnostic signals [2,3,17] (in the future, including the diagnostic information quality [18,19,20]). Such an approach was presented in this paper, however, the particular attention was paid to its use in the intrusion detection systems.

2. RATIONALISATION OF PERIODIC INSPECTIONS

By designing the electronic safety systems, it is possible to affect reliability indices, among others, with the use of appropriate reliability structures [9,12]. Therefore, it is possible to correct the failure intensity rate of the designed system. Despite such an approach in the design of such systems, it is also necessary to take into account the readiness index, in accordance with the following formula:

$$K_g = \frac{T_m}{T_m + T_n} \tag{1}$$

where: T_m - mean correct operation time between failures,

T_n - mean time to repair.

Expression (1) represents a simplified dependency of the readiness rate and refers to a very simple model.

The readiness index can be defined as the ability of the system to remain in a state where it is possible to perform the required functions under specified conditions, within a specified time interval with assumption that external conditions are ensured.

The given relationship (1) shows that the system can be in one of two states (Fig. 1):

- usage state (usability, S_0),
- repair state (unfitness, S_1).

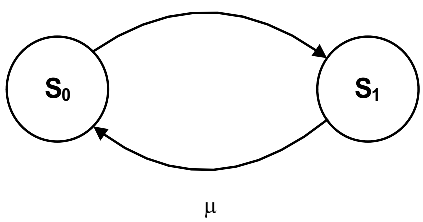

Fig. 1. Graph of switching between the usage and repair states (source: own development]. Markings in Fig.: λ - failure intensity rate, μ - repair intensity rate

During the actual operation process of the intrusion detection systems, the periodic inspections are carried out. By observing the operation process of actual intrusion detection systems, it is possible to assume that there are two types of inspections:

- quarterly with a basic range of activities,
- annual with an extended range of activities.

Therefore, the graph showed in Fig. 1 will be supplemented with two following states (Fig. 2):

- S01 (during which basic activities, required by the scope of services, are performed),
- S10 (during which the extended range of activities is performed).

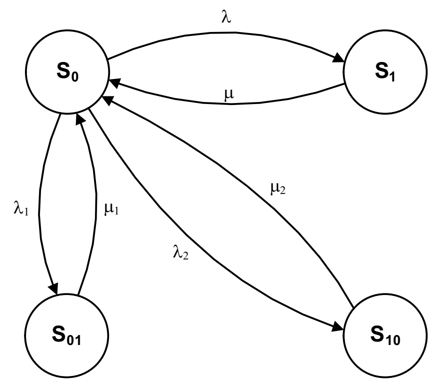

Fig. 2. Graph of switching between the usage and repair states as well as the inspection states of I and II types (source: own development]. Markings in Fig.: λ - failure intensity rate, μ - repair intensity rate, λ_1 - intensity rate of I type inspection, μ_1 – intensity rate of I type inspection performance, λ_2 – intensity rate of II type inspection, μ_2 – intensity rate of II type inspection performance

There are already the developments presenting modification of the graph of relationships (Fig. 2) in the system which, among others, allow to maximise the readiness index, maximise effectiveness of financial resources intended for periodic inspections, rationalisation of the duration of individual periodic inspections. However, these considerations did not include diagnostic subsystems and signals obtained from them. Therefore, a thesis to include them in a model of the intrusion detection system's operation process seems to be right.

By analysing the operation process of the intrusion detection systems equipped with diagnostic subsystems, it can be assumed that the graph of relationships presented in Fig. 2 will adopt the following form (presented in Fig. 3). Therefore, the system may be in one of five states:

- usage state (S_0),
- repair state (S_1),
- diagnosis state (S_D),
- state of I type inspection (S_{01}),
- state of II type inspection (S_{10}).

The system staying in the diagnosis state decides (based on diagnostic information) about a type of the periodic inspection, which is to be carried out. For this purpose, among others, the following measurements can be made:

- voltages and currents of the primary and backup power,
- voltages and currents of individual devices of the intrusion detection system,
- activation of individual outputs of the intrusion detection system,
- use of individual buttons on the keypads.

The obtained information allows to determine the level of using individual devices of the alarm system, and thus, to rationally select a specific periodic inspection.

In order to determine the relationships, which we are interested in, of the system's staying in particular states, the graph of relationships presented in Fig. 3 should be described by the following equations:

$$\begin{aligned}
&-\lambda \cdot P_0 + \mu \cdot P_1 - \lambda_D \cdot P_0 + \mu_D \cdot P_D = 0 \\
&\lambda \cdot P_0 - \mu \cdot P_1 = 0 \\
&-\lambda_1 \cdot P_D - \lambda_2 \cdot P_D - \mu_D \cdot P_D + \\
&+\lambda_D \cdot P_0 + \mu_1 \cdot P_{01} + \mu_2 \cdot P_{10} = 0 \\
&\lambda_1 \cdot P_D - \mu_1 \cdot P_{01} = 0 \\
&\lambda_2 \cdot P_D - \mu_2 \cdot P_{10} = 0
\end{aligned} \tag{2}$$

Markings used in equations (2):

- P_0 – probability of system staying in the state of usage (S_0),
- P_1 – probability of staying in the state of repair (S_1),
- P_D – probability of staying in the state of diagnosis (S_D),
- P_{01} – probability of staying in the state of I type inspection (S_{01}),
- P_{10} – probability of staying in the state of II type inspection (S_{10}).

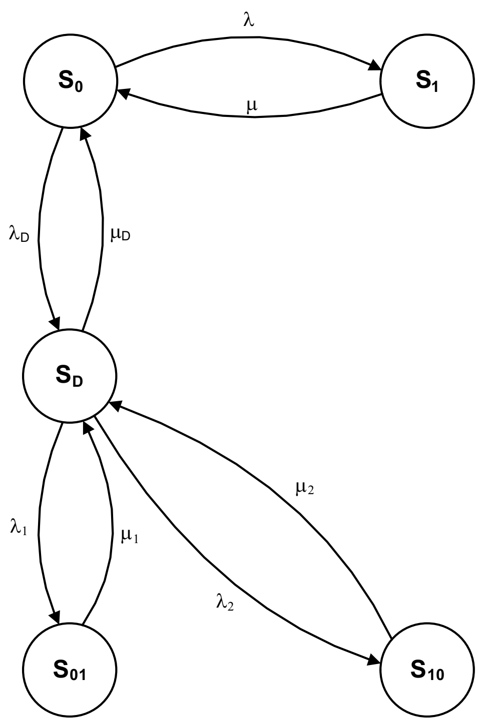

Fig. 3. Graph of switching between the usage, repair and diagnosis states as well as the inspection states of I and II types (source: own development]. Markings in Fig.: λ – failure intensity rate, μ – repair intensity rate, λ_D – diagnosis intensity rate, μ_D – intensity rate of the diagnosis implementation, λ_1 – intensity rate of I type inspection, μ_1 – intensity rate of I type operation, λ_2 – intensity rate of II type inspection, μ_2 – intensity rate of II type operation

By transformation, it is possible to obtain:

$$\begin{aligned}
&P_1 = \frac{\lambda}{\mu} \cdot P_0 \\
&P_D = \frac{\lambda_D}{\lambda_1 + \lambda_2 + \mu_D} \cdot P_0 + \frac{\mu_1}{\lambda_1 + \lambda_2 + \mu_D} \cdot P_{01} + \\
&+ \frac{\mu_2}{\lambda_1 + \lambda_2 + \mu_D} \cdot P_{10} \\
&P_{01} = \frac{\lambda_1}{\mu_1} \cdot P_D \\
&P_{10} = \frac{\lambda_2}{\mu_2} \cdot P_D
\end{aligned} \tag{3}$$

Of course:

$$P_0 + P_1 + P_D + P_{01} + P_{10} = 1 \tag{4}$$

Thus:

$$P_0 \cdot \left(1 + \frac{\lambda}{\mu} + \frac{\lambda_D}{\mu_D} + \frac{\lambda_1}{\mu_1} \cdot \frac{\lambda_D}{\mu_D} + \frac{\lambda_2}{\mu_2} \cdot \frac{\lambda_D}{\mu_D}\right) = 1 \tag{5}$$

$$K_{g1} = P_0 = \frac{1}{1 + \frac{\lambda}{\mu} + \frac{\lambda_D}{\mu_D} + \frac{\lambda_1}{\mu_1} \cdot \frac{\lambda_D}{\mu_D} + \frac{\lambda_2}{\mu_2} \cdot \frac{\lambda_D}{\mu_D}} \tag{6}$$

$$K_{g1} = P_0 = \frac{\mu \cdot \mu_D \cdot \mu_1 \cdot \mu_2}{\mu \cdot \mu_D \cdot \mu_1 \cdot \mu_2 + \lambda \cdot \mu_D \cdot \mu_1 \cdot \mu_2 + \lambda_D \cdot \mu \cdot \mu_1 \cdot \mu_2 + \lambda_1 \cdot \lambda_D \cdot \mu \cdot \mu_2 + \lambda_2 \cdot \lambda_D \cdot \mu \cdot \mu_1} \quad (7)$$

Therefore, on the basis of this expression (7), it is possible to determine the probability value, which we are interested in, of the electronic safety system's staying in the state of usability. Numerically, it is equal to the readiness index value.

A readiness index K_{g1} can be defined as the ability of the system to remain in a state where it is possible to perform the required functions under specified conditions, within a specified time interval, with assumption that external conditions are ensured and the diagnostic subsystem is used.

Computer simulation and computer-aided analysis facilitate to relatively quickly determine the influence of change in reliability parameters of individual components on reliability of the entire system. Of course, the reliability structure of both the entire system and its components has to be known beforehand.

By using the computer aid, it is possible to determine the probability value of the system staying in the usage state S_0.

Example

The following quantities were defined for the system:

- transition rate from the usage state S_0 into the repair state S_1:
  $\lambda = 0{,}000001$
- transition rate from the repair state S_1 into the usage state S_0:
  $\mu = 0{,}1$
- transition rate from the usage state S_0 into the diagnosis state S_D:
  $\lambda_D = 0{,}01$
- transition rate from the diagnosis state S_D into the usage state S_0:
  $\mu_D = 1$
- transition rate from the diagnosis state S_D into the state of I type inspection S_{01}:
  $\lambda_1 = 0{,}001$
- transition rate from the state of I type inspection S_{01} into the diagnosis state S_D:
  $\mu_1 = 0{,}5$
- transition rate from the diagnosis state S_D into the state of II type inspection S_{10}:
  $\lambda_2 = 0{,}0001$
- transition rate from the state of II type inspection S_{10} into the diagnosis state S_D:
  $\mu_2 = 0{,}25$

For the above input values according to equation (7) is obtained:

$$K_g = 0{,}990065681$$

Figures 4, 5 and 6 presents the relationship:

$$K_g = P_0 = f(\mu)$$

$$K_g = P_0 = f(\mu_1)$$

$$K_g = P_0 = f(\mu_2)$$

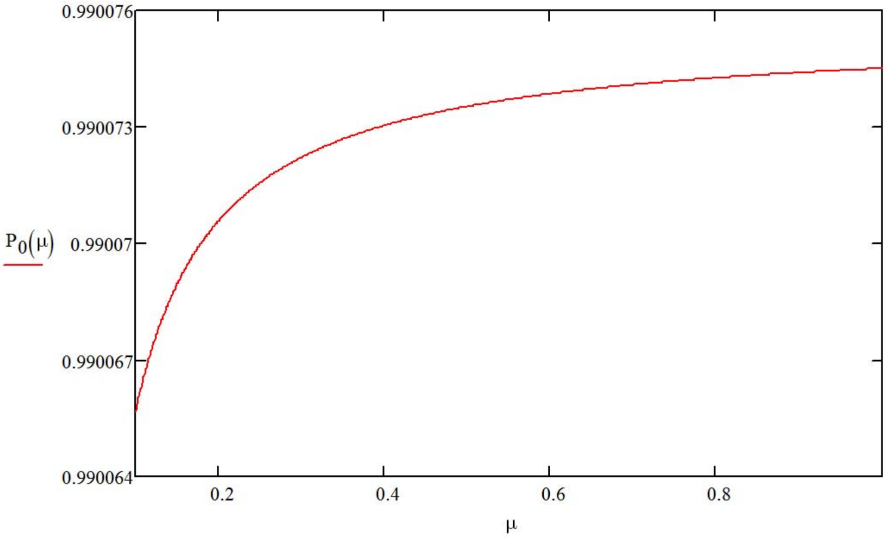

Fig. 4. The relationship between probability of system in the usage state as a function μ

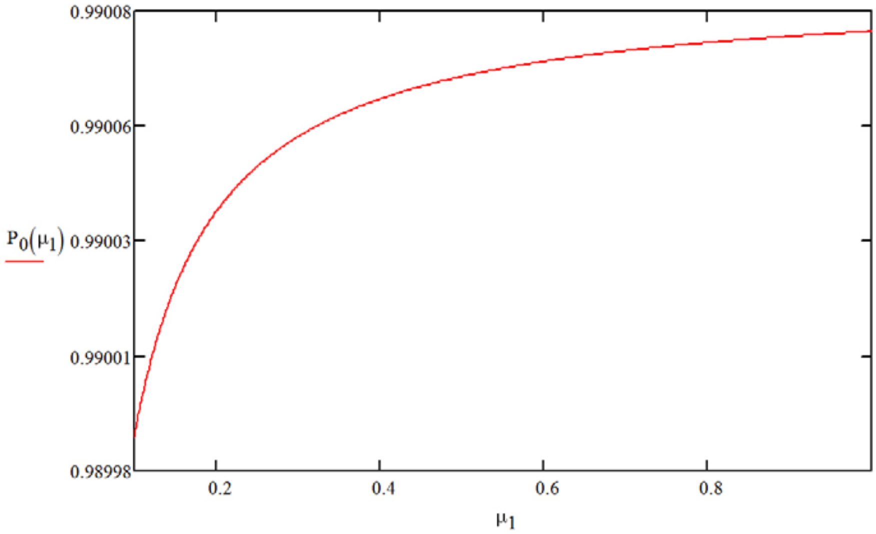

Fig. 5. The relationship between probability of system in the usage state as a function μ_1

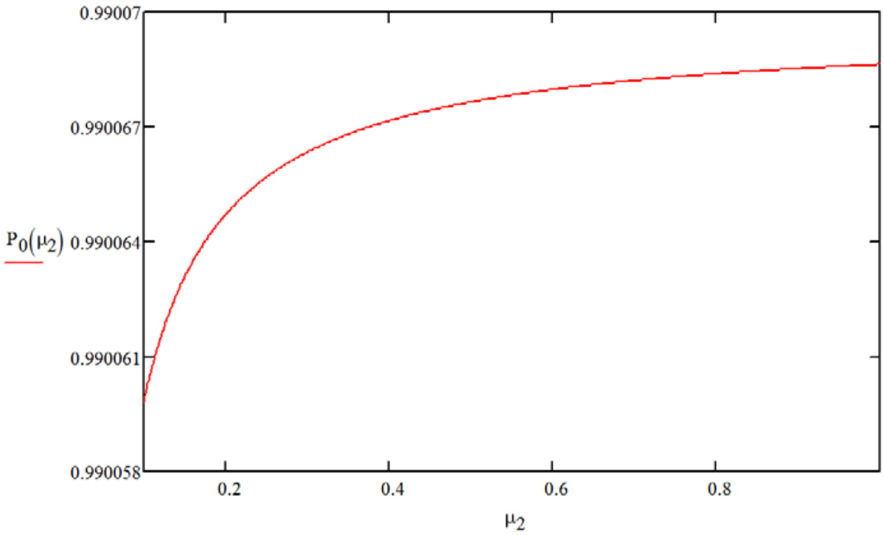

Fig. 6. The relationship between probability of system in the usage state as a function μ_2

In charts presented in fig. 4, 5 and 6 denotations to the left of horizontal red lines mark the colour of analysed quantity line. Those are default denotations and colours used by computer-aided calculations software.

The aforementioned example illustrates the practical implementation of theoretical analysis shown in this article.

3. SUMMARY AND CONCLUSIONS

The considerations presented in the paper were related to electronic safety systems. At the same time, the particular attention was paid to the issues related to the operation process, including the periodic inspections and information from the diagnostic subsystems. The essential issue in this type of systems is to provide a specific value of the operation indices, especially, including the readiness index. Therefore, the authors focused their deliberations on developing a model that allows to rationalize the readiness index value taking into account specific types of periodic inspections.

In the further research of this issue, it is planned to consider the situation in which the first detectable symptoms of the occurring failure appear as first, and the failure occurs after a specified period of time. Such a concept of the exploitation strategy is called DTA (Delay-Time Analysis).

REFERENCES

[1] Będkowski L, Dąbrowski T. The basis of exploitation, part II: The basis of exploational reliability. Military Academy of Technology, Warsaw 2006.

[2] Dąbrowski T, Bednarek M, Fokow K, Wiśnios M. The method of threshold-comparative diagnosing insensitive on disturbances of diagnostic signals. Przeglad Elektrotechniczny - Electrical Review, vol. 88, issue: 11A, 2012, pp. 93-97.

[3] Dyduch J, Paś J, Rosiński A. The basic of the exploitation of transport electronic systems. Technical University of Radom, Radom 2011.

[4] Kaniewski P, Lesnik C, Susek W, Serafin P. Airborne radar terrain imaging system. 16th International Radar Symposium (IRS), Dresden, Germany, JUN 24-26, 2015. pp. 248-253.
[5] Kierzkowski A, Kisiel T. Airport security screeners reliability analysis. In: „Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management IEEM 2015", Singapore 2015. pp. 1158-1163.
[6] Lubkowski P, Laskowski D. The selected issues of reliable identification of object in transport systems using video monitoring services. In the monograph Telematics – support for transport, given as the monographic publishing series – „Communications in Computer and Information Science", vol. 471. Springer-Verlag, Berlin Heidelberg, 2014, pp. 59-68.
[7] Niziński, S., Wierzbicki S.: Zintegrowany system informatyczny sterowania pojazdów. Diagnostyka, 2004; 30: 47-52.
[8] Paś J. Operation of electronic transportation systems. Publishing House University of Technology and Humanities, Radom 2015.
[9] Paś J, Siergiejczyk M. Interference impact on the electronic safety system with a parallel structure. Diagnostyka, vol. 17, no. 1, 2016. pp. 49-55.
[10] Paś J. Shock a disposable time in electronic security systems, Journal of KONBiN 2(38)2016, pp. 5-31.
[11] Rosiński A. Modelling the maintenance process of transport telematics systems. Publishing House Warsaw University of Technology, Warsaw 2015.
[12] Siergiejczyk M, Krzykowska K, Rosiński A. Reliability assessment of integrated airport surface surveillance system. In: Proceedings of the Tenth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX, editors: W.Zamojski, J. Mazurkiewicz, J. Sugier, T. Walkowiak, J. Kacprzyk, given as the monographic publishing series – „Advances in intelligent systems and computing", vol. 365. Springer, 2015: 435-443.
[13] Siergiejczyk M, Paś J, Rosiński A. Issue of reliability–exploitation evaluation of electronic transport systems used in the railway environment with consideration of electromagnetic interference. IET Intelligent Transport Systems 2016; 10(9): 587–593. DOI: 10.1049/iet-its.2015.0183.
[14] Siergiejczyk M, Paś J, Rosiński A. Modeling of process of maintenance of transport telematics systems with regard to electromagnetic interferences. In Tools of Transport Telematics, editors: Mikulski J., given as the monographic publishing series – „Communications in Computer and Information Science", vol. 531. Berlin Heidelberg: Springer-Verlag, 2015: 99-107.
[15] Siergiejczyk M, Paś J, Rosiński A. Reliability and maintenance analysis of CCTV systems used in rail transport. Journal Of KONBiN nr 3(35)2015, Warsaw 2015, pp. 137–146.
[16] Siergiejczyk M, Paś J., Rosiński A. Train call recorder and electromagnetic interference. Diagnostyka, vol. 16, no. 1, 2015, pp. 19-22
[17] Siergiejczyk M, Perlicki K. Measurement procedures for railway telecommunications network based on synchronius digital hierarchy and wavelength division multiplexing transmission techniques. Przeglad Elektrotechniczny - Electrical Review, vol. 9/2013, str. 148-151.
[18] Siergiejczyk M. Assessing transport telematic systems in terms of data services quality. The monograph „Telematics in the transport environment", editors: Jerzy Mikulski, given as the monographic publishing series – „Communications in Computer and Information Science", Vol. 329. The publisher: Springer-Verlag, Berlin Heidelberg, pages: 356-363, 2012.
[19] Stawowy M, Dziula P. Comparison of uncertainty multilayer models of impact of teleinformation devices reliability on information quality. In: Proceedings of the European Safety and Reliability Conference ESREL 2015, editors: Podofillini L., Sudret B., Stojadinovic B., Zio E., Kröger W. CRC Press/Balkema, 2015: 2685-2691.
[20] Stawowy M. Comparison of uncertainty models of impact of teleinformation devices reliability on information quality. Proceedings of the European Safety and Reliability Conference ESREL 2014, CRC Press/Balkema, 2015, pp. 2329-2333
[21] Sumiła M, Miszkiewicz A. Analysis of the problem of interference of the public network operators to GSM-R. In: Tools of Transport Telematics, editors: Mikulski J., given as the monographic publishing series – „Communications in Computer and Information Science", vol. 531. Berlin Heidelberg: Springer-Verlag, 2015: 76-82.
[22] Wiśnios M, Dąbrowski T, Bednarek M. The security increasing level method provided by biometric access control system. Przegląd Elektrotechniczny, nr 10/2015, s. 229-232.

Received 2017-07-03
Accepted 2017-10-25
Available online 2017-11-06

Jarosław ŁUKASIAK MSc Eng – is a graduate of the Military University of Technology, where he studied at the Faculty of Electronics, scientific fields of interests concern among electronic security systems and acoustic issues.

Adam ROSIŃSKI Associate Professor PhD. Eng. - scientific interests (reliability, exploitation, diagnostics, projecting) are problems connected with comprehended wide electronic systems of the safety both for stationary as well as for movable objects.