Journal of KONBiN 43(2017)
ISSN 1895-8281
DOI 10.1515/jok-2017-0053 ESSN 2083-4608

RELIABILITY ANALYSIS OF A TYPE B POWER SUPPLY USED IN A INTRUSION DETECTION SYSTEM (IDS)

ANALIZA NIEZAWODNOŚCIOWA ZASILACZA TYPU B ZASTOSOWANEGO W SYSTEMIE SYGNALIZACJI WŁAMANIA I NAPADU (SSWIN)

Mirosław Siergiejczyk, Małgorzata Pędzierska, Adam Rosiński

Warsaw University of Technology, Faculty of Transport
Politechnika Warszawska, Wydział Transportu

***Abstract**: One of the electrical security systems used to protect critical infrastructure facilities is the intrusion detection system. Its purpose is to increase the safety level for the persons and property within the protected facility. The paper presents consideration regarding the reliability analysis of a type B power supply used in an intrusion detection system. This takes into account the guidelines regarding the analysed power supply system included in the standard "PN-EN 50131-1:2009: Alarm systems - Intrusion detection systems - Part 1: System requirements". Next, a reliability analysis was performed, which enables the determination of the readiness indicator value. The conduction of further analyses of IDS power supply systems, though of distributed structures, is planned in subsequent studies regarding this issue.*

***Keywords:** reliability, power supply, intrusion and hold-up systems*

***Streszczenie:** Jednym z elektronicznych systemów zabezpieczeń stosowanych do ochrony obiektów infrastruktury krytycznej jest system sygnalizacji włamania i napadu. Celem jego stosowania jest zwiększenie poziomu bezpieczeństwa osobom i mieniu znajdującemu się w chronionym obiekcie. W artykule zaprezentowano zagadnienia dotyczące analizy niezawodnościowej zasilacza typu B zastosowanego w systemie sygnalizacji włamania i napadu. Uwzględniono wytyczne dotyczące analizowanego układu zasilania zawarte w normie „PN-EN 50131-1:2009: Systemy alarmowe - Systemy sygnalizacji włamania i napadu – Część 1: Wymagania systemowe". Następnie dokonano analizy niezawodnościowej, która umożliwiła wyznaczenie wartości wskaźnika gotowości. W dalszych badaniach tego zagadnienia planuje się przeprowadzenie kolejnych analiz układów zasilania SSWiN, ale o strukturach rozproszonych.*

***Słowa kluczowe:** niezawodność, zasilanie, system sygnalizacji włamania i napadu*

RELIABILITY ANALYSIS OF A TYPE B POWER SUPPLY USED IN A INTRUSION DETECTION SYSTEM (IDS)

1. Introduction

The Government Centre for Security developed a document titled „The National Critical Infrastructure Protection Programme" for the Republic in Poland, which mentions 11 systems falling within the critical infrastructure [5]:
- supply with power, power raw materials and fuels,
- communications,
- ICT networks,
- finances,
- food supply,
- water supply,
- health care
- transport,
- emergency services,
- ensuring continuity of the public administration operation,
- production, deposition, storage and the use of chemicals and radioactive substances, including pipelines with hazardous substances.

Their correct operation is necessary to ensure the functional continuity of domestic administrative structures, as well as to maintain a specific level of citizen safety. Among these systems, one of the most important is transport [9]. It includes [5]:
- railway transport,
- road transport,
- air transport,
- pipeline transport,
- inland shipping,
- maritime shipping.

Safe transport of people and goods requires ensuring an appropriate level of safety to transport facilities. It applies to both, stationary, as well as mobile objects. This is why electronic protection systems are used. They provide safety and are developed from the following systems, distinguished depending on the detected threats, as:
- intrusion detection systems (IDS),
- fire signalling systems,
- access control systems,
- CCTV systems,
- security systems for external areas.

The protection resulting from the functioning of these systems, often in very vast transport facilities, is supplemented by the following systems:
- health condition and personal threat alarm,
- environmental threat alarm,
- anti-theft,
- sound alarm systems,
- car protection against burglary and abduction.

One of the most important subsystems of the listed electronic safety systems are the alarm transmission systems. They include, i.a., ICT equipment and networks [16, 24], used to transfer information about the state of one or more security systems to one or more alarm reception centres (e.g. safety management centres).
In light of the currently potential terrorist acts and other threats of criminal nature, it is important for the security system integrated within the transport process counteracts them as much as possible. At the same time, the reliability-operational indicators of the utilized systems should have rational values [4, 11, 15], adequate to the protected facilities and the functions they execute. This is why the paper pay particular attention to the power supply systems used in intrusion detection systems.
An adequate safety level, which electronic safety systems of transport facilities are supposed to provide, depends not only on the efficiency of used individual safety systems [7, 10, 21, 27] but also on the correct functioning of the power supply systems (also, taking into account the electromagnetic interference [13, 18]). This is why the authors began with characterizing systems of such type, according to the information included in the standard PN-EN 50131-1:2009 "Alarm systems - Intrusion detection systems - System requirements".
Issues associated with the reliability of power systems have been taken into consideration by authors of different papers, both domestic and international, for many years. One of the more significant publications is [2]. It presents issues associated with the reliability of power systems. A relationship was determined between the reliability of the considered systems and the financial efforts allocated to increasing its value. Different primary reliability models of the systems were also presented, which take into account the intensity of failures and the repairs. This elaboration presents also a reliability chart, including the state of operability and inoperability and a chart additionally containing the status of a device's exclusion from the operation of the entire system.
One of the more important aspects of the reliability-operational analysis of the power systems is the power supply redundancy. This is why, the analysis of using back-up power supplies are very important. Such an approach was presented in the publications [25, 26]. These elaborations put strong emphasis on the emergency power supply systems. Such solutions are currently used very often in order to increase the state of readiness of the entire system (in particular, the ones falling within critical infrastructure and impacting a threat to human life). The mentioned elaboration analyses the solutions in the form of different power supplies, such as: uninterrupted power supplies UPS, generator sets, eco-friendly solutions in the form of solar panels or wind powered electricity generators. The performed studies allowed to state that using the mentioned solutions enables increasing the values of reliability-operational indicators. Of course, it is necessary for those systems to have correctly designed circuits controlling the switching between used electricity sources.

The power supplies used in electronic safety systems, and the ones used in transport facilities falling within the state critical infrastructure in particular, are required to meet many significant criteria. One of the most important include, i.a., high efficiency, miniaturization, functionality, appropriate values of reliability-operational indicators [1, 17, 19], the ability to diagnose subsystems taking into account the quality of information [23], resistance to electromagnetic interference [6, 12] and vibrations [3]. Satisfying these expectations requires the development of plausible reliability-operational models of power systems.
Despite the performed analysis in the scope of reliability and operation of power supply systems, it seems necessary to conduct research in terms of the functional analysis of power systems supplying electronic safety systems. Such an approach was already presented in previous elaboration of the authors of this paper, however, there are no detailed considerations in the scope of individual types of power supplies (taking into account the guidelines included in the PN-EN 50131-1:2009 standard).

2. Characteristics of a type B power supply used in a IDS according to the PN-EN 50131-1:2009 standard

An intrusion detection system, depending on the applied design solutions and the protection degree, requires a specific type of power supply. It is executed by a set of devices, which include [8, 14, 20]:

- a power feeder, ensuring primary power supply and power feed switching to a back-up source, as a result of the main power failure,
- a battery, usually in the form of a rechargeable, chemical power source.

Generally, the primary functions in the scope of the power system in intrusion detection systems are executed by an alarm control unit, with a power supply as its integral part. According to PN-EN 50131-12009: Alarm systems - Intrusion detection systems - System requirements" [22], the following types of power supplies used in IDSs are distinguished:

- type A: primary power source and a back-up power source, which is controlled and charged by the intrusion detection system,
- type B: primary power source and a back-up power source, which is not charged by the intrusion detection system,
- type C: primary power source with finite capacity.

Fig. 1 presents a type B power supply. It has a primary source, which is used to supply the IDS or its part in normal operating conditions. In the case of the primary power (~230 V AC), the switch to the back-up source is automatic and the current flows from a battery to the alarm system (fig. 1a). The battery is in no way recharged by the intrusion detection system. However, a solution is possible, in which a system is used which automatically controls and recharges the battery. It is not, however, a component of an alarm control unit.

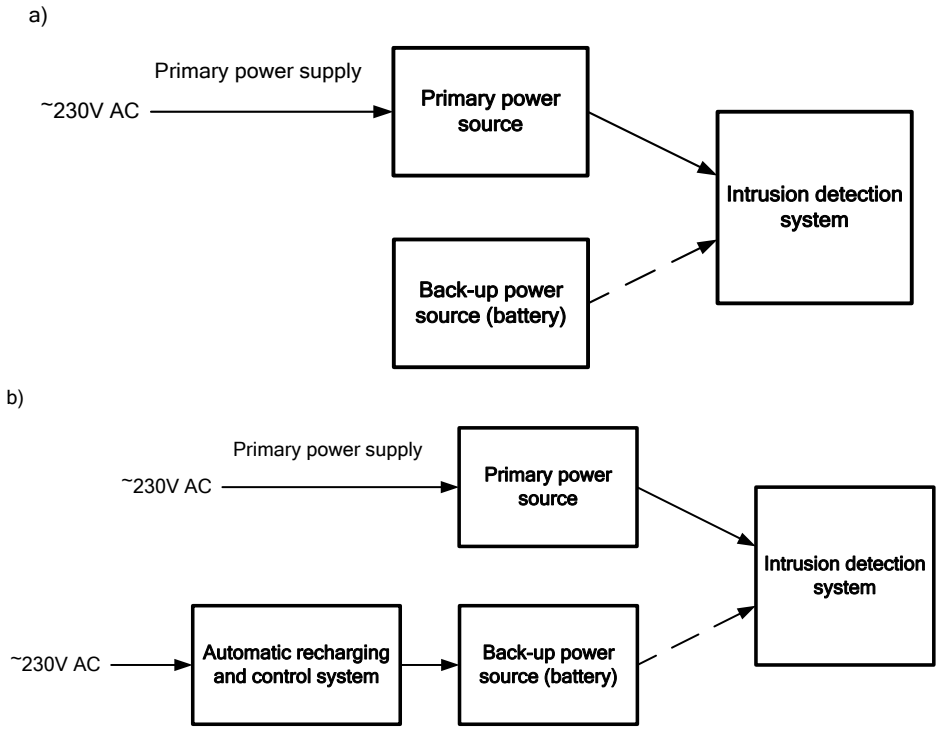


Fig. 1 An example of a type B power supply for an intrusion detection system: a) without recharging of a back-up power supply (battery), b) with control and automatic recharging of the back-up power supply (battery) [source: own elaboration]

3. A reliability-operational analysis of a type B power supply

Certain assessment criteria need to be adapted when performing a reliability-operational analysis of a type B power supply used in an IDS. It can be the reliability function, frequency of damage, intensity of damage, etc. The authors, however, chose the readiness indicator, since it enables to take into account the activities restoring the state of operability to the considered power supply systems. Generally, the readiness indicator may be expressed:

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

where: T_m - average correct operation time between failures,
T_n - average repair time.

The shown relationship indicates that a power supply can be in one of two states:

- operating state,
- repair state.

When considering the functioning of a type B power supply, a relationship graph will have a form presented in fig. 2. In the considered situation, an intrusion detection system does not diagnose a back-up power source, therefore, its technical condition is unknown (e.g. voltage, charge level, operating temperature). Therefore, there is a possibility of direct transition from a state of full operability to a state of inoperability.

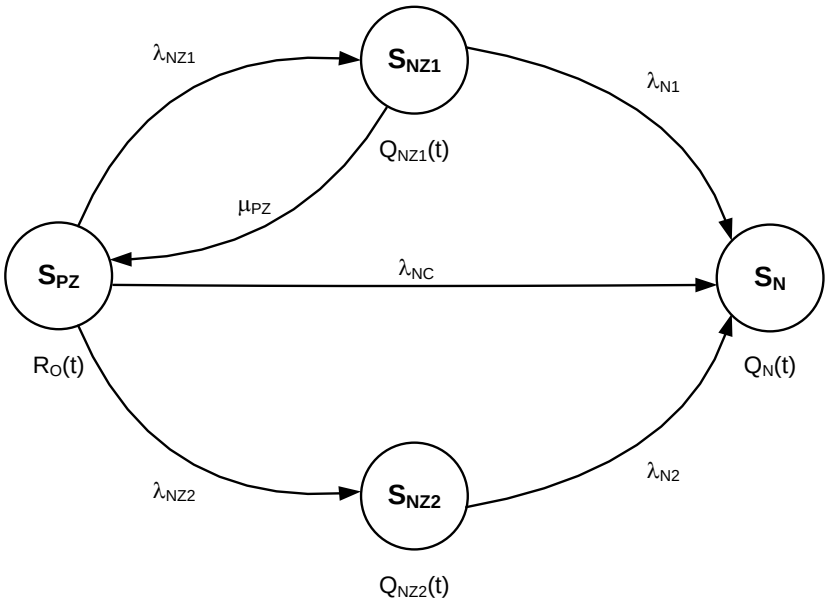


Fig. 2 Relationships of a type B power supply used in an IDS
Marking in the fig.: $R_O(t)$ – a probability function of a power supply in a state of full operability $Q_{NZ1}(t)$ – a probability function of a power supply in a state of partial operability 1, $Q_{NZ2}(t)$ – a probability function of a power supply in a state of partial operability 2, $Q_N(t)$ – a probability function of a power supply in a state of inoperability, λ_{NZ1}, λ_{NZ2} – intensities of transitions from a state of full operability to a state of partial operability μ_{PZ} – intensity of transition from a state of partial operability1 to a state of full operability, $\lambda_{N1,}$ λ_{N2} – intensities of transitions from a state of partial operability to a state of inoperability, λ_{NC} – intensity of transitions from a state of operability to a state of inoperability [source: own elaboration].

A failure of the primary power source causes a transition from a state of full operability S_{PZ} to a state of partial operability S_{NZ1}. Restoring a state of operability to the primary power supply causes a transition from a state of partial operability S_{NZ1} to a state of full operability $S_{PZ.}$ In the case of a type B power supply in state S_{NZ1} and a failure of the back-up power supply, a transition to a state of inoperability S_N takes place.

A damage of the back-up power source (with an operable primary power supply) causes a transition from a state of full operability S_{PZ} to a state of partial operability S_{NZ2}. Due to a lack of diagnosing of the back-up power source, it is impossible to switch from a state of partial operability S_{NZ2} to a state of full operability $S_{PZ.}$ In the case of a type B power supply in state S_{NZ2} and a failure of the back-up power supply, a transition to a state of inoperability S_N takes place.
Simultaneous damage of both power sources cause immediate transition from a state of full operability S_{PZ} to a state of inoperability S_N.
The system shown in Fig. 2 can be described by the following Chapman–Kolmogorov equations:

$$\begin{aligned}
R_0'(t) &= -\lambda_{NZ1} \cdot R_0(t) + \mu_{PZ} \cdot Q_{NZ1}(t) - \lambda_{NZ2} \cdot R_0(t) - \lambda_{NC} \cdot R_0(t) \\
Q_{NZ1}'(t) &= \lambda_{NZ1} \cdot R_0(t) - \mu_{PZ} \cdot Q_{NZ1}(t) - \lambda_{N1} \cdot Q_{NZ1}(t) \\
Q_{NZ2}'(t) &= \lambda_{NZ2} \cdot R_0(t) - \lambda_{N2} \cdot Q_{NZ2}(t) \\
Q_N'(t) &= \lambda_{N1} \cdot Q_{NZ1}(t) + \lambda_{N2} \cdot Q_{NZ2}(t) + \lambda_{NC} \cdot R_0(t)
\end{aligned} \tag{2}$$

Assuming baseline conditions:

$$\begin{aligned}
R_0(0) &= 1 \\
Q_{NZ1}(0) &= Q_{NZ2}(0) = Q_N(0) = 0
\end{aligned} \tag{3}$$

and applying the Laplace transform, the following system of linear equations is obtained:

$$\begin{aligned}
s \cdot R_0^*(s) - 1 &= -\lambda_{NZ1} \cdot R_0^*(s) + \mu_{PZ} \cdot Q_{NZ1}^*(s) - \lambda_{NZ2} \cdot R_0^*(s) - \lambda_{NC} \cdot R_0(t) \\
s \cdot Q_{NZ1}^*(s) &= \lambda_{NZ1} \cdot R_0^*(s) - \mu_{PZ} \cdot Q_{NZ1}^*(s) - \lambda_{N1} \cdot Q_{NZ1}^*(s) \\
s \cdot Q_{NZ2}^*(s) &= \lambda_{NZ2} \cdot R_0^*(s) - \lambda_{N2} \cdot Q_{NZ2}^*(s) \\
s \cdot Q_N^*(s) &= \lambda_{N1} \cdot Q_{NZ1}^*(s) + \lambda_{N2} \cdot Q_{NZ2}^*(s) + \lambda_{NC} \cdot R_0(t)
\end{aligned} \tag{4}$$

Transforming it, a record in the schematic view is obtained:

$$\begin{aligned}
R_0^*(s) &= \frac{b_1}{a \cdot b_1 - \lambda_{NZ1} \cdot \mu_{PZ}} \\
Q_{NZ1}^*(s) &= \frac{\lambda_{NZ1}}{a \cdot b_1 - \lambda_{NZ1} \cdot \mu_{PZ}} \\
Q_{NZ2}^*(s) &= \frac{b_1 \cdot \lambda_{NZ2}}{a \cdot b_1 \cdot b_2 - b_2 \cdot \lambda_{NZ1} \cdot \mu_{PZ}} \\
Q_N^*(s) &= \frac{b_1 \cdot b_2 \cdot \lambda_{NC} + b_2 \cdot \lambda_{N1} \cdot \lambda_{NZ1} + b_1 \cdot \lambda_{N2} \cdot \lambda_{NZ2}}{a \cdot b_1 \cdot b_2 \cdot s - b_2 \cdot s \cdot \lambda_{NZ1} \cdot \mu_{PZ}}
\end{aligned} \tag{5}$$

where:

$$\begin{aligned} a &= s + \lambda_{NZ1} + \lambda_{NZ2} + \lambda_{NC} \\ b_1 &= s + \mu_{PZ} + \lambda_{N1} \\ b_2 &= s + \lambda_{N2} \end{aligned} \tag{6}$$

With the use of computer assistance, it is possible to make calculations enabling the determination of the probability value for a type B power supply to be in a state of full operability. Such a procedure is shown in the following example.

Example

Let us assume the following values describing the analysed system:

- duration of research – 1 year (the value of this time is given in the units as hours [h]):

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

- intensity of transitions from a state of complete operability to a state of partial operability I λ_{NZ1}:

$$\lambda_{NZ1} = 0{,}000001$$

- intensity of transitions from a state of complete usability to a state of partial usability II λ_{NZ2}:

$$\lambda_{NZ2} = 0{,}0000001$$

- intensity of transitions from a state of partial operability I to a state of inoperability λ_{N1}:

$$\lambda_{N1} = 0{,}0000001$$

- intensity of transitions from a state of partial operability II to a state of inoperability λ_{N2}:

$$\lambda_{N2} = 0{,}000001$$

- intensity of transitions from a state of full operability to a state of inoperability λ_{NC}:

$$\lambda_{NC} = 0{,}00000001$$

- intensity of transitions from a state of partial operability I to a state of full operability μ_{PZ}:

$$\mu_{PZ} = 0{,}1$$

As a result of transformations, we obtain:

$$R_0(t) = 0{,}000009999902\, e^{-0{,}1000011\, t} + 0{,}999990000097999\, e^{-1{,}099999\, t}$$

As a final result, we obtain: $R_O = 0{,}999026875$

The practical application of the presented considerations allows the determination of the impact of the intensity values of transition from a state of partial operability to a state of full operability μ_{PZ} on the probability value of the system's staying in a state of full operability. Intensity μ_{PZ} shall be understood as the inverse of time t_{PZ}, which determines the time of restoring full operability.
The presented type B model assumes that the state of inoperability is an absorbing state. The aim of comparing all sorts of manufacturer solutions and their use in actual conditions is for an IDS not to achieve this state.
The presented model of a type B power supply in intrusion detection systems may be used to determine the probability values of the analysed systems being in the states of: full operability S_{PZ}, partial operability S_{NZ1} and S_{NZ2} inoperability S_N. It will then make it possible to compare different types of solution and to select a specific one, which meets the assumed criteria.

4. Conclusions

The paper presents reliability-operational considerations regarding a type B power supply used in intrusion detection systems. This takes into account the guidelines regarding power supplies included in the standard "PN-EN 50131-1:2009: Alarm systems - Intrusion Detection System". This enabled the development of a relation graph in the considered system, and next, to obtain the relationships allowing the calculation of the probability values of the analysed systems staying in the states of: full operability S_{PZ}, partial operability S_{NZ1} and S_{NZ2} inoperability S_N. In further scientific considerations, the authors plan to conduct analyses and develop models, taking into consideration the diagnosis process.

5. References

[1] Będkowski L., Dąbrowski T.: Podstawy eksploatacji, cz. II Podstawy niezawodności eksploatacyjnej. Wojskowa Akademia Techniczna, Warszawa 2006.
[2] Billinton R., Allan R. N.: Reliability evaluation of power systems. New York: Plenum Press, 1996.
[3] Burdzik R., Konieczny Ł.: Research on structure, propagation and exposure to general vibration in passenger car for different damping parameters. Journal of Vibroengineering Vol. 15, Issue 4, 2013, pp. 1680-1688.
[4] Dyduch J., Paś J., Rosiński A.: The basis of the exploitation of transport electronic systems. Publisher Technical University of Radom, Radom 2011.
[5] Government Security Centre, National Programme for Critical Infrastructure Protection. Annex 1: Summary of critical infrastructure systems, Warsaw 2013.
[6] Kaniewski P., Lesnik C., Susek W., Serafin P.: Airborne Radar Terrain Imaging System. 16th International Radar Symposium (IRS), Dresden, Germany, 2015. pp. 248-253.
[7] 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.

[8] Korczak D., Rosiński A.: A discussion of the reliability and performance of the power supply systems used in the airport security systems. In: the monograph „Wyzwania inżynierii ruchu lotniczego", editor: J. Skorupski, Warsaw University of Technology, Faculty of Transport, Warsaw 2016. pp. 129-137.
[9] Kłodawski M., Lewczuk K., Jacyna-Gołda I., Zak J.: Decision making strategies for warehouse operations. Archives of Transport, vol. 41, issue 1, 2017. pp. 43-53.
[10] Łubkowski P, Laskowski D.: Selected issues of reliable identification of object in transport systems using video monitoring services. In: „Communication in Computer and Information Science", editor: J. Mikulski, vol. 471. Springer, Berlin Hedelberg 2015. pp. 59-68.
[11] Paś J.: Operation of electronic transportation systems. Publishing House University of Technology and Humanities in Radom, Radom 2015.
[12] Paś J.: Shock a disposable time in electronic security systems. Journal of KONBiN, 2(38)2016. pp. 5-31.
[13] Paś J., Siergiejczyk M.: Interference impact on the electronic safety system with a parallel structure. Diagnostyka, Vol. 17, No. 1, 2016. pp. 49-55.
[14] Rosinski A., Dabrowski T.: Modelling reliability of uninterruptible power supply units. Eksploatacja i Niezawodnosc – Maintenance and Reliability, Vol.15, No. 4, 2013. pp. 409-413.
[15] Rosiński A.: Modelling the maintenance process of transport telematics systems. Publishing House Warsaw University of Technology, Warsaw 2015.
[16] Rychlicki M., Kasprzyk Z.: Increasing performance of SMS based information systems. In: „Proceedings of the Ninth International Conference Dependability and Complex Systems DepCoS-RELCOMEX", given as the monographic publishing series – „Advances in intelligent systems and computing", Vol. 286. Springer, 2014. pp. 373-382.
[17] 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", given as the monographic publishing series – „Advances in intelligent systems and computing", vol. 365. Springer 2015. pp. 435-443.
[18] 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,vol. 10, issue 9, 2016, pp. 587–593.
[19] Siergiejczyk M., Rosiński A., Krzykowska K.: Reliability assessment of supporting satellite system EGNOS. In: W. Zamojski, J. Mazurkiewicz, J. Sugier, T. Walkowiak, J. Kacprzyk (eds) New results in dependability and computer systems, given as the monographic publishing series – „Advances in intelligent and soft computing", Vol. 224. Springer, 2013. pp. 353-364.
[20] Siergiejczyk M., Rosiński A.: Analysis of power supply maintenance in transport telematics system. „Solid State Phenomena" vol. 210 (2014). pp. 14-19.

[21] Skorupski J., Uchroński P.: A fuzzy reasoning system for evaluating the efficiency of cabin luggage screening at airports. Transportation Research Part C - Emerging Technologies 54, 2015. pp. 157-175.
[22] Standard PN-EN 50131-1:2009: Alarm systems - Intrusion and hold-up systems - System requirements.
[23] 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: L. Podofillini, B. Sudret, B. Stojadinovic, E. Zio, W. Kröger. CRC Press/Balkema, 2015. pp. 2685-2691.
[24] Sumiła M., Miszkiewicz A.: Analysis of the problem of interference of the public network operators to GSM-R. In: the monograph „Tools of Transport Telematics",editors: J. Mikulski, given as the monographic publishing series – „Communications in Computer and Information Science", Vol. 531, Springer, 2015, pp. 76-82.
[25] Wiatr J., Miegoń M.: Zasilacze UPS oraz baterie akumulatorów w układach zasilania gwarantowanego. Warszawa: Dom Wydawniczy MEDIUM, 2008.
[26] Wiatr J.: Zespoły prądotwórcze w układach awaryjnego zasilania obiektów budowlanych. Warszawa: Dom Wydawniczy MEDIUM, 2009.
[27] Wiśnios M., Dąbrowski T., Bednarek M.: Metoda zwiększania poziomu bezpieczeństwa zapewnianego przez system biometrycznej kontroli dostępu. Przegląd Elektrotechniczny 2015, nr 10, s. 229-232.

Prof. Miroslaw Siergiejczyk, PhD. Eng. *- scientific fields of interest of the paper co-author concern among other issues of architecture and services provided by telecommunications networks and systems, especially from perspective of their applications in transport, reliability and operation of telecommunications networks and systems, modelling, designing and organising telecommunications systems for transport.*

Małgorzata Pędzierska Eng.*- scientific fields of interest of the paper co-author concern among the intelligent transport systems, their influence of traffic safety and reliability analysis of electronic safety systems.*

Adam Rosiński Ph.D. 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.*

ANALIZA NIEZAWODNOŚCIOWA ZASILACZA TYPU B ZASTOSOWANEGO W SSWIN

1. Wstęp

W opracowanym przez Rządowe Centrum Bezpieczeństwa dokumencie pt. „Narodowy Program Ochrony Infrastruktury Krytycznej" w Rzeczypospolitej Polskiej, wymieniono 11 systemów zaliczanych do infrastruktury krytycznej [5]:

- zaopatrzenia w energię, surowce energetyczne i paliwa,
- łączności,
- sieci teleinformatycznych,
- finansowe,
- zaopatrzenia w żywność,
- zaopatrzenia w wodę,
- ochrony zdrowia,
- transportowe,
- ratownicze,
- zapewniające ciągłość działania administracji publicznej,
- produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Ich prawidłowe funkcjonowanie jest niezbędne, by zapewnić ciągłość funkcjonowania struktur administracyjnych kraju, jak też i utrzymania określonego poziom bezpieczeństwa obywateli. Wśród wymienionych systemów jednym z istotniejszych jest transport [9]. W skład niego zaliczono [5]:

- transport kolejowy,
- transport samochodowy,
- transport lotniczy,
- transport rurociągowy,
- żeglugę śródlądową,
- żeglugę morską.

Bezpieczny przewóz osób i towarów wymaga zapewnienia odpowiedniego poziomu bezpieczeństwa obiektom transportowym. Dotyczy to zarówno obiektów stacjonarnym jak i ruchomym. Dlatego też stosuje się systemy ochrony elektronicznej. Zapewniają one bezpieczeństwo i są tworzone z następujących systemów wyróżnianych zależnie od wykrywanych zagrożeń, jako systemy:

- sygnalizacji włamania i napadu (SSWiN),
- sygnalizacji pożaru,
- kontroli dostępu,
- monitoringu wizyjnego,
- ochrony terenów zewnętrznych.

Ochrona wynikająca z funkcjonowania tych systemów, dość często w rozległych terytorialne obiektach transportowych, jest uzupełniana przez systemy:
- sygnalizacji stanu zdrowia lub zagrożenia osobistego,
- sygnalizacji zagrożeń środowiska,
- przeciwkradzieżowe,
- dźwiękowe systemy ostrzegawcze,
- zabezpieczenia samochodów przed włamaniem i uprowadzeniem.

Jednym z istotniejszych podsystemów wymienionych elektronicznych systemów bezpieczeństwa są systemy transmisji alarmu. W skład nich wchodzą m.in. urządzenia i sieci teleinformatyczne [16,24], wykorzystywane do przekazywania informacji o stanie jednego lub więcej systemów bezpieczeństwa do jednego lub kilku alarmowych centrów odbiorczych (np. centrów zarządzania bezpieczeństwem).

Wobec występujących obecnie potencjalnych aktów terrorystycznych i innych zagrożeń o charakterze kryminalnym, istotne jest by w procesie transportowym zintegrowany system bezpieczeństwa możliwie jak najszerzej im przeciwdziałał. Jednocześnie też wskaźniki niezawodnościowo-eksploatacyjne stosowanych systemów powinny mieć racjonalne wartości [4,11,15], adekwatnie do chronionych obiektów i realizowanych przez nie funkcji. Dlatego też w artykule zwrócono szczególną uwagę na układy zasilania zastosowane w systemach sygnalizacji włamania i napadu.

Odpowiedni poziom bezpieczeństwa jaki mają zapewnić elektroniczne systemy bezpieczeństwa obiektów transportowych, jest zależy nie tylko od skuteczności zastosowanych poszczególnych systemów bezpieczeństwa [7,10,21,27], ale także od prawidłowego funkcjonowania układów zasilających (także z uwzględnieniem zakłóceń elektromagnetycznych [13,18]). Dlatego też autorzy na początku scharakteryzowali tego rodzaju systemy zgodnie z informacjami zawartymi w normie PN-EN 50131-1:2009 „Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Wymagania systemowe".

Kwestie związane z niezawodnością systemów zasilania są rozważane przez różnych autorów w pozycjach literaturowych zarówno krajowych jak i międzynarodowych już od wielu lat. Jedną z istotniejszych publikacji jest pozycja [2]. Przedstawiono w niej zagadnienia związane z niezawodnością systemów energetycznych. Wyznaczono zależność pomiędzy niezawodnością rozpatrywanych systemów, a nakładami finansowymi przeznaczonymi na zwiększenie jej wartości. Zaprezentowano także różne podstawowe modele niezawodnościowe systemów, które uwzględniają intensywności uszkodzeń i intensywności napraw. W opracowaniu tym przedstawiono także graf niezawodnościowy zawierający stan zdatności i niezdatności oraz graf zawierający dodatkowo stan wykluczenia urządzenia z pracy całego systemu.

Jednym z istotniejszych aspektów analizy niezawodnościowo-eksploatacyjnej systemów zasilania, jest redundancja zasilania. Dlatego też bardzo ważne są analizy zastosowania rezerwowych źródeł zasilania. Takie podejście przedstawiono w publikacjach [25,26].

W opracowaniach tych dużą uwagę zwrócono na systemy zasilania awaryjnego. Takie rozwiązania są obecnie bardzo często stosowane w celu zwiększenia poziomu gotowości całego systemu (w szczególności tych zaliczanych do infrastruktury krytycznej i mających wpływ na zagrożenie życia osób). W wymienionych opracowaniach dokonano analizy rozwiązań w postaci różnych zasilacz, takich jak: zasilacze bezprzerwowe UPS, zespoły prądotwórcze, ekologiczne rozwiązania w postaci paneli solarnych czy generatorów prądu napędzanych siłą wiatru. Przeprowadzone rozważania pozwoliły stwierdzić, iż zastosowanie wymienionych rozwiązań umożliwia zwiększenie wartości wskaźników niezawodnościowo-eksploatacyjnych. Oczywiście niezbędne są w tych systemach prawidłowo zaprojektowane układy sterujące przełączaniem pomiędzy zastosowanymi źródłami energii elektrycznej.
Od zasilaczy stosowanych w elektronicznych systemach bezpieczeństwa, a w szczególności w zastosowanych w obiektach transportowych zaliczanych do infrastruktury krytycznej państwa, wymaga się spełnienia wielu istotnych kryteriów. Do jednych z ważniejszych można zaliczyć m. in. duża sprawność, miniaturyzację, funkcjonalność, odpowiednie wartości wskaźników niezawodnościowo-eksploatacyjnych [1,17,19], możliwość diagnozowania podsystemów z uwzględnieniem jakości informacji [23], odporność na zakłócenia elektromagnetyczne [6,12] i wibracje [3]. Spełnienie tych oczekiwań wymaga opracowania wiarygodnych modeli niezawodnościowo-eksploatacyjnych systemów zasilających.
Pomimo przeprowadzonych analiz z zakresu niezawodności i eksploatacji systemów zasilania, wydaje się konieczne przeprowadzenie rozważań z zakresu analizy funkcjonalnej układów zasilających elektroniczne systemy bezpieczeństwa. Takie podejście zostało już zaprezentowane we wcześniejszych opracowaniach autorów niniejszego artykułu, ale brak jest szczegółowych rozważań z zakresu poszczególnych typów zasilaczy (z uwzględnieniem wytycznych zawartych w normie PN-EN 50131-1:2009).

2. Charakterystyka zasilacza typu B zastosowanego w SSWiN według normy PN-EN 50131-1:2009

System sygnalizacji włamania i napadu, zależnie od zastosowanych rozwiązań konstrukcyjnych i stopnia zabezpieczenia, wymaga określonego rodzaju zasilania. Jest ono realizowane za pomocą zespołu urządzeń, w skład których można zaliczyć [8,14,20]:

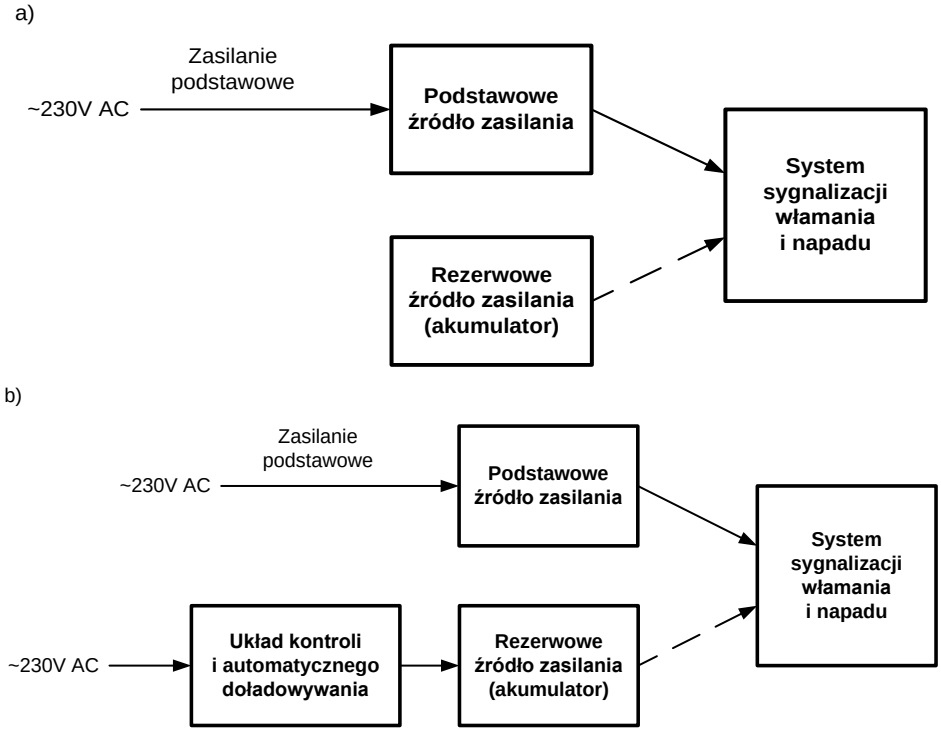
- urządzenie zasilające, zapewniające zasilanie podstawowe oraz przełączenie zasilania na rezerwowe źródło w przypadku zaniku zasilania głównego,
- akumulator, zwykle w postaci ładowalnego, chemicznego źródła energii.

W systemach sygnalizacji włamania i napadu najczęściej podstawowe funkcje z zakresu układu zasilania realizuje centrala alarmowa, której integralną częścią jest zasilacz.

Według normy „PN-EN 50131-1:2009: Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Wymagania systemowe” [22] wyróżnia się następujące typy zasilaczy stosowanych w SSWiN:

- typ A: podstawowe źródło zasilania i rezerwowe źródło zasilania, które jest kontrolowane i doładowywane przez system sygnalizacji włamania i napadu,
- typ B: podstawowe źródło zasilania i rezerwowe źródło zasilania, które nie jest doładowywane przez system sygnalizacji włamania i napadu,
- typ C: podstawowe źródło zasilania o skończonej pojemności.

Na rys. 1 przedstawiono zasilacz typu B. Zastosowano w nim źródło podstawowe, które jest wykorzystywany do zasilania SSWiN lub jego części w normalnych warunkach pracy. W przypadku zaniku zasilania podstawowego (~230 V AC) następuje automatyczne przełączenie na źródło rezerwowe i prąd płynie z akumulatora do systemu alarmowego (rys. 1a). Akumulator nie jest w żaden sposób doładowywany przez system sygnalizacji włamania i napadu. Możliwe jest jednak rozwiązanie, w którym to zastosowano układ kontroli i automatycznego doładowywania akumulatora. Nie jest on jednak elementem składowym centrali alarmowej.



Rys. 1 Przykład zasilacza typu B systemu sygnalizacji włamania i napadu: a) przy braku doładowywania zasilacza rezerwowego (akumulatora), b) z kontrolą i automatycznym doładowywaniem zasilacza rezerwowego (akumulatora) [źródło: opracowanie własne]

3. Analiza niezawodnościowo-eksploatacyjna zasilacza typu B

Dokonując analizy niezawodnościowo-eksploatacyjnej zasilacza typu B zastosowanego w SSWiN należy przyjąć określone kryteria ich oceny. Może to być funkcja niezawodności, gęstość uszkodzeń, intensywność uszkodzeń, itp. Autorzy zdecydowali się jednak na wskaźnik gotowości, ponieważ umożliwia on uwzględnienie czynności przywracających stan zdatności rozpatrywanym układom zasilania. Ogólnie wskaźnik gotowości, można zapisać:

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

gdzie: T_m - średni czas poprawnej pracy między uszkodzeniami,
T_n - średni czas naprawy.

Z przedstawionej zależności wynika, że zasilacz może znajdować się w jednym z dwóch stanów:

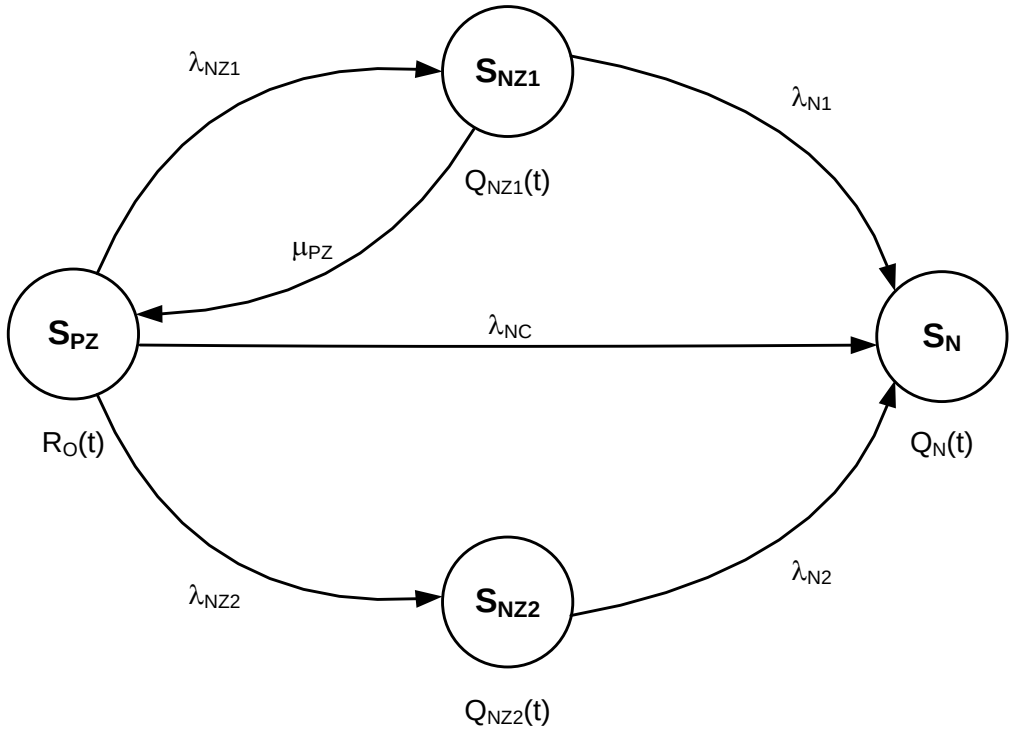
- stan użytkowania,
- stan naprawy.

Rozpatrując funkcjonowanie zasilacza typu B, graf relacji będzie miał postać przedstawioną na rys. 2. W rozpatrywanej sytuacji system sygnalizacji włamania i napadu nie diagnozuje rezerwowego źródła zasilania, a zatem nie jest znany jego stan techniczny (np. napięcie, poziom naładowania, temperatura pracy). Zatem istnieje możliwość bezpośredniego przejścia ze stanu pełnej zdatności do stanu niezdatności.

Uszkodzenie podstawowego źródła zasilania powoduje przejście ze stanu pełnej zdatności S_{PZ} do stanu niepełnej zdatności S_{NZ1}. Przywrócenie stanu zdatności zasilaniu podstawowemu powoduje przejście ze stanu niepełnej zdatności S_{NZ1} do stanu pełnej zdatności $S_{PZ.}$ W przypadku, gdy układ zasilacza typu B znajduje się w stanie S_{NZ1} i nastąpi uszkodzenie rezerwowego źródła zasilania, to następuje przejście do stanu niezdatności S_N.

Uszkodzenie rezerwowego źródła zasilania (przy zdatnym zasilaniu podstawowym) powoduje przejście ze stanu pełnej zdatności S_{PZ} do stanu niepełnej zdatności S_{NZ2}. Wobec braku diagnozowania rezerwowego źródła zasilania nie ma możliwości przejścia ze stanu niepełnej zdatności S_{NZ2} do stanu pełnej zdatności $S_{PZ.}$ W przypadku, gdy układ zasilacza typu B znajduje się w stanie S_{NZ2} i nastąpi uszkodzenie podstawowego źródła zasilania, to następuje przejście do stanu niezdatności S_N.

Uszkodzenie jednoczesne obu źródeł zasilania powoduje bezpośrednie przejście ze stanu pełnej zdatności S_{PZ} do stanu niezdatności S_N.



Rys. 2 Relacje w zasilaczu typu B zastosowanego w SSWiN
Oznaczenia na rys.: $R_O(t)$ – funkcja prawdopodobieństwa przebywania zasilacza w stanie pełnej zdatności, $Q_{NZ1}(t)$ – funkcja prawdopodobieństwa przebywania zasilacza w stanie niepełnej zdatności 1, $Q_{NZ2}(t)$ – funkcja prawdopodobieństwa przebywania zasilacza w stanie niepełnej zdatności 2, $Q_N(t)$ – funkcja prawdopodobieństwa przebywania zasilacza w stanie niezdatności, λ_{NZ1}, λ_{NZ2} – intensywności przejść ze stanu pełnej zdatności do stanu niepełnej zdatności, μ_{PZ} – intensywność przejścia ze stanu niepełnej zdatności 1 do stanu pełnej zdatności, λ_{N1}, λ_{N2} – intensywności przejść ze stanu niepełnej zdatności do stanu niezdatności, λ_{NC} – intensywność przejść ze stanu pełnej zdatności do stanu niezdatności [źródło: opracowanie własne]

System przedstawiony na rys. 2 może być opisany następującymi równaniami Kołmogorowa-Chapmana:

$$\begin{aligned}
R_0'(t) &= -\lambda_{NZ1} \cdot R_0(t) + \mu_{PZ} \cdot Q_{NZ1}(t) - \lambda_{NZ2} \cdot R_0(t) - \lambda_{NC} \cdot R_0(t) \\
Q_{NZ1}'(t) &= \lambda_{NZ1} \cdot R_0(t) - \mu_{PZ} \cdot Q_{NZ1}(t) - \lambda_{N1} \cdot Q_{NZ1}(t) \\
Q_{NZ2}'(t) &= \lambda_{NZ2} \cdot R_0(t) - \lambda_{N2} \cdot Q_{NZ2}(t) \\
Q_N'(t) &= \lambda_{N1} \cdot Q_{NZ1}(t) + \lambda_{N2} \cdot Q_{NZ2}(t) + \lambda_{NC} \cdot R_0(t)
\end{aligned} \tag{2}$$

Przyjmując warunki początkowe:

$$R_0(0) = 1$$
$$Q_{NZ1}(0) = Q_{NZ2}(0) = Q_N(0) = 0 \tag{3}$$

oraz stosując przekształcenie Laplace'a otrzymujemy następujący układ równań liniowych:

$$\begin{aligned}
&s \cdot R_0^*(s) - 1 = -\lambda_{NZ1} \cdot R_0^*(s) + \mu_{PZ} \cdot Q_{NZ1}^*(s) - \lambda_{NZ2} \cdot R_0^*(s) - \lambda_{NC} \cdot R_0(t) \\
&s \cdot Q_{NZ1}^*(s) = \lambda_{NZ1} \cdot R_0^*(s) - \mu_{PZ} \cdot Q_{NZ1}^*(s) - \lambda_{N1} \cdot Q_{NZ1}^*(s) \\
&s \cdot Q_{NZ2}^*(s) = \lambda_{NZ2} \cdot R_0^*(s) - \lambda_{N2} \cdot Q_{NZ2}^*(s) \\
&s \cdot Q_N^*(s) = \lambda_{N1} \cdot Q_{NZ1}^*(s) + \lambda_{N2} \cdot Q_{NZ2}^*(s) + \lambda_{NC} \cdot R_0(t)
\end{aligned} \tag{4}$$

Przekształcając go otrzymujemy zapis w ujęciu schematycznym:

$$R_0^*(s) = \frac{b_1}{a \cdot b_1 - \lambda_{NZ1} \cdot \mu_{PZ}}$$

$$Q_{NZ1}^*(s) = \frac{\lambda_{NZ1}}{a \cdot b_1 - \lambda_{NZ1} \cdot \mu_{PZ}}$$

$$Q_{NZ2}^*(s) = \frac{b_1 \cdot \lambda_{NZ2}}{a \cdot b_1 \cdot b_2 - b_2 \cdot \lambda_{NZ1} \cdot \mu_{PZ}} \tag{5}$$

$$Q_N^*(s) = \frac{b_1 \cdot b_2 \cdot \lambda_{NC} + b_2 \cdot \lambda_{N1} \cdot \lambda_{NZ1} + b_1 \cdot \lambda_{N2} \cdot \lambda_{NZ2}}{a \cdot b_1 \cdot b_2 \cdot s - b_2 \cdot s \cdot \lambda_{NZ1} \cdot \mu_{PZ}}$$

gdzie:

$$\begin{aligned}
a &= s + \lambda_{NZ1} + \lambda_{NZ2} + \lambda_{NC} \\
b_1 &= s + \mu_{PZ} + \lambda_{N1} \\
b_2 &= s + \lambda_{N2}
\end{aligned} \tag{6}$$

Stosując wspomaganie komputerowe można przeprowadzić obliczenia umożliwiające wyznaczenie wartości prawdopodobieństwa przebywania zasilacza typu B w stanie pełnej zdatności. Postępowanie takie przedstawia poniższy przykład.

Przykład

Przyjmijmy następujące wartości opisujące analizowany układ:

- czas badań – 1 rok (wartość tego czasu podano w jednostkach, jako godz. [h]):
$$t = 8760 \ [h]$$
- intensywności przejść ze stanu pełnej zdatności do stanu niepełnej zdatności I λ_{NZ1}:
$$\lambda_{NZ1} = 0{,}000001$$
- intensywności przejść ze stanu pełnej zdatności do stanu niepełnej zdatności II λ_{NZ2}:
$$\lambda_{NZ2} = 0{,}0000001$$
- intensywności przejść ze stanu niepełnej zdatności I do stanu niezdatności λ_{N1}:
$$\lambda_{N1} = 0{,}0000001$$
- intensywności przejść ze stanu niepełnej zdatności II do stanu niezdatności λ_{N2}:
$$\lambda_{N2} = 0{,}000001$$
- intensywności przejść ze stanu pełnej zdatności do stanu niezdatności λ_{NC}:
$$\lambda_{NC} = 0{,}00000001$$
- intensywności przejść ze stanu niepełnej zdatności I do stanu pełnej zdatności μ_{PZ}:
$$\mu_{PZ} = 0{,}1$$

W wyniku przekształceń otrzymujemy:

$$R_0(t) = 0{,}000009999902\, e^{-0{,}1000011\, t} + 0{,}999990000097999\, e^{-1{,}099999\, t}$$

Jako wynik końcowy otrzymujemy: $R_O = 0{,}999026875$

Praktyczne zastosowanie zaprezentowanych rozważań pozwala na określenie wpływu wartości intensywności przejścia ze stanu niepełnej zdatności I do stanu pełnej zdatności μ_{PZ} na wartość prawdopodobieństwa przebywania zasilacza w stanie pełnej zdatności. Intensywność μ_{PZ} należy rozumieć jako odwrotności czasu t_{PZ} który określa czas przywrócenia stanu pełnej zdatności.

W przedstawionym modelu zasilacza typu B założono, iż stan niezdatności jest stanem pochłaniającym. Porównując różnego rodzaju rozwiązania producenckie i ich użytkowanie w warunkach rzeczywistych, dąży się, aby ten stan nie był osiągnięty przez SSWiN.

Przedstawiony model zasilacza typu B stosowanego w systemach sygnalizacji włamania i napadu może posłużyć do wyznaczenia wartości prawdopodobieństw przebywania analizowanych systemów w stanach: pełnej zdatności S_{PZ}, niepełnej zdatności S_{NZ1} i S_{NZ2} oraz niezdatności S_N. Umożliwi to wówczas porównanie różnego rodzaju rozwiązań i wyboru określonego, spełniającego założone kryteria.

4. Podsumowanie

W artykule zaprezentowano rozważania niezawodnościowo-eksploatacyjne dotyczące zasilacza typu B zastosowanego w systemach sygnalizacji włamania i napadu. Uwzględniono w tym celu wytyczna dotyczące zasilaczy zawarte w normie „PN-EN 50131-1:2009: Systemy alarmowe – Systemy sygnalizacji włamania i napadu". Umożliwiło to opracowanie grafu relacji w rozpatrywanym układzie, a następnie uzyskania zależności pozwalających obliczyć wartości prawdopodobieństw przebywania analizowanych systemów w stanach: pełnej zdatności S_{PZ}, niepełnej zdatności S_{NZ1} i S_{NZ2} oraz niezdatności S_N. W dalszych rozważaniach naukowych autorzy planują przeprowadzenie analiz i opracowanie modeli z uwzględnieniem procesu diagnozowania.

5. Literatura

[1] Będkowski L., Dąbrowski T.: Podstawy eksploatacji, cz. II Podstawy niezawodności eksploatacyjnej. Wojskowa Akademia Techniczna, Warszawa 2006.
[2] Billinton R., Allan R. N.: Reliability evaluation of power systems. New York: Plenum Press, 1996.
[3] Burdzik R., Konieczny Ł.: Research on structure, propagation and exposure to general vibration in passenger car for different damping parameters. Journal of Vibroengineering Vol. 15, Issue 4, 2013, pp. 1680-1688.
[4] Dyduch J., Paś J., Rosiński A.: The basis of the exploitation of transport electronic systems. Publisher Technical University of Radom, Radom 2011.
[5] Government Security Centre, National Programme for Critical Infrastructure Protection. Annex 1: Summary of critical infrastructure systems, Warsaw 2013.
[6] Kaniewski P., Lesnik C., Susek W., Serafin P.: Airborne Radar Terrain Imaging System. 16th International Radar Symposium (IRS), Dresden, Germany, 2015. pp. 248-253.
[7] 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.
[8] Korczak D., Rosiński A.: A discussion of the reliability and performance of the power supply systems used in the airport security systems. In: the monograph „Wyzwania inżynierii ruchu lotniczego", editor: J. Skorupski, Warsaw University of Technology, Faculty of Transport, Warsaw 2016. pp. 129-137.
[9] Kłodawski M., Lewczuk K., Jacyna-Gołda I., Zak J.: Decision making strategies for warehouse operations. Archives of Transport, vol. 41, issue 1, 2017. pp. 43-53.
[10] Łubkowski P, Laskowski D.: Selected issues of reliable identification of object in transport systems using video monitoring services. In: „Communication in Computer and Information Science", editor: J. Mikulski, vol. 471. Springer, Berlin Hedelberg 2015. pp. 59-68.

[11] Paś J.: Operation of electronic transportation systems. Publishing House University of Technology and Humanities in Radom, Radom 2015.
[12] Paś J.: Shock a disposable time in electronic security systems. Journal of KONBiN, 2(38)2016. pp. 5-31.
[13] Paś J., Siergiejczyk M.: Interference impact on the electronic safety system with a parallel structure. Diagnostyka, Vol. 17, No. 1, 2016. pp. 49-55.
[14] Rosinski A., Dabrowski T.: Modelling reliability of uninterruptible power supply units. Eksploatacja i Niezawodnosc – Maintenance and Reliability, Vol.15, No. 4, 2013. pp. 409-413.
[15] Rosiński A.: Modelling the maintenance process of transport telematics systems. Publishing House Warsaw University of Technology, Warsaw 2015.
[16] Rychlicki M., Kasprzyk Z.: Increasing performance of SMS based information systems. In: „Proceedings of the Ninth International Conference Dependability and Complex Systems DepCoS-RELCOMEX", given as the monographic publishing series – „Advances in intelligent systems and computing", Vol. 286. Springer, 2014. pp. 373-382.
[17] 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", given as the monographic publishing series – „Advances in intelligent systems and computing", vol. 365. Springer 2015. pp. 435-443.
[18] 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,vol. 10, issue 9, 2016, pp. 587–593.
[19] Siergiejczyk M., Rosiński A., Krzykowska K.: Reliability assessment of supporting satellite system EGNOS. In: W. Zamojski, J. Mazurkiewicz, J. Sugier, T. Walkowiak, J. Kacprzyk (eds) New results in dependability and computer systems, given as the monographic publishing series – „Advances in intelligent and soft computing", Vol. 224. Springer, 2013. pp. 353-364.
[20] Siergiejczyk M., Rosiński A.: Analysis of power supply maintenance in transport telematics system. „Solid State Phenomena" vol. 210 (2014). pp. 14-19.
[21] Skorupski J., Uchroński P.: A fuzzy reasoning system for evaluating the efficiency of cabin luggage screening at airports. Transportation Research Part C - Emerging Technologies 54, 2015. pp. 157-175.
[22] Standard PN-EN 50131-1:2009: Alarm systems - Intrusion and hold-up systems - System requirements.
[23] 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: L. Podofillini, B. Sudret, B. Stojadinovic, E. Zio, W. Kröger. CRC Press/Balkema, 2015. pp. 2685-2691.

[24] Sumiła M., Miszkiewicz A.: Analysis of the problem of interference of the public network operators to GSM-R. In: the monograph „Tools of Transport Telematics",editors: J. Mikulski, given as the monographic publishing series – „Communications in Computer and Information Science", Vol. 531, Springer, 2015, pp. 76-82.
[25] Wiatr J., Miegoń M.: Zasilacze UPS oraz baterie akumulatorów w układach zasilania gwarantowanego. Warszawa: Dom Wydawniczy MEDIUM, 2008.
[26] Wiatr J.: Zespoły prądotwórcze w układach awaryjnego zasilania obiektów budowlanych. Warszawa: Dom Wydawniczy MEDIUM, 2009.
[27] Wiśnios M., Dąbrowski T., Bednarek M.: Metoda zwiększania poziomu bezpieczeństwa zapewnianego przez system biometrycznej kontroli dostępu. Przegląd Elektrotechniczny 2015, nr 10, s. 229-232.

Prof. nadzw. dr hab. inż. Mirosław Siergiejczyk *- zainteresowania naukowe współautora referatu obejmują między innymi problemy architektury i usług systemów i sieci telekomunikacyjnych ze szczególnym uwzględnieniem możliwości ich wykorzystania w transporcie, niezawodności i eksploatacji systemów i sieci teleinformatycznych, modelowanie, projektowanie i organizacja sieci i systemów teleinformatycznych w transporcie. (Share 33,3%)*

Inż. Małgorzata Pędzierska *- zainteresowania naukowe współautorki obejmują inteligentne systemy transportowe, ich wpływ na bezpieczeństwo ruchu drogowego oraz zagadnienia analizy niezawodnościowo-eksploatacyjnej elektronicznych systemów bezpieczeństwa. (Share 33,3%)*

Dr hab. inż. Adam Rosiński *- zainteresowania naukowe współautora referatu obejmują analizę niezawodnościowo-eksploatacyjną systemów telematyki transportu oraz inteligentnych systemów transportowych. W dorobku naukowym posiada kilkadziesiąt publikacji naukowych. (Share 33,3%)*