

Krzysztof JAKUBOWSKI¹, Jacek PAŚ²

¹ Ministry of National Defence (Ministerstwo Obrony Narodowej, Legionowo)

² Military University of Technology (Wojkowa Akademia Techniczna)

RELIABILITY ANALYSIS OF ALARM SIGNALS TRANSMITTING SYSTEMS USED TO MONITORING BUILDINGS

Niezawodność systemów transmisji sygnałów alarmowych stosowanych w monitorowaniu obiektów

Abstract: The article presents a general method for identifying the security risk factor for alarm signal transmission systems (ASTS), which are used in monitoring buildings and critical infrastructure. The security of the transmission of alarm signals to an alarm receiving center (ARC) is a property of the process, which is associated with performing of tasks and functions, human factor, hardware and environment components. The process of transmitting alarm signals should be characterized by minimizing risk of external and internal interception/distortion or deformation of transmitted signals and in ideal case signals should be encrypted and integrity checked. Determining the security risk indicator for ASTS will allow optimal organization of electronic security systems.

Keywords: signal transmission systems, model system, reliability

Streszczenie: W artykule przedstawiona została wstępna metoda określenia niezawodności systemów transmisji sygnałów alarmowych (STSA) w monitorowaniu obiektów budowlanych i infrastruktury krytycznej. Bezpieczeństwo transmisji sygnałów alarmowych to właściwość realizowanego procesu. Proces transmisji sygnałów alarmowych powinien charakteryzować się minimalizowaniem ryzyka, a w idealnym przypadku – przy zastosowaniu np. szyfrowania – brakiem wystąpienia zagrożeń związanych z przechwyceniem sygnału. Wyznaczenie niezawodności STSA umożliwi optymalną organizację elektronicznych systemów bezpieczeństwa (ESB), w tym STSA. W dalszych badaniach związanych z realizacją pracy badawczej dla różnych konfiguracji ESB zostaną wyznaczone wskaźniki niezawodności w oparciu o dane eksploatacyjne.

Słowa kluczowe: systemy transmisji sygnałów, model systemu, niezawodność

1. General issues regarding the alarm signal transmission system in object monitoring

The concept of signal transmission system in object monitoring is perceived in this article as an ordered system of three subsystems: electronic security system (ESS), transmitter and receiver of the transmission channel (s) and the alarm receiving center (ARC) [6, 9, 11, 15] - fig. 1. These systems create a logical internally balanced whole, which enables to achieve specific goal – i.e. sending alarm signals [16, 17]. Modelling the functioning of transmission systems by using deterministic models is not always possible [5, 7]. The results (realizations) are affected by external and internal disturbances (random factors - e.g. electromagnetic interference), which make it impossible to accurately predict subsequent states [10, 12, 14, 18]. In such cases, we model systems' behaviour by using probabilistic methods, e.g. stochastic processes [2, 7, 17, 19]. An important class of stochastic processes are Markov processes. Some applications of these processes are presented in [6, 7, 9, 17]. The basis of their use is the fulfilment of Markov's property: the future does not depend on the past when the present is known. An alternative to technical systems, e.g. signal transmission not satisfying Markov's properties, are classic reliability methods [5, 8, 14, 17]. These methods allow to determinate empirical characteristics regarding, for example, stream or renewal intensity [17] and time to the next damage [2, 8, 13, 17]. This makes it possible to calculate the main system evaluation measures on their basis [3, 6, 17, 19]. In the literature, as part of similar reliability tests, various models are presented [7, 8, 14, 17], including semi-Markov [4] as well as those using artificial neural networks, reliability models [5, 6, 8, 17] or e.g. error trees. There are no studies in available literature that relate to the reliability analysis of alarm signal transmission systems in ESS [6, 8, 9, 17]. Scientific studies on this issue only present general requirements for signal transmission paths in signal transmission applications [6, 9, 11, 17]. The authors of the article presented general considerations and graph of the process of operation of these systems. In further research, it is planned to determine the indicators of the process of operation of these systems based on research of real technical facilities. The selection of the type of alarm transmission system to Emergency Receiving Center (ERC) should depend on the required level of information reliability or confidentiality [9, 16, 17]. In order to increase the transmission reliability, the construction facility - receiving center uses more independent transmission channels - information excess. Fig. 1 shows the safety system with one transmission channel [3, 8].

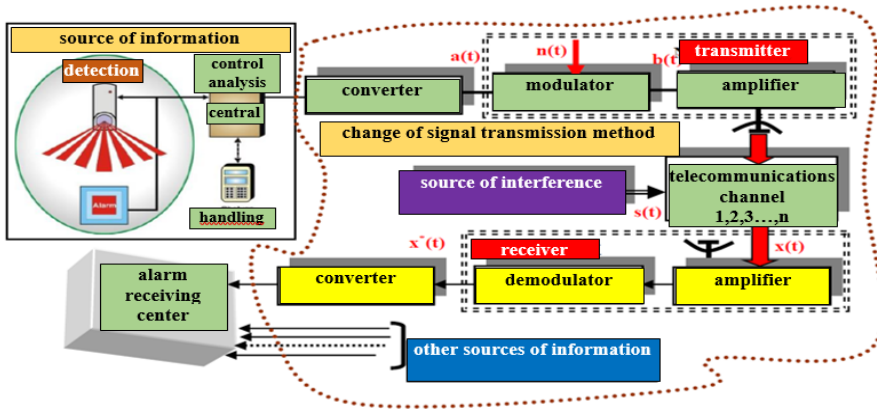


Fig. 1. A simplified diagram of a transceiver in the electronic security systems (ESS) wireless, where $a(t)$ - the modulating signal $x^*(t)$ - reconstructed the modulating signal in the demodulator, $n(t)$ - noise signal $b(t)$ - modulated signal of high frequency when modulator, $s(t)$ - source of interference in the telecommunications channel - electromagnetic wave propagation

In order to achieve information redundancy, ESS can be connected to a remote center using more than one transmission link. e.g. a separate wireless and digital transmission path through a public switched or digital network with radio transmission - fig. 2 [15, 16]. In monitoring systems, automatic signals and propagation conditions that prevent the proper functioning of STSA should cause a fault signal to be sent to ERC. Communication between the alarm system and the receiving center should meet certain requirements that relate to the appropriate class of security system [17]. In technical conditions, after the technical object has been transferred to the investor, the degree of deterioration of the alarm transmission system properties in the event of exceeding a certain transmission speed should be given [15,16]. This deterioration should be gradual, e.g. the transmission time should increase slowly until the speed of sending signals equivalent to one signal per minute from transmitters covering up to 10% of the system capacity is achieved and there should be a return to the state in which the requirements of the PN - 93 / E standard are met - 08390/51 [1, 9, 15].

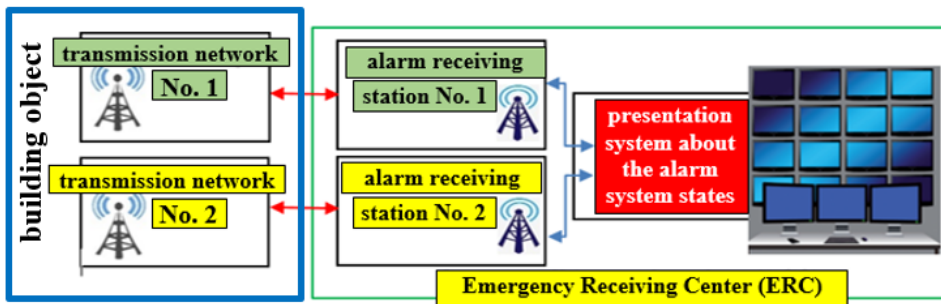


Fig. 2. Information redundancy at STSA - construction works - ERC

All connections should be tested in STSA and ERC - wired and wireless between individual elements and system devices e.g. short circuit, opening, tamper or damage - fig. 3. The element responsible in the ESB for this function is the control panel (CA) which generates reference signals connected to individual transmission channels or detection lines where the system elements are located - fig. 4. In ESB there is a priority of the alarm signal over testing [1, 7, 18]. When the detector detects a threat and reporting the alarm to CA, testing is interrupted and the security system returns to the alarmed state.

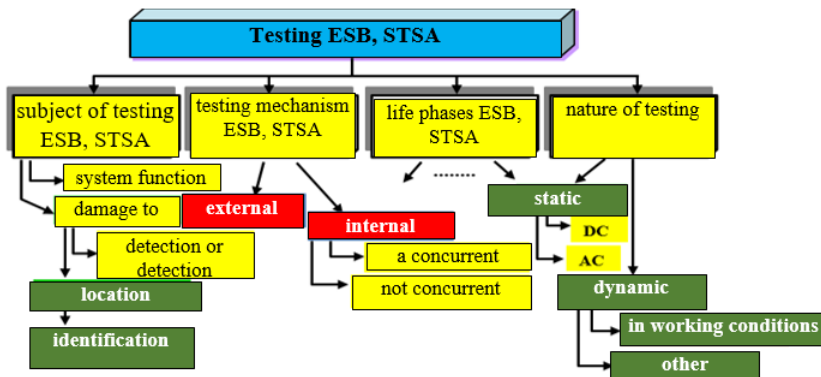


Fig. 3. Testing all internal and external connections, wired and wireless in the ESS.

In ESS, all connections between individual components and devices that make up ESS can be divided as follows:

- wired connections (including fiber optic),
- wireless connections using coded modulation - analogue or digital using a wireless path using an electromagnetic field at a specific frequency, eg 433; 866 MHz [6, 9, 17].

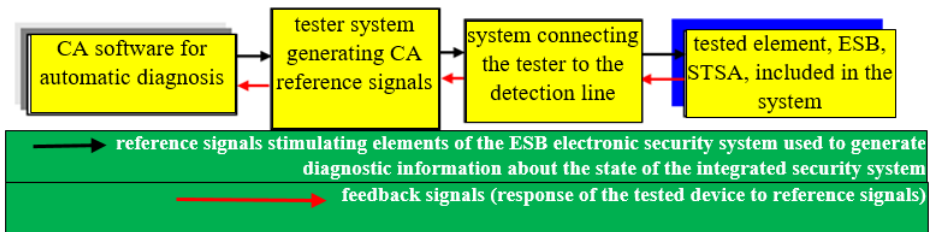


Fig. 4. Implementation of testing, i.e. diagnosis of technical conditions in the ESS and STSA via the control panel

In ESBs that have a redundant information structure in STSA, the following reliability states can be distinguished:

- airworthiness condition ϵ_Z - all system functions are correctly carried out,
- failure condition ϵ_N - all functions are performed incorrectly, so-called time of unavailability of the signal transmission system,

- partial suitability of the ε_{ZN} security system - only certain functions are correctly implemented by making the connection, eg. through one channel [8, 11, 17, 19].

The time during which the alarm transmission system is considered inaccessible is the period from the last moment of which it is known that the transmission system was available, i.e. without damage, until damage was detected, repaired and the transmission system track checked [15, 16].

2. Analysis of the flow of information in the system alarm signals and damages in the ESS

Figure 5 shows the organizational requirements- technical Commander-in-Chief of the State Fire Service (SFS) functional diagram of the fire alarm transmission system UTASU device [15, 16]. The device is installed in a supervised facility. From UTASU, the signal (alarm or damage) is transmitted via a wired or wireless transmission network directly to the fire alarm receiving center (FARC) or via the intermediary station of the GSM system operator. Damage signals from fire alarm system (FAS) are directed directly to the operator - the service team, whose task is to constantly monitor the technical condition and respond to damage at a specified time. For ESS-supervised facilities that can be classified as critical infrastructure - e.g. military units, public buildings - three independent alarm signal transmission paths are used due to the reliability of the connection - fig. 6. The first element of the Fire Alarm Transmission System (FATS) is These tracks work in the so-called hot reserve and the alarm system operator or the user decides about the time and period of testing the line (connects) the supervised object - the user [15,16]. Link testing (short circuit, opening, no connection, device replacement, tamper, etc.) is carried out automatically by the security control panel [15, 16].

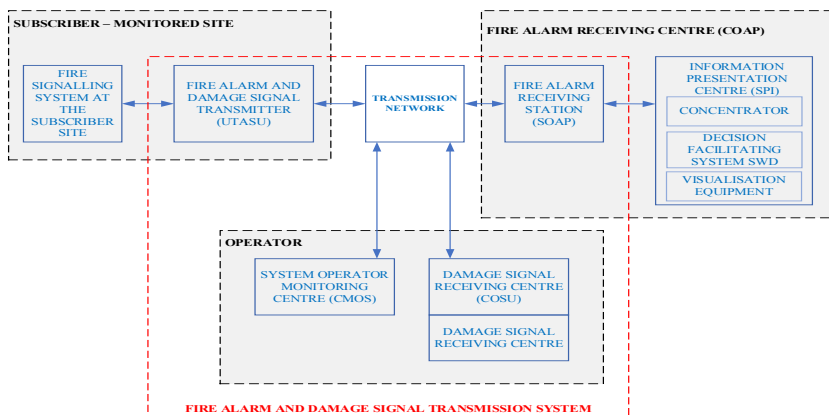


Fig. 5. The scheme of transmission of fire alarms and damage signals in the fire alarm system (FAS) (based on [15, 16])

In the event of an alarm signal - the system's response to burglary, robbery, fire, etc. during the test time, this operating mode is automatically switched off and the technical object enters the basic working state, e.g. supervision [7, 18]. When performing manual attempts to establish communication during connection checking (supervised object - user - ACO) with the participation of the service team and the security system user, a note should be made regarding the operation of the alarm signal transmission system. This note should be stored in the documentation of the main safety system - table 1 [15, 16].

Table 1

Test and trial table for STSA (2nd stage alarm triggered) connection- protected facility - Rescue and Fire Fighting Unit (RaFFU) PSP [15, 16]

Test STSA (alarm level II) do (RaFFU) PSP Warszawa		Attempts have been made to transmit alarm signals to RaFFU PSP					
		Detection line No. 1		Detection line No. 2		Detection line No. n	
		MCP	sensor	M CP	sensor	MCP	sensor
FAS operating mode - supervision	Radio track	X	X	—	X	X	X
	Phonetrack	X	X	X	X	X	X

where: x - connection via radio and telephone via STSA,- no connection via radio via STSA in detection line 2 for a manual call point (MCP).

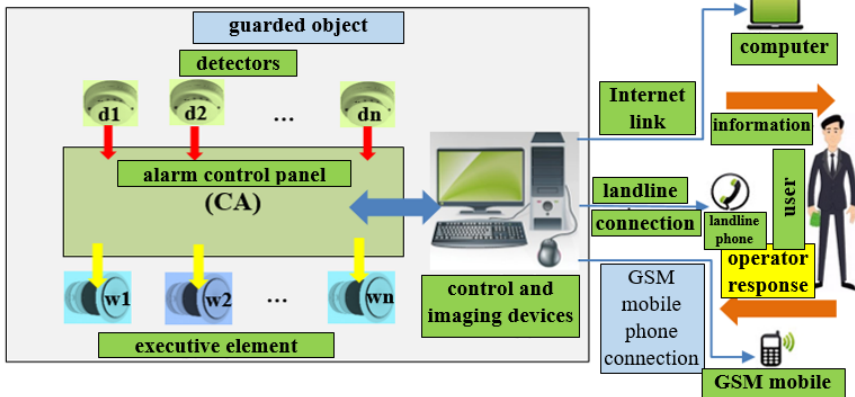


Fig. 6. Diagram of the alarm signal and damage signal transmission system in electronic security systems

3. Reliability structure of selected alarm and damage signal transmission systems

The organization of alarm and damage signal transmission systems to the user and the receiving center depends on the type of protected objects and the threats. In intruder alarm systems and robbery (IASaR) we distinguish four different classes of these systems. In the III and IV class for IASaR, STSA is required depending on the type of threats and accumulated goods of high material or intangible value (religious buildings, libraries, museums, etc.). In class IV, we always use two independent paths for transmitting information on hazards - alarms. The testing period and time at IASaR is carried out by the system executive system - the control panel. The graph of the STSA system operation process is shown in figs. 7 and 8 for two different variants of the security system connection, which are shown in figs. 1 and 2. In the case of fire alarm systems, the device for transmitting alarm and damage signals is mandatory [15, 16]. This is specified in laws, regulations and SSP regulations. In SSP, fire alarm control panel (FACP) in the supervised facility it is wired to the first element of the fire alarm transmission system, which is the UTASU device - fig. 5. UTASU is installed in a supervised facility, usually near the IASaR. This is most often implemented in the same room where the security service or service team is located. From UTASU, the signal is transmitted via the transmission network directly to the COAP or via the system operator's intermediate station to the event visualization system or to the mobile synoptic table [15, 16].

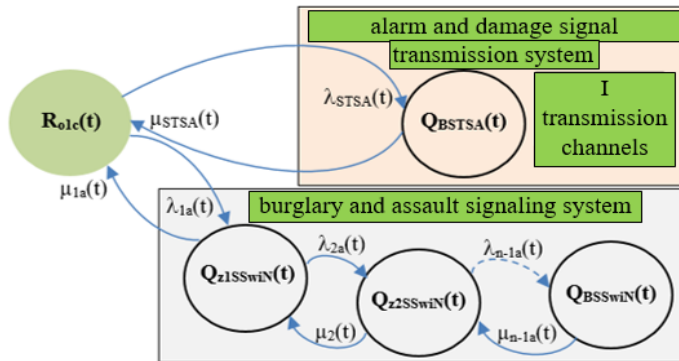


Fig. 7. Graph of the STSA operation process for UTASU as in fig. 1

Considering the graphs of the STSA operation process for the alarm and fault signal transmission system - figs. 7 to 9, it can be seen that in the simplest information transmission system there are only two operating states - $R_{01c}(t)$ - the function of the probability of the system being in the state of full SPZ and $Q_{BSTSA}(t)$ - the function of the probability of STSA being in the security system (SS) security unreliability - fig. 7.

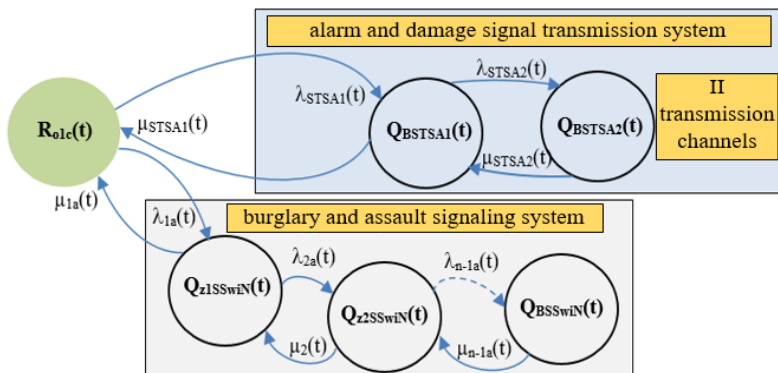


Fig. 8. Graph of the STSA exploitation process chart for UTASU as in fig. 2

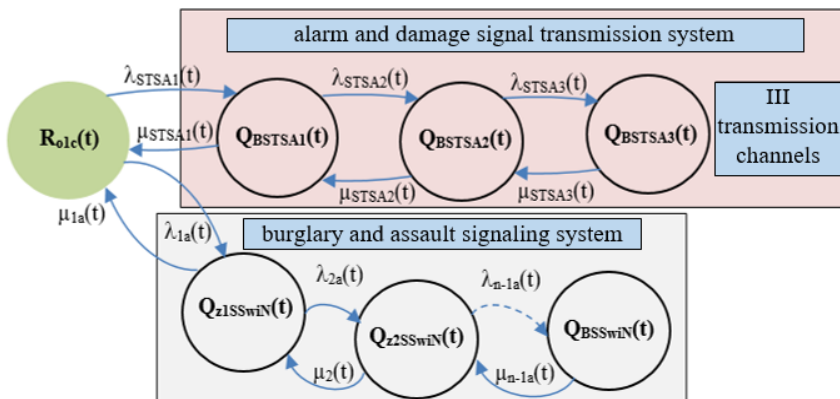


Fig. 9. Graph of the STSA operation process for UTASU as in fig. 6

Fault signals that occur in electronic security systems are sent directly to the system operator - the service team. For protected facilities that are very important for your operation, the service team is always available at the system's place of use, and has a specific time to intervene, i.e. repair damage with an intensity of pass μ_{1-5z} transitions from $Q_{BSTSA}(t)$ safety failure to $R_{01c}(t)$ full airworthiness of the ARF. By using two or three alarm and damage signal transmission channels in electronic security systems, we obtain a redundant information structure - figs. 8, 9 [6, 17]. The use of such technical solutions is forced by very important functions that perform protected objects. They are classified as so-called critical infrastructure of a given country. Damage to a single alarm signal transmission channel does not cause STSA to switch to SS security failure. In the technical solution, as in fig. 8, there is a single state $Q_{BSTSA1}(t)$ - i.e. the function of the probability of the system being in the security threat state of

SMS, while using the solution with three independent transmission channels we obtain two states of security threat SZB - $Q_{BSTSA1}(t)$, $Q_{BSTSA2}(t)$. Damage to all three independent information transfer channels causes the electronic security system to switch to $Q_{BSTSA3}(t)$ - the function of the probability of the system staying in the SS security failure mode - fig. 9. In the event of damage to the system, the operator is obliged to immediately notify the alarm receiving center of the damage that prevents sending the fire alarm of the supervised object [6,17]. After making the repair, the operator notifies that the system has been restored.

4. Conclusions

The independent alarm and fault signal transmission system as well as the electronic safety system have a complex non-reliability, mixed parallel-series structure. There is a system in the alarm signal transmission system, in which various types of redundancy can be used, e.g. additional components - e.g. transmitters, receivers; endurance - various types of routes and cable assemblies which are arranged in metal housings, information - various ways of transmitting information to alarm and damage information presentation systems. The purpose of using such technical solutions in electronic security systems is to increase the reliability of these systems in all operating states, e.g. supervision, damage or alarming. The systems also use the principle of safe damage, especially in alarm control panels and STSA. Single damage to the system does not cause catastrophic damage. The alarm transmission device installed in the same facility that supervises the system should be located in the same fire-separated room, which significantly affects the reliability of the transmission of fire signals and damage. The alarm and fault signal transmission system must always be based on a cable connection and a radio transmission system. Further in the STSA research, it is expected to obtain actual operational data and determine safety indicators of the operation process. In further studies, the authors of this article plan to determine the indicators of the operation process of real STSA SSP.

5. References

1. Ding Q., Peng Z., Liu T., Tong Q.: Building Fire Alarm System with Multi-sensor and Information Fusion Technology Based on D-S Evidence Theory, 2014 International Symposium on Computer, Consumer and Control, Taichung, 2014, DOI 10.1109/IS3C.2014.238.
2. Foucher B., Boullie J., Meslet B., Das D.: A review of reliability prediction methods for electronic devices. *Microelectronics Reliability* 2002; 42(8): DOI 10.1016/S0026-2714(02)00087-2.
3. Joglar F.: Reliability, Availability, and Maintainability. In M. Hurley (ed.), „SFPE Handbook of Fire Protection Engineering”, DOI 10.1007/978-1-4939-2565-0_74.

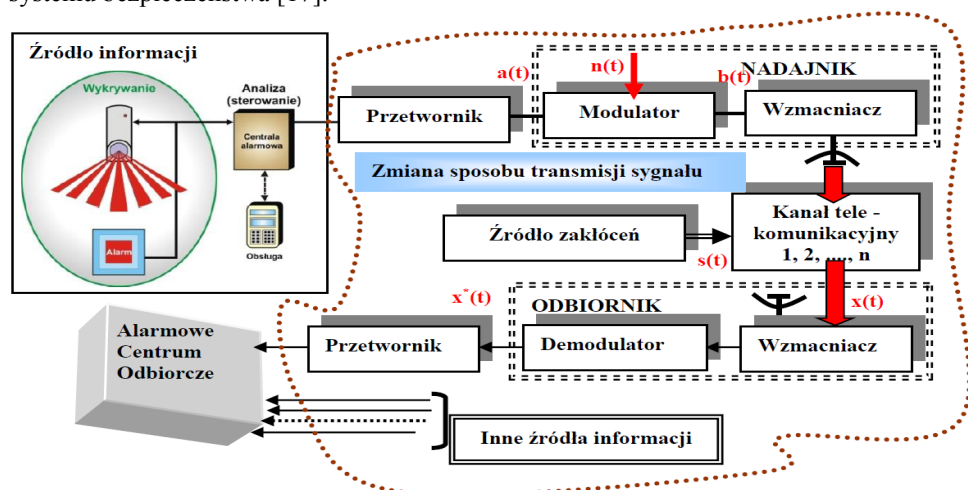
4. Knopik L., Migawa K.: Semi-Markov system model for minimal repair maintenance. *Eksplatacja i Niezawodność – Maintenance and Reliability* 2019; 21 (2), DOI 10.17531/ein.2019.2.9.
5. Kheir N.A., Holmes W.M.: On Validating Simulation Models of Missile Systems. *Simulation*; 30(4), 1978, DOI 10.1177/003754977803000404.
6. Klimczak T., Paś J.: Selected issues of the reliability and operational assessment of a fire alarm system, *Eksplatacja i Niezawodność – Maintenance and Reliability*, Vol. 21, No. 4, DOI 10.17531/ein.2019.4.3, 2019.
7. Kołowrocki K., Soszyńska-Budny J.: Complex Technical System Operation Processes Identification. In: *Reliability and Safety of Complex Technical Systems and Processes*. Springer Series in Reliability Engineering. Springer, London 2011.
8. McLeish J., Blattau N.: CAE apps for physics of failure reliability & durability simulations. In *2014 Reliability and Maintainability Symposium, IEEE 2014*, DOI 10.1109/RAMS.2014.6798444.
9. Paś J., Klimczak T.: Operational System Modelling in a Focused Fire Alarm System with an Open and Signal Detection Circuit Supervising Railway Station Premises. *Research Methods and Solutions to Current Transport Problems. ISCT21 2019. Advances in Intelligent Systems and Computing*, vol. 1032. Springer, Cham, DOI 10.1007/978-3-030-27687-4_31.
10. Paś J., Choromański W.: Results of measurement and determination of threshold electric field component for transport security systems. *Archives of Transport Systems Telematics*, Vol. 8, Iss. 1, 2015.
11. Paś J.: Selected methods for increases reliability the of electronic systems security. *Journal of KONBiN*, 3(35), 2015, DOI 10.1515/jok-2015-047.
12. Paś J.: Shock a disposable time in electronic security systems. *Journal of KONBiN*, 2(38), 2016, DOI 10.1515/jok-2016-0016.
13. Pecht M., Gu J.: Physics-of-failure-based prognostics for electronic products. *Transactions of the Institute of Measurement and Control* 2009; 31(3-4), DOI 10.1177/0142331208092031.
14. Pecht MG, Nash FR. Predicting the reliability of electronic equipment. *Proceedings of the IEEE* 1994; 82(7), DOI 10.1109/5.293157.
15. PN-EN 54-21:2009 Systemy sygnalizacji pożarowej. Część 21: Urządzenia transmisji alarmów pożarowych i sygnałów uszkodzeniowych.
16. PN-EN 54-25:2011, PN-EN 54-25:2011/AC:2012 Systemy sygnalizacji pożarowej. Część 25: Podzespoły wykorzystujące łącza radiowe.
17. Rosiński A.: *Modelling the maintenance process of transport telematics systems*, Publishing House Warsaw University of Technology, Warsaw 2015.
18. Xu, Chen, Yang: Optimal replacement policy for safety-related multi-component multi-state systems. *Reliability Engineering and System Safety* 2012; 99: DOI 10.1016/j.ress.2011.11.010.
19. Wawrzyński W.: *Bezpieczeństwo systemów sterownia w transporcie*. Biblioteka Problemów Eksploatacji, Warszawa 2004.

NIEZAWODNOŚĆ SYSTEMÓW TRANSMISJI SYGNAŁÓW ALARMOWYCH STOSOWANYCH W MONITOROWANIU OBIEKTÓW

1. Ogólne zagadnienia dotyczące systemu transmisji sygnałów alarmowych w monitorowaniu obiektów

Pojęcie systemu transmisji sygnałów w monitorowaniu obiektów postrzegane jest w niniejszym artykule jako uporządkowany układ trzech podsystemów: elektronicznego systemu bezpieczeństwa (ESB), nadajnika i odbiornika kanału(-ów) transmisyjnych oraz alarmowego centrum odbiorczego (ACO) [6, 9, 11, 15] – rys. 1. Systemy te tworzą logiczną, zrównoważoną wewnątrznie całość, umożliwiającą osiągnięcie konkretnego celu, tj. przesłanie sygnałów alarmowych [16, 17]. Modelowanie funkcjonowania systemów transmisyjnych, za pomocą modeli deterministycznych nie zawsze jest możliwe [5, 7]. Na wyniki (realizacje) wpływają zaburzenia zewnętrzne i wewnętrzne (czynniki losowe, np. zakłócenia elektromagnetyczne), które uniemożliwiają dokładne przewidywanie kolejnych stanów [10, 12, 14, 18]. W takich przypadkach zachowanie systemów modelujemy metodami probabilistycznymi, np. za pomocą procesów stochastycznych [2, 7, 17, 19]. Ważną klasę procesów stochastycznych stanowią procesy Markowa. Pewne możliwości zastosowań tych procesów przedstawiono w pracach [6, 7, 9, 17]. Podstawą ich użycia jest spełnienie własności Markowa: przyszłość nie zależy od przeszłości, gdy znana jest teraźniejszość. Alternatywą dla systemów technicznych, np. transmisji sygnałów niespełniających własności Markowa, są klasyczne metody niezawodnościowe [5, 8, 14, 17]. Metody te pozwalają na wyznaczenie empirycznych charakterystyk dotyczących np. strumienia czy intensywności odnowy [17] i czasu do następnego uszkodzenia [2, 8, 13, 17]. Umożliwia to obliczanie na ich podstawie głównych miar oceny systemu [3, 6, 17, 19]. W literaturze, w ramach podobnych badań niezawodnościowych prezentowane są różne modele [7, 8, 14, 17], w tym semi-Markowa [4], a także wykorzystujące sztuczne sieci neuronowe, modele niezawodnościowe [5, 6, 8, 17] czy np. drzewa błędów. W dostępnej literaturze brak jest opracowań, które dotyczą analizy niezawodnościowej systemów transmisji sygnałów alarmowych w ESB [6, 8, 9, 17]. W opracowaniach naukowych dotyczących tego zagadnienia przedstawiono tylko wymagania ogólne dotyczące torów transmisji sygnałów w zastosowaniach do transmisji sygnałów [6, 9, 11, 17]. Autorzy artykułu przedstawili ogólne rozważania i graf procesu eksploatacji tych systemów. W dalszych badaniach planowane jest wyznaczenie wskaźników procesu eksploatacji tych

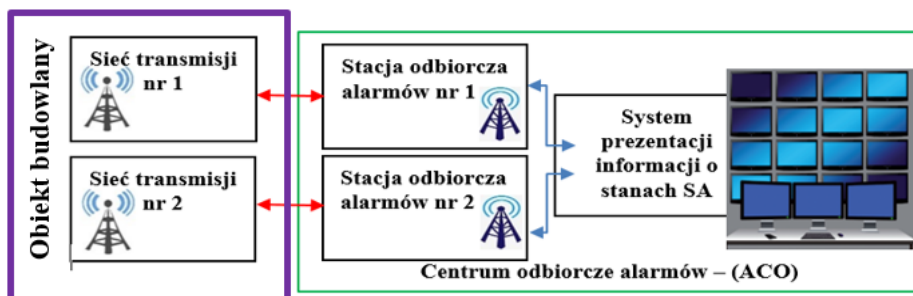
systemów w oparciu o badania rzeczywistych obiektów technicznych. Wybór typu systemu transmisji alarmu do ACO powinien być zależny od wymaganego poziomu niezawodności lub poufności informacji [9, 16, 17]. W celu zwiększenia niezawodności transmisji obiekt budowlany – centrum odbiorcze stosuje się więcej niezależnych kanałów transmisyjnych – nadmiar informacyjny. W celu osiągnięcia nadmiarowości informacji elektroniczny system bezpieczeństwa (ESB) może być połączony z centrum oddalonym za pomocą więcej niż jednego łącza transmisji, np. wydzieloną drogą transmisyjną bezprzewodową i cyfrowo przez publiczną sieć komutowaną lub cyfrową z transmisją radiową – rys. 2 [15, 16]. W systemach monitorowania automatycznie sygnały i warunki propagacji, które uniemożliwiają prawidłowe funkcjonowanie STSA, powinny spowodować nadanie sygnału uszkodzenia do ACO. Komunikacja między systemem alarmowym a alarmowym centrum odbiorczym powinna spełniać określone wymagania, które dotyczą odpowiedniej klasy systemu bezpieczeństwa [17].



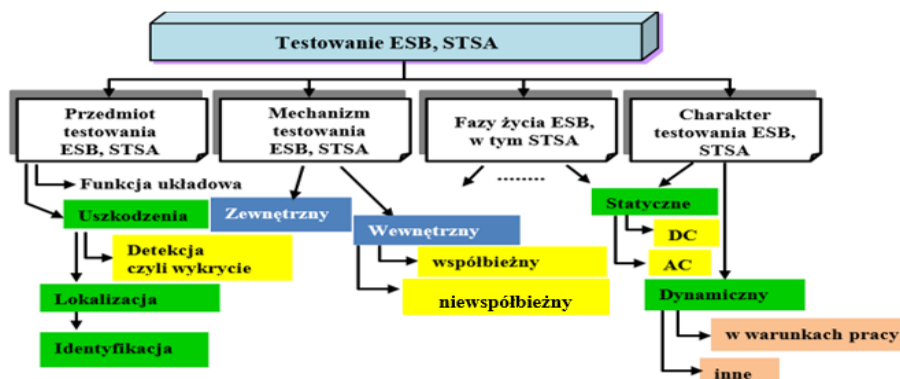
Rys. 1. Uproszczony schemat urządzenia nadawczo-odbiorczego w ESB bezprzewodowym, gdzie: $a(t)$ – sygnał modulujący, $x^*(t)$ – odtworzony sygnał modulujący w demodulatorze, $n(t)$ – sygnał zakłócający, $b(t)$ – sygnał zmodulowany wysokiej częstotliwości po modulatorze, $s(t)$ – źródło zakłóceń w kanale telekomunikacyjnym – propagacji fali elektromagnetycznej

W warunkach technicznych powinien być podany stopień pogarszania się właściwości sytemu transmisji alarmu w przypadku przekroczenia określonej szybkości transmisji [15, 16]. Pogarszanie to powinno następować stopniowo, np. czas transmisji powinien rosnąć wolno, aż osiągnie się szybkość wysyłania sygnałów równoważną jednemu sygnałowi na minutę z nadajników pokrywających do 10% pojemności systemu i powinien nastąpić powrót do stanu, w którym spełniane są wymagania normy. W STSA oraz ESB należy zapewnić testowanie wszystkich połączeń – przewodowych i bezprzewodowych pomiędzy poszczególnymi elementami i urządzeniami systemu np. na zwarcie, rozwarcie, sabotaż czy uszkodzenie – rys. 3. Elementem odpowiedzialnym w ESB za realizację tej funkcji jest

centrala alarmowa (CA), która generuje wzorcowe sygnały przyłączane do poszczególnych kanałów transmisyjnych lub linii dozorowych, gdzie znajdują się elementy systemu – rys. 4. W ESB występuje priorytet sygnału alarmu nad testowaniem [1, 9, 15]. W chwili wykrycia przez czujkę zagrożenia i zgłoszenia alarmu do CA, testowanie jest przerywane i system bezpieczeństwa powraca do stanu alarmowania.



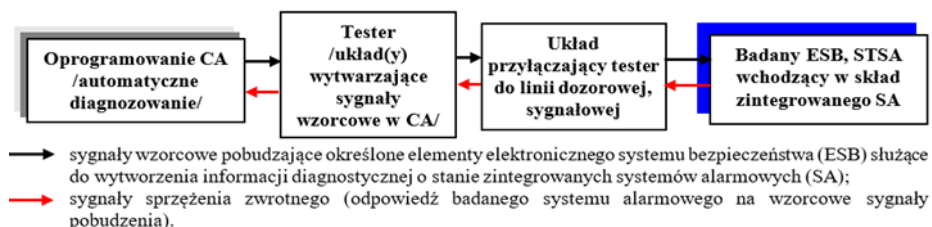
Rys. 2. Nadmiarowość informacji w STSA – obiekt budowlany – ACO



Rys. 3. Testowanie wszystkich połączeń wewnętrznych i zewnętrznych, przewodowych i bezprzewodowych w ESB

W ESB wszystkie połączenia pomiędzy poszczególnymi elementami i urządzeniami można podzielić następująco:

- połączenia przewodowe (w tym światłowodowe),
- połączenia bezprzewodowe z wykorzystaniem modulacji kodowanej (analogowej lub cyfrowej) z wykorzystaniem fal radiowych o ściśle określonej częstotliwości, np. 433; 866 MHz [6, 9, 17].



Rys. 4. Realizacja testowania, tj. diagnozowania stanów technicznych w ESB i STSA

W ESB, które posiadają nadmiarową strukturę informacyjną, w STSA można wyróżnić następujące stany niezawodnościowe:

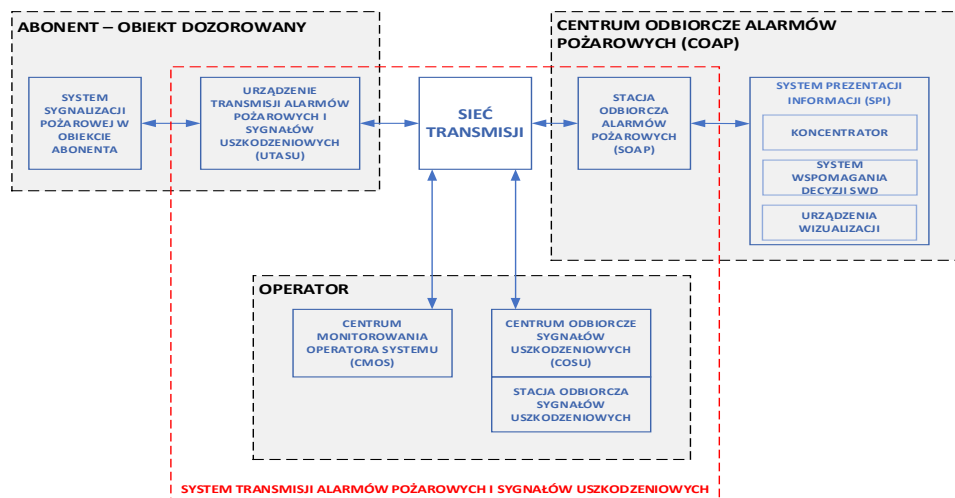
- stan zdatności ε_Z – poprawnie realizowane są wszystkie funkcje systemu,
- stan niezdatności ε_N – wszystkie funkcje są realizowane nieprawidłowo, występuje tzw. czas niedostępności systemu transmisji sygnału,
- częściowa zdatność sytemu bezpieczeństwa ε_{ZN} – poprawnie realizowane są tylko niektóre funkcje poprzez realizację połączenia np. poprzez jeden kanał [8, 11, 17, 19].

Czas, w którym system transmisji alarmów uważa się za niedostępny, jest to okres od ostatniej chwili, o której wiadomo, że system transmisji był dostępny, tj. bez uszkodzeń, aż do chwili, gdy nastąpiło wykrycie uszkodzenia, naprawa i sprawdzenie toru sytemu transmisji [15, 16].

2. Analiza przepływu informacji w systemie transmisji sygnałów alarmowych i uszkodzeniowych w ESB

Na rys. 5 przedstawiono zgodny z ramowymi wymaganiami organizacyjno-technicznymi Komendanta Głównego Państwowej Straży Pożarnej (PSP) schemat funkcjonalny urządzenia transmisji alarmów i sygnałów uszkodzeniowych (UTASU) [15, 16]. Urządzenie jest instalowane w obiekcie dozorowanym. Z UTASU sygnał (alarm lub uszkodzenie) przekazywany jest poprzez sieć transmisji przewodowej lub bezprzewodowej bezpośrednio do centrum odbiorczego alarmów pożarowych (COAP) lub też za pośrednictwem stacji pośredniczącej operatora systemu GSM. Sygnały uszkodzeniowe z SSP kierowane są bezpośrednio do operatora – zespołu serwisu, którego zadaniem jest ciągle nadzorowanie stanu technicznego i reagowanie na uszkodzenia w określonym czasie. Dla nadzorowanych przez ESB obiektów, które można zaliczyć do infrastruktury krytycznej, np. jednostki wojskowe, budynki użyteczności publicznej, wykorzystuje się trzy niezależne tory transmisji sygnałów alarmowych ze względu na niezawodność połączenia – rys. 6. Pierwszym z elementów systemu transmisji alarmów pożarowych (STAP) jest to, iż tory te pracują w tzw. rezerwie gorącej, a operator systemu alarmowego lub użytkownik decyduje o czasie i okresie testowania linii (łączy) obiekt dozorowany – użytkownik [15, 16]. Testowanie łączy (zwarcie, rozwarcie, brak połączenia, podmiana urządzenia, sabotaż itd.)

realizowane jest automatycznie przez centralę alarmową systemu bezpieczeństwa. W przypadku wystąpienia sygnału alarmu – reakcja systemu na włamanie, napad, pożar, itd. podczas testowania, ten tryb pracy zostaje wyłączony automatycznie i obiekt techniczny przechodzi w podstawowy stan pracy, tj. np. dozorowanie. Podczas ręcznych prób nawiązania łączności w trakcie sprawdzenia łączy (obiekt dozorowany – użytkownik – ACO) z udziałem zespołu serwisowego i użytkownika systemu bezpieczeństwa należy sporządzić notatkę dotyczącą działania systemu transmisji sygnałów alarmowych. Notatka ta powinna być przechowywana w dokumentacji systemu bezpieczeństwa u głównego użytkownika – tabela 1 [15, 16].



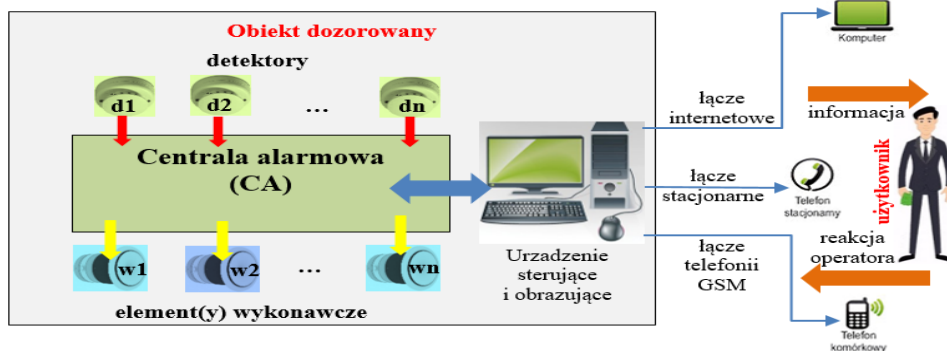
Rys. 5. Schemat transmisji alarmów pożarowych i sygnałów uszkodzeniowych w systemie sygnalizacji pożaru (opracowano na podstawie [15,16])

Tabela 1

Tabela testów i prób dla UTASU (wywołany alarm II stopnia) połączenie – chroniony obiekt – Jednostka Ratowniczo – Gaśnicza (JRG) PSP [15, 16]

Test STSA (alarm II stopnia) do (JRG) PSP Warszawa		Podjęte próby transmisji sygnałów alarmowych do JRG PSP					
		Linia dozorowa nr 1		Linia dozorowa nr 2		Linia dozorowa nr n	
		ROP	czujka	ROP	czujka	ROP	czujka
Tryb pracy SSP - dozorowanie	Tor radiowy	X	X	—	X	X	X
	Tor telefoniczny	X	X	X	X	X	X

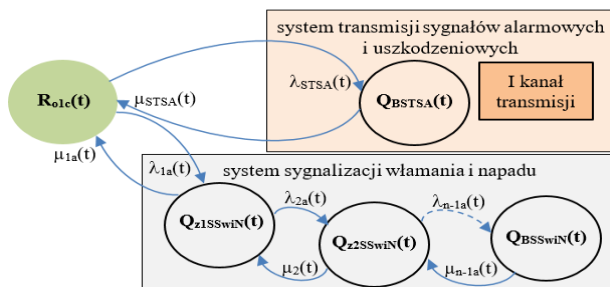
gdzie: x – nawiązanie połączenia torem radiowym i telefonicznym przez STSA, — brak połączenia torem radiowym przez STSA w linii dozorowej nr 2 dla ręcznego ostrzegacza pożarowego (ROP).



Rys. 6. Schemat systemu transmisji sygnałów alarmowych i sygnałów uszkodzeniowych w elektronicznych systemach bezpieczeństwa

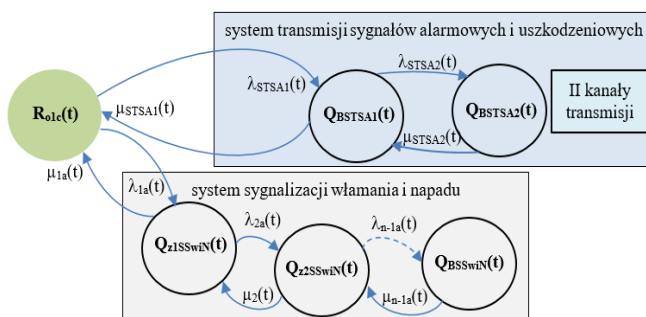
3. Struktura niezawodnościowa wybranych systemów transmisji sygnałów alarmowych i uszkodzeniowych

Organizacja systemów transmisji sygnałów alarmowych i uszkodzeniowych do użytkownika oraz ACO uzależniona jest od rodzaju ochraniających obiektów i występujących zagrożeń. W systemach sygnalizacji włamania i napadu (SSWiN) rozróżniamy cztery różne klasy tych systemów. W III oraz IV klasie dla SSWiN wymagany jest STSA o strukturze zależnej od rodzaju występujących zagrożeń oraz zgromadzonych dóbr o dużej wartości materialnej lub niematerialnej (obiekty sakralne, biblioteki, muzea itd.). W klasie IV stosujemy zawsze dwa niezależne tory przekazywania informacji o zagrożeniach – alarmie. Okres oraz czas testowania w SSWiN realizowany jest przez układ wykonawczy systemu – centralę alarmową. Graf procesu eksploatacji systemu STSA przedstawiono na rys. 7 oraz 8 dla dwóch różnych wariantów połączenia systemu bezpieczeństwa, które pokazano na rys. 1 i 2. W przypadku systemów sygnalizacji pożaru urządzenie transmisji sygnałów alarmowych i uszkodzeniowych jest wymagane obligatoryjnie [15, 16]. Jest to określone w ustawach, przepisach i rozporządzeniach dotyczących SSP. W SSP centrala sygnalizacji pożarowej (CSP) w obiekcie nadzorowanym połączona jest przewodowo z pierwszym elementem systemu transmisji alarmów pożarowych, którym jest urządzenie UTASU – rys. 5. UTASU jest zainstalowane w obiekcie dozorowanym, zwykle w pobliżu CSP. Jest to najczęściej realizowane w tym samym pomieszczeniu, gdzie znajduje się służba ochrony lub zespół serwisowy. Z UTASU sygnał przekazywany jest poprzez sieć transmisji bezpośrednio do COAP lub za pośrednictwem stacji pośredniczącej operatora systemu do układu wizualizacji zdarzeń lub na wynośną tablicę synoptyczną [6, 9].

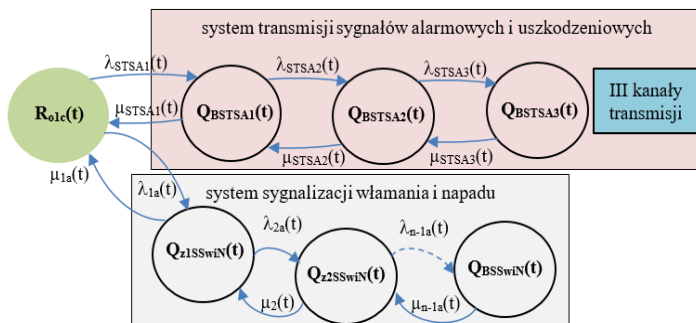


Rys. 7. Graf procesu eksploatacji STSA dla UTASU jak na rys. 1

Rozpatrując grafy procesu eksploatacji STSA dla układu transmisji sygnałów alarmowych i uszkodzeniowych (rys. 7–9) można zauważyć, iż w najprostszym systemie przekazywania informacji występują tylko dwa stany eksploatacyjne – $R_{01c}(t)$ – funkcja prawdopodobieństwa przebywania systemu w stanie pełnej zdatności SPZ oraz $Q_{BSTSA}(t)$ – funkcja prawdopodobieństwa przebywania STSA w stanie zawodności bezpieczeństwa SB – rys. 7. Sygnały uszkodzeniowe, które występują w elektronicznych systemach bezpieczeństwa kierowane są bezpośrednio do operatora systemu – zespół serwisowy. Dla obiektów chronionych bardzo ważnych ze względów funkcjonowanie państwa zespół serwisowy zawsze dostępny jest na miejscu użytkowania systemu i ma określony czas na podjęcie interwencji, tj. naprawę uszkodzenia z intensywnością przejść μ_{1-5z} ze stanu zawodności bezpieczeństwa $Q_{BSTSA}(t)$ do stanu $R_{01c}(t)$ pełnej zdatności SPZ.



Rys. 8. Graf procesu eksploatacji STSA dla UTASU jak na rys. 2



Rys. 9. Graf procesu eksploatacji STSA dla UTASU jak na rys. 6

Stosując dwa lub trzy kanały transmisji sygnałów alarmowych i uszkodzeniowych w elektronicznych systemach bezpieczeństwa otrzymujemy nadmiarową strukturę informacyjną – rys. 8, 9 [6, 17]. Zastosowanie takich rozwiązań technicznych jest wymuszone poprzez bardzo ważne funkcje, które realizują ochraniające obiekty. Zaliczane są one do tzw. infrastruktury krytycznej danego państwa. Uszkodzenie pojedynczego kanału transmisji sygnałów alarmowych nie powoduje przejścia STSA do stanu zawadności bezpieczeństwa S_B [6,17]. W rozwiązaniu technicznym jak na rys. 8 występuje pojedynczy stan $Q_{BSTSA1}(t)$, tzn. funkcja prawdopodobieństwa przebywania systemu w stanie zagrożenia bezpieczeństwa S_{ZB} , natomiast stosując rozwiązanie z trzema niezależnymi kanałami transmisyjnymi, otrzymujemy dwa stany zagrożenia bezpieczeństwa S_{ZB} : $Q_{BSTSA1}(t)$ i $Q_{BSTSA2}(t)$. Uszkodzenie wszystkich trzech niezależnych kanałów przekazywania informacji powoduje przejście elektronicznego systemu bezpieczeństwa do stanu $Q_{BSTSA3}(t)$ – funkcja prawdopodobieństwa przebywania systemu w stanie zawadności bezpieczeństwa S_B – rys. 9. W razie uszkodzenia systemu operator zobowiązany jest do niezwłocznego powiadomienia centrum odbiorczego alarmów o uszkodzeniu uniemożliwiającym przesłanie alarmu pożarowego obiektu dozorowanego [16, 17]. Po dokonaniu naprawy operator powiadamia o przywróceniu sprawności systemu.

4. Wnioski

Niezależny układ transmisji alarmów i sygnałów uszkodzeniowych oraz elektroniczny system bezpieczeństwa posiada złożoną strukturę niezawodnościową, mieszaną równoległo-szeregową. W systemie transmisji sygnałów alarmowych występuje system, w którym mogą być stosowane różnego rodzaju nadmiarowości, np. dodatkowe elementy – np. nadajniki, odbiorniki, wytrzymałościowe – różnego rodzaju trasy i zespoły kablowe, które ułożone są w metalowych obudowach, informacyjne – różne sposoby przekazywania informacji do systemów prezentacji informacji alarmowych i uszkodzeniowych. Celem stosowania takich rozwiązań technicznych w elektronicznych systemach bezpieczeństwa jest zwiększenie niezawodności funkcjonowania tych systemów we wszystkich stanach pracy, np. dozorowania, uszkodzenia lub alarmowania. W systemach wykorzystuje się

także zasadę bezpiecznego uszkodzenia, szczególnie w centralach alarmowych i STSA. Pojedyncze uszkodzenie w systemie nie powoduje wystąpienia uszkodzenia katastroficznego. Urządzenie transmisji alarmów instalowane w tym samym obiekcie, który nadzoruje system powinno znajdować się w tym samym, wydzielonym pożarowo pomieszczeniu, co znacznie wpływa na niezawodność przesyłu sygnałów pożarowych i uszkodzeniowych. System transmisji alarmów i sygnałów uszkodzeniowych zawsze musi opierać się na łączu kablowym oraz systemie transmisji radiowej. W dalszej części badań STSA przewiduje się pozyskanie rzeczywistych danych eksploatacyjnych i wyznaczenie wskaźników bezpieczeństwa procesu eksploatacji. W kolejnych badaniach autorzy artykułu planują wyznaczenie wskaźników procesu eksploatacji rzeczywistych STSA SSP.

5. Literatura

1. Ding Q., Peng Z., Liu T., Tong Q.: Building Fire Alarm System with Multi-sensor and Information Fusion Technology Based on D-S Evidence Theory, 2014 International Symposium on Computer, Consumer and Control, Taichung, 2014, DOI 10.1109/IS3C.2014.238.
2. Foucher B., Boullie J., Meslet B., Das D.: A review of reliability prediction methods for electronic devices. *Microelectronics Reliability* 2002; 42(8): DOI 10.1016/S0026-2714(02)00087-2.
3. Joglar F.: Reliability, Availability, and Maintainability. In M. Hurley (ed.), „SFPE Handbook of Fire Protection Engineering”, DOI 10.1007/978-1-4939-2565-0_74.
4. Knopik L., Migawa K.: Semi-Markov system model for minimal repair maintenance. *Eksploatacja i Niezawodność – Maintenance and Reliability* 2019; 21 (2), DOI 10.17531/ein.2019.2.9.
5. Kheir N.A., Holmes W.M.: On Validating Simulation Models of Missile Systems. *Simulation*; 30(4), 1978, DOI 10.1177/003754977803000404.
6. Klimczak T., Paś J.: Selected issues of the reliability and operational assessment of a fire alarm system, *Eksploatacja i Niezawodność – Maintenance and Reliability*, Vol. 21, No. 4, DOI 10.17531/ein.2019.4.3, 2019.
7. Kołowrocki K., Soszyńska-Budny J.: Complex Technical System Operation Processes Identification. In: *Reliability and Safety of Complex Technical Systems and Processes*. Springer Series in Reliability Engineering. Springer, London 2011.
8. McLeish J., Blattau N.: CAE apps for physics of failure reliability & durability simulations. In 2014 Reliability and Maintainability Symposium, IEEE 2014, DOI 10.1109/RAMS.2014.6798444.
9. Paś J., Klimczak T.: Operational System Modelling in a Focused Fire Alarm System with an Open and Signal Detection Circuit Supervising Railway Station Premises. *Research Methods and Solutions to Current Transport Problems. ISCT21 2019. Advances in Intelligent Systems and Computing*, vol. 1032. Springer, Cham, DOI 10.1007/978-3-030-27687-4_31.

10. Paś J., Choromański W.: Results of measurement and determination of threshold electric field component for transport security systems, Archives of Transport Systems Telematics, Vol. 8, Iss. 1, 2015.
11. Paś J.: Selected methods for increases reliability the of electronic systems security. Journal of KONBiN, 3(35), 2015, DOI 10.1515/jok-2015-047.
12. Paś J.: Shock a disposable time in electronic security systems. Journal of KONBiN, 2(38), 2016, DOI 10.1515/jok-2016-0016.
13. Pecht M., Gu J.: Physics-of-failure-based prognostics for electronic products. Transactions of the Institute of Measurement and Control 2009; 31(3-4), DOI 10.1177/0142331208092031.
14. Pecht M.G., Nash F.R.: Predicting the reliability of electronic equipment. Proceedings of the IEEE 1994; 82(7), DOI 10.1109/5.293157.
15. PN-EN 54-21:2009 Systemy sygnalizacji pożarowej. Część 21: Urządzenia transmisji alarmów pożarowych i sygnałów uszkodzeniowych.
16. PN-EN 54-25:2011, PN-EN 54-25:2011/AC:2012 Systemy sygnalizacji pożarowej. Część 25: Podzespoły wykorzystujące łącza radiowe.
17. Rosiński A.: Modelling the maintenance process of transport telematics systems, Publishing House Warsaw University of Technology, Warsaw 2015.
18. Xu, Chen, Yang: Optimal replacement policy for safety-related multi-component multi-state systems. Reliability Engineering and System Safety 2012; 99: DOI 10.1016/j.ress.2011.11.010.
19. Wawrzyński W.: Bezpieczeństwo systemów sterownia w transporcie. Biblioteka Problemów Eksploatacji, Warszawa 2004.