Journal of KONBiN 2020
Volume 50, Issue 2
DOI 10.2478/jok-2020-0027

Jacek PAŚ[1], Krzysztof JAKUBOWSKI[2]
[1]*Military University of Technology (Wojskowa Akademia Techniczna)*
[2]*Ministry of National Defence (Ministerstwo Obrony Narodowej)*

INDICATOR ANALYSIS OF SECURITY RISK FOR ELECTRONIC SYSTEMS USED TO PROTECT FIELD COMMAND POSTS OF ARMY GROUPINGS

Analiza wskaźnika zagrożenia bezpieczeństwa dla systemów elektronicznych wykorzystywanych do zabezpieczenia polowych stanowisk dowodzenia

Abstract: *The article presents a method for determining the security risk indicator for electronic systems that are used to secure field command posts (FCP). Security of FCP of army groupings is a property of the process they carry out which is related to the tasks and functions performed, the human, hardware and environment components. Determining the security risk indicator for FCPs with different organizational structures will allow optimal organization of integrated electronic security systems, including: selection of these devices, their configuration, project implementation and optimal implementation of technical structures, which should also take into account reliability and operational aspects.*
Keywords: field command posts, electronic security system

Streszczenie: *W artykule przedstawiona została metoda określenia wskaźnika zagrożenia bezpieczeństwa dla systemów elektronicznych, wykorzystywanych do zabezpieczenia polowych stanowisk dowodzenia (PSD). Bezpieczeństwo PSD zgrupowań wojska to właściwość realizowanego przez nie procesu, który związany jest z wykonywanych zadań i funkcji, składowych: ludzkiej, sprzętowej oraz otoczenia. Wyznaczenie wskaźnika zagrożenia bezpieczeństwa dla PSD o różnych strukturach umożliwi optymalną organizację zintegrowanych elektronicznych systemów bezpieczeństwa, w tym: dobór tych urządzeń, ich konfigurację, realizację projektu i optymalną realizację struktur technicznych, które powinny uwzględniać także aspekty niezawodnościowo-eksploatacyjne.*
Słowa kluczowe: polowe stanowiska dowodzenia, elektroniczny system bezpieczeństwa

1. Characteristics of field command posts into account the impacts

Armed conflicts, stabilization and peace missions clearly indicate that the factor that significantly affects the achievement of the objectives of the carried out activities is the quick and accurate decision-making. The above-mentioned activities are related to delivery and processing of information from reliable sources at the appropriate time. The resulting decision must be forwarded to the appropriate forces and means in order to take action. This chain of processing and elaborating decisions for the operation of personnel and technical means depends on a properly functioning system – management at a specific level of command – fig. 1. The factors which determine the entire system of command are a command posts, stationary or field. The command post is a hierarchical organization, designed to plan and perform specific activities from obtained / processed information in appropriate organizational cells – fig. 1. From the degree of reliability of the entire decision chain and technical equipment which is used directed to the implementation of tasks depends the entire effectiveness of the command process [5, 17, 18]. Minimizing the impact of external and internal threats through the appropriate use of existing technical protection measures, we can significantly increase the level of security of the command process and the developed decisions at the field command post [4, 10, 12].

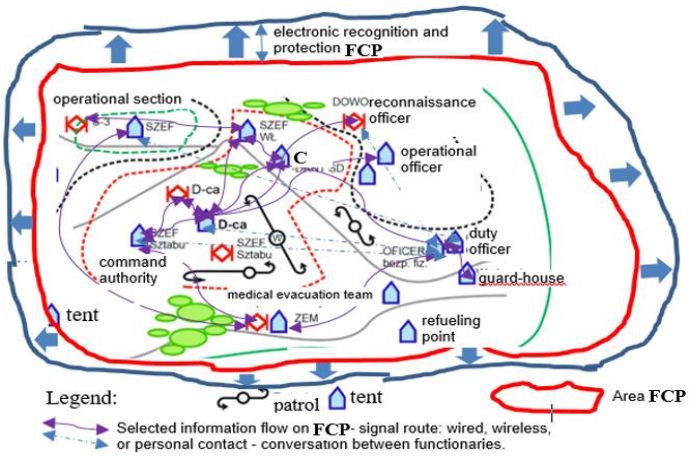


Fig. 1. Example arrangement of elements of the field command post. where: FCP - field command post, C - commander

The analysis of threats that may occur during the use of FCP is a well-oriented approach, which is mainly aimed at ensuring security. It includes identifying and estimating the scale of threats from the point of view of requirements related to ensuring continuity of the command process. This is accomplished through continuous, ongoing analysis of reliability and risk of hazards during all stages of the station's functioning. The analysis of external and internal threats is based on evidence of knowledge about existing or emerging

threats. It covers the context, mechanisms, indicators as well as the consequences and expert advice. A well-developed one can be used to develop a decision on how to respond to an existing threat. The result of thoroughly developed threat analysis determines the selection of appropriate methods. This helps to increase the level of security through the use of electronic security systems (ESS) [2, 6, 10]. The range of available actions also includes military solutions and earlier development of the concept of their use on FCP. FCP is characterized by high mobility, and depending on the dynamics of operations and terrain, it is located in places enabling convenient masking, protection and defence. An important issue in the functioning of FCP is also the proper organization and provision of communication, recognition and counteracting radio-electronics [1, 3, 8, 16]. At the FCP stand, a continuous process of planning activities and direct command of subordinate units to implement tasks is carried out. When identifying sensitive components to occurring threats, to ensure a certain level of security, attention should be paid to the following potential extortions:

- living matter, which is part of a given position or may be located on an ad hoc basis in this area. This is called universal security. It is a condition that gives a sense of insecurity, certainty and a guarantee of its behaviour. During actions at risk, a slight increase in the sense of universal security is of positive importance for achieving the objectives [9, 10, 15],
- inanimate matter – movable and immovable property being the basis for achieving the goals and functions of the station (vehicles, communication systems, armament, means to combat objects, encryption devices, etc.). An appropriate flow of information must be secured using electronic processing means [5, 13, 19].

When carrying out the analysis, it is necessary to take into account the characteristics of the position, identify potential threats, take into account the current state of protection and defence, assess the risk – i.e. vulnerability to occurring attacks, and make a selection of possible technical safeguards from those available for use [13, 18].

2. The concept of technical security system for FCP

On the basis carried out security risk analyses, for ensuring the adequate security of building, it will be used security:

- external – perimeter (perimeter) on distant approaches to FCP,
- internal – using available electronic security systems and military means.

Perimeter protection (perimeter) will be made using barriers using different frequency in the microwave range e.g. 24 GHz and infrared. The basic requirements that determine the technical and tactical parameters of the barriers used include: infrared barriers (BP), a minimum of 10 IR beams, operating range up to 100 m, power supply from the network, solar panels and accumulator batteries – fig. 2a. Microwave barrier (BM), minimum detection range up to 200 m – fig. 2b. For BP and BM it is possible to install the system in all weather conditions. Alarm options – silent with radio notification, sound or visual. For the aforementioned security systems, the probability of correct detection is a minimum of

0,98 – the FORTEZA FMC-24 barrier. Systems resistant to harsh environmental conditions, e.g. rain, snow, fog. Radio alarm notification on two independent channels [11, 14, 16].

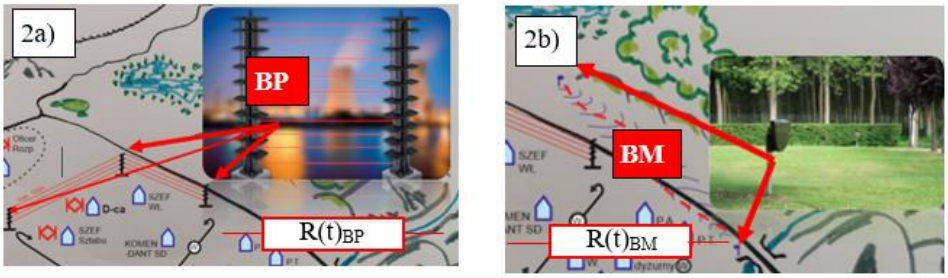


Fig. 2. Infrared and microwave barriers on PSD, 2a) infrared barrier - BP, 2b) microwave barrier - BM, where: R $(t)_{BP}$, R $(t)_{BM}$ - barrier reliability

CCTV system and access control system (SKD) with biometric readers have been used for internal protection, which have the ability to work with so-called "Life band". The CCTV system should have a solar power option. Cameras placed on a boom 6–9 m high. Transmission of information about a wireless alarm – fig. 3a. SKD uses biometric readers. Authentication and database access using iris, fingerprints or facial image. Life bands use RFID connections, the database stored in the device is 250,000 records, wireless communication with the alarm receiving center – fig. 3b [4, 11].

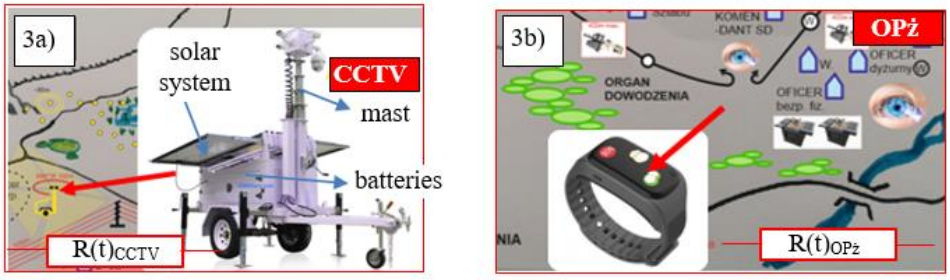


Fig. 3. CCTV and SKD on FCP, 3a) camera and power distribution, 3b) SKD with a life band, where: R $(t)_{CCTV}$, R $(t)_{OPż}$ - CCTV and SKD reliability

The life band is at the same time recognizing the owner through e.g. the veins of the wrist, as well as an anti-seizure button, measurement of pressure, pulse, as well as communication with the duty officer and built-in GPS location [3, 16]. Thanks to the use of RFID technology, it is possible to identify online. Location of people through automatic monitoring of radio tags assigned to a given band by integration with dedicated software. The PSD uses passive RFID systems. The bands do not have an integrated power source, and they take the energy they need from the electromagnetic waves sent by the receiver when reading the marker.The electronic security system can be supplemented with the use of seismic-acoustic detectors (CSA) on the opponent's planned approach – fig. 4a. The CSA

detector system is scalable, has a large operating range and uses energy harvester power with the option of solar panels. In the case of energy harvesting, you can also use the phenomenon of temperature gradients, and therefore use the thermoelectric energy obtained based on the Seebeck phenomenon. Observation of the battlefield FCP with the use of unmanned drone-type means. Defence against unmanned drone assault means – fig. 4b is the use of propellant guns and laser weapons – OD. The concept of using the available electronic security measures to ensure FCP security - one of the variants is presented in fig. 5 [2, 4, 5, 14].

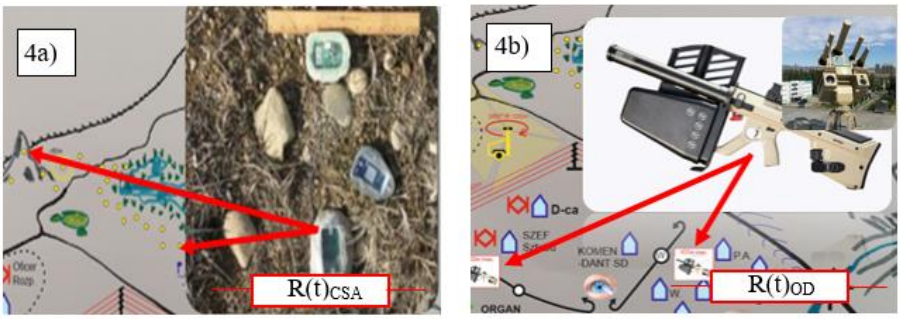


Fig. 4. Seismic detectors and defence against unmanned drone seizure means, 4a) arrangement of CSA seismic detectors, 4b) defence against drone seizure means FCP, where: $R(t)_{CSA}$, $R(t)_{OD}$ - CSA and OD reliability

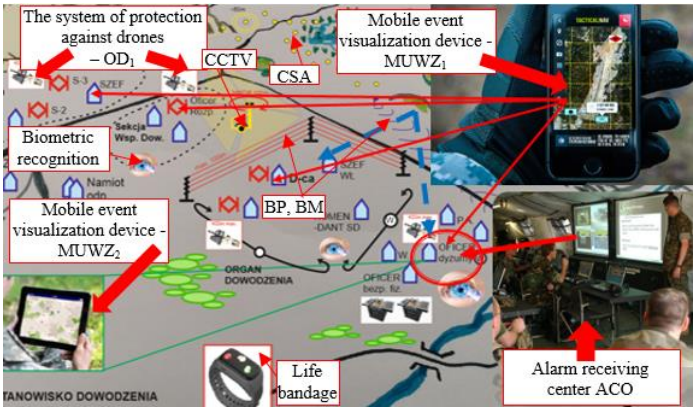


Fig. 5. FCP using available ESB - solution variant

3. Analysis of the security risk indicator for electronic systems used to secure FCP

Figure 6 shows the ranges of acceptable ranges risk values for FCP protection systems. The reliability model of the FCP protection system is shown in fig. 7 for interacting threats [4, 11, 16].

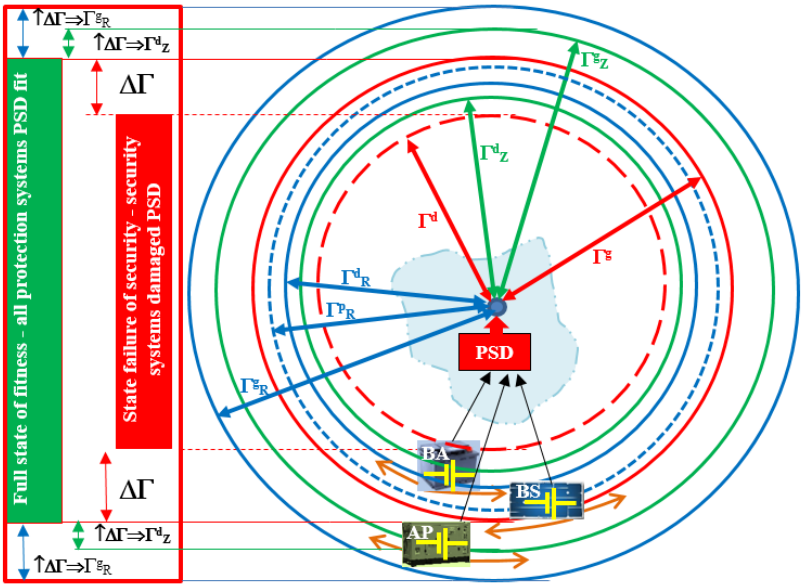
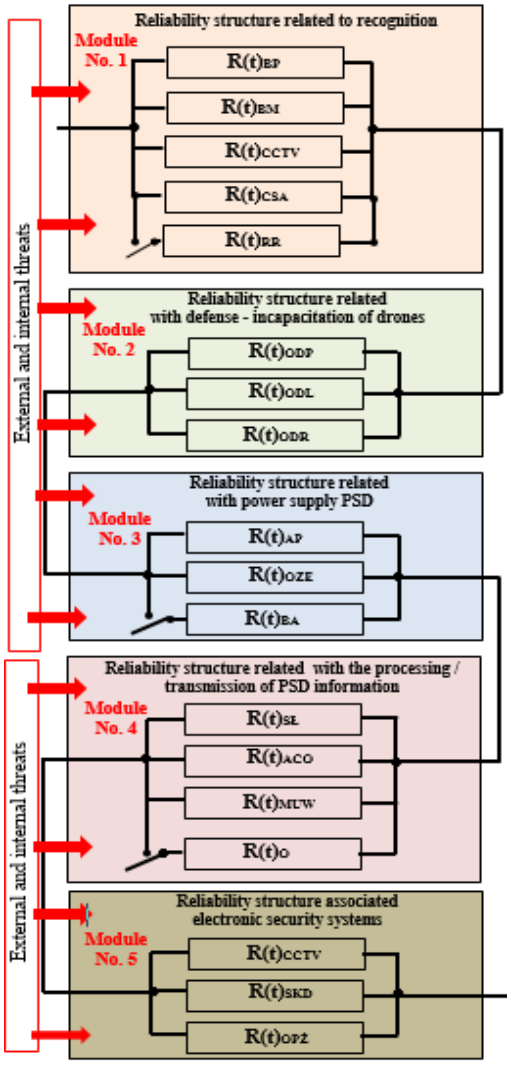


Fig. 6. The ranges of acceptable ranges risk values for FCP protection systems: Γ_d - lower allowable safety risk indicator for FCP, Γ_g - upper allowable safety risk indicator for FCP, unacceptable decrease in the security risk indicator $\Delta\Gamma = \Gamma_g - \Gamma_d$, Γ_{gR} - upper allowable safety risk indicator for FCP related to ensuring recognition, Γ^{p}_{R} - intermediate allowable security risk indicator for PSD related to providing recognition, Γ^{d}_{R} - upper allowable security risk indicator for FCP related to providing recognition, $\Delta\Gamma_R = \Gamma^{g}_{R} - \Gamma^{d}_{R}$ acceptable decrease in security risk index related to providing recognition, Γ^{g}_{Z} - upper allowable safety threat indicator for PSD related to ensuring drone control, Γ^{d}_{Z} - lower allowable safety threat indicator for FCP related to providing drone control, AP, BA, BS - allowable indicator values safety hazards for FCP, AP - power generator, BA - battery, BS - solar power for selected FCP elements.

The acceptable values of the external and internal hazard indicator that occur for FCP are presented in fig. 6. Specified by means of circles – ranges of operation / detection of individual electronic devices that specify the maximum protection values for FCP [9, 11]. These are the acceptable requirements of the values of these indicators specified in the tactical and technical requirements for FCP protection systems [9, 11]. Some modules used in the wide area of FCP have a greater potential impact range than the allowable one specified in tactical requirements for FCP – e.g. Γ^{g}_{Z} (module No. 2) or Γ^{g}_{R} (module No. 1).



Lp.	Name	Markings in fig. 7
1	$R(t)_{BP}$	N. recognition - infrared barrier
2	$R(t)_{BM}$	N. recognition - microwave barrier
3	$R(t)_{CCTV}$	N. recognition - CCTV
4	$R(t)_{CSA}$	N. recognition - seismic detectors
5	$R(t)_{RR}$	N. reconnaissance - radar station
6	$R(t)_{ODP}$	N. defense (drones) – a propellant gun
7	$R(t)_{ODL}$	N. defense (drones) - laser weapon
8	$R(t)_{ODR}$	N. defense (drones) - own resources (weapon)
9	$R(t)_{AP}$	N. power generator set
10	$R(t)_{OZE}$	N. power renewable energy sources
11	$R(t)_{BA}$	N. battery power supply
12	$R(t)_{SŁ}$	N. communication systems
13	$R(t)_{ACO}$	N. ACO communication systems
14	$R(t)_{MUW}$	N. MUW communication systems
15	$R(t)_{O}$	N. operator information transfer
16	$R(t)_{CCTV}$	N. CCTV observation
17	$R(t)_{SKD}$	N. access control system
18	$R(t)_{OPŻ}$	N. life bands
N. – reliability, ACO – alarm receiving center, MUM – mobile visualization device, CCTV – closed - circuit television		

Fig. 7. The reliability structure of the FCP protection system - modules M1-M5

Due to the fact that external and internal threats simultaneously affect the entire FCP protection system, damage to a single FCP protection module causes malfunction of the entire site protection object [3, 8, 14]. In individual modules there is a hot reserve, e.g. protection against attacks using drones – module No. 2, or protection by electronic security systems – module No. 5 [5, 11, 14].

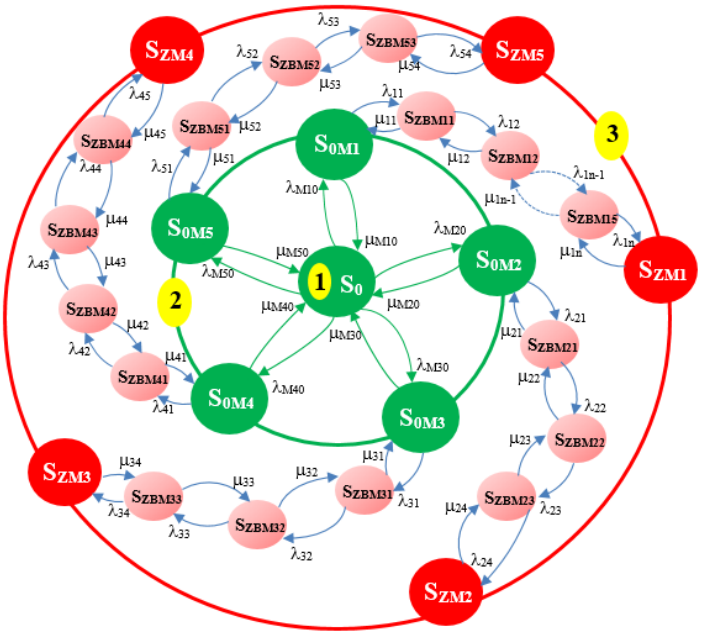


Fig. 8. Graph of the FCP safety process - M1-M5 modules, where: S_0, S_{0M3}, ..., S_{ZM2} - model safety states, μ_{31}, μ_{M30}, ..., μ_{11} - renewal intensity, λ_{11}, λ_{32}, ..., λ_{M30} - damage intensity, 1,2,3 - circles of potential FCP protection system states

In order to increase the level of reliability of the FCP protection system, we use an unencumbered reserve, where it is technically and financially possible (e.g. module No. 3 power supply) [9, 11]. FCP is also characterized by specific tactical and technical requirements. FCP must be expanded and collapsed in a short period of time. Therefore, technical objects and devices used for protection against security threats should have appropriate technical parameters, e.g. min. false alarm probability value on the level 0,01; large detection range – up to 20 km, adequate fire zone for destroying drones, minimum response time to external threat defined in ms, etc. Ensuring continuity - reliability of power supply over a wide area of FCP is a very important issue. Increasing the upper security risk indicator for FCP Γ^g – fig. 6 is possible by building safety modules M1-M5.

4. Conclusions

The FCP protection system has a serial reliability structure. Individual modules responsible for implementing the protection function have a parallel or non-loaded structure. The graph model of security process of FCP consists of five separate modules responsible for implementing security. The entire security system is in a state of

airworthiness. The states of suitability of individual modules responsible for ensuring FCP security are located on District 2. In case of damage of signal transmission with the intensity λ_{0M1}, λ_{0M2}, ...,λ_{0M5} the individual protection system goes from the state S_0 to one of states S_{0M1}, S_{0M2}, ...,S_{0M5}. In the case of module repair, the system with repair intensity μ_{0M1}, μ_{0M2},...,μ_{0M5} returns to the S_0 state. In the absence of renewal, the protection system passes through intermediate states, threats to the state of safety failure, e.g. module 3 – $S_{0M3} \Rightarrow S_{ZBM31} \Rightarrow$ ... S_{ZM3}. Using renewal processes for module 3 μ_{31}, μ_{32},...,μ_{34}, we can go to the S_0 state. Providing protection for FCP is a priority in the military's operations. Taking into account difficult environmental conditions and very short rolling times and developing FCP components, devices and systems should be properly selected in technical, tactical and environmental terms. In tests concerning operational safety, the weakest fire should be taken into account in the modules responsible for implementing the protection function.

5. References

1. Benford J., Swegle J.: High Power Microwaves. Taylor & Francis Group (2007), 2019.
2. Burdzik R., Konieczny Ł., Figlus T.: Concept of on-board comfort vibration monitoring system for vehicles. In: the monograph Activities of Transport Telematics, editors: Mikulski J., TST 2013, CCIS 395. Heidelberg: Springer, 2013: 418-425, DOI 10.1007/978-3-642-41647-7_51.
3. Chen S., Ho T., Mao B.: Maintenance schedule optimisation for a railway power supply system. International Journal of Production Research, 51(16), 2013.
4. Kaniewski P., Smagowski P., Konatowski S.: Ballistic Target Tracking with Use of Cinetheodolites, International Journal of Aerospace Engineering, Volume 2019, Article ID 3240898, DOI 10.1155/2019/3240898.
5. Klimczak T., Paś J.: Selected issues of the reliability and operational assessment of a fire alarm system. Eksploatacja i Niezawodnosc – Maintenance and Reliability, Vol. 21, No. 4, 2019, DOI 10.17531/ein.2019.4.3.
6. Klimczak T., Paś J.: Analysis of reliability structures for fire signaling systems in the field of fire safety and hardware requirements. Journal of KONBiN, vol. 46, 2018, DOI 10.2478/jok-2018-0030.
7. Kołowrocki K., Soszyńska-Budny J.: Reliability and safety of complex technical systems and processes. Springer, London 2011.
8. Laskowski D., Łubkowski P., Pawlak E., Stańczyk P.: Anthropotechnical systems reliability. In: Nowakowski T., Młyńczak M., Jodejko-Pietruczuk, A., Werbińska-Wojciechowska S. (eds.) Safety and Reliability: Methodology and Applications - Proceedings of the European Safety and Reliability Conference ESREL 2014. CRC Press/Balkema, London 2015.
9. Loeffler C., Spears E.: Uninterruptible power supply system. In: Hwaiyu Geng P.E. (eds.): Data Center Handbook, John Wiley & Sons, 2015.

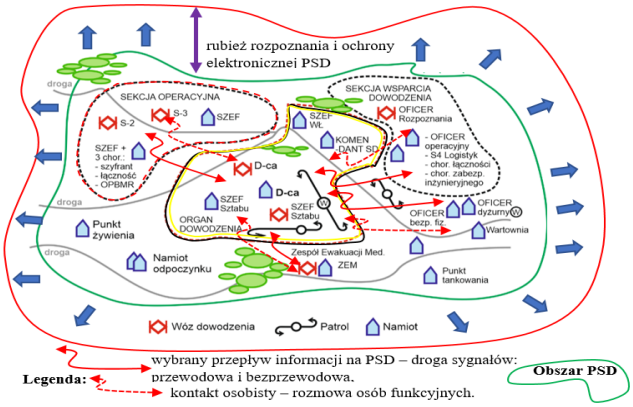
10. Paś J.: Shock a disposable time in electronic security systems. Journal of KONBiN Vol. 2(38), 2016, DOI 10.1515/jok-2016-0016.
11. Paś J., Klimczak T.: Modeling of the process of selected fire signaling systems. Diagnostyka, Vol. 20, No. 4, 2019, DOI 10.29354/diag/113047.
12. Reddig K., Dikunow B., Krzykowska K.: Proposal of big data route selection methods for autonomous vehicles. Internet Technology Letters, Vol. 1(36), 2018.
13. Jodejko-Pietruczuk A., Werbińska-Wojciechowska S.: Analysis of maintenance models' parameters estimation for technical systems with delay time. Eksploatacja i Niezawodnosc – Maintenance and Reliability, Vol. 16, No. 2, 2014.
14. Tchórzewska-Cieślak B.: Method of assessing of risk of failure in water supply system. European safety and reliability conference ESREL. Risk, reliability and societal safety. Taylor & Francis, tom 2, Norway, Stavanger 2007.
15. Siergiejczyk M., Stawowy M.: Modelling of uncertainty for continuity quality of power supply. In: "Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL 2016", eds. Lesley Walls, Matthew Revie, Tim Bedford. CRC Press/Balkema, 2017.
16. Stawowy M., Kasprzyk Z.: Identifying and simulation of status of an ICT system using rough sets, Tenth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX Springer 2015.
17. Zajkowski K., Rusica I., Palkova Z.: The use of CPC theory for energy description of two nonlinear receivers, MATEC Web of Conferences 2018.
18. Zhuo H.-Y., Liu Z.-Q., Ge Ch.-L.: Development of HPM measurement and control system based on fiber communication. 2017 IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), IEEE, Chengdu, China 2017.
19. Zhang Y.-H., Chai Ch.-Ch., Liu Y., Yang Y.-T., Shi Ch.-L., Fan Q.-Y., Liu Y.-Q.: Modeling and understanding of the thermal failure induced by high power microwave in CMOS inverter. Chinese Physics B, Vol. 26(5), 2017.

ANALIZA WSKAŹNIKA ZAGROŻENIA BEZPIECZEŃSTWA DLA SYSTEMÓW ELEKTRONICZNYCH WYKORZYSTYWANYCH DO ZABEZPIECZENIA POLOWYCH STANOWISK DOWODZENIA

1. Charakterystyka polowych stanowisk dowodzenia z uwzględnieniem oddziaływujących zagrożeń

Konflikty zbrojne, misje stabilizacyjne i pokojowe jednoznacznie wskazują, że czynnikiem, który w zasadniczy sposób wpływa na osiągnięcie celów prowadzonych działań to szybkie i trafne podejmowanie odpowiednich decyzji. Wyżej wymienione czynności związane są z dostarczeniem, przetworzeniem informacji z wiarygodnych źródeł w odpowiednim czasie. Wypracowana decyzja musi być przekazana do właściwych sił i środków w celu podjęcia działania. Ten łańcuch przetwarzania oraz wypracowania decyzji do działania sił osobowych i środków technicznych uzależniony jest od właściwie funkcjonującego systemu – zarządzania na określonym szczeblu dowodzenia – rys. 1. Elementami decydującymi o całym systemie dowodzenia są stanowiska dowodzenia stacjonarne lub polowe. Stanowisko dowodzenia to organizacja hierarchiczna, przeznaczona do planowania i wykonywania określonych czynności z informacji pozyskanych/przetworzonych, w odpowiednich komórkach organizacyjnych – rys. 1. Od stopnia niezawodności całego łańcucha decyzyjnego i użytkowanego sprzętu technicznego skierowanego do realizacji zadań zależy cała skuteczność procesu dowodzenia [5, 17, 18]. Minimalizując wpływ zagrożeń zewnętrznych oraz wewnętrznych poprzez odpowiednie wykorzystanie istniejących technicznych środków ochrony, możemy w istotny sposób zwiększyć poziom bezpieczeństwa procesu dowodzenia i wypracowanych decyzji na polowym stanowisku dowodzenia [4, 10, 12]. Analiza zagrożeń, które mogą wystąpić w czasie użytkowania PSD to odpowiednio zorientowane postępowanie, które ma głównie na celu zapewnienie bezpieczeństwa. Obejmuje ono identyfikację i szacowanie skali zagrożeń z punktu widzenia wymagań związanych z zapewnieniem ciągłości procesu dowodzenia. Realizowane to jest poprzez ciągłą i bieżącą analizę niezawodności oraz ryzyka wystąpienia zagrożeń podczas wszystkich etapów funkcjonowania stanowiska. Analiza zagrożeń zewnętrznych oraz wewnętrznych jest oparta na dowodach wiedzy o istniejącym lub kształtujących się zagrożeniach. Obejmuje kontekst, mechanizmy, wskaźniki, a także konsekwencje i porady ekspertów. Dobrze opracowana

może być wykorzystana przy wypracowaniu decyzji o reakcji na występujące zagrożenie. Wynik opracowanej rzetelnie analizy zagrożeń decyduje o wyborze właściwych metod. Przyczynia się to do zwiększenia poziomu bezpieczeństwa, poprzez wykorzystanie elektronicznych systemów bezpieczeństwa (ESB) [2, 6, 10]. W wachlarzu dostępnych działań istnieją również rozwiązania militarne i wcześniejsze opracowanie koncepcji ich wykorzystania na PSD. PSD charakteryzuje się dużą mobilnością, a w zależności od dynamiki działań i ukształtowania terenu lokowane jest w miejscach umożliwiających dogodne maskowanie, ochronę i obronę. Ważnym zagadnieniem w funkcjonowaniu PSD jest także właściwa organizacja oraz zapewnienie łączności, rozpoznania i przeciwdziałania radioelektronicznego [1, 3, 8, 16].



Rys. 1. Przykładowe rozmieszczenie elementów polowego stanowiska dowodzenia, gdzie: PSD – polowe stanowisko dowodzenia, D-ca – dowódca

Na stanowisku PSD realizowany jest ciągły proces planowania działań oraz bezpośrednie dowodzenie podległymi jednostkami w celu realizacji zadań. Przeprowadzając identyfikację elementów wrażliwych na występujące zagrożenia, celem zapewnienia określonego poziomu bezpieczeństwa należy zwrócić uwagę na następujące potencjalne wymuszenia:

- materię ożywioną, która wchodzi w skład danego stanowiska lub może znajdować się doraźnie na tym obszarze. Jest to tzw. bezpieczeństwo powszechne. Jest to stan, który daje poczucie braku odczuwania zagrożenia, pewność i gwarancję jego zachowania. W czasie działań w zagrożeniu niewielki wzrost poczucia bezpieczeństwa powszechnego ma pozytywne znaczenie dla realizacji celów [9, 10, 15],
- materię nieożywioną – mienie ruchome i nieruchome będące podstawą realizacji celów i funkcji stanowiska (pojazdy, systemy łączności, uzbrojenie, środki do zwalczania obiektów, urządzenia szyfrujące, itd.). Musi być zabezpieczony odpowiedni przepływ informacji z wykorzystaniem środków elektronicznego przetwarzania [5, 13, 19].

Przeprowadzając analizę należy uwzględnić charakterystykę stanowiska, zidentyfikować potencjalne zagrożenia, uwzględnić aktualny stan ochrony i obrony, oszacować

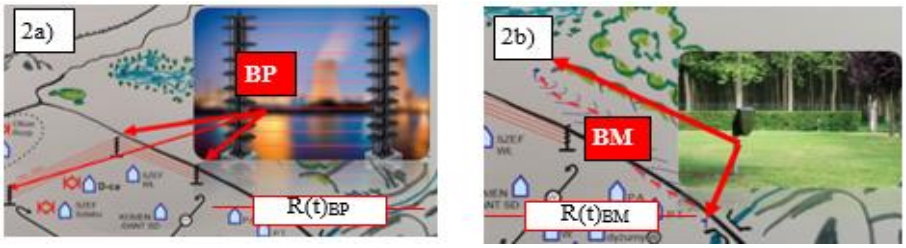
ryzyko, tj. podatność na występujące ataki, oraz dokonać wyboru możliwych technicznych zabezpieczeń z dostępnych do zastosowania [13, 18].

2. Koncepcja technicznego systemu bezpieczeństwa dla PSD

Na podstawie przeprowadzonych analiz zagrożenia bezpieczeństwa dla zapewnienia odpowiedniej ochrony obiektu wykorzystana będzie ochrona:

- zewnętrzna – obwodowa (perymetryczna) na dalekich podejściach do PSD,
- wewnętrzna – z wykorzystaniem dostępnych elektronicznych systemów bezpieczeństwa oraz środków militarnych.

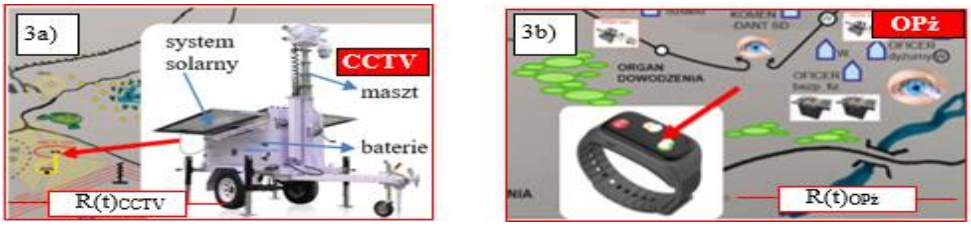
Ochrona obwodowa (perymetryczna) zostanie wykonana z użyciem barier wykorzystujących częstotliwości z zakresu mikrofal np. 24 GHz i podczerwieni. Do podstawowych wymagań, które określają parametry techniczno-taktyczne użytych barier należą: bariery podczerwieni (BP) minimum 10 wiązek IR, zasięg działania do 100 m, zasilanie energetyczne z sieci, paneli solarnych i baterii akumulatorów – rys. 2a. Bariera mikrofalowa (BM), zasięg wykrywania minimalny do 200 m – rys. 2b. Dla BP oraz BM możliwa instalacja systemu w każdych warunkach atmosferycznych [11, 14, 16].



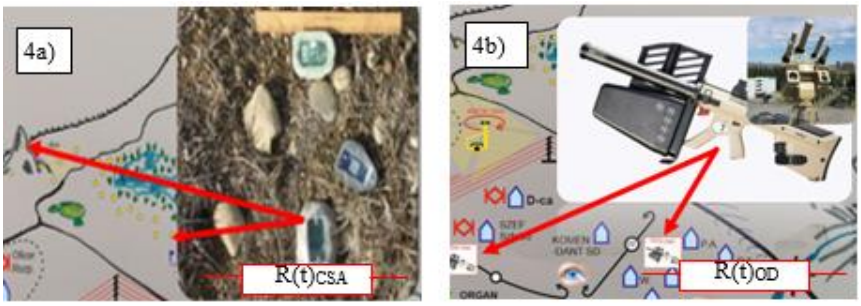
Rys. 2. Bariery podczerwieni i mikrofalowe na PSD, 2a) bariera podczerwieni – BP, 2b) bariera mikrofalowa – BM, gdzie: $R(t)_{BP}$, $R(t)_{BM}$ – niezawodność barier

Opcje alarmu – cichy z powiadomieniem radiowym, dźwiękowy lub wizualny. Dla ww. systemów bezpieczeństwa prawdopodobieństwo poprawnego wykrycia wynosi minimum 0,98 – bariera typu FORTEZA FMC-24. Systemy odporne na trudne warunki środowiskowe, np. deszcz, śnieg, mgła. Powiadomienie o alarmie radiowym na dwóch niezależnych kanałach. Do ochrony wewnętrznej wykorzystano system telewizji dozorowej CCTV, system kontroli dostępu (SKD) z czytnikami biometrycznymi, które posiadają możliwość współpracy z opaską tzw. „życia". System CCTV powinien posiadać opcję zasilania solarnego. Kamery umieszczone na wysięgniku o wysokości 6 – 9 m. Przekazywanie informacji o alarmie bezprzewodowe – rys. 3a. SKD wykorzystuje czytniki biometryczne. Uwierzytelnianie i dostęp do bazy danych z wykorzystaniem tęczówki oka, odcisków palca lub obrazu twarzy. Opaski życia wykorzystują połączenia typu RFID, baza danych przechowywana w urządzeniu to 250 000 rekordów, łączność bezprzewodowa z alarmowym centrum

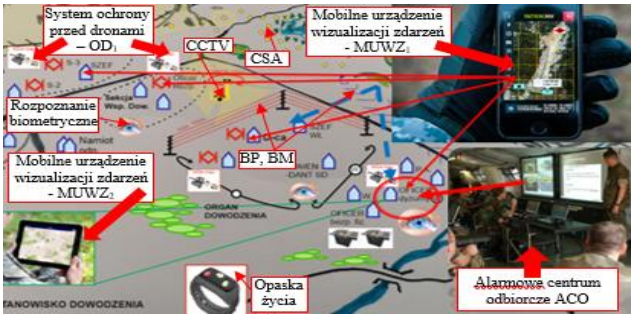
odbiorczym – rys. 3b [4, 11]. Opaska życia to jednocześnie rozpoznawanie właściciela poprzez np. układ żył nadgarstka, a także przycisk antynapadowy, pomiar ciśnienia, tętna oraz łączność do oficera dyżurnego i wbudowana lokalizacja GPS. Dzięki wykorzystaniu technologii RFID istnieje możliwość identyfikacji on-line. Lokalizacja osób poprzez automatyczny monitoring znaczników radiowych przypisanych do danej opaski poprzez integrację z dedykowanym oprogramowaniem. Na PSD wykorzystuje się systemy pasywne RFID. Opaski nie mają zintegrowanego źródła zasilania, a energię potrzebną do pracy pobierają z fal elektromagnetycznych wysyłanych przez odbiornik podczas odczytu znacznika. Uzupełnieniem elektronicznego systemu bezpieczeństwa dla ochrony PSD może być wykorzystanie czujek sejsmiczno-akustycznych (CSA) na planowanym podejściu przeciwnika – rys. 4a. System czujek CSA jest skalowalny, charakteryzuje się dużym zasięgiem działania oraz wykorzystuje zasilanie typu *energy harwesting* z opcją paneli słonecznych. W przypadku *energy harwesting* można również wykorzystać zjawisko gradientów temperatury, a więc wykorzystać energię termoelektryczną, pobieraną w oparciu o zjawisko Seebecka. Obserwacja rubieży pola walki PSD z wykorzystaniem bezpilotowych środków typu dron. Obrona przed bezpilotowymi środkami napadu typu dron – rys. 4b, to wykorzystanie pistoletów miotających oraz broni laserowej – OD. Koncepcja wykorzystania dostępnych elektronicznych środków bezpieczeństwa do obrony PSD – jeden z wariantów przedstawiono na rys. 5 [3, 16].



Rys. 3. CCTV i SKD na PSD, 3a) rozmieszczenie kamery i zasilania, 3b) SKD z opaską życia, gdzie: $R(t)_{CCTV}$, $R(t)_{OPż}$ – niezawodność CCTV oraz SKD



Rys. 4. Czujki sejsmiczne i obrona przed bezpilotowymi środkami napadu typu dron, 4a) rozmieszczenie czujek sejsmicznych CSA, 4b) obrona przed środkami napadu PSD typu dron, gdzie: $R(t)_{CSA}$, $R(t)_{OD}$ – niezawodność CSA oraz OD

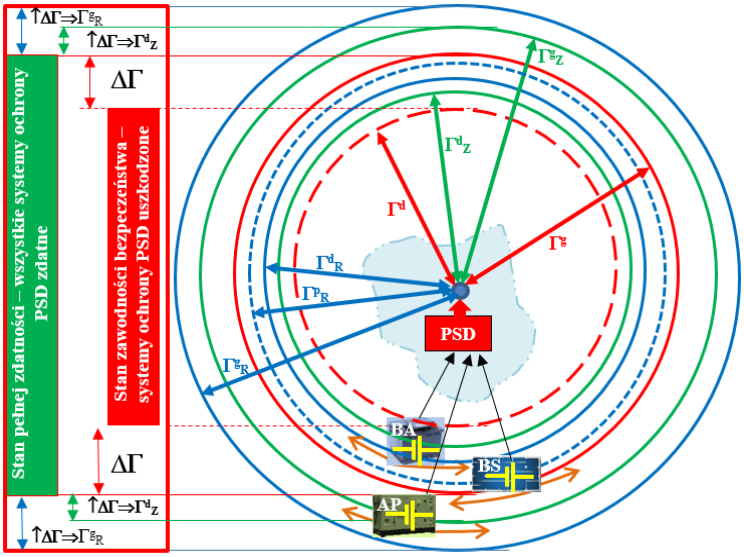


Rys. 5. PSD z wykorzystaniem dostępnych ESB – wariant rozwiązania

3. Analiza wskaźnika zagrożenia bezpieczeństwa dla systemów elektronicznych wykorzystywanych do zabezpieczenia PSD

Na rys. 6 przedstawiono zakresy dopuszczalnych wartości zagrożenia bezpieczeństwa dla systemów ochrony PSD. Model niezawodności systemu ochrony PSD dla oddziaływujących zagrożeń pokazano na rys. 7 [4, 11, 16]. Dopuszczalne wartości wskaźnika zagrożenia zewnętrznego i wewnętrznego, które występują dla PSD przedstawiono na rys. 6. Określono za pomocą okręgów – zasięgi działania/wykrywania poszczególnych urządzeń elektronicznych, które określają maksymalne wartości ochrony dla PSD [9, 11]. Są to dopuszczalne wymagania wartości tych wskaźników określone w wymaganiach taktycznych oraz technicznych dla systemów ochrony PSD. Niektóre moduły użytkowane na rozległym obszarze PSD mają większy potencjalny zasięg oddziaływania, niż dopuszczalny określony w wymaganiach taktycznych dla PSD – np. Γ^{g}_{Z} (moduł 2) lub Γ^{g}_{R} (moduł 1). Ze względu na to, że zagrożenia zewnętrzne i wewnętrzne oddziaływają jednocześnie na cały system ochrony PSD uszkodzenie pojedynczego modułu ochrony PSD powoduje niesprawność całego obiektu ochrony stanowiska. W poszczególnych modułach występuje rezerwa gorąca, np. zabezpieczenie przed atakiem z wykorzystaniem dronów – moduł nr 2, lub ochrona przez elektroniczne systemy bezpieczeństwa – moduł nr 5. W celu zwiększenia poziomu niezawodności systemu ochrony PSD stosujemy rezerwę nieobciążoną, tam gdzie jest to możliwe technicznie i finansowo (np. moduł nr 3 zasilanie energetyczne) [9, 11]. PSD charakteryzuje się także szczególnymi wymaganiami taktyczno-technicznymi. PSD muszą być rozwijane i zwijane w krótkim czasie [3, 8, 14]. Dlatego obiekty techniczne, urządzenia służące do ochrony przed zagrożeniami bezpieczeństwa powinny posiadać odpowiednie parametry techniczne np. wartość prawdopodobieństwa fałszywego alarmu na poziomie 0,01, duży zasięg wykrywania – do 20 km, odpowiednia strefa ognia do niszczenia dronów, minimalny czas reakcji na wymuszenie zewnętrzne zagrożenia określony w ms, itd. [5, 11, 14]. Bardzo ważnym zagadnieniem jest zapewnienie ciągłości

– niezawodności zasilania energetycznego na rozległym obszarze PSD. Zwiększenie górnego wskaźnika zagrożenia bezpieczeństwa dla PSD Γ^g – rys. 6 jest możliwe poprzez rozbudowę modułów bezpieczeństwa M1-M5.

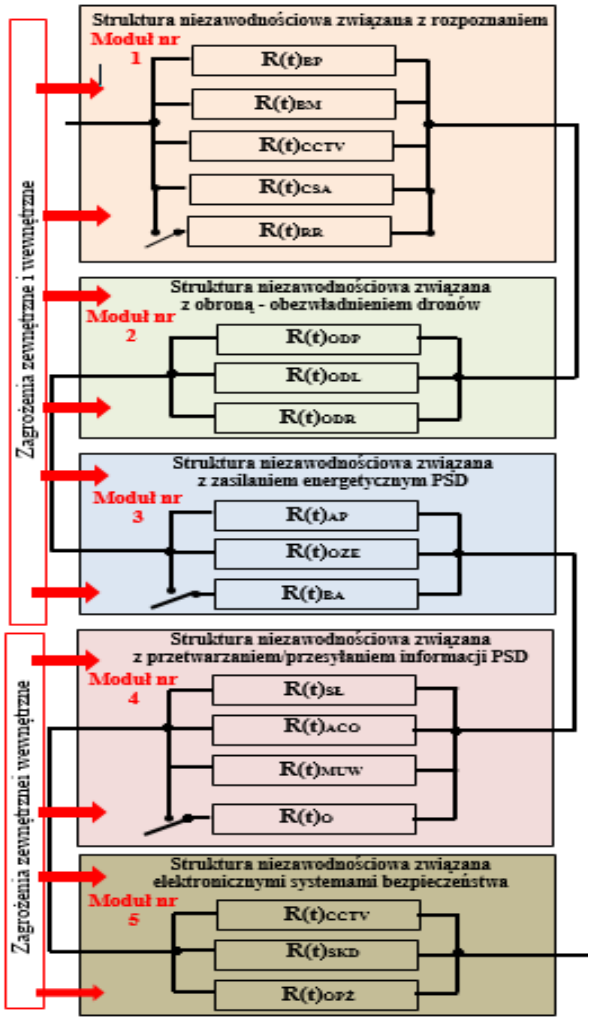


Rys. 6. Zakresy dopuszczalnych wartości zagrożenia bezpieczeństwa dla systemów ochrony PSD gdzie: Γ^d – dolny dopuszczalny wskaźnik zagrożenia bezpieczeństwa dla PSD, Γ^g – górny dopuszczalny wskaźnik zagrożenia bezpieczeństwa dla PSD, dopuszczalny spadek wskaźnika zagrożenia bezpieczeństwa $\Delta\Gamma = \Gamma^g - \Gamma^d$, $\Gamma^g{}_R$ – górny dopuszczalny wskaźnik zagrożenia bezpieczeństwa dla PSD związany z zapewnieniem rozpoznania, $\Gamma^p{}_R$ – pośredni dopuszczalny wskaźnik zagrożenia bezpieczeństwa dla PSD związany z zapewnieniem rozpoznania, $\Gamma^d{}_R$ – górny dopuszczalny wskaźnik zagrożenia bezpieczeństwa dla PSD związany z zapewnieniem rozpoznania, $\Delta\Gamma_R = \Gamma^g{}_R - \Gamma^d{}_R$ dopuszczalny spadek wskaźnika zagrożenia bezpieczeństwa związany z zapewnieniem rozpoznania, $\Gamma^g{}_Z$ – górny dopuszczalny wskaźnik zagrożenia bezpieczeństwa dla PSD związany z zapewnieniem zwalczania dronów, $\Gamma^d{}_Z$ – dolny dopuszczalny wskaźnik zagrożenia bezpieczeństwa dla PSD związany z zapewnieniem zwalczania dronów, AP, BA, BS – dopuszczalne wartości wskaźnika zagrożenia bezpieczeństwa dla zasilania PSD, AP – agregat prądotwórczy, BA – bateria akumulatorów, BS – zasilanie solarne wybranych elementów PSD.

4. Wnioski

System ochrony PSD posiada szeregową strukturę niezawodnościową. Poszczególne moduły odpowiedzialne za realizację funkcji ochrony posiadają strukturę równoległą obciążoną lub nie. Model grafu procesu bezpieczeństwa PSD składa się z pięciu odrębnych

modułów odpowiedzialnych za realizację ochrony – rys. 7. Cały system bezpieczeństwa w stanie zdatności znajduje się w stanie S_0.

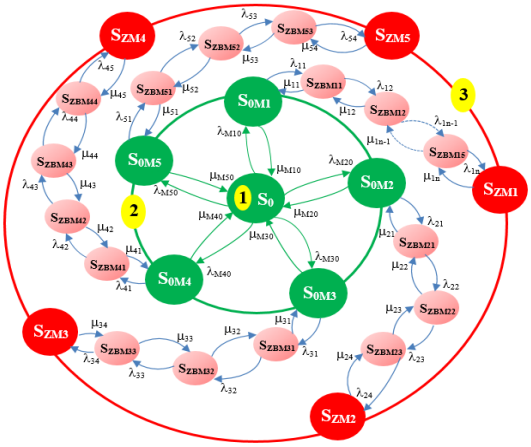


Lp.	Nazwa	Oznaczenia na rys. 7
1	$R(t)_{BP}$	N. rozpoznania – bariera podczerwieni
2	$R(t)_{BM}$	N. rozpoznania – bariera mikrofalowa
3	$R(t)_{CCTV}$	N. rozpoznania – telewizja dozorowa
4	$R(t)_{CSA}$	N. rozpoznania – czujki sejsmiczne
5	$R(t)_{RR}$	N. rozpoznania – stacja radiolokacyjna
6	$R(t)_{ODP}$	N. obrony (drony) pistolet miotający
7	$R(t)_{ODL}$	N. obrony (drony) broń laserowa
8	$R(t)_{ODR}$	N. obrony (drony) środki własne (broń)
9	$R(t)_{AP}$	N. zasilania agregat prądotwórczy
10	$R(t)_{OZE}$	N. zasilania, źródła odnawialne
11	$R(t)_{BA}$	N. zasilania, bateria akumulatorów
12	$R(t)_{SŁ}$	N. systemów łączności
13	$R(t)_{ACO}$	N. systemów łączności ACO
14	$R(t)_{MUW}$	N. systemów łączności MUW
15	$R(t)_{O}$	N. przekazywania informacji operator
16	$R(t)_{CCTV}$	N. obserwacji telewizja dozorowa
17	$R(t)_{SKD}$	N. systemu kontroli dostępu
18	$R(t)_{OPŻ}$	N. opasek życia
gdzie: N. – niezawodność; ACO – alarmowe centrum odbiorcze, MUM – mobilne urządzenie wizualizacji		

Rys. 7. Struktura niezawodnościowa systemu ochrony PSD – moduły M1 – M5

Stany zdatności poszczególnych modułów odpowiedzialnych za zapewnienie bezpieczeństwa PSD znajdują się na okręgu nr 2. W przypadku uszkodzenia transmisji sygnału z intensywnością $\lambda_{0M1},\lambda_{0M2,...},\lambda_{0M5}$ do poszczególnych modułów system ochrony przechodzi ze stanu S_0 do jednego stanów $S_{0M1},S_{0M2,...},S_{0M5}$. W przypadku naprawy modułów system z intensywnością naprawy $\mu_{0M1},\mu_{0M2,...},\mu_{0M5}$ wraca do stanu S_0 – rys. 8. W przypadku braku odnowy system ochrony przechodzi poprzez stany pośrednie, zagrożenia do stanu zawodności bezpieczeństwa, np. moduł 3 - $S_{0M3} \Rightarrow S_{ZBM31} \Rightarrow \ldots S_{ZM3}$. Stosując proces odnowy dla

modułu nr 3 $\mu_{31},\mu_{32,\ldots},\mu_{34}$ możemy przejść do stanu S_0. Zapewnienie ochrony dla PSD to priorytet w działaniach wojska. Uwzględniając trudne warunki środowiskowe oraz bardzo krótkie czasy zwijania i rozwijania PSD elementy, urządzenia i systemy powinny być odpowiednio dobrane pod względem technicznym i taktycznym, oraz środowiskowym. W badaniach dotyczących bezpieczeństwa eksploatacji należy uwzględnić najsłabsze ogniowo w modułach odpowiedzialnych za realizację funkcji ochrony.



Rys. 8. Graf procesu bezpieczeństwa PSD – moduły M1-M5, gdzie: $S_0,S_{0M3},\ldots, S_{ZM2}$ – stany bezpieczeństwa modelu, $\mu_{31},\mu_{M30,\ldots},\mu_{11}$ – intensywność odnowy, $\lambda_{11},\lambda_{32},\ldots, \lambda_{M30}$ – intensywność uszkodzeń, 1,2,3 – okręgi potencjału stanów sytemu ochrony PSD

5. Literatura

1. Benford J., Swegle J.: High Power Microwaves. Taylor & Francis Group (2007), 2019.
2. Burdzik R., Konieczny Ł., Figlus T.: Concept of on-board comfort vibration monitoring system for vehicles. W: the monograph Activities of Transport Telematics, editors: Mikulski J., TST 2013, CCIS 395. Heidelberg: Springer, 2013: 418-425, DOI 10.1007/978-3-642-41647-7_51.
3. Chen S., Ho T., Mao B.: Maintenance schedule optimisation for a railway power supply system. International Journal of Production Research, 51(16), 2013.
4. Kaniewski P., Smagowski P., Konatowski S.: Ballistic Target Tracking with Use of Cinetheodolites, International Journal of Aerospace Engineering, Volume 2019, Article ID 3240898, DOI 10.1155/2019/3240898.
5. Klimczak T., Paś J.: Selected issues of the reliability and operational assessment of a fire alarm system. Eksploatacja i Niezawodnosc – Maintenance and Reliability, Vol. 21, No. 4, 2019, DOI 10.17531/ein.2019.4.3.

6. Klimczak T., Paś J.: Analysis of reliability structures for fire signaling systems in the field of fire safety and hardware requirements. Journal of KONBiN, Vol. 46, 2018, DOI 10.2478/jok-2018-0030.
7. Kołowrocki K., Soszyńska-Budny J.: Reliability and safety of complex technical systems and processes. Springer, London 2011.
8. Laskowski D., Łubkowski P., Pawlak E., Stańczyk P.: Anthropotechnical systems reliability. W: Nowakowski T., Młyńczak M., Jodejko-Pietruczuk A., Werbińska-Wojciechowska S. (red.): Safety and Reliability: Methodology and Applications - Proceedings of the European Safety and Reliability Conference ESREL 2014. CRC Press/Balkema, London 2015.
9. Loeffler C., Spears E.: Uninterruptible power supply system. In: Hwaiyu Geng P.E. (eds.): Data Center Handbook, John Wiley & Sons, 2015.
10. Paś J.: Shock a disposable time in electronic security systems. Journal of KONBiN Vol. 2(38), 2016, DOI 10.1515/jok-2016-0016.
11. Paś J., Klimczak T.: Modeling of the process of selected fire signaling systems. Diagnostyka, Vol. 20, No. 4, 2019, DOI 10.29354/diag/113047.
12. Reddig K., Dikunow B., Krzykowska K.: Proposal of big data route selection methods for autonomous vehicles. Internet Technology Letters, Vol. 1(36), 2018.
13. Jodejko-Pietruczuk A., Werbińska-Wojciechowska S.: Analysis of maintenance models' parameters estimation for technical systems with delay time. Eksploatacja i Niezawodnosc – Maintenance and Reliability, Vol. 16, No. 2, 2014.
14. Tchórzewska-Cieślak B.: Method of assessing of risk of failure in water supply system. European safety and reliability conference ESREL. Risk, reliability and societal safety. Taylor & Francis, tom 2, Norway, Stavanger 2007.
15. Siergiejczyk M., Stawowy M.: Modelling of uncertainty for continuity quality of power supply. W: "Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL 2016", red. Lesley Walls, Matthew Revie, Tim Bedford. CRC Press/Balkema, 2017.
16. Stawowy M., Kasprzyk Z.: Identifying and simulation of status of an ICT system using rough sets, Tenth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX Springer 2015.
17. Zajkowski K., Rusica I., Palkova Z.: The use of CPC theory for energy description of two nonlinear receivers, MATEC Web of Conferences 2018.
18. Zhuo H.-Y., Liu Z.-Q., Ge Ch.-L.: Development of HPM measurement and control system based on fziber communication. 2017 IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), IEEE, Chengdu, China 2017.
19. Zhang Y.-H., Chai Ch.-Ch., Liu Y., Yang Y.-T., Shi Ch.-L., Fan Q.-Y., Liu Y.-Q.: Modeling and understanding of the thermal failure induced by high power microwave in CMOS inverter. Chinese Physics B, Vol. 26(5), 2017.