Journal of KONBiN 2020
Volume 50, Issue 4
DOI 10.2478/jok-2020-0073

Jacek PAŚ, Adam ROSIŃSKI, Marek SZULIM, Jarosław ŁUKASIAK
Military University of Technology (Wojskowa Akademia Techniczna)

RELIABILITY AND OPERATIONAL ANALYSIS OF AN ELECTRONIC SECURITY SYSTEM TAKING INTO ACCOUNT THE IMPACT OF STRONG ELECTROMAGNETIC PULSES

Analiza niezawodnościowo-eksploatacyjna elektronicznego systemu bezpieczeństwa z uwzględnieniem oddziaływania silnych impulsów elektromagnetycznych

Abstract: *In this article, the authors presented a short historical overview of the visual monitoring systems' development. Attention was also drawn to the features distinguishing the solutions within this group from other electronic systems. Further, the authors conducted a reliability analysis of selected, sample segments of a CCTV system, at the same out highlighting that such a system – considered globally – is distinguished by a mixed reliability structure. The authors suggested a reliability and operational model for a video surveillance system, which takes into account the impact of strong electromagnetic pulses on a fragment of its transmission channel and the mechanical properties of transmission media.*
Keywords: reliability and operational analysis, electronic security systems, strong electromagnetic pulses

Streszczenie: *W artykule autorzy przedstawili krótki rys historyczny rozwoju systemów monitoringu wizyjnego. Zwrócono również uwagę na cechy odróżniające rozwiązania tej grupy od pozostałych systemów elektronicznych. W dalszej kolejności przeprowadzono analizę niezawodnościową wybranych, przykładowych fragmentów systemu CCTV, jednocześnie sygnalizując, że system tego typu rozpatrywany globalnie wyróżnia się mieszaną strukturą niezawodnościową. Autorzy zaproponowali model niezawodnościowo-eksploatacyjny systemu telewizji dozorowej uwzględniający oddziaływanie silnych impulsów elektromagnetycznych na fragment jego toru transmisyjnego oraz właściwości mechanicznych mediów transmisyjnych.*
Słowa kluczowe: analiza niezawodnościowo-eksploatacyjna, elektroniczne systemy bezpieczeństwa, silne impulsy elektromagnetyczne

1. Introduction

CCTV (*Closed Circuit Television*), also called video surveillance systems (alternatively, industrial TV), are a separate group of electronic security systems (ESS). Until just recently, the solutions of such type were used almost solely in commercial applications, i.e., transport (railway areas, airports, bus stations) and manufacturing plants, as well as in strategic public facilities and structures within the critical infrastructure. The referenced phenomenon resulted, among others, from the significant costs of the very equipment making up the system (excluding their installation), which could not be borne by private individuals and from – the then – dominant specificity of the characterized solutions. The principle task of first CCTV generation was depicting numerous scenes within supervised zones to an operator sitting at a station equipped with a monitor and control panel, who was forced to analyse the situation in real-time. An advantage of the group of systems in question is the fact that the operators will not have to remain within the monitored area – which at the same time is a potential hazardous area (currently, an operator can be almost anywhere in the world, without being directly exposed to their impact). When an employee recording an event potentially hazardous to property or people within a supervised zone, he/she took appropriate procedural actions (calling an intervention patrol, notifying appropriate emergency services, deciding to evacuate people and property from the exposed area). Such a designed security system, already at its root, was burdened with significant imperfection in the form of a human factor, and more specifically, physiology (ability to concentrate limited in time). The second of the main CCTV features was limited to recording video material from monitored areas, which in the event of a threat acted as evidence. It should be noted that documenting the cause of damage that had already occurred and caused losses, does not fall in line with the essence of electronic security systems. A preventive aspect of CCTV (discouraging potential aggressors from acting) is closer to achieving the aforementioned outcome. Further development of computational technology, and in consequence, the implementation of image recognition algorithms, as well as biometric and data exploration and image algorithms in contemporary microcontrollers, decreased costs of the electronic device manufacturing cycle, significant improvement of recorded image quality and dissemination of fast, wireless communication, etc. expedited further popularization of video surveillance not only in industry, but also among private consumers. This enabled to partially exclude the human share in the stage of detecting, analysing and taking appropriate response to phenomena identified as a threat (including the notification of a facility owner – administrator). No need for system operator presence, who at the same time monitored the correct functioning of CCTV, necessitates increased requirements associated with appropriate operation and reliability of the analysed solutions.

The available studies within the characterized field indicate positions addressing general operational aspects [11] regarding the aforementioned group of electronic security systems, with particular emphasis on their application in railway transport [12, 13] and telematics [14]. Very few research papers discuss the operational and reliability analysis of

a video surveillance system implemented within railway [16] and road transport [15] areas. Both cases follow the same approach, which assumes a tri-state model (state of fitness, safety hazards and safety unreliability). The papers propose conducting four-type periodic inspections of a video surveillance system.

2. CCTV system characteristics

A video surveillance system, depending on the configuration, topology and complexity contains the following elements:

- Camera with lenses (integrated or stand alone, replaceable accessories);
- Transmission media with intermediate elements (coaxial cable – analogue CCTV, UTP (*Unshielded Twisted Pair*) cable, fibre optic cable, radio transmission, e.g. Wi-Fi, package transmission, etc. – digital CCTV);
- Recording devices (VHS recorders – *Video Home System* used formerly), with DVR – *Digital Video Recorder* used currently, equipped with a single hard drive or drive array and recording servers with software (NVR – *Network Video Recorder*, used today in the most advanced systems);
- Control devices (control panels for PTZ – *Pan Tilt Zoom* cameras);
- Imaging devices (CRT – *Cathode-Ray Tube* screens used formerly, LCD – *Liquid Crystal Display* screens used currently);
- Power supply systems (including UPS with batteries);
- Additional equipment (processing equipment, illuminators, special purpose enclosures for cameras, etc.).

Fig. 1. The structure of a typical analogue video surveillance system for private use and minor commercial objects

One of the most popular, and at the same time simplest embodiments of a contemporary analogue CCTV, has been shown in fig. 1. To ensure the minimum peripheral protection of a structure designed on a rectangle, the presented system requires 4 cameras (four-channel DVR). To further expand the characterized solution, it is required to use a digital recorder equipped with eight, sixteen or thirty-two channels. The presented solution is still one of the most frequent choices for physical consumers and small entrepreneurs. The DVR has an integrated analogue-to-digital converter and an image divider. The analysed configuration stands out owing to a low degree of complexity and a reasonably low cost, and is a compromise in terms of the relation between the system price and the offered quality of recorded image.

Much more extensive systems are tailored to the individual needs of large enterprises, typically industrial facilities, as well as the ones classified as critical infrastructure. In such a case, a decision to install the aforementioned group of electronic security systems is often preceded by a thorough risk analysis including local hazard sources, which justifies financing such solutions. Conventional transmission media based on copper cables are being increasingly replaced with fibre optic links, mainly owing to their gradual popularization and significant price reductions. To set up such a data exchange channel, apart from the fibre itself, one requires optical-to-electrical signal converters on both its ends, which also convert in the opposite direction. Devices of this type can be encountered as an element, which is integrated with or connected to a network point (switch, router) in the form of an insert. They are also found as stand-alone products. An embodiment of a more advanced video surveillance, which partially utilizes a fibre optic medium, is shown in fig. 2.

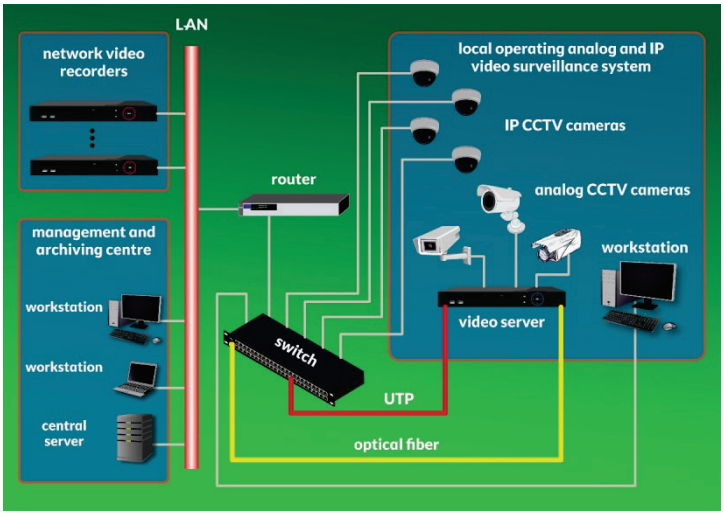


Fig. 2. Sample configuration of an expanded CCTV system, taking into account partial utilization of a fibre optic transmission channel

3. Reliability and operational characteristics of a CCTV system taking into account the impact of strong electromagnetic pulses

The security systems, along with the development of electronics and constantly growing possibilities of practically implementing mathematical algorithms in contemporary microcontrollers and processor systems, increasingly require less intervention of an operator to correctly execute their functions. The fundamental task of such solutions, associated with ensuring security at a specific level both in terms of property, as well as human health and life, can be fulfilled by direct impact on the hazard factor, detecting and communicating its occurrence as early as possible, and also supporting the process of isolating or evacuating people and property away from its source.

Such a high level of responsibility of electronic security systems implies the need to apply technical and procedural measures and mechanisms aimed at ensuring the highest possible unreliability level [4].

When analysing the reliability structure of a CCTV system from fig. 2, one can distinguish basic structures for its individual segments. In case of the camera – video server section, it is a serial structure. Considering a video server and a set of cameras – under certain assumptions – it will be a K and N structure. Whereas the fibre optic link (converter – cable optic fibre – converter) will also exhibit a serial structure. The power supply system with an emergency power source in the form of battery forms a parallel structure with unloaded reserve (in a normal operation state, the battery is unloaded and only charged up). When considering advanced CCTV systems in a global context, it should be concluded that they are characterized by a mixed structure.

In the case of electronic security systems – an operational and reliability analysis taking into account the features typical for the solutions within this group and the topology itself – is certainly an incomplete approach. It is also important to include, at least, the environmental conditions under which the systems referred to are operated. The operating environment of electronic devices, apart from weather conditions, is made up also of their electromagnetic surroundings, which in large industrial and transport (e.g. railway) areas can be significantly disturbed by, among others, artificial, natural, unintended and intentional high-power microwave pulse sources. Such interference, conducted or radiated, can negatively impact video surveillance system elements (operational disturbance or irreversible damage in extreme cases). Importantly, due to the specificity of the analysed group of electronic systems, they are also prone to intentional impact of artificial high-power microwave pulse sources, which can lead to intended destabilization of system functionality or even its complete neutralization. The available source literature contains studies addressing the issues associated with the impact and prevention against such interference. The activities, among others, included an approach to design variants of CCTV camera screening enclosures using lead glass and a metal mesh acting as a microwave seal installed at the camera lens aperture [6]. Further considerations also include the impact of

mesh shape of various cross-sections [7]. Few publications contain the results of tests covering the electromagnetic compatibility of a simple CCTV system (treated as an interference source) [8] and its individual elements, paying particular attention to the cameras (unlike the aforementioned study, the authors conduct measurements not only in the semi-anechoic chamber but also in the GTEM changer [9]. Yet, another research paper concentrates on the idea of modelling electromagnetic compatibility (therefore, the resistance to such radiation and low emission level, related to ESS components) through screening of CCTV system elements [17]. The authors proposed a design of an enclosure in the form of a post, which, in addition to the camera itself, can house a fibre optic media converter. Greater attention to a transmission channel using the aforementioned technology was paid in the publications [1] and [2], where fibre optic converters were studied in terms of their resistance to the impact of high-power microwave pulses (therefore for level highly exceeding the typical tests for conformity with EMC (Electro-Magnetic Compatibility)), simultaneously assessing dedicated shielding enclosures. It should be noted that, when considering all electronic security systems, more attention should be paid to fibre optic transmission channels, which gradually oust conventional hardwired connections, owing to a series of properties. This is supported by, for example, the constantly decreasing price of devices required by such configuration, high bandwidth of a fibre optic transmission medium, low attenuation, no emissions, complete resistance of an optic fibre to electromagnetic and electrical interference, large distances over which data transmission is possible without the need to use intermediate signal amplifiers, and, of course, the very material forming the fibre optic cable, which is not within the scope of interest of people involved in salvaging raw materials. The listed set of features results in the characterized medium being particularly applicable in fields with an extremely unfavourable electromagnetic environment, e.g. industrial or transport areas. This variant should only take into account the possibility of a physical damage to the fibre optic channel. Such an approach was presented in the article [3], whereas the reliability perspective was discussed in [5]. It should be noted that the team of authors, for example in the elaboration [10], drew attention to the legitimacy of taking the impact of strong electromagnetic pulses into account in the operational modelling of electronic devices and systems.

4. Reliability and operational model of a CCTV system utilizing a fibre optic transmission channel, taking into account the impact of high-power electromagnetic pulses

This study contains a preliminary reliability and operational analysis of a CCTV system in the context of strong electromagnetic pulses impacting a segment of its transmission channel, and the technical properties of transmission channels. Consideration was given to a part of a video surveillance system from fig. 2, more specifically, the section comprising a video server, network infrastructure point in the form of a switch and a parallel

transmission channel, which ensures communication between the aforementioned devices, formed of a UTP cable and a single-mode optic fibre. The following assumptions were suggested based on the review of the source literature:

- Appropriate technical measures, in the form of screening, were applied to the video server and switch in order to protect them against direct impact of a strong electromagnetic field (radiated interference). In consequence, the impact of strong electromagnetic pulses on the aforementioned elements, through the mentioned mechanism, was considered negligible.
- Fibre optic media converters, in the form of a dedicated insert were, integrated both within the video server, as well as the switch.
- The only elements exposed to strong electromagnetic radiation (resulting in the possible presence of conducted interference) are within the area with transmission media in the form of a UTP cable and a single-mode optic fibre.
- The simultaneous damage to one of the transmission media and disturbed video server or switch operation is a phenomenon that is so unlikely that it can be omitted.

Given the presented assumptions, the reliability process of the discussed video surveillance system segment, taking into account the technical properties of transmission channels and the impact of a strong electromagnetic field, can be depicted in the form of a graph in fig. 3, where the reliability states are interpreted as follows:

- $\boldsymbol{S_{PZ}}$ – full fitness state (safety state);
- $\boldsymbol{S_{ZB1}}$ – safety hazard state resulting from mechanical damage to the transmission medium in the form of a UTP cable;
- $\boldsymbol{S_{ZB2}}$ – safety hazard state resulting from mechanical damage to the transmission medium in the form of an optic fibre;
- $\boldsymbol{S_{ZB3}}$ – safety hazard state resulting from a disturbance in the operation of a video server due to the impact of strong electromagnetic pulses, which penetrated the device through the conduction mechanism in the transmission medium;
- $\boldsymbol{S_{ZB4}}$ – safety hazard state resulting from a disturbance in the operation of a switch due to the impact of strong electromagnetic pulses, which penetrated the device through the conduction mechanism in the transmission medium;
- $\boldsymbol{S_{ZB5}}$ – safety hazard state resulting from a disturbance in the operation of a switch and video server due to the impact of strong electromagnetic pulses, which penetrated the devices through the conduction mechanism in the transmission medium;
- $\boldsymbol{S_{NZ}}$ – system unfitness state (safety unreliability state).

In turn, the following intensities of transition between reliability states have the definition as follows:

- $\boldsymbol{\lambda_F}$ – damage rate;
- $\mu_{\boldsymbol{R}}$ – repair rate;
- $\boldsymbol{\lambda_{MUTP}}$ – rate of mechanical damage to a communication medium in the form of a UTP cable;

- μ_{MUTP} – rate of repairs of mechanical damage to a communication medium in the form of a UTP cable;
- λ_{MOF} – rate of mechanical damage to a communication medium in the form of a single-mode optic fibre;
- μ_{MOF} – rate of repairs of mechanical damage to a communication medium in the form of a single-mode optic fibre;
- λ_{VSEMI} – rate of electromagnetic interference action, the intensity of which results in disturbed video server operation;
- λ_{DVSEMI} – rate of electromagnetic interference action, the intensity of which results in video server damage;
- λ_{SWEMI} – rate of electromagnetic interference action, the intensity of which results in disturbed switch operation;
- λ_{DSWEMI} – rate of electromagnetic interference action, the intensity of which results in disturbed switch operation;
- $\lambda_{DSWVSEMI}$ – rate of electromagnetic interference action, the intensity of which results in switch and video server damage.

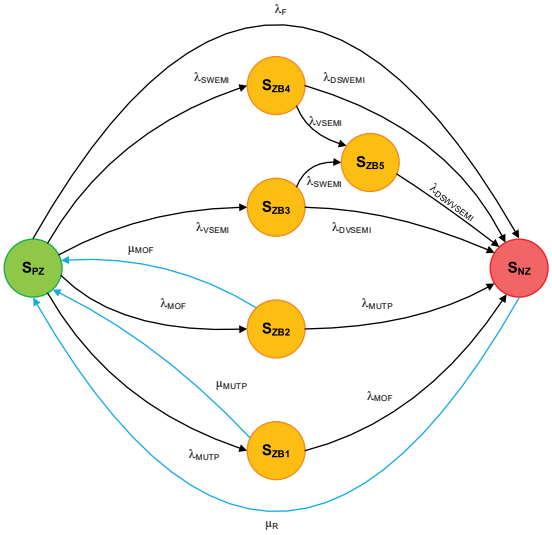


Fig. 3. The reliability process of the video surveillance system segment, taking into account the technical properties of transmission channels and the impact of a strong electromagnetic field

The graph can be presented in the form of an equivalent system of Kolmogorov-Chapman equations.

$$-\lambda_F \cdot S_{PZ} - \lambda_{SWEMI} \cdot S_{PZ} - \lambda_{VSEMI} \cdot S_{PZ} + \mu_{MOF} \cdot S_{ZB2} - \lambda_{MOF} \cdot S_{PZ} + \mu_{MUTP} \cdot S_{ZB1}$$
$$-\lambda_{MUTP} \cdot S_{PZ} + \mu_R \cdot S_{NZ} = 0$$

$$\lambda_{SWEMI} \cdot S_{PZ} - \lambda_{DSWEMI} \cdot S_{ZB4} - \lambda_{VSEMI} \cdot S_{ZB4} = 0$$

$$\lambda_{VSEMI} \cdot S_{ZB4} + \lambda_{SWEMI} \cdot S_{ZB3} - \lambda_{DSWVSEMI} \cdot S_{ZB5} = 0$$

$$\lambda_{VSEMI} \cdot S_{PZ} - \lambda_{SWEMI} \cdot S_{ZB3} - \lambda_{DVSEMI} \cdot S_{ZB3} = 0$$

$$-\mu_{MOF} \cdot S_{ZB2} + \lambda_{MOF} \cdot S_{PZ} - \lambda_{MUTP} \cdot S_{ZB2} = 0$$

$$-\mu_{MUTP} \cdot S_{ZB1} + \lambda_{MUTP} \cdot S_{PZ} - \lambda_{MOF} \cdot S_{ZB1} = 0$$

$$\lambda_F \cdot S_{PZ} + \lambda_{DSWEMI} \cdot S_{ZB4} + \lambda_{DSWVSEMI} \cdot S_{ZB5} + \lambda_{DVSEMI} \cdot S_{ZB3} + \lambda_{MUTP} \cdot S_{ZB2} + \\ + \lambda_{MOF} \cdot S_{ZB1} - \mu_R \cdot S_{NZ} = 0$$

5. Summary and conclusions

The suggested reliability and operational model for a CCTV system takes into account the impact of strong electromagnetic pulses on its transmission media, as well as their mechanical properties. The presented approach can become a useful tool for comparing and classifying electronic security systems, which is important for the process of evaluating the resistance of ESS to high-power microwave radiation. After adopting certain values of individual transition intensities, it will be possible to determine the values of probabilities for an analysed video surveillance system to remain in distinguished reliability and operating states. It should be noted that there is a justified demand for research work aimed at estimating individual values of transition intensities, based on practical measurements. In the course of future research, the authors plan to introduce factors, which take into account individual values of individual transmission channel variations on the impact of strong electromagnetic pulses, and intend to extend the suggested model with further video surveillance system devices.

Acknowledgement
The work was supported by the Polish National Centre for Research and Development within the project "Methods and ways of protection and defence against HPM impulses" pending within strategic project: "New weaponry and defense systems of directed energy".

6. References

1. Adami C., Braun C., Clemens P., et al.: High Power Microwave Tests of Media Converters. International Symposium on Electromagnetic Compatibility - EMC EUROPE, 17-21.09.2012 Roma, C4:5, DOI: 10.1109/EMCEurope.2012.6396758.

2. Adami C., Braun C., Clemens P., et al.: Susceptibility of Two Deployable C4I Systems to HPM – Improvement by Hardening. [In:] Aschenbruck N., Martini P., Meier M., Tölle J.: Future security: 7th Security Research Conference, Future Security 2012, Bonn, Germany, September 4-6, 2012: Proceedings, Communications in Computer and Information Science, Vol. 318, DOI: 10.1007/978-3-642-33161-9_34.
3. Brönnimann R., Nellen P. M., Sennhauser U.: Application and reliability of a fiber optical surveillance system for a stay cable bridge. Smart Materials and Structures, 1998, Vol. 7, No. 2, DOI: 10.1088/0964-1726/7/2/010.
4. Caban D., Walkowiak T.: Dependability Analysis of Hierarchically Composed System-of-Systems. [In:] Zamojski W., Mazurkiewicz J., Sugier J., Walkowiak T., Kacprzyk J. (eds.) Contemporary Complex Systems and Their Dependability. DepCoS-RELCOMEX 2018. Advances in Intelligent Systems and Computing, vol. 761, 2019. Springer, Cham. DOI: 10.1007/978-3-319-91446-6_12.
5. Chołda P., Jajszczyk A.: Ocena gotowości w sieciach telekomunikacyjnych. Przegląd Telekomunikacyjny, Vol. 75, nr 2-3, 2003.
6. Kovář S., Mach V., Valouch J., Adámek M.: Design of shielding enclosure to protect security devices. 2017 Progress in Electromagnetics Research Symposium - Fall (PIERS - FALL): Proceedings, 19-22 Nov. 2017 Singapore, DOI: 10.1109/PIERS-FALL.2017.8293543.
7. Kovář S., Valouch J., Adámek M., Zacek P.: Shielding protection comparison for security cameras lenses. 22nd International Conference Electronics, Palanga 18-20 June 2018, DOI: 10.1109/ELECTRONICS.2018.8443631.
8. Kovář S., Valouch J., Urbančoková H., Adámek M.: Electromagnetic interference of CCTV. International Conference on Information and Digital Technologies, Zilina, 7-9 July 2015, Slovakia, DOI: 10.1109/DT.2015.7222968.
9. Kovář S., Valouch J., Urbančoková H., Adámek M.: Impact of security cameras on electromagnetic environment in far and near-field. International Conference on Information and Digital Technologies (IDT), Rzeszów 5-7 July 2016, Poland, DOI: 10.1109/DT.2016.7557166.
10. Paś J., Rosiński A., Łukasiak J., Szulim M.: The Impact of Strong Electromagnetic Pulses on the Operation Process of Electronic Equipment and Systems Used in Intelligent Buildings. [In:] Zamojski W., Mazurkiewicz J., Sugier J., Walkowiak T., Kacprzyk J. (eds.): Engineering in Dependability of Computer Systems and Networks. DepCoS-RELCOMEX 2019, July 1-5 2019 Brunów Poland. Seria wydawnicza: Advances in Intelligent Systems and Computing, vol. 987. Springer, Cham, Switzerland, DOI: 10.1007/978-3-030-19501-4_38.
11. Paś J., Rosiński A., Wiśnios M., Majda-Zdancewicz E., Łukasiak J.: Elektroniczne systemy bezpieczeństwa: Wprowadzenie do laboratorium. Wojskowa Akademia Techniczna, Warszawa 2018.
12. Siergiejczyk M., Chmiel J., Rosiński A.: Modern solutions of CCTV systems used in rail transport. Problemy kolejnictwa, Vol. 59, z. 166, 2015.

13. Siergiejczyk M., Korczak D., Rosiński A.: Wspomaganie informatyczne funkcjonowania systemów monitoringu wizyjnego w kolejowych obiektach transportowych. Prace naukowe Politechniki Warszawskiej: Transport, z. 113, 2016.
14. Siergiejczyk M., Paś J., Rosiński A.: Application of closed circuit television for highway telematics. [in:] Mikulski J. (ed.): Telematics in the Transport Environment: 12th International Conference on Transport Systems Telematics (TST 2012), Katowice-Ustroń, Poland, October 10–13, 2012, Selected Papers, Communications in Computer and Information Science, Vol. 329, DOI: 10.1007/978-3-642-34050-5_19.
15. Siergiejczyk M., Paś J., Rosiński A.: Evaluation of safety of highway CCTV system's maintenance process. [in:] Mikulski J. (ed.): Telematics - Support for Transport: 14th International Conference on Transport Systems Telematics (TST 2014), pp. 69-79, Communications in Computer and Information Science, Vol. 471, DOI: 10.1007/978-3-662-45317-9_8.
16. Siergiejczyk M., Paś J., Rosiński A.: Reliability and maintenance analysis of CCTV systems used in rail transport. Journal of KONBiN, 2015, No. 3 (35), DOI: 10.1515/jok-2015-0047.
17. Urbančoková H., Valouch J.: Monitoring of the tests EMS information technology equipment using the CCTV system. International Journal of Circuits, Systems and Signal Processing, Vol. 9, 2015.

ANALIZA NIEZAWODNOŚCIOWO-EKSPLOATACYJNA ELEKTRONICZNEGO SYSTEMU BEZPIECZEŃSTWA Z UWZGLĘDNIENIEM ODDZIAŁYWANIA SILNYCH IMPULSÓW ELEKTROMAGNETYCZNYCH

1. Wprowadzenie

Systemy monitoringu wizyjnego – CCTV (ang. *Closed Circuit Television*), zwane również systemami telewizji dozorowej (alternatywnie telewizji przemysłowej), stanowią odrębną grupę elektronicznych systemów bezpieczeństwa (ESB). Jeszcze do niedawna rozwiązania tego typu wykorzystywano niemal wyłącznie w zastosowaniach komercyjnych, a więc obszarach transportowych (tereny kolejowe, porty lotnicze, dworce autobusowe), zakładach produkcyjnych, a także w strategicznych obiektach publicznych oraz należących do infrastruktury krytycznej. Przytoczone zjawisko wynikało m.in. ze znacznych kosztów samych urządzeń składających się na system (nie uwzględniając ich montażu), na których poniesienie nie mogły pozwolić sobie osoby prywatne, oraz z ówczesnej – dominującej specyfiki charakteryzowanych rozwiązań. Głównym zadaniem pierwszych generacji CCTV było obrazowanie wielu scen dozorowanych stref przed operatorem siedzącym przy stanowisku wyposażonym w monitor i pulpit sterowniczy, który zmuszony był analizować sytuację w czasie rzeczywistym. Zaletą opisywanej grupy systemów jest fakt, że personel obsługi nie musiał znajdować się w monitorowanym obszarze – będącym jednocześnie potencjalnym terytorium występowania zagrożeń (obecnie może przebywać niemal w dowolnym miejscu na ziemi, nie będąc bezpośrednio narażonym na ich oddziaływanie). W sytuacji gdy pracownik odnotował zdarzenie stwarzające niebezpieczeństwo dla mienia lub osób znajdujących się w strefie objętej nadzorem, podejmował odpowiednie działania proceduralne (wezwanie patrolu interwencyjnego, powiadomienie odpowiednich służb ratunkowych, podjęcie decyzji o ewakuacji osób i mienia z zagrożonego obszaru). Tak skonstruowany system bezpieczeństwa już u swoich podstaw obarczony był znaczną niedoskonałością w postaci czynnika ludzkiego, a dokładniej jego fizjologii (ograniczonej w czasie zdolności koncentracji). Druga z głównych funkcji telewizji dozorowej ograniczała się do zapisu materiału filmowego z monitorowanych stref, który w przypadku wystąpienia zagrożenia odgrywał rolę dowodową. Należy stwierdzić, że dokumentowanie przyczyn szkody, która już się dokonała i spowodowała straty, nie wpisuje się w istotę elektronicznych systemów bezpieczeństwa.

Bliższy osiągnięcia wspomnianego rezultatu jest aspekt prewencyjny CCTV (zniechęcający potencjalnych agresorów do działania).

Dalszy rozwój technologii obliczeniowej, a w konsekwencji implementacja algorytmów rozpoznawania w obrazie, biometrycznych, eksploracji i analizy danych do współczesnych mikrokontrolerów, zmniejszone koszty cyklu produkcyjnego urządzeń elektronicznych, znaczna poprawa jakości rejestrowanego obrazu oraz upowszechnienie szybkiej komunikacji bezprzewodowej przyspieszyły popularyzację monitoringu wizyjnego nie tylko w przemyśle, ale również wśród odbiorców prywatnych. Pozwoliło to na częściowe wyłączenie udziału człowieka w etapie wykrywania, analizowania i podejmowania odpowiednich reakcji na zjawiska identyfikowane jako zagrożenie (w tym powiadamiania właściciela – zarządcy obiektu). Brak konieczności obecności operatora systemu, który jednocześnie sprawował kontrolę nad poprawnością funkcjonowania CCTV wymusza zwiększenie wymagań związanych z odpowiednią eksploatacją i niezawodnością analizowanych rozwiązań.

W dostępnych opracowaniach z charakteryzowanego obszaru wiedzy można odszukać pozycje poruszające ogólne aspekty eksploatacji [11] wspomnianej grupy elektronicznych systemów bezpieczeństwa ze szczególnym uwzględnieniem zastosowania ich w transporcie kolejowym [12, 13] i telematyce [14]. Nieliczne artykuły naukowe przedstawiają analizę niezawodnościowo-eksploatacyjną monitoringu wizyjnego implementowanego na obszarach kolejowych [16] i transportu autostradowego [15]. W obydwu przypadkach wykorzystano takie samo podejście, zakładające model trójstanowy (stan zdatności, stan zagrożenia bezpieczeństwa oraz stan zawodności bezpieczeństwa). W publikacjach zaproponowano przeprowadzanie czterorodzajowych przeglądów okresowych monitoringu wizyjnego.

2. Charakterystyka systemu CCTV

W skład systemu monitoringu wizyjnego w zależności od konfiguracji, topologii i stopnia złożoności wchodzą następujące elementy:

- kamery z obiektywami (zintegrowanymi lub stanowiącymi osobne – wymienne akcesoria);
- media transmisyjne wraz z elementami pośredniczącymi (przewód koncentryczny – CCTV analogowe, kabel UTP (ang. *Unshielded Twisted Pair*), światłowód, transmisja radiowa np. Wi-Fi, transmisja pakietowa itp. – CCTV cyfrowe);
- urządzenia rejestrujące (dawniej wykorzystywano rejestratory VHS – ang. *Video Home System*), obecnie stosuje się rejestratory cyfrowe DVR – ang. *Digital Video Recorder*, wyposażone w pojedynczy dysk twardy lub macierz dyskową, serwery rejestrujące wraz z oprogramowaniem (NVR – ang. *Network Video Recorder*, stosowane współcześnie w najbardziej zaawansowanych systemach);
- urządzenia sterujące (pulpity sterownicze dla kamer PTZ – ang. *Pan Tilt Zoom*);
- urządzenia obrazujące (dawniej stosowano monitory CRT – ang. *Cathode-Ray Tube*, obecnie wykorzystuje się monitory LCD – ang. *Liquid Crystal Display*);

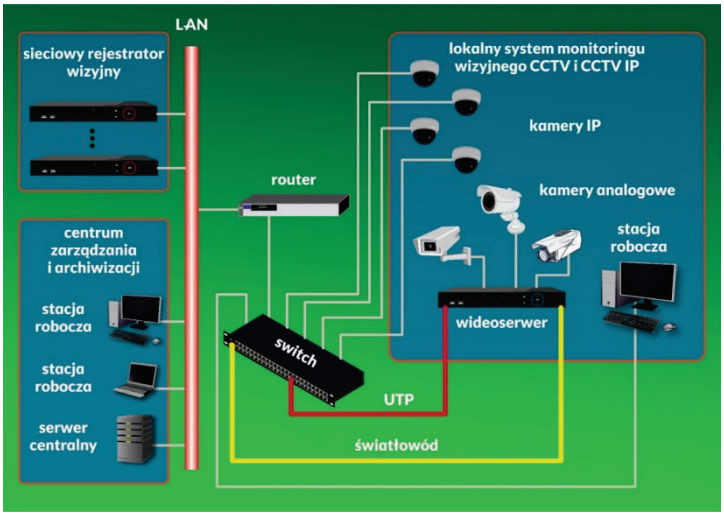
- układy zasilające (w tym zasilacze rezerwowe wraz z akumulatorami);
- dodatkowy osprzęt (urządzenia przetwarzające, doświetlacze, obudowy specjalnego przeznaczenia dla kamer itp.).

Jedną z najbardziej popularnych i jednocześnie najprostszych realizacji współcześnie stosowanego analogowego CCTV zilustrowano na rys. 1. Przedstawiony system do zapewnienia minimalnej ochrony peryferyjnej obiektu skonstruowanego na planie prostokąta wymaga czterech kamer (DVR czterokanałowy). Do dalszej jego rozbudowy niezbędne jest zastosowanie cyfrowego rejestratora wyposażonego w 8, 16 lub 32 kanały. Zaprezentowane rozwiązanie jest wciąż jednym z najczęstszych wyborów wśród odbiorców fizycznych i niewielkich przedsiębiorców. DVR posiada zintegrowany przetwornik analogowo-cyfrowy i dzielnik obrazu. Analizowana konfiguracja wyróżnia się niewielkim stopniem złożoności i racjonalnie niedużym kosztem oraz jest kompromisem stosunku ceny systemu do oferowanej jakości rejestrowanego obrazu.

Rys. 1. Struktura typowej konfiguracji analogowego systemu monitoringu wizyjnego do zastosowań prywatnych i w niewielkich obiektach komercyjnych

Znacznie bardziej rozbudowane systemy tworzone są na indywidualne potrzeby dużych przedsiębiorstw, obiektów typowo przemysłowych, jak również zaliczanych do infrastruktury krytycznej. W takim przypadku decyzja o instalacji systemów bezpieczeństwa często poprzedzona jest gruntowną analizą ryzyka z uwzględnieniem lokalnych źródeł zagrożeń, która uzasadnia finansowanie rozwiązań tego typu. Konwencjonalne media transmisyjne oparte na kablach miedziowych coraz częściej zastępowane są łączami światłowodowymi głównie za sprawą ich stopniowego upowszechnienia i znacznej redukcji cen. Do zestawienia takiego toru wymiany danych oprócz samego włókna niezbędne są na jego obydwu końcach konwertery zmieniające sygnał optyczny na elektryczny oraz dokonujące wspomnianej przemiany w kierunku odwrotnym. Urządzenia tego typu można spotkać jako element zintegrowany lub dołączany do punktu sieciowego (switch, router) w postaci wkładki, występują również jako osobne produkty. Przykład

realizacji bardziej zaawansowanego systemu monitoringu wizyjnego, częściowo wykorzystującego medium światłowodowe, zaprezentowano na rys. 2.



Rys. 2. Przykładowa konfiguracja rozbudowanego CCTV z uwzględnieniem częściowego wykorzystania światłowodowego toru transmisyjnego

3. Charakterystyka niezawodnościowo-eksploatacyjna systemu CCTV z uwzględnieniem oddziaływania silnych impulsów elektromagnetycznych

Systemy bezpieczeństwa wraz z postępującym rozwojem elektroniki oraz stale zwiększającymi się możliwościami praktycznego implementowania algorytmów matematycznych we współczesnych mikrokontrolerach i układach procesorowych w coraz mniejszym stopniu wymagają ingerencji operatora do prawidłowego realizowania swoich funkcji. Podstawowe zadanie rozwiązań tego typu związane z zapewnieniem bezpieczeństwa na określonym poziomie zarówno w odniesieniu do mienia, jak i zdrowia oraz życia ludzkiego może być spełniane poprzez bezpośrednie oddziaływanie na czynnik stwarzający zagrożenie, możliwie najwcześniejsze wykrywanie i informowanie o jego wystąpieniu, a także wspomaganie procesu odizolowania lub ewakuacji osób i mienia od jego źródła.

Tak znaczna odpowiedzialność elektronicznych systemów bezpieczeństwa implikuje konieczność stosowania mechanizmów, środków technicznych i proceduralnych mających na celu zapewnienie im możliwie najwyższego poziomu niezawodności [4].

Analizując strukturę niezawodnościową systemu CCTV z rys. 2, można dla jego poszczególnych fragmentów wydzielić struktury podstawowe. W przypadku odcinka: kamera–wideoserwer będzie to struktura szeregowa. Wideoserwer i zestaw kamer – przy

pewnych założeniach będzie strukturą typu K z N. Z kolei łącze światłowodowe (konwerter – włókno światłowodu – konwerter) również odznaczać się będzie strukturą szeregową. Układ zasilania z awaryjnym źródłem zasilania w postaci akumulatora utworzy strukturę równoległą z rezerwą nieobciążoną (akumulator w trwającym stanie normalnej pracy systemu nie jest obciążany, a jedynie doładowywany). Rozpatrując zaawansowany CCTV w ujęciu globalnym, stwierdzić należy, że charakteryzuje się strukturą mieszaną.

W przypadku elektronicznych systemów bezpieczeństwa wzięcie pod uwagę cech typowych dla rozwiązań tej grupy oraz samej topologii w analizie eksploatacyjno-niezawodnościowej z pewnością jest podejściem niepełnym. Istotne jest również uwzględnienie chociażby warunków środowiskowych, w których eksploatowane są wspomniane systemy. Na środowisko pracy urządzeń elektronicznych oprócz warunków klimatycznych składa się także ich otoczenie elektromagnetyczne, które na rozległych obszarach przemysłowych i transportowych (np. kolejowych) może być w znacznym stopniu zaburzane m.in. przez sztuczne, naturalne, niezamierzone i intencjonalne źródła impulsów mikrofalowych dużej mocy. Takie zakłócenia (przewodzenie lub promieniowanie) mogą mieć negatywny wpływ na elementy systemu monitoringu wizyjnego (zaburzenie pracy lub w skrajnym przypadku nieodwracalne uszkodzenie). Co ważne, ze względu na specyficzny charakter analizowanej grupy systemów elektronicznych, są one również narażone na intencjonalne oddziaływanie sztucznych źródeł impulsów mikrofalowych dużej mocy, które doprowadzić mają do zamierzonej destabilizacji funkcjonowania systemu lub nawet jego całkowitego zneutralizowania. Dostępne są opracowania podejmujące tematykę wpływu oraz przeciwdziałania takim zakłóceniom. Podjęto m.in. próbę zaprojektowania wariantów obudów ekranujących kamery CCTV kolejno z zastosowaniem szkła ołowiowego oraz metalowej siatki pełniącej funkcję uszczelki mikrofalowej, montowanej przed aperturą obiektywu kamery [6]. W dalszych rozważaniach uwzględniono również wpływ kształtu oczek o różnym przekroju [7]. W nielicznych publikacjach zamieszczono wyniki badań kompatybilności elektromagnetycznej prostego systemu CCTV (traktowanego jako źródło zakłóceń) [8] oraz jego poszczególnych elementów, poświęcając szczególną uwagę kamerom (w przeciwieństwie do uprzednio wymienionego opracowania autorzy przeprowadzają pomiary nie tylko w komorze częściowo bezodbiciowej (ang. *semi-anechoic chamber*), ale również w komorze GTEM [9]. Kolejna pozycja również koncentruje się na idei modelowania kompatybilności elektromagnetycznej (a więc odporności na promieniowanie tego typu oraz niskiego poziomu emisji, odniesionych do urządzeń składowych ESB) poprzez ekranowanie elementów systemu CCTV [17]. Zaproponowano projekt obudowy w postaci słupka, w którym oprócz samej kamery można ulokować mediakonwerter światłowodowy. Większą uwagę torowi transmisyjnemu wykorzystującemu wspomnianą technologię poświęcono w publikacjach [1, 2] gdzie konwertery światłowodowe badano pod kątem odporności na wpływ impulsów mikrofalowych dużej mocy (a więc dla poziomów znacznie przewyższających typowe badanie na zgodność z EMC (ang. *Electro-Magnetic Compatibility*), równocześnie poddając ocenie dedykowane obudowy ekranujące. Rozpatrując wszelkie elektroniczne systemy bezpieczeństwa coraz częściej należy brać pod

uwagę światłowodowe tory transmisyjne, które za sprawą szeregu właściwości stopniowo wypierają konwencjonalne połączenia przewodowe. Przemawia za tym chociażby coraz niższa cena urządzeń koniecznych do wykonania takiej konfiguracji, duża przepustowość światłowodowego medium transmisyjnego, niskie tłumienie, brak emisji, całkowita odporność włókna światłowodu na zakłócenia elektromagnetyczne i elektryczne, duże odległości, na których możliwa jest transmisja danych bez konieczności stosowania pośredniczących urządzeń wzmacniających sygnał, i oczywiście sam materiał tworzący światłowód, który nie znajduje się w polu zainteresowania osób trudniących się zbieraniem surowców na odzysk. Wymieniony zestaw cech sprawia, że charakteryzowane medium ma szczególne zastosowanie w obszarach o wyjątkowo niekorzystnym środowisku elektromagnetycznym, jak np. tereny przemysłowe czy transportowe. W takim wariancie należy jedynie uwzględniać możliwość fizycznego uszkodzenia toru światłowodowego. Podejście tego typu przedstawiono w artykule [3], z kolei spojrzenie z perspektywy niezawodnościowej ujęto w [5]. Należy zaznaczyć, że zespół autorski chociażby w opracowaniu [10] zwracał uwagę na zasadność uwzględniania oddziaływania silnych impulsów elektromagnetycznych w procesie modelowania procesu eksploatacji urządzeń i systemów elektronicznych.

4. Model niezawodnościowo-eksploatacyjny systemu CCTV korzystającego ze światłowodowego toru transmisyjnego z uwzględnieniem oddziaływania impulsów elektromagnetycznych dużej mocy

Niniejsze opracowanie zawiera wstępną analizę niezawodnościowo-eksploatacyjną CCTV z uwzględnieniem oddziaływania silnych impulsów elektromagnetycznych na fragment jego toru transmisyjnego oraz właściwości mechanicznych mediów transmisyjnych. Rozważaniom poddano część systemu monitoringu wizyjnego z rys. 2, a dokładniej odcinek składający się z wideoserwera, punktu infrastruktury sieciowej w postaci switcha i zrównoleglonego toru transmisyjnego, zapewniającego komunikację pomiędzy wymienionymi urządzeniami, utworzonego z przewodu UTP i jednomodowego włókna światłowodowego.

Na podstawie przeprowadzonego przeglądu literaturowego zaproponowano następujące założenia:

- W stosunku to wideoserwera i switcha zastosowano odpowiednie środki techniczne w postaci ekranowania w celu ochrony przed bezpośrednim oddziaływaniem silnego pola elektromagnetycznego (zaburzenia promieniowane). W rezultacie wpływ silnych impulsów elektromagnetycznych oddziałujących na wspomniane elementy poprzez przytoczony mechanizm uznano za pomijalny.
- Mediakonwertery światłowodowe zostały zintegrowane zarówno w wideoserwerze, jak i switchu w postaci dedykowanej wkładki.

- Jedynym elementem narażonym na silne promieniowanie elektromagnetyczne (w konsekwencji możliwe jest występowanie zaburzeń przewodzonych) jest obszar, na którym ulokowano media transmisyjne w postaci kabla UTP oraz jednomodowego włókna światłowodowego.
- Jednoczesne wystąpienie uszkodzenia jednego z mediów transmisyjnych oraz zakłócenie pracy wideoserwera lub switcha jest zjawiskiem na tyle mało prawdopodobnym, że można je pominąć.

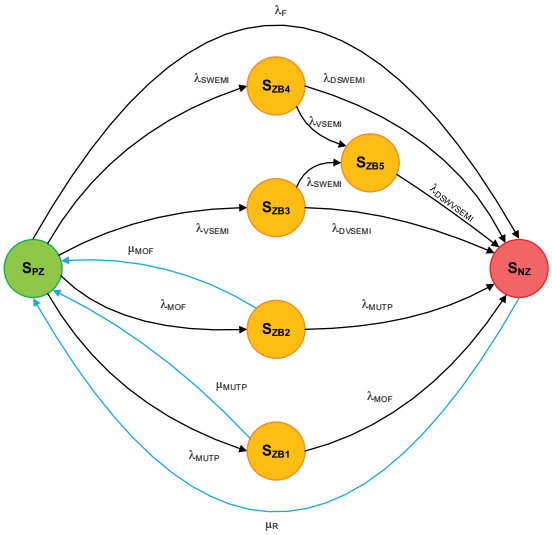
Biorąc pod uwagę przedstawione założenia, proces niezawodnościowy zaprezentowanego fragmentu systemu monitoringu wizyjnego z uwzględnieniem właściwości technicznych torów transmisyjnych oraz oddziaływania silnego pola elektromagnetycznego można zilustrować grafem z rys. 3, gdzie stany niezawodnościowe mają następującą interpretację:

- $\boldsymbol{S_{PZ}}$ – stan pełnej zdatności (stan bezpieczeństwa);
- $\boldsymbol{S_{ZB1}}$ – stan zagrożenia bezpieczeństwa wynikający z mechanicznego uszkodzenia medium transmisyjnego w postaci kabla UTP;
- $\boldsymbol{S_{ZB2}}$ – stan zagrożenia bezpieczeństwa wynikający z mechanicznego uszkodzenia medium transmisyjnego w postaci włókna światłowodowego;
- $\boldsymbol{S_{ZB3}}$ – stan zagrożenia bezpieczeństwa wynikający z zaburzenia pracy wideoserwera na skutek oddziaływania silnych impulsów elektromagnetycznych, które dostały się do urządzenia poprzez mechanizm przewodzenia w medium transmisyjnym;
- $\boldsymbol{S_{ZB4}}$ – stan zagrożenia bezpieczeństwa wynikający z zaburzenia pracy switcha na skutek oddziaływania silnych impulsów elektromagnetycznych, które dostały się do urządzenia poprzez mechanizm przewodzenia w medium transmisyjnym;
- $\boldsymbol{S_{ZB5}}$ – stan zagrożenia bezpieczeństwa wynikający z zaburzenia pracy switcha oraz wideoserwera na skutek oddziaływania silnych impulsów elektromagnetycznych, które dostały się do urządzeń poprzez mechanizm przewodzenia w medium transmisyjnym;
- $\boldsymbol{S_{NZ}}$ – stan niezdatności systemu (stan zawodności bezpieczeństwa).

Intensywności przejść pomiędzy stanami niezawodnościowymi oznaczone na rys. 3:

- $\boldsymbol{\lambda_F}$ – intensywność uszkodzeń;
- $\mu_{\boldsymbol{R}}$ – intensywność napraw;
- $\boldsymbol{\lambda_{MUTP}}$ – intensywność uszkodzeń mechanicznych medium komunikacyjnego w postaci kabla UTP;
- $\mu_{\boldsymbol{MUTP}}$ – intensywność napraw uszkodzeń mechanicznych powstałych w medium komunikacyjnym w postaci kabla UTP;
- $\boldsymbol{\lambda_{MOF}}$ – intensywność uszkodzeń mechanicznych medium komunikacyjnego w postaci jednomodowego włókna światłowodowego;
- $\mu_{\boldsymbol{MOF}}$ – intensywność napraw uszkodzeń mechanicznych powstałych w medium komunikacyjnym w postaci jednomodowego włókna światłowodowego;
- $\boldsymbol{\lambda_{VSEMI}}$ – intensywność oddziaływania zaburzeń elektromagnetycznych, których poziom natężenia skutkuje zaburzeniem pracy wideoserwera;

- $\boldsymbol{\lambda_{DVSEMI}}$ – intensywność oddziaływania zaburzeń elektromagnetycznych, których poziom natężenia skutkuje uszkodzeniem wideoserwera;
- $\boldsymbol{\lambda_{SWEMI}}$ – intensywność oddziaływania zaburzeń elektromagnetycznych, których poziom natężenia skutkuje zaburzeniem pracy switcha;
- $\boldsymbol{\lambda_{DSWEMI}}$ – intensywność oddziaływania zaburzeń elektromagnetycznych, których poziom natężenia skutkuje uszkodzeniem switcha;
- $\boldsymbol{\lambda_{DSWVSEMI}}$ – intensywność oddziaływania zaburzeń elektromagnetycznych, których poziom natężenia skutkuje uszkodzeniem switcha oraz wideoserwera.



Rys. 3. Proces niezawodnościowy fragmentu systemu monitoringu wizyjnego z uwzględnieniem właściwości technicznych torów transmisyjnych oraz oddziaływania silnego pola elektromagnetycznego

Zaprezentowany graf można przedstawić w postaci równoważnego układu równań Kołmogorowa-Chapmana.

$$-\lambda_F \cdot S_{PZ} - \lambda_{SWEMI} \cdot S_{PZ} - \lambda_{VSEMI} \cdot S_{PZ} + \mu_{MOF} \cdot S_{ZB2} - \lambda_{MOF} \cdot S_{PZ} + \mu_{MUTP} \cdot S_{ZB1} - \lambda_{MUTP} \cdot S_{PZ} + \mu_R \cdot S_{NZ} = 0$$

$$\lambda_{SWEMI} \cdot S_{PZ} - \lambda_{DSWEMI} \cdot S_{ZB4} - \lambda_{VSEMI} \cdot S_{ZB4} = 0$$

$$\lambda_{VSEMI} \cdot S_{ZB4} + \lambda_{SWEMI} \cdot S_{ZB3} - \lambda_{DSWVSEMI} \cdot S_{ZB5} = 0$$

$$\lambda_{VSEMI} \cdot S_{PZ} - \lambda_{SWEMI} \cdot S_{ZB3} - \lambda_{DVSEMI} \cdot S_{ZB3} = 0$$

$$-\mu_{MOF} \cdot S_{ZB2} + \lambda_{MOF} \cdot S_{PZ} - \lambda_{MUTP} \cdot S_{ZB2} = 0$$

$$-\mu_{MUTP} \cdot S_{ZB1} + \lambda_{MUTP} \cdot S_{PZ} - \lambda_{MOF} \cdot S_{ZB1} = 0$$

$$\lambda_F \cdot S_{PZ} + \lambda_{DSWEMI} \cdot S_{ZB4} + \lambda_{DSWVSEMI} \cdot S_{ZB5} + \lambda_{DVSEMI} \cdot S_{ZB3} + \lambda_{MUTP} \cdot S_{ZB2} + \lambda_{MOF} \cdot S_{ZB1} - \mu_R \cdot S_{NZ} = 0$$

5. Podsumowanie i wnioski

Zaproponowany model eksploatacyjno-niezawodnościowy systemu CCTV uwzględnia oddziaływanie silnych impulsów elektromagnetycznych na jego media transmisyjne oraz bierze pod uwagę ich właściwości mechaniczne. Prezentowane podejście może być przydatnym narzędziem służącym do porównywania i klasyfikowania elektronicznych systemów bezpieczeństwa, które ma istotne znaczenie w procesie oceny odporności ESB na promieniowanie mikrofalowe dużej mocy. Po przyjęciu pewnych wartości poszczególnych intensywności przejść możliwe będzie określenie wartości prawdopodobieństw przebywania analizowanego systemu monitoringu wizyjnego w wyróżnionych stanach niezawodnościowo-eksploatacyjnych. Należy zaznaczyć, że istnieje uzasadnione zapotrzebowanie na prace badawcze mające na celu oszacowanie poszczególnych wartości intensywności przejść na podstawie praktycznych pomiarów. W dalszych pracach zespół autorski planuje wprowadzenie współczynników, które uwzględnią indywidualne właściwości poszczególnych odmian torów transmisyjnych na oddziaływanie silnych impulsów elektromagnetycznych, oraz zamierza rozszerzyć zaproponowany model o kolejne urządzenia systemu telewizji dozorowej.

Podziękowanie
Badania zostały sfinansowane przez NCBiR - Umowa DOB-1-3/1/PS/2014 pn. „Metody i sposoby ochrony i obrony przed impulsami HPM" w ramach programu strategicznego „Nowe systemy uzbrojenia i obrony w zakresie energii skierowanej".

6. Literatura

1. Adami C., Braun C., Clemens P. et al.: High Power Microwave Tests of Media Converters. International Symposium on Electromagnetic Compatibility - EMC EUROPE, 17-21.09.2012 Rzym, artykuł C4:5, DOI: 10.1109/EMCEurope.2012.6396758.
2. Adami C., Braun C., Clemens P. et al.: Susceptibility of Two Deployable C4I Systems to HPM – Improvement by Hardening [w:] Aschenbruck N., Martini P., Meier M., Tölle J.: Future security: 7th Security Research Conference, Future Security 2012, Bonn, Germany, September 4-6, 2012: Proceedings,

Communications in Computer and Information Science, Vol. 318, DOI: 10.1007/978-3-642-33161-9_34.
3. Brönnimann R., Nellen P. M., Sennhauser U.: Application and reliability of a fiber optical surveillance system for a stay cable bridge. Smart Materials and Structures, 1998, Vol. 7, No. 2, DOI: 10.1088/0964-1726/7/2/010.
4. Caban D., Walkowiak T.: Dependability Analysis of Hierarchically Composed System-of-Systems. [w:] Zamojski W., Mazurkiewicz J., Sugier J., Walkowiak T., Kacprzyk J. (eds.): Contemporary Complex Systems and Their Dependability. DepCoS-RELCOMEX 2018. Advances in Intelligent Systems and Computing, vol. 761, 2019. Springer, Cham. DOI: 10.1007/978-3-319-91446-6_12.
5. Chołda P., Jajszczyk A.: Ocena gotowości w sieciach telekomunikacyjnych. Przegląd Telekomunikacyjny, r. 75, nr 2-3, 2003.
6. Kovář S., Mach V., Valouch J., Adámek M.: Design of shielding enclosure to protect security devices. 2017 Progress in Electromagnetics Research Symposium - Fall (PIERS - FALL): Proceedings, 19-22 Nov. 2017 Singapore, DOI: 10.1109/PIERS-FALL.2017.8293543.
7. Kovář S., Valouch J., Adámek M., Zacek P.: Shielding protection comparison for security cameras lenses. 2018 22nd International Conference Electronics, Palanga 18-20 June 2018, DOI: 10.1109/ELECTRONICS.2018.8443631.
8. Kovář S., Valouch J., Urbančoková H., Adámek M.: Electromagnetic interference of CCTV. 2015 International Conference on Information and Digital Technologies, Zilina, 7-9 July 2015, Slovakia, DOI: 10.1109/DT.2015.7222968.
9. Kovář S., Valouch J., Urbančoková H., Adámek M.: Impact of security cameras on electromagnetic environment in far and near-field. 2016 International Conference on Information and Digital Technologies (IDT), Rzeszów 5-7 July 2016, Poland, DOI: 10.1109/DT.2016.7557166.
10. Paś J., Rosiński A., Łukasiak J., Szulim M.: The Impact of Strong Electromagnetic Pulses on the Operation Process of Electronic Equipment and Systems Used in Intelligent Buildings. [w:] Zamojski W., Mazurkiewicz J., Sugier J., Walkowiak T., Kacprzyk J. (red.): Engineering in Dependability of Computer Systems and Networks. DepCoS-RELCOMEX 2019 July 1-5 2019 Brunów Poland. Seria wydawnicza: Advances in Intelligent Systems and Computing, vol. 987. Springer, Cham, Switzerland, DOI: 10.1007/978-3-030-19501-4_38.
11. Paś J., Rosiński A., Wiśnios M., Majda-Zdancewicz E., Łukasiak J.: Elektroniczne systemy bezpieczeństwa: Wprowadzenie do laboratorium. Wojskowa Akademia Techniczna, Warszawa 2018.
12. Siergiejczyk M., Chmiel J., Rosiński A.: Modern solutions of CCTV systems used in rail transport. Problemy kolejnictwa, Vol. 59, z. 166, 2015.
13. Siergiejczyk M., Korczak D., Rosiński A.: Wspomaganie informatyczne funkcjonowania systemów monitoringu wizyjnego w kolejowych obiektach transportowych. Prace naukowe Politechniki Warszawskiej: Transport, z. 113, 2016.

14. Siergiejczyk M., Paś J., Rosiński A.: Application of closed circuit television for highway telematics. [in:] Mikulski J. (red.): Telematics in the Transport Environment: 12th International Conference on Transport Systems Telematics (TST 2012), Katowice-Ustroń, Poland, October 10–13, 2012, Selected Papers, Communications in Computer and Information Science, Vol. 329, DOI: 10.1007/978-3-642-34050-5_19.
15. Siergiejczyk M., Paś J., Rosiński A.: Evaluation of safety of highway CCTV system's maintenance process. [w:] Mikulski J. (red.): Telematics - Support for Transport: 14th International Conference on Transport Systems Telematics (TST 2014), Communications in Computer and Information Science, Vol. 471, DOI: 10.1007/978-3-662-45317-9_8.
16. Siergiejczyk M., Paś J., Rosiński A.: Reliability and maintenance analysis of CCTV systems used in rail transport. Journal of KONBiN, 2015, No. 3 (35), DOI: 10.1515/jok-2015-0047.
17. Urbančoková H., Valouch J.: Monitoring of the tests EMS information technology equipment using the CCTV system. International Journal of Circuits, Systems and Signal Processing, Vol. 9, 2015.