Journal of KONBiN 46(2018)
ISSN 1895-8281
DOI 10.2478/jok-2018-0031 ESSN 2083-4608

TEACHING METHODOLOGY OF DIAGNOSIS PROCESS ON THE EXAMPLE OF INTRUSION AND HOLD-UP ALARM SYSTEM

METODYKA NAUCZANIA PROCESU DIAGNOZOWANIA NA PRZYKŁADZIE SYSTEMU SYGNALIZACJI WŁAMANIA I NAPADU

Jacek Paś

Military University of Technology, Faculty of Electronics
Wojskowa Akademia Techniczna, Wydział Elektroniki

***Abstract**: The article presents a teaching methodology of the diagnosis process of the technical and functional condition of intrusion and hold-up alarm system (SSWiN). Laboratory model SSWiN is a representation of a real intrusion and hold-up system. The lecturer has the opportunity to ask a dozen different independent damages. The aim of the laboratory exercises is to familiarize students with the methodology and structure of the diagnosis SSWiN.*

***Keywords:** detector, intrusion and hold-up alarm system, diagnosis*

***Streszczenie:** W artykule przedstawiono metodę nauczania procesu diagnozowania stanu technicznego i funkcjonalnego systemu sygnalizacji włamania i napadu (SSWiN). Laboratoryjny model SSWiN jest odwzorowaniem rzeczywistego układu sygnalizacji włamania i napadu. Prowadzący zajęcia ma możliwość zadawania kilkunastu różnych niezależnych uszkodzeń. Celem ćwiczenia laboratoryjnego jest zapoznanie studentów z metodyką i strukturą procesu diagnozowania SSWiN.*

***Słowa kluczowe:** czujka, system sygnalizacji włamania i napadu, diagnozowanie*

TEACHING METHODOLOGY OF DIAGNOSIS PROCESS ON THE EXAMPLE OF INTRUSION AND HOLD-UP ALARM SYSTEM

1. General characteristics of burglary and assault signaling systems

Intrusion detection system is generally a set of devices used to secure an object against intruder or other undesirable events and threats [5,8,15]. Apart from Fire Alarm Systems (SSPs), these systems belong to the group called Alarm Systems (SA), which belong to a wider group of Electronic Security Systems (ESB). The extensive Intrusion Detection Systems most often contain the following components:

- mainboards and LCD keypads or partition keypads (keypads),
- detectors, signaling devices (e.g. optical-acoustic) and code locks,
- expanders: enter and exit including addressable addresses and speech,
- synoptic boards,
- expanders of contactless card readers or "dallas pellets" (transponders).

Depending on the manufacturer of SSWiN, individual market solutions may differ, due to the integration of some elements with the motherboard. Connections between particular elements mentioned in the SSWiN can be divided into connections [5,8,12,14]:

- wired (including fiber optic);
- wireless using coded modulation - an analog or digital electromagnetic field with a strictly defined frequency, e.g. 433, 866 MHz - Figure 1.

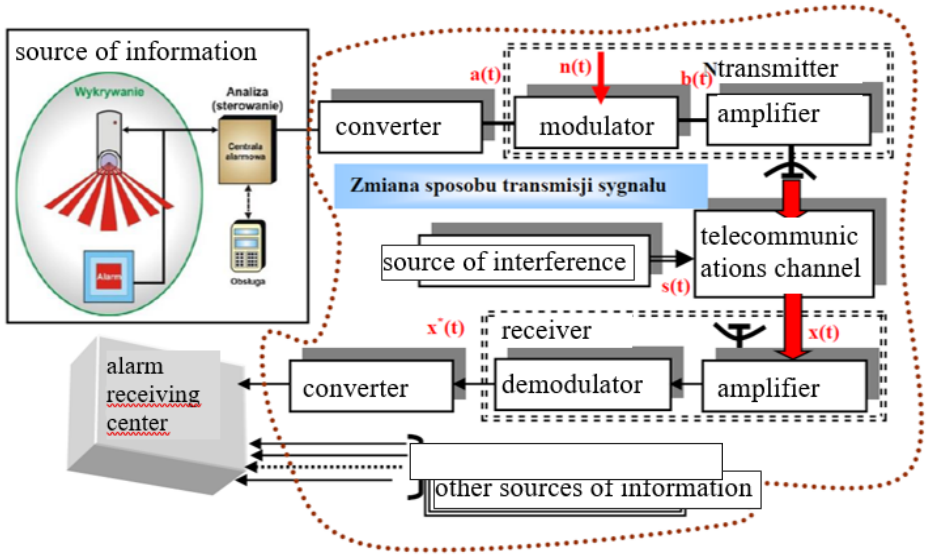


Fig. 1 Simplified diagram of the transceiver device in the electronic wireless security system, a(t) - modulating signal, x(t) - reconstructed modulating signal in the demodulator, n(t) - interfering signal, b(t) - signal modulated high frequency after the modulator, s(t) - source of interference in the propagation channel of the electromagnetic wave*

The design, implementation and performance of periodic inspections of the Burglary and Robbery System for a large and extensive facility such as the following facilities: airport, transport base, railway station, etc. requires a lot of technical knowledge, experience and significant financial outlays. There are objects, so-called extensive, which for economic reasons (e.g. length of power lines, signal lines, etc.), as well as logistic (e.g, the lack of possibility to interfere with the appearance of sacral objects, making connections using underground tunnels) can be protected only by using the integration of smaller systems.
Electronic security systems are complex technical objects, because they carry out many different functions like monitoring the object, auto diagnosising of system components (detectors, cameras, power lines, I / O devices, reserve power sources, etc.), alarming about the threat, initiating anti-sabotage activities including anti-destructive ones. In electronic security systems, the following conditions can be distinguished:
- fitness ε^Z - all system functions are correctly implemented;
- disability status ε^N - all functions are performed incorrectly;
- partial fitness of the ε^{NZ} protection system - some functions of the system are correctly implemented [2,3,4,6].

In general, for technical and operational reasons, electronic security systems can be divided into two classes:

I. Electronic Simple Security System – ESB_P

These systems perform one function. Usually damage to any element (detector, control panel) prevents the correct operation of the entire ESB_P. The reliability of indicators are determined by:
- quality of designing and execution - the main R_O depends on this, mainly due to the uncorruptability of construction (we cannot be sure that the ESB_P is safe when it is started to use);
- slow (and in principle irreversible) physical changes taking place in ESB_P components (e.g. slow change in sensitivity of the sensor) - these processes are characterized by the so-called parametric reliability R_N;
- stepwise (sudden, random) changes in the physical properties of ESB_P elements (e.g. break in the wire transmitting the signal from the sensor to the control panel) - this phenomenon is characterized by the so-called catastrophic failure of R_K;
- correct operation, i.e. service, control, power, use - these processes shape the so-called operational reliability of the ESB_P R_E.

All these reliability indicators are ESB_P time and point functions

.

II. Electronic Security System submitted – ESB_Z

In principle, all currently installed ESB can be included in this group, because they carry out many different functions in building facilities and in extensive transport areas.

The following ESB_Z statuses can be distinguished:

- state of fitness (all functions assumed and designed - alarming, supervision, coding, blocking, etc. ESB_Z are implemented correctly);
- disability status (all ESB_Z functions assumed and designed are implemented incorrectly) [2,4,8];
- partial airworthiness (only some of the ESB_Z functions assumed and designed are implemented correctly).

ESB_Z are created from simple systems, so damage to one or more of them does not cause total system damage, but reduces its efficiency. ESBs are renewable objects, i.e. they are repairable in the event of damage (e.g. it is possible to replace a damaged detector). Repair may disrupt the implementation of ESB scheduled tasks (e.g. replacement of the detector requires turning off the entire signal path or transmission bus) [1, 5,10,11].

2. Diagnosing the signaling and burglary system

Complex ESBs are equipped with self-monitoring systems, i.e. systems for automatic monitoring of technical condition. This monitoring consists in permanent diagnosis of individual system elements (i.e. detectors, elements of the control panel, cameras, monitors, optical signals, etc.). The control panel generates reference signals that stimulate individual components of the system [4,8,9]. These elements generate the standard response signals which are processed in the alarm control panel to diagnostic information of the type: fit system – unfit system. The task of constructors is to determine at the stage of constructing a system of permissible tolerances of forcing signals and responses [4,8,10,13]. Information about the system status can be in visual or acoustic form and can be presented in the alarm control panel or in a remote alarm center. The element responsible for the implementation of the security system surveillance algorithm is the microprocessor of the central alarm control center controller, which performs a programmed sequence of diagnostic actions. Stimulated by diagnostic signals, generated by the self-monitoring system, the alarm detectors "respond" with pulses of the assumed sequence, e.g. time. This means the appearance of response pulses (e.g, sequences of zeros and ones) corresponding to the condition of individual detectors in the security system detection line at a given time.

Each detector built-in in the detection line has its own unique address (assignment of the same address for two detectors causes CA inability to signal). Information on the states of fitness or detector's lessness appears on the LCD display or in the visual signaling module. In the event of an alarm condition such as fire alarm occurring while checking the technical condition of the system, the test procedure is interrupted (the alarm signal has a higher priority than the diagnostic signals) and the information and therapeutic actions are started.

3. Stand for diagnosing the burglary signaling system

The intrusion alarm system is intended to detect and alert the intruder in order to take appropriate action. The general operating principle "Intrusion signaling device" will be discussed on the basis of the MATRIX Alarm Control Panel. The device includes the following basic elements - alarm control panel with power supply system and seizure detectors. Smoke detectors can also be connected to the MATRIX alarm panel. The following types of detectors can be connected to the MATRIX control panel:

– detectors with connected limit switch - NC contacts (contacts normally closed at the door);
– detectors with connected limit switch - NO contacts (contacts normally open at the door);
– detectors with connected reed contact - NC contacts [4,8,10,15].

One or two resistors can be connected to the detectors. The detectors can be equipped with an additional switch with the inscription "TAMPER" used to check the operation of the burglary signaling device.

Lines without resistors, with NC contacts, are normally closed lines that distinguish only two states:

– closing the door - closing the limit switch contacts (short circuit - $R_L = 0\ \Omega$) - this is the Monitoring status;
– door opening - contact opening (open circuit - $R_L = \infty$) - this is the Alarm status. Usually one detector or reed switch is placed on such lines.

EOL lines with a single resistor, with NC contacts, are lines that distinguish three states:

– closing the door - closing the limit switch contacts (short circuit - $R_L = 4.7\ k\Omega$) - this is the Monitoring status;
– door opening - contact opening (open circuit - $R_L = \infty$) - this is the Alarm status;
– short-circuit of the line wires between the detector and the control panel ($R_L = 0\ \Omega$) - this is the sabotage status.

If the line consists of several detectors, in the case of a burglary into one room, the "Alarm control panel" signals "Alarm", but it does not distinguish the room number (detector) – fig. 2.

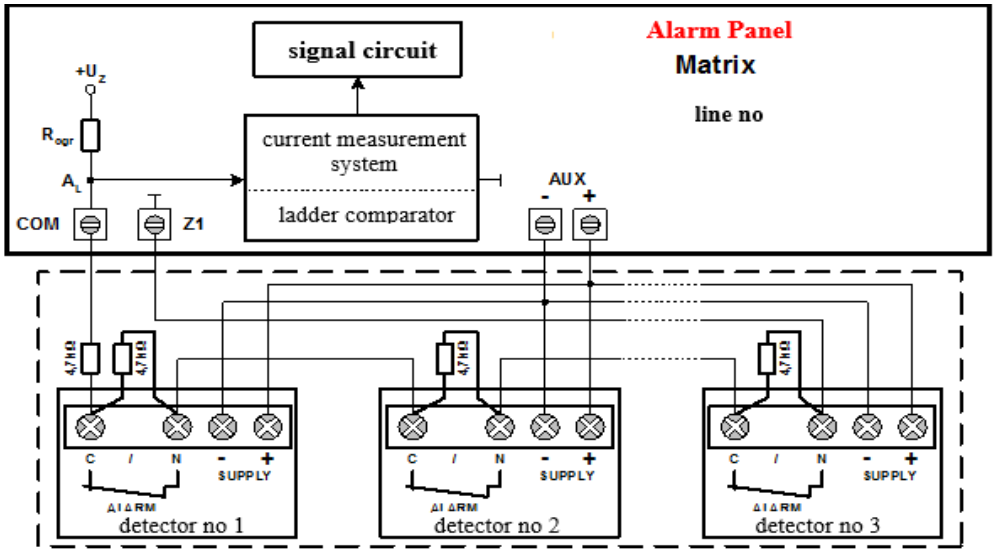


Fig. 2 Connection of several detectors in one line to the alarm control panel - DEOL line

The alarm panel is equipped for each line in:
– limiting resistor - R_{ogr};
– line current measurement system;
– signaling system.

4. Description of the laboratory stand to diagnose the condition of SSWiN

Figure 3 shows the front panel view of the station. Control panel allows the the measurement:
– models of DEOL detectors and the alarm control panel, including switches and switches controlling the work of the station;
– control resistor, measuring sockets and signaling diodes.

Measurement sockets enable to measure voltage at selected points of the line. Circuit breakers with the word "Damage" ($U_1 \div U_{14}$) are used to inflict damage. The diodes are used to signal the operating status of the "Intrusion Detection System". Voltage setting system at points A_{L1} and A_{L2}, to determine the voltage values at which the respective signaling diodes are lit.

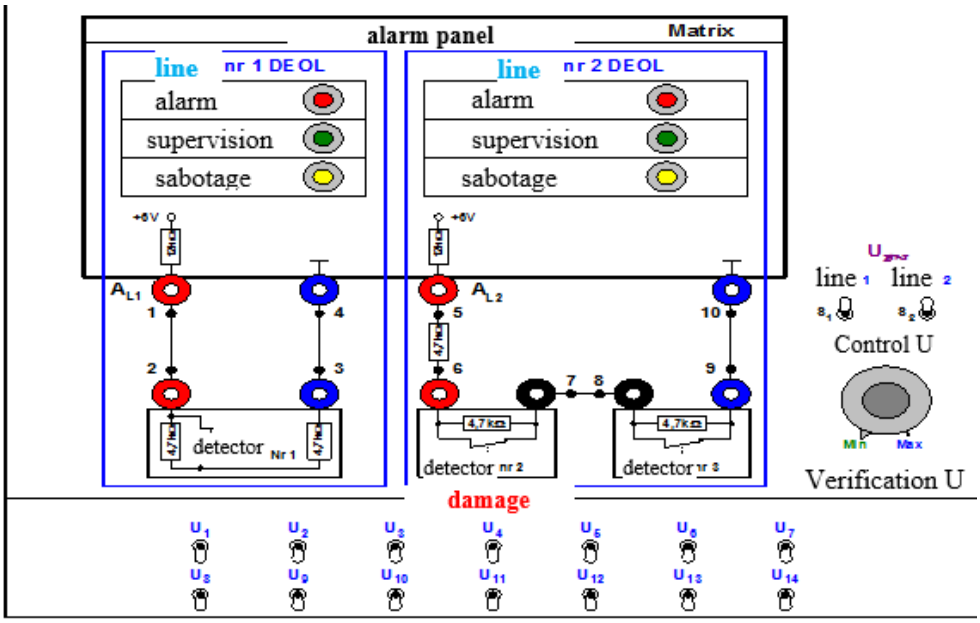


Fig. 3 View of the faceplate of the station for diagnosing the system

Below is described the methodology of diagnosing the "Intrusion Alarm System" using a voltmeter on the example of the DEOL line, which consists of 3 detectors (this line does not have such a position) – fig. 5. After switching on one of the "Damage" switches, the "Intrusion alarm system" will be damaged. A sign of the failure of the system is the yellow diode signaling "Sabotage" or the red diode signaling "Alarm" (burglary).

Diagnosis of the system in the event of an "Alarm" red diode:

– If the red diode "Alarm" lights up and the voltage at the AL point of the given line falls within the "Alarm" status range, it means that a burglary occurred or the detector was damaged (opening the contacts of the detector switch at the door). In the exercise, we assume that there was no break-in.
– During the diagnostics of the detectors, to measure whether the contacts of the circuit breaker are shorted or open, the output voltage and the detector input should be measured. If these voltages are equal, the detector switch contacts are closed.
– If the red diode "Alarm" lights up and the voltage at the A_L point of the given line falls within the scope of the "Supervision" status, it means that the "Voltage measurement system" has been damaged. In this case, please check the "Voltage measurement system" with the breaker switch on the specified fault.

In order to diagnose the system, the necessary number of steps must be performed.

1st diagnostic step.

After activating the fault switch, eg U_7 in table 1 note:
– Symptom of O_i damage.
– Assumed hypothesis.
– The decision to make the check.
– The result of the check - the next symptom of O_i.
– A diagnosis made.

Symbols used in the table: U_6 - voltage in point 6; UPN - voltage monitoring system – fig. 4.

The next diagnostic step - if no diagnosis was made in the previous step, should be performed. The methodology for diagnosing several variants of DEOL line 3 defects is presented below. Figure 4 shows the scheme of "Intrusion Alarm System" with the DEOL line, which consists of 3 detectors.

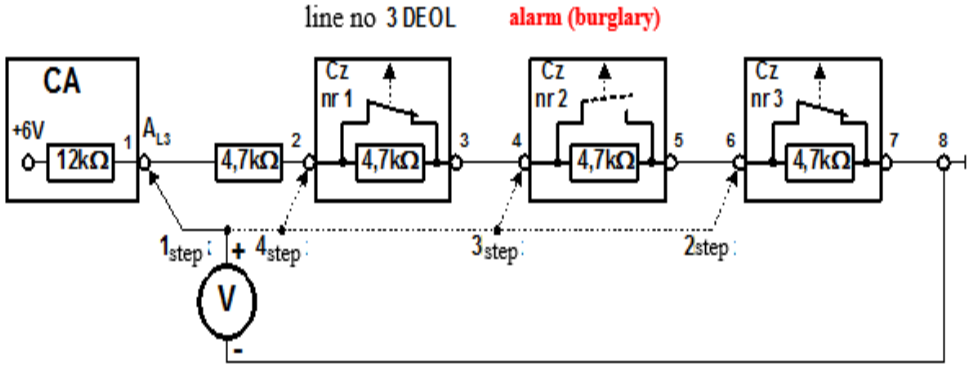


Fig. 4 The SSWiN diagram with the DEOL line, which consists of 3 detectors

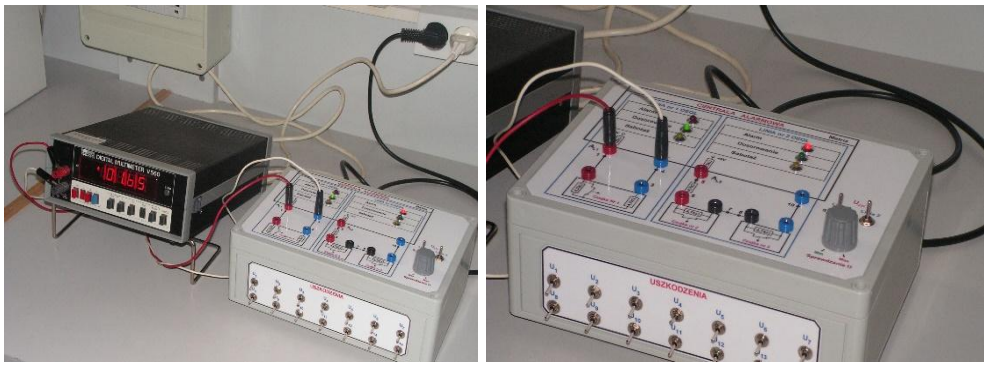


Fig. 5 View of the laboratory stand of the SSWiN system

Tab. 1 Variant 1

Damage		**Switch on, e.g. U_7**
Step 1	Symptom	O_1. The red diode "Alarm".
	Hypothesis	Damaged line no 3 DEOL.
	Check command	Measure the voltage value at the point A_{L3}.
	Result of the check, symptom	O_2 - U_{AL3} = 1,65 V.
Step 2	Hypothesis	Since the value of the measured U is within the limits of the status of "Supervision", then the hypothesis is - Defective UPN CA in line no. *3*.
	Check command	Check the UPN in line 3 with the "U_7" switch on and compare it with the voltage values in table.
	Result of the check, symptom	A_T 4. U_{MIN} of the "Alarm" state = 1.42 V. The value of this voltage is lower than the value in the system's fitness status (U_{MIN} of the "Alarm" state = 1.9 V).
Diagnosis		**Damaged voltage measurement system CA in line No. 3.**

4. Conclusions

The article presents a laboratory standpoint and laboratory exercise developed in the Department of Exploitation of Electronic Systems at WEL WAT regarding the methodology of the SSWiN diagnosis teaching process. SSW and N consist of a CA alarm control panel with two lines for supervising the status of protected rooms - DEOL lines. In the surveillance line No. 1 there is one detector with two resistors, and in the surveillance line No. 2 there are two detectors. Before the laboratory exercise, the lecturer gives the numbers of the breakers – i.e. the specified damage. After completing the process of diagnosing one damage, turn on the next switch, inflicting next damage. It was assumed that only one disability exists in the diagnosed system at a given moment. Active learning, which can be included, e.g. laboratory exercise has many advantages, because it engages different senses of the student, which allows for better understanding and remembering the content taught. The students generally remember only 10% of what they hear (e.g. lecture); 40% of what they are talking about (e.g. discussion, accounting exercises), but as much as 90% of what they do (e.g. laboratory exercises, staging). The constructed laboratory models correspond to real systems installed and operated in security systems [3,5,8,17,18]. Using the functional diagram of SSWiN, students determine the type and cause of damage, and also consolidate knowledge in the field of general principles of diagnosis - and in particular diagnostic inference based on the observed symptoms of the condition of the diagnosed system.

5. Literature

[1] Kołowrocki K., Soszyńska-Budny J.: *Reliability and safety of complex technical systems and processes.* Springer, London 2011
[2] Dyduch J., Paś J., Rosiński A.: *Podstawy eksploatacji transportowych systemów elektronicznych*. Wydawnictwo Politechniki Radomskiej, Radom 2011.
[3] Dąbrowski T., Paś J., Olchowik W., Rosiński A., Wiśnios M.: *Podstawy eksploatacji systemów*, *Laboratorium*. WAT Warszawa 2014
[4] Paś J., Rosiński A., Wiśnios M., Majda-Zdancewicz E., Łukasiak J.: *Electronic security systems. Introduction to the laboratory,* ISBN 978-83-7938-150-0. Military University of Technology, Warsaw 2018.
[5] Paś J.: *Eksploatacja elektronicznych systemów transportowych*. Uniwersytet Technologiczno - Humanistyczny, Radom 2015.
[6] Żółtowski B., Niziński S.*: Modelowanie procesów eksploatacji maszyn*, AT-R 2002
[7] Laskowski, D., Łubkowski, P., Pawlak, E., Stańczyk, P.: *Anthropotechnical systems reliability*. In: the monograph „Safety and Reliability: Methodology and Applications - Proceedings of the European Safety and Reliability Conference ESREL 2014", editors: Nowakowski T., Młyńczak M., Jodejko-Pietruczuk A. &Werbińska–Wojciechowska S. CRC Press/Balkema, London, 2015, pp. 399-407.
[8] Rosiński A.: *Modelowanie procesu eksploatacji systemów telematyki transportu*. Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2015.
[9] Siergiejczyk M., Paś J., Rosiński A.: *Train call recorder and electromagnetic interference*. Diagnostyka 2015, vol. 16, no. 1, pp. 19-22.
[10] Siergiejczyk M., Rosiński A., Paś J.: *Analysis of unintended electromagnetic fields generated by safety system control panels*. Diagnostyka 2016, vol. 17, no. 3, pp. 35-40.
[11] Stawowy M., Dziula P.: *Comparison of uncertainty multilayer models of impact of teleinformation devices reliability on information quality*. In: "Proceedings of the European Safety and Reliability Conference ESREL 2015", editors: L. Podofillini, B. Sudret, B. Stojadinovic, E. Zio, W. Kröger. CRC Press/Balkema, 2015. pp. 2685-2691.
[12] Paś J., Dąbrowski T., Wiśnios M.: *Teaching methodology of the diagnosing process on the example of the fire alarm system*, DOI 10.1515jok-2017-0014, Journal of KONBiN 41(2017), s. 277-308.
[13] Siergiejczyk M., Paś J., Rosiński A.: Issue *of reliability–exploitation evaluation of electronic transport systems used in the railway environment with consideration of electromagnetic interference*, IET Intelligent Transport Systems, ISSN 1751-956X, doi: 10.1049/iet-its.2015.0183, Source: Volume 10, Issue 9, November 2016, pp. 587 – 593.

[14] Siergiejczyk M., Paś J., Rosiński A.: *Issue of reliability–exploitation evaluation of electronic transport systems used in the railway environment with consideration of electromagnetic interference*, IET Intelligent Transport Systems, ISSN 1751-956X, doi: 10.1049/iet-its.2015.0183, Source: Volume 10, Issue 9, November 2016, s. 587 – 593.
[15] Siergiejczyk M., Rosiński A., Paś J.: *Analysis of unintended electromagnetic fields generated by safety system control panels*, DIAGNOSTYKA, 2016, Vol. 17, No. 3, ISSN 1641-6414, e-ISSN 2449-5220, s. 35-46.
[16] Paś J., Choromański W.: *Results of measurement and determination of threshold electric field component for transport security systems*, Archives of Transport Systems Telematics, Volume 8, Issue 1, February 2015, s. 24-29, ISSN 1899-8208.
[17] Siergiejczyk M., Rosiński A., Paś J.,: *Analysis of unintended electromagnetic fields generated by safety system control panels*, DIAGNOSTYKA, 2016, Vol. 17, No. 3, ISSN 1641-6414, pp. 35-46.
[18] Paś J.: *Analysis of exploitation access control system selected object*, Przegląd Elektrotechniczny, vol 2015, no 10, ISSN 0033-2097, R. 91, pp. 219 – 224.

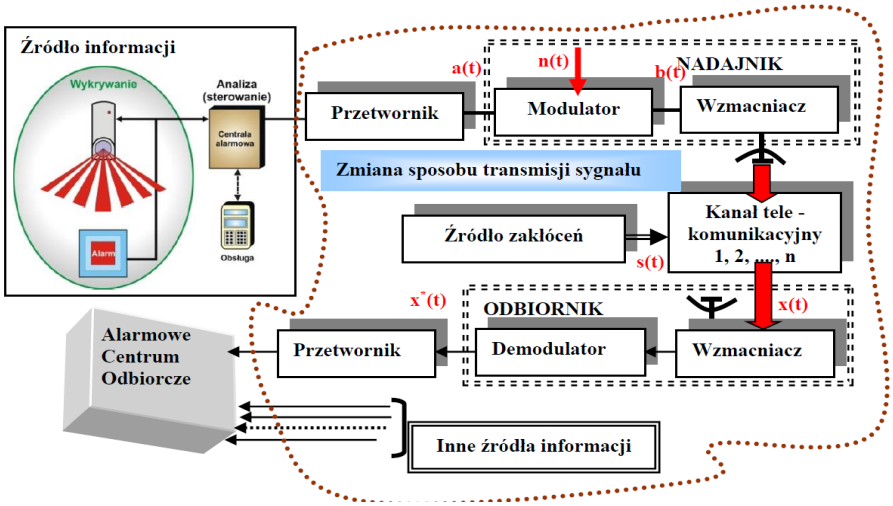
Jacek Paś Ph.D., D.Sc., Eng., professor *of Military University of Technology – Division Electronic Systems Exploitations Manager, scientific interests (electromagnetic compatibility, analog circuits, reliability, low frequency noise, exploitation, diagnostics, projecting) are problems connected with comprehended wide of the safety both for stationary as well as for movable objects. He is the author of three books and more than 200 articles. His research interests include also environmental studies of electromagnetic the range at low frequencies at (electrosmog).*

METODYKA NAUCZANIA PROCESU DIAGNOZOWANIA NA PRZYKŁADZIE SYSTEMU SYGNALIZACJI WŁAMANIA I NAPADU

1. Ogólna charakterystyka systemów sygnalizacji włamania i napadu

System sygnalizacji włamania i napadu stanowi najczęściej zespół urządzeń służących zabezpieczeniu danego obiektu przed intruzem lub innymi niepożądanymi zdarzeniami i zagrożeniami [5,8,15]. Systemy te obok Systemów Sygnalizacji Pożarowej (SSP) należą do grupy określanej jako Systemy Alarmowe (SA) wchodzące z kolei do szerszej grupy Elektronicznych Systemów Bezpieczeństwa (ESB). Rozbudowane Systemy Sygnalizacji Włamania i Napadu zawierają najczęściej następujące części składowe:
– płyty główne i manipulatory LCD lub klawiatury strefowe (manipulatory),
– czujki, sygnalizatory (np. optyczno-akustyczne) i zamki szyfrowe,
– ekspandery: wejść i wyjść w tym wejść adresowalnych i mowy,
– tablice synoptyczne,
– ekspandery czytników kart zbliżeniowych lub „pastylek dallas" (transpondery).

W zależności od producenta SSWiN poszczególne rozwiązania rynkowe mogą się różnić, a to za sprawą zintegrowania niektórych elementów z płytą główną. Połączenia pomiędzy poszczególnymi w/w elementami wchodzącymi w skład SSWiN, można podzielić na połączenia [5,8,12,14]:
– przewodowe (w tym światłowodowe);
– bezprzewodowe z wykorzystaniem modulacji kodowanej - analogowej lub cyfrowej pola elektromagnetycznego o ściśle określonej częstotliwości, np. 433, 866 MHz – rys. 1.



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

Zaprojektowanie, realizacja i późniejsze wykonywanie przeglądów okresowych Systemu Sygnalizacji Włamania i Napadu dla dużego i rozległego obiektu jakim mogą być następujące obiekty: lotnisko, baza transportowa, dworzec kolejowy, itd. wymaga dużej wiedzy technicznej, doświadczenia, oraz znacznych nakładów finansowych. Istnieją obiekty, tzw. rozległe które ze względów ekonomicznych (np. długość linii zasilających, sygnałowych, itd.), a także logistycznych (np. brak możliwości do ingerencji wygląd obiektów np. sakralnych, wykonania połączeń za pomocą tuneli podziemnych) można zabezpieczyć tylko poprzez zastosowanie integracji mniejszych systemów. – rys. 2.

W elektronicznych systemach bezpieczeństwa można wyróżnić następujące stany:

– stan zdatności ε^{Z} – poprawnie realizowane są wszystkie funkcje systemu;
– stan niezdatności ε^{N} – wszystkie funkcje są realizowane nieprawidłowo;
– częściowa zdatność sytemu ochrony ε^{ZN} – poprawnie realizowane są niektóre funkcje systemu [2,3,4,6].

Ogólnie ze względów technicznych i eksploatacyjnych elektroniczne systemy bezpieczeństwa można podzielić na dwie klasy:

I. Elektroniczny System Bezpieczeństwa prosty – ESB_P

Systemy te realizują jedną funkcję. Zwykle uszkodzenie dowolnego elementu (czujki, centrali) uniemożliwia poprawną pracę całego **ESB_P**.

O wskaźnikach niezawodności takiego obiektu decydują:

– jakość projektowania i wykonania – od tego głównie zależy nieuszkadzalność początkowa R_O zwana często nieuszkadzalnością konstrukcyjną (rozpoczynając użytkowanie możemy nie mieć pewności, że ESB_P jest zdatny);
– powolne (i w zasadzie nieodwracalne) zmiany fizyczne zachodzące w elementach składowych ESB_P (np. powolna zmiana czułości czujnika) – procesy te charakteryzują się tzw. nieuszkadzalność parametryczna R_N;
– skokowe (nagłe, losowe) zmiany właściwości fizycznych elementów ESB_P (np. uszkodzenie typu przerwa w przewodzie transmitującym sygnał z czujnika do centrali alarmowej) – zjawiska tego typu charakteryzuje tzw. nieuszkadzalność katastroficzna R_K;
– poprawność eksploatacji tj. obsługi, sterowania, zasilania, użytkowania – procesy te kształtują tzw. nieuszkadzalność eksploatacyjną R_E ESB_P.

Wszystkie te wskaźniki niezawodności są funkcjami czasu oraz punktu pracy ESBP.

II. Elektroniczny System Bezpieczeństwa złożony – ESB_Z

W zasadzie wszystkie obecnie instalowane ESB można zaliczyć do tej grupy, gdyż realizują wiele różnych funkcji w obiektach budowlanych i na rozległych terenach transportowych.

Można wyróżnić następujące stany użytkowania ESB_Z :
- stan zdatności (wszystkie założone i zaprojektowane funkcje – alarmowanie, dozorowanie, kodowanie, blokowanie, itd. ESB_Z są realizowane poprawnie);
- stan niezdatności (wszystkie założone i zaprojektowane funkcje ESB_Z są realizowane niepoprawnie) [2,4,8];
- stan częściowej zdatności (tylko niektóre założone i zaprojektowane funkcje ESB_Z są realizowane poprawnie).

ESB_Z tworzone są z systemów prostych, zatem uszkodzenie jednego lub kilku z nich nie powoduje całkowitego uszkodzenia systemu, lecz zmniejsza jego efektywność działania. **ESB** są obiektami odnawialnymi, tzn. w przypadku uszkodzenia są naprawialne (np. możliwa jest wymiana uszkodzonej czujki). Naprawa może zakłócić realizację planowych zadań **ESB** (np. wymiana czujki wymaga wyłączenia całego toru sygnałowego lub magistrali transmisyjnej) [1,5,10,11].

2. Diagnozowanie systemu sygnalizacji i włamania

Złożone ESB wyposażane są w układy samokontroli tj. układy automatycznego dozorowania stanu technicznego. Dozorowanie to polega na permanentnym diagnozowaniu poszczególnych elementów systemu (tj. czujek, elementów centrali alarmowej, kamer, monitorów, sygnalizatorów optycznych itd.). Centrala alarmowa wytwarza wzorcowe sygnały, które pobudzają poszczególne elementy składowe sytemu [4,8,9]. Elementy te generują wzorcowe sygnały odpowiedzi, które są przetwarzane w centrali alarmowej na informację diagnostyczną typu: system zdatny – niezdatny. Zadaniem konstruktorów jest określenie na etapie konstruowania systemu dopuszczalnych tolerancji sygnałów wymuszających i odpowiedzi [4,8,10,13]. Informacja o stanie systemu może mieć formę wizualną lub akustyczną i może być prezentowana w centrali alarmowej lub w oddalonym centrum alarmowym.

Elementem odpowiedzialnym za realizację algorytmu dozorowania systemu bezpieczeństwa jest mikroprocesor sterownika centralnego centrali alarmowej, który realizuje określoną programowo sekwencję działań diagnostycznych. Pobudzone sygnałami diagnostycznymi, wytworzonymi przez układ samokontroli, czujki alarmowe „odpowiadają" impulsami o założonej sekwencji np. czasowej. Oznacza to pojawienie się w określonym czasie impulsów odpowiedzi (np. sekwencji zer i jedynek) odpowiadających stanowi poszczególnych czujek w linii dozorowej systemu bezpieczeństwa. Każda czujka zabudowana w linii dozorowej posiada swój własny, unikalny adres (przypisanie tego samego adresu dla dwóch czujek powoduje sygnalizację niezdatności w CA). Informacja o stanach zdatności lub niezdatności czujek pojawia się na wyświetlaczu LCD lub w module sygnalizatorów wizualnych. W przypadku wystąpienia, podczas sprawdzania stanu technicznego systemu, stanu alarmu np. przeciwpożarowego, przerywana jest procedura testowania (sygnał alarmu posiada większy priorytet niż sygnały diagnostyczne) i uruchamiane są działania informacyjno-terapeutyczne.

3. Stanowisko do diagnozowania układu sygnalizacji włamania

Układ sygnalizacji włamania (napadu) ma na celu wykrywanie włamania oraz alarmowanie o nim w celu podjęcia odpowiednich działań. Ogólna zasada działania „Urządzenie sygnalizacji włamania" zostanie omówiona na bazie Centrali alarmowej MATRIX. W skład tego urządzenia wchodzą następujące podstawowe elementy - centrala alarmowa wraz z systemem zasilania w energię elektryczną oraz czujki napadu. Do Centrali alarmowej MATRIX mogą być także przyłączone czujki dymu. Do centrali MATRIX mogą być przyłączone następujące rodzaje czujek:

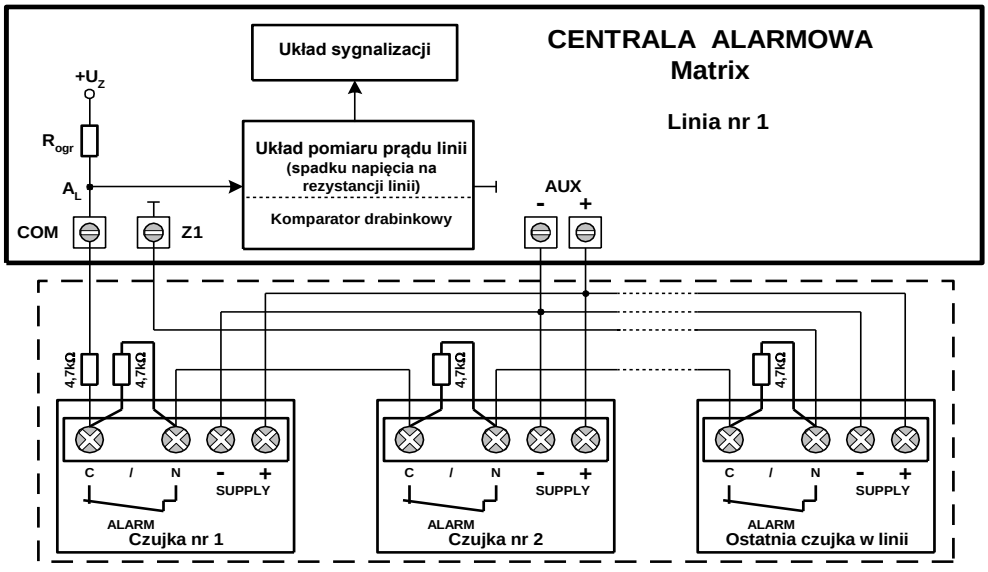
– czujki z przyłączanym wyłącznikiem krańcowym - styki NC (styki normalnie zwarte przy drzwiach zamkniętych);
– czujki z przyłączanym wyłącznikiem krańcowym - styki NO (styki normalnie rozwarte przy drzwiach zamkniętych);
– czujki z przyłączanym kontaktronem - styki NC [4,8,10,15].

Do czujek mogą być przyłączone pojedyncze lub podwójne rezystory. Czujki mogą być wyposażone w dodatkowy wyłącznik z napisem „TAMPER" służący do sprawdzenia działania urządzenie sygnalizacji włamania.

Linie bez rezystorów, ze stykami NC, są to linie normalnie zwarte, które rozróżniają tylko dwa stany:

– zamknięcie drzwi – zwarcie styków wyłącznika krańcowego (obwód zwarty - $R_L = 0\ \Omega$) – jest to stan Dozorowania – rys. 2;
– otwarcie drzwi - rozwarcie styków (obwód rozwarty – $R_L = \infty$) – jest to stan Alarmu.

Na liniach takich zwykle umieszcza się jedną czujkę lub kontaktron.



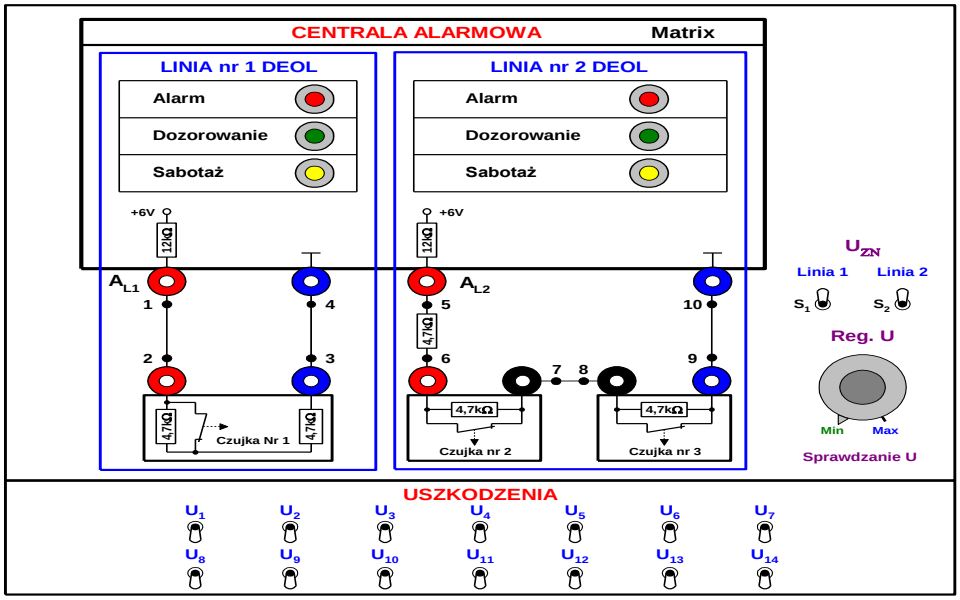
Rys. 2 Przyłączenie kilku czujek w jednej linii do centrali alarmowej – linia DEOL

Centrala alarmowa wyposażona jest dla każdej linii w:
– rezystor ograniczający – R_{ogr};
– układ pomiaru prądu linii;
– układ sygnalizacji.

4. Opis stanowiska laboratoryjnego do diagnozowania stanu SSWiN

Na rysunku 3 przedstawiono widok płyty czołowej stanowiska.
Pulpit sterująco - pomiarowy zawiera:
– modele czujek DEOL i centrali alarmowej w tym wyłączniki i przełączniki sterujące pracą stanowiska;
– rezystor regulacyjny, gniazda pomiarowe i diody sygnalizacyjne.

Gniazda pomiarowe umożliwiają pomiar napięcia w wybranych punktach linii. Wyłączniki z napisem „Uszkodzenia" (U1 ÷ U14) służą do zadawania uszkodzeń. Diody służą do sygnalizacji stanu pracy „Układu sygnalizacji włamania". Układ zadawania napięcia w punktach A_{L1} i A_{L2}, w celu określenia wartości napięć, przy których zapalają się odpowiednie diody sygnalizacyjne – rys. 5.



Rys. 3 Widok płyty czołowej stanowiska do diagnozowania układu

Poniżej została opisana metodyka diagnozowania „Układu sygnalizacji włamania" za pomocą woltomierza na przykładzie linii DEOL, która składa się z 3 czujek (takiej linii stanowisko nie posiada). Po włączeniu jednego z wyłączników „Uszkodzenia" nastąpi uszkodzenie „Układu sygnalizacji włamania".

Objawem niezdatności układu jest zapalenie żółtej diody sygnalizującej „Sabotaż" lub diody czerwonej sygnalizującej „Alarm" (włamanie). Diagnozowanie układu w przypadku zapalenia się diody czerwonej „Alarm":

– Jeżeli zapali się dioda czerwona „Alarm", a napięcie w punkcie A_L danej linii mieści się w zakresie stanu „Alarm", to oznacza że nastąpiło włamanie, lub nastąpiło uszkodzenie czujki (rozwarcie styków wyłącznika czujki przy drzwiach zamkniętych). W ćwiczeniu zakładamy, że nie nastąpiło włamanie.
– W czasie diagnozowania czujek, aby stwierdzić czy styki wyłącznika są zwarte lub rozwarte, należy pomierzyć napięcie na wyjściu i wejściu czujki. Jeżeli te napięcia są sobie równe, to styki wyłącznika czujki są zwarte.
– Jeżeli zapali się dioda czerwona „Alarm", a napięcie w punkcie A_L danej linii mieści się w zakresie stanu „Dozorowanie", to oznacza że nastąpiło uszkodzenie „Układu pomiaru napięcia". W takim przypadku należy sprawdzić „Układ pomiaru napięcia" przy włączonym wyłączniku zadanego uszkodzenia.

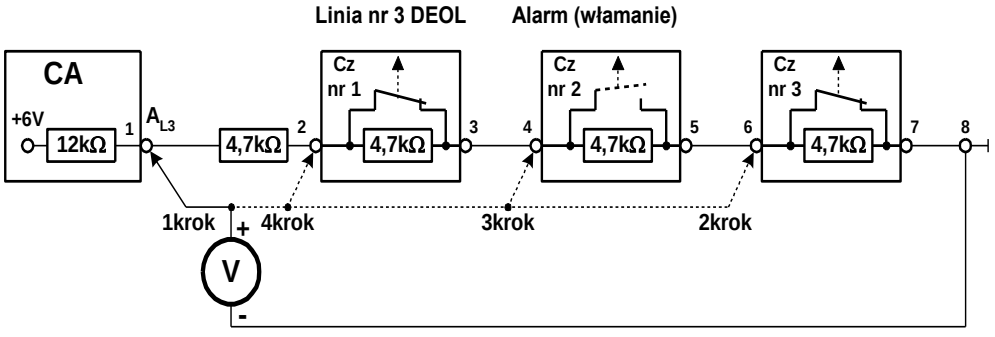
Aby przeprowadzić diagnozowanie układu należy wykonać niezbędną ilość kroków.

1-szy krok diagnozowania. Po włączeniu wyłącznika uszkodzenia np. U_7 w tabeli 1, zanotować:

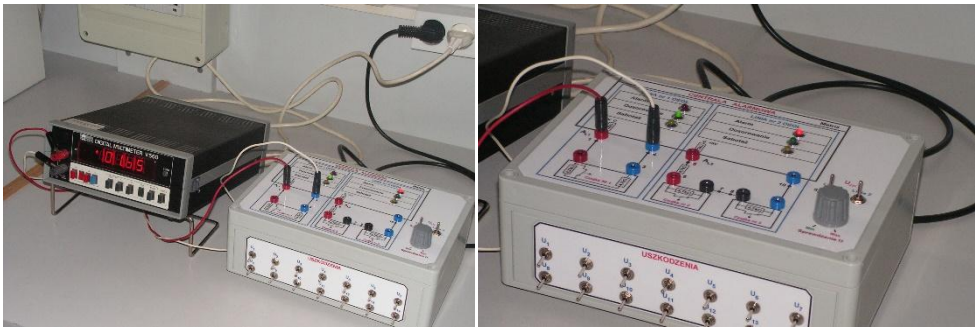
– Objaw uszkodzenia O_i.
– Postawioną hipotezę.
– Podjętą decyzję, jakie należy wykonać sprawdzenie.
– Wynik wykonanego sprawdzenia – kolejny objaw O_i.
– Postawioną diagnozę.

Oznaczenia użyte w tabeli: U_6 – napięcie w punkcie 6; UPN – układ pomiaru napięcia Centrali alarmowej.

Kolejny krok diagnozowania - jeżeli w poprzednim kroku nie została postawiona diagnoza, to należy wykonać następne kroki diagnostyczne. Poniżej przedstawiono metodykę diagnozowania dla kilku wariantów uszkodzeń linii nr 3 DEOL. Na rysunku 4 przedstawiono schemat „Układu sygnalizacji włamania" z linią DEOL, która składa się z 3 czujek.



Rys. 4 Schemat SSWiN z linią DEOL, która składa się z 3 czujek



Rys. 5 Widok stanowiska laboratoryjnego systemu SSWiN

Tab. 1 Wariant 1

Zadane uszkodzenie		Włączony wyłącznik np. U_7
Krok 1	Objaw	O_1. Świeci dioda czerwona „Alarm”.
	Hipoteza	Uszkodzona linia nr 3 DEOL.
	Polecenie sprawdzenia	Pomierzyć wartość napięcia w punkcie A_{L3}.
	Wynik sprawdzenia, objaw	O_2 - U_{AL3} = 1,65 V.
Krok 2	Hipoteza	Ponieważ wartość pomierzonego U mieści się w granicach napięć stanu „Dozorowanie” (tab. 2), to hipoteza brzmi – *Uszkodzony UPN CA w linii nr 3.*
	Polecenie sprawdzenia	Sprawdzić UPN w linii nr 3 przy włączonym wyłączniku „U_7” i porównać go z wartościami napięć zawartymi w tabeli 2.
	Wynik sprawdzenia Objaw	O_4. U_{MIN} stanu „Alarm” = 1,42 V. Wartość tego napięcia jest mniejsza od wartości w stanie zdatności układu (tabela 2.2 - U_{MIN} stanu „Alarm” = 1,9 V).
Diagnoza		Uszkodzony układ pomiaru napięcia CA w linii nr 3.

4. Wnioski

W artykule przedstawiono opracowane w Zakładzie Eksploatacji Systemów Elektronicznych WEL WAT stanowisko i ćwiczenie laboratoryjne dotyczące metodyki procesu nauczania diagnozowania SSWiN. SSW i N składa się z centrali alarmowej CA z dwoma liniami dozorowania stanu chronionych pomieszczeń – linie DEOL. W linii dozorowania nr 1 znajduje się jedna czujka z dwoma rezystorami, a w linii dozorowania nr 2 znajdują się dwie czujki. Przed rozpoczęciem ćwiczenia laboratoryjnego wykładowca podaje numery wyłączników – tj. określone uszkodzenie.

Po przeprowadzeniu procesu diagnozowania jednego uszkodzenia, należy włączyć następny wyłącznik, zadając kolejne uszkodzenie. Założono, że w układzie diagnozowanym istnieje w danej chwili tylko jedna niezdatność. Aktywne uczenie, do których można zaliczyć, np. ćwiczenie laboratoryjne ma wiele zalet, bowiem angażuje różne zmysły ucznia, co pozwala na lepsze zrozumienie i zapamiętanie nauczanych treści. Uczący się generalnie pamiętają tyko 10% tego, co słyszą (np. wykład); 40% tego, o czym rozmawiają (np. dyskusja, ćwiczenia rachunkowe), ale aż 90% tego, co robią (np. ćwiczenia laboratoryjne, inscenizacja). Zbudowane modele laboratoryjne odpowiadają rzeczywistym układom instalowanym i eksploatowanym w systemach bezpieczeństwa [3,5,8,17,18]. Wykorzystując schemat funkcjonalny SSWiN studenci określają rodzaj i przyczynę uszkodzenia a ponadto utrwalają wiedzę w zakresie ogólnych zasad diagnozowania - a zwłaszcza wnioskowania diagnostycznego na podstawie zaobserwowanych objawów stanu diagnozowanego układu.

5. Literatura

[1] Kołowrocki K., Soszyńska-Budny J.: *Reliability and safety of complex technical systems and processes.* Springer, London 2011

[2] Dyduch J., Paś J., Rosiński A.: *Podstawy eksploatacji transportowych systemów elektronicznych.* Wydawnictwo Politechniki Radomskiej, Radom 2011.

[3] Dąbrowski T., Paś J., Olchowik W., Rosiński A., Wiśnios M.: *Podstawy eksploatacji systemów, Laboratorium.* WAT Warszawa 2014

[4] Paś J., Rosiński A., Wiśnios M., Majda-Zdancewicz E., Łukasiak J.: „Electronic security systems. Introduction to the laboratory". ISBN 978-83-7938-150-0. Military University of Technology, Warsaw 2018.

[5] Paś J.: *Eksploatacja elektronicznych systemów transportowych*. Uniwersytet Technologiczno - Humanistyczny, Radom 2015.

[6] Żółtowski B., Niziński S.*: Modelowanie procesów eksploatacji maszyn*, AT-R 2002

[7] Laskowski, D., Łubkowski, P., Pawlak, E., Stańczyk, P.: *Anthropotechnical systems reliability*. In: the monograph „Safety and Reliability: Methodology and Applications - Proceedings of the European Safety and Reliability Conference ESREL 2014", editors: Nowakowski T., Młyńczak M., Jodejko-Pietruczuk A. &Werbińska–Wojciechowska S. CRC Press/Balkema, London, 2015, pp. 399-407.

[8] Rosiński A.: *Modelowanie procesu eksploatacji systemów telematyki transportu*. Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2015.

[9] Paś J., Rosiński A.: Selected issues regarding the reliability-operational assessment of electronic transport systems with regard to electromagnetic interference, Eksploatacja i Niezawodnosc – Maintenance and Reliability, Vol.19, No. 3, 2017 I, pp. 375-381, http://dx.doi.org/10.17531/ ein.2017.3.8., ISSN 1507-2711

[10] Siergiejczyk M., Rosiński A., Paś J.: *Analysis of unintended electromagnetic fields generated by safety system control panels*. Diagnostyka 2016, vol. 17, no. 3, pp. 35-40.
[11] Stawowy M., Dziula P.: *Comparison of uncertainty multilayer models of impact of teleinformation devices reliability on information quality*. In: "Proceedings of the European Safety and Reliability Conference ESREL 2015", editors: L. Podofillini, B. Sudret, B. Stojadinovic, E. Zio, W. Kröger. CRC Press/Balkema, 2015. pp. 2685-2691.
[12] Paś J., Dąbrowski T., Wiśnios M.: *Teaching methodology of the diagnosing process on the example of the fire alarm system*, DOI 10.1515jok-2017-0014, Journal of KONBiN 41(2017), s. 277-308.
[13] Siergiejczyk M., Paś J., Rosiński A.: Issue of reliability–exploitation evaluation of electronic transport systems used in the railway environment with consideration of electromagnetic interference, IET Intelligent Transport Systems, ISSN 1751-956X, doi: 10.1049/iet-its.2015.0183, www.ietdl.org, The Institution of Engineering and Technology 2016, Volume 10, Issue 9, pp. 587 – 593
[14] Siergiejczyk M., Paś J., Rosiński A.: *Issue of reliability–exploitation evaluation of electronic transport systems used in the railway environment with consideration of electromagnetic interference*, IET Intelligent Transport Systems, ISSN 1751-956X, doi: 10.1049/iet-its.2015.0183, Source: Volume 10, Issue 9, November 2016, s. 587 – 593.
[15] Siergiejczyk M., Rosiński A., Paś J.: *Analysis of unintended electromagnetic fields generated by safety system control panels*, DIAGNOSTYKA, 2016, Vol. 17, No. 3, ISSN 1641-6414, e-ISSN 2449-5220, s. 35-46.
[16] Paś J., Choromański W.: *Results of measurement and determination of threshold electric field component for transport security systems*, Archives of Transport Systems Telematics, Volume 8, Issue 1, February 2015, s. 24-29, ISSN 1899-8208.
[17] Siergiejczyk M., Rosiński A., Paś J.,: *Analysis of unintended electromagnetic fields generated by safety system control panels*, DIAGNOSTYKA, 2016, Vol. 17, No. 3, ISSN 1641-6414, pp. 35-46.
[18] Paś J.: *Analysis of exploitation access control system selected object*, Przegląd Elektrotechniczny, vol 2015, no 10, ISSN 0033-2097, R. 91, pp. 219 – 224.

Dr hab. inż. Jacek Paś, profesor nadzwyczajny *na Wydziale Elektroniki Wojskowej Akademii Technicznej. Jego zainteresowania naukowe obejmują analizę niezawodnościowo-eksploatacyjną elektronicznych systemów bezpieczeństwa, systemów telematyki transportu oraz zagadnienia kompatybilności elektromagnetycznej. W dorobku naukowym posiada kilkadziesiąt publikacji naukowych.*