Analiza dydaktycznych stanowisk Elektronicznych Systemów Bezpieczeństwa nadzorowanych i zarządzanych informatycznie

Waldemar Szulc

Wyższa Szkoła Menedżerska w Warszawie, Wydział Informatyki Stosowanej i Technik Bezpieczeństwa

Streszczenie: W artykule przeanalizowano funkcjonalność 28 stanowisk laboratoryjnych do zastosowań dydaktycznych i badawczych, które utworzono w unikalnym Zespole Laboratoriów Systemów Bezpieczeństwa w Wyższej Szkole Menedżerskiej w Warszawie na Wydziale Informatyki Stosowanej i Technik Bezpieczeństwa.

Słowa kluczowe: elektroniczne systemy bezpieczeństwa, systemy alarmowe, bezpieczeństwo, monitoring wizyjny, kontrola dostępu

DOI: 10.14313/PAR_203/67

1. Wstęp

Utworzenie w 2006 r. pierwszej w Polsce specjalności *Bezpieczeństwo Obiektów i Informacji* na Wydziale Informatyki Stosowanej i Technik Bezpieczeństwa Wyższej Szkoły Menedżerskiej w Warszawie było przyczynkiem budowy Zespołu Laboratoriów Systemów Bezpieczeństwa – ZLSA. Autor – długoletni pracownik naukowy Wydziału Elektroniki Politechniki Warszawskiej, następnie Wydziału Transportu oraz współpracownik Wydziału Elektroniki WAT – zajmował się i zajmuje problematyką elektronicznych systemów bezpieczeństwa oraz ich informatycznym nadzorem i zarządzaniem [1–3]. Zbudowanie unikalnego laboratorium było ogromnym wyzwaniem. W efekcie powstały stanowiska dydaktyczne i badawcze:

1. Systemy Sygnalizacji Włamania i Napadu (wraz z elementami składowymi systemów),
2. Systemy Kontroli Dostępu (wraz z elementami składowymi systemów),
3. Systemy Sygnalizacji Pożarowej (wraz z elementami składowymi systemów),
4. Systemy Dźwiękowego Ostrzegania (DSO),
5. Systemy Monitoringu Wizyjnego (wraz z elementami składowymi systemów),
6. Zintegrowane Systemy Bezpieczeństwa,
7. Elementy Budynków Inteligentnych wraz z okablowaniem strukturalnym,
8. Zarządzanie i nadzór nad elektronicznymi systemami bezpieczeństwa,
9. Mechaniczne i Elektromechaniczne elementy składowe systemów bezpieczeństwa,
10. Monitoring przewodowy i bezprzewodowy.

Koncepcję Laboratorium Systemów Bezpieczeństwa utworzono równolegle z powstaniem specjalności. Ze względu na wysokie koszty, budowę rozpoczęto w 2008 r. dzięki zaangażowaniu wielu sponsorów. Wstępnie planowano cztery stanowiska, faktycznie powstało ich 12. Do głównych można zaliczyć: 6 stanowisk dotyczących telewizji analogowej i cyfrowej wraz z kamerami IP (sponsorowane przez SONY Poland przy współudziale ALTRAM), 6 stanowisk dotyczących Sygnalizacji Włamania i Napadu (sponsorem SATEL przy współudziale ASTRAL i MULTISYSTEM). Nowoczesne stanowiska dotyczące elektronicznej ochrony obiektów wyposażała firma AAT. Uroczyste otwarcie Zespołu Laboratoriów Systemów Bezpieczeństwa nastąpiło w marcu 2009 r.

2. Syntetyczny wykaz stanowisk laboratoryjnych

1. Zastosowanie Systemu Sygnalizacji Włamania i Napadu do sterowania urządzeniami infrastruktury technicznej budynku (SATEL),
2. System Sygnalizacji Włamania i Napadu jako system bezprzewodowy (SATEL),
3. System Sygnalizacji Włamania i Napadu realizujący funkcje Systemu Kontroli Dostępu (SATEL),
4. Zarządzanie Systemem Sygnalizacji Włamania i Napadu przez sieć Ethernet (SATEL),
5. Badanie czujek (wszystkie typy) współpracujących z elektronicznymi systemami bezpieczeństwa, (SATEL),
6. Aktywna bariera podczerwieni (SATEL),
7. System Sygnalizacji Włamania i Napadu w wersji rozproszonej (SATEL),
8. System Sygnalizacji Włamania i Napadu w wersji mieszanej (SATEL),
9. System Sygnalizacji Włamania i Napadu w wersji skupionej (SATEL),
10. Analogowy System Monitoringu Wizyjnego (SONY),
11. System monitoringu wizyjnego CCTV i CCTV IP (SONY),
12. Inteligentna kamera IP (SONY),
13. Zastosowanie podczerwieni w Systemach Monitoringu Wizyjnego (SONY),
14. System Sygnalizacji Włamania i Napadu DSC typ PC1832 (AAT),

Rys. 1. Widok Laboratorium Systemów Alarmowych

Fig. 1. View of Alarm Systems Laboratory

15. Domofony (GDE COMMAX),
16. Systemy wideodomofonowe (GDE COMMAX),
17. Systemy wieloabonentowe (GDE COMMAX)
18. Systemy sygnalizacji pożarowej w transporcie (ELTRONIK),
19. System Kontroli Dostępu (ROGER,)
20. Bezprzewodowy System Bezpieczeństwa Agility (RISCO),
21. Zintegrowany System Bezpieczeństwa ProSYS (RISCO),
22. Zdalne zarządzanie elektronicznymi systemami bezpieczeństwa (SATEL, SONY, AAT, RISCO),
23. Badanie bezprzewodowych elektronicznych systemów bezpieczeństwa Firmy JABLOTRON
24. Badanie analogowych i impulsowych systemów zasilających elektroniczne systemy bezpieczeństwa,
25. Cyfrowe systemy domofonowe i wideodomofonowe Firmy ACO,
26. Badanie dźwiękowych systemów ostrzegawczych (DSO) firmy TOA,
27. Badanie cyfrowych systemów ppoż. firmy Schrack-Seconet Polska.
28. Zintegrowany System ppoż. IP (Schrack-Seconet Polska) z DSO (TOA).
29. Mechaniczne i elektromechaniczne urządzenia (DOM POLSKA)

Wszystkie stanowiska mają adresy IP. Są zarządzane i nadzorowane w sposób informatyczny. Wiele pracy poświęcono monitoringowi wizyjnemu. Ta część laboratorium została wyposażona w 28 kamer wysokiej rozdzielczości, które współpracują z wideoserwerami oraz kamery IP współpracujące z siecią informatyczną. Na rys. 1 przedstawiono kilka stanowisk dydaktycznych do badań różnych elektronicznych systemów bezpieczeństwa. Na wprost przedstawiono stanowisko do badań zasilaczy stosowanych w monitoringu wizyjnym.

Stanowiska laboratoryjne umożliwiły realizację wielu badań i poznanie zagadnień związanych z monitoringiem wizyjnym:

1. Właściwości użytkowe kamery z naciskiem na parametry optyczne, pole widzenia, znajdowanie ustawienia umożliwiającego obserwację tablicy testowej.
2. Właściwości obiektywów, ze szczególnym naciskiem na aberrację widoczną podczas obserwacji tablicy testowej.
3. Zagadnienie rozdzielczości toru wizyjnego z wyraźnym podziałem na ograniczenia natury optycznej i elektrycznej.
4. Wprowadzanie obrazów z kamer do sieci IP, prawdziwe kamery IP, kamery analogowe z koderem IP, różnice, wady, zalety.
5. Kamery z opcją PTZ, podstawowe cechy, sposób sterowania, zastosowania.
6. Praca kamer IP bez urządzeń dodatkowych, połączenie przez wewnętrzny serwer www kamery, możliwość konfiguracji przez sieć IP, dostępne parametry.
7. Praca kamer w większych systemach, wykorzystanie oprogramowania zarządzającego, wady, zalety, porównanie z pracą samodzielną (przez serwer www kamery).

Ćwiczenia laboratoryjne prowadzone w Zespole Laboratoriów Systemów Bezpieczeństwa umożliwiają badanie i analizę Elektronicznych Systemów Bezpieczeństwa (ESB) różnych typów, zarówno samodzielnych jak i zintegrowanych (sprzętowo i programowo). Stanowiska umożliwiają też prowadzenie badań naukowych. Ze względu na b. dużą liczbę stanowisk, sukcesywnie opracowywane są instrukcje laboratoryjne. Jest planowane wydanie unikalnego podręcznika dot. ESB. Dołączone fotografie ilustrują tylko małą część stanowisk dydaktycznych, które są na wyposażeniu Zespołu Laboratoriów Systemów Bezpieczeństwa.

3. Charakterystyka dydaktycznych stanowisk ESB w aspekcie informatycznego nadzoru i zarządzania

Stanowisko 1 – Zastosowanie Systemów Sygnalizacji Włamania i Napadu do sterowania urządzeniami infrastruktury budynków – składa się z płyty głównej centrali alarmowej INTEGRA64, manipulatora INT-KLCD-BL,

Rys. 2. Stanowisko dydaktyczne do badań central INTEGRA 64

Fig. 2. Didactic stand for studying systems INTEGRA 64

Rys. 3. Stanowisko dydaktyczne do badań monitoringu wizyjnego i analizy obrazu

Fig. 3. Didactic stand for studying visual monitoring and picture analysis

modułu rozszerzeń wyjść CA-64 O-R, czujki GRAPHITE, sterownika RE-4K wraz z dwoma pilotami czterokanałowymi, modułu GSM-4, komputera z oprogramowaniem DLOADX i GUARDX (fot. 2). Możliwa jest współpraca z wieloma modemami.

Stanowisko 2 – umożliwia badania wszystkich typów czujek współpracujących z Systemami Sygnalizacji Włamania i Napadu – czujki przewodowe, czujki współpracujące z liniami dozorowymi oraz bezprzewodowe.

Stanowisko 3 – System Sygnalizacji Włamania i Napadu jako System bezprzewodowy – przeznaczone do badań możliwości zastosowania urządzeń bezprzewodowych w Systemach Sygnalizacji Włamania i Napadu. Składa się z płyty głównej centrali alarmowej INTEGRA32, manipulatora INT-KLCD-BL, modułu kontrolera systemu bezprzewodowego ACU-100, bezprzewodowej pasywnej czujki podczerwieni APD-100, bezprzewodowej czujki magnetycznej AMD-101, bezprzewodowego sygnalizatora zewnętrznego ASP-105, bezprzewodowego sterownika 230 V AC typu ASW-100E, testera poziomu sygnału radiowego ARF-100, czujki AQUA Plus, komputera z oprogramowaniem DLOADX i GUARDX. Na stanowisku jest stosowany analizator widma.

Stanowisko 4 – System Sygnalizacji Włamania i Napadu realizujący funkcję Kontroli Dostępu – przeznaczone do badań możliwości zastosowania Systemów Sygnalizacji Włamania i Napadu jako System Kontroli Dostępu. Składa się z płyty głównej centrali alarmowej INTEGRA128, manipulatora INT-KLCD-BL, modułu ethernetowego ETHM-1, modułu generatora komunikatów głosowych VMG-16, modułu czytnika kart zbliżeniowych CA-64 SR, czytnika kart zbliżeniowych CZ-EMM2, kart zbliżeniowych KT-STD-1, dualnej czujki ruchu SILVER (lub innych), komputera z oprogramowaniem DLOADX i GUARDX.

Stanowisko 5 – Zarządzanie Systemem Sygnalizacji Włamania i Napadu przez sieć Ethernet – przeznaczone do badań możliwości zdalnego zarządzania Systemem Sygnalizacji Włamania i Napadu przez sieć Ethernet (np. LAN lub WAN) oraz wykorzystania sieci z protokołem TCP/IP do integracji elektronicznych systemów bezpieczeństwa. Składa się z: płyty głównej centrali alarmowej INTEGRA128, manipulatora INT-KLCD-BL, modułu ethernetowego ETHM-1, dualnej czujki ruchu SILVER, komputera z oprogramowaniem DLOADX i GUARDX.

Stanowisko 6 – Aktywna Bariera Podczerwieni – przeznaczone do badań 8-wiązkowej programowalnej bariery nadawczo-odbiorczej do ochrony m.in.: wejść, wyjść i innych dużych przestrzeni. Składa się z aktywnej bariery podczerwieni ACTIVA-7, komputera z portem RS-232 i oprogramowaniem ACTIVA. Stanowisko pracuje w warunkach rzeczywistych, m.in. kontroluje wejście do laboratorium. Podgląd wiązek podczerwieni odbywa się informatycznie. Bariera aktywna jest podłączona do centrali alarmowej INTEGRA 128.

Stanowisko 7 – System Sygnalizacji Włamania i Napadu w wersji rozproszonej – przeznaczone do badań niezawodności, eksploatacji i możliwości funkcjonalnych Systemów Sygnalizacji Włamania i Napadu zrealizowanych jako system o strukturze rozproszonej. Składa się z płyty głównej centrali alarmowej INTEGRA128, manipulatora INT-KLCD-BL, manipulatora INT-KLCD-BL, wielofunkcyjna klawiatura INT-SCR-BL, modułu ethernetowego ETHM-1, modułu wejść adresowalnych CA-64 ADR, modułu wyjść na szynę DIN: INT-ORS, czujek AQUA (lub innych), dualnych czujek ruchu SILVER (lub innych), czujki ruchu sufitowej AQUA RING, czujek magnetycznych, czujki zbitcia szkła INDIGO, przycisków napadowych z pamięcią, testera czujek zbitcia – tester INDIGO, komputera z oprogramowaniem DLOADX i GUARDX.

Stanowisko 8 – Kontrola Dostępu firmy SATEL – wyposażone w czytniki biometryczne oraz standardowe (w trakcie uruchamiania), system KD ma nadzór informatyczny.

Stanowisko 9 – System Sygnalizacji Włamania i Napadu w wersji mieszanej – składa się z płyty głównej centrali alarmowej CA-10P, manipulatora CA-10KLED, dwóch modułów wejść CA-10E, modułu syntezera mowy SM-2, czujek AQUA, dualnych czujek ruchu SILVER, komputera z oprogramowaniem DLOAD10.

Stanowisko 10 – System Sygnalizacji Włamania i Napadu w wersji skupionej – składa się z płyty głównej centrali alarmowej CA-5, manipulatora CA-5KLED, manipulatora CA-5KLED, czujek AQUA, dualnych czujek ruchu SILVER.

Stanowisko 11 – Analogowy System Monitoringu Wizyjnego – składa się z czterech kamer analogowych, przełącznika sekwencyjnego 8-wejściowego, 4-wejściowego dzielnika obrazu, monitora czarno-białego 17" nadzoru wizyjnego.

Rys. 4. Stanowisko dydaktyczne do badania monitoringu wizyjnego z kamerami IP

Fig. 4. Didactic stand for studying visual monitoring with IP cameras

go, monitora czarno-białego 10" nadzoru wizyjnego. Jedną z kamer jest połączona z przełącznikiem sekwencyjnym torem bezprzewodowym pracującym na częstotliwości $f = 2,4$ GHz. Pozostałe kamery wykorzystują tor przewodowy (kabel koncentryczny).

Stanowisko 12 – System Monitoringu Wizyjnego CCTV i CCTV IP – przeznaczone do badań niezawodności, eksploatacji i możliwości funkcjonalnych systemów monitoringu wizyjnego analogowych oraz cyfrowych. Składa się z 4 kamer analogowych czarno-białych SSC-M383CE, 4 kamer analogowych kolorowych o wysokiej rozdzielczości poziomej SSC-E453P, 4 kamer analogowych kolorowych typu dzień/noc o wysokiej rozdzielczości poziomej SSC-E478P, 4 kamer kolorowych sieciowych z protokołem TCP/IP, 4 wideoserwerów SNT-V704 do przesyłania obrazu z kamer analogowych przez sieć TCP/IP, 4 komputerów z oprogramowaniem: IP Setup Program (do wyszukiwania adresów IP kamer i wideoserwerów pracujących w sieci) i Real Shot Manager (do tworzenia inteligentnych systemów monitoringu wizyjnego). Całość jest połączona siecią komputerową.

Stanowisko 13 – Inteligentna kamera IP – przeznaczone do badań możliwości funkcjonalnych i eksploatacyjnych kamer IP stosowanych w Systemach Monitoringu Wizyjnego. Składa się z kamery IP typu SNC-RZ50P, komputera z oprogramowaniem: IP Setup Program i Real Shot Manager. Zastosowana kamera jest zintegrowana z obiektywem umożliwiającym 26-krotną zmianę ogniskowej. Kamera wytwarza dwa strumienie danych wyjściowych, każdy może być kompresowany za pomocą algorytmów JPEG, MPEG-4 lub H.264. Liczne funkcje cyfrowej obróbki obrazów, w tym inteligentna detekcja ruchu, pozwalają na dostosowanie kamery SNC-RZ50P do warunków

eksploatacji. Na podkreślenie zasługuje funkcja cyfrowej stabilizacji obrazów eliminująca ich drżenie w przypadku montażu kamery na niestabilnym podłożu, np. na wysokim maszcie. Dynamiczna integracja obrazów pozwala na ostre i czytelne odwzorowanie obiektów ruchomych, co jest szczególnie istotnie podczas przechwytywania pojedynczych klatek wizyjnych.

Stanowisko 14 – Zastosowanie podczerwieni w Systemach Monitoringu Wizyjnego składa się z kamery analogowej z oświetlaczem podczerwieni, kamery analogowej kolorowej typu dzień/noc o wysokiej rozdzielczości poziomej, oświetlacza podczerwieni o zasięgu 100 m, monitora kolorowego 7" nadzoru wizyjnego. Na fot. 4 przedstawiono stanowisko dydaktyczne do badań kamer IP w systemie monitoringu wizyjnego z możliwością zastosowania reflektorów podczerwieni dużej mocy – podgląd obrazu. Kamera jest sterowana i nadzorowana informatycznie.

Stanowisko 15 – System Sygnalizacji Włamania i Napadu DSC typ PC1832 – składa się z płyty głównej centrali alarmowej PC 1832, manipulatora PK 5516-LED, manipulatora LCD RFK5500 z modulem bezprzewodowym, modułu rozszerzeń wejść PC5108, czujek przewodowych (PIR, PIR+MW, czujki wibracyjnej zbitcia szkła, czujki magnetycznej) i bezprzewodowych czujek dymu i temperatury, sterownika bezprzewodowego z pilotami, nadajnika monitorującego GSM/GPRS, komputera z oprogramowaniem (rys. 5).

Stanowisko 16 – Domofony – składa się ze stacji bramowej DR 2A2N, stacji domowej DP 201R, stacji domowej DP-20HR.

Stanowisko 17 – Systemy wideodomofonowe – składa się ze stacji bramowej z kamerą DRC 4CH, monitora kolorowego CDV-71BE, kamery kolorowej CRC-41BQ.

Rys. 5. Stanowisko dydaktyczne do badań przewodowych i bezprzewodowych SSWiN z monitoringiem radiowym (typ DSC)

Fig. 5. Didactic stand for studying wire and remote connected SSWiN with radio monitoring (DSC type)

Rys. 6. Stanowisko dydaktyczne do badań systemu ppoż. dla potrzeb transportu

Fig. 6. Didactic stand for studying fire detection systems applied in transportation

Stanowisko 18 – Systemy wieloabonentowe (do 2400 użytkowników) – składa się ze stacji bramowej z kamerą DRC-MSC, dystrybutora budynkowego sygnałów CCU-BS, dystrybutora mieszkaniowego sygnałów CCU-FS, stacji domowej CAV-51M.

Stanowisko 19 – Systemy sygnalizacji pożarowej w transporcie – przeznaczone do badań w zakresie funkcjonalności, konfiguracji, programowania i eksploatacji systemów sygnalizacji pożarowej stosowanych w obiektach mobilnych, np. w pociągach INTERCITY. Składa się z centrali sygnalizacji pożarowej CSP1, koncentratora czujek CSP1CA, symulatorów czujek pożarowych (rys. 6).

Stanowisko 20 – System Kontroli Dostępu – składa się (rys. 7) z centrali kontroli dostępu CPR32-SE, interfejsu

Rys. 7. Stanowisko dydaktyczne do badań systemu cyfrowego kontroli dostępu (ROGER)

Fig. 7. Didactic stand for studying digital access control systems (ROGER)

komunikacyjnego USB-RS-232 typu UT-2USB, kontrolera zintegrowanego z czytnikiem PR621, czytnika zbliżeniowego PRT66LT, kontrolera zintegrowanego z czytnikiem PR611, czytnika zbliżeniowego z klawiaturą PRT64LT, kontrolera zintegrowanego z czytnikiem PR311SE, czytnika zbliżeniowego PRT12LT-BK, modułu rozszerzeń we/wy. XM-2, kontrolera z zasilaczem PR411DR, czytnika zbliżeniowego PRT62LT (2 szt.), symulatorów we/wy (5 szt.).

Stanowisko 21 – Bezprzewodowy System Bezpieczeństwa Agility – składa się z centrali alarmowej Agility Wireless, szyfratora LCD z czytnikiem zbliżeniowym, modułu we/wy z wbudowanym interfejsem X10, detektora zewnętrznego PIR, detektora PIR, detektora PIR/PET, detektora wstrząsowego stłuczenia szkła, detektora zalania, kontaktronu, sterownika zdalnego, pilota 4-przyciskowego,

Rys. 8. Stanowisko dydaktyczne do badań bezprzewodowych SSWiN z nadzorem informatycznym

Fig. 8. Didactic stand for studying remote operated SSWiN under computer control

Rys. 9. Stanowisko dydaktyczne do badań bezprzewodowego SSWiN (Jablotron)

Fig. 9. Didactic stand for studying remote operated SSWiN (Jablotron)

Rys. 10. Stanowisko dydaktyczne do badań Dźwiękowych Systemów Ostrzegawczych

Fig. 10. Didactic stand for studying Sound Alarm Systems

pilota sygnalizacji napadu, pilota sygnalizacji napadu w wersji „zegarek”, zewnętrznego sygnalizatora akustyczno-optycznego.

Stanowisko 22 – Zintegrowany System Bezpieczeństwa ProSYS – składa się z płyty głównej ProSYS, klawiatury dotykowej z czytnikiem zbliżeniowym, klawiatury LCD, modułu rozszerzenia 8-liniowego, zasilacza impulsowego 3 A (SMPS), zaawansowanego modułu komunikacji IP, interaktywnego modułu głosowego, modułu nasłuchu, modułu zintegrowanej kontroli dostępu, czytnika kart zbliżeniowych, modułu 44 wyjść przekaźnikowych, 8-liniowego rozszerzenia bezprzewodowego, 4-przyciskowego pilota bezprzewodowego, detektora przemysłowego WATCHIN, detektora zewnętrznego WATCHOUT, detektora dualnego serii iWISE, detektora PIR serii Zodiac, detektora zbitcia szkła, detektora wstrząsowego, kart zbliżeniowych (5 szt.).

Stanowisko 23 – Zdalne zarządzanie elektronicznymi systemami bezpieczeństwa – przeznaczone do badań systemów ochrony terenów zewnętrznych za pomocą analogowej i cyfrowej sieci telefonicznej, sieci komputerowej i interfejsów komunikacyjnych RS-232 i RS-485. Składa się z komputera z oprogramowaniem (DLOADX, GUARDX, DLOAD10, IP Setup Program, Real Shot Manager, opro-

gramowanie DSC oraz RISCO) dołączonego do sieci komputerowej (umożliwiającej połączenie z innymi stanowiskami), linii telefonicznej analogowej, modułu cyfrowej telefonii komórkowej GSM. Na rys. 8 przedstawiono stanowisko do badań bezprzewodowego systemu alarmowego z wieloma czujkami z możliwością satelitarnego przekazu zagrożeń. System jest zarządzany i nadzorowany informatycznie. System ma adres IP.

Stanowisko 24 – Bezprzewodowa radiowa sygnalizacja włamania i napadu – system pracuje na częstotliwości $f = 866 \text{ MHz}$, Stanowisko zostało wyposażone we wszystkie typy czujek stosowanych w elektronicznych systemach bezpieczeństwa. Na rys. 9 przedstawiono stanowisko do badań bezprzewodowego systemu alarmowego z wieloma czujkami, także bezprzewodowymi. Widoczna jest specjalizowana kamera TV, której obraz przekazywany jest przez GSM.

Stanowisko 25 – Uniwersalne systemy zasilające firmy PULSAR przeznaczone do zasilania monitoringu wizyjnego, kontroli dostępu, systemów ppoż., systemów sygnalizacji włamania i napadu. Stanowisko umożliwia też badanie rezerwowych źródeł zasilających – akumulatorów.

Stanowisko 26 – Cyfrowe systemy domofonowe i wideodomofonowe – od prostych po systemy z kontrolą dostępu (karty magnetyczne).

Stanowisko 27 – Dźwiękowe systemy ostrzegania – typ VM-3000 (Integrated Voice Evacuation System) firmy TOA, stosowany w przypadku zagrożenia pożarowego. Stanowisko (rys. 10) współpracuje, za pośrednictwem łącza transmisyjnego, z cyfrowym systemem ppoż. dowolnego typu (tu z systemem IP firmy Schrack-Seconet Polska).

Stanowisko 28 – Cyfrowe systemy ppoż. IP firmy Schrack-Seconet Polska. Stanowisko umożliwia symulowanie róż-

Rys. 11. Stanowisko dydaktyczne do badań Systemu Sygnalizacji Pożarowej: INTEGRAL IP

Fig. 11. Didactic stand for studying Fire Alarm Systems INTEGRAL IP

Rys. 12. Układ blokowy zasilacza wyposażony w rezerwowe źródło $U = 24 \text{ V}$ ($\pm 15 \%$) z mikroprocesorowym nadzorem pracy

Fig. 12. Block scheme of a power supply unit equipped with a reserve power source $U = 24 \text{ V}$ ($\pm 15 \%$) controlled by a microprocessor

Rys. 13. Charakterystyki: $U_{wy} = f(U_{we})$, gdy $I_{wy} = I_0 = \text{const}$

Fig. 13. Characteristic: $U_{out} = f(U_{in})$ for $I_{out} = I_0 = \text{constant}$

nych zagrożeń pożarowych (różne typy czujek, rys. 11). Może współpracować z Dźwiękowym Systemem Ostrzegawczym firmy TOA. Wizualizacja zagrożeń jest realizowana na dwóch monitorach współpracujących ze specjalną kartą graficzną komputera. Na monitorach jest edytowany chroniony obiekt, a na nim wszystkie czujki ppoż. oraz występujące zagrożenia i zdarzenia.

4. Przykładowe wyniki badań

Spośród wielu przedstawionych stanowisk laboratoryjnych wybrano (dla przedstawienia istotnych danych) to, które

dotyczy zasilania elektronicznych systemów bezpieczeństwa. Przykładowe wyniki badań i pomiarów (stanowisko 25) dotyczą zasilacza (rys. 12) stosowanego w systemach ppoż. (stanowiska 28 i 27).

Wybrane istotne wyniki badań zostały przedstawione na rys. 13–15. Charakterystyka obciążeniowa $U_{wy} = f(U_{we})$ dla $I_{wy} = I_0 = \text{const}$ (rys. 12) świadczy o dobrym wskaźniku stabilizacji napięcia wyjściowego.

Charakterystyka $U_{wy} = f(I_{wy})$, gdy $U_{we} = \text{const}$ (rys. 14) przedstawia utrzymanie stabilnego napięcia wyjściowego U_{wy} ($24,16 \text{ V} \leq U_{wy} \leq 23,85 \text{ V}$) przy dużych zmianach napięcia wejściowego od 190 V do 260 V.

Rys. 14. Charakterystyki: $U_{wy} = f(I_{wy})$, gdy $U_{we} = \text{const}$

Fig. 14. Characteristic: $U_{out} = f(I_{out})$ for $U_{in} = \text{constant}$

Rys. 15. Charakterystyki: sprawność $\eta = f(I_{wy})$ dla $U_{we} = \text{const}$

Fig. 15. Characteristic: efficiency $\eta = f(I_{out})$ when $U_{in} = \text{constant}$

Na rys. 15. przedstawiono charakterystykę sprawności η badanego zasilacza w zależności od zmian napięcia wejściowego – w zakresie od 190 V do 260 V. Otrzymane wyniki świadczą o dużej sprawności zasilacza przeznaczonego do stosowania w systemach ppoż.

Sprawność η dla zasilaczy impulsowych z nadzorem mikroprocesorowym (rys. 12), znacznie wzrasta i może zawierać się w granicach $84 \% \leq \eta \leq 94 \%$.

Zbadano również wskaźnik określający niezawodność pracy zasilaczy, które są specjalnie projektowane do stosowania w ESB

$$K_G = \frac{T_m}{T_m + T_n}$$

Jest to tzw. wskaźnik gotowości K_G zasilaczy [8]. Badanie wskaźnika K_G jest długofalowe i żmudne, ale bardzo istotne. W trakcie badań niezawodnościowo-eksploatacyjnych trwających 12 miesięcy (8760 h), określając czas naprawy pojedynczego uszkodzenia $T_n = 0,5$ h oraz znając czas poprawnej pracy układu zasilającego T_m , określono wskaźnik gotowości $K_G = 0,9994$, co

stanowi bardzo dobry rezultat. Należy wyraźnie podkreślić, że badane zasilacze były wykonane bardzo starannie przez renomowaną polską firmę specjalizującą się w budowie tego typu urządzeń. Trzeba także pamiętać, że zasilacze zasilające systemy ppoż. to urządzenia, które muszą mieć (ze względu na bezpieczeństwo ludzi i obiektów) bardzo wysoki wskaźnik niezawodnościowy (gotowości).

5. Podsumowanie i wnioski

Ważną rolę przy budowie i konfiguracji stanowisk odgrywa Studenckie Koło Naukowe Technik Bezpieczeństwa, którego opiekunem naukowym jest autor.

Bardzo istotna jest budowa nowoczesnego Laboratorium Miernictwa i Elektroniki, bez którego badania naukowe oraz zajęcia dydaktyczne są niemożliwe. Dotychczas laboratorium było realizowane w postaci wirtualnej za pomocą kolejnych wersji programu TINA, od stycznia 2013 r. budowane jest w wersji rzeczywistej. To duże wyzwanie zważywszy, że literatura na temat ESB jest bardzo uboga. Trzeba pamiętać o nowych normach, które obowiązują od przystąpienia Polski do UE. Prawie wszystkie istniejące normy PN uległy zmianie. Ponieważ stanowiska wyposażone są w różne czujniki i czytniki (także biometryczne), konieczna jest wiedza z chemii, fizyki i medycyny oraz znajomość zjawisk kompatybilności elektromagnetycznej. Prezentowane stanowiska dydaktyczne i badawcze stanowią nowość w Polsce. Zespół Laboratoriów Systemów Bezpieczeństwa to największy projekt zrealizowany na polskiej uczelni.

Bibliografia

1. Szulc W., Rosiński A., *Prace badawcze własne, Bezpieczeństwo Obiektów i Informacji*, WSM, Warszawa, 2009–2013.
2. Szulc W., Rosiński A., *Wybrane zagadnienia z miernictwa i elektroniki dla informatyków* (część I analogowa), Wyd. WSM, Warszawa 2012.
3. Szulc W., Rosiński A., *Wybrane zagadnienia z elektroniki cyfrowej dla informatyków* (część II cyfrowa), Wyd. WSM, Warszawa 2012.
4. Instrukcje serwisowe firm: SATEL, ROGER, JABLOTRON, SCHRACK-SECONET- Polska, TOA, RISCO, ROGER, ELTRONIK, AAT, SONY, PULSAR, GDE, ACO, DOM POLSKA, NDN, GALAXY (2009–2013).
5. Nawrocki W., *Komputerowe systemy pomiarowe*, Wyd. WKiŁ, Warszawa 2002.
6. Kałużny P., *Telewizyjne systemy dozоровe*, Wyd. WKiŁ, Warszawa 2008.
7. Normy: PN-EN 50130, PN-EN 50133, PN-EN 50132, PN-EN 50130, PN-EN-50131-6, PN-EN 50131-1 Zasilacze, PN-E-08350-4:1997 Systemy pożarowe, Zasilacze, PN-EN 50132-7:2003 Systemy alarmowe. Systemy dozоровe CCTV w zastosowaniach doty-

czących zabezpieczenia. Zalecenia dotyczące zastosowań.

8. Szulc W., *Problemy niezawodnościowo-eksploatacyjne układów zasilających elektroniczne systemy bezpieczeństwa*, „Pomiary Automatyka Robotyka”, nr 1/2012, 54–63. ■

Analysis of didactic stands for Electronic Safety Systems from the point of view of computer supervision and management

Abstract: The article is devoted to the analysis of 28 laboratory stands in the unique Alarm System Laboratories built and operated in the Department of Applied Computer Science of the Warsaw Management Academy.

Keywords: electronic safety systems, alarm systems, safety, vision control, access control

Artykuł recenzowany, nadesłany 9.12.2013 r., przyjęty do druku 27.12.2013 r.

doc. dr inż. Waldemar Szulc

Od 1965 r. pracownik naukowy Politechniki Warszawskiej na Wydziałach: Komunikacji, Elektroniki, Instytutu Transportu oraz na Wydziale Transportu. Zajmował się problematyką: Telekomunikacji, Radiokomunikacji, Radiolokacji, Podstaw Elektroniki i Elektroniki ze szczególnym uwzględnieniem układów dla potrzeb Transportu oraz Elektronicznymi Systemami Bezpieczeństwa Obiektów. Od 2011 r. jest kierownikiem Katedry Technik Bezpieczeństwa. Jest autorem lub współautorem ponad 10 patentów oraz autorem lub współautorem ponad 52 wdrożeń urządzeń elektronicznych dla potrzeb PKP. Jest autorem lub współautorem ponad 150 publikacji. Brał udział w ponad 35 pracach o charakterze naukowo-badawczym. Był dziekanem i prodziekanem Wydziału Informatyki Stosowanej i Technik Bezpieczeństwa w Wyższej Szkole Menedżerskiej w Warszawie. Jest autorem lub współautorem wielu unikalnych rozwiązań z dziedziny Bezpieczeństwa Obiektów o charakterze specjalnym. Współautor koncepcji, zaprojektowania i uruchomienia Zespołu Laboratoriów Systemów Bezpieczeństwa w Wyższej Szkole Menedżerskiej w Warszawie.

e-mail: waldemar.szulc@mac.edu.pl