Artykuł został przetłumaczony na język angielski na podstawie zadania finansowanego w ramach umowy nr 805/P-DUN/2017 ze środków Ministra Nauki i Szkolnictwa Wyższego przeznaczonych na działalność upowszechniającą naukę – stworzenie anglojęzycznych wersji wydawanych publikacji. **Jego oficjalną wersją jest wersja anglojęzyczna.** Niniejszy plik jest pierwotną wersją autorską po recenzjach, bez weryfikacji językowej i składu komputerowego.

mgr inż. Jarosław Łukasiak
Wojskowa Akademia Techniczna
Wydział Elektroniki
Instytut Systemów Elektronicznych
Zakład Eksploatacji Systemów Elektronicznych
ul. gen. S. Kaliskiego 2, 00-908 Warszawa, Polska
E-mail: jaroslaw.lukasiak@wat.edu.pl

dr hab. inż. Adam Rosiński – autor do kontaktów
Politechnika Warszawska
Wydział Transportu
Zakład Telekomunikacji w Transporcie
ul. Koszykowa 75, 00-662 Warszawa, Polska
E-mail: adro@wt.pw.edu.pl

MANIPULATOR GRAFICZNY W SYSTEMIE SYGNALIZACJI WŁAMANIA I NAPADU

Streszczenie

Systemy Sygnalizacji Włamania i Napadu (SSWiN) wchodzą w skład elektronicznych systemów bezpieczeństwa. Są one obecnie instalowane w wielu obiektach, zarówno użyteczności publicznej jak i prywatnych. Z tego też m.in. względu stosowane są różnego rodzaju rozwiązania interfejsów człowiek – system sygnalizacji włamania i napadu. W artykule przedstawiono wymagania funkcjonalne SSWiN, a następnie dokonano przeglądu wybranych rozwiązań interfejsów człowiek – SSWiN.

Słowa kluczowe: elektroniczne systemy bezpieczeństwa, interfejsy, bezpieczeństwo

1. WPROWADZENIE

Polska norma PN-EN 50131-1:2009 „Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Wymagania systemowe" [7], która jest tożsama z normą europejską EN 50131-1:2006 „Alarm systems – Intrusion and hold-up systems – Part 1: System requirements", zawiera wykaz elementów składowych, które powinien zawierać System Sygnalizacji Włamania i Napadu (SSWiN). Są to mianowicie następujące urządzenia: centrala alarmowa, jedna lub więcej czujek, jeden lub więcej sygnalizatorów i/lub systemów transmisji alarmu, zasilacz podstawowy, zasilacz rezerwowy. Wymienione elementy są niezbędne, by SSWiN mógł prawidłowo funkcjonować i realizować cele, które wyznaczono podczas procesu projektowania.

Połączenia pomiędzy elementami SSWiN powinny spełniać określone wymagania, a jednocześnie też muszą zawierać się w dopuszczalnych przez producenta parametrach. Z tego też względu są produkowane różnego rodzaju systemy, które spełniają wymagania zawarte w normie PN-EN 50131-1:2009 „Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Wymagania systemowe" odnośnie stopnia zabezpieczenia. Wyróżnia się następujące poziomy:

- stopień 1: Ryzyko małe (zakłada się, że intruz ma minimalną wiedzę na temat systemu alarmowego i posiada łatwo dostępne narzędzia w ograniczonym wyborze),
- stopień 2: Ryzyko małe do średniego (zakłada się, że intruz ma minimalną wiedzę na temat systemu alarmowego i posiada ogólno dostępne narzędzia i przenośne urządzenia, np. multimetr),
- stopień 3: Ryzyko średnie do wysokiego (zakłada się, że intruz zna biegle system alarmowy i posiada złożony zestaw zaawansowanych narzędzi i przenośnego sprzętu elektronicznego),
- stopień 4: Ryzyko wysokie (ma zastosowanie, gdy bezpieczeństwo ma priorytet nad wszystkimi innymi czynnikami. Zakłada się, że intruz posiada zdolności bądź środki by szczegółowo zaplanować włamanie i posiada zestaw dowolnego sprzętu, łącznie ze środkami do zastąpienia kluczowych elementów elektronicznego systemu alarmowego).

Po określeniu stopnia zabezpieczenia jaki system sygnalizacji włamania i napadu ma spełniać, dobiera się urządzenia, które spełniają założone wymagania. Jednym z istotniejszych elementów jest interfejs człowiek – SSWiN. Ma on wpływ nie tylko na

komfort użytkowania systemu przez użytkowników, ale także na bezpieczeństwo chronionego obiektu. Dość często o tym fakcie projektanci tych systemów zapominają i pomijają te kwestie przy analizie skuteczności funkcjonowania SSWiN. W niniejszym artykule autorzy zwrócili szczególną uwagę na ewolucję interfejsów człowiek – system sygnalizacji włamania i napadu oraz ich powiązanie z bezpieczeństwem obiektów.

2. WYMAGANIA FUNKCJONALNE W SSWIN

Systemy sygnalizacji włamania i napadu można zaliczyć do grupy urządzeń elektronicznych, ale ze względu na specyfikę ich funkcjonowania i zastosowania, powinny wyróżniać się określonymi cechami. Jedną z nich jest odpowiedzialność, jaka na nich (i na projektantach SSWiN) spoczywa. Od początku stosowania systemów SWiN były one kojarzone prawie wyłącznie z ochroną mienia i osób. Dlatego też w tym kierunku głównie postępował ich stopniowy rozwój. To przekonanie wśród większości naszego społeczeństwa z całą pewnością funkcjonuje do dnia dzisiejszego.

Systemy bezpieczeństwa, w tym także SSWiN, powinny cechować się odpowiednimi wartościami wskaźników niezawodnościowo-eksploatacyjnych [1, 2, 4, 9], które zazwyczaj w elektronicznych urządzeniach konsumenckich nie są na tak wysokich poziomach. Wskaźniki niezawodnościowo-eksploatacyjne można rozpatrywać w znaczeniu niezawodności i eksploatacji konstrukcyjnej wszelkich elementów i układów elektronicznych wchodzących w skład SSWiN. Jednym z takich wskaźników jest MTBF (ang. Mean Time Between Failures). Żeby zapewnić odpowiednią wartość należy już na etapie projektowania poszczególnych urządzeń składowych systemu uwzględnić m.in.: rozlokowanie elementów na płytce PCB (ang. Printed Circuit Board), sposób prowadzenia ścieżek, dobór ich szerokości oraz ewentualna ilość warstw płytki drukowanej, technikę montowania podzespołów (przewlekana, powierzchniowa, mieszana). W dalszej kolejności następuje wybór podzespołów oferowanych przez producentów. Z punktu widzenia eksploatacyjnego to właśnie od jakości użytych w procesie produkcji podzespołów zależy długotrwała, bezawaryjna praca urządzenia. Kwestia ta jest szczególnie istotna w przypadku urządzeń, które pracują w trybie ciągłym (a typowym przykładem charakteryzującym się wymienioną właściwością może być chociażby płyta główna centrali alarmowej systemu SWiN). Wspomniany zakres czynności ma również kluczowe znaczenie w celu otrzymania założonych parametrów niezawodnościowych i eksploatacyjnych

produkowanych urządzeń, których spełnienie producent deklaruje chociażby w przypadku dyrektywy "Nowego Podejścia" Unii Europejskiej, która nakłada szereg wymagań wobec urządzeń elektronicznych w zakresie kompatybilności elektromagnetycznej.

Systemy sygnalizacji włamania i napadu z racji swojego specyficznego przeznaczenia mają zastosowanie w najrozmaitszych obiektach. Konsekwencją tak szerokiego zbioru potencjalnych miejsc instalacji i późniejszej eksploatacji jest konieczność posiadania przez SSWiN kolejnej cechy, jaką jest łatwość obsługi z zachowaniem odpowiedniego poziomu bezpieczeństwa. Wspomniana uniwersalność i powszechność wymaga, aby obsługa poszczególnych urządzeń mających kontakt z użytkownikiem końcowym była tak opracowana, aby nie sprawiała żadnych trudności w trakcie montażu, konfiguracji i eksploatacji dla osób, które będą z nimi miały styczność. Systemy te projektowane są tak, aby niezależnie od stopnia zaznajomienia danej osoby z nowoczesną techniką czy chociażby poziomu jej wykształcenia była możliwa ich przystępna obsługa. Jednocześnie też proces uczenia się przez użytkowników obsługi SSWiN nie powinien być procesem czasochłonnym i kosztownym. Obsługa urządzeń SSWiN powinna być zrozumiała i intuicyjna zarówno dla osób młodych, jak i starszych (których często mają problemy zdrowotne związane z wzrokiem i słuchem) chcących zabezpieczyć swój obiekt.

Z racji wspomnianego zróżnicowania użytkowników, którzy mają dostęp do SSWiN, większość systemów opracowywana jest w taki sposób, aby uniemożliwić użytkownikowi przypadkowe zdestabilizowanie funkcjonowania całego systemu. Przyczyny takiego postępowania przez osoby mogą wynikać m.in. z braku wiedzy i odpowiedniego przeszkolenia lub pomyłki. Zapobiega się takim zdarzeniom m.in. poprzez racjonalny przydział uprawnień danego użytkownika do funkcji i informacji z systemu.

Aby możliwe było realizowanie wyżej wymienionych cech konieczne było wprowadzenie kolejnego rozwiązania charakteryzującego systemy SWiN. Mianowicie w systemach bezpieczeństwa, których szczególnych przypadkiem są systemy sygnalizacji włamania i napadu, nie może zaistnieć sytuacja, w której nie mamy pełnej wiadomości o stanie wszystkich obszarów i modułów systemu [11]. Dlatego tak ważne jest monitorowanie stanu poprawności funkcjonowania linii wejściowych i wyjściowych [12, 13]. Wspomniany monitoring obejmuje również zasilanie podstawowe i rezerwowe, a więc napięcie zasilające sieci elektrycznej i kontrolowanie

stanu akumulatora [8]. Obszarem podlegającym kontroli jest także stan dostępności torów transmisyjnych przeznaczonych do transmisji sygnałów alarmowych [10]. Oczywiście opisane monitorowanie i testowanie całego systemu może i powinno odbywać się bez potrzeby ingerencji użytkownika. Istotne jest też informowanie o wszelkich nieprawidłowościach, które mogą doprowadzić do zmniejszenia skuteczności funkcjonowania systemu sygnalizacji włamania i napadu lub w skrajnym przypadku całkowitego jego zneutralizowania.

Ostatnią z istotnych cech rozwiązań SSWiN jest bez wątpienia ich skalowalność. Pozwala to na zabezpieczenie przy pomocy tych samych urządzeń zarówno budynku biurowego jak i niewielkiego domu mieszkalnego. Oczywiście obydwa systemy będą się różnić liczbą zastosowanych elementów.

3. WYBRANE ROZWIĄZANIA INTERFEJSÓW CZŁOWIEK – SSWIN A BEZPIECZEŃSTWO OBIEKTÓW

Elementem systemu sygnalizacji włamania i napadu, z którym użytkownik końcowy ma najczęstszy kontakt jest manipulator (nazywany często także klawiaturą, szyfratorem). Dlatego naturalnym jest wniosek, że wszelkie wprowadzane modyfikacje i ulepszenia w wspomnianym urządzeniu oraz zupełnie nowe produkty tej kategorii są najszybciej dostrzegalnymi nowinkami rynkowymi z punktu widzenia przeciętnego użytkownika systemu SWiN. Zatem właśnie w tym segmencie urządzeń producenci systemów alarmowych starają się wprowadzać najciekawsze i najbardziej innowacyjne rozwiązania.

Należy zwrócić uwagę, że umieszczając na początku osi rozwoju manipulatorów urządzenia konwencjonalne (których reprezentanta przedstawiono na rys. 1), dalej poprzez warianty z sensoryczną technologią wprowadzania danych, a kończąc na obecnie najwyższym stadium rozwoju tej grupy urządzeń w postaci produktów wyposażonych w dotykowe, kolorowe wyświetlacze ciekłokrystaliczne, można zaobserwować znaczącą zmianę proporcji rozwoju poszczególnych typów interfejsów (także w aspekcie bezpieczeństwa).

Rys. 1. Przedstawiciel jednych z najbardziej podstawowych interfejsów człowiek – system wykorzystywanych w systemach SWiN na przykładzie manipulatora INT-KLCD [3]

Przedstawiony na rys. 1 manipulator umożliwia użytkownikowi (a wcześniej instalatorowi i serwisantowi) wprowadzanie danych do SSWiN. Oczywiście uprawnienia poszczególnych osób są uzależnione od wymaganego poziomu bezpieczeństwa, jaki w obiekcie przyjęto podczas projektowania systemu.

Można zaobserwować, że współczesne manipulatory systemów sygnalizacji włamania i napadu najwyższej klasy (w kontekście użytej technologii) na drodze swojej ewolucji starają się upodobnić do tabletów (rys. 2), które to w ciągu ostatnich kilku lat są bardzo popularne na rynku elektroniki użytkowej. Nie bez powodu czołowi producenci podjęli decyzję o poczynieniu takich kroków.

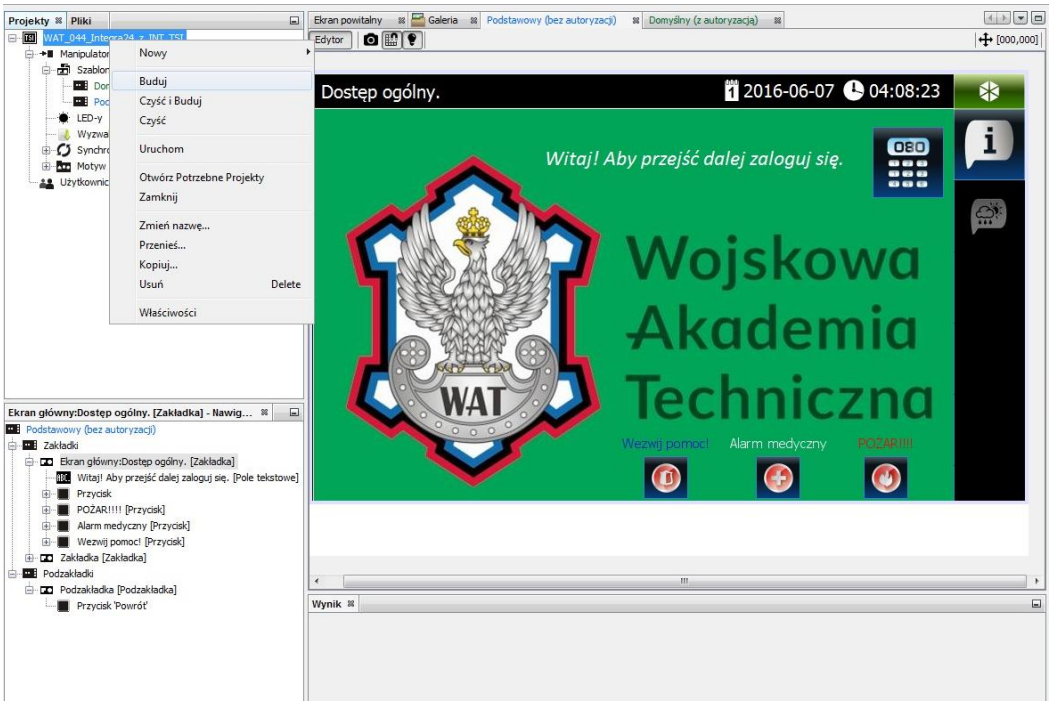
Urządzenia te dzięki zastosowaniu wyświetlaczy o wysokiej rozdzielczości sprawiają, że można przy ich pomocy prezentować więcej informacji i przedstawić je w bardziej czytelnej postaci (np. wykresy). Oczywiście wprowadzenie manipulatorów typu tabletowego skutkuje wzrostem zagrożeń, które to przedstawiono w dalszej części niniejszego artykułu.

Rys. 2. Wygląd manipulatorów typu tabletowego INT-TSI (szary) oraz INT-TSG (czarny) [3]

Seria manipulatorów INT-TSG jest to najbardziej ekonomiczne rozwiązanie z oferty jednego z producentów spośród manipulatorów tego segmentu. Urządzenie wyposażono w pojemnościowy, kolorowy ekran dotykowy o przekątnej 4,3". Obsługa manipulatora oparta jest na interfejsie graficznym, korzystającym w głównej mierze z prostych w obsłudze ikon lub w zależności od preferencji użytkownika oferującym widok opcji menu w postaci listy (analogicznie jak w manipulatorze tradycyjnym). Producent uwzględnił także możliwość tworzenia własnych ikon (funkcja MAKRO), których kliknięcie spowoduje wykonanie przez system szeregu uprzednio zdefiniowanych czynności. Przykładem takiej sytuacji może być wyłączenie świateł w całym budynku lub określonych pomieszczeniach, zasunięcie przeciwwłamaniowych rolet okiennych oraz zamknięcie bramy wjazdowej z pięciominutową zwłoką w przypadku uzbrojenia systemu SWiN dla wszystkich stref obiektu. Dobrze skonfigurowane funkcje „Makro" pozwalają na wzrost poziomu bezpieczeństwa poprzez automatyczne wykonywanie wcześniej zaplanowanych czynności.

Seria manipulatorów INT-TSI jest to na chwilę obecną najbardziej zaawansowana rodzina manipulatorów producenta, którego urządzenia zostały wykorzystane w badaniach. Oprócz obsługi wszelkich funkcji, które oferowane są przez wspomniane tańsze modele, urządzenia tej serii oferują także szereg bardzo zaawansowanych rozwiązań.

Pierwszą cechą odróżniającą omawianą grupę urządzeń w stosunku do już przedstawionych jest większy zakres personalizacji ekranu urządzenia. Kompozycja i konfiguracja ekranu tych manipulatorów mogą być indywidualnie projektowane dla każdego zdefiniowanego użytkownika lub dokonana poprzez wybór jednej z kilku gotowych, predefiniowanych propozycji. Dodatkowo możliwy jest wybór szeregu widżetów, czyli bardzo prostych funkcjonalnie miniprogramów działających w tle w trakcie pracy urządzenia. Jednym z przykładów takiej aplikacji może być widżet pogodowy, który w przypadku, gdy system został połączony z siecią Internet, będzie automatycznie pobierał informacje o prognozie pogody dla uprzednio skonfigurowanej lokalizacji. Co więcej, istnieje możliwość personalizacji poprzez wielkość zajmowanego obszaru tych elementów na wyświetlaczu manipulatora. Innym udogodnieniem dla użytkownika systemu jest możliwość zwięzłej prezentacji stanu systemu zamiast wygaszacza ekranu w momencie, gdy urządzenie przejdzie w tryb spoczynku. Wszelkie wspomniane opcje wyglądu i zakresu funkcji menu są konfigurowalne przy pomocy dedykowanej aplikacji TSI Builder przygotowanej przez firmę.



Rys. 3. Przykładowy projekt interfejsu użytkownika przez program TSI Builder [3]

Aplikacja TSI Builder umożliwia użytkownikowi zaprojektowania w pełni indywidualnego i bardzo rozbudowanego funkcjonalnie interfejsu użytkownika. Należy

zaznaczyć, że nie jest to zakres funkcji, który mógłby równać się z spotykanym w przeciętnym tablecie, jednakże w odniesieniu do branży SSWiN jest bez wątpienia kamieniem milowym. Na rys. 3 przedstawiono jeden z etapów realizacji przykładowego projektu interfejsu użytkownika.

Kolejnym rozwiązaniem, które zasługuje na szczególne uznanie pod kątem bezpieczeństwa jest możliwość prezentacji obrazu z kamer monitoringu wizyjnego pracujących w oparciu o protokół IP (ang. Internet Protocol). Muszą one być połączone z systemem SWiN poprzez sieć LAN/WAN. Takie rozwiązanie pozwala użytkownikowi na podgląd obrazu z kamer i adekwatne podejmowanie działań w stosunku do zaistniałych sytuacji.

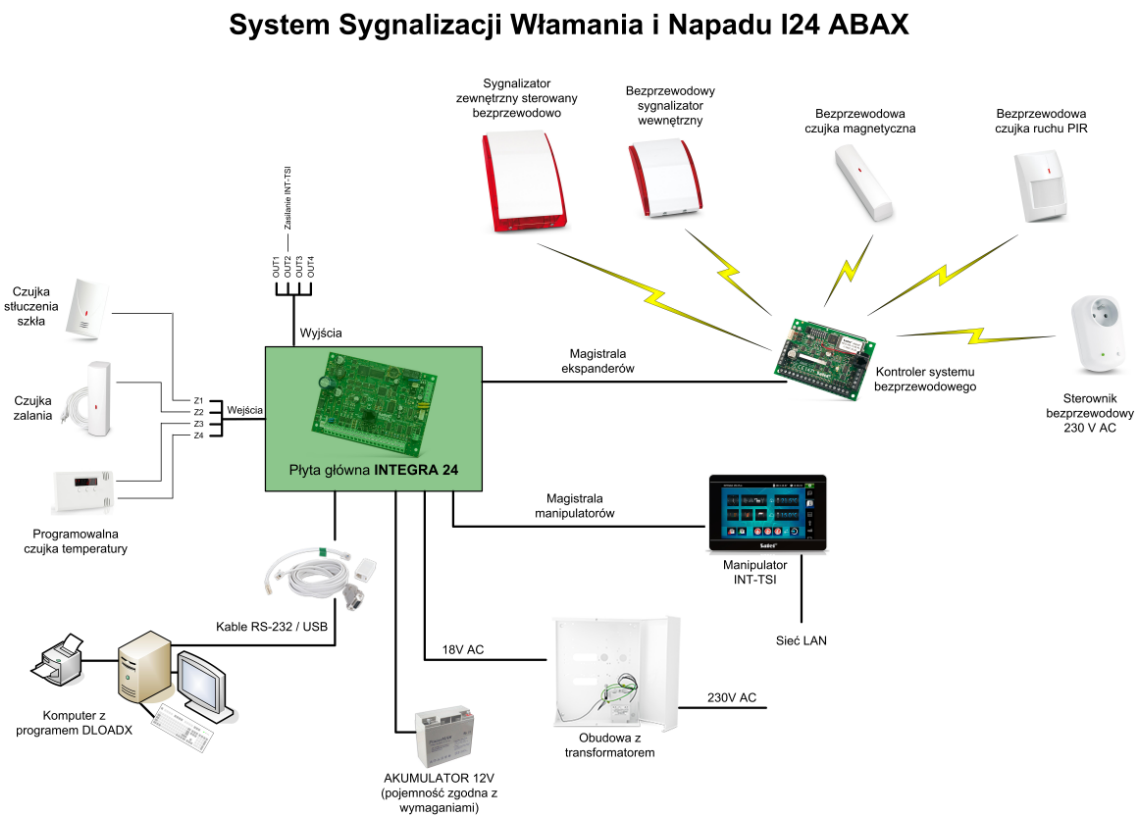
Niezmiernie istotną właściwością z punktu widzenia bezpieczeństwa całego systemu sygnalizacji włamania i napadu opartego na opisywanym urządzeniu jest wirtualna klawiatura manipulatora przeznaczona do wprowadzania haseł użytkowników. Pojawia się ona każdorazowo w innym fragmencie wyświetlacza urządzenia. Ma to na celu uniemożliwienie podjęcia próby częściowego lub całkowitego odgadnięcia sekwencji kodu danego użytkownika poprzez identyfikację śladów palców pozostawionych na szklistej powierzchni ekranu dotykowego.

O ile moduły rozszerzające ilość wejść i wyjść systemu SWiN raczej nie mogą być określane mianem interfejsów, to urządzenie zapewniające komunikację systemu z siecią internetową już z całą pewnością spełniają odpowiednie kryteria. Przykładem takiego rozwiązania może być moduł ETHM-1, który łączy centralę systemu alarmowego wykorzystującą szeregowy protokół komunikacyjny RS-232 z praktycznie dowolnym, przewidzianym do współpracy urządzeniem, które jest przyłączone do sieci Internet. Wygląd przytoczonego interfejsu zaprezentowano na rys. 4.

Rys. 4. Interfejs fizyczny dedykowany do komunikacji między urządzeniami na przykładzie modułu ETHM-1 [3]

Analogicznymi przykładami mogą być moduły umożliwiające integrację i sterowanie elementami wykonawczymi automatyki budynkowej. Podobnie i w tym przypadku opisywany interfejs pełni rolę „tłumacza", dzięki któremu system sygnalizacji włamania i napadu jest w stanie porozumieć się i współpracować z elementami takich systemów jak: KNX, PLC (ang. Programmable Logic Controller), Z-Wave lub Xcomfort.

Do badania opisanych elementów SSWiN posłużyły stanowiska dydaktyczne, wykorzystywane w procesie nauczania studentów Wydziału Elektroniki Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego w Warszawie na specjalności inżynieria systemów bezpieczeństwa [5, 6]. Demonstratory funkcjonują w oparciu o centrale alarmowe z serii Integra. Na rys. 5 przedstawiono schemat blokowy jednego z autorski stanowisk laboratoryjnych SSWiN.



Rys. 5. Schemat blokowy autorskiego stanowiska laboratoryjne SSWiN [opracowanie własne]

Badania przeprowadzone w laboratorium umożliwiają studentom poznanie zasad funkcjonowania i konfiguracji SSWiN. Zwracana jest przy tym szczególna uwaga nie tylko na kwestie związane z projektowaniem, ale także z poziomem bezpieczeństwa

oferowanym przez różnego rodzaju rozwiązania konstrukcyjne. Takie podejście umożliwia opracowywanie nowych koncepcji rozwiązań w interfejsach człowiek – system sygnalizacji włamania i napadu, które cechują się innowacyjnością w zakresie bezpieczeństwa.

4. PODSUMOWANIE I WNIOSKI

W wyniku przeprowadzenia przeglądu wybranych rozwiązań interfejsów człowiek – system sygnalizacji włamania i napadu w aspekcie bezpieczeństwa obiektów można stwierdzić, że obecnie najdynamiczniej rozbudowywany jest segment związany manipulatorami typy tabletowego. Ich stosowanie zwiększa funkcjonalność SSWiN poprzez prezentowanie jednocześnie większej liczby informacji przeznaczonych dla użytkownika. Może powodować jednak podejmowanie przez niedoświadczonych użytkowników decyzji nieadekwatnych do zaistniałych sytuacji.

Obecnie prowadzone są badania nad interfejsami człowiek – system sygnalizacji włamania i napadu w celu opracowania i testowania nowych rozwiązań, ze szczególnym uwzględnieniem bezpieczeństwa i innowacyjności.

Literatura

[1] Będkowski L., Dąbrowski T., *Podstawy eksploatacji, cz. II Podstawy niezawodności eksploatacyjnej*, Wojskowa Akademia Techniczna, Warszawa, 2006.

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

[3] Łukasiak J. M., *Koncepcja zastosowania interfejsów człowiek system w systemach sygnalizacji włamania i napadu*, Praca dyplomowa magisterska, Wojskowa Akademia Techniczna Wydział Elektroniki, Warszawa, 2016.

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

[5] Paś J., Rosiński A., Wiśnios M., Berczyński R., *Stanowisko badawczo-dydaktyczne Systemu Sygnalizacji Włamania i Napadu*, Logistyka nr 6/2014, wyd. Instytut Logistyki i Magazynowania, Poznań, 2014.

[6] Paś J., Rosiński A., Wiśnios M., *Stanowisko badawczo-dydaktyczne bezprzewodowego Systemu Sygnalizacji Włamania i Napadu*, Logistyka nr 6/2015, wyd. Instytut Logistyki i Magazynowania, Poznań, 2015.

[7] PN-EN 50131-1:2009 - Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Część 1: Wymagania systemowe.

[8] Rosinski A., Dąbrowski T., *Modelling reliability of uninterruptible power supply units*, Eksploatacja I Niezawodnosc – Maintenance and Reliability, Vol.15, No. 4, 2013.

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

[10] Siergiejczyk M., Rosinski A., *Reliability analysis of electronic protection systems using optical links*, the monograph „Dependable Computer Systems", editors: Wojciech Zamojski, Janusz Kacprzyk, Jacek Mazurkiewicz, Jarosław Sugier and Tomasz Walkowiak, given as the monographic publishing series – „Advances in intelligent and soft computing", Vol. 97. Springer-Verlag, Berlin Heidelberg, 2011.

[11] Szulc W., Rosiński A., *Systemy sygnalizacji włamania. Część 1 – Konfiguracje central alarmowych*, Zabezpieczenia Nr 2(66)/2009, wyd. AAT, Warszawa, 2009.

[12] Szulc W., Rosiński A., *Wybrane zagadnienia z elektroniki cyfrowej dla informatyków (część II – cyfrowa)*, Wydawnictwo Wyższej Szkoły Menedżerskiej w Warszawie, Warszawa, 2012.

[13] Szulc W., Rosiński A., *Wybrane zagadnienia z miernictwa i elektroniki dla informatyków (część I – analogowa)*, Oficyna Wydawnicza WSM, Warszawa, 2012.

GRAPHIC KEYPAD IN INTRUSION ALARM SYSTEMS

Abstract

Intruder alarm systems (SSWiN) can be classified into the electronic security systems group. Mentioned solutions have recently become very popular in wide range of buildings, both public and private. Therefore many specialized solutions to interfaces have been being implemented for last years. The article presents the functional

requirements of SSWiN, followed by a review of selected solutions to interfaces for human – intrusion alarm systems interaction.

Key words: electronic security system, interfaces, security

Artykuł opracowany na podstawie referatu wygłoszonego na XXX Międzynarodowej Konferencji Naukowo-Technicznej „Ekomilitaris 2016" Zakopane, 13-16.09.2016 r.

Praca finansowana w ramach działalności statutowej Wydziału Transportu Politechniki Warszawskiej.