Rozległy i rozproszony elektroniczny system bezpieczeństwa w aspekcie zarządzania danymi

Waldemar Szulc

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

Abstract: W artykule przedstawiono istotne problemy dotyczące nadzoru i zarządzania dużym elektronicznym systemem bezpieczeństwa, jak również zarządzania danymi istotnymi z punktu widzenia prawidłowej pracy rozległego i rozproszonego systemu. Autor zbudował również niezawodnościowo-eksploatacyjny model, w którym uwzględnił tunel SSH dla podniesienia bezpieczeństwa zarządzanymi danymi drogami informatycznymi. Dokonano również analizy matematycznej tego modelu. Autor wykonał wiele badań długofalowych, które umożliwią określenie istotnych wskaźników eksploatacyjnych i niezawodnościowych, tak ważnych dla prawidłowego funkcjonowania elektronicznego systemu bezpieczeństwa w aspekcie zarządzania danymi.

Słowa kluczowe: elektroniczny system bezpieczeństwa, internet, niezawodność

1. Wprowadzenie

Zaprojektowanie oraz realizacja rozproszonego Systemu Sygnalizacji Włamania i Napadu (SSWiN) dla dużego rozległego obiektu wymaga sporej wiedzy technicznej, jak również dużego doświadczenia. Istnieją obiekty, w których ze względów ekonomicznych, jak i logistycznych propozycja okablowania strukturalnego, a więc budynku inteligentnego stają się trudne do zrealizowania. Może więc wchodzić w rachubę integracja mniejszych systemów. Szczególnie trudne w realizacji są obiekty, które są eksploatowane ze stochastyczną intensywnością. Można więc zaprojektować SSWiN złożony z kilku central, np. o pojemności 128 linii dozorowych każda, i jeśli to możliwe, integrować je. Z analizy różnych systemów wynika, że niewiele typów central alarmowych można ze sobą łączyć, a więc integrować. Ponadto, nie zawsze jest to konieczne. Ze względów logistycznych można zastosować kilka central alarmowych o sporej liczbie linii dozorowych, które będą obsługiwać np. określone fragmenty obiektu, a więc każda z central będzie posiadała własny manipulator, za pomocą którego będzie można realizować określone funkcje systemu wynikające z potrzeb.

Takie rozwiązanie przyjęto w jednym z dużych i rozległych obiektów użyteczności publicznej, które stało się swoistym rodzajem rzeczywistego poligonu doświadczalnego. W obiekcie zastosowano siedem central rozproszonych produkcji polskiej typu INTEGRA 128. Tak zbudowany system to 896 punktów dozoru wewnętrznego i zewnętrznego. Do dyspozycji użytkowników obiektu producent przewidział 32 strefy dla jednej centrali alarmowej, tworzącej niezależny podsystem. Ze względu na charakter użytkowania tego naukowo-dydaktycznego obiektu oraz mimo bardzo dużej złożoności SSWiN, przyjęto generalną zasadę uproszczenia do minimum sposobu obsługi części systemu (podsystemu) przez użytkowników. Dokonano analizy liczby stref niezbędnych do prawidłowego funkcjonowania poszczególnych central. Przyjęto zasadę, że dany fragment SSWiN (podsystem) ma minimum jeden własny manipulator z wyświetlaczem LCD i klawiaturą do wprowadzania PIN-kodów, np. użytkownika. Każdy manipulator jest wyposażony również w czytnik kart magnetycznych. Karcie magnetycznej przyporządkowano ściśle określonego użytkownika dla jego łatwej identyfikacji oraz określone strefy, do których użytkownik ma dostęp. Można więc w dwojaki sposób kodować bądź dekodować daną strefę lub strefy dozorowe: przez wprowadzenie PIN-kodu użytkownika lub za pomocą karty magnetycznej. W pomieszczeniach recepcji obiektu zostały zainstalowane tablice synoptyczne, na których istnieje informacja o aktualnym stanie stref oraz stanie wybranych linii dozorowych całego SSWiN. Elementami informującymi obsługę o stanie linii dozorowych na tablicach synoptycznych są dwukolorowe diody LED. Odpowiednio zaprogramowana sekwencja świecenia diod daje pełną informację o stanie stref oraz stanie wybranych linii dozorowych, i tak przykładowo: kolor *zielony* to informacja, że dana strefa jest zakodowana, kolor *czerwony pulsujący* oznacza, że wystąpił alarm włamaniowy, wynikający z naruszenia czujki danego pomieszczenia (strefy), *czerwony ciągły* alarm pożarowy, wynikający z naruszenia optycznej czujki dymowej w danego pomieszczenia, brak świecenia diody LED oznacza, że dana strefa jest zdekodowana. Dodatkowo, informacje o wystąpieniu alarmu w danej konkretnej centrali alarmowej (podsystemie) są przesyłane drogą radiową do centrali C-7, która jest centralą odpowiedzialną za monitoring zewnętrzny oraz alarm głośny w pomieszczeniu recepcyjnym, czynnym 24 godz./dobę. Jest to jakby pierwszy stopień monitorowania SSWiN. Jest jeszcze drugi stopień monitorowania o wystąpieniu zagrożenia. Po godz. 22^{00} automatyczne centrala C-7 ma możliwość przekazywania informacji o alarmie drogami komutowanymi (przez własną sieć telekomunikacyjną) lub drogami radiokomunikacyjnymi (także własna sieć radiokomunikacyjna) do Straży chroniącej fizycznie bardzo rozległy kompleks obiektów. Ochrona, po zweryfikowaniu alarmu z opisywanego obiektu, wysyła patrole

interwencyjne. Warto również nadmienić, że ze względu na bardzo rozbudowany SSWiN autorzy bardzo starannie dobrali rezerwowe źródła zasilania (wynika to z bilansu energetycznego). Na rys. 1 przedstawiono rozproszony SSWiN złożony z 7 jednostek mikroprocesorowych typu INTEGRA 128, do których za pośrednictwem magistral transmisyjnych dołączono wiele różnych modułów. Cały system SSWiN za pośrednictwem modemów ETHM, przez sieć LAN, współpracuje z serwerem umożliwiającym zarządzanie i administrowanie tak bardzo złożonym systemem bezpieczeństwa. System bezpieczeństwa, złożony z 7 niezależnych central alarmowych, nie jest połączony ze sobą w sposób galwaniczny. Tak więc, każdy z 7 podsystemów centralowych, chroniących elektronicznie określone kondygnacje, może pracować niezależnie.

Tak zbudowany system bezpieczeństwa tworzy model niezawodnościowy równoległy. Każdy z podsystemów może być zarządzany z klawiatury LCD w sposób niezależny. Ponadto każda z w/w central ma gniazdo RJ do współpracy z komputerem po RS-232. Taka konfiguracja umożliwia indywidualne zarządzanie podsystemem (jednym z siedmiu) a więc programowanie centrali zgodnie z potrzebami danej kondygnacji. Umożliwia również wizualizację wszystkich stanów, w jakim jest aktualnie podsystem. Istnieje możliwość informatycznego zdalnego zarządzania i nadzoru tak dużego systemu. Muszą być jednak spełnione ściśle określone kryteria bezpieczeństwa wynikające z przepisów normatywnych (PN-EN). W związku z nową konfiguracją, powstał duży rozproszony elektroniczny system bezpieczeństwa chroniący obiekt o charakterze rozległym. System został zaprojektowany w 2006 r. i starannie przez ten okres był obserwowany. Stanowi nowum w obszarze integracji elektronicznych systemów bezpieczeństwa. Przez ten okres autor zbierał dane o charakterze niezawodnościowo-eksploatacyjnym. Warto więc dokonać analizy dotyczącej zarządzania całym systemem bezpieczeństwa oraz jego podsystemami.

2. Konfiguracja rozproszonego SSWiN dla dużego rozległego obiektu oraz założenia

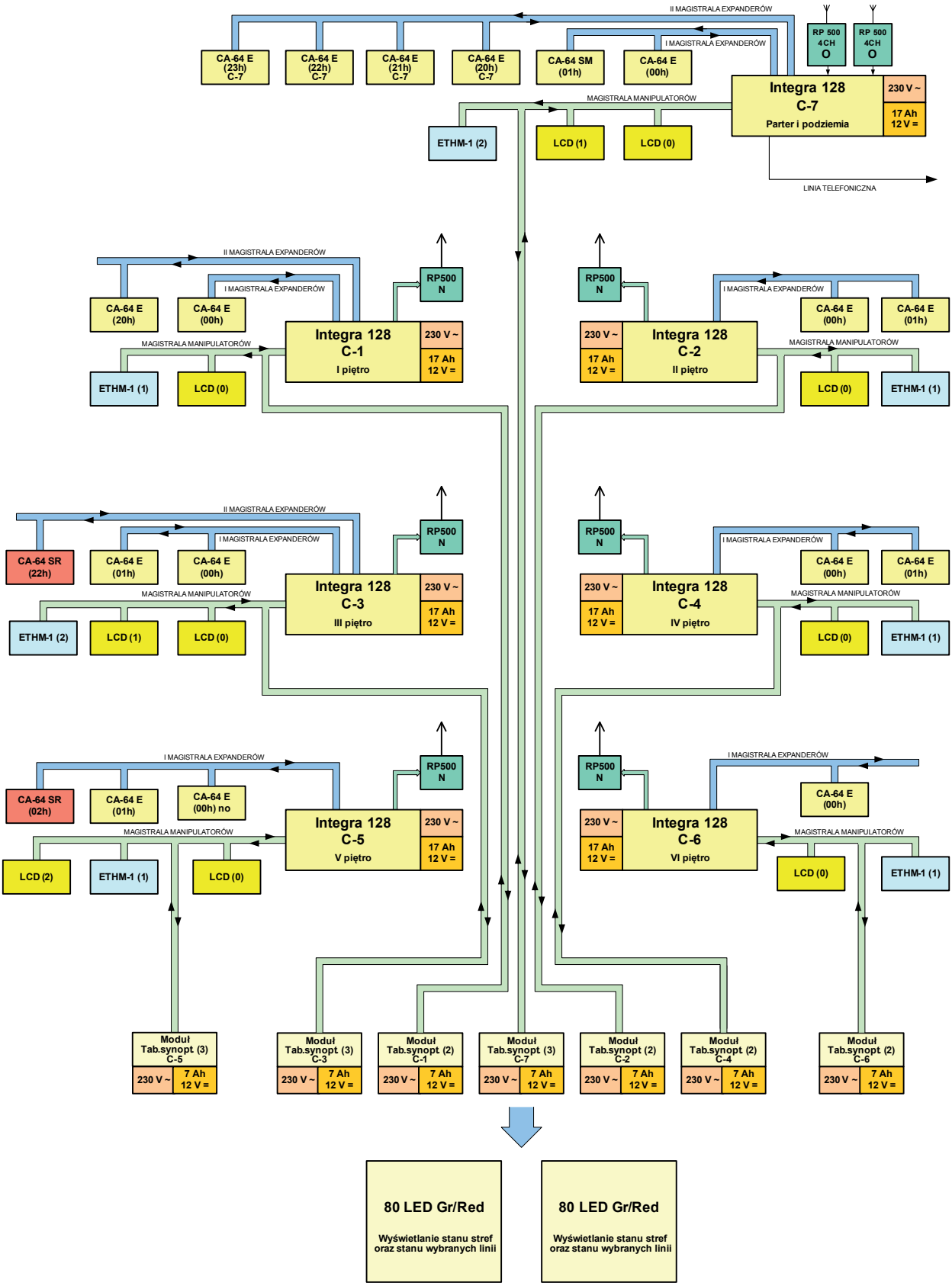
W trakcie projektowania oraz późniejszej realizacji rozproszonego sytemu bezpieczeństwa autor przyjął następujące założenia:

a) obiekt, w którym ma być realizowany SSWiN, jest obiektem rozległym o kilku piętrach,
b) konfiguracja SSWiN ma charakter rozproszony i ma być wielocentralowym systemem bezpieczeństwa,
c) maksymalna liczba linii dozorowych (perspektywiczna) wynosi 896, w pierwszym etapie liczba linii dozorowych wynosiła 240,
d) maksymalna ilość central typu INTEGRA 128 wynosi 7 (od C-1 do C-7); są one zlokalizowane na różnych piętrach obiektu, również na tych piętrach rozmieszczono klawiatury sterujące wraz z czytnikami kart,
e) liczba stref w jednym systemie bezpieczeństwa nie przekroczy 32,
f) system bezpieczeństwa umożliwia realizację lokalnej kontroli dostępu,
g) system pracuje przez 24 godziny, ze szczególnym uwzględnieniem pracy między godz. 7^{00} a 22^{00},
h) kategoria zagrożeń: zgodnie z kategorią III (dawne Z3),
i) klasa SSWiN to kategoria III, (dawne SA3),
j) kategoria sprzętowa związana z kategorią III,
k) system bezpieczeństwa (zaprojektowany i zrealizowany) jest monitorowany minimum jedną drogą (do godz. 22^{00} i dwoma drogami po godz. 22^{00}),
l) system bezpieczeństwa musi mieć minimum 7 klawiatur z 7 czytnikami kart magnetycznych (zintegrowane klawiatury zlokalizowane na piętrach, tak aby użytkownicy mieli łatwy dostęp w godz. od 7^{00} do 22^{00}),
m) system bezpieczeństwa ma lokalną kontrolę dostępu z czytnikami kart magnetycznych w wybranych pomieszczeniach,
n) system bezpieczeństwa jest wyposażony w tablice synoptyczne z awaryjnym źródłem zasilania, zlokalizowane w pomieszczeniach recepcyjnych dla klarownej wizualizacji zaistniałych zdarzeń,
o) każda z central INTEGRA 128 powinna być wyposażona w moduł (modem) ETHM do współpracy z serwerem przez sieć LAN do administrowania i zarządzania SSWiN; każdej z central alarmowych nadano adres IP,
p) system bezpieczeństwa zaprojektowany i zrealizowany, wyposażono w rezerwowe źródła zasilania tak, aby w razie zaniku zasilania zasadniczego (230 V) SSWiN mógł pracować przez ok. 40 godz.,
q) system bezpieczeństwa SSWiN jest wspomagany przez 32 kamery telewizyjne (zewn. i wewn.), z zapisem zdarzeń na HDD z możliwością podglądu po lokalnych sieciach internetowych,
r) wszystkie zdarzenia zaistniałe w trakcie eksploatacji tak dużego systemu bezpieczeństwa są rejestrowane w pamięciach central, na drukarkach systemowych oraz w pamięci HDD centralnego komputera,
s) został również przewidziany obwodowy system ochrony obiektu, który został dołączony do centrali C-7.

3. Syntetyczny opis budowy rozproszonego systemu bezpieczeństwa dla dużego obiektu

Na rys. 1 przedstawiono uproszczony schemat blokowy rozproszonego elektronicznego systemu bezpieczeństwa dla dużego obiektu. SSWiN został zaprojektowany w oparciu o jednostkę mikroprocesorową typu INTEGRA 128 produkcji polskiej. Za pośrednictwem linii dozorowych wprost do płyty głównej zostały dołączone czujki usytuowane blisko central alarmowych (np. na określonym piętrze i korytarzu), w tym system obwodowy chroniący obiekt na zewnątrz. Pomieszczenia odległe od central alarmowych są obsługiwane za pośrednictwem modułów typu CA-64E (ekspandery wejść).

Każda z central alarmowych została wyposażona w manipulator (klawiatura z wyświetlaczem LCD oraz wewn. czytnikiem kart magnetycznych). Manipulatory zostały zlokalizowane na korytarzach kolejnych pięter obiektu w widocznych miejscach i zabezpieczone mechanicznie (obudowy metalowe zamykana na zamek patentowy).



Rys.1. Uproszczony schemat blokowy elektronicznego rozproszonego systemu bezpieczeństwa dla dużego obiektu
Fig. 1. Simplified block diagram of a dispersed electronic security system for a large object

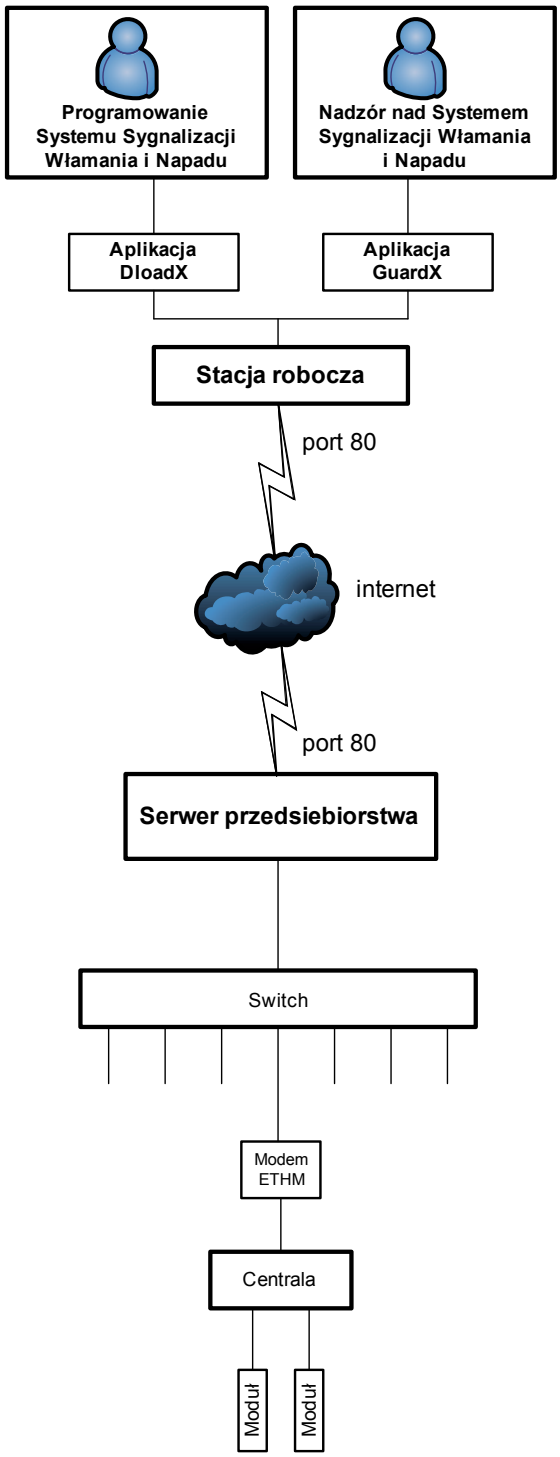
Lokalizacja tych manipulatorów została starannie dobrana tak, aby w możliwie prosty sposób upoważniony użytkownik danego piętra mógł dekodować lub kodować określone strefy chroniące pomieszczenia, do których posiada uprawnienia. Użytkownik tę czynność może wykonywać w dwojaki sposób: używając przydzielonego PIN-kodu lub karty magnetycznej, przynależnej użytkownikowi. Oba sposoby kodowania bądź dekodowania stref są tożsame.

Centrala C-7 pełni dodatkową, w pewnym sensie integracyjną rolę w rozproszonym SSWiN. Każda z central (od CA-1 do CA-6) została uzbrojona w wielokanałowy nadajnik typu RP-500N (zasięg wynoszący 500 m w otwartej przestrzeni), transmitujący drogą radiową sygnał alarmowy właśnie do centrali C-7, która wyposażona w dwa radiowe czterokanałowe odbiorniki sygnalizuje alarm z poszczególnych podsystemów. Do centrali C-7 został dołączony moduł CA-64 SM (ekspander syntezerów mowy umożliwiający nagranie do 16 komunikatów słownych). Moduł CA-64SM umożliwia wysyłanie 15 sekundowych komunikatów słownych wykorzystywanych do powiadamiania telefonicznego o zdarzeniach w systemie bezpieczeństwa, np. o alarmach włamaniowych, alarmach napadowych, alarmach pożarowych, sabotażach, awariach (w szczególności zasilania głównego i rezerwowego) itp. Tylko centrala C-7 jest połączona przez wewnętrzny dialer z lokalną siecią telefoniczną. Centrala C-7 obsługuje również system ochrony obwodowej (bariery aktywne IR, bariery zewnętrzne PIR oraz zewn., czujki PIR). Manipulatory, ze względu na logistykę obiektu, znajdują się w pomieszczeniach recepcyjnych (dot. centrali alarmowej C-7). Do centrali C-7 (lub jej modułów) dołączone są linie dozorowe, bardzo starannie wyselekcjonowane z punktu widzenia uprawnień użytkowników.

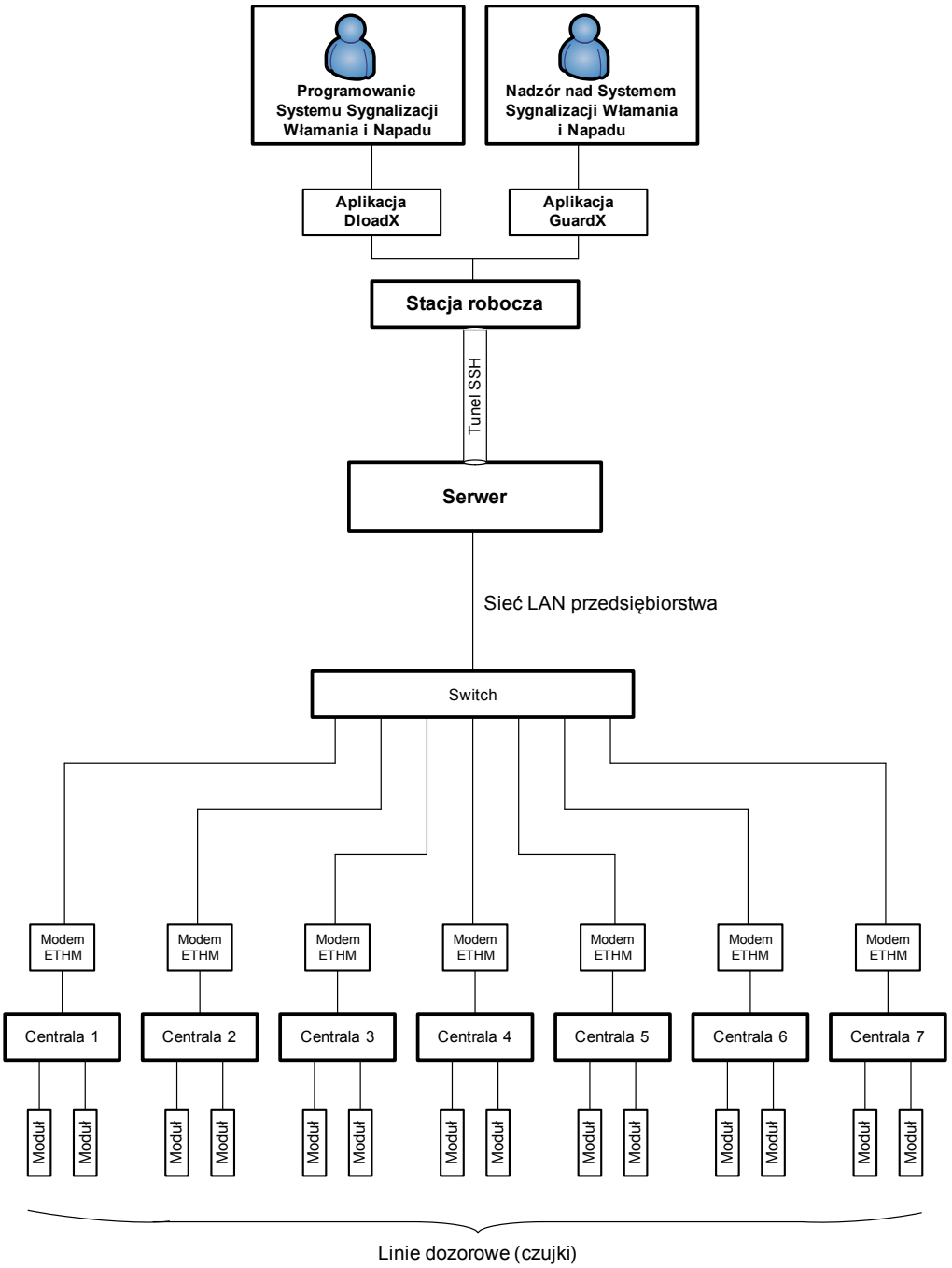
Również pewnym wyjątkiem są centrale alarmowe C-3 i C-5, do których dołączono dwa manipulatory – klawiatury (LCD-0 i LCD-1) wraz z czytnikami kart magnetycznych. W obu przypadkach za pośrednictwem magistral transmisyjnych (poza klasycznymi modułami rozszerzającymi typu CA-64E) zostały dołączone moduły CA -64SR (ekspandery czytników kart zbliżeniowych), które współpracują z lokalną kontrolą dostępu przeznaczoną dla pomieszczeń szczególnie chronionych. Drzwi wejściowe do części chronionej przez centrale C-3 i C-5 współpracują z ryglami elektromagnetycznymi, które są sterowane przez moduły CA-64SR. Z modułami typu CA-64SR współpracują czytniki kart zbliżeniowych typu CZ-EMM (zamontowane obok drzwi wejściowych). Moduł ten może współpracować z 1 lub 2 czytnikami kart zbliżeniowych (magnetycznych). Powyższe pomieszczenia to pomieszczenia o specjalnym przeznaczeniu, również nadzorowane za pośrednictwem kamer telewizyjnych.

Centrale alarmowe typu INTEGRA 128 zostały w obiekcie zainstalowane w miejscach trudnodostępnych dla osób postronnych. Każda z central poza zasilaniem głównym (230 V) została wyposażona w źródło rezerwowe w postaci akumulatora żelowego o pojemności 17 Ah. Dobór pojemności akumulatorów wynika z obliczeń bilansu energetycznego.

Zdarzenia z central alarmowych drogą kablową (po magistrali transmisyjnej) docierają do modułów tablic synoptycznych CA-64 PTSA, które sterują dwukolorowymi diodami LED. Moduły CA-64 PTSA oraz tablice z diodami LED są umieszczone w pomieszczeniu recepcji na parterze budynku. Na tablicy synoptycznej zapala się LED czerwony (sygnalizuje alarm w określonej strefie). Jak już wspomniano, tablice synoptyczne (2 szt.) zawierające po



Rys. 2. Przykład połączenia użytkownika z jedną centralą przez niezabezpieczoną sieć Internet
Fig. 2. Example of connection of the user with one central over an insecure Internet network



Rys. 3. Przykład połączenia użytkownika z centralami przez sieć LAN, z wykorzystaniem protokołu SSH (ang. *Secure Shell*)
Fig. 3. Example of connection of the user with the centrals via LAN net using SSH protocol

80 dwukolorowych diod LED wyświetlających stany 224 stref dozorowych całego SSWiN oraz aktualny stan specjalnie wybranych 96 linii dozorowych (takich jak: linie pożarowe, zewnętrzne, napadowe, 24-godzinne). Moduły tablic synoptycznych CA-64 PTSA, poza własnym zasilaniem zasadniczym (230 V), zostały wyposażone w akumulatory rezerwowe o pojemnościach 7 Ah (pojemność obliczona na podstawie bilansu energetycznego).

4. Zdalna obsługa rozproszonego systemu SSWiN oraz nadzór i administracja danych

Rozproszony System SWiN opisywany wcześniej, ze względu na wiele autonomicznych podsystemów (centrale C-1 do C-7) o dużej złożoności, musi być poddawany okresowym przeglądom i obsłudze serwisowej dla zapewnienia wyso-

kiego poziomu gotowości. Obsługa serwisowa takiego systemu wymaga od serwisantów sporo wysiłku i czasu. Serwisant musi podłączyć komputer do każdego podsystemu w celu dokonania podstawowego przeglądu serwisowego.

Dlatego też SSWiN, składający się z siedmiu podsystemów opartych na jednostkach centralnych INTEGRA 128 firmy Satel, wyposażono w moduły ethernetowe ETHM, które umożliwiają obsługę serwisową oraz nadzór i administrację przez LAN lub przez Internet.

Przykład połączenia „Administratora Systemu" z jedną centralą „INTEGRA 128" przez niezabezpieczoną sieć Internet został przedstawiony na rys. 2. W trakcie eksploatacji elektronicznego systemu bezpieczeństwa przedstawionego na rys. 1 stwierdzono szereg prób „włamania" do systemu. To bardzo poważne zagrożenie dla poprawnej i bezpiecznej pracy tak skomplikowanego systemy bezpieczeństwa. Warto dokonać analizy dotyczącej pracy tak skonfigurowanego systemu bezpieczeństwa.

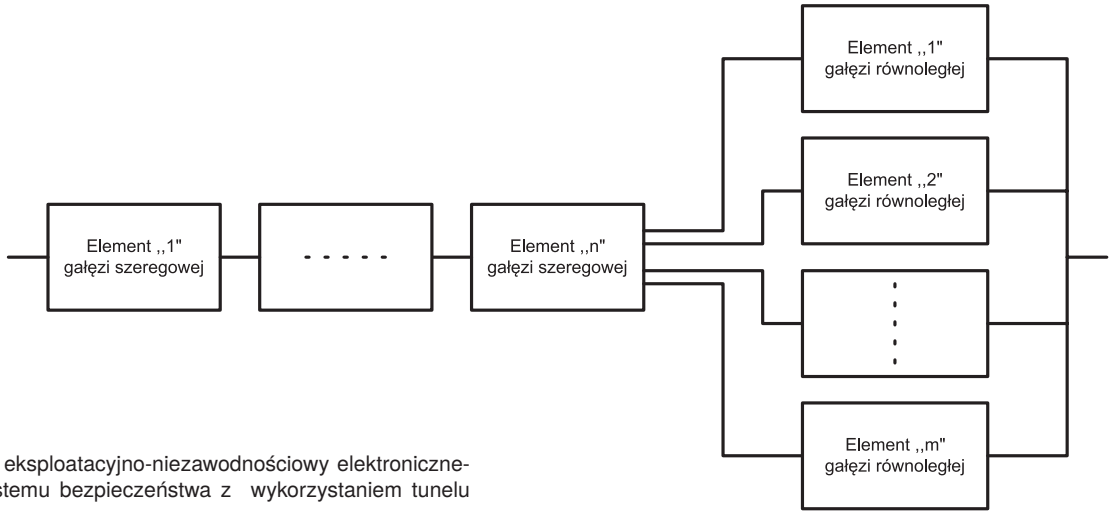
W celu nawiązania połączenia przez Administratora Systemu przesyłane są informacje przez niezabezpieczoną sieć Internet do modemu ETHM. Producent wyposażył modem ETHM w 12-znakowy alfanumeryczny klucz, który porównywany jest z kluczem wysyłanym przez zdalnego administratora. Jednak ze względu na niezabezpieczoną sieć istnieje możliwość podsłuchania transmisji lub przechwycenie klucza. Dla bezpieczeństwa należy także zachować pewien margines nieuczciwości instalatorów systemu.

W przypadku kiedy zdalne zarządzanie i administrowanie odbywa się wewnątrz sieci LAN, niebezpieczeństwo podsłuchu lub ataku jest zdecydowanie mniejsze, ale nadal istnieje. Chcąc wykluczyć dostęp osób nieuprawnionych do nadzorowanego i zarządzanego zdalnie SSWiN przez sieć LAN przedsiębiorstwa, zastosowano środki bezpieczeństwa na poziomie połączenia administratora systemu (klienta) z poszczególnymi podsystemami rozproszonego SSWiN. Po wielu próbach, został dodatkowo wprowadzony tunel SSH.

Rozwiązaniem problemu zagrożenia podsłuchem (ang. *sniffing*) jest zastosowanie tunelu (ang. *tunelling*) wykorzystując program SSH (ang. *Secure Shell*). Na rys. 3 przedstawiono przykład połączenia „Administratora Systemu" z centralami alarmowymi INTEGRA 128 przez sieć LAN z wykorzystaniem tunelu SSH. Jest to dość proste, a zarazem skuteczne rozwiązanie. Cała operacja polega na utworzeniu szyfrowanego połączenia tam, gdzie sieć jest najbardziej narażona na atak, czyli wtedy, gdy dane są przesyłane przez sieć, której nie można kontrolować (np. Internet). Programy służące do nadzoru, serwisu i administracji, zamiast połączyć się ze zdalnym serwerem, np. przez Internet (port 80), łączą się z lokalnym komputerem (klient), wykorzystując port (najczęściej 22), na którym czuwa tunel SSH. Na tym odcinku połączenia dane są przesyłane w sposób jawny, lecz nie może być tutaj mowy o podsłuchiwaniu. Natomiast połączenie klient–serwer jest już szyfrowane. Tunel SSH na serwerze, z którym jesteśmy połączeni, przekazuje dane do właściwego portu na tym właśnie serwerze, dalej przez ściśle określone porty elementów sieci LAN przedsiębiorstwa do modułów ethernetowych podsystemów SSWiN. Na tym odcinku dane nie są kodowane, lecz jeśli korzystamy z danej usługi na serwerze, z którym łączymy się właśnie poprzez tunel z wykorzystaniem SSH, możemy czuć się bezpieczni.

Zasada działania protokołu SSH opiera się na kryptograficznej technologii RSA (nazwa RSA jest akronimem utworzonym z pierwszych liter nazwisk jego twórców). Każdy z komputerów, na którym zainstalowane jest oprogramowanie SSH, ma parę kluczy: tzw. klucz prywatny, dostępny tylko dla administratora komputera (i oczywiście oprogramowania systemowego obsługującego protokół SSH) oraz klucz publiczny dostępny dla wszystkich użytkowników sieci. Klucze te są tak zbudowane, że informację zaszyfrowaną kluczem prywatnym można rozszyfrować tylko przy pomocy klucza publicznego i odwrotnie – informację zaszyfrowaną kluczem publicznym można rozszyfrować wyłącznie przy pomocy klucza prywatnego. Klucze są więc ze sobą powiązane, ale żadnego z nich nie można odtworzyć na podstawie znajomości drugiego. Połączenie SSH inicjowane jest po stronie programu – klienta SSH. Klient łączy się z serwerem i otrzymuje od niego jego klucz publiczny.

Klucz ten porównywany jest z zachowanym w wewnętrznej bazie danych klienta z poprzednich połączeń. Następnie klient przekazuje serwerowi swój klucz publiczny, generuje losową 256-bitową liczbę, szyfruje ją swoim kluczem prywatnym oraz kluczem publicznym serwera. Serwer po otrzymaniu tak zakodowanej liczby rozszyfrowuje ją swo-



Rys. 4. Model eksploatacyjno-niezawodnościowy elektronicznego systemu bezpieczeństwa z wykorzystaniem tunelu SSH

Fig. 4. Model operational - reliability of electronic security system with using of the SSH tunnel

im kluczem prywatnym i kluczem publicznym klienta. Tak otrzymana liczba jest losowa, znana tylko klientowi i serwerowi. Jest ona używana jako klucz do kodowania podczas dalszej komunikacji. Ze względu na duża komplikację elektronicznego systemu bezpieczeństwa, warto zastanowić się również nad modelem eksploatacyjno-niezawodnościowym tego skomplikowanego układu. Na rys 4 przedstawiono model eksploatacyjno-niezawodnościowy elektronicznego systemu bezpieczeństwa, z wykorzystaniem tunelu SSH. Charakter tego układu jest mieszany a struktura niezawodnościowa jest równoległo-szeregowa.

5. Analiza niezawodnościowo--eksploatacyjna rozproszonego SSWiN

W wyniku analizy schematu systemu SWiN przedstawionego na rys. 3, opracowano model eksploatacyjno-niezawodnościowy (rys. 4).

Uszkodzenie któregoś z elementów (stacja robocza, serwer, switch) znajdujących się w gałęzi szeregowej (n = 3) struktury powoduje przejście systemu ze stanu pełnej zdatności $R_O(t)$ do stanu zawodności bezpieczeństwa $Q_B(t)$. Uszkodzenie którejś z central (m = 7), znajdujących się w gałęzi równoległej struktury, powoduje przejście ze stanu pełnej zdatności $R_O(t)$ do stanu zagrożenia bezpieczeństwa $Q_{ZB}(t)$. Przeprowadzając analizę, można podać następujące równania Kołmogorowa-Chapmana opisujące rozpatrywany system:

$$R_0'(t) = -\lambda_B \cdot R_0(t) - \lambda_{ZB1} \cdot R_0(t)$$
$$Q_{ZB1}'(t) = \lambda_{ZB1} \cdot R_0(t) - \lambda_{ZB2} \cdot Q_{ZB1}(t)$$
$$Q_{ZB2}'(t) = \lambda_{ZB2} \cdot Q_{ZB1}(t) - \lambda_{ZB3} \cdot Q_{ZB2}(t)$$
$$\ldots$$
$$Q_{ZBm-1}'(t) = \lambda_{ZBm-1} \cdot Q_{ZBm-2}(t) - \lambda_{ZBm} \cdot Q_{ZBm-1}(t)$$
$$Q_B'(t) = \lambda_B \cdot R_0(t) + \lambda_{ZBm} \cdot Q_{ZBm-1}(t)$$

Przyjmując warunki początkowe:

$$R_0(0) = 1$$
$$Q_{ZB1}(0) = Q_{ZB2}(0) = \ldots = Q_{ZBm-1}(0) = Q_B(0) = 0$$

i stosując określone przekształcenia wyznaczono:

$$R_0(t) = e^{-(\lambda_B + \lambda_{ZB1})\cdot t}$$

$$Q_{ZB1}(t) = \lambda_{ZB1} \cdot \left[\frac{e^{-(\lambda_B+\lambda_{ZB1})\cdot t} - e^{-\lambda_{ZB2}\cdot t}}{\lambda_{ZB2} - \lambda_B - \lambda_{ZB1}} \right]$$

$$Q_{ZB2}(t) = \lambda_{ZB1} \cdot \lambda_{ZB2} \cdot \left[\begin{array}{l} \dfrac{e^{-(\lambda_B+\lambda_{ZB1})\cdot t}}{(\lambda_B+\lambda_{ZB1}-\lambda_{ZB3})\cdot(\lambda_B+\lambda_{ZB1}-\lambda_{ZB2})} - \\ - \dfrac{e^{-\lambda_{ZB2}\cdot t}}{(\lambda_B+\lambda_{ZB1}-\lambda_{ZB2})\cdot(\lambda_{ZB2}-\lambda_{ZB3})} + \\ + \dfrac{e^{-\lambda_{ZB3}\cdot t}}{(\lambda_{ZB2}-\lambda_{ZB3})\cdot(\lambda_B+\lambda_{ZB1}-\lambda_{ZB3})} \end{array} \right]$$

$$Q_{ZBm-1}(t) = \lambda_{ZB1} \cdot \lambda_{ZB2} \cdot \ldots \cdot \lambda_{ZBm-1} \cdot (-1)^{m+1} \cdot$$
$$\cdot \left[\begin{array}{l} \dfrac{e^{-(\lambda_B+\lambda_{ZB1})\cdot t}}{(\lambda_B+\lambda_{ZB1}-\lambda_{ZB2})\cdot(\lambda_B+\lambda_{ZB1}-\lambda_{ZB3})\cdot\ldots\cdot(\lambda_{B1}+\lambda_{ZB2}-\lambda_{ZBm})} + \\ + \dfrac{e^{-\lambda_{ZB2}\cdot t}}{(\lambda_{ZB2}-\lambda_B-\lambda_{ZB1})\cdot(\lambda_{ZB2}-\lambda_{ZB3})\cdot\ldots\cdot(\lambda_{ZB2}-\lambda_{ZBm})} + \ldots + \\ + \dfrac{e^{-\lambda_{ZBm}\cdot t}}{(\lambda_{ZBm}-\lambda_B-\lambda_{ZB1})\cdot(\lambda_{ZBm}-\lambda_{ZB2})\cdot\ldots\cdot(\lambda_{ZBm}-\lambda_{ZBm-1})} \end{array} \right]$$

$$Q_B(t) = \frac{\lambda_B}{\lambda_B + \lambda_{ZB1}} \cdot \left[1 - e^{-(\lambda_B+\lambda_{ZB1})\cdot t}\right] + \lambda_{ZB1} \cdot \lambda_{ZB2} \cdot \ldots \cdot \lambda_{ZBm-1} \cdot \lambda_{ZBm} \cdot$$
$$\cdot \left[\begin{array}{l} (-1)^m \cdot \left(\begin{array}{l} \dfrac{e^{-(\lambda_B+\lambda_{ZB1})\cdot t}}{(\lambda_B+\lambda_{ZB1})\cdot(\lambda_B+\lambda_{ZB1}-\lambda_{ZB2})\cdot(\lambda_B+\lambda_{ZB1}-\lambda_{ZB3})\cdot\ldots\cdot(\lambda_B+\lambda_{ZB1}-\lambda_{ZBm-1})(\lambda_B+\lambda_{ZB1}-\lambda_{ZBm})} + \\ + \dfrac{e^{-\lambda_{ZB2}\cdot t}}{(\lambda_{ZB2}-\lambda_B-\lambda_{ZB1})\cdot\lambda_{ZB2}\cdot(\lambda_{ZB2}-\lambda_{ZB3})\cdot\ldots\cdot(\lambda_{ZB2}-\lambda_{ZBm-1})(\lambda_{ZB2}-\lambda_{ZBm})} + \ldots + \\ + \dfrac{e^{-\lambda_{ZBm-1}\cdot t}}{(\lambda_{ZBm-1}-\lambda_B-\lambda_{ZB1})\cdot(\lambda_{ZBm-1}-\lambda_{ZB2})\cdot(\lambda_{ZBm-1}-\lambda_{ZB3})\cdot\ldots\cdot\lambda_{ZBm-1}\cdot(\lambda_{ZBm-1}-\lambda_{ZBm})} + \\ + \dfrac{e^{-\lambda_{ZBm}\cdot t}}{(\lambda_{ZBm}-\lambda_B-\lambda_{ZB1})\cdot(\lambda_{ZBm}-\lambda_{ZB2})\cdot(\lambda_{ZBm}-\lambda_{ZB3})\cdot\ldots\cdot(\lambda_{ZBm}-\lambda_{ZBm-1})\cdot\lambda_{ZBm}} \end{array} \right) + \\ + \dfrac{1}{(\lambda_B+\lambda_{ZB1})\cdot\lambda_{ZB2}\cdot\lambda_{ZB3}\cdot\ldots\cdot\lambda_{ZBm-1}\cdot\lambda_{ZBm}} \end{array} \right]$$

Otrzymane zależności pozwalają na wyznaczenie prawdopodobieństw przebywania systemu w stanach pełnej zdatności R_O, zagrożenia bezpieczeństwa Q_{ZB} i zawodności bezpieczeństwa Q_B.

6. Zakończenie

Zaproponowany i zrealizowany przez autora SSWiN dla potrzeb rozległego obiektu wraz z jego systemem zarządzania i administrowania danych to dosyć trudne zadanie z punktu widzenia eksploatacyjno-niezawodnościowego. Stąd autor przedstawił model niezawodnościowo-eksploatacyjny tego złożonego systemu bezpieczeństwa wraz z równaniami dla obliczenia niezawodności R_S. Problematyka dotycząca rozproszonych systemów bezpieczeństwa wraz z matematyczną analizą eksploatacyjno-niezawodnościową, była przez autora poruszana w dwumiesięczniku „Zabezpieczenia" Nr 1(47) w 2006 r. Jest to problem skomplikowany i wymagający długofalowych badań. Aktualnie są zbierane dane i z całą pewnością zostanie obliczo-

ny tzw. wskaźnik gotowości K_G, ale po min. 24 miesiącach użytkowania. Trwają prace nad budową modelu eksploatacyjno-niezawodnościowego tego bardzo skomplikowanego systemu bezpieczeństwa znacznie bardziej skomplikowanego niż ten, który zaprezentowano na rys. 4. Dodatkowym utrudnieniem jest zaproponowany system nadzoru, administrowania i zarządzania danymi SSWiN przez lokalne sieci Ethernet. Nasuwają się także bardzo ostrożne wnioski:

– konfiguracje tak skomplikowanych systemów bezpieczeństwa należy wykonywać po bardzo szczegółowej analizie rozległego obiektu, z uwzględnieniem wymogów logistycznych oraz niezawodnościowych i eksploatacyjnych,
– zaproponowany SSWiN wymagał bardzo starannej instalacji, z uwzględnieniem kompatybilności elektromagnetycznej wraz z przemyślaną lokalizacją central oraz modułów,
– niezmiernie istotną sprawą, przy tak dużym i rozproszonym SSWiN, jest dobór zasilania zarówno zasadniczego, jak i rezerwowego (wynika z bilansu energetycznego),
– nowatorski system nadzoru i administrowania rozproszonego sytemu bezpieczeństwa, wraz z zabezpieczeniem danych (podany powyżej), należy do bardzo trudnych i skomplikowanych procedur informatycznych.

Bibliografia

1. Cole E., Krutz R. L., Conley J., *Bezpieczeństwo sieci. Biblia*, Helion, Gliwice 2005.
2. Dostalek L., *Bezpieczeństwo protokołu TCP/IP*. Seria: (Nie)bezpieczeństwo. Wydawnictwo Naukowe PWN 2006.
3. Haykin S., *Systemy Telekomunikacyjne*, Tom 1 i 2, Wyd. WKiŁ, Warszawa 2000.
4. Instrukcje i materiały firmy SATEL, Gdańsk 2011, 2012.
5. Karbowski M., Podstawy kryptografii, Wydanie II. Helion, Gliwice 2007.
6. Norma PN-EN 50131-1:2009: *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Wymagania systemowe*. 2009.
7. Rosiński A., *Design of the electronic protection systems with utilization of the method of analysis of reliability structures*, 19th International Conference On Systems Engineering (ICSEng 2008), Las Vegas, USA 2008.
8. Szulc W., Rosiński A., *Systemy sygnalizacji włamania*, Część 3 – *Magistrale transmisyjne i metody transmisji danych*, „Zabezpieczenia" Nr 4(68)/2009, Wyd. AAT, Warszawa 2009.
9. Szulc W., Szmigiel A., Prace własne dot. *Elektroniczne Systemy Bezpieczeństwa*, Politechnika Warszawska, Wydział Transportu, Warszawa 2008.
10. [www.satel.pl].
11. „Zabezpieczenia" Nr 1/47 2006.
12. Szulc W., Rosiński A., *Rozproszony System Bezpieczeństwa z informatyczna opcją zarządzania i administrowania*, Konferencja Naukowa Cyberterorryzm, Org: WSM w Warszawie, Wyższa Szkoła Policji w Szczytnie, Warszawa 2009.

Data management aspects of an extended dispersed electronic security system

Abstract: In the article the author presents important problems related to management of large electronic security systems as well as management of data significant for the correct functioning of extended dispersed systems. Additionally he designed the reliable operating model with the SSH tunnel to increase the security of computer data channels. The mathematical analysis of that model is also given. The author has done long term research to define operating indices crucial for proper functioning of elactronic security systems from the point of view of data management.

Keywords: electronic security system, internet, reliability

doc. dr inż. Waldemar Szulc

Od 1965 roku 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. 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 Laboratorium Systemów Bezpieczeństwa w Wyższej Szkole Menedżerskiej w Warszawie.

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