

Spis treści

I. System sygnalizacji włamania i napadu.....	2
1. Zakres projektu.....	2
2. Opis systemu.....	2
2.1. Wykaz stref dozorowych.....	3
2.2. Zalecenia montażowe.....	3
2.3. Wytyczne systemu dla pozostałych instalacji.....	3
II. System kontroli dostępu.....	4
1. Zakres opracowania.....	4
2. Podstawy opracowania.....	4
3. Charakterystyka ogólna obiektu.....	4
3.1. Założenie projektowe.....	4
3.2. Dobór elementów systemu.....	5
3.3. Podstawowe dane techniczne.....	5
3.4. Obsługa systemu KD.....	6
3.5. Przeglądy okresowe systemu KD.....	6
4. Spis rysunków.....	6

I. System sygnalizacji włamania i napadu

1. Zakres projektu

Zakres projektu obejmuje zabezpieczenie systemem sygnalizacji włamania i napadu budynku administracyjnego Urzędu Marszałkowskiego województwa Warmińsko-Mazurskiego przy ul. Głowackiego 17 w Olsztynie tj:

- budynek „A” w części użytkowanej przez Urząd Marszałkowski,
- łącznik pomiędzy budynkiem „A” i „B”,
- budynek „B”,
- budynek „C” w części użytkowanej przez Urząd Marszałkowski (Departament Społeczeństwa Informacyjnego, Archiwum)

w zakresie rozmieszczenia:

- centrali sygnalizacji włamania i napadu,
- ekspandery wejść oraz wyjść,
- klawiatur szyfrowych,
- czujek ruchu,
- magnetycznych czujników otwarcia,
- czujników sejsmicznych.

2. Opis systemu

Podstawową częścią systemu jest jednostka centralna INTEGRA 256 Plus. Decyduje ona o możliwościach sprzętowych i programowych systemu. Za pomocą magistrali transmisyjnej RS485 dołączone są do jednostki centralnej moduły systemu niezbędne do realizacji danego projektu:

- funkcje linii dozorowych oraz wyjść wykonawczych są realizowane w systemie poprzez ekspandery (INT-E),
- zazbrajanie i rozbrajanie systemu poprzez manipulator INT-KLCD-GR.

Zabezpieczany obiekt przedstawiony w powyższej dokumentacji posiada systemy zapewniające w sposób profesjonalny ochronę osób i mienia. Oprócz tego zainstalowany system zapewnia przegląd i rejestrację zdarzeń umożliwiając w ten sposób identyfikację zagrożeń i kontrolę nad chronionym obiektem. System sygnalizacji włamania posiada również możliwość podłączenia przez nadajnik do systemu monitoringu pozwalającego na szybkie powiadomienie służb interwencyjnych.

Zastosowany system rozpoznaje rodzaje zagrożeń, podaje (z dokładnością do jednego elementu dozorowego) lokalizację ich powstawania oraz - w razie awarii - zapewnia niezależność działania składowych podsystemów. Wszystkie informacje o sygnałach, zarówno alarmowych, jak i uszkodzeniach technicznych oraz status poszczególnych partycji i stref systemów są obrazowane na klawiaturach systemowych LCD, w

sposób czytelny i jednoznaczny oraz rejestrowane w pamięci, z której będą mogły być odtwarzane. Niezbędne procedury zaprogramowane w systemie są zabezpieczone przed skasowaniem przez celowe zakłócenie lub wyłączenie zasilania. Proste oprogramowanie i dostęp do wielu funkcji ułatwiają eksploatację systemu.

Projektowana instalacja ma spełnić następujące funkcje:

- ostrzegać o przebywaniu osób niepowołanych w załączonych w dozór strefach alarmowych budynku,
- ostrzegać o próbie otwarcia drzwi, będących granicą poszczególnych stref dozorowych,
- ostrzegać o próbie sabotażu zainstalowanych urządzeń.

System zabezpieczenia budynku oparty został na czujkach magnetycznych oraz czujkach dualnych. Wystąpienie alarmu włamaniowego spowoduje zasygnalizowanie alarmu poprzez manipulator INT-KLCD-GR. Zastosowane elementy systemu sygnalizacji włamania i napadu są zabezpieczone przeciwsabotażowo. Centrala zlokalizowana jest w budynku „B” w pomieszczeniu ochrony na poziomie 0. Manipulator INT-KLCD-GR budynku „B” w pomieszczeniu ochrony na poziomie 0. Manipulator w łączniku pomiędzy budynkami „A” i „B” na korytarzu przy wejściu do budynku „A”. Kolejny manipulator na poziomie 0 jest w budynku „B” w wejściu do Departamentu Społeczeństwa Informatycznego. Manipulator w budynku „B” na poziomie 1 znajduje się przed wejściem do kasy. Ponadto w budynku „B” będą zamontowane dwa manipulatory na poziomie 2, jeden przy pomieszczeniu 206, a drugi przy pomieszczeniu 220 Biura ds. Obronnych i Bezpieczeństwa Publicznego.

2.1. Wykaz stref dozorowych

Podział na strefy realizowany jest na poziomie software-owym. Podziału należy dokonać po ustaleniu szczegółów z inwestorem.

2.2. Zalecenia montażowe

- Magistrale systemowe należy wykonać przewodem np. YTKSY 6x2x0,8,
- Linie dozorowe do czujników ruchu i magnetycznych należy wykonać przewodem YTDY 6x0,5,
- Nie wolno prowadzić przewodów linii dozorowych, sygnalizacyjnych, sterujących i monitorujących z przewodami elektrycznymi 230V w tym samym przepuście,
- Przy wyznaczaniu ciągów instalacyjnych należy dążyć do jak najmniejszej liczby zbliżeń i skrzyżowań z innymi instalacjami elektroenergetycznymi. Wskazane jest zachowanie odległości 30 cm od tych instalacji.

2.3. Wytyczne systemu dla pozostałych instalacji

Na etapie realizacji należy dobrać typy czujek magnetycznych w zależności od typu drzwi. Drzwi w których zainstalowane będą elementy systemu sygnalizacji włamania i napadu oraz kontroli dostępu powinny zostać wyposażone w dwa magnetyczne czujniki otwarcia.

System sygnalizacji włamania będzie zasilany z najbliższej tablicy elektrycznej przewodem YDY 3x1,5. Przewód doprowadzić do pomieszczenia i wyprowadzić na wysokości około 2,5 m (będzie on wprowadzany bezpośrednio do urządzenia) wszelkie wątpliwości co do lokalizacji czujek, prowadzenia instalacji należy uzgodnić z projektantem i Inwestorem w czasie montażu.

II. System kontroli dostępu

1. Zakres opracowania

Przedmiotem projektu jest wykonanie systemu kontroli dostępu (KD) w budynku administracyjnym Urzędu Marszałkowskiego województwa Warmińsko-Mazurskiego w Olsztynie przy ul. Głowackiego 17.

Projektowana instalacja składa się z 4 przejść kontrolowanych jednostronnie wyposażonych w czynniki kart zbliżeniowych, kontrolery systemowe, zasilacze i elektrozwojory. Zarządzanie systemem będzie odbywać się poprzez komputer administratora podłączony poprzez port ethernet do systemu kontroli dostępu. W miejscu wskazanym przez Inwestora należy ułożyć magistralę RS-485 oraz konwerter RS-485/TCP/IP. System będzie umożliwiać dalszą rozbudowę o kolejne przejścia kontrolowane.

2. Podstawy opracowania

Podstawę opracowania niniejszej dokumentacji stanowią następujące dokumenty i opracowania:

- Umowa na wykonanie niniejszego opracowania.
- Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. Nr 114, poz. 740, z późn. zm.).
- Wytyczne inwestora określające zakres projektowania.
- Normy branżowe.
- Informacje producentów urządzeń systemów kontroli dostępu.

3. Charakterystyka ogólna obiektu

Budynek Urzędu Marszałkowskiego województwa Warmińsko-Mazurskiego zlokalizowany w Olsztynie przy ul. Głowackiego 17 jest budynkiem administracyjno-biurowym. Budynek składa się z 3 brył nazwanych „A”, „B” i „C”. Pomieszczenia objęte kontrolą dostępu znajdują się w bryle „B” na pierwszym i drugim piętrze.

3.1. Założenie projektowe

Zgodnie z założeniami projektowymi system kontroli dostępu powinien:

- współpracować z kartami zbliżeniowymi UNIQUE 125kHz. Systemy kontroli dostępu w oparciu o powyższe karty są już w strukturach Urzędu Marszałkowskiego.
- umożliwiać programowanie kart za pomocą dedykowanego programatora oraz wybranego czytnika kontroli dostępu,

- realizować bezkontaktowy odczyt karty przez czytnika
- posiadać pamięć w kontrolerach, w której zapisywane są operacje dokonywane za pomocą kart
- zapewniać dostęp do systemu poprzez sieć komputerową.

3.2. Dobór elementów systemu

Do realizacji kontroli dostępu w budynku Urzędu Marszałkowskiego proponuje się kontroler PR402DR polskiego producenta firmy ROGER. Kontrolery serii PR402DR mogą pracować jako autonomiczne jednostki kontroli dostępu jak i w zintegrowanym sieciowym systemie kontroli dostępu. W trybie autonomicznym kontrolery PR402DR mogą dozorować obustronne przejście bez potrzeby komunikacji z urządzeniami nadrzędnymi, zdarzenia są rejestrowane w wewnętrznym buforze kontrolera, a funkcje związane z czasem są sterowane przez jego wewnętrzny zegar. System kontroli dostępu na bazie kontrolerów PR402DR może być zarządzany lokalnie za pośrednictwem portów szeregowych COM lub USB albo zdalnie przez sieć komputerową WAN/LAN. Kontrolery PR402DR posiadają wbudowany zasilacz buforowy, mogą współpracować z 1 lub 2 czytnikami oraz umożliwiają montaż na szynie DIN.

3.3. Podstawowe dane techniczne.

- zasilanie 12 VDC
- zasilanie 24 VDC, 18 VAC (oprócz PR402DR-12VDC)
- montaż na szynie DIN
- 8 programowalnych linii wejściowych
- 4 programowalne linie wyjściowe
- 2 wyjścia przekaźnikowe 1,5 A/30 V oraz 5 A/30 V lub 230 VAC
- programowanie zdalne z komputera
- interfejs komunikacyjny RS485, RACS Clock&Data, Wiegand 26..66bit, Magstripe
- współpraca z czytnikami RFT1000
- współpraca z czytnikami dalekiego zasięgu
- do 4 tys. użytkowników
- 32 tys. zdarzeń we wbudowanym buforze
- zegar czasu rzeczywistego
- grupy użytkowników
- strefy dostępu
- harmonogramy czasowe
- kontrola dostępu w windach (wymagany XM-8)
- Anti-passback lokalny
- śluza bankowa
- funkcje: wejście komisyjne, wejście warunkowe, tryb high security
- obsługa kołowrotów (tripodów)

- obsługa szlabanów
- losowe wyznaczanie użytkowników do kontroli
- integracja z rejestracją czasu pracy (RCP Master)
- integracja z systemami alarmowymi
- integracja z telewizją przemysłową (CCTV-DVR)
- znak CE

3.4. Obsługa systemu KD.

System oraz jego części składowe powinny obsługiwać tylko osoby posiadające potwierdzone przez firmę instalacyjną przeszkolenie w niezbędnym do obsługi zakresie. Szkolenia powinny być wznawiane przy zmianie obsługi systemu oraz po modernizacji instalacji lub rekonfiguracji programowej systemu. Wszelkie zmiany oraz szkolenia, powinny być rejestrowane w książce eksploatacji i obsługi systemu KD przez upoważnione do tego osoby ze strony użytkownika systemu i firmy instalacyjnej (serwisującej system). Nazwiska osób odpowiedzialnych powinny być zapisane w książce eksploatacji i być na bieżąco aktualizowane. Użytkownik systemu w ramach wewnętrznych regulacji powinien określić tryb i osoby upoważnione do dostępu i dokonywania zmian w bazach danych.

3.5. Przeglądy okresowe systemu KD.

W celu zapewnienia ciągłego poprawnego funkcjonowania instalacji, powinna ona być regularnie sprawdzana i poddawana okresowym przeglądom. Umowy na ten temat powinny być zawarte pomiędzy użytkownikiem a organizację serwisową natychmiast po zakończeniu instalowania, niezależnie od tego, czy obiekt jest zasiedlony, czy też nie.

4. Spis rysunków

SWN-01 – LEGENDA

SWN-02 – Plan Systemu Sygnalizacji Włamania i Napadu – BUDYNEK „A” PIWNICA

SWN-03 – Plan Systemu Sygnalizacji Włamania i Napadu – BUDYNEK „A” PARTER

SWN-04 – Plan Systemu Sygnalizacji Włamania i Napadu – BUDYNEK „B” PIWNICA

SWN-05 – Plan Systemu Sygnalizacji Włamania i Napadu – BUDYNEK „B” PARTER

SWN-06 – Plan Systemu Sygnalizacji Włamania i Napadu – BUDYNEK „B” PIĘTRO I

SWN-07 – Plan Systemu Sygnalizacji Włamania i Napadu – BUDYNEK „B” PIĘTRO II

SWN-08 – Plan Systemu Sygnalizacji Włamania i Napadu – BUDYNEK „B” PIĘTRO III

SWN-09 – Plan Systemu Sygnalizacji Włamania i Napadu – BUDYNEK „C” PARTER

SWN-10 – SCHEMAT – Systemu Sygnalizacji Włamania i Napadu

SWN-11 – SCHEMAT – System Kontroli Dostępu