Jednostka Projektowa	ARCHICO **ul. Garncarska 5 IVp. 70-377 Szczecin** **tel./fax 91/880 38 93 e-mail: biuro@archico.eu www.archico.eu**	
Nazwa projektu:	**PROJEKT WYKONAWCZY**	
Zadanie:	**Przebudowa, remont i rewaloryzacja zabytkowej willi z ogrodem - siedziby Oddziału IPN w Szczecinie**	
Kategoria obiektu budowlanego:	**XII - budynek administracji publicznej**	
Adres obiektu budowlanego:	**ul. Piotra Skargi 14 w Szczecinie, dz. nr 3/4 obręb 1022**	
Inwestor:	**Instytut Pamięci Narodowej - Komisja Ścigania Zbrodni przeciwko Narodowi Polskiemu** **ul. Wołoska 7, 02-675 Warszawa**	
Oświadczenie projektantów	**Zgodnie z art.20 ust.4 Ustawy z dnia 7 lipca 1994 r. Prawo budowlane (tj. Dz. U. Nr 243 z 2010r. poz. 1623 z późniejszymi zmianami)** oświadczamy, że przedmiotowy projekt budowlany – został sporządzony zgodnie z obowiązującymi przepisami i zasadami wiedzy technicznej.	
BRANŻA ELEKTRYCZNA - IT		
Autor	*Projektant - autor branży inst. elektrycznych:* **mgr inż. Piotr Markowski** **upr. proj. ZAP/0218/POOE/11** *Sprawdzający:* **mgr inż. Mariusz Piątkowski** **upr. bud. ZAP/0125/PWOE/11**	
Szczecin, czerwiec 2018 r.		**egz.**

Spis treści

Spis załączników

Spis rysunków

1. Przedmiot i zakres opracowania

Projekt wykonawczy dla remontowanego obiektu:

Przebudowa, remont i rewaloryzacja zabytkowej willi z ogrodem - siedziby Oddziału IPN w Szczecinie

adres inwestycji:

ul. Piotra Skargi 14 w Szczecinie

dz. nr 3/4 obręb 1022

inwestor:

Instytut Pamięci Narodowej -

Komisja Ścigania Zbrodni przeciwko Narodowi Polskiemu

ul. Wołoska 7, 02-675 Warszawa

2. Podstawa prawna opracowania

- umowa pomiędzy Inwestorem a projektantem
- koncepcja rozwiązań techniczno - technologicznych oraz ustalenia pomiędzy Inwestorem, a Projektantem;
- projekty branżowe instalacji i architektury
- obowiązujące normy i przepisy
- katalogi, karty katalogowe producentów.

2.1. Obowiązujące przepisy i normy

Obowiązujące przepisy:

- Dyrektywa z dnia 12 grudnia 2006 r. w sprawie harmonizacji ustawodawstwa państw członkowskich odnoszących się do sprzętu elektrycznego przewidzianego do stosowania w określonych granicach napięcia
- Dyrektywa z dnia 15 grudnia 2004 r. w sprawie zbliżenia ustawodawstwa Państw Członkowskich odnoszących się do kompatybilności elektromagnetycznej
- Dyrektywa z dnia 21 grudnia 1988 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich odnoszących się do wyrobów wykonawczych
- Norma PN-EN 12464 Światło i oświetlenie. Oświetlenie miejsca pracy – część 1: Miejsca pracy we wnętrzach
- Norma PN-EN 62305 Ochrona odgromowa obiektów wykonawczych
- Norma wielo-arkuszowa PN-IEC 60364 Instalacje elektryczne w obiektach wykonawczych wraz z

wprowadzoną Normą PN-HD 60364 Instalacje elektryczne niskiego napięcia

- Rozporządzenie Ministra Infrastruktury z dnia 12 kwietnia 2002r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie
- Rozporządzenie Ministra Infrastruktury z dnia 3 lipca 2003 r. w sprawie szczegółowego zakresu i formy projektu budowlanego
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 21 kwietnia 2006 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów wykonawczych i terenów
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 16 czerwca 2003 r. w sprawie uzgadniania projektu budowlanego pod względem ochrony przeciwpożarowe
- Ustawa z dnia 10 kwietnia 1997r. Prawo Energetyczne
- Ustawa z dnia 13 kwietnia 2007r. o kompatybilności elektromagnetycznej
- Ustawa z dnia 16 kwietnia 2004 r. o wyrobach wykonawczych
- Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej
- Ustawa z dnia 7 lipca 1994r. Prawo budowlane

2.2 Warunki środowiskowe

Warunki środowiskowe (wpływy zewnętrzne) określają miejscowe warunki, w których będą pracować urządzenia i instalacje elektryczne.

Przyjęto, że w projektowanym budynku instalacja urządzeń elektrycznych panować będą warunki środowiskowe normalne, zgodnie z PN-HD 60346-3.

Przyjęto następujące klasyfikacje wg PN-HD 60364-3,

- ***środowiskowe***

- wpływ temp. - AA5 (+5°C - +40°C)

- wpływ ciał obcych - AE4 (lekkie zapylenie)

- ***klasyfikacje osób***

BA4	Poinstruowane	Osoby odpowiednio poinformowane albo nadzorowane przez osoby wykwalifikowane, w sposób zapewniający unikanie niebezpieczeństw jakie może stwarzać elektryczność (personel obsługi i konserwacji)	Obszary obsługi wyposażenia elektrycznego
BC2	Rzadka	Osoby nie mające w normalnych warunkach styczności z częściami przewodzącymi obcymi lub nie stojące na powierzchniach przewodzących	Obszary obsługi wyposażenia elektrycznego

3. Zakres opracowania

Przedmiotem niniejszego opracowania jest montaż okablowania oraz urządzeń zabezpieczeń technicznych w ramach prowadzonych prac remontowo – budowlanych w zakresie budynku zabytkowej willi z ogrodem siedziby oddziału IPN w Szczecinie.

Zakres rzeczowy obejmuje wymianę urządzeń oraz rozbudowę systemów w ramach przebudowywanych pomieszczeń, w tym:

- opracowanie koncepcji systemu sygnalizacji włamań i napadów,
- opracowanie koncepcji systemu telewizji dozorowej,
- opracowanie koncepcji systemu kontroli dostępu,
- dobór urządzeń,
- doposażenie systemu zasilania systemów,

4. Koncepcja systemu zabezpieczeń technicznych

4.1 System sygnalizacji włamania i napadu (SSWIN)

Na obiekcie projektuje się budowę instalacji sygnalizacji włamania i napadu SSWiN w celu ochrony osób i mienia przed skutkami włamania i napadu. Zamontowana zostanie mikroprocesorowa centrala SSWiN oraz zespół detektorów w tym czujki PIR+MW, kontaktrony, przyciski napadowe, czujniki zbicia szkła, temperatury i zalania na całym obiekcie zgodnie z przyjętą klasyfikacją budynku. System podzielony zostanie na podstrefy i uzbrajany będzie za pomocą lokalnych manipulatorów.

Możliwości centrali w zakresie rozbudowy za pomocą modułów rozszerzenia zostały wykorzystane i dlatego też rozbudowa systemu może być wykonana w nieznacznym zakresie z wykorzystaniem eksploatowanych linii dozorowych. Na schemacie każdy ekspander ma zaznaczone rezerwowe linie.

Rozmieszczenie elementów należy nanieść zgodnie z rzutami. Centrale SSWIN zamontować w miejscu niedostępnym dla osób 3-cich, zgodnie z rzutem w pomieszczeniu informatyka. Zasilanie ekspanderów wykonać przewodem YDY 3x2,5mm, a instalacje SSWIN wykonywać przewodem typu YDY 8x0.5mm.

Zastosowana centrala np. INTEGRA 256 PLUS posiada wbudowany komunikator GSM/GPRS z funkcjami monitoringu, powiadamiania i zdalnego sterowania. W celu chronienia obiektu należy skonfigurować centralę o transmisję zdarzeń do obiektu przy ul. Janickiego.

Najważniejsze cechy tej centrali:

- Ekspandery do 64
- Klasa środowiskowa wg EN50130-5 II
- Magistrale komunikacyjne 1+2
- Maksymalna liczba wejść programowalnych 256
- Maksymalna liczba wyjść programowalnych 256
- Manipulatory do 8
- Stopień zabezpieczenia wg EN 50131Grade 3
- Strefy 32
- Użytkownicy + Administratorzy 240+8
- Wejścia przewodowe programowalne 16

- Wydajność prądowa zasilacza (zasilanie urządzeń + ładowanie akumulatora) 2000 + 1500 mA
- Wyjścia przewodowe programowalne 16
- Wyjścia zasilające 3
- wbudowany dwukierunkowy interfejs bezprzewodowy 868 MHz w technologii ABAX,
- magistrale komunikacyjne do podłączania manipulatorów i modułów rozszerzeń,
- wbudowany komunikator GSM/GPRS z funkcjami monitoringu, powiadamiania i zdalnego sterowania,
- obsługa systemu przy pomocy manipulatorów LCD, klawiatur strefowych, pilotów i kart zbliżeniowych oraz zdalnie, z użyciem komputera lub telefonu komórkowego,
- port RS–232 – gniazdo RJ ,
- możliwość aktualizacji oprogramowania za pomocą komputera ,
- wbudowany zasilacz impulsowy o wydajności 2 A z funkcjami ładowania akumulatora i diagnostyki ,
- kompatybilność z gamą akcesoriów i modułów INTEGRA oraz ABAX ,
- opcja niezgłaszania do centrali alarmowej awarii serwera SATEL (INTEGRA Firmware 1.16 lub nowszy) .

Stosować czujki np. PIR+MW COBALT Plus o właściwościach:

- podwójny pyroelement
- tor PIR i mikrofalowy
- funkcja antymaskingu realizowana przez tor mikrofalowy
- cyfrowy algorytm detekcjiStosować czujki zbicia szyby INDIGO o właściwościach:
- zaawansowana mikroprocesorowa dwutorowa analiza sygnału
- wykrywanie zbicia szkła zwykłego, hartowanego i laminowanego
- funkcja autodiagnostyki
- płynna regulacja czułości

Stosować kontraktony np. B-1 o właściwościach:

DANE TECHNICZNE

Maksymalne napięcie przełączalne kontaktronu	100 V
Maksymalny prąd przełączalny	0,5 A
Odległość zamknięcia styków kontaktronu	24 mm
Odległość otwarcia styków kontaktronu	29 mm
Wymiary obudowy magnesu	28 x 12,5 mm

Stosować czujki sufitową np. PIR+MW SRX360X sufitowy o właściwościach:

- Poczwórny PIR – element
- Tor mikrofali z anteną paskową
- Zasięg 360 st./20 m z wysokości 3,6m
- Technologia mikroprocesorowa
- Wysoka odpornośc na zakłócenia RFI i EMI
- Zastosowanie w ciężkich warunkach otoczenia
- Podwójna kompensacja temperatury

- Częstotliwość mikrofali 10.525GHz

W pomieszczeniach 1.7 i 1.8 należy stosować elementy bezprzewodowe. Kontrolerem systemu np.ABAX jest kontroler np.ACU-120 o charakterystyce:

DANE TECHNICZNE

Napięcie zasilania (±15%)	12 V DC
Wymiary obudowy	126 x 158 x 32 mm
Wymiary płytki elektroniki	103 x 139 mm
Zakres temperatur pracy	-10 °C...+55 °C
Pobór prądu w stanie gotowości	50 mA
Maksymalny pobór prądu	75 mA
Masa	202 g
Maksymalna wilgotność	93±3%
Pasmo częstotliwości pracy	868,0 ÷ 868,6 MHz
Zasięg komunikacji radiowej (w terenie otwartym)	do 500 m
Klasa środowiskowa wg EN50130-5	II
Spełniane normy	EN 50130-4, EN 50130-5, EN 50131-1, EN 50131-3, EN 50131-5-3
Stopień zabezpieczenia wg EN50131-3	Grade 2

Kontroler zapewnia współprace z centralami alarmowymi z rodzin: INTEGRA i VERSA(podłączanie przez magistralę komunikacyjną)

•obsługa do 48 urządzeń bezprzewodowych systemu ABAX:
•obsługa do 8 manipulatorów bezprzewodowych w ramach systemu ABAX(w zależności od centrali)
•obsługa do 248 pilotów APT-100 (w zależności od centrali)
•dwukierunkowa kodowana komunikacja radiowa w paśmie częstotliwości 868 MHz
•nowoczesny układ radiowy
•dywersyfikacja anten
•programowanie kontrolera za pośrednictwem centrali alarmowej przy pomocy:
    •manipulatora w trybie serwisowym
    •programu DLOADX
•port RS-232 TTL do podłączenia komputera, umożliwiający aktualizację oprogramowania kontrolera bez konieczności jego demontażu
•styk sabotażowy reagujący na otwarcie obudowy
•wejście sabotażowe

4.2 Telewizja dozorowa CCTV

Modernizowany system CCTV ma spełniać wymogi 3 stopnia zabezpieczenia i zapewnić archiwizację zdarzeń, przed pożarem, kradzieżą i innym niebezpieczeństwem grożącym ich zniszczeniem lub utratą, przez okres 14 dni. Należy podłączyć drugi istniejący rejstrator w obiekcie na ul. Janickiego w pomieszczeniu służby ochrony z projektowaną szafą GPD na ul. Piotra Skargi za pomocą sieci IPN.

W ramach prowadzonych prac należy zainstalować wszystkie kamery zgodnie z rzutami i schematami. Kamery które są na zewnątrz budynku muszę zostać wymienione na kamery 4- megapikselowych lub równoważne i należy je podłączyć do rejestratora cyfrowego np. LC-6436 NVR . Doposażony rejestrator cyfrowy wraz z monitorem zasilić poprzez zasilacz UPS. W celu obserwacji należy przewidzieć 2 jednostki do obserwacji jedną w pomieszczeniu informatyka, a drugą w szatni..

System ma za zadanie monitorować:

- cały teren zewnętrzny budynku,
- wejscia i wyjscia z placówki,
- garaż

Zespół rejestratorów należy instalować w projektowanej szafce GPD 19". W systemie należny przewidzieć rejestrator cyfrowy z dyskiem twardym zapewniającym zapis obrazów z kamer z prędkością 30kl/s przez minimum 14 dni.

Dla 22 kamer przewiduje się dyski twarde o łącznej pojemności 27TB np. 4x 8TB SATA 6Gb/s 64MB. Zgodnie z obliczeniami pozwolą one na zapis wideo w kompresji H.264-10 w jakości 1080p 24/7 z możliwością zapisu do 14 dni w 30kl/s.

Poniżej znajduję się specyfikacja techniczna dla rejestratora LC-6436 NVR:

Specyfikacja techniczna

Kanały IP	64 lub 49 (1280 x 960 px) / 36 (1920 x 1080 px) / 25 (2048 x 1536 px) / 25 x (2592 x 1944 px)
Wyjścia wideo	1 x VGA, 1 x HDMI
Wejścia audio	64 / 36 / 25 / 16
Wyjścia audio	1 x RCA
Prędkość zapisu [FPS]	30
Wielkość obrazu [px]	1920 x 1080, 1280 x 960, 1280 x 720
Archiwizacja danych	9 x HDD SATA, 1 x HDD E-SATA (max. 4TB każdy)
Sieć WiFi	TAK
Oprogramowanie	Linux
Wejścia alarmowe	4
Wyjścia alarmowe	4
Porty sieciowe	2 x RJ45 10M/100M/1000M Ethernet
Port RS-485	TAK
P2P	TAK
ONVIF	TAK
RTSP	TAK
Detekcja ruchu	TAK
Porty USB	1 x USB 3.0, 2 x USB 2.0
Obsługiwane platformy mobilne	iOS, Windows Mobile, BlackBerry, Symbian, Android
Tryb nagrywania	Ręczny, Harmonogram, Zdarzeniowy

W ramach prowadzonych prac należy zainstalować wszystkie kamery w pomieszczeniach komunikacyjnych zgodnie z rzutami i schematami. Kamery na zewnątrz budynku np. NVAHD-4DN3202H/IR-1 o parametrach:

- Kamera AHD w obudowie IP 66 i IK10,
- Przetwornik obrazu 1/3” OV
- Tryb pracy AHD 4MPX
- Liczba efektywnych pikseli 2560 (H) x 1440 (V)
- Rozdzielczość 4MPX
- Czułość:
  - 0.03 lx/F1.4 - tryb kolorowy,
  - 0 lx (IR wł.) - tryb czarno-biały
- Stosunek sygnału do szumu > 50 dB (wyłączona ARW)
- Elektroniczna migawka automatyczna: 1/25 s ~ 1/50000 s
- Szeroki zakres dynamiki (WDR)
- Cyfrowa redukcja szumu (DNR)
- Typ obiektywu ze zmienną ogniskową, f=2.8 ~ 12 mm/F1.4
- Rodzaj przełączania mechaniczny filtr podczerwieni

oraz na wewnątrz budynku:

- Kamera wandaloodporna w obudowie IP66 i IK10,
- Przetwornik obrazu 1/3” OV
- Tryb pracy AHD 4MPX

- Liczba efektywnych pikseli 2560 (H) x 1440 (V)
- Rozdzielczość 4MPX
- Czułość:
  - 0.03 lx/F1.4 - tryb kolorowy,
  - 0 lx (IR wł.) - tryb czarno-biały
- Stosunek sygnału do szumu > 50 dB (wyłączona ARW)
- Elektroniczna migawka automatyczna: 1/25 s ~ 1/50000 s
- Szeroki zakres dynamiki (WDR)
- Cyfrowa redukcja szumu (DNR)
- Typ obiektywu ze zmienną ogniskową, f=2.8 ~ 12 mm/F1.4
- Rodzaj przełączania mechaniczny filtr podczerwieni

4.3 System kontroli dostępu

Charakterystyka obiektu wymaga aby zaprojektowany system SKD służyły ochronie mienia. Zainstalowany system składa się z kontrolera, elektrozaczepu, dwóch kontrolerów przejścia oraz przycisku wyjścia ewakuacyjnego. System został postawiony w oparciu o rozwiązania firmy Kantech które są kompatybilne z projektwanym SSWIN oraz depozytorem kluczy.Wszystkie parametry funkcjonalne tej instalacji, wraz z określeniem siatki dostępu, siatki czasu, klas rozpoznania, klas dostępu itp. określone zostaną przez użytkownika na etapie realizacji i stanowić będą wymagania funkcjonalne do zaprogramowania systemu. System zamontować w pomieszczeniach zgodnie z rzutami i schematami.

Zamontowany SSYSTEM SKD składa się z :

- Kontrolera KT-1-PCB
- Czytnika kart zbliżeniowych KDH-CK3300U/U/H/M
- Elektrozaczep
- Przycisk wyjścia awaryjnego KDH-EXIT1030-P

Wszystkie kontrolery współpracują z elektrozaczepem oraz przyciskiem wyjścia awaryjnego. System posiada ustanowionego jednego administratora mającego uprawnienie do przydzielania użytkowników i kontroli logów systemu. Programowanie odbywa się za pomocą czytnika administratora np. KDH-CADM-U24 który jest wymagany aby zaprogramować karty. Zgodnie z wymaganiami użytkownika system ma możliwość wyłączenia na kluczyk kontroli dostępu oraz dodatkowo istnieje możliwość wyłączenia kontroli dostępu za pomocą oprogramowania na określony czas lub karty administratora.

4.4 Depozytor kluczy

W projekcie przewiduję się umieszczenie elektroniczno-mechanicznego depozytora kluczy np. HT ES 30 DD. Przeznaczony jest do bezpiecznego zdawania, przechowywania i pobierania kluczy, które nie powinny opuszczać obiektu. Przewiduję się umieszczenie w szatni pokój 1.2 zgodnie z rzutem. Ochrona klucza zawiera kontrolę wydawania, alarmy i ustawienia przedziałów czasowych dla różnych zadań. Zaawansowane raportowanie jest aktywne i zawiera audyt, status bezpieczeństwa i możliwość generowania raportów. Depozytor posiada 30 miejsc na klucze z możliwością rozbudowy do 40 w ramach tej samej obudowy. Najważniejsze możliwości i cechy depozytora:

- wyświetlacz LCD
- System posiada mechaniczną blokadę kluczy
- Liczba kluczy: 30 (z możliwością rozbudowy do max 40 w ramach tej samej obudowy)
- Pamięć: 512 kB
- Ustawienie i zapamiętywanie czasu

- Możliwość ustawienia “okna otwarcia”
- Możliwość połączenia z czytnikiem kart
- Możliwość podłączenia do systemu alarmowego
- Zasilanie, 230V / 50HZ
- Jednostka sterująca – mikroprocesor
- 1GHz procesor, 1 GB RAM
- Pamięć kodów PIN
- Zamek elektromagnetyczny
- Wbudowane podtrzymanie pamięci
- Ilość użytkowników: do 1000
- Audyt wykonanych operacji: 20 000
- Możliwość rozbudowy systemu
- Praca w sieci TCP/IP
- Oprogramowanie dostosowane do środowiska Windows, jak i aplikacji internetowych.
- Autoryzacja może przebiegać za pomocą kodu PIN, RFID (różne protokoły, takie jak LEGIC, Mifare, HID) i najnowsze metody biometryczne. W razie potrzeby każde metody mogą być łączone.
- Komunikacji pomiędzy serwerem i systemami odbywa się poprzez TCP / IP w określonej sieci lub drogą WiFi. Połączenia telefoniczne takie jak ISDN, GSM, są również zintegrowane.
- Awaryjne zasilanie z akumulatora

4.6 Instalacja domofonowa

W budynku projektuje się instalację domofonową. Jako podstawowe wyposażenie należy przewidzieć stację wywoławcze domofonowe przy 2-ch wejściach do budynku, a w pomieszczeniu sekretariatu 2.1 2 sztuki unifonów oraz po jednej sztucę w szatni pomieszczenie 1.2 oraz sekretariat OBUW i M pomieszczenie 0.5 z możliwością otwarcia drzwi. Szczegóły instalacji zgodnie ze schematem i rzutem. Instalację należy wykonać zgodnie ze schematem przewodem UTP 4x2x0,5mm.

4.7 Integracja

W budynku projektuje się instalację SSWIN, KD oraz depozytor kluczy. Do każdego z systemów przewiduje się możliwość korzystania z systemu bezdotykowych kart np. Mifare. Cały system należy tak skonfigurować aby można było korzystać z jednej karty dla systemu SSWIN, KD oraz depozytora kluczy. Wszystkie systemy mogą być monitorowane oraz mogą być do nich nadawane uprawnienia przez posterunek SO IPN w obiekcie przy ul. Janickiego 30.

Projektuje się aby wszystkie systemy zostały scalone za pomocą oprogramowania VENO. Oprogramowanie powinno współpracować:

- centralami alarmowymi wiodących producentów w tym: DSC, Satel, Siemens i inne opcjonalnie
- systemami kontroli dostępu wiodących producentów w tym: KaDe, Kantech, ASSA ABLOY i inne opcjonalnie
- systemami ochrony przeciwpożarowej wiodących producentów w tym: Polon Alfa i inne
- systemami telewizji przemysłowej wiodących producentów w tym: NOVUS i inne opcjonalnie
- depozytorami kluczy wiodących producentów w tym: Hartman Systems i inne
- *sieciowymi modułami wejść/wyjść przekaźnikowych wiodących producentów w tym: Moxa i inne opcjonalnie*

Oprogramowanie integrujące powinno spełniać poniższe wymagania:

- Posiadać intuicyjny interfejs graficzny użytkownika obsługiwany za pomocą myszki PC i klawiatury PC
- Możliwość stworzenia systemu w strukturze rozproszonej serwer-klient (wielu klientów)
- Możliwość podłączenia centrali SSWiN, rejestratora CCTV, kontrolerów KD lub serwera KD, centrali pożarowej PPOŻ, sieciowych modułów przekaźnikowych
- Możliwość sterowania podłączonymi urządzeniami w ramach ich możliwości oraz przepisów
    - SSWiN m.in.: wysyłanie polecenia: uzbrój/rozbrój podsystem lub wszystkie podsystemu i inne
    - SKD m.in.: wysyłanie polecenia: odrygluj/zarygluj drzwi, odrygluj czasowo, zablokuj i inne
    - CCTV m.in.: sterowanie PTZ, odtwarzanie nagrań i inne
    - moduły sieciowe m.in.: włącz/wyłącz wyjście lub wszystkie wyjścia,
- Możliwość budowania interfejsu niezależnie dla każdego użytkownika lub stanowiska nadzoru
- Możliwość zarządzania stacją serwerową z dowolnego stanowiska nadzoru
- Możliwość automatycznego reagowania na zdarzenia oraz przechwytywania, przechowywania i przeszukiwania informacji (logów) o zdarzeniach zaistniałych w systemie

Interfejs graficzny

Oprogramowanie zarządzające powinno posiadać interfejs graficzny użytkownika (GUI) o następującej funkcjonalności:

Interfejs powinien składać się z okien programu (paneli) umożliwiających ich dowolną konfigurację. Wszystkie stany z urządzeń powinny być pobierane automatycznie bez konieczności ingerencji operatora Użytkownik powinien mieć dowolnej konfiguracji panelu dodając odpowiednie elementy:

elementy z podłączonych urządzeń:

- SSWiN czujki, partycje, centrale, wyjścia i inne w ramach możliwości
- SKD centrale, wejścia alarmowe, wyjścia przekaźnikowe i inne w ramach możliwości
- PPOŻ centrale, czujki, moduły wejść i wyjść i inne dodatkowe w ramach możliwości
- CCTV kamery, wejścia i wyjścia alarmowe, serwery i inne dodatkowe w ramach możliwości
- I/O moduł wejścia i wyjścia

elementy z aplikacji:

- okna wideo
- panel odtwarzania
- panel PTZ
- przyciski reakcji
- przyciski link
- etykiety
- obrazki
- zdjęcia
- okno logów
- okno alarmów
- punkty nawigacyjne
- wirtualne strefy
- inne w ramach możliwości

Struktura rozproszona serwer-klient

- Oprogramowanie powinno posiadać możliwość rozdzielenia funkcji serwera i klienta. Część serwerowa powinna działać jako usługa co gwarantuje podwyższony poziom bezpieczeństwa.
- Możliwość instalacji na jednej stacji roboczej obu modułów, tzn. realizacji funkcji serwer i klient na jednej stacji roboczej
- Oprogramowanie pracujące w trybie serwer powinno:
    - rejestrować zdarzenia pochodzące z podłączonych systemów

- rejestrować zmiany konfiguracji wykonywane na stacjach operatorskich
- umożliwiać przesyłanie informacji do nieograniczonej programowo liczby stacji klienckich

- Oprogramowanie w wersji klient
  - umożliwiać podgląd zdarzeń przychodzących z podłączonych systemów
  - umożliwiać reagowanie na zdarzenia przychodzące z podłączonych systemów (w ramach przypisanych uprawnień)
  - umożliwiać odtwarzanie nagrań zarejestrowanych na rejestratorze CCTV podłączonym do serwera integrującego

Systemy SSWiN

Systemy SSWiN powinny mieć możliwość podłączenia do serwera integrującego za pomocą dedykowanego modułu kompatybilnego z centralą dostarczanego przez producenta. Jako metodę komunikacji uznaje się połączenie za pomocą portu RS, protokołu TCP/IP, konwertera RS na TCP/IP.

Oprogramowanie integrujące/ wizualizujące powinno móc rejestrować zdarzenia przychodzące z integrowanego systemu SSWIN w zakresie: alarm, naruszenie, uszkodzenie, uzbrojenie, rozbrojenie, sabotaż, czujnik zablokowany, odliczanie czasu na wejście/wyjście, błąd połączenia, połączony, rozłączony, strefa blokowana, wyście wł/wył, przetrzymanie, błąd synchronizacji czasu, drzwi zamknięte/otwarte. Poszczególne stany elementów powinny być wizualizowane z pomocą odpowiednich ikon o różnych kolorach.

Oprogramowanie integrujące powinno mieć możliwość zarządzania systemem SSWIN w zakresie (funkcje wykonawcze): uzbrojenie, rozbrojenie, blokowanie/odblokowanie czujki, kasuj alarm, włącz/wyłącz wyjście/ odrygluj drzwi, zarządzanie użytkownikami.

Oprogramowanie integrujące z racji swojego charakteru i przeznaczenia nie może wpływać na konfigurację cen trali SSWiN. Zapewnia to bezpieczeństwo pracy centrali SSWiN jako odrębnego systemu co gwarantuje niezawodność jej działania. Oprogramowanie powinno umożliwiać zarządzanie uprawnieniami użytkowników. Odczyt uprawnień powinien zachodzić automatycznie.

Nadawanie uprawnień powinno umożliwiać co najmniej:

- nadanie nazwy użytkownika
- ustawienie hasła
- typ dostępu (normalny, jednorazowy, na czas (odnawialny/nieodnawialny), przymus, steruje wyjściami „mono" stref, steruje wyjściami „bi" stref, włącza blokadę czasową stref, wartownik, schematowi
- strefa

Systemy SKD

Systemy SKD powinny mieć możliwość podłączenia do serwera integrującego za pomocą dedykowanego modułu kompatybilnego z centralą, serwerem zarządzającym, dostarczanego przez producenta. Jako metodę komunikacji uznaje się połączenie za pomocą portu RS, protokołu TCP/IP, konwertera RS na TCP/IP.

Oprogramowanie integrujące/ wizualizujące powinno móc rejestrować zdarzenia przychodzące z integrowanego systemu SKD w zakresie co najmniej: alarm, uszkodzenie, drzwi zaryglowane/odryglowane, drzwi przetrzymane, czytnik aktywny/nieaktywny, dostęp zezwolony/zabroniony, kartę dodano/usunięto/zmodyfikowano, monitorowanie wejście wł/wył, przekaźnik wł/wył, błąd połączenia, połączony, rozłączony. Poszczególne stany elementów powinny być wizualizowane z pomocą odpowiednich ikon o różnych kolorach.

Oprogramowanie integrujące powinno mieć możliwość zarządzania systemem SKD w zakresie (funkcje wykonawcze): zarygluj/odrygluj drzwi, odrygluj drzwi chwilowo, przywróć do stanu normalnego, włącz/wyłącz czytnik, włącz/wyłącz przekaźnik, włącz przekaźnik chwilowo, włącz.wyłącz monitorowanie, zarządzanie kartami.

Oprogramowanie integrujące z racji swojego charakteru i przeznaczenia nie może wpływać na konfigurację SKD. Zapewnia to bezpieczeństwo pracy SKD jako odrębnego systemu co gwarantuje niezawodność jej działania. Oprogramowanie powinno umożliwiać zarządzanie uprawnieniami użytkowników. Odczyt uprawnień powinien zachodzić automatycznie.

Nadawanie uprawnień powinno umożliwiać co najmniej:

- data początkowa
- data końcowa
- usuwanie po terminie ważności
- numer karty
- nazwa użytkownika
- typ karty
- grupa dostępu
- stan karty
- wydłużony czas dostępu do drzwi
- karta śledzona
- musi używać PIN
- kod PIN

Systemy depozytorów kluczy

Systemy Depozytorów Kluczy powinny mieć możliwość podłączenia do serwera integrującego za pomocą dedykowanego modułu kompatybilnego z rejestratorem lub serwerem dostarczanym przez producenta. Jako metodę komunikacji uznaje się połączenie za pomocą portu RS, protokołu TCP/IP, konwertera RS na TCP/IP.

Oprogramowanie integrujące/ wizualizujące powinno móc rejestrować zdarzenia przychodzące z integrowanego systemu depozytora kluczy w zakresie co najmniej: baza danych dostępna/niedostępna, drzwi zamknięte/otwarte, drzwi otwarte zbyt długo, drzwi zamknięte po zbyt długim otwarciu, klucz wyjęty, klucz włożony, klucz włożony w złe miejsce, zły pin x3, uprawnienia użytkowników do kluczy. Poszczególne stany elementów powinny być wizualizowane z pomocą odpowiednich ikon o różnych kolorach. Oprogramowanie integrujące z racji swojego charakteru i przeznaczenia nie może wpływać na konfigurację Depozytora Kluczy. Zapewnia to bezpieczeństwo pracy Depozytora Kluczy jako odrębnego systemu co gwarantuje niezawodność jej działania

Systemy / moduły wejść i wyjść przekaźnikowych

Systemy wejść/wyjść sieciowych powinny mieć możliwość podłączenia do serwera integrującego za pomocą dedykowanego modułu kompatybilnego z centralą, serwerem zarządzającym, dostarczanego przez producenta.

Jako metodę komunikacji uznaje się połączenie za pomocą portu RS, protokołu TCP/IP, konwertera RS naTCP/IP. Oprogramowanie integrujące/ wizualizujące powinno móc rejestrować zdarzenia przychodzące z integrowanego sieciowego modułu wejść/wyjść w zakresie co najmniej: V-1000/IOM: wejście włączone/wyłączone, wyjście włączone/wyłączone, błąd połączenia, połączenie utracono, połączony, rozłączony, wyjście PWM włączono/wyłączono, stany dla wejścia analogowego (maksymalny, wysoki, średni, niski, minimalny). Poszczególne stany elementów powinny być wizualizowane z pomocą odpowiednich ikon o różnych kolorach. Oprogramowanie integrujące powinno mieć możliwość zarządzania modułami wejść/wyjść sieciowych w zakresie (funkcje wykonawcze): V-1000/IOM: włącz/wyłącz wyjście, włącz/wyłącz wszystkie wyjścia, przełącz wyjście, przełącz wszystkie wyjścia, włącz/wyłącz PWM, ustaw wypełnienie PWM

Oprogramowanie integrujące z racji swojego charakteru i przeznaczenia nie może wpływać na konfigurację moduły wejść/wyjść sieciowych. Zapewnia to bezpieczeństwo pracy urządzenia jako odrębnego systemu co gwarantuje niezawodność jej działania.

Użyte moduły wejść/wyjść przekaźnikowych powinny posiadać możliwość podłączenia dodatkowych akcesoriów takich jak:

- płytki przekaźnikowe do 16A
- czujnik temperatury
- rozgałęziacz
- czujnik prądu do 15A
- czujnik temperatury i wilgotności

Program integrujący/wizualizujący

- Program powinien być kompatybilny z systemem operacyjnym Windows 7 i Windows 8. Użycie takiego środowiska zapewnia łatwość instalacji, oraz łatwość obsługi.
- Program powinien pracować w architekturze klient – serwer. Umożliwia to sprawne zarzadzanie architekturą sprzętową systemu oraz jego łatwą rozbudowę. Zastosowanie stacji klienckiej nie wymaga używania dodatkowego serwera integracji.
- Konfiguracja systemu powinna opierać się na panelach (oknach, widokach). Zapewnia to elastyczną i łatwą modyfikację poszczególnych widoków.
- Panele powinny mieć opcję kopiowania. Dzięki temu uzyskujemy prosty mechanizm na powielanie jednego panelu w razie konieczności dostosowania go do potrzeb wielu użytkowników.
- Program powinien umożliwiać tworzenie widoków (paneli, okien) niezależnych dla każdego z operatora. Dzięki temu każdy z użytkowników ma możliwość dostosowania interfejsu programu integrującego do własnych upodobań i potrzeb.
- Uprawnienia do programu powinny być nadawane na poziomie dostępu do paneli. Dzięki temu unika się sytuacji gdy zmiana w ustawieniach urządzenia integrowanego wpływa bezpośrednio na uprawnienia użytkowników.
- Uprawnienia nadane użytkownikowi podążają za jego loginem i hasłem. Gwarantuje to iż logując się na dowolnej stacji klienckiej użytkownik zawsze uzyska dostęp do tych samych przypisanych do niego paneli. Dodatkowo zapisany dla niego układ okien zostanie odtworzony.
- Panele powinny mieć opcję zbliżenia co w przypadku dużych obiektów z wieloma elementami umożliwia łatwe zarządzanie widokiem.
- Panele powinny mieć możliwość automatycznego zbliżenia się na element w alarmie. Stopień zoomu powinien być definiowany niezależnie dla każdego z paneli osobno.
- Informowanie o alarmie powinno odbywać się automatycznie. Dzięki temu podstawową funkcjonalność uzyskuje się już w momencie podłączenie integrowanego systemu do sytemu integrującego.
- Program powinien zapewniać możliwość tworzenia filtrów alarmów dla każdego użytkownika. Dzięki temu poszczególni operatorzy otrzymują dane tylko z interesujących ich urządzeń, stref, lokalizacji itp.
- Potwierdzenie alarmu w programie wizualizującym może wymagać podania hasła operatora i/lub wpisania komentarza.

- Program powinien umożliwiać tworzenie zaawansowanych scenariuszy zadziałania. Zastosowanie scenariuszy umożliwia stworzenie automatyki zadziałania programu, wysterowanie poszczególnych urządzeń itp. na wypadek wystąpienia zdarzenia w systemie (tzw. Reakcja).
- Scenariusze powinny być powiązane z reakcją lub reakcjami tworzonymi w programie.
- Wśród reakcji wyjściowych wyróżnia się co najmniej:
  - reakcje oprogramowania: zamknij, wyloguj, otwórz okno, uruchom program, czytaj komunikat tekstowy, email, SMS, email i inne.

• reakcje w systemach integrowanych np: uzbrój/rozbrój dla systemu SSWIN, wysteruj wyjście przekaźnikowe dla systemu SSWIN, CCTV, SKD, sieciowych modułów WE/WYJ i inne.

- Każda ze stworzonych reakcji powinna być opatrzona parametrem „opóźnienie". Dzięki temu możliwe jest stworzenie sekwencji działań programu na wypadek zajścia zdarzenia.
- Oprogramowanie powinno mieć możliwość czytania komunikatów generowanych przez użytkownika i komunikatów alarmowych. Opcja czytanie powinna być realizowana przez syntezator mowy. Wybór rodzaju/producenta syntezatora mowy nie powinien być ograniczony.
- Wyzwolenie scenariusza może odbywać się na: wystąpienie zdarzenia (np.: alarm, naruszenie, detekcja ruchu, pożar, i inne), zmianę stanu urządzenia (np.: rozłączony, połączony, alarm aktywny, wejście aktywne i inne), na określony czas (np.: o 12:00, 15:15 itd.) z dokładnością co 15 minut.
- Wystąpienie zdarzenia lub zmiana stanu urządzenia może być powiązana dodatkowo z harmonogramem. Umożliwia to stworzenie scenariusza z ograniczeniami czasowymi.
- Akcje wyzwalające scenariusz mogą być ze sobą powiązane logicznie poprzez zastosowanie warunków logicznych AND lub OR. Akcje wyzwalające mogą być grupowane w nawiasy. Taka funkcjonalność zapewnia możliwość tworzenia bardzo zaawansowanych warunków wystąpienia zdarzenia.
- Wszystkie scenariusze i reakcje powinny mieć możliwość kopiowania. Zapewnia to możliwość szybkiego powielania scenariuszy i reakcji i dostosowywania ich pod wymagania poszczególnych użytkowników.
- Przeszukiwanie listy logów zapisanych w bazie powinno się odbywać z możliwością ich filtrowania. Filtrowanie powinno się odbywać na poziomie urządzeń, użytkowników, osób, aplikacji oraz akcji przychodzących m.in. alarm, alarm przymusu, błąd email, błąd logowania, błąd połączenia, błąd synchronizacji czasu, dostęp zabroniony/zezwolony, kartę dodano/usunięto/zmodyfikowano, koniec alarmu/naruszenia w alarmie/sabotażu/uszkodzenia, logowanie, zły format daty i czasu, zmiana konfiguracji i inne dostępne w programie.
- Wyszukana i wyfiltrowana lista zdarzeń powinna móc się zapisać do co najmniej formatu pdf.
- Połączenie stacji klienckiej do serwera odbywa się dwustopniowo. Gwarantuje to podwyższony poziom bezpieczeństwa, dzięki czemu nieuprawnione osoby nie będą miały dostępu do systemu.
- Oprogramowanie powinno pozwalać definiować punkty nawigacyjne (wskaźniki) na panelu. Dzięki temu dostępna jest funkcja wirtualnych obchodów na panelu co w przypadku dużych, rozległych systemów jest pożądane.
- Oprogramowanie powinno mieć możliwość tworzenia wielozadaniowych obiektów. Obiekty te powinny móc zmieniać kolor oraz sposób działania w zależności od stanu wybranego lub wybranych elementów w systemie, harmonogramu czasu, wystąpienia zdarzenia.
- Oprogramowanie powinno mieć możliwość zdefiniowania parametrów serwera poczty email używanego do przesyłania informacji po wystąpieniu zdarzenia.

4.8 Montaż

- Detektory ruchu montować w koordynacji z aranżacją pomieszczenia w celu eliminacji martwych stref,
- Elementy systemu alarmowego montować zgodnie z zaleceniami producenta, podłączenia linii dozorowych wykonać jako podwójnie zbalansowane, rezystorami 4,7kΩ (zgodnie z kartą katalogową urządzeń). Sprawdzić adresowanie wszystkich modułów, sprawdzić działanie wszystkich linii dozorowych pod kątem sygnalizacji włamania oraz sabotażu. Przeprowadzić inicjację centrali alarmowej, programować zgodnie z instrukcją producenta i wymaganiami użytkowników z komputera PC z pomocą oprogramowania technicznego.
- Ochroną przejść przez stropy i ściany:
    - Wszystkie przepusty przez ściany i stropy uszczelnić atestowanymi materiałami o odpowiedniej odporności ogniowej

5. Wskazówki eksploatacyjne

Dla instalatora po uruchomieniu systemu:

1. sprawdzić działanie wszystkich elementów systemu SwiN, SKD oraz CCTV,

2. sprawdzić transmisję kryterium alarmu do Alarmowego Centrum Odbiorczego,

3. w STD sprawdzić archiwizację zdarzeń, wyszukiwanie zdarzeń i odtwarzanie,

4. dostarczyć użytkownikowi:

- pisemne instrukcje obsługi systemu, w tym instrukcje użytkownika

- rejestr obsługi systemu

2. praktycznie zademonstrować działanie systemu i przeszkolić z obsługi systemu

wskazanych przez użytkownika pracowników

3. sporządzić oraz przekazać:

− protokół zdawczo - odbiorczy systemu

− deklaracje zgodności wykonanych systemów,

− zaświadczenia kwalifikacyjne, certyfikaty lub aprobaty techniczne zainstalowa-

nych materiałów i urządzeń

− dokumentację powykonawczą z naniesionymi zmianami.

− Odbiór końcowy systemu poprzedzony będzie próbnym okresem eksploatacji

przez okres 21 dni od dnia uruchomienia systemu (Rozporządzenie Ministra Kultury i

Dziedzictwa Narodowego z dnia 2 września 2014 r. w sprawie zabezpieczania zbiorów muzeum

przed pożarem, kradzieżą i innym niebezpieczeństwem grożącym ich zniszczeniem lub utratą).

Wskazówki eksploatacyjne:

Konserwacja i testowanie systemu

- w pierwszym roku eksploatacji testowanie systemu prowadzić jeden raz na trzy miesiące zwracając szczególną uwagę na awaryjne źródła zasilania,
- podczas sprawdzania systemu realizować „test chodzenia”
- przydzielić kody dostępu tylko niezbędnym użytkownikom dobierając odpowiednio poziomy dostępu
- zachować szczególne środki ostrożności przy wprowadzaniu kodu Administratora
- prowadzić raz w miesiącu wyrywkowy przegląd zdarzeń

6. Bramy wjazdowe

Zgodnie z wytycznymi projektuje się zasilanie siłowników dwóch bram wjazdowych od ulicy Moniuszki. Należy zasilić oraz wyprowadzić sterowanie z pomieszczenia szatni na parterze 1.2. Z pomieszczenia tego projektuje się umieszczenie przycisku do zamknięcia obu bram oraz możliwość otwierania i zamykania bram i szlabany za pomocą pilotów.

7. Ochrona od porażeń prądem elektrycznym

Z punktu widzenia ochrony przeciwporażeniowej sieć odbiorcza będzie pracować w układzie TN-S z osobnymi przewodami ochronnymi PE i przewodem neutralnymi N. Rozdział przewodu PEN na przewód PE i N w rozdzielnicy TG. Punkt rozdziału należy uziemić. Dla wszystkich tablic rozdzielczych projektuje się system prądu przemiennego 5-przewodowy (L1,L2,L3, N i PE).

Jako środek ochrony dodatkowej przed dotykiem zastosowano szybkie samoczynne wyłączenie zasilania. Dodatkowo w obwodach gniazd zastosowano wyłączniki przeciwporażeniowe różnicowoprądowe o znamionowym prądzie różnicowym 0,03A.

8. Obliczenia techniczne

- Spadki napięć na instalacjach wewnętrznych zgodnie z normą.
- Czasy wyłączenia prądów zwarciowych dla przyjęte średnic przewodów zachowane.
- Urządzenia dobrane na prądy zwarciowe.

9. Uwagi końcowe

- całość instalacji wykonać zgodnie z obowiązującymi normami i przepisami z zachowaniem przepisów BHP,
- instalacje elektryczne układać po wykonaniu głównych robót budowlanych,
- po wykonaniu instalacji dokonać niezbędnych pomiarów,
- Instalację teletechniczną układać w korytach kablowych.
- ***Zaproponowane w projekcie rozwiązania materiałowe, urządzenia, elementy i technologie należy traktować jako wymagany standard jakości a nie wybór producenta. Dopuszcza się rozwiązania równorzędne pod warunkiem spełnienia założonych parametrów technicznych, estetycznych i formalno-prawnych zgodne z opisem technicznym rozwiązań materiałowych***.

Projektował: mgr inż. Piotr Markowski

upr. proj. ZAP/0218/POOE/11

Sprawdził: mgr inż. Mariusz Piątkowski

upr. proj. ZAP/0125/PWOE/11