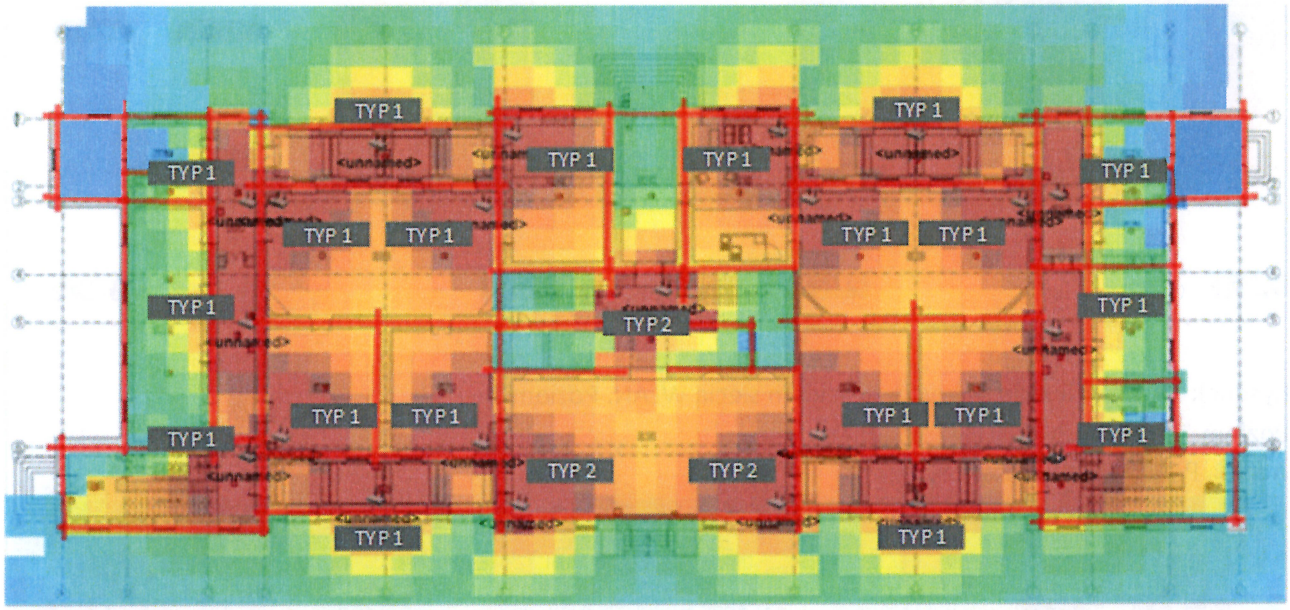
1152

Rysunek 10.2. Symulacja pokrycia zasięgiem siecią WLAN. Poziom -1

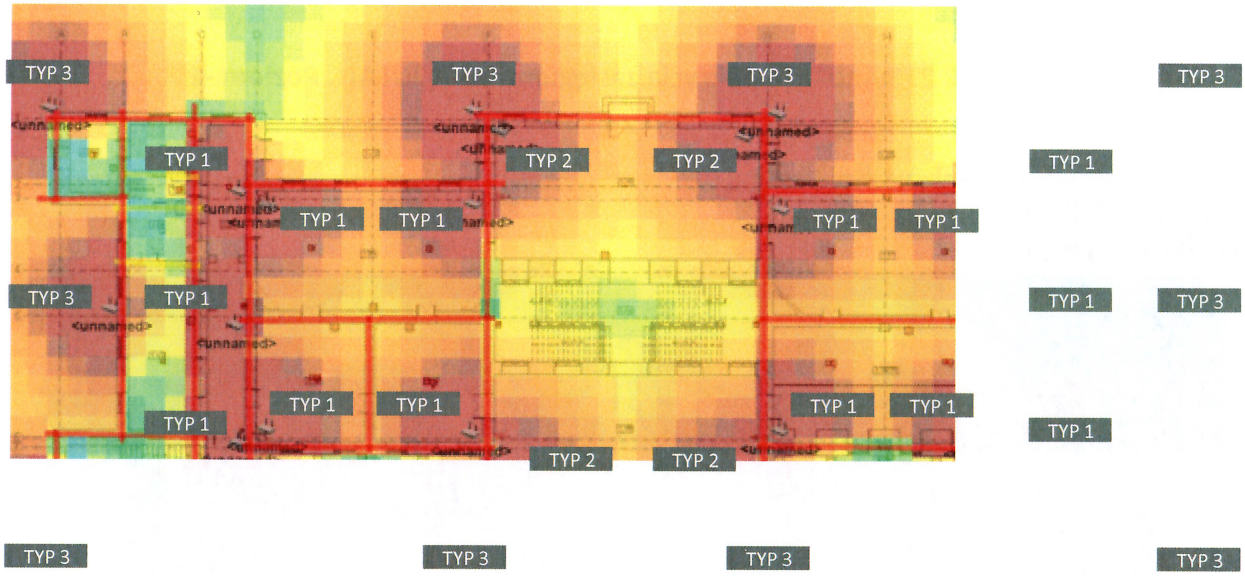
Poziom 0: PAS-120-PB-IT-LAN-R-02
Access Point TYP 1 Ilość: 20
Access Point TYP 2 Ilość: 3



Rysunek 10.3. Symulacja pokrycia zasięgiem siecią WLAN. Poziom 0

Poziom 1: PAS-120-PB-IT-LAN-R-03
Access Point TYP 1 Ilość: 14
Access Point TYP 2 Ilość: 4
Access Point TYP 3 Ilość: 10

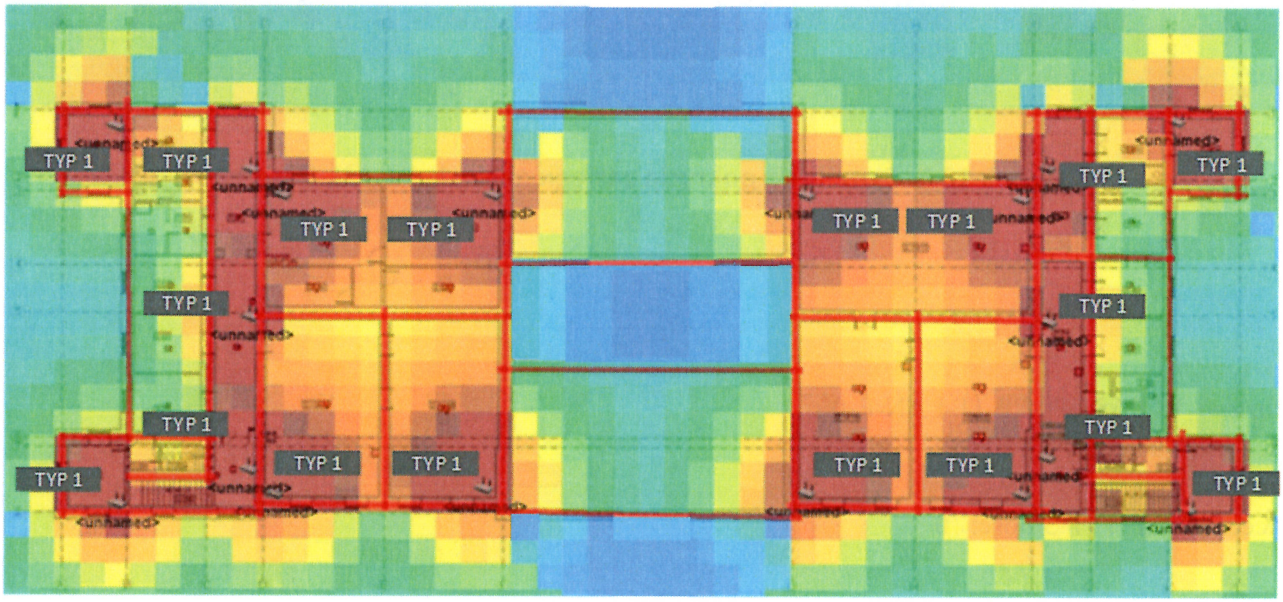
1153



Rysunek 10.4. Symulacja pokrycia zasięgiem siecią WLAN. Poziom 1

Poziom 2: PAS-120-PB-IT-LAN-R-04

Access Point TYP 1 Ilość: 18



Rysunek 10.5. Symulacja pokrycia zasięgiem siecią WLAN. Poziom 2

Poniższa tabela określa ilości punktów dostępowych per kondygnacja z podziałem na typ.

Tabela 10-2. Zestawienie ilościowe AP z podziałem na typ.

		Ilość AP		
Lp.	Poziom	TYP 1	TYP 2	TYP 3
1	-1	20		
2	0	20	3	

3	1	14	4	10
4	2	18		
SUMA		**72**	**7**	**10**

Zestawienie ilościowe AP z podziałem na typ.

Do punktów WIFI zewnętrznych należy zastosować urządzenia typu Net Protector, który pozwoli na zachowanie toru transmisyjnego. Urządzenie musi być montowane na wejściu do budynku w korytach i podłączone do uziemienia koryta. Wymaga się pełnego dostępu serwisowego np. rewizji.

W związku z wymogiem centralnego zarządzania całą siecią WLAN za pomocą posiadanego przez Zamawiającego klastra kontrolera sieci WLAN model Alcatel-Lucent OAW-4550 należy dokupić dodatkowe licencje w pełni kompatybilne z obecnie posiadanymi przez Zamawiającego kontrolerem WLAN

Tabela 10-3. Dodatkowe lic. oraz wpsarcie do lic. na kontroler sieci WLAN OAW-4550

	Ilość [szt .]	Wsparcie 3 letnie [szt.]
Licencje do obsługi przez kontroler kolejnych AP	89	89
Licencje typu Firewall	89	89

Dodatkowe licencje oraz wsparcie do licencji na kontroler sieci WLAN OAW-4550

Wraz z rozbudową kontrolera sieci WLAN o dodatkowe licencje do obsługi nowych punktów dostępowych przewidziano odnowienie kontraktu serwisowego na 3 lata dla:

- oprogramowania OV3600 do zarządzania siecią WLAN
- 204 licencje AirWave obecnie działające na systemie OV3600

Tabela 10-4. Zestawienie kontraktów serwisowych niezbędnych do odnowienia kontraktu dla systemu OV3600 oraz obecnych lic. typu AirWave.

	Ilość [szt .]	Wsparcie 3 letnie [szt.]
Odnowienie kontraktu serwisowego dla OV3600-MASTER	1	1
OV3600-AM	204	204

Zestawienie kontraktów serwisowych niezbędnych do odnowienia kontraktu dla systemu OV3600 oraz obecnych licncji typu AirWave

Parametry dla poszczególnych typów Access Point znajdują się w STWiOR

11. SYSTEM TELEFONII ABONENCKIEJ

Aktualnie w obiekcie zainstalowana jest autonomiczna cyfrowa abonencka centrala telefoniczna typu Coral firmy Tadiran, współpracująca z siecią użytku publicznego za pośrednictwem łącza ISDN PRA.

Projektuje się nowy system telefonii abonenckiej jako moduł wyniesiony istniejącej w siedzibie głównej Zamawiającego przy ul. Niepodległości 213 centrali telefonicznej (serwera telekomunikacyjnego) VoIP Alcatel-Lucent OmniPCX Enterprice (WARIANT: 1a, 1b) lub jako odrębną abonencką centralę telefoniczną typu VoIP z możliwością obsługi linii analogowych (WARIANT 2a, 2b). Schemat blokowy projektowanej centrali telefonicznej pokazano na rysunku zamieszczonym w projekcie.

Urządzenia abonenckiego systemu telefonicznego zainstalować w szafie BPD-12 zgodnie z przykładowym zagospodarowaniem, pokazanym na rysunku zagospodarowania szaf 19". W przypadku innego zagospodarowania szafy, Wykonawca dokona stosownych uzgodnień z Projektantem.

Dla przyłączenia wewnętrznych aparatów telefonicznych wykorzystać sieć strukturalną LAN w części dedykowanej dla telefonii.

Do krosowań w szafie 19" stosować wyłącznie patch-cordy RJ45-RJ45 tego samego typu i koloru (zgodnie z przyjętym kodem kolorystycznym dla obiektu) oraz odpowiednio dobranej długości nie dłuższe niż 0,5m, aby nie powodować powstawania plątaniny podczas eksploatacji systemu. Do podłączeń wszelkich urządzeń końcowych do gniazd sieci LAN stosować wyłącznie kable przyłączeniowe, zakończone od strony gniazd wtykami RJ45.

Podłączenie zewnętrznych przyłączy telekomunikacyjnych wykonać poprzez odpowiednie krosowania w BPD-1 oraz w budynkowym punkcie styku PS.

Wszelkie instalacje oraz programowanie i uruchomienie systemu wykonać zgodnie dokumentacją techniczno-ruchową producenta oraz tabelami programowymi, uzgodnionymi na roboczo z Zamawiającym.

Projekt systemu telefonicznego (centrali abonenckiej) został zaprojektowany na podstawie szczegółowych wytycznych Zamawiającego.

Dane ogólne systemu

pojemność wewnętrzna: minimum 48 z możliwością rozbudowy do minimum 64,

obsługa ruchu zewnętrznego: ISDN PRA, minimum 8x PSTN, VoIP minimum 2 Mb/s,

połączenia przychodzące: automatyczne w systemie numeracji DDI oraz dla wyznaczonych numerów półautomatyczne za pośrednictwem obsługi stanowiska pośredniczącego (awiza),

połączenia wychodzące: automatyczne, po wybraniu jedno-cyfrowego prefiksu

połączenia do centrali nadrzędnej BN: skrócone, po wybraniu numeru wewnętrznego lub prefiksu i numeru wewnętrznego. Zakres integracji usług zgodnie z zastosowanym rozwiązaniem technicznym,

numeracja wewnętrzna: 4-cyfrowa, skorelowana z numeracją w siedzibie głównej przy al. Niepodległości 213.

Wymagania funkcjonalne wobec systemu

System powinien posiadać standardowe możliwości usługowe, oferowane przez współczesne centrale abonenckie, pracujące w sieciach korporacyjnych o jednolitej numeracji DDI z pełną integracją usług. W szczególności wymagane są następujące funkcje:

- identyfikacja abonenta wywołującego
- klasy abonentów – możliwość określenia wyjść na poszczególnych numerach
- grupy wywoływania
- grupy przechwytywania połączeń
- przekierowanie połączeń: natychmiastowe, przy zajętości i braku odpowiedzi
- przekierowanie połączeń na linie zewnętrzne
- zakaz przekierowania na określone kierunki

organizacja połączeń przychodzących w ramach call-center określone na etapie uruchomienia systemu łącza przychodzące będą obsługiwane automatycznie w systemie call center w minimum 4-stopnioym drzewie decyzyjnym automatycznego wyboru połączenia (ACD). Możliwość powrotu z dowolnego miejsca drzewa do pozycji startowej.

Przykładowy schemat dystrybucji ilustruje poniższa tabela:

KROK 1			KROK 2		KROK 3		KROK 4	
Start	Wybór 1	Cel	Wybór 2	Cel	Wybór 3	Cel	Wybór 4	Cel

- sygnał marszrutowania podczas wybierania połączeń
- gorąca linia
- połączenia konferencyjne i naprzemienne
- zawieszanie i parkowanie połączeń
- wielokrotne przełączanie połączenia do innego abonenta
- informacja o połączeniu oczekującym
- automatyczne oddzwanianie
- rezerwacja połączenia do abonenta zajętego
- możliwość zaprogramowania co najmniej 8 układów sekretarsko-dyrektorskich dla co najmniej 3 abonentów w każdej grupie
- muzyka podczas podtrzymania
- funkcja „nie przeszkadzać"

- abonent wywołujący abonenta wewnętrznego systemu w ruchu przychodzącym i lokalnym powinien otrzymać sygnał zajętości w przypadku jego zajętości.
- możliwość zarządzania systemem centrali przez graficzny interfejs przy użyciu komputera
- szczegółowe raporty o połączeniach wychodzących
- możliwość wyszukiwania abonentów w książce telefonicznej z poziomu klawiatury alfabetycznej aparatu
- połączenia alarmowe
- możliwość zabezpieczenia telefonu kodem PIN lub hasłem

Wymagania funkcjonalne wobec aparatów telefonicznych

a.) Parametry dla telefonów systemowych VoIP – 8 sztuk

- klawiatura numeryczna
- klawiatura alfabetyczna
- wyświetlacz graficzny minimum 5 linii tekstu
- wyświetlanie daty i godziny
- wyświetlanie numerów lub nazw dla identyfikacji połączeń
- przyciski nawigacyjne umożliwiające sprawne nawigowanie funkcjami telefonu na wyświetlaczu
- przyciski programowalne bezpośredniego wyboru abonenta - co najmniej 8 szt.
- możliwość zaprogramowania dodatkowych przycisków funkcyjnych
- aparat telefoniczny zasilany z PoE bez konieczności stosowania zasilacza w aparacie
- możliwość podłączenia zasilacze zewnętrznego w aparacie telefonicznym
- wbudowany głośnik umożliwiający prowadzenie rozmowy bez podnoszenia słuchawki z funkcją regulacji głośności
- możliwość podłączenie słuchawki nagłownej
- wybór języka komunikatów systemowych w tym język polski

b.) Parametry dla telefonów VoIP – 40 sztuk

- klawiatura numeryczna
- wyświetlacz graficzny minimum 1 linii tekstu
- wyświetlanie daty i godziny
- wyświetlanie numerów lub nazw dla identyfikacji połączeń
- przyciski nawigacyjne umożliwiające sprawne nawigowanie funkcjami telefonu na wyświetlaczu
- przyciski programowalne bezpośredniego wyboru abonenta - co najmniej 4 szt.
- możliwość zaprogramowania dodatkowych przycisków funkcyjnych
- aparat telefoniczny zasilany z PoE bez konieczności stosowania zasilacza w aparacie
- możliwość podłączenia zasilacze zewnętrznego w aparacie telefonicznym
- wbudowany głośnik umożliwiający prowadzenie rozmowy bez podnoszenia słuchawki z funkcją regulacji głośności
- możliwość podłączenie słuchawki nagłownej
- wybór języka komunikatów systemowych w tym język polski

Należy dostarczyć dodatkowo 15 zasilaczy dla telefonów VoIP.

Uwagi do Wykonawcy

Obowiązkiem wykonawcy jest zapewnienie wszystkich elementów sprzętowych i licencyjnych umożliwiających realizację wskazanych powyżej funkcji nowej centrali telefonicznej oraz ewentualne uzupełnienie istniejącego systemu Alcatel-Lucent w siedzibie głównej Zamawiającego przy al. Niepodległości 213. Jeżeli do rozbudowy niezbędne będzie podniesienie wersji oprogramowania centrali telefonicznej przy Al. Niepodległości 213 do wyższej wersji Wykonawca na własnym koszt i własnym staraniem zakupi wszystkie stosowne licencje i przeprowadzi upgrade oprogramowania do wymaganej wersji. Upgrade zostanie przeprowadzony przez certyfikowanego inżyniera posiadającego stosowny certyfikat Alcatel-Lucent.

Wykonawca w pełni odpowiada za prawidłowy dobór wszystkich elementów systemu telefonicznego wraz z dostosowaniem parametrów transmisyjnych, decydujących o wysokiej jakości świadczonych usług głosowych i transmisji danych (w tym także na potrzeby telefaksów i terminali płatniczych). Przez zachowanie wysokiej jakości świadczonych usług należy w szczególności rozumieć nie występowanie niekorzystnych efektów, takich jak:

- pogłos, trzaski i inne sygnały zakłócające podczas prowadzonej rozmowy telefonicznej,
- zbyt niski poziom słyszalności prowadzonej rozmowy,
- „zrywanie" trwających połączeń,
- zniekształcenia treści dokumentów w transmisji telefaksowej,
- brak lub niewłaściwe sygnały informacyjne podczas realizacji połączeń (np. brak zwrotnego sygnału wywołania),
- brak właściwej prezentacji numeru abonenta wywołującego dla połączeń wychodzących.

Przed przystąpieniem do realizacji Wykonawca przedstawi:

- proponowaną konfigurację systemu
- szczegóły instalacyjne urządzeń
- szczegóły podłączeń kablowych i krosowań
- niezbędne i czytelne rysunki warsztatowe
- tabele programowe dla wszystkich funkcji systemu wraz z propozycją konfiguracji softwarowej
- zestawienie wymaganych przyłączy telekomunikacyjnych

12. INSTALACJA PRZYZYWOWA

Istniejąca instalacja zostanie zmodernizowana o kolejne elementy dla toalet osób niepełnosprawnych. Okablowanie platformy dla osób niepełnosprawnych przed wejściem od strony południowej oraz platformy wewnątrz budynku zostanie doprowadzone do nowego pomieszczenia. Centrala przyzywowa dla osób niepełnosprawnych zostanie przeniesiona do nowo powstałego pomieszczenia 2.11a na poziomie +2.

Wszystkie nowe łazienki dla osób niepełnosprawnych zostaną wyposażone w nowe elementy systemu. Funkcja systemu pozostanie bez zmian.

System, powinien spełniać europejską normę VDE 0834 część 1 w obszarze zastosowania A.

Zadaniem systemu przywoławczego dla osób niepełnosprawnych jest zapewnienie możliwości wezwania pomocy - obsługi obiektu w przypadku wystąpienia utrudnień podczas korzystania z pomieszczenia zamkniętego, jakim jest pomieszczenie toalety dla niepełnosprawnych.

Toalety nowopowstałe dla niepełnosprawnych zlokalizowano w kilku lokalizacjach na poziomie parteru i piętra +1 jako ogólnodostępne dla użytkowników obiektu.

Użytkownik podczas korzystania z toalety powinien mieć możliwość w każdej chwili i bezzwłocznie powiadomić osoby znajdujące się na zewnątrz toalety oraz w pomieszczeniu 2.11a o potrzebie interwencji i udzielenia pomocy. W celu zapewnienia takiej komunikacji wewnątrz pomieszczenia toalety będzie zamontowany przycisk pociągowy zlokalizowany w zasięgu ręki osoby korzystającej z umywalki i miski ustępowej, a także w przypadku upadku na podłogę.

Szczegółowe rozmieszczenie i funkcje elementów pokazano na rzutach instalacji strukturalnej LAN oraz na schemacie blokowym systemu.

PRZYCISK POCIĄGOWY

Przycisk pociągowy ma być zamontowany wewnątrz pomieszczenia na wysokości 2,4m od posadzki w puszce podtynkowej, jako wpuszczany. Cięgło przycisku doprowadzić do 30cm od posadzki w celu zapewnienia możliwości pociągnięcia w przypadku upadku osoby korzystającej z pomieszczenia i zakończyć elementem naciągowym. Pod przyciskiem na wysokości 1,6m od posadzki należy zamontować opis działania systemu i zasady korzystania. Opis ma być wykonany w języku polskim i w sposób trwały przymocowany do ściany. Ze względu na charakter pomieszczenia opis należy zabezpieczyć przed wilgocią.

SYGNALIZATOR AKUSTYCZNY I OPTYCZNY (LAMPKA)

Sygnalizator ma być zamontowany na zewnątrz pomieszczenia toalety dla niepełnosprawnych, nad drzwiami wejściowymi na wysokości 2,5m od posadzki. Montować, jako podtynkowy w puszcze montażowej. Pod sygnalizatorem ma być umieszczona instrukcja postępowania oraz informacja, czego dotyczy sygnał alarmowy. Opis ma być wykonany w języku polskim i w sposób trwały przymocowany do ściany.

PRZYCISK KASUJĄCY

Przycisk kasujący ma być zamontowany na zewnątrz pomieszczenia na wysokości 1,6m od posadzki w odległości 10cm od ościeżnicy drzwi wejściowych po przeciwnej stronie, co zawiasy drzwi. Montować, jako podtynkowy w puszcze montażowej. Pod przyciskiem należy zamontować opis działania systemu i zasady korzystania. Opis ma być wykonany w języku polskim i w sposób trwały przymocowany do ściany.

ZASILANIE

Zasilacz systemu (np. transformator) należy zamontować w przestrzeni nad sufitem podwieszonym w miejscu niedostępnym dla osób postronnych Zasilanie z sieci 230V dla systemu przewidziano w projekcie instalacji elektrycznych. System nie wymaga zasilania awaryjnego.

MATRYCA SYGNALIZACJI WEZWANIA ALARMU

W pomieszczeniu 2.11a należy zamontować kontroler sygnalizacji wezwania alarmu, który będzie informował pracowników sygnałem świetlnym i dźwiękowym o zaistniałej sytuacji alarmowej w toalecie dla niepełnosprawnych. Na kontrolerze tym będą wyświetlane informacje dokładnie identyfikujące pomieszczenie skąd zostało wysłane wezwanie.

13. SYSTEM SYGNALIZACJI WŁAMANIA I NAPADU

13.1. Opis stanu istniejącego

W obiekcie funkcjonuje klasyczny system alarmowy zorganizowany w oparciu o czujki bezprzewodowe firmy Satel ABAX. Jego działanie ogranicza się do podstawowego zabezpieczenia przestrzeni wewnętrznych tras komunikacyjnych i wybranych pomieszczeń. Podgląd stanu systemu jest realizowany przy wykorzystaniu klawiatury kodowej SATEL LCD zainstalowanej w przestrzeni nadzorowanej przez pracownika ochrony. Obecnie funkcjonujące urządzenia i elementy infrastruktury kablowej należy w całości zdemontować i przekazać Zamawiającemu lub zutylizować w zależności od uzgodnień na etapie wykonawczym.

13.2. Opis projektu

Celem zastosowania SSWiN jest objęcie ochroną przeciwwłamaniową i przeciwnapadową całej przestrzeni obiektu z uwzględnieniem jego podziału funkcjonalno-użytkowego, w szczególności sal wystawienniczych, pomieszczeń przygotowania wystaw, pomieszczeń administracyjnych i technicznych, drzwi ewakuacyjnych i międzystrefowych oraz wyposażenie pracowników w urządzenia do sygnalizacji napadu.

System Sygnalizacji Włamania i Napadu ma za zadanie ochronę wszystkich pomieszczeń przed włamaniem oraz podniesienie bezpieczeństwa obsługi w przypadku napadu.

Ochrona pomieszczeń przed włamaniem jest realizowana poprzez zastosowanie:

- pasywnych czujek podczerwieni, przestrzennych oraz kurtynowych – PIR, z funkcją antymaskingu;
- dualnych czujek pasywnych podczerwieni i mikrofalowych – PIR/MW, z funkcją antymaskingu;
- czujek otwarcia stykowych (magnetycznych) tzw. kontaktronowych z ochroną antysabotażową;

Ochrona wejść do budynku jest zrealizowana poprzez zastosowanie:

- dualnych czujek pasywnych podczerwieni i mikrofalowych – PIR/MW, z funkcją antymaskingu;
- czujek otwarcia stykowych (magnetycznych) tzw. kontaktronowych z ochroną antysabotażową - w drzwiach.

Ochrona szachtów kablowych i wentylacyjnych oraz rozdzielnic elektrycznych realizowana jest poprzez zastosowanie:

- czujek otwarcia stykowych (magnetycznych) z ochroną antysabotażową w drzwiach do szachtów oraz drzwiach rewizyjnych;

Ochrona poddasza jest zrealizowana poprzez zastosowanie:

- czujek otwarcia stykowych (magnetycznych),

Ochrona zewnętrzna jest zrealizowana poprzez zastosowanie:

- dualnych czujek pasywnych podczerwieni i mikrofalowych – PIR/MW, z funkcją antymaskingu – do zastosowań zewnętrznych;

Sygnalizacja napadu jest realizowana w oparciu o:

- stacjonarne przyciski antynapadowe (przewodowe);
- mobilne przyciski antynapadowe (radiowe);

Zainstalowany system alarmowy ma wydzielone cztery podstawowe strefy detekcji:

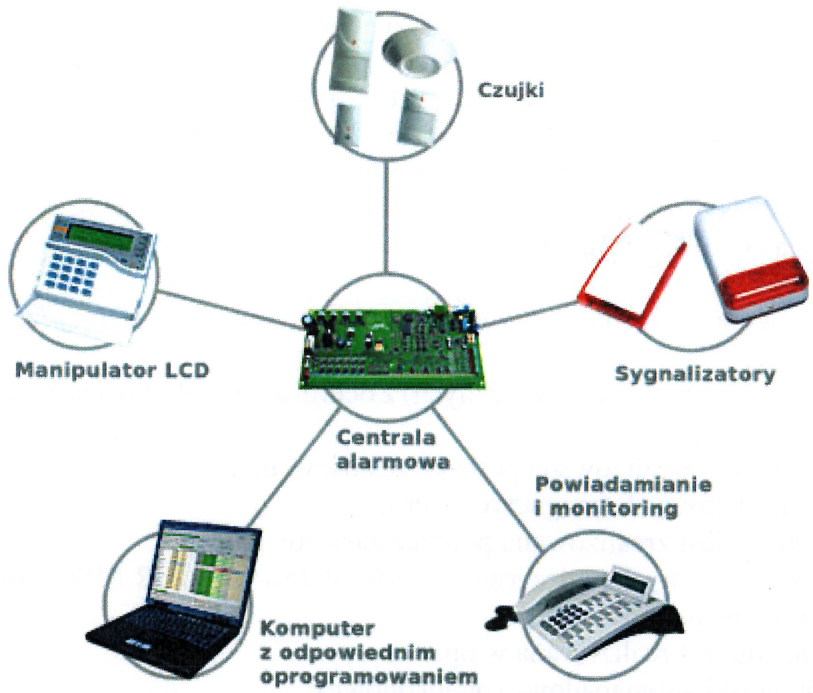
- **Strefa alarmowa 1** – chroniąca wnętrze obiektu - zbiory biblioteczne oraz sale Rycerską i Kariatyd;
- **Strefa alarmowa 2** – chroniąca wnętrze obiektu – pomieszczenia administracyjne i techniczne oraz komercyjne (restauracyjne i sklepowe);
- **Strefa alarmowa 3** – chroniąca otwory drzwiowe i okienne;
- **Strefa alarmowa 4** – chroniąca zewnętrzną część obiektu (zewnętrzne balkony);

Rozmieszczenie poszczególnych urzadzęń oraz przykładowy schemat blokowy pokazano na rysunkach nr.:

- PAS-120-PW-IT-SB-R-01-Rzut- piwnica
- PAS-120-PW-IT-SB-R-02-Rzut- parter
- PAS-120-PW-IT-SB-R-03-Rzut- piętro 1
- PAS-120-PW-IT-SB-R-04-Rzut- piętro 2
- PAS-120-PW-IT-SB-R-05-Rzut- poddasze
- PAS-120-PW-IT-SSWiN-SCH-05- Schemat, System Sygnalizacji Włamnia i Napadu

13.3. Opis organizacji SSWiN

Centralnym punktem systemu jest modułowa centrala alarmowa adresowalna z wbudowanym interfejsem TCP/IP umożliwiającym zarządzanie systemem ze Stanowiska Operatorskiego oraz za pośrednictwem dedykowanych paneli sterujących LCD.



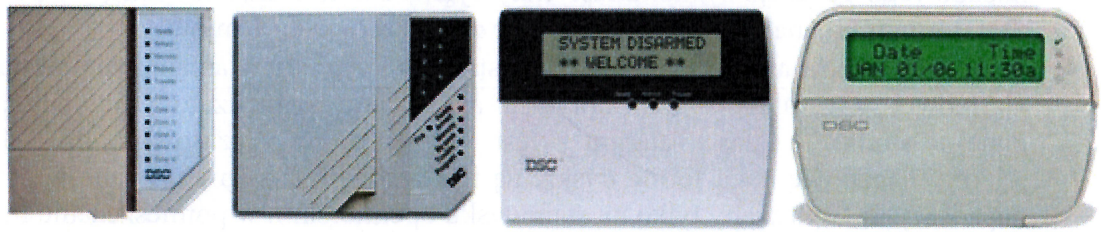
Rysunek 13.1. Przykładowa struktura systemu SSWiN

Klawiatury rozmieszczono w odpowiednich strefach umożliwiając obsługę podsystemu/strefy alarmowej. Nadzór i sterowanie SSWiN odbywa się ze stanowiska operatorskiego, obsługiwanego przez pracowników ochrony (operatorów). W tym celu SSWiN został zintegrowany z SMS (Security Management System). Dzięki takiemu rozwiązaniu istnieje możliwość centralnej wizualizacji wszystkich stanów systemu/ów oraz rejestracji zdarzeń.

System SWiN jest zbudowany zgodnie z wymogami normy PN-EN 50131-1:2009: Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Wymagania systemowe dla stopnia zabezpieczenia 2.

Obsługa systemu jest możliwa za pomocą:

- Klawiatur strefowych rozmieszczonych w następujących miejscach obiektu:
  - Korytarz administracyjny - poziom piwnicy
  - Korytarz administracyjny - poziom parteru
  - Pomieszczenia restauracyjne - poziom parteru
  - Korytarz administracyjny - poziom +1
  - Korytarz administracyjny - poziom +2
  - Pomieszczenie ochrony - poziom +2



Rysunek 13.2. Przykładowe klawiatury strefowe.

- Zintegrowanej stacji operatorskiej SMS
  - Zlokalizowanej w pomieszczeniu monitoringu (pomieszczenie ochrony WSO) za pomocą aplikacji z wydzieloną częścią przeznaczoną do zarządzania SSWiN;

Rysunek 13.3. Przykładowa aplikacja integrująca

Sygnalizacja stanów alarmowych zgłaszanych przez SSWiN realizowana jest:

- na stacji operatorskiej monitoringu, graficznie i dźwiękowo, obsługiwanej przez operatora. Graficzna postać zdarzenia zawiera datę, godzinę, miejsce wystąpienia zdarzenia oraz jego rodzaj. Każdorazowo zgłaszane przez system zdarzenie musi zostać potwierdzone przez operatora przy użyciu odpowiedniej komendy opisanej w instrukcji użytkowania SSWiN;

Rysunek 13.4. Przykładowa sygnalizacja alarmu w centrum monitoringu.

- przez wewnętrzne sygnalizatory akustyczno-optyczne:
  - 1 szt. - zlokalizowanym w pomieszczeniu ochrony - wyzwolenie alarmu włamaniowego lub napadowego generuje sygnał akustyczny sygnalizatora zainstalowanego w pomieszczeniu monitoringu. Sygnalizowanie jest ograniczone czasowo do 1 minuty.
  - 2 szt. - zlokalizowane w poszczególnych strefach - sygnały włamaniowe powstałe w strefie alarmowej wyzwalają sygnał optyczno-akustyczny sygnalizatora przyporządkowanego danej strefie. Czas alarmu jest ograniczony czasowo do 1 minuty. Alarmy napadowe mają formę dyskretną i nie mogą być sygnalizowane w strefie. Alarm napadowy jest zgłaszany tylko na stanowisku operatorskim w pomieszczeniu monitoringu.

- przez klawiatury strefowe (LCD)

  Zdarzenia alarmowe (za wyjątkiem sygnałów napadowych) są sygnalizowane akustycznie przez wewnętrzny przetwornik elektroakustyczny klawiatury strefowej. Obsługa alarmu tj. wyłączenie alarmu, sprawdzenie statusu etc. jest możliwa po zastosowaniu hasła dostępu tylko przez osobę posiadającą uprawnienia do obsługi danej strefy np.:
  - administrator systemu;
  - pracownik strefy;
  - operator monitoringu;

- za pomocą wiadomości SMS lub mail wysłanej do wybranych osób (opcja).

W przypadku wystąpienia alarmu w danej strefie (grupie), następuje proces alarmowania polegający na:

- przesłaniu informacji do centrali alarmowej,
- rejestracji alarmu w pamięci centrali,
- wysterowaniu wyjść alarmowych – wysterowaniu sygnalizatorów,
- sygnalizacji graficznej oraz dźwiękowej na klawiaturze sterującej,
- wyświetleniu informacji, zobrazowaniu jej na planie oraz sygnalizacji dźwiękowej na stacji operatorskiej,

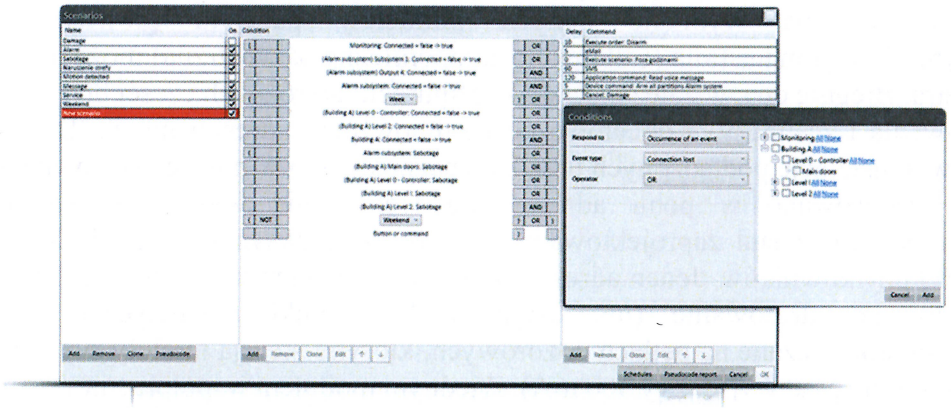
- weryfikacji alarmu przez pracownika ochrony - operatora (osobiście lub z wykorzystaniem STD),
- potwierdzeniu obsługi alarmu.

13.4. Sygnalizacja alarmów technicznych i stanu systemu

W celu przekazywania informacji dotyczących stanu omawianego systemu centrala alarmowa generuje sygnały techniczne. Różnorodność i ich specyfika pozwala na wstępne zdiagnozowanie stanu systemu tj. awaria podzespołu, brak zasilania podstawowego, rozładowanie akumulatora etc.

Wszystkie stany alarmowe dotyczące stanu technicznego SSWiN wyświetlane są za pomocą aplikacji SMS na ekranie stacji roboczej w pomieszczeniu monitoringu. Adekwatnie do rodzaju zdarzenia operator monitoringu zgodnie z przyjętą procedurą wykonuje dalsze czynności np.: w przypadku powstania usterki systemu związanej z brakiem zasilania lub awarii poszczególnych podsystemów wzywa serwis techniczny.

Odebranie sygnału alarmu technicznego wiąże się każdorazowo z przejściem procedury obsługi zdarzenia przez operatora.



Rysunek 13.5. Reakcja na sygnały (scenariusz reakcji na zdarzenia techniczne, alarmowe etc.)

13.5. Rejestracja zdarzeń, odczyt, obsługa

System alarmowy umożliwia automatyczną rejestrację wszystkich zdarzeń alarmowych oraz technicznych, jakie w nim wystąpiły. W związku z integracją na poziomie aplikacji softwarowej SMS odbywa się on w dwojaki sposób. Pierwszym podstawowym rodzajem jest zapis w buforze nieulotnej pamięci systemu alarmowego oraz drugi na dyskach pamięci serwera aplikacji integrującej. Zarówno jedna jak i druga pamięć jest dostępna dla operatora monitoringu i umożliwia odtworzenie historii, jaka miała miejsce w systemie SSWiN. Obsługa i odczyt wykonywane są zgodnie z instrukcją obsługi systemu będącą na wyposażeniu stanowiska monitoringu – stacji SMS.

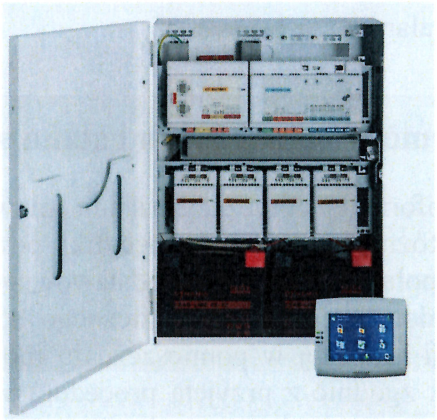
W przypadku awarii stacji SMS - możliwy jest także odczyt zdarzeń bezpośrednio z centrali lub za pomocą klawiatury LCD w pomieszczeniu monitoringu.

13.6. Elementy składowe SSWiN

Przedstawione poniżej parametry i nazwy sprzętu należy traktować przykładowo jako jedną z wielu możliwości doboru elementów i konfiguracji parametrów urządzeń.

1165

Centrala alarmowa



Rysunek 11.5a. Przykładowa centrala SSWiN

Centralnym punktem systemu jest modułowa centrala alarmowa z wbudowanym interfejsem TCP/IP, który umożliwia zarządzanie systemem ze Stanowiska Operatorskiego. Poszczególne elementy systemu są podłączone do panelu głównego poprzez dwa rodzaje magistral danych DB (Data Bus). Pierwsza magistrala danych (wewnętrzna) może mieć długość do sześciu metrów od centrali. Kontroluje ona wymianę danych pomiędzy panelem głównym i modułami komunikacyjnymi. Druga magistrala (całkowicie autonomiczna, zewnętrzna) może mieć długość do jednego kilometra. Biegnie ona, w zależności od konfiguracji, do różnych części budynku i prowadzi do paneli sterowania i zasilaczy, a docelowo do modułów pętli adresowalnych. Długa magistrala danych umożliwia instalację podłączonych urządzeń bezpośrednio w miejscu stosowania.

W centrali zastosowano w pełni adresowalną technologię wykorzystującą lokalną sieć bezpieczeństwa. System został zaprojektowany do obsługi maksymalnie do 1500 adresów, 500 obszarów i 1000 użytkowników. Jeden adres odpowiada pojedynczemu wejściu lub pojedynczemu wyjściu. Urządzenia adresowalne (np. czujki ruchu, czujki magnetyczne czy przyciski antynapadowe) są umieszczane na pętlach dozorowych, którymi sterują moduły zapewniające także zasilanie (maksymalny prąd wyjściowy 300 mA). Z jednym modułem współpracuje do 127 urządzeń. Dzięki utworzeniu pętli w sieci zostaje zapewniona pełna funkcjonalność wszystkich podłączonych urządzeń, także w przypadku zwarcia lub przerwania pojedynczego przewodu. System powinien zarządzać co najmniej ośmioma modułami adresowymi.

W obudowie centralnej znajdują się cztery takie moduły. Dodatkowe obudowy (rozszerzające) zawierają kolejne cztery, które są bezpośrednio podłączone do magistrali danych. W obudowie centralnej mieści się także zasilacz oraz źródło zasilania rezerwowego w postaci dwóch akumulatorów 40 Ah. Opcjonalna obudowa rozszerzająca ma własny zasilacz i dwa kolejne akumulatory, każdy z nich po 18 Ah. Dostępna jest również dodatkowa obudowa źródła zasilania, która mieści zasilacz o mocy 150 W i do czterech akumulatorów awaryjnych, każdy z nich po 40 Ah.

Oprócz zasilaczy i modułów pętlowych do panelu głównego może być dołączony także moduł interfejsu komunikacyjnego. Interfejs ten steruje modułem transmisyjnym i drukarką zdarzeń. Ponadto są w nim trzy konfigurowalne wyjścia do sygnalizatorów akustycznych i optycznych oraz innych lokalnych urządzeń sygnalizacyjnych. Projektowana centrala SSWiN jest zgodna z wymogami normy PN-EN 50131-1:2009 Systemy alarmowe -- Systemy sygnalizacji włamania i napadu -- Wymagania systemowe. minimum dla dla systemu stopnia 2.

Parametry elektryczne centrali:

- Napięcie sieciowe: 100 VAC (-10%) - 230 VAC (+10%)
- Częstotliwość napięcia sieciowego: 47 - 63 Hz

- Pobór mocy: 150 W na zasilacz (maks. 32 zasilacze sieciowe)
- Zakres napięcia stałego na magistrali: 9 - 30 VDC; znamionowo 28 VDC
- Pojemność akumulatorów: maks. 80 Ah na zasilacz (maks. 32 zasilacze sieciowe)
- Napięcie ładowania akumulatorów: 28 VDC
- Czas podtrzymania zasilania: określany przez pojemność akumulatorów i obciążenie systemu

Parametry mechaniczne centrali
- Obudowa centrali metalowa ze stykiem sabotażowym
- Obudowa rozszerzeń metalowa ze stykiem sabotażowym

Parametry systemowe centrali:
- Liczba adresów: minimum 1000
- Liczba obszarów: minimum 100

Liczba urządzeń
- Moduły pętlowe maks. 8; każdy z 1 pętlą lub 2 odgałęzieniami
- Panel sterowania: minimum 16
- Zasilacze 150W: minimum 16
- Drukarka: minimum 1

Liczba wejść
- Wejścia: minimum. 8 wejść na płycie i 1 wejście tampera;

Liczba użytkowników
- Kody PIN: minimum 100
  kody PIN mogą zawierać minimum 8 cyfr ,

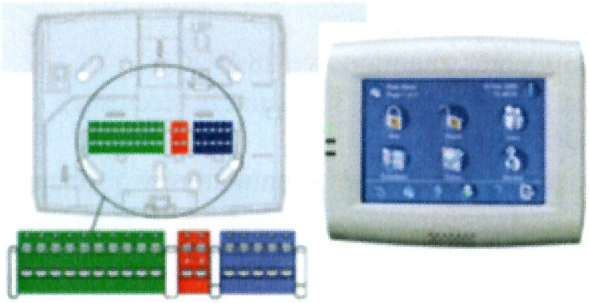
Liczba wyjść
- Programowalne wyjścia na magistrali pętlowej:ograniczone do maksymalnej liczby adresów w systemie

Centrala główna:
- 2 wyjścia sterowania zasilaniem;
- 2 styki beznapięciowe;
- 1 wyjście zasilania zewnętrznego
- Moduł łącznie 5: 3 wyjścia nadzorowane i 2 typu otwarty kolektor

Parametry środowiskowe
- Temperatura pracy: -10 ÷ +55°C
- Temperatura przechowywania: -20 ÷ +60°C
- Wilgotność względna: 5 - 95% (bez kondensacji) przy temperaturze pracy i przechowywania

Sterowanie manipulatorem LCD

11 67



Parametry użytkowe:

- Ekran dotykowy - 14 cm (5,7") LCD z regulowanym podświetleniem LED
- Interfejs graficzny (16-bitowa paleta barw przy rozdzielczości 320 x 240 pikseli) składający się z intuicyjnych ikon i menu
- Wersje językowe do wyboru przez użytkownika
- Wbudowany głośnik z regulowaną głośnością
- Brak odsłoniętych części przy dostępie do zacisków; okablowanie w podstawie dołączane do zacisków wciskanych

Panel sterowania posiada głośnik generujący następujące sygnały:

- Sygnał naciśnięcia właściwego przycisku: potwierdzenie dokonania wyboru poprzez naciśnięcie obrazu na ekranie dotykowym.
- Sygnał niewłaściwego wyboru: wskazanie naciśnięcia nieaktywnego przycisku lub pola bez obrazu przycisku.
- Sygnał opóźnienia wejścia: powiadomienie o rozbrojeniu systemu w zaprogramowanym czasie.
- Sygnał opóźnienia wyjścia: powiadomienie o przygotowaniu do uzbrojenia systemu w zaprogramowanym czasie.
- Sygnał alarmu włamaniowego: wskazanie warunku alarmowego.
- Sygnał nadzoru włamaniowego: wskazanie warunku nieprawidłowości (problemu) nadzorowanego punktu.
- Sygnał problemu włamaniowego: wskazanie warunku nieprawidłowości (problemu) punktu.
- Gong: wskazanie uaktywnienia punktu.
- Sygnał problemu systemowego: wskazanie warunku problemu systemowego w rodzaju awarii sieci energetycznej.

Elementy regulacyjne obrazu i dźwięku

- Panel sterowania posiada wbudowaną regulację głośności i jaskrawości. Ponieważ każdy panel sterowania jest regulowany indywidualnie, zmiana głośności czy jaskrawości w jednym z nich nie ma wpływu na inne panele w tym samym systemie.

Różne Języki

- Dla każdego nowo utworzonego użytkownika wybiera się preferowany język (angielski, niemiecki, francuski i holenderski). Po zalogowaniu użytkownika w panelu sterowania ustawiany jest preferowany język.

Wejście tampera

- Obudowa panelu sterowania posiada wbudowany tamper wykrywający oderwanie od ściany lub zdjęcie pokrywy.

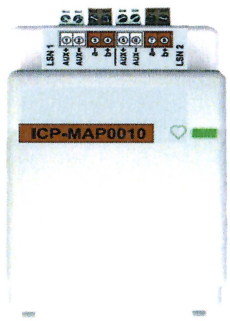
Parametry mechaniczne

- Wymiary:146x171,5x44,5 mm
- Masa: 600 g
- Właściwości ekranu dotykowego: panel TFT-LCD o przekątnej 14 cm (5,7"); 320 x 240 pikseli z 16-bitową paletą barw; białe diody LED podświetlenia z regulowaną jaskrawością (podświetlenie aktywne i spoczynkowe); proporcja boków = 4:3
- Materiał obudowy: biały plastik fakturowany
- Wskaźniki:trzy diody LED
  - zielona: zasilanie
  - żółta: usterka
  - czerwona: alarm
- Połączenia: 4-żyłowa magistrala BDB (dane i zasilanie); 2 zestawy zacisków do okablowania łańcuchowego wejść / wyjść; zacisk śrubowy lub przełącznik do okablowania odgałęzienia

Komunikacja pętlowa

Wewnętrzna magistrala sieciowa pracuje w oparciu o protokół CAN (ang. Controller Area Network), łącząc centralę alarmową z takimi elementami systemu jak bramy pętlowe, zasilacze, interfejsy użytkownika w postaci ekranów dotykowych oraz moduły komunikacji z portami szeregowymi i równoległymi. Ponadto technologia Can-Bus zapewnia komunikację do 1000 metrów, co pozwala na obsługę rozległych obiektów. Zewnętrzna magistrala sieciowa IP zapewnia połączenie z systemami zainstalowanymi w innych budynkach. Dzięki otwartym interfejsom istnieje możliwość integracji centrali alarmowej z innymi systemami bezpieczeństwa i automatyki budynkowej. W przypadku współpracy ze zintegrowanym systemem automatyki budynkowej systemem można sterować bezpośrednio za pomocą stacji roboczej. Obsługa oświetlenia, trasy strażników, kontrola dostępu czy obsługa systemów sygnalizacji włamania - wszystkimi tymi zadaniami można kierować z jednej lokalizacji.

Moduł bramy pętlowej



Każda z bram jest połączona z jedną pętlą lub dwoma liniami otwartymi o maksymalnym obciążeniu wyjściowym 300 mA. Każda brama obsługuje maksymalnie 127 urządzeń adresowalnych. Konfiguracja z obwodem pętli toleruje pojedynczy stan zwarcia lub otwarcia przy zapewnieniu pełnej funkcjonalności w pętli. Brama obsługuje dwa pojedyncze wyjścia nadzorowane z zabezpieczeniem przeciwprzepięciowym.

Parametry :

- Obsługuje maksymalnie 127 urządzeń, maksymalne obciążenie pętli 300 mA
- Umożliwia utworzenie elastycznych struktur sieci (jedna pętla lub dwie linie otwarte)

- Zapewnia nadmiarowość po jednej awarii w konfiguracjach z pętlą (nie w konfiguracjach z liniami otwartymi)
- Wyposażony w dwa pomocnicze wyjścia zasilania (500 mA każde)

Dane techniczne
Parametry elektryczne

- Minimalne napięcie robocze (V DC) 16
- Maksymalne napięcie robocze (V DC) 29
- Napięcie znamionowe (V DC) 28
- Natężenie znamionowe (mA)1600

Pobór prądu w trybie gotowości

- Maksymalne natężenie prądu wyjściowego AUX (mA) 2 x 500
- 3 Moduł bramy

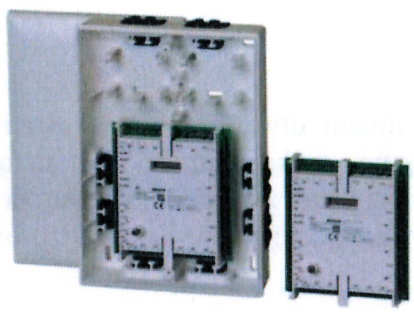
Parametry mechaniczne

- Wymiary (cm) (wys. x szer. x głęb.) 15.88 x 8.26 x 6.35
- Masa (g) 365
- Materiał obudowy
- Tworzywo ABS
- Kolor biały
- Wskaźnik Zielona dioda LED zasilania

Parametry środowiskowe

- Minimalna temperatura robocza (°C) -10
- Maksymalna temperatura robocza (°C) 55
- Minimalna temperatura magazynowania (°C) -20
- Maksymalna temperatura magazynowania (°C) 60
- Minimalna wilgotność względna (%) 5 (bez kondensacji)
- Maksymalna wilgotność względna (%) 95 (bez kondensacji)
- Klasa ochronna IP30, IP31
- Poziom zabezpieczeń IK04, IK06
- Klasa środowiskowa II: EN50130-5, VdS 2110
- Wykorzystanie wewnętrzne

Moduł wejść/ wyjść



Do dołączenia elementów konwencjonalnych wykorzystuje się moduł urządzeń konwencjonalnych. Obsługuje on 6 wejść w konfiguracji NC, EOL i DEOL, a także 4 wyjścia. Moduł

instaluje się na pętli podobnie jak urządzenia detekcyjne wykonane w pętli. Element monitoruje linię główną pod kątem występowania alarmu, zwarcia i przerwy. Posiada Rozbudowane systemowe wartości graniczne w „ulepszonej wersji" trybu i oraz styk antysabotażowy (alarm antysabotażowy).

Parametry elektryczne:
Część pętlowa:

- Minimalne napięcie robocze (VDC) 15
- Maksymalne napięcie robocze (VDC) 33
- Maksymalny pobór prądu (mA) 4.95

Inne funkcje modułu rozszerzenia :

- Minimalne napięcie robocze (VDC) 9
- Maksymalne napięcie robocze (VDC) 30
- Maksymalny pobór prądu (mA) przy 12V 370
- Maksymalny pobór prądu (mA) przy 28V 180

Urządzenia zewnętrzne

- Minimalne napięcie wyjściowe (VDC) 11.9
- Maksymalne napięcie wyjściowe (VDC) 16.3

Urządzenia detekcyjne (czujki, przyciski):
Podczas projektowania systemu sygnalizacji włamania i napadu przyjęto następujące założenia:

- w oparciu o analizę zagrożeń dla obiektu system powinien być wykonany w oparciu o urządzenia, co najmniej stopnia 2 (wg PN-EN50131)
- w celu zwiększenia niezawodności działania, magistrala czujek musi mieć możliwość zamknięcia w pętle
- ochrona oparta o adresowalne czujki ruchu z antymaskingiem,czujki wstrząsowe oraz adresowalne i klasyczne czujki magnetyczne

Do ochrony wnętrza pomieszczeń należy zastosować pasywne czujki podczerwieni oraz czujki dualne. Zaleca się zastosowanie czujek wyposażonych w funkcję antymaskingu dla zapewnienia wyższego poziomu ochrony.

Minimalne parametry czujek:

- Zasięg minimum 18 x 25 m i możliwość wyboru krótkiego zasięgu co najmniej 8 x 10 m
- Technologia przetwarzania sygnałów z kilku detektorów
- Aktywna redukcja białego światła
- Dynamiczna kompensacja temperaturowa
- Wysokość montażu od 2 do 3 m; bez konieczności regulacji
- Zgodność z normą EN50131-2-4, stopień 2
- Zdalny autotest
- Zakres napięć zasilania: od 9 do 28VDC
- Praca w technologii dwuprzewodowej (współpraca z centralą opartą na technologii CAN poprzez szeregowe złącze komunikacyjne magistrali adresowej)
- Trójogniskowy układ optyczny zapewniający trzy długości ogniskowania: soczewka dalekiego, średniego i krótkiego zasięgu
- Dwa detektory piroelektryczne zapewniające wzmocnienie optyczne

Czujka typu TriTech+ z antymaskingiem

Czujki TriTech+ z funkcją antymaskingu MANTIS posiadają te same właściwości detekcyjne zarówno w wersji adresowalnej jak i konwencjonalnej. Inny jest jedynie sposób podłączenia i późniejszej konfiguracji – w ujęciu adresowalnym czujka przesyła wszystkie rodzaje alarmów, jest konfigurowana, a także zasilana poprzez połączenie 2-żyłowe bez konieczności fizycznej zmiany przełączników na urządzeniu.

Główne funkcje:

Technologia przetwarzania sygnałów z kilku detektorów (Sensor Data Fusion):

Czujka dualna powinna korzystać z algorytmu przetwarzania danych z kilku źródeł w celu zapewnienia jak najwyższej skuteczności wykrywania bez narażania inwestora na ryzyko wystąpienia fałszywego alarmu. Wbudowany mikrokontroler powinien dokonywać analizy sygnałów ze źródeł co najmniej dwóch detektorów piroelektrycznych, detektora mikrofalowego o regulowanym zasięgu, detektora temperatury i detektora poziomu białego światła, a także dedykowanego obwodu antymaskingu.

Optyka:

Układ optyczny czujki powinien wykorzystywać trzy soczewki, które zapewnią trzy różne długości ogniskowej dla dalekiego, średniego i bliskiego zasięgu wykrywania. Wspomniane długości powinny dzielić obszar na 86 stref wykrywania w celu uzyskania do 11 kurtyn detekcji. Czujka wyposażona w dwa detektory piroelektryczne powinna dodatkowo zapewnić podwójne wzmocnienie sygnału w odniesieniu od podstawowych rozwiązań stosowanych na rynku.

Antymasking (MANTIS):

Czujka powinna zapewniać funkcję wielopunktowego wykrywania maskowania. Funkcja ma chronić przed celowym lub nieumyślnym ograniczaniem zasięgu lub właściwości detekcyjnych urządzenia i wysyłać alarm nawet w przypadku, gdy strefa detekcyjna nie jest uzbrojona. Ważne jest, aby zastosowany algorytm spełniał międzynarodowe normy dotyczące wykrywania obiektów maskujących z uwzględnieniem wielu materiałów, takich jak tkaniny, papier, metal, plastik, taśmę i spray. Do detekcji wspomnianych elementów czujka powinna używać do trzech niezależnych technologii dedykowanych do danego rodzaju sposobu maskowania.

Redukcja światła białego:

Czujka powinna posiadać wbudowany detektor światła białego do pomiaru wiązki padającej nań bezpośrednio, a mogącej wywołać fałszywy alarm lub ograniczyć zdolności detekcyjne. Pomiar wiązki światła padającego powinien być wykorzystywany przez algorytm przetwarzania sygnałów z kilku detektorów, w celu dostosowania odpowiednio czułości dla wszystkich komponentów urządzenia.

Kompensacja temperatury otoczenia:

Czujka powinna posiadać funkcję pomiaru temperatury otoczenia w celu dostosowania czułości pozostałych podzespołów. Kompensacja temperatury powinna umożliwiać stałe odróżnianie potencjalnych intruzów w jak najszerszym zakresie temperatur, co jest szczególnie ważne dla zakresu temperatur zbliżonych do temperatury ludzkiego ciała.

Regulacja zasięgu:

Standardowy zasięg czujki powinien wynosić przynajmniej 18 x 25 m przy czym producent powinien dodatkowo zapewnić opcję wyboru zasięgu krótkiego, np. 8 x 10 m, który mógłby być wykorzystywany w aplikacjach o ograniczonej przestrzeni ze względu na różne czynniki organizacyjne. (*W przypadku czujki konwencjonalnej to mikroprzełącznik, a w czujkach*

adresowalnych zmianę zasięgu edytuje się zdalnie, za pomocą oprogramowania do konfiguracji centrali bez konieczności zdejmowania pokrywy czujki).

Ochrona antysabotażowa:
Czujka powinna oferować możliwość monitorowania zdjęcia obudowy lub oderwania od ściany w celu detekcji zachowania sabotażowego.

Dioda LED:
Czujka powinna być wyposażona w diodę LED, która służy do wykonania poprawnego obchodu testowego. W aplikacjach pracy normalnej dioda LED nie powinna zdradzać swoim zachowaniem zasięgu wykrywania, aby nie dostarczać tego typu informacji dla potencjalnych intruzów znajdujących się w obiekcie podczas gdy system nie jest uzbrojony. Jasność diody LED powinna dostosowywać się do otoczenia automatycznie analizując wcześniej poziom światła w otoczeniu.

Pamięć alarmów i usterek:
Czujka powinna zapewniać pamięć alarmów. Pamięć alarmów powinna być sterowana zewnętrznie, np. poprzez sterowanie napięciem z centrali alarmowej.

Auto test:
Czujka powinna oferować funkcję zdalnego auto testu, którą można wywołać z zewnątrz. W razie niepowodzenia testu czujka powinna uaktywnić przekaźnik odpowiedzialny za usterkę.

Odporność:
Czujka swoją budową powinna zapewniać odporność na czynniki środowiskowe minimalizując jednocześnie ryzyko spowodowania fałszywego alarmu. Czujka powinna oferować hermetycznie zamkniętą obudowę, podczas instalacji której ryzyko uszkodzenia lub zabrudzenia któregokolwiek z elementów optycznych lub detekcyjnych będzie uniemożliwione. Zwarta budowa powinna zabezpieczać czujkę przed cyrkulacjami powietrza, pyłem i owadami, a specjalnie dostosowana czułość powinna zabezpieczać czujkę przed fałszywymi alarmami wywołanymi przez zwierzęta do 4,5 kg, np. gryzonie.

Programowanie:
Czujka powinna zapewniać czytelny dostęp do mikroprzełączników służących do programowania funkcji czujki. W przypadku wersji adresowalnej czujkę konfiguruje się zdalnie z poziomu aplikacji inżynierskiej lub z poziomu centrali alarmowej.

OPIS:
Czujka powinna zapewniać trzy aktywne technologie detekcji zamaskowania. W tym celu urządzenie powinno używać czterech aktywnych emiterów podczerwieni i trzech fotodiod. Zastosowanie powyższych podzespołów powinno służyć detekcji czynników maskujących, a zatem ograniczać ryzyko umyślnego i nieumyślnego upośledzania zdolności detekcyjnych urządzenia.

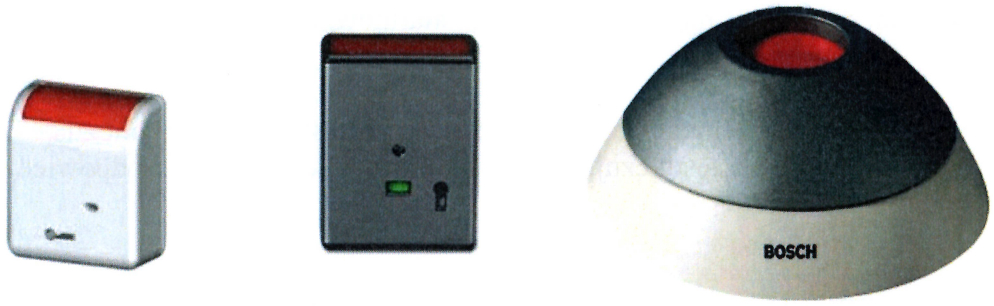
Opis poszczególnych technologii:
Pierwsza z aktywnych technologii (Bounce back technology) używanych do wykrywania maskowania powinna zapewniać ochronę przed przedmiotami ograniczającymi zasięg urządzenia bezstykowo, jak na przykład pudełko do butów lub po prostu elementy zwisające z sufitu. W tym celu czujka powinna emitować promieniowanie IR tworzące wokół niej sferę o promieniu 30 cm mierzonego od środka urządzenia. W momencie normalnej pracy i braku zakłóceń w wartości

emitowanej wiązki przekaźnik antymaskingu jest niewykorzystywany. Alarm zostaje wyzwalany po pojawieniu się w zasięgu sfery materiału obiektu maskującego.

Druga z technologii (Retro reflector) dotyczy wykrywania próby zamalowania czujnika np. farbą w sprayu lub lakierem. Dioda czujki znajdująca się w przedniej części nie jest tylko wskaźnikiem, a jednocześnie jest strukturą złożoną z wielu pryzmatów, które służą do odbijania energii IR generowanej z wnętrza czujki. W przypadku, gdy czujka zostaje pomalowana na granicach ośrodków dochodzi do załamania fali a co za tym idzie zmienia się współczynnik odbicia uaktywniając alarm.

Trzecia technologia (Through the lens) polega na detekcji próby maskowania strefy podejścia czujki. Dwa pryzmaty umieszczone przy strefie dolnej rozpraszają promieniowanie IR, a znajdująca się dedykowana fotodioda sprawdza w sposób ciągły poziom promieniowania.

13.7.System sygnalizacji napadu stacjonarny.



Rysunek 13.6. Przykładowe elementy systemu antynapadowego / pomocy

Rozmieszczenie poszczególnych urządzeń wskazano na rysunkach technicznych w części graficznej u uwzględniając podstawowe założenia dotyczące wyposażenia w system przestrzeń biurową (sekretariat, dyrektor placówki) oraz wystawową tzn. zlokalizowane w miejscach dostępnych dla personelu oraz pracowników ochrony (miejsca dobrane pod kątem wyposażenia wystawienniczego na bazie projektu konserwatorskiego.)

W projekcie zastosowano stacjonarne, adresowane przyciski antynapadowe dedykowane do systemu w stopniu 3 według normy PN-EN 50131-3:2010 Systemy alarmowe -- Systemy sygnalizacji włamania i napadu -- Część 3: Urządzenia sterujące i obrazujące.

Każdorazowe użycie (wciśnięcie przyciski) powoduję opisaną w dziale integracji systemów reakcje na zdarzenie. Przycisk generuje alarm w formie czasowej bez konieczności resetu elementu.

Charakterystyka przycisku

- Przycisk antynapadowy w technologii pętlowej
- Do podłączenia do antywłamaniowego panelu sterowania
- Przekazywanie sygnału alarmu i sabotażu za pomocą magistrali pętlowej
- Styk antysabotażowy Kabel do montażu natynkowego lub podtynkowego
- Nakładka z pokrywą, jako zabezpieczenie przycisku (opcjonalna)

Specyfikacja techniczna

- Napięcie robocze (część pętlowa) Od +12 V do 30 V
- Zużycie prądu (napięcie liniowe) Ok. 0,5 mA

- Temperatura otoczenia Od - 0°C do +50°C
- Warunki otoczenia DIN 40040 R14
- Klasa ochrony IP 40
- Obudowa
- Materiał ABS
- Kolor RAL 9002 (obudowa)
- Szary (osłona)
- Masa ok. 70 g
- Wymiary (gł. x wys.) 8 1 x 3 1 m
- Klasa środowiskowa 2

Przypisanie przycisku do danej strefy użycia zostanie rozwiązane w sposób organizacyjny i opisany w SSWiN i SMS w uzgodnieniu z Zamawiającym.

13.8. Bezprzewodowy system antynapadowy SN

W ramach budowy systemu sygnalizacji napadu wskazuje się na zastosowanie systemu bezprzewodowego pracującego, jako system wspomagający. Konfiguracja uwzględnia wykorzystanie urządzeń przekaźnikowych wielokanałowych, pracujących w ramach odseparowanej galwanicznie struktury (np. poprzez moduły wejść). Użycie przycisku generuje zdarzenia typu NAPAD w systemie SWiN oraz przekazuje zgodnie z koncepcją alarm na stanowisko SMS.

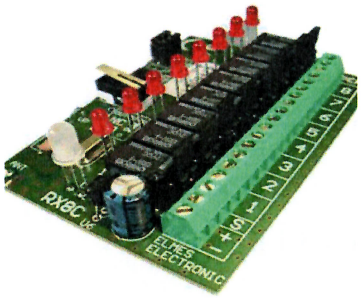
Konfiguracja systemu musi zapewniać identyfikację użycia każdego pilota poprzez zadziałanie dedykowanego przekaźnika. Każdorazowe użycie danego pilota musi aktywować dedykowaną linię/ wejście modułu EMIL. Konsekwencją rozwiązania będzie identyfikacja sygnału napadu z rozróżnieniem aktywacji poszczególnych pilotów. W tym zakresie projekt dopuszcza zastosowanie i budowę osobnego systemu antynapadowego opartego o urządzenia bezprzewodowe z rozróżnieniem poszczególnych przycisków oraz integracją z systemem SMS. Np. Zastosowanie centrali alarmowej z modułem TCP/IP (podłączona do integratora SMS, jako osobny podsystem) z podłączonymi odbiornikami przycisków bezprzewodowych. Należy zaznaczyć, że w takim wypadku wykonawca musi zapewnić podobne parametry zasilania awaryjnego zgodne z bilansem prądowym pozostałej części systemu antynapadowego opartego o przyciski stacjonarne (bilans systemu SSWiN) oraz pełne pokrycie zasięgiem pilotów w całej przestrzeni obiektu (pokrycie zasięgiem całego obiektu musi być zapewnione dla każdego z rozwiązań systemu antynapadowego).

Budowa systemu antynapadowego bezprzewodowego ma umożliwiać przekazanie sygnału użycia przycisku bezprzewodowego w całym budynku i w promieniu 10 m od zewnętrznych ścian budynku. Pozostałe elementy bezprzewodowe należy dobrać pod kątem wyposażenia pracowników patrolowych ochrony fizycznej oraz wyznaczonych pracowników obsługi przestrzeni wystawy (ilość pilotów określona na bazie uzgodnień roboczych).

Rysunek 13.7. Przykładowe elementy systemu antynapadowego / pomocy

1175

13.8.1. Parametry systemu



Rysunek 11.8 Odbiornik 8 kanałowy. Odbiornik superheterodynowy CH8HR

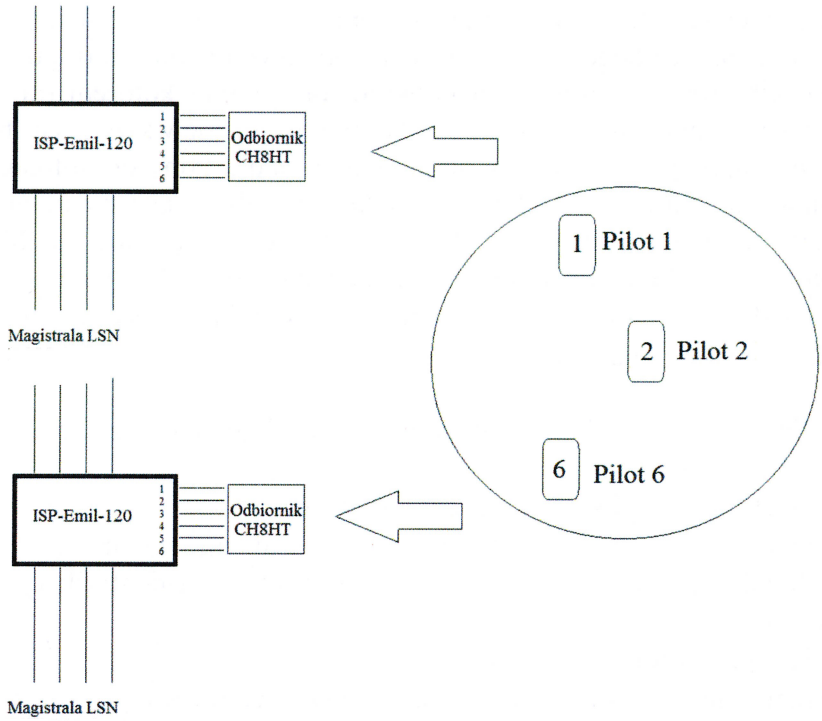
Odbiornik przeznaczony jest do bezprzewodowych systemów alarmowych i zdalnego sterowania, w których używa się wielu nadajników z dynamicznym kodem zmiennym i wymagana jest ich identyfikacja. Posiada 8 wyjść przekaźnikowych typu NO (normalnie rozwarte) lub NC (normalnie zwarte) separowanych galwanicznie oraz 8 diod LED do optycznej sygnalizacji załączenia wyjść przekaźnikowych. Sygnalizuje rozładowanie baterii w nadajnikach i otwarcie obudowy (antysabotażowa funkcja TAMPER) oraz brak łączności z detektorami (PTX, GBX, CTX4H). Współpracuje ze wszystkimi nadajnikami i pilotami Elmes. Do każdego kanału odbiornika można przypisać dowolną ilość nadajników, ale łączna ich ilość w systemie nie może przekroczyć 40. Piloty wielokanałowe oraz nadajnik RP501 przełączają zawsze kolejne, sąsiadujące ze sobą kanały. Detektory PTX50, GBX, CTX pracują w dwóch kanałach: detekcja w dowolnym kanale od 1 do 8, a antysabotaż w kanale 8 przydzielanym automatycznie.

Podstawowe parametry:

- częstotliwość pracy 433,92MHz, odbiornik superheterodynowy,
- współpraca ze wszystkimi nadajnikami ELMES 433,92MHz,
- maksymalna ilość nadajników 40,
- 8 wyjść przekaźnikowych NO/NC, praca włącz/wyłącz lub czasowa,
- sygnalizacja załączenia kanałów na diodach LED,
- sygnalizacja słabej baterii nadajników.

Przykładowe parametry pilota antynapadowego

- częstotliwość pracy 433,92MHz;
- moc < 10mW;
- bateria 9V;
- wymiary (dł/szer/wys) 113/33/21mm.



Rysunek 11.9 przykładowy schemat podłaczenia systemu antynapadowego

Zastosowanie podwójnej ochrony antynapadowej pozwoli zaspokoić wymagania stawiane obiektowi jednocześnie zapewniając właściwy stopień zabezpieczenia (system SSWiN).

13.8.2. Charakterystyka

Podsystem zorganizowany, jako autonomiczna struktura odseparowana galwanicznie od istniejącego systemu SSWiN zgodnie z dostępnymi rozwiązaniami rynkowymi. W ramach organizacji sprzętowej należy wykonać infrastrukturę opartą o urządzenia dublujące system stałych przycisków. Każdy z zastosowanych odbiorników /pilotów alarmowych musi przesyłać w trybie on-line do centrali alarmowej następujące komunikaty:

- stan spoczynku
- stan naruszenia
- stan alarmowy
- stan sabotażu
- stan bliskiego wyczerpania baterii zasilającej

13.8.3. Funkcjonalność

Funkcjonalność systemu antynapadowego opiera się w głównej mierze na doposażeniu stacjonarnego systemu antynapadowego pracującego na bazie systemu SSWiN. Element bezprzewodowy jest systemem uzupełniającym i rozszerzającym możliwości systemu poprzez wywołanie alarmu napadu z przenośnego przycisku radiowego dla:

- Pracowników WSO – patrol
- Pracowników WSO - dedykowany posterunek
- Pracownik etatowy – opiekun pomieszczenia, przewodnik etc.

W zakresie dopuszczonych rozwiązań projekt wskazuje na zastosowanie radiolinii o dużym zasięgu (z powodu znacznej grubości ścian i konstrukcji budynku) z potwierdzeniem odebrania sygnału.

Oczekiwana funkcjonalność radiolinii:

Przyciśnięcie przycisku pilota spowoduje zapalenie diody informacyjnej (zadziałania urządzenia przenośnego) i wysłania cichego powiadomienia pracownika monitoringu. Otrzymanie sygnału (odebranie przez odbiornik radiolinii) jest potwierdzone innym kolorem (np. zielony) na pilocie. Opcja znacząco podnosi pewność wezwania pomocy przez osobę wzywającą służbę WSO.

System ochrony antynapadowej (mobilnej) zostanie podłączony do aplikacji integrującej SMS. Wszystkie komunikaty alarmowe, techniczne będą zwizualizowane na mapie klienta PC w celu szybkiej oceny sytuacji przez pracownika WSO . Konfiguracja systemu możliwi operatorowi stacji klienckiej podstawową obsługę systemu pod kątem codziennej funkcjonalności polegającej na :

- Kasowaniu alarmów napadowych bez możliwości rozbrajania wybranej strefy lub grup stref;
- Przeglądaniu historii zdarzeń;

Wywołanie zdarzenia typu alarm napadowy* powoduje rozpoczęcie algorytmu działania w następujących zależnościach:

- Alarm dźwiękowy w aplikacji SMS oraz SSWiN;
- Alarm wizualny w aplikacji SMS ze wskazaniem na mapie powstania alarmu z dokładnościądo przycisku, który go wygenerował (identyfikacja zadziałania pilota bezprzewodowego);
- Określenie typu alarmu tzn.: napad;
- Wyświetlenie na aplikacji SMS scenariusza alarmowego ze wskazaniem sposobu postępowania i listy osób do powiadomienia np.: administrator budynku, dyrekcja, służby techniczne, ochrona zewnętrzna etc.

* Uwaga: wyjątek stanowi wywołanie alarmu napadowego w pomieszczeniu monitoringu . Dla tego przypadku sygnał powinien zostać wysłany do zewnętrznych służb ochronnych np. zmotoryzowanego patrolu/zespołu interwencyjnego. Do ustalenia na etapie wykonawczym.

13.9.Charakterystyka SSWiN

Wykonany system musi uwzględniać zabezpieczenia okien na poziomie piwnicy, parteru oraz w Sali Wilanowskiej planuje się wykonać w całości w II etapie inwestycji. Na pozostałych kondygnacjach w drugim etapie inwestycji należy doprowadzić do okien drożne trasy kablowe, z wprowadzonym przewodem, od głównych tras kablowych, od strony okien zakończone puszką podtynkową z sygnalizacją otwarcia. Zapas przewodu umożliwiający późniejsze podłączenie czujników pozostawić po stronie głównych tras kablowych.

System alarmowy zorganizowany jest, jako struktura pętlowa – magistralowa z pełną adresacją elementów detekcyjnych – czujek alarmowych i przycisków do sygnalizacji napadu.

Każdy z zastosowanych elementów detekcyjnych przesyła do centrali alarmowej komunikaty zgodnie z 2 stopniem zabezpieczenia oraz dodatkowo stan zasłonięcia czujki ruchu (zamaskowania) oraz zapewnia regulację podstawowych parametrów pracy bezpośrednio z aplikacji zarządzającej centralą alarmową. Funkcja ta jest stosowana dla obsługi urządzeń zlokalizowanych w trudno dostępnych miejscach, uniemożliwiających regulacje urządzeń bez ingerencji (przesuwanie, zdejmowanie etc.) w eksponaty wystawowe lub inne wyposażenie muzealne tj. demontaż gablot, osłon, zabezpieczeń mechanicznych.

Dla czujki otwarcia stykowej (zewnętrznej) chroniącej strefę (właz studzienki kablowej) rewizji teletechnicznej zastosowano separację galwaniczną od SSWiN.

13.10. Funkcjonalność SSWiN

System sygnalizacji włamania i napadu zostanie podłączony do aplikacji integrującej SMS. Wszystkie komunikaty alarmowe i techniczne generowane przez SSWiN będą zwizualizowane na mapie synoptycznej stacji roboczej stanowiska operatorskiego (klienta PC). Konfiguracja systemu umożliwi zarówno użytkownikowi (klawiatury LCD) jak i operatorowi SMS pełną obsługę systemu pod kątem codziennej funkcjonalności polegającej na :

- Uzbrajaniu / rozbrajaniu poszczególnych stref alarmowych z uwzględnieniem uprawnień poszczególnych kodów;
- Kasowaniu alarmów bez możliwości rozbrajania wybranej strefy lub grup stref;
- Blokowaniu / odblokowaniu poszczególnych stref alarmowych, detektorów z uwzględnieniem hierarchizacji uprawnień;
- Aktywacji zaprogramowanych funkcji korelacji międzysystemowych np. aktywacja i dezaktywacja automatyki otwarcia drzwi wejściowych dla gości z pozycji centrali oraz aplikacji SMS;
- Przeglądaniu historii zdarzeń.

SSWiN musi zapewnić hierarchiczność kodów dostępu i skalowalność stref alarmowych. Wymaga się, aby system umożliwiał utworzenie minimum 50 stref alarmowych.

W podstawowym zakresie proponuje się skonfigurowanie 30 stref dostępu tzn.:

- Strefa korytarzowa 1 poziom piwnicy – korytarze komunikacyjne, toalety etc.;
- Strefa korytarzowa 2, 3 poziom od 0 do +1 – korytarze komunikacyjne, toalety etc.;
- Strefa korytarzowa 4 poziom od 2 – korytarze komunikacyjne, toalety etc.;
- Strefa zewnętrzna 5 poziom +1 – balkony zewnętrzne ;
- Strefa wystawiennicza 5 do 15 – poziomy 0 do +2;
- Strefa gastronomiczna 16,17 – część zaplecza poziom parteru oraz poziom piętra +1;
- Strefy magazynowa 18-25 dla poszczególnych pomieszczeń magazynowych;
- Strefy biurowe 25,26,27 dla poszczególnych poziomów;
- Strefa dyrekcji 28,29 – sekretariat, dyrektor;
- Strefa magazynu WSO 30- magazyn broni;
- Strefa serwerowa 31 – serwerownia.

Zastosowany SMS oraz jego konfiguracja mają zapewnić monitorowanie wszystkich sygnałów generowanych przez SSWiN. Integracja SSWiN z SMS musi uwzględniać programowe połączenie funkcjonalne pozostałych systemów i ich reakcję na otrzymany z systemu sygnał.

Dla przykładu:

Wywołanie zdarzenia **„alarm włamaniowy"** powoduje następującą sekwencję reakcji/zadziałań:

- Alarm dźwiękowy w klawiaturach LCD;
- Alarm dźwiękowy w przyporządkowanych do stref sygnalizatorach optyczno- akustycznych;
- Alarm dźwiękowy w aplikacji SMS;
- Alarm wizualny w aplikacji SMS ze wskazaniem na mapie powstania alarmu z dokładnością do pomieszczenia i czujnika, który go wygenerował;
- Wyświetlenie na monitorze systemu SMS obrazu z kamery obserwującej strefę w alarmie lub jej najbliższą z możliwością zaprogramowania czasu wyprzedzenia, z jakim ma się wyświetlać obraz z nagrania;
- W przypadku alarmu z pomieszczeń graniczących z zewnętrznymi ścianami skierowanie kamery PTZ na strefę w stanie alarmu;

- Wyświetlenie na aplikacji SMS scenariusza alarmowego ze wskazaniem postepowania i parametrów osób do powiadomienia np.: administrator budynku, dyrekcja, służby techniczne etc;

Wywołanie zdarzenia **„alarm napadowy"***) powoduje następującą sekwencję reakcji/zadziałań:

- Alarm dźwiękowy w aplikacji SMS;
- Alarm wizualny w aplikacji SMS ze wskazaniem na mapie powstania alarmu z dokładnością do pomieszczenia i przycisku, który go wygenerował;
- Określenie typu alarmu tzn.: napad, sabotaż, jako równoważne zdarzenie z sygnałem napadu;
- Wyświetlenie na monitorze systemu SMS kamery obserwującej strefę w alarmie lub jej najbliższą z możliwością zaprogramowania czasu wyprzedzenia, z jakim ma się wyświetlać obraz z nagrania;
- W przypadku alarmu z pomieszczeń graniczących z zewnętrznymi ścianami skierowanie kamery PTZ na strefę w stanie alarmu;
- Wyświetlenie na aplikacji SMS scenariusza alarmowego ze wskazaniem postepowania i parametrów osób do powiadomienia np.: administrator budynku, dyrekcja, służby techniczne, ochrona zewnętrzna etc.

*) **Uwaga:** wyjątek stanowi wywołanie alarmu napadowego z pomieszczenia monitoringu. Dla tego przypadku sygnał powinien zostać wysłany do zewnętrznych służb ochronnych (stacji monitoringu alarmów) i spowodować wysłanie zmotoryzowanego patrolu (grupy interwencyjnej). Do ustalenia na etapie wykonawczym.

Sygnalizacja typów sygnałów alarmowych i technicznych generowanych przez SSWiN zostanie ustalona z Zamawiającym na etapie wykonawczym.

13.11. Zasilanie SSWiN.

System SSWiN jest zasilany z dwóch źródeł: podstawowego i rezerwowego. Zasilanie podstawowe jest realizowane z sieci elektroenergetycznej 230V/50Hz. Natomiast zasilanie rezerwowe jest oparte na baterii akumulatorów z zasilaczem buforowym typu A. Pojemność baterii akumulatorów wynika z bilansu mocy z czasem gotowości odpowiednim dla 2. stopnia zabezpieczeń. Ze względu na zastosowanie alternatywnego zasilania podstawowego – agregatu prądotwórczego włączanego po zaniku zasilania podstawowego – czas gotowości rezerwowego zasilacza **typu A** wynosi **24 godziny**. Rezerwowe źródło zasilania jest doładowywane do 80% pojemności w czasie nie dłuższym niż **72 godziny**.

Tabela 13-1. Szacunkowy bilans mocy systemu SSWiN

1180

Lp.	Rodzaj	Typ	Ilość	Prąd spoczynkowy Ic (a)	Prąd alarmu Ia (A)	Całkowity prąd spoczynkowy Ics (A)	Całkowity prąd alarmu Ica (A)
1	Centrala alarmowa	Adresowalna	1	0,3	0,6	0,3	0,6
2	Expander rozszerzeń	Linii	6	0,06	0,12	0,36	0,72
3	Expander rozszerzeń	Wyjść	4	0,005	0,16	0,02	0,64
4	Klawiatura strefowa	Lcd	15	0,06	0,175	0,9	2,625
5	Sygnalizator wewnętrzny	Opt.-akustyczny	1	0	0,9	0	0,9
6	Czujka ruchu	PIR	28	0,005	0,005	0,14	0,14
7	Czujka ruchu	PIR/MW	96	0,005	0,005	0,48	0,48
8	Czujka ruchu	PIR - kurtyna	10	0,005	0,005	0,05	0,05
9	Czujka ruchu zewnętrzna	PIR/MW	4	0,02	0,02	0,08	0,08
10	Czujka kontaktronowa	Drzwiowa Wpuszczana Nawierzchniowa	194	0,005	0,005	0,97	0,97
11	Czujka inercyjna	Inercyjna	6	0,0025	0,0025	0,015	0,015
12	Przycisk antynapadowy	Adresowalny	10	0,0005	0,0005	0,005	0,005
13	Odbiornik radiowy	Bezprzewodowy	2	0,02	0,015	0,04	0,03
14	Prąd całkowity					3,36	7,255
15	Czas pracy spoczynkowej	Ts- 24 h	Zgodnie ze wzorem ((Ts * Ics) +(Ta * Ica)) /0,7 =				
16	Czas pracy alarmowej	Ta- 0,25 h (15 minut)					
17	Wielkość akumulatorów = ((24 *3,36) + (0,25*7,255) / 0,7= 80 ,64 +1, 81/0,7=82,45/0.7=118 Ah						

Szacowana pojemność baterii akumulatorów ok. 118 Ah.Wykonawca zoobowiązany jest do opracowania bilansu energetycznego SSWiN i dopasowania pojemności akumulatorów do przyjętego czasu podtrzymania i zastosowanych w trakcie realizacji urządzeń.

14. SYSTEM OCHRONY INDYWIDUALNEJ ZBIORÓW – SYSTEM BEZPRZEWODOWY (RADIOWY).

System indywidualnej ochrony zbiorów przeznaczony jest do indywidualnej ochrony eksponatów umieszczonych w gablotach oraz do zabezpieczenia innych eksponatów podczas wystaw czasowych lub stałych. W skład systemu wchodzą odbiorniki, czujki bezprzewodowe, elementy wyposażenia oraz system wizualizacji zdarzeń za pomocą mapy ochronionego obszaru z wrysowanymi w plan urządzeniami detekcyjnymi i pomiarowymi. Program do obsługi systemu jest niezależną aplikacją zainstalowaną na osobnym stanowisku komputerowym np. laptop.

Organizacja systemu alarmowego zapewnia identyfikację alarmu napadowego z dokładnością do poszczególnych rejonów pracy. Na etapie wykonawczym przewiduje się ułożenie magistrali komunikacyjnej typu RS485 pod kontem przyszłościowej budowy dodatkowego elementu ochrony indywidualnej muzealiów. Zakres projektu wykonawczego wskazuje ułożenie w trasach komunikacyjnych dodatkowej magistrali komunikacyjnej do wskazanego systemu.

1181

15. SYSTEM KONTROLI DOSTĘPU (SKD)

W obiekcie występują przejścia kontrolowane za pomocą lokalnych klawiatur sterujących elektrozaczepami. Obecnie użytkowany sprzęt należy zdemontować i przekazać Zamawiającemu lub zutylizować w zależności od ustaleń z Zamawiającym.

W ramach budowy systemu regulującego ruch osobowy w obiekcie należy dostarczyć system kontroli dostępu oparty o kontrolery systemowe zintegrowane z czytnikami kart zbliżeniowych lub alternatywnie system w konfiguracji kontroler – czytnik. Do zapewnienia komunikacji na poziomie aplikacji zarządzającej należy zastosować centralę SKD podłączoną do maksymalnie szesnastu drzwi objętych kontrolą ruchu osobowego, zapewnić pełną komunikację i wymianę danych pomiędzy serwerem SKD, a dedykowaną aplikacją administracyjną. Konfiguracja systemu musi uwzględniać możliwość otwarcia drzwi za pomocą kart zbliżeniowych (oraz kodów dostępowych) oraz z poziomu dedykowanej stacji roboczej z oprogramowaniem zarządzającym systemem kontroli oraz aplikacji integrującej SMS. Należy przewidzieć na etapie wykonawczym fizyczne (certyfikowane w zakresie ochrony przeciwpożarowej) połączenie systemu SKD z systemem przeciwpożarowym. Zgodnie ze scenariuszem pożarowym oraz tabelą współdziałania urzadzeń w przypadku wygenerowania alarmu II stopnia z systemu SSP system musi automatycznie odblokować przejścia SKD zlokalizowane na drodze ewakuacyjnej, umożliwiając przeprowadzenie sprawnej ewakuacji osób przebywających w Pałacu tj. korytarze komunikacyjne oraz wyjścia ewakuacyjne.

W celu zachowania kompatybilności stosowanych już przez użytkownika rozwiązań należy dobrać urządzenia zapewniające spójność softwareową i hardwareową z istniejącą infrastrukturą użytkownika. Zastosowane rozwiązanie musi umożliwiać jednorodne administrowanie systemem za pomocą jednej platformy programowej (pełne zarządzanie systemem SKD tj. dodawanie i usuwanie uprawnień, kart, użytkowników, odczyt pamięci zdarzeń, logów systemowych etc.). Rozmieszczenie poszczególnych elementów wskazano odpowiednio na schematach i rzutach:

- PAS-120-PW-IT-SB-R-01-Rzut- piwnica
- PAS-120-PW-IT-SB-R-02-Rzut- parter
- PAS-120-PW-IT-SB-R-03-Rzut- piętro 1
- PAS-120-PW-IT-SB-R-04-Rzut- piętro 2
- PAS-120-PW-IT-SB-R-05-Rzut- poddasze
- PAS-120-PW-IT-SKD-SCH-01- Schemat, System Kontroli Dostępu