

SPIS TREŚCI

1.	DANE OGÓLNE	5
1.1.	WYKONAWCA DOKUMENTACJI	5
1.2.	PODSTAWA OPRACOWANIA	5
1.3.	PRZEDMIOT OPRACOWANIA.....	5
1.4.	WYKAZ NORM.....	5
1.5.	PROJEKTY ZWIĄZANE	6
1.7.	SYSTEMY ZABEZPIECZENIA PRZECIWPOŻAROWEGO	6
2.	SYSTEM SYGNALIZACJI ALARMU POŻAROWEGO (SAP) - OPIS TECHNICZNY	7
2.1.	INSTALACJA SYGNALIZACJI ALARMU POŻAROWEGO – ZASADY OCHRONY OBIEKTU	7
2.2.	OGÓLNY OPIS INSTALACJI SYGNALIZACJI ALARMU POŻAROWEGO	7
2.2.1.	CENTRALA SYGNALIZACJI POŻARU	7
2.2.2.	CZUJKI DETEKCYJNE	8
2.2.3.	RĘCZNY OSTRZEGACZ POŻAROWY (ROP)	9
2.2.4.	MODUŁ INTERFEJSU WE/WY 8 KANAŁOWY	10
2.2.5.	MODUŁ PRZEKAŹNIKA WE/WY 1 KANAŁOWY	10
2.2.6.	SYGNALIZATOR DŹWIĘKOWY	11
2.3.	BILANS MOCY I OBLICZENIE POJEMNOŚCI PĘTLI	11
2.4.	OPIS SPOSOBU ALARMOWANIA CENTRALI SYSTEMU SAP	12
2.5.	INSTRUKCJA REAGOWANIA NA SYGNAŁY ALARMOWE CENTRALI SAP	12
2.6.	MONTAŻ INSTALACJI SYGNALIZACJI POŻARU.....	13
2.7.	TRASY KABLOWE	13
2.8.	SCENARIUSZ POSTĘPOWANIA W RAZIE POŻARU.....	13
2.9.	UWAGI OGÓLNE	14
2.10.	SYSTEM NAPOWIETRZANIA.....	14
2.10.1.	NAPOWIETRZANIE KLATKI SCHODOWEJ.....	14
2.10.2.	ODDYMIAŁNIE KLATKI SCHODOWEJ I SZYBU WINDOWEGO	15
2.10.3.	CENTRALA SYSTEMU ODDYMIAŁNIA	15
2.11.	Specyfikacje central oddymiania :	15
2.11.1.	Centrala CSO1.....	15
2.11.2.	Centrala CSO2.....	16
2.11.3.	Centrala CSO3.....	16
2.12.	WYTYCZNE BRANŻOWE	16
3.	UWAGI KOŃCOWE	16
4.	KONTROLA DOSTĘPU (KD)	16
4.1.	Centrala kontroli dostępu:	16
4.2.	Terminal drzwiowy:	17
4.3.	Czytnik zbliżeniowy na karty:	18
4.4.	Karta zbliżeniowa:.....	18
4.5.	Zwora elektromagnetyczna :	18
4.6.	Konfiguracja systemu kontroli dostępu:.....	18
4.7.	Zarządzanie systemem.....	18
4.8.	Nadzorowanie obecności studentów.....	18
4.9.	Zajętość sal	19
4.10.	Opis montażu systemu kontroli dostępu w budynku:.....	19
4.11.	Programowanie kart i drukarka kart:	19
4.12.	Opis montażu systemu videodomofonu:	19
4.13.	Uwagi końcowe:	19
4.14.	System Portiernia	20
4.14.1.	Założenia ogólne.....	20

4.14.2.	Wydawanie i zwrot kluczy i pozostałych elementów	20
4.14.3.	Elektroniczne systemy depozytowe.....	20
4.14.4.	Cele projektu wdrożenia systemu Portiernia	20
4.14.5.	Planowane korzyści	21
4.14.6.	Użytkownicy systemu.....	21
4.14.7.	Lista głównych funkcjonalności systemu	21
5.	SYSTEM PRZYZYWOWY.....	24
5.1.	Elementy systemu	24
5.1.1.	Centralka alarmowa	24
5.1.2.	Sufitowy przełącznik ciągowy	24
5.1.3.	Przycisk resetujący	24
5.1.4.	Lokalny sygnalizator akustyczno-optyczny	24
5.1.5.	Przełącznik sufitowy	24
5.1.6.	Sygnalizator akustyczno-optyczny	25
5.1.7.	Przycisk resetujący	25
5.2.	Działanie.....	25
5.3.	Bateria	25
5.4.	Instalacja	25
5.5.	Instalacja – zasilanie centrali alarmowej	25
5.6.	Instalacja – okablowanie niskonapięciowe	25
5.7.	Funkcja Potwierdzenia.....	25
5.8.	Dezaktywacja przycisku Reset na centralce	25
5.9.	Funkcja Self-test.....	26
6.	SYSTEM SYGNALIZACJI WŁAMANIA I NAPADU	26
6.1.	Struktura systemu:.....	26
6.2.	Cechy techniczne systemu:	27
6.2.1.	System sygnalizacji włamania i napadu:	27
6.2.2.	Magistrala:	28
6.2.3.	Komunikacja:	28
6.3.	Jednostka centralna centrali alarmowej CA:	28
6.4.	Moduł dodatkowe współpracujące z centralą (wyposażenie dodatkowe centrali):	29
6.5.	Programator –	30
6.6.	Elementy zewnętrzne systemu SSWiN:	30
6.6.1.	Klawiatura LCD, 2x16 znaków:	30
6.6.2.	Zasilacz z ekspanderem 8 wejść / 2 wyjść:	30
6.6.3.	Czujka dualna ruchu i zbitcia szkła:.....	30
6.6.4.	Czujka magnetyczna:.....	30
6.7.	Opis instalacji systemu sygnalizacji włamania:	31
6.8.	BILANS MOCY I OBLICZENIE POJEMNOŚCI PĘTLI	31
6.9.	Czas działania systemu:	32
6.10.	Uwagi końcowe:	32
7.	Zintegrowany System Zarządzania Bezpieczeństwem	32

SPIS RYSUNKÓW

Rzut PARTERU Instalacje zabezpieczające.....	rys. Z-01
Rzut PIĘTRA I Instalacje zabezpieczające.....	rys. Z-02
Rzut PIĘTRA II Instalacje zabezpieczające.....	rys. Z-03
Rzut KONDYGNACJI TECHNICZNEJ Instalacje zabezpieczające	rys. Z-04
Schemat systemu sygnalizacji alarmu pożarowego.....	rys. Z-05
Algorytm działania systemu sygnalizacji pożaru	rys. Z-06
Matryca sterowań systemu SAP	rys. Z-07
Schemat sterowania systemem napowietrzania klatki schodowej NR1	rys. Z-08
Schemat sterowania systemem napowietrzania klatki schodowej NR2	rys. Z-09
Schemat podłączenia układów SAP-nr1	rys. Z-10
Schemat sterowania systemem klap ppoż w kanałach wentylacyjnych-NR3	rys. Z-11
Schemat systemu KD	rys. Z-12
Schemat przejścia TYP2	rys. Z-13
Schemat przejścia TYP4	rys. Z-14
Schemat systemu zarządzającego SMS	rys. Z-15
Schemat systemu przyzywowego	rys. Z-16
Schemat systemu SSWiN	rys. Z-17
Schemat podłączenia systemów KD (teren zewnętrzny)	rys. Z-18

1. DANE OGÓLNE

1.1. WYKONAWCA DOKUMENTACJI

GPVT Pracownia Architektoniczna S.C.
ul. Pamiątkowa 2/37
61-512 Poznań

1.2. PODSTAWA OPRACOWANIA

- umowa z Inwestorem,
- wytyczne Inwestora,
- podkłady architektoniczno-konstrukcyjne,
- wizja lokalna w terenie,
- uzgodnienia branżowe,
- Ustawa z dnia 07.07.1994 r. Prawo Budowlane (Dz.U. nr 156 poz. 1118 z 2006 r.), z późniejszymi zmianami,
- Rozporządzenie Ministra Infrastruktury z dnia 03.07.2003 r. w sprawie szczegółowego zakresu i formy projektu budowlanego (Dz.U. nr 120 poz. 1133),
- Rozporządzenie Ministra Infrastruktury z dnia 12.04.2002 r. w sprawie warunków technicznych jakim powinny odpowiadać budynki i ich usytuowania (Dz.U. nr 75 poz. 690), wraz z późniejszymi zmianami z dnia 12.03.2009 r.,
- Ustawa z dnia 24.08.1991 r. o ochronie przeciwpożarowej (Dz.U. nr 81 poz. 351), z późniejszymi zmianami,
- Ustawa z dnia 22.01.1999 r. o ochronie informacji niejawnych (Dz.U. nr 11 poz. 95), z późniejszymi zmianami (Dz.U. 2005 nr 196 poz. 1631),
- Zarządzenie Ministra Sprawiedliwości z dnia 27.07.2007 r. w sprawie szczegółowego sposobu organizacji kancelarii tajnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych,
- Wytyczne dotyczące standardów projektowania, budowy i wdrażania sieci LAN w jednostkach resortu. Ministerstwo Sprawiedliwości RP,
- Obowiązujące przepisy i Polskie Normy,
- Dyrektywa 2006/95/WE UE z 12.12.2006 r. , w sprawie harmonizacji ustawodawstwa państw członkowskich odnoszących się do sprzętu elektrycznego przewidzianego do stosowania w określonych granicach napięcia.

1.3. PRZEDMIOT OPRACOWANIA

Przedmiotem opracowania jest wykonanie projektu teletechnicznego na etapie opracowania wykonawczego dla zadania „BUDOWA CENTRUM SYMULACJI MEDYCZNEJ (BUDYNEK G) PRZY UL.MICKIEWICZA 21 W SANOKU”.

Opracowanie obejmuje:

- Instalacje sygnalizacji pożaru,
- Oddymianie,
- Instalacje kontroli dostępu,
- Instalacje videodomofonową,
- Instalacje przyzywową.
- Instalacje SSWiN

1.4. WYKAZ NORM

- PN-E 08390-1:1996 – Systemy alarmowe. Terminologia,
- PN-EN 54-1:1998 - Systemy sygnalizacji pożarowej – Wprowadzenie,
- PN-EN 54-2:2002 - Systemy sygnalizacji pożarowej – Część 2: Centrale sygnalizacji pożarowej,
- PN-EN:54-3:2002 (U) - Systemy sygnalizacji pożarowej – Część 3: Pożarowe sygnalizatory akustyczne,

- PN-EN 54-4:2001 - Systemy sygnalizacji pożarowej – Część 4: Zasilacze,
- PN-EN 54-5:2002 (U) - Systemy sygnalizacji pożarowej – Część 5: Punktowe czujki ciepła,
- PN-EN 54-7:2002 (U) - Systemy sygnalizacji pożarowej – Część 7: Czujki punktowe działające z wykorzystaniem światła rozproszonego, światła przechodzącego lub jonizacji,
- PN-EN 54-10:2002 (U) - Systemy sygnalizacji pożarowej – Część 10: Wykrywacze płomieni – Czujki punktowe,
- PN-EN 54-11:2002 (U) - Systemy sygnalizacji pożarowej – Część 11: Ręczne ostrzegacze pożarowe,
- PN-EN 50130-4:2002 - Systemy alarmowe – Część 4: Kompatybilność elektromagnetyczna – Norma dla grupy wyrobów: Wymagania dotyczące odporności urządzeń systemów alarmowych pożarowych, włamaniowych i osobistych,
- PN-EN 54-08350-14:2002 - Systemy sygnalizacji pożarowej – Projektowanie, zakładanie, odbiór, eksploatacja i konserwacja instalacji,
- PN-EN 55103-1:2000 - Kompatybilność elektromagnetyczna (EMC). Profesjonalne urządzenia akustyczne,
- PN-EN 50130-4:2002 - Systemy alarmowe – Część 4: Kompatybilność elektromagnetyczna – Norma dla grupy wyrobów: Wymagania dotyczące odporności urządzeń systemów alarmowych pożarowych, włamaniowych i osobistych,
- Wytyczne projektowania instalacji sygnalizacji pożaru opracowane przez CNBOP w Józefowie,
- Wytyczne projektowania Dźwiękowych Systemów Ostrzegawczych opracowane przez CNBOP w Józefowie,
- Systemy sygnalizacji pożarowej. Część 14: Wytyczne planowania, projektowania, instalowania, odbioru i konserwacji: PKN-CEN/TS 54-14,
- PN-EN 60849 Dźwiękowe systemy ostrzegawcze.

1.5. PROJEKTY ZWIĄZANE

- Projekt wykonawczy branży architektonicznej,
- Projekt wykonawczy branży konstrukcyjnej,
- Projekt instalacji elektrycznych wewnętrznych,
- Wytyczne p.poż.

1.7. SYSTEMY ZABEZPIECZENIA PRZECIWPOŻAROWEGO

W związku z prawidłowym funkcjonowaniem obiektu oraz ze względu na konieczność stosowania zabezpieczeń przeciwpożarowych przyjęto określone rozwiązania techniczne zapewniające właściwą ochronę osób i mienia podczas akcji ratunkowej. Elementy wyposażenia związane z powyższym to:

- Zastosowanie okablowania zasilającego umożliwiającego działanie urządzeń ratunkowych (kable zasilające o odporności ogniowej E90 dla zasilania wybranych urządzeń itp.) – wg oddzielnego opracowania „Instalacje elektryczne wewnętrzne”,
- Zastosowanie systemów umożliwiających wykrycie zagrożenia pożarowego - system sygnalizacji alarmu pożarowego SAP,
- Zastosowanie systemu sterowania klapami p.poż. w kanałach wentylacyjnych,
- Zastosowanie systemu napowietrzania i otwierania klap oddymiających,
- Zastosowanie zabezpieczeń ognioodpornych przy przejściach przez przegrody ogniowe budynku,
- Zastosowanie elementów wyposażenia instalacji elektrycznej niezbędne podczas ewakuacji (główny przycisk wyłączenia zasilania, oświetlenie ewakuacyjne i awaryjne) – wg oddzielnego opracowania „Instalacje elektryczne wewnętrzne”.

Przyjęto następujący scenariusz akcji ratunkowej podczas zagrożenia:

- Wykrycie pożaru przez system SAP i powiadomienie PSP,
- Awaryjne odłączenie zasilania poprzez przycisk zdalny,
- Zadziałanie oświetlenia awaryjnego i ewakuacyjnego,
- Sprowadzenie windy osobowej na parter i unieruchomienie z drzwiami otwartymi,
- Odblokowanie drzwi w przejściach kontrolowanych,
- Odłączenie z działania systemu wentylacji bytowej,
- Zamknięcie klap p.poż w kanałach wentylacyjnych,
- Uruchomienie systemu napowietrzania klatki schodowej nr 1,2,
- Otwarcie automatyczne klap oddymiających i napowietrzających.

2. SYSTEM SYGNALIZACJI ALARMU POŻAROWEGO (SAP) - OPIS TECHNICZNY

2.1. INSTALACJA SYGNALIZACJI ALARMU POŻAROWEGO – ZASADY OCHRONY OBIEKTU

Dla zabezpieczenia projektowanych pomieszczeń przed zagrożeniem pożarowym, wewnątrz i na zewnątrz zostanie zainstalowany system sygnalizacji alarmu pożarowego (SAP). System będzie się składał z szeregu elementów podłączonych do centrali pożarowej takich jak: automatyczne czujki, ręczne ostrzegacze pożarowe oraz zewnętrzne i wewnętrzne sygnalizatory optyczno-akustyczne. System SAP zaprojektowano jako trzy pętlowy. Zastosowanie powyższego systemu pozwoli na szybkie automatyczne wykrycie, zasygnalizowanie i zlokalizowanie ewentualnego pożaru oraz podjęcie odpowiedniej akcji gaśniczej. Dodatkowo szybkie powiadomienie o pożarze będzie możliwe dzięki zastosowaniu w ciągach komunikacyjnych ręcznych ostrzegaczy pożarowych. Pozwoli to na natychmiastowe, po zaobserwowaniu przez osoby przebywające w budynku, wszczęcie alarmu pożarowego. System pozwala rejestrować wszystkie zdarzenia (alarmy pożarowe, uszkodzenia) jakie zaszły na obiekcie. Zastosowany system jest w pełni adresowalny, prosty w obsłudze i łatwy do rozbudowy oraz posiada możliwość wyniesienia sygnałów alarmowych. System SAP sterować będzie następującymi instalacjami:

- windy osobowe – sprowadzenie na parter, otwarcie drzwi i zablokowanie,
- klapami p.poż. w kanałach wentylacyjnych – zamknięcie określonych stref,
- centralami wentylacji ogólnej – wyłączenie z działania,
- systemem napowietrzającym,
- urządzeniami oddymiającymi,
- zwolnieniem blokady drzwi objętych kontrolą dostępu,

Po zaniku napięcia sieciowego system SAP będzie działał przez 72 godziny i zapewni czas alarmowania przez 30 minut.

Budynek wyposażono w windy osobowe. System SAP w razie pożaru podaje sygnał sterujący dla windy osobowej, która zjeżdża na parter i pozostaje otwarta.

2.2. OGÓLNY OPIS INSTALACJI SYGNALIZACJI ALARMU POŻAROWEGO

Wszystkie zastosowane elementy systemu sygnalizacji alarmu pożarowego przeciwpożarowego muszą posiadać wymagane aktualne świadectwa dopuszczenia do stosowania (CNBOP Józefów). Projektuje się zastosowanie systemu SAP niezależnego dla projektowanego budynku.

2.2.1. CENTRALA SYGNALIZACJI POŻARU

Centrala sygnalizacji pożaru (CSP) jest odporna na zwarcia i przerwy w obwodzie - pętle dozоровe zapewniają maksymalną niezawodność działania oraz niskie koszty instalacji. Centrala sygnalizacji pożaru przystosowana jest do pracy w sieci.

Najważniejsze cechy centrali sygnalizacji pożaru:

- ekran dotykowy,
- wbudowana drukarka zdarzeń,
- możliwość rozbudowy

- możliwość wymiany poszczególnych modułów funkcjonalnych bez konieczności wyłączania całego systemu oraz ponownego programowania centrali po wymianie modułów,
- możliwość dowolnego umieszczania modułów w slotach (zabudowana elektronika we wszystkich modułach funkcjonalnych, brak możliwości dostępu do elementów elektroniki modułów zapewnia zwiększona odporność mechaniczną i elektrostatyczną),
- możliwość stworzenia 4096 stref dozorowych,
- możliwość wpustowej i powierzchniowej instalacji centrali,
- możliwość zapewnienia wyjść przekaźnikowych o obciążalności 230 V AC 5A w centrali,
- możliwość integracji kilku języków w panelu,
- możliwość podłączenia do pętli dozorowej modułów przekaźnikowych o obciążalności styków 1A/30VDC,
- możliwość podłączenia do pętli dozorowej modułów przekaźnikowych o obciążalności styków 10A/230VAC,
- wielodetektorowa czujka optyczno-termiczna z dodatkowym sensorem chemicznym z możliwością wyboru czułości czujki dopasowanej do konkretnego pomieszczenia,
- możliwość adresowania elementów liniowych instalowanych w pętli dozorowej (czujki, ropy, moduły wejścia/wyjścia) przy pomocy wewnętrznych przełączników umieszczonych w tych elementach lub z poziomu centrali sygnalizacji pożaru,
- wszystkie elementy posiadają wbudowane izolatory zwarć,
- ręczne ostrzegacze pożarowe dwustadniowe (uruchomienie wymaga zbitcia szybki i wciśnięcia przycisku),
- adresowanie elementów na pętli z poziomu centrali SAP lub indywidualnie,
- możliwość instalacji 254 elementów na pętli dozorowej,
- modułowa konfiguracja,
- możliwość podtrzymania zasilania za pomocą akumulatorów,
- duża elastyczność w zakresie możliwości dostosowania do istniejących lub zmieniających się wymagań lokalizacyjnych,
- możliwość pracy central w sieci po łączu światłowodowym,
- prosta obsługa przez 1 osobę,
- ostrzeżenia o konieczności dokonania przeglądu,
- ostrzeżenia o zabrudzeniach i uszkodzeniach czujek,
- testy czujek,
- łatwa instalacja i konfiguracja,
- tryb dzienny i nocny ustawienia czułości,
- zgodność z normami i przepisami,
- możliwość podłączenia pola obsługi dla straży pożarnej,
- możliwość sterowania dowolnymi urządzeniami za pomocą karty przekaźników.

2.2.2. CZUJKI DETEKCyjne

Czujki montowane we wszystkich pomieszczeniach budynku. Montaż do konstrukcji stropu podwieszanego i do konstrukcji stropu podstawowego (wersja z wyniesionym wskaźnikiem zadziałania). Podstawowe parametry jakie muszą spełniać czujki stosowane w projektowanym obiekcie:

- wyposażenie w wewnętrzne detektory optyczne i termiczne,
Zasada działania detektora optycznego polega na pomiarze rozproszenia światła. Dioda LED wysyła światło do komory pomiarowej, gdzie zostaje ono pochłonięte przez układ optyczny. W razie pożaru unoszący się dym dostaje się do komory pomiarowej, powodując rozproszenie światła emitowanego przed diodę LED. Ilość światła trafiającego do diody optycznej jest następnie przekształcana na odpowiedni sygnał elektryczny.

Zależnie od klasy czujki, detektor ciepła wyzwała alarm po przekroczeniu temperatury maksymalnej - 54°C lub 69°C (czujki nadmiarowe) lub w przypadku wzrostu temperatury o określoną wartość w danym czasie (czujki różnicowe),

- tryb pracy czujki – mieszany (optyczny, termiczno-nadmiarowy, termiczno-różnicowy),
- wewnętrzna elektronika diagnostyczna umożliwiająca wzajemną konfigurację i skojarzenie detektorów,
- wbudowane izolatory zwarć (zachowanie komunikacji w przerwanej pętli podczas zerwania kabla lub uszkodzenia elementu),
- możliwość analizy krzywej czasu sygnałów pożaru oraz sygnałów nieprawidłowości,
- elastyczne struktury sieci, w tym „T-taping” bez elementów dodatkowych,
- automatyczne lub ręczne adresowanie czujki za pomocą przełącznika obrotowego, zawsze z lub bez funkcji autodetekcji,
- możliwość wykorzystania oprogramowania RPS/WinPara do dostosowania właściwości czujki do wymaganego zastosowania,
- możliwość odczytywania następujących danych: numer seryjny, poziom zanieczyszczenia detektora optycznego, godziny pracy, bieżące wartości analogowe (wartość systemu optycznego, zabrudzenie, wartość CO),
- automonitoring detektora (awaria układu elektronicznego, poziom zabrudzenia podczas pracy, nieprawidłowość podczas silnego zabrudzenia - zamiast fałszywego alarmu),
- konstrukcja układu optycznego i pokrywy odporna na kurz,
- wyposażenie z diodę LED migająca podczas alarmu (widoczna z każdej strony),
- możliwość zdalnego wyświetlania komunikatu na urządzeniu zewnętrznym,
- zintegrowany system prowadzenia kabli zapobiegający ich wysuwaniu po zakończeniu instalacji,
- wyposażenie podstawy w mechaniczną blokadę zapobiegającą wykręceniu czujki,
- Zasięg maks. 120 m²,
- Maksymalna wysokość montażu 11,0 m (czujka dymu) oraz 8,0m (czujka ciepła).
- Czujki liniowe wyposażone w zwierciadło (pomiar wiązki światła wysłanej z czujki do zwierciadła)

Parametry elektryczne czujek:

- napięcie sterujące 15 – 33 VDC,
- pobór prądu <0,51 mA,
- wyjście alarmowe – słowo danych przesyłane po linii dwużyłowej,
- wyjście wskaźnika – typu otwarty kolektor, przełączające napięcie 0V poprzez rezystor 1,5 kΩ, maks. 15 mA.

Parametry mechaniczne czujek:

- Wymiary: bez podstawy Ø99,5 x 52mm; z podstawą Ø120 x 63,5mm,
- Obudowa: materiał – plastik, tworzywo ABS,
- Kolor: biały, RAL 9010, wykończenie matowe,
- Masa: ok. 80g.

Parametry środowiskowe:

- Temperatura pracy -20°C do +65°C,
- Dopuszczalna względna wilgotność powietrza 95% (bez kondensacji),
- Dopuszczalna prędkość powietrza 20 m/s,
- Kategoria ochrony IP40.

2.2.3. RĘCZNY OSTRZEGACZ POŻAROWY (ROP)

Podstawowe parametry jakie muszą spełniać ręczne ostrzegacze pożarowe stosowane w projektowanym obiekcie:

- automatyczne lub ręczne adresowanie za pomocą przełącznika obrotowego,
- wskaźnik LED informujący o włączonym alarmie lub o potrzebie kontroli,
- procedury sprawdzania ostrzegaczy z testowaniem i wielokierunkowa transmisją – poprzez monitorowanie pętli alarmowej,
- indywidualne adresowanie.

Parametry elektryczne:

- napięcie zasilania 24VDC (15 – 33 VDC),
- pobór prądu 0,4 mA.

Parametry mechaniczne:

- Wymiary (szer x wys x gł) 135x135x40 mm,
- Obudowa: materiał – plastik, tworzywo ASA,
- Kolor: czerwony, RAL 3001, wykończenie matowe,
- Masa: ok. 235 g.

Parametry środowiskowe:

- Temperatura pracy -10°C do +55°C,
- Kategoria ochrony IP52.

2.2.4. MODUŁ INTERFEJSU WE/WY 8 KANAŁOWY

Podstawowe parametry jakie muszą spełniać moduły 8 we/wy stosowane w projektowanym obiekcie:

- możliwość wyboru funkcji monitorowania (EOL lub styk) niezależnie dla każdego z 8 wejść,
- maksymalny prąd przełączania: 2A/30VDC,
- wysyłanie komunikatu o usterce do centrali sygnalizacji pożaru w przypadku zwarcia lub przerwy w pętli sieci LSN,
- łatwość okablowania dzięki zaciskom zasilania,
- monitorowanie max. 8 wejść.

Parametry elektryczne:

- napięcie wejściowe sieci LSN: 15VD – 33 VDC,
- pobór prądu: 5,5 mA,
- minimalny czas włączenia wejść IN 1..8: >3,2ms,
- przekaźnik (niskiego napięcia): NC/COM/styk NO,

Parametry mechaniczne:

- wymiary (szer x wys x gł) 140x200x48 mm,
- obudowa: materiał – plastik, tworzywo ABS+PC-FR,
- ustawienia adresów: 3 przełączniki obrotowe,
- masa: ok. 480 g.

Parametry środowiskowe:

- temperatura pracy -20°C do +65°C,
- kategoria ochrony IP43,
- wilgotność względna: <96%.

2.2.5. MODUŁ PRZESŁANIKI WE/WY 1 KANAŁOWY

Podstawowe parametry jakie muszą spełniać moduły 1 we/wy stosowane w projektowanym obiekcie:

- maksymalny prąd przełączania 1A,
- wysyłanie komunikatu o usterce do centrali sygnalizacji pożaru w przypadku zwarcia lub przerwy w pętli sieci LSN,
- łatwość okablowania dzięki zaciskom zasilania,
- monitorowanie max. 1 wejść.

Parametry elektryczne:

- napięcie wejściowe sieci LSN: 15VD – 33 VDC,
- pobór prądu: 2,1 mA,
- minimalny czas włączenia wejść IN 1..8: >3,2ms,
- przekaźnik (niskiego napięcia): NC/COM/styk NO,

Parametry mechaniczne:

- wymiary (Ø x wys) 50 x 22 mm,
- obudowa: materiał – plastik, tworzywo ABS+PC-Blend

- masa: ok. 130 g.

Parametry środowiskowe:

- temperatura pracy -20°C do $+55^{\circ}\text{C}$,
- kategoria ochrony IP30,
- klasa bezpieczeństwa II,
- wilgotność względna: $<96\%$.

2.2.6. SYGNALIZATOR DŹWIĘKOWY

Podstawowe parametry jakie muszą spełniać sygnalizatory zewnętrzne stosowane w projektowanym obiekcie:

- poziom ciśnienia akustycznego do 114 dB(A),
- zwarta, wytrzymała konstrukcja,
- praca bezobsługowa,
- hermetycznie zamknięty układ elektroniczny,
- możliwość wygenerowania 28 różnych sygnałów akustycznych,
- kodowanie za pomocą wbudowanego 5-pozycyjnego przełącznika,
- wbudowany potencjometr dla regulacji głośności.

Parametry elektryczne:

- napięcie pracy: stałe od 10V do 28V,
- pobór prądu: $<32\text{ mA}$,
- zakres częstotliwości: 400 Hz do 2900 Hz ($\pm 0,15\%$),
- Prąd/czas załączania: 30mA (ponad 2s) / 1,5ms.

Parametry mechaniczne:

- wymiary (\varnothing x wys) 93 x 81 mm,
- obudowa: materiał – plastik, tworzywo ABS,
- masa: ok. 320 g,
- kolor: czerwony RAL 3001.

Parametry środowiskowe:

- temperatura pracy -40°C do $+80^{\circ}\text{C}$,
- kategoria ochrony IP65.

2.3. BILANS MOCY I OBLICZENIE POJEMNOŚCI PĘTLI

Obliczenia wykonano celem doboru akumulatorów podtrzymujących pracę systemu przez okres 72 godzin od momentu zaniku zasilania.

Rodzaj urządzenia	Ilość	Pobór prądu w spoczynku (mA)	Pobór prądu w czasie alarmu (mA)
Centrala CSP	1	300	500
Czujka	270	0,23	5
Przycisk ROP	29	0,5	4,0
Izolator w podstawie czujki	270	0,03	6
Wskaźnik działania	147	0,9	X
Moduł ster	26	0,4	X

Obliczenie pojemności akumulatorów:

$$Q_a = 1,25 \times (72h \times I_d + 0,3h \times I_a)$$

Prąd dozoru I_d :

$$I_d = 1 \times 300mA + 270 \times 0,23mA + 29 \times 0,5mA + 270 \times 0,03mA + 147 \times 0,9mA + 26 \times 0,4mA = 300mA + 78,89mA + 14,5mA + 10,29mA + 132,3mA + 10,4mA = 546,38mA$$

Prąd w stanie alarmu I_a :

$$I_a = 1 \times 500mA + 270 \times 0,23mA + 29 \times 0,5mA + 270 \times 0,03mA + 147 \times 0,9mA + 26 \times 0,4mA = 746,38mA$$

$$Q_a = 1,25 \times (72h \times 0,546 + 0,3h \times 0,746) = 1,25 \times (39,312 + 0,223) = 49,41h$$

Dobieram akumulator o pojemności 2x50Ah

2.4. OPIS SPOSOBU ALARMOWANIA CENTRALI SYSTEMU SAP

Sygnalizacja alarmu w zastosowanym systemie w zależności od sytuacji może przebiegać dwustopniowo. System może w pierwszej kolejności sygnalizować alarm 1 stopnia, a następnie pełny alarm pożarowy.

Alarm 1 stopnia jest stanem, sygnalizowanym przez centralę wtedy, gdy przy odczycie informacji z czujki zostanie przekroczony poziom alarmu 1 stopnia. Zwykle jest to stan, który poprzedza pełny alarm pożarowy, gdy ilość dymu nie jest jeszcze wystarczająca do wywołania alarmu. Alarm 1 stopnia sygnalizowany jest wyłącznie poprzez buczek centrali SAP.

Programując centralę SAP należy ustawić czas 20 s na potwierdzenie alarmu oraz czas 5 min. na weryfikację alarmu. Nie potwierdzenie alarmu w ciągu 20 s lub potwierdzenie i nie skasowanie alarmu w ciągu 5 min. spowoduje pełny alarm pożarowy.

Pełny alarm pożarowy powoduje wywołanie informacji dźwiękowej oraz odpowiednieysterowanie klap ppoż w kanałach wentylacyjnych, sprowadzenie i zablokowanie wind na parterze oraz odblokowanie drzwi z kontrolą dostępu. Możliwe jest również przekazanie sygnału alarmowego na zewnątrz. W tym celu Inwestor powinien podpisać umowę z podmiotem świadczącym takie usługi. Urządzenie pośredniczące w przekazaniu sygnału dostarcza jednostka, do której sygnał ten będzie przekazywany.

UWAGA: Czas weryfikacji alarmu pożarowego potwierdzić rzeczywistym pomiarem na obiekcie wybudowanym dla najbardziej oddalonego miejsca.

2.5. INSTRUKCJA REAGOWANIA NA SYGNAŁY ALARMOWE CENTRALI SAP

W razie wystąpienia alarmu 1 stopnia włączy się buczek centrali. Na wyświetlaczu LCD będzie informacja o urządzeniu, które wywołało alarm 1 stopnia (wraz z jego opisem). Po odczytaniu informacji należy nacisnąć klawisz WYCISZ BUCZEK, aby wyłączyć wewnętrzny buczek centrali oraz aby potwierdzić przyjęcie alarmu. Po wyciszeniu bucza należy zbadać przyczynę powstania alarmu 1 stopnia. Gdy sytuacja została opanowana (przyczyna alarmu 1 stopnia zlokalizowana) należy przywrócić stan spoczynkowy centrali. W tym celu należy przekręcić klucz w pozycję *odblokowany* i nacisnąć klawisz RESET.

Jeżeli wystąpi pełny alarm pożarowy zaświecą się dwie czerwone diody z opisem POŻAR. Uruchomi się wewnętrzny buczek centrali, włączone zostaną syreny, centrala poda sygnał otwarcia sterownikom klap oddymiających, Zaświecą się również czerwone diody stref w których wykryto pożar.

Na wyświetlaczu LCD będzie informacja o urządzeniu, które wywołało pożar (wraz z jego oznaczeniem poprzez numer urządzenia/piętro/nr pętli). Po odczytaniu informacji należy nacisnąć klawisz WYCISZ BUCZEK, aby wyłączyć wewnętrzny buczek centrali oraz aby potwierdzić przyjęcie alarmu.

Jeżeli zakończono ewakuację ludzi z budynku lub po weryfikacji alarm okazał się fałszywy, można wyłączyć syreny poprzez przekręcenie klucza w pozycję *odblokowany* i naciśnięcie klawisza WYŁĄCZ SYRENY. W razie stwierdzenia, że konieczna jest dalsza sygnalizacja akustyczna należy ponownie nacisnąć klawisz WYŁĄCZ SYRENY, a syreny ponownie się uruchomią.

Gdy sytuacja została opanowana (pożar zlokalizowany i pod kontrolą lub sprawdzone miejsce powstania fałszywego alarmu) należy przywrócić stan spoczynkowy centrali. W tym celu należy przekręcić klucz w pozycję *odblokowany* i nacisnąć klawisz RESET.

Uwaga:

Wykonawca zobowiązany jest do przeszkolenia personelu pod kątem obsługi systemu SAP oraz wykonania instrukcji postępowania w przypadku wystąpienia alarmu pożarowego w porozumieniu z Inwestorem/Użytkownikiem, przed oddaniem instalacji SAP do użytkowania.

2.6. MONTAŻ INSTALACJI SYGNALIZACJI POŻARU

Centrala CSP zamontowana będzie w pomieszczeniu ochrony. Przy centrali należy zamontować zasilacze. Zasilacz wyposażać w dwa akumulatory 2x50Ah/12V.

Poszczególne elementy systemu należy połączyć kablem niepalnym YnTKSYekw 2x2x1,0 w kolorze czerwonym w pętłę (czujki, ROP-y, moduły: we./wy., moduły sterowników syren). Do sterowania syrenami służyć będą moduły sterujące umieszczone w centrali na płycie głównej.

Kabel zasilający centralę SAP i zasilacze prowadzone z rozdzielni elektrycznej zostały ujęte w projekcie branży elektrycznej pt. „Instalacje elektryczne wewnętrzne”.

Centralę należy uziemić do szyny zbiorczej uziemień. Do obwodu zasilającego systemu pożarowe nie wolno podłączać żadnych innych odbiorników.

Kable instalacji SAP w korytarzach prowadzić w korytkach kablowych. Od korytek do czujek kable układać w rurach elektroinstalacyjnych. Dla prowadzenia zespołów kablowych należy zastosować korytka i wsporniki niepalne o klasie niepalności 90min. Dla zespołów kablowych mocowanie kabla uchwytami PH90 wykonać co 30 cm.

Należy zwrócić szczególną uwagę na właściwe podłączenie kabla YnTKSYekw 2x2x1,0 w urządzeniach (odporność na zakłócenia elektromagnetyczne). Wszystkie łączenia kabli systemu SAP należy wykonywać bezpośrednio w urządzeniach- nie należy łączyć przewodów na trasie kablowej. Należy stosować kable przedstawione w projekcie lub inne zgodne z DTR urządzenia/systemu.

Centrale SAP należy zamontować na ścianie na wys. 1,50m (spód urządzenia).

Czujki w pomieszczeniach i korytarzach montować na suficie. Czujki zasilane są z CSP. Czujki włączyć w pętłę alarmową poprzez gniazda montażowe. Przestrzeń międzystropową należy wyposażać w czujki z wyniesionym wskaźnikiem zadziałania. Wskaźniki zadziałania instalować bezpośrednio pod miejscem montażu czujki do której są one adresowane. Wskaźniki montować tak aby były widoczne z poziomu danego pomieszczenia.

Centrala SAP w czasie alarmu II stopnia spowoduje windy na parter i spowoduje zablokowanie.

Rozmieszczenie elementów systemu SAP w pomieszczeniach przedstawiono na rysunkach technicznych. Schemat połączeń elementów pętli alarmowych i syren optyczno-akustycznych pokazano w części rysunkowej. Przejścia przez stropy należy uszczelnić pianą ognioodporną o klasie odporności takiej jak przegroda.

2.7. TRASY KABLOWE

Trasy kablowe wykonać jako koryta układane w przestrzeni stropu podwieszanego. Stosować wydzielone koryta dla prowadzenia instalacji elektrycznych i teletechnicznych.

Dla instalacji teletechnicznych stosować koryto 300x100. W szachcie elektrycznym zabudować drabinkę kablową dla prowadzenia przewodów. Stosować drabinkę 300x100 w ilości 2 szt. Przewody w drabince układać równolegle z miejscowym pogrupowaniem za pomocą opasek zaciskowych. Poszczególne linie kablowe należy oznaczyć zgodnie z numeracją określoną przez użytkownika.

2.8. SCENARIUSZ POSTĘPOWANIA W RAZIE POŻARU

STREFA POŻAROWA	BUDYNEK PROJEKTOWA NY	BUDYNEK PROJEKTOWA NY	BUDYNEK PROJEKTOWA NY
	ALARM I STOPNIA	ALARM II STOPNIA	AWARIA
ALARM NA STANOWISKU OCHRONY OBIEKTU	X	X	X
WYŁĄCZENIE WENTYLACJI MECHANICZNEJ		X	
ZAMKNIĘCIE KLAP POŻAROWYCH ODCINAJĄCYCH NA WENTYLACJI		X	
URUCHOMIENIE SYSTEMU NAPOWIETRZANIA	X		
URUCHOMIENIE SYSTEMU ODDYMIAANIA	X		
SYGNAŁ AKUSTYCZNY I ŚWIETLNY W BUDYNKU		X	
SPROWADZENIE WIND OSOBOWYCH NA PARTER I ZABLOKOWANIE		X	
ODBLOKOWANIE DRZWI NA DROGACH EWAKUACJI		X	
POWIADOMIENIE STANOWISKA KIEROWANIA PSP		X	
POWIADOMIENIE FIRMY MONITORUJĄCEJ I KONSERWUJĄCEJ SYSTEM		X	X

2.9. UWAGI OGÓLNE

- Zastosowane urządzenia w poszczególnych systemach muszą posiadać stosowne dopuszczenia do stosowania w ochronie przeciwpożarowej.
- Szczegóły montażowe urządzeń i instalacji zawarte są w DTR dostarczanej przy zakupie przez producenta/dystrybutora.
- Integralną częścią dokumentacji projektowej są karty katalogowe urządzeń i ich DTR – dostarczane przy zakupie.
- Firma wykonująca instalacje powinna posiadać stosowne uprawnienia oraz potwierdzenia przeszkolenia w zakresie montażu, programowania i obsługi systemu wydane przez producenta lub przedstawicielstwo firmy.

2.10. SYSTEM NAPOWIETRZANIA

2.10.1. NAPOWIETRZANIE KLATKI SCHODOWEJ

System napowietrzania zrealizowany będzie poprzez siłownik w drzwiach umieszczonych na poziomie parteru. Siłownik po uzyskaniu sygnalizacji z centrali systemu CSO otwiera drzwi. Jednocześnie centrala CSP uruchamia poprzez centrale oddymiające poszczególne klapy ppoż w kanałach wentylacyjnych (zamknięcie i monitorowanie stanu) oraz otwiera klapy oddymiające w dachu nad klatką schodową. Alarmowanie z centrali CSP odbywa się poprzez wykrzycie zagrożenia dymowego przez czujki pożarowe lub poprzez uruchomienie ręczne przycisku ROP. Zasilanie urządzenia napowietrzającego zrealizowane zostało zgodnie z projektem instalacji elektrycznych. Kable sterujące układać przy pomocy uchwytów atestowanych przez CNBOP układanych na podłożu niepalnym.

2.10.2. ODDYMIANIE KLATKI SCHODOWEJ I SZYBU WINDOWEGO

System oddymiania klatki schodowej i szyb windowego zrealizowany będzie poprzez kłapy oddymiające umieszczone w płaszczyźnie dachu nad częścią komunikacyjną klatek schodowych oraz nad szybem windowym. Przy klapach zamontowane zostaną siłowniki uruchamiające daną klapę. Siłowniki sterowane są z centrali systemu oddymiania. Siłowniki połączyć z centralą CSO1,2 za pomocą przewodów HDGs 3x2,5mm². Kable sterujące układać przy pomocy uchwytów atestowanych przez CNBOP układanych na podłożu niepalnym. Przewiduje się również uruchomienie klap oddymiających bezpośrednio w chwili alarmowania poprzez uruchomienie przycisków oddymiających zlokalizowanych na każdym poziomie budynku przy wejściu z klatki schodowej. Dodatkowo przewiduje się wykorzystanie klap oddymiających w funkcji przewietrzania. W tym celu należy zainstalować dodatkowe przyciski przewietrzające przy wejściach na klatkę schodową. Do centrali CSO1,2 należy doprowadzić sygnał monitorujący z zainstalowanej na dachu centrali pogodowej. Umożliwi to zamknięcie automatyczne klap oddymiających w przypadku nagłego pogorszenia warunków pogodowych. System oddymiania pełni nadrzędną funkcję nad systemem przewietrzania.

2.10.3. CENTRALA SYSTEMU ODDYMIANIA

Do sterowania klapami ppoż wentylacji ogólnej zaprojektowano centralę zasilająco-sterującą urządzeniami oddymiającymi w systemach kontroli rozprzestrzeniania dymu i ciepła, umożliwiającą obsługę siłowników klap lub przepustnic w zakresie kontroli położenia wyłączników krańcowych klap za pomocą wejść sygnalizujących następujące stany:

1. przerwa (linia uszkodzona),
2. zwarcie (wyłącznik krańcowy zwarty),
3. kontrola ciągłości linii poprzez rezystor wpięty na zaciski wyłącznika krańcowego,
4. kontrola parametrów czasowych zmian położenia wyłączników krańcowych;

,a także transmisję wybranych danych pomiędzy poszczególnymi centralami za pomocą otwartego protokołu transmisji RS485 (opcja); transmisję wybranych danych do paneli operatorskich, graficznych stacji sterowania i nadzoru systemów BMS za pomocą otwartego protokołu transmisji RS485 (opcja); współpracę z innymi centralami oddymiania tego samego typu i systemami sygnalizacji pożarowej, które posiadają wyjścia sterownicze nadzorowane do urządzeń przeciwpożarowych wg PN-EN 54-1:2011 wyposażoną w:

- dedykowane mikroprocesorowe moduły monitorowania i sterowania
- dedykowane mikroprocesorowe moduły zarządzająco-komunikacyjne
- blok dedykowanego zasilacza modułów mikroprocesorowych
- wyposażony w przeciwzakłóceńowy filtr sieciowy z zabezpieczeniem przeciwprzepięciowym,
- blok wyłącznika głównego centrali,
- blok zabezpieczeń nadprądowych obwodów automatyki i zasilania,
- wbudowany system testowania podłączonych urządzeń,
- obudowa IP54,
- wbudowany inteligentny system samokontroli poprawności pracy modułów

Funkcjonalność centrali powinna zostać potwierdzona certyfikatem zgodności wydanym przez CNBOP oraz świadectwem dopuszczenia do stosowania w ochronie p.poż.

Monitorowanie klap na kanałach wentylacyjnych powinno być dwustopniowe tzn. informacja widziana na centrali CSP – kłapa zamknięta/kłapa otwarta.

2.11. Specyfikacje central oddymiania :

2.11.1. Centrala CSO1

- Napięcie zasilania 230V
- Częstotliwość 50Hz
- Ilość klap sterowanych – 6

- Grupa przycisków oddymiania – 1 (4 przycisków)
- Ilość central pogodowych – 1
- Grupa przycisków oddymiania – 1 (1 przycisk)
- Akumulator 20Ah – 2 szt.

2.11.2. Centrala CSO2

- Napięcie zasilania 230V
- Częstotliwość 50Hz
- Ilość klap sterowanych – 8
- Grupa przycisków oddymiania – 1 (4 przycisków)
- Ilość central pogodowych – 1
- Grupa przycisków oddymiania – 1 (4 przycisk)
- Ilość sterowanych wejść – 1 grupa (2 sztyki)
- Akumulator 20Ah – 2 szt.

2.11.3. Centrala CSO3

- Napięcie zasilania 230V
- Częstotliwość 50Hz
- Ilość klap sterowanych – 14
- Akumulator 20Ah – 1 szt.

2.12. WYTYCZNE BRANŻOWE

Dla prawidłowej pracy systemu sygnalizacji pożaru należy:

- Zapewnić zasilanie dla poszczególnych elementów systemu SAP nie zasilanych z centrali,
- Zapewnić nadzór zewnętrzny w przypadku wystąpienia alarmu w porze nocnej lub poza okresem urzędowania – podpisanie umowy z PSP (łączność analogowa i radiowa),
- Zapewnić właściwe uziemienie centrali CSP, CSO.

3. UWAGI KOŃCOWE

W trakcie realizacji projektu powinien być prowadzony nadzór autorski ze strony projektanta oraz nadzór ze strony Inwestora i przyszłego użytkownika.

W sprawach wątpliwych występujących w trakcie realizacji należy zwrócić się do osoby pełniącej nadzór Inwestorski. Kable elektryczne instalacji prowadzone w gruncie nad poziomem piwnicy parteru układać w rurach osłonowych.

Projekt budowlany zakłada pewne rozwiązania materiałowe które określają zakładany standard wykonania. Wykonawca jest zobowiązany do zachowania wymaganego standardu z możliwością zastosowania materiałów i rozwiązań równoważnych lecz nie gorszych niż podanych w projekcie.

Całość prac należy wykonać zgodnie z obowiązującymi przepisami i normami. Po zakończeniu prac należy wykonać wszystkie wymagane pomiary, a protokół przekazać Inwestorowi.

Wykonawca jest zobowiązany do przedstawienia protokołów:

- zadymienia wszystkich czujników dymu,
- sprawdzenie poprawności działania wszystkich elementów,
- rezystancji linii.

Wszystkie elementy SAP, napowietrzania i oddymiania muszą być trwale opisane.

4. KONTROLA DOSTĘPU (KD)

4.1. Centrala kontroli dostępu:

Centrala urządzeniem wykorzystywanym systemie kontroli dostępu RACS, która poszerz jego funkcjonalność dodatkowe funkcje takie jak: rejestrację zdarzeń, definiowanie czasowych praw dostępu, a także możliwość realizacji funkcji globalnych takich jak strefy APB i strefy alarmowe.

Głównymi zadaniami centrali jest zarządzanie i koordynacja pracy niezależnych urządzeń wchodzących w skład systemu kontroli dostępu typu RACS.

Główne funkcje centrali:

- sterowanie harmonogramami czasowymi,
- zbieranie i magazynowanie zdarzeń które wystąpiły w systemie
- synchronizacja zegarów urządzeń funkcjonujących w systemie.

Charakterystyka centrali:

- Możliwość podłączenia do 32 kontrolerów w ramach jednej podsieci (podsystemu).
- Zegar czasu rzeczywistego z podtrzymaniem baterijnym.
- Nieulotny bufor 250.000 zdarzeń.
- Programowalne linie wejściowe i wyjściowe.
- Dwa wyjścia przekaźnikowe 1.5A/30V.
- Dwa wyjścia tranzystorowe 1A/15V.
- Cztery wejścia NO/NC.
- Interfejs komunikacyjny RS485 (dowolna topologia).
- Sygnalizacja stanów alarmowych.
- Możliwość aktualizacji oprogramowania firmowego (fleszowanie).

W celu komunikacji centrali kontroli dostępu z siecią zastosowano moduł komunikacyjny (interfejs RS232/RS485/RS422-Ethernet). Interfejs komunikacyjny umożliwia komunikację z urządzeniami wyposażonymi w port szeregowy za pośrednictwem sieci komputerowej typu LAN lub WAN. Od strony portu szeregowego może być skonfigurowany do standardu RS232, RS422 lub RS485, od strony sieci komputerowej posiada gniazdo 100/10 BaseT Ethernet. Układ jest identyfikowany w sieci komputerowej za pośrednictwem numeru IP.

4.2. Terminal drzwiowy:

Terminal drzwiowy to kontroler dostępu przeznaczony dla jednego przejścia. Kontroler obsługuje dwa czytniki interfejsem Wiegand 26-66 bit oraz posiada wbudowany zasilacz buforowy 1.5A i może być wykorzystany zarówno w instalacjach autonomicznych jak i sieciowych nieprzekraczających 10000 użytkowników. Pracując w trybie autonomicznym kontroler nie oferuje harmonogramów czasowych oraz rejestracji zdarzeń, jednakże po uzupełnieniu systemu o centralę obie wymienione wcześniej funkcje stają się dostępne.

Charakterystyka terminala:

- Wbudowany czytnik zbliżeniowy
- Możliwość dołączenia dodatkowego czytnika zewnętrznego (obustronna kontrola przejścia).
- Możliwość dołączenia dwóch czytników pracujących w formacie Wiegand.
- Wbudowany zasilacz buforowy 1.5A.
- Tryby drzwi (Normalny, Zablokowane, Odblokowane i Warunkowo Odblokowane).
- Komunikacja przez RS485.
- Dowolna topologia magistrali komunikacyjnej.
- 10000 użytkowników w systemie.
- Obsługa dodatkowych użytkowników typu „gość” definiowanych indywidualnie na każdym kontrolerze.
- Ochrona antysabotażowa (tamper).
- Możliwość podziału systemu na podsystemy.

Funkcje dodatkowe dostępne tylko w systemach wyposażonych w centralę CPR32-SE:

- 99 harmonogramów czasowych.
- 250 grup dostępu.
- 250.000 zdarzeń w buforze.
- Lokalny anti-passback.
- Globalny anti-passback.
- Globalne sterowanie stanem uzbrojenia z podziałem na strefy alarmowe.

4.3. Czytnik zbliżeniowy na karty:

Czytnik zbliżeniowy wykorzystywany jest jako terminal zbliżeniowy i podłączany jest do nadrzędnego terminala drzwiowego.

Charakterystyka czytnika:

- Karty 13.56 MHz standardu ISO/IEC 14443A i MIFARE®.
- Konfigurowalny format transmisji danych wyjściowych.
- Formaty wyjściowe: Wiegand 26..66 bit, Magstripe (Clock & Data), RS232, RACS (Roger) i inne.
- Różne warianty transmisji kodów PIN.
- Osobne wejścia do kontroli wskaźnika LED oraz głośnika.
- Ochrona antysabotażowa (tamper).

4.4. Karta zbliżeniowa:

Karta zbliżeniowa jest cienka i wykonana z PVC, posiada wydrukowanym numerem, rozmiar ISO oraz ma możliwość nadruku zdjęcia i tekstu przy użyciu dedykowanych drukarek PVC.

Charakterystyka:

- pamięć Rom 4kB, programowana fabrycznie,
- częstotliwość pracy 13,56 MHz MIFARE,

4.5. Zwora elektromagnetyczna :

Zwora przeznaczona jest do dwustronnej kontroli dostępu. Zamek można w każdej chwili odblokować za pomocą klucza.

Funkcje monitoringu: pozycja rygla, pozycja spustu, użycie klamki, użycie klucza.

Charakterystyka :

- Styki mikroprzełączników.
- Wysunięcie rygla: 20mm rygiel prostokątny, 10mm zatrask.
- Monitoring: pozycja rygla, pozycja spustu, użycie klamki, użycie klucza.
- Backset: 30, 35, 40, 45 mm.
- Szerokość blachy czołowej: 24 lub 28 mm.
- Trzpień klamki: 9 i 8 mm.
- Tryb pracy: NC/NO.
- Kierunek otwierania: lewy/prawy.

4.6. Konfiguracja systemu kontroli dostępu:

- System kontroli dostępu jest konfigurowany przy pomocy centrali nadzorującej, która nadzoruje wszystkie terminale drzwiowe.
- Kontrolą dostępu obejmuje:
- Wejście do sal dydaktycznych.
- Wejścia do budynku na parterze (wejście główne i boczne).

4.7. Zarządzanie systemem

Programowanie i zarządzanie systemem odbywać się będzie z poziomu stanowiska komputerowego wraz z oprogramowaniem umożliwiającym wizualizację, sterowanie, nadzorowanie, dodawanie nowych użytkowników. System musi wykorzystywać system istniejących legitymacji studenckich (MIFARE). Należy umożliwić rejestrację logowania się studenta w celach weryfikacji obecności na zajęciach. System musi umożliwiać rejestrację zajętości Sali poprzez wskazanie na panelach wyświetlaczy zlokalizowanych w poszczególnych wejściach do sal oraz na korytarzach głównych.

4.8. Nadzorowanie obecności studentów

System kontroli dostępu wykorzystujący karty zbliżeniowe (MIFARE) musi umożliwiać rejestrację wejścia studentów na zajęcia w danym pomieszczeniu. System musi być kompatybilny z kartami studenckimi. Rejestracja obecności musi zostać zapisana na dysku serwera poprzez podłączenie do sieci okablowania strukturalnego. System musi

być kompatybilny z systemami kontroli dostępu zainstalowanymi w pozostałych obiektach użytkownika.

4.9. Zajętość sal

Należy zapewnić łączność systemu kontroli dostępu do Sali z monitorem systemu rezerwacji podającym zajętość danej Sali.

System rezerwacji sal powinien posiadać następujące funkcje:

- obsługa systemu poprzez przeglądarkę internetową,
- możliwość integracji systemu z Microsoft Active Directory,
- dostęp do API systemu umożliwiający integrację z innymi systemami używanymi w uczelni,
- kompatybilność systemu z kontrolą dostępu.

4.10. Opis montażu systemu kontroli dostępu w budynku:

- W pomieszczeniu serwerowni 0.06 należy zamontować centralę systemu (CEN) na wysokości 1,6m. Nad drzwiami w miejscach zaznaczonych na rysunkach w przestrzeni między sufitowej (w przypadku braku sufitu podwieszanego terminale należy montować na wysokości $h=2,5m$) należy zamontować terminal drzwiowy. Wszystkie manipulatory należy zamontować na wysokości 1,4m.
- Kontroler połączyć z terminalami kablem YTKSY 1x2x0,8mm² zgodnie z schematem blokowym.
- Terminale drzwiowe połączyć z urządzeniami sterującymi zgodnie z schematem blokowym poszczególnych typów przejść.

4.11. Programowanie kart i drukarka kart:

Programowanie kart kontroli dostępu odbywa się za pomocą dedykowanego zestawu. W skład zestawu wchodzi: czytnik, 10 niezaprogramowanych kart zbliżeniowych, interfejs komunikacyjny. Oprogramowanie dedykowane do programowania kart jest ogólnodostępne.

Nadruk na kartach odbywa się za pomocą drukarki kolorowej dwustronnej do kart PCV.

W zakresie wykonawcy jest dostawa opisanych wyżej urządzeń wraz z instalacją. System musi być obsługiwany z jednostki sterującej BMS.

4.12. Opis montażu systemu videodomofonu:

- Pierwszy videodomofon projektuje się przed wejściem do holu (0.24) od przodu budynku w celu możliwości otwarcia drzwi. Videodomofon umieścić na wysokości 1,4m. Drugi videodomofon projektuje się przy wejściu tylnym do holu (0.24).
- W pomieszczeniu 0.25 przywidziano montaż videomonitora odbiorczego.
- Video monitor ma możliwość przyciskiem wymuszenie otwarcia drzwi wejściowych. Funkcja wymuszania otwarcia realizowana jest poprzez połączenie videodomofonu z terminalem drzwiowym.

4.13. Uwagi końcowe:

- montaż, uruchomienie oraz stały serwis (nadzór) nad systemami kontroli dostępu należy zlecić jednostce (firmie) posiadającej odpowiednie uprawnienia i certyfikaty.
- przed rozpoczęciem instalacji oraz uruchomieniem systemu należy zapoznać się z instrukcjami montażu dostarczonymi przez producenta wraz z urządzeniami. Podczas montażu i programowania urządzeń należy bezwzględnie przestrzegać zaleceń producenta,
- wszystkie roboty objęte niniejszym projektem należy wykonać zgodnie z obowiązującymi normami, przepisami i warunkami na roboty teletechniczne,
- przy pracach wykonawczych należy bezwzględnie przestrzegać przepisów BHP,
- przed rozpoczęciem instalacji oraz uruchomieniem systemu należy zapoznać się z instrukcjami montażu dostarczonymi przez producenta wraz z urządzeniami. Podczas montażu i programowania urządzeń należy bezwzględnie przestrzegać zaleceń producenta,

- do wykonania instalacji wg niniejszego opracowania należy użyć materiałów wymienionych w zestawieniu poniżej lub równoważnych o nie gorszych parametrach technicznych,
- wszystkie zmiany wprowadzone na budowie w trakcie realizacji należy uzgodnić z projektantem i Inwestorem.
- po wykonaniu instalacji należy opracować dokumentację powykonawczą.

4.14. System Portiernia

4.14.1. Założenia ogólne

Autoryzowani użytkownicy mogą pobierać klucze, bez konieczności tradycyjnego wpisywania się do papierowego rejestru. OPTIpass Portiernia działa z wykorzystaniem identyfikatorów zbliżeniowych dołączonych do kluczy. Aby pobrać klucz z portierni potrzebna jest kart pracownicza. System rejestruje wszystkie wydania i zwroty oraz umożliwia szybki podgląd historii wypożyczeń. W wyjątkowych okolicznościach portier może wydać klucze osobom nieupoważnionym i ręcznie uzupełniać dane w systemie. Na komputerach w portierni instalowane są czytniki zbliżeniowe i odpowiednie oprogramowanie. Użytkownik poprzez zbliżenie karty do czytnika powoduje wyświetlenie swoich danych na monitorze. Następnie do czytnika przykładana się klucz z identyfikatorem zbliżeniowym i wydanie klucza zostaje zapisane w systemie.

4.14.2. Wydawanie i zwrot kluczy i pozostałych elementów

System musi umożliwić prowadzenie rejestru wypożyczeń różnego rodzaju sprzętu, narzędzi i urządzeń. Poszczególne urządzenia muszą zostać zarejestrowane w systemie, muszą zostać nakleione na nie etykiety zbliżeniowe i przydzielone uprawnienia odpowiednim użytkownikom. Sama zasada działania jest identyczna jak w przypadku wydawania kluczy.

4.14.3. Elektroniczne systemy depozytowe

Wspomagają pracę Administratorów Budynków, ułatwiając i porządkując zarządzanie kluczami na obiekcie. Są połączeniem standardowych mechanicznych zabezpieczeń, takich jak sejfy, kasy pancerne, szafki, skrytki z najnowszymi rozwiązaniami elektronicznymi. Dzięki takiej integracji, końcowy użytkownik otrzymuje produkt, przy pomocy którego może w bezpieczny sposób przechowywać wartościowe przedmioty, będąc pewnym, że zdeponowane przedmioty będą użytkowane tylko przez osoby do tego uprawnione. Depozytory kluczowe oferują nadzór nad przechowywaną zawartością. Wszystkie moduły operacyjne są wyposażone w zamki kodowe. Użytkownik przy pomocy indywidualnego kodu PIN może otworzyć drzwiczki do depozytu. Dodatkowo, do identyfikacji użytkowników może zostać wykorzystany identyfikator zbliżeniowy (np. karta procesorowa). Wszystkie działania, wykonane przez użytkownika, są zapisywane w pamięci kontrolera. Administrator systemu może w prosty sposób przejrzeć historię zdarzeń. Nieprawidłowości w systemie, alarmy, nietypowe zdarzenia np. związane ze zwróceniem nieprawidłowego klucza są automatycznie sygnalizowane w oknie monitorowania. Zdeponowane klucze są połączone przy pomocy specjalnej plomby z tagiem posiadającym swój indywidualny numer seryjny. Po włożeniu taga do gniazda jest on blokowany, a kontroler czytuje numer taga i porównuje z numerem zapisanym w bazie. Zwracane klucze mogą być deponowane w dowolne puste gniazdo lub być na stałe przypisane przez administratora do odpowiednich gniazd.

Rozwiązaniem dedykowanym do przechowywania i zarządzania kluczami jest seria metalowych szaf wyposażonych w zestaw szyn z wbudowanymi gniazdami.

4.14.4. Cele projektu wdrożenia systemu Portiernia

- Obsługa procesów związanych z rejestracją i wydawaniem kluczy do pomieszczeń
- Nadzór nad wykorzystywaniem pomieszczeń
- Generowanie raportów dot. wykorzystania pomieszczeń
- Nadzór nad uprawnieniami dostępu do pomieszczeń
- Obsługa procesu wydawania kluczy do pomieszczeń
- Rejestracja gości przebywających na terenie kampusu

4.14.5. Planowane korzyści

- Ograniczone zaangażowanie pracowników w proces wydawania kluczy
- Pełny nadzór nad dostępem do pomieszczeń
- Ewidencja osób przebywających na terenie budynków
- Ewidencja wydanych kluczy do pomieszczeń
- Informacja dot. fizycznej obecności osób w budynkach w sytuacjach awaryjnych (np. pożar, ewakuacja)

4.14.6. Użytkownicy systemu

Wśród głównych użytkowników systemu należy wymienić:

- Operator systemu
- Pracownicy dydaktyczni
- Pracownicy administracyjni
- Studenci
- Portierzy
- Goście

4.14.7. Lista głównych funkcjonalności systemu

Poniższe zestawienie zawiera listę Podstawowych funkcjonalności systemu PORTIERNIA.

NR.	Nazwa Funkcjonalności
	PORTIERNIA
1.	Oprogramowanie przeznaczone do wykonywania zadań dla portierów i pracowników administracyjnych budynków. Umożliwia: <ul style="list-style-type: none"> – wydawanie kluczy użytkownikom, – Rejestrację gości na terenie kampusu, – Nadawanie uprawnień do pomieszczeń, – Integrację z systemem kontroli dostępu, – Integrację z systemem rezerwacji pomieszczeń,
2.	Obsługuje powiązanie kluczy z elementami służącymi do identyfikacji kluczy w systemie (np. brelok Mifare).
3.	Umożliwia przypisanie więcej niż jednego klucza do jednego elementu identyfikującego.
4.	Wykorzystuje, do identyfikacji użytkowników (pracowników/studentów), karty procesorowe wydawane na uczelni
5.	Pozwala obsłużyć aktywne karty procesorowe (Legitymacje studenckie/ Legitymacje doktoranckie/Karty pracownicze) wydane na uczelni
6.	Pozwala na identyfikację osoby (wyświetlać zdjęcie i podstawowe informacje o osobie) w momencie przyłożenia karty procesorowej do czytnika kart oraz wskazuje listę kluczy, do których osoba ma przypisane uprawnienie.
7.	Pozwala na pobranie, przez jedną osobę, więcej niż jednego klucza w ramach procesu wypożyczenia kluczy.
8.	Pozwala na wpisanie uwag podczas procesu wypożyczania klucza.
9.	Umożliwia nadawanie uprawnień do jednego klucza dla wielu osób.

10.	Podczas pobierania klucza, oprogramowanie weryfikuje bieżące uprawnienia osoby do pobierania klucza.
11.	Oprogramowanie, w razie braku uprawnienia do pobrania klucza, rejestruje i sygnalizuje za pomocą dźwięku oraz widocznego na ekranie monitora komunikatu. Próba pobrania klucza przez nieuprawnioną osobą jest zarejestrowana w systemie.
12.	Pozwala na rejestrację operatorów systemu Portiernia (n.: portierzy, pracownicy administracyjni)
13.	System zabezpieczony jest przed nieuprawnionym dostępem poprzez proces logowania operatorów za pomocą loginów i haseł bądź przypisanych do operatorów kart procesorowych.
14.	Operatorzy wydający klucze muszą być zalogowani do systemu w celu identyfikacji wykonawców operacji w systemie.
15.	Oprogramowanie pozwala na obsługę nielimitowanej ilości kluczy zarejestrowanych w systemie.
16.	Oprogramowanie pozwala na obsługę nielimitowanej ilości użytkowników.
17.	Oprogramowanie pozwala na definiowanie przedziałów czasowych pozwalających ograniczyć możliwość wypożyczania kluczy dla użytkowników oraz grup użytkowników indywidualnie dla każdego pomieszczenia.
18.	Oprogramowanie obsługujące wydawanie kluczy może być zintegrowane, z użytkowanym na uczelni, Systemem Personalizacyjnym Karty procesorowe.
19.	Oprogramowanie posiada spójną listę użytkowników oraz kart procesorowych z Systemem personalizacyjnego Karty procesorowe oraz uaktualnia ją na bieżąco.
20.	Oprogramowanie pozwala na tworzenie kont dla administratorów i użytkowników (gości) oraz nadawania im uprawnień.
21.	Oprogramowanie rejestruje i archiwizuje dane/logi/zdarzenia
22.	Oprogramowanie pracujące w tle, w momencie przyłożenia karty procesorowej do czytnika, uaktywnia aplikację prezentując ją na pierwszym planie ekranu monitora.
•	PORTIERNIA – CZĘŚĆ ADMINISTRACYJNA
23.	Oprogramowanie posiada moduł przeznaczony do zarządzania i konfiguracji systemu
24.	Dostęp do części administracyjnej jest możliwy wyłącznie dla uprawnionych użytkowników, po zalogowaniu do systemu.
25.	Oprogramowanie umożliwia zarządzanie grupami użytkowników.
26.	Oprogramowanie umożliwia zarządzanie kluczami do budynków i pomieszczeń.
27.	Oprogramowanie umożliwia zarządzanie rolami użytkowników.
28.	Oprogramowanie umożliwia zarządzanie uprawnieniami użytkowników do pobierania kluczy.
29.	Oprogramowanie pozwala na nadawanie czasowych uprawnień dla użytkowników do pobierania kluczy poprzez podanie dat i godzin obowiązywania uprawnienia.
30.	Oprogramowanie umożliwia zarządzanie opisem działań (akcji), jakie ma podjąć portier lub pracownik administracyjny w przypadku sytuacji alarmowych (np. pożar,

	ewakuacja).
31.	Oprogramowanie ma możliwość generowania zestawień i raportów z konfiguracji systemu.
32.	Oprogramowanie ma możliwość generowania zestawień i raportów stanu kluczy na portierni oraz wypożyczonych kluczy.
33.	Oprogramowanie ma możliwość konfiguracji indywidualnych zestawień i raportów na podstawie danych zgromadzonych w systemie.
34.	Oprogramowanie ma możliwość generowania Raportów dotyczących zdarzeń zachodzących w systemie np. „zalogowanie”, „wylogowanie”, „wypożyczenie”, „próba pobrania klucza bez uprawnień”
35.	Oprogramowanie ma możliwość generowanie raportu zawierającego listę kluczy z przyporządkowanymi osobami, którzy aktualnie posiadają uprawnienie do pobrania danego klucza.
36.	Oprogramowanie pozwala na eksport wyników raportów do pliku CSV i PDF.
37.	Oprogramowanie zrealizowane jest w technologii klient - serwer.
38.	Oprogramowanie może pracować na tym samym serwerze bazy danych, co System Personalizacji Kart funkcjonujący na [Nazwa Uczelni] oraz odwzorowywać strukturę synchronizowanych danych zachowując ich spójność.
39.	Unieważnienie karty procesorowej w Systemie Personalizacyjnym, wykorzystywanym na [Nazwa Uczelni] do personalizacji i przedłużania ważności kart procesorowych, może skutkować odebraniem praw do wypożyczania kluczy, realizowanym przy pomocy tej karty.
40.	Oprogramowanie umożliwia zdefiniowanie struktury organizacyjnej budynków i pomieszczeń [Nazwa Uczelni]
41.	Oprogramowanie powinno ma możliwość importu listy budynków i pomieszczeń wraz z ich wzajemnymi powiązaniami.
42.	Oprogramowanie ma możliwość importu struktury uprawnień użytkowników do pomieszczeń z pliku Excel.
43.	Komunikacja z terminalami (wydanie i zwrot kluczy) odbywa się w oparciu o istniejącą u Zamawiającego infrastrukturę sieciową z wykorzystaniem standardu Ethernet (protokoły IP, TCP, UDP).
44.	Oprogramowanie na serwerze ma możliwość pracy w środowisku wirtualnym, na systemie operacyjnym Windows Server 2008 R2 lub nowszym.
45.	Oprogramowanie ma możliwość instalacji na dowolnie wskazanym stanowisku pracy opartym na środowisku Windows Win7 (32 lub 64) lub nowszym.
•	INTEGRACJA Z DEPOZYTORAMI KLUCZY
46.	System PORTIERNIA umożliwia integrację z autonomicznym Depozytorem Kluczy.
47.	Zastosowanie Depozytorów Kluczy pozwala na zastosowanie systemu zarządzania kluczami w budynkach, w których nie ma portierni.
48.	System zapewnia jednolite zarządzanie uprawnieniami dla użytkowników końcowych, korzystających z depozytorów kluczy.

49.	System umożliwia integrację z Kontrolerem Domeny Zamawiającego oraz synchronizację uprawnień pomiędzy systemami Kontroli Dostępu, PORTIERNIA i depozytorami kluczy
50.	System Pozwala obsłużyć wyjścia ewakuacyjne na wypadek sytuacji awaryjnej (np. pożar, ewakuacja)
51.	System obsługuje Karty Procesorowe wydane na uczelni poprzez czytnik zbliżeniowy.
52.	System depozytorów pozwala na elastyczną rozbudowę o dodatkowe szyny z gniazdami na klucze.
53.	System Pozwala na unikatowe identyfikowanie kluczy
54.	System depozytorów ma możliwość zastosowania dodatkowego zasilania awaryjnego.
55.	System pozwala na obsługę nawet 100 depozytorów w ramach jednej organizacji.
56.	System ma szeroki zakres konfiguracji obejmujący m. inn. możliwość deponowania kluczy w układzie: a) każdy klucz ma przypisane na stałe swoje gniazdo lub b) zwrot klucz do dowolnego, wolnego gniazda

5. SYSTEM PRZYZYWOWY

5.1. Elementy systemu

5.1.1. Centralka alarmowa

Moduł zasilacza z kontrolerem oraz przyciskiem resetującym, dźwiękową sygnalizacją alarmu i dioda sygnalizacyjną LED.

5.1.2. Sufitowy przełącznik ciągowy

Wyposażony w sznur pociągowy z dwoma uchwytami oraz diodę sygnalizacji zadziałania LED.

5.1.3. Przycisk resetujący

Moduł z przyciskiem resetującym oraz diodą sygnalizacyjną LED. Umożliwia lokalne skasowanie alarmu.

5.1.4. Lokalny sygnalizator akustyczno-optyczny

Instalowany po stronie zewnętrznej nad drzwiami lokalnie sygnalizuje stan alarmu wewnątrz pomieszczenia.

Cechy:

- Wbudowany moduł zasilacza
- Wyjście przekaźnikowe
- Załączona bateria awaryjna
- Sygnalizacja dźwiękowa oraz świetlna
- Funkcja potwierdzenia przywołania
- Załączanie/Wyłączanie przycisku Reset
- Funkcja self-test
- Zdejmowane kostki połączeniowe
- 2 uchwyty typu G

5.1.5. Przełącznik sufitowy

Musi zostać zainstalowany w miejscu umożliwiającym użycie z poziomym muszli WC oraz z podłogi w pobliżu tej muszli. Przełącznik dostarczony jest z dwoma uchwytami

typu G. Jeden z nich powinien zostać ustawiony na wysokości ok. 80 – 90 cm a drugi na wysokości ok 10 cm od podłogi.

5.1.6. **Sygnalizator akustyczno-optyczny**

powinien zostać zainstalowany w miejscu gwarantującym dobrą widoczność i słyszalność dla osób mogących udzielić pomocy w sytuacji gdy taka pomoc jest wymagana.

5.1.7. **Przycisk resetujący**

powinien zostać zlokalizowany wewnątrz pomieszczenia w miejscu umożliwiającym użycie go z wózka inwalidzkiego oraz WC.

5.2. **Działanie**

W trybie standby załączona jest dioda 'ON' centrali alarmowej natomiast sygnalizator dźwiękowy oraz sygnalizacyjna dioda alarmowa LED są nieaktywne.

Po załączeniu alarmy przy użyciu przełącznika sufitowego sygnalizatory dźwiękowy i świetlny centrali zostaną uruchomione. Równolegle załączony zostanie lokalny sygnalizator akustyczno-optyczny. Przywołanie może zostać skasowane za pomocą przycisku resetującego wewnątrz pomieszczenia WC. Zależnie od konfiguracji przywołania mogą być resetowane bądź potwierdzone za pomocą przycisku na centralce alarmowej. Jeżeli w czasie 120 sekund od potwierdzenia przywołania na centralce nie zostanie ono zresetowane za pomocą lokalnego przycisku resetującego wówczas centrala ponownie zaszyfralizuje stan „alarm-przywołanie”.

5.3. **Bateria**

Stan baterii jest ciągle monitorowany a wskaźnikiem jest dioda „ON”. Jeżeli dioda jest przyciemniona lub wygaszona wówczas należy baterię wymienić..

5.4. **Instalacja**

Montaż komponentów systemu (z wyjątkiem przełącznika sufitowego) należy przeprowadzić w puszkach elektrycznych dostępnych oddzielnie. Centrala alarmowa wymaga puszek o głębokości 35 mm. Sygnalizator lokalny oraz przycisk resetujący wymagają puszek o głębokości 25 mm.

5.5. **Instalacja – zasilanie centrali alarmowej**

Zasilanie główne 230VDC powinno zostać doprowadzone zgodnie z krajowymi regulacjami. **Zasilanie powinno zostać doprowadzone do centrali bezpośrednio z tablicy elektrycznej, z pominięciem dodatkowych łączówek czy puszek.** Należy zastosować kabel typu YDY min. 3x0.75mm². Obwód należy wyposażyć w zabezpieczenie 3A. Przewód uziemiający należy dołączyć do centrali (zacisk E) oraz do odpowiedniego zacisku puszek, gdy zastosowano puszkę metalową.

5.6. **Instalacja – okablowanie niskonapięciowe**

Do połączeń należy zastosować kabel alarmowy typu YTDY 4 lub 6x0.5 mm. Nie należy prowadzić przewodów alarmowych równolegle do kabli napięciowych.

5.7. **Funkcja Potwierdzenia**

Przycisk Reset na centrali alarmowej może zostać skonfigurowany jako przycisk potwierdzenia. Tryb potwierdzenia aktywny jest przez 120 sekund od chwili użycia przycisku. Jeżeli w tym czasie nie nastąpi reset przywołania na lokalnym przycisku Reset wówczas Sygnalizacja przywołania na centralce zostanie ponownie aktywowana a jej wyłączenie możliwe będzie tylko z poziomu lokalnego przycisku Reset. W celu aktywacji tej funkcji należy delikatnie nawiercić wiertłem o średnicy 3mm punkt MODE na płycie centrali usuwając złotą ścieżkę. Po aktywacji funkcji potwierdzenia nie wolno nawiercać punktu RESET.

5.8. **Dezaktywacja przycisku Reset na centralce**

W celu zapewnienia, że wszystkie skasowania przywołań nastąpią z lokalnego przycisku Reset w toalecie należy dezaktywować przycisk Reset na centralce alarmowej.

Dezaktywację należy wykonać poprzez delikatne nawiercenie punktu RESET na płycie centrali wiertłem o średnicy 3 mm usuwając tym samym złotą ścieżkę z tego punktu.

5.9. Funkcja Self-test

Możliwe jest przetestowanie wszystkich sygnalizatorów dźwiękowych oraz diod sygnalizacyjnych LED z poziomu centrali alarmowej. W tym celu należy w trybie Standby wcisnąć przycisk Reset na centralce. Wszystkie sygnalizatory dźwiękowe i świetlne zostaną aktywowane na krótką chwilę.

6. SYSTEM SYGNALIZACJI WŁAMANIA I NAPADU

6.1. Struktura systemu:

Centrale alarmowe zaprojektowano z myślą o obsłudze małych, średnich oraz dużych obiektów. Niezależnie od wielkości, każda z central posiada rozległe możliwości funkcjonalne. Stworzone na ich bazie systemy alarmowe mogą zostać łatwo rozbudowane przy wykorzystaniu takich samych dla każdej centrali modułów rozszerzających. Daje to również możliwość bezproblemowej wymiany centrali na większą, jeśli rozbudowa systemu tego wymaga.

Centrale alarmowe gwarantują ochronę obiektu przed włamaniem, ale udostępniają też rozbudowane funkcje kontroli dostępu i automatycznego sterowania szeregiem urządzeń.

Centrala charakteryzuje się następującymi właściwościami:

- Modułowa konstrukcja do wszystkich zastosowań dzięki możliwości rozbudowy aż do 512 linii systemy serii SPC nadają się do szerokiej gamy zastosowań. Modułowa konstrukcja umożliwia użycie wspólnych klawiatur, urządzeń oraz modułów rozszerzenia, wchodzących w skład całej rodziny central SPC do rozbudowy systemu zgodnie z potrzebami. Ułatwia to etap planowania niezależnie od wielkości systemu oraz umożliwia jego rozbudowę wraz z rosnącymi wymaganiami klienta.
- Kontrolery serii SPC bazują na wydajnej i zaawansowanej architekturze najnowszego procesora ARM, spełniającej wymagania w zakresie wysokiej wydajności, możliwości komunikacyjnych oraz rozbudowanych funkcji zabezpieczeń.
- Wszystkie kontrolery obsługują „rzeczywisty” podział systemu na partycje, umożliwiając budowę systemu składającego się z wielu obszarów obsługiwanych przez wielu użytkowników. Systemy umożliwiają raportowanie zdarzeń systemowych i działań użytkowników do stacji monitorujących, jak też indywidualne powiadamianie określonych użytkowników o stanach systemu SMS-ami. Podwyższony poziom zabezpieczenia systemu uzyskiwany jest przez powiązanie dostępu użytkownika do generowanej strony internetowej z posiadanymi przez niego uprawnieniami w każdej z partycji.
- Kontrolery mogą łączyć się z SMA (stacjami monitorowania alarmów) za pomocą sieci PSTN, GSM oraz Ethernet. Jeśli wymagane są różne sposoby komunikacji, centrale można zaprogramować tak, by wykorzystywane kanały komunikacyjne posiadały wymagane priorytety. Ponadto do SMA lub na zaprogramowane numery telefonów komórkowych mogą być przesyłane przez sieć GSM komunikaty w formie SMS.
- Koncepcja budowy systemu gwarantuje stały poziom wydajności niezależnie od wielkości systemu. Koncepcja ta opiera się na magistrali lokalnej charakteryzującej się dużą szybkością i długością, stanowiącej idealne rozwiązanie dla dużych instalacji systemowych ze względu na odporność na awarie (konfiguracja pętli) oraz możliwość dołączania urządzeń do magistrali w odległości do 400 m.
- Większe centrale można konfigurować zdalnie przez dowolny kanał komunikacji (PSTN, GSM lub sieć Ethernet dla modelu SPC6000) za pomocą wbudowanej strony internetowej lub oprogramowania narzędziowego zainstalowanego w komputerze. Programowanie zdalne minimalizuje wysokie koszty związane z diagnostyką i wymaganym wsparciem instalatora i może przyczynić się do obniżenia całkowitego kosztu eksploatacji systemu przez użytkownika końcowego.
- Centralę można konfigurować także lokalnie przy użyciu klawiatury, oprogramowania PC lub kopiowania wstępnych ustawień z programatora (funkcja szybkiego

programowania). Łatwe w obsłudze menu (oparte na koncepcji znanej z telefonów komórkowych) wraz z możliwością wyboru typu systemu sprawia, że centrale SPC są jednymi z najszybciej i najłatwiej programowanych za pomocą klawiatury.

- 32-znakowa klawiatura z wyświetlaczem zapewnia nowoczesny i funkcjonalny interfejs użytkownika dowolnej centrali. Klawiatura wyposażona jest w przyciski nawigacji działające w różnych kierunkach, 2 przyciski funkcyjne oraz zintegrowany interfejs czytnika kart. Odznacza się ponadto ergonomiczną budową i umożliwia obsługę we wszystkich warunkach oświetleniowych. Dostępne są dwie wersje klawiatury – jedna zawierająca czytnik kart, druga bez czytnika.
- Wszystkie centrale są zgodne z europejską normą EN 50131 stopień 2 i 3 (EN 50131-1:2006, TS 50131-3: 2003 oraz EN 50131-6:2008), a tym samym instalacje systemowe spełniają wymagania najnowszych norm.
- Centrale posiadają dwa wstępnie zdefiniowane typy instalacji, oba obsługujące wiele partycji oraz różne tryby pracy (ROZBROJENIE, UZBROJENIE, UZBROJENIE CZĘŚCIOWE itd.): tryb rezydencyjny jest przeznaczony do instalacji domowych lub małych obiektów handlowych, składających się z niewielkiej liczby linii dozorowych. Tryb komercyjny oferuje bardziej zaawansowane funkcje oraz programowalne sposoby sygnalizacji alarmów i przeznaczony jest do instalacji komercyjnych z większą liczbą linii dozorowych.
- Rodzaje alarmów generowane przez systemy zależą od typu linii dozorowej, która wyzwoliła alarm (każdy typ linii uaktywni własny, unikalny sygnał wyjściowy – flagę wewnętrzną lub wskaźnik, który można następnie zapisać lub przypisać do wyjścia fizycznego w celu uaktywnienia określonego urządzenia).
 - Uaktywnienie **alarmu pełnego** zostanie zgłoszone do stacji monitorowania alarmów (SMA), jeśli ta została wcześniej skonfigurowana.
 - Uaktywnienie **alarmu lokalnego** nie spowoduje powiadomienia SMA, nawet jeśli stacja została skonfigurowana.
 - Uaktywnienie **alarmu cichego** nie wygeneruje wizualnego ani dźwiękowego sygnału alarmu. Alarm zostanie zgłoszony do SMA.
- Wszystkie klawiatury i moduły rozszerzenia w systemie są dołączone za pomocą magistrali lokalnej charakteryzującej się wysoką szybkością i dużą dopuszczalną długością. Magistrala lokalna może mieć postać standardowej konfiguracji gałęziowej lub postać pętli zamkniętej. Topologia pętli chroni system przed ewentualnymi awariami magistrali przez izolowanie uszkodzonego odcinka w pierścieniu, bez wpływu na pozostałą część systemu. Koncepcja magistrali lokalnej umożliwia bezpieczną dystrybucję zasilania, ponieważ może być podzielona na odcinki niezależnie zasilające urządzenia.

6.2. Cechy techniczne systemu:

6.2.1. System sygnalizacji włamania i napadu:

- Programowane partycje: 32.
- Liczba linii na płycie głównej: 8.
- Max. liczba linii przewodowych: 512.
- Nadzorowanie wejść: NO, NC, pojedynczy EOL, podwójny EOL, potrójny EOL.
- Wartość rezystorów EOL: fabrycznie 4,7KΩ, możliwość wyboru innych wartości.
- Liczba wejść na płycie głównej: 6.
- Maks. liczba wyjść: 512.
- Maks. liczba użytkowników: 512.
- Pamięć zdarzeń: 10000 dla systemu włamaniowego / 10000 dla kontroli dostępu.
- Zegar czasu rzeczywistego: na płycie, zasilany z oddzielnej baterii.
- Język: możliwość wyboru z klawiatury, web serwera.
- Kalendarze: 64 schematy wł/wył przypisywane do użytkownika, partycji, wejść i wyjść.

- Przyczyna & skutek: program sterujący dla 64 wyjść bazujący na swobodnie programowanych stanach systemu (stan linii, wyjść systemowych i partycji, kodów użytkownika, przycisków klawiatury, kalendarzy) lub ich logicznych kombinacji.

6.2.2. Magistrala:

- Konfiguracja magistrali: (2 gałęzie lub 1 pętla).
- Liczba urządzeń na magistrali: 128 (z klawiaturami i kontrolerami drzwi).
- Max. liczba klawiatur: 32.
- Max. liczba ekspanderów 8 we / 2 wy: 63.
- Max. liczba ekspanderów 8 wy: 63.
- Max. liczba zasilaczy z 8 we / 2 wy: 63.
- Max. liczba kontrolerów drzwi: 32.
- Max. liczba odbiorników czujek radiowych (zalecana): 32.

6.2.3. Komunikacja:

- Web serwer: HTTPS.
- Programator: tak.
- Lokalna i zdalna konfiguracja: tak.
- Aktualizacja oprogramowania: lokalna / zdalna centrali i ekspanderów
- X-10: obsługa kontrolera X-10 i poleceń X-10.
- Ethernet: na płycie.
- Interfejsy komunikacyjne: podłączany do płyty PSTN lub GSM (system obsługuje 2 moduły jednocześnie).
- Komunikacja zdarzeń: SMS-em GSM i PSTN.

6.3. Jednostka centralna centrali alarmowej CA:

Projekt systemu zabezpieczeń (centrala CA) wykorzystuje centralę obsługującą max. 512 linii oraz max. 512 wyjść i są dostępne w obudowach metalowych zgodnych z normą EN 50131 stopień 2 (akumulator maks. 7 Ah) lub stopień 3 akumulator maks. 17 Ah). Oba modele central zawierają zintegrowany zasilacz sieciowy, 8 wejść przewodowych, 6 wyjść, 2 interfejsy rozszerzenia, generowaną stronę internetową oraz port Ethernet. Obsługują połączenia dial-up PPP lub GSM przy zastosowaniu dodatkowych modemów.

Podstawowe parametry techniczne:

- Klasa bezpieczeństwa EN50131-1: 2006 Klasa 2 / 3, poziom II - wewnętrzne, ogólne.
- Zgodność: DD243, Garda, UL.
- Maksymalna liczba linii dozorowych: 32 – 128 (maks.).
- Liczba linii dozorowych na płycie kontrolera: 8 - (parametryzacja domyślna: DEOL 2K2).
- Parametryzacja: bez EOL / SEOL / DEOL / MPIR / czujki inercyjne.
- Programowalne wyjścia: 6 – 128.
- Urządzenia magistrali: maks. 32 (16 modułów rozszerzenia i 16 klawiatur).
- Obsługiwane rodzaje urządzeń magistrali X-BUS: klawiatura standardowa, moduły rozszerzeń 8 wejść / 2 wyjścia, moduły, rozszerzeń 8 wejść, zasilacz systemowy.
- Klawiatury: maks. 16.
- Klawiatury z odbiornikami bezprzewodowymi: maks. 8.
- Partycje: maks. 16.
- Użytkownicy: maks. 256.
- Interfejsy fizyczne: RJ45, USB, łączówka śrubowa, moduły podłączane od gniazd na płycie.
- Zabezpieczenie antysabotażowe (Tamper): wbudowany przełącznik otwarcia obudowy + 2 dodatkowe wejścia zabezpieczenia antysabotażowego.
- Zasilacz SPC: zintegrowany z płytką kontrolera (2,5 A).
- Wyjścia na płycie kontrolera: 1 przekaźnik lampy błyskowej (o obciążeniu rezystancyjnym równym 1 A), 1 tranzystor wewnętrznego sygnalizatora dźwiękowego (o obciążeniu rezystancyjnym równym 400 mA), 1 tranzystor zewnętrznego

sygnalizatora dźwiękowego (o obciążeniu rezystancyjnym równym 400 mA), 3 tranzystory konfigurowalne (o obciążeniu rezystancyjnym równym 400 mA).

- Złącza modułów telefonicznych: PSTN V.90 SMS, PPP, GSM.
- USB: połączenie z komputerem PC umożliwiające korzystanie z opcji programowania przy użyciu Web serwera i programu SPC Pro.
- PPP: pełna obsługa.
- Osadzony serwer sieciowy: http.
- Pamięć zewnętrzna do szybkiego programowania: pamięć zewnętrzną można podłączyć do specjalnie przeznaczonego portu w celu umożliwienia szybkiego pobierania plików konfiguracyjnych.
- Zegar wbudowany i dodatkowo zasilany bateryjnie zegar czasu rzeczywistego.
- RS232: 2 porty RJ45 obsługujące protokół X10 lub połączenia zewnętrzne.
- Rejestr zdarzeń: wspólny dla wszystkich partycji rejestr do 20 000 zdarzeń.
- Kopia zapasowa konfiguracji: wykonanie kopii bezpieczeństwa konfiguracji do pliku oraz/lub do pamięci EEPROM.
- Zasilanie sieciowe: 230 AC, +10 do -15%, 50 Hz.
- Bezpiecznik: 250mA T.
- Pobór prądu: 200mA (230VAC).
- Akumulator: szczelny, żelowy.
- Pojemność akumulatora: max. 17Ah / 12V.
- Ładowanie akumulatora: maks. 24h do 80% pojemności.
- Temperatura pracy: 5 – 40 °C.
- Wilgotność względna: maks. 90% (bez kondensacji).
- Kolor RAL: 9003.
- Klasa zabezpieczenia obudowy: IP30.
- Montaż: na ścianie.
- Materiał obudowy: stal, >2,2mm.
- Obudowa: metalowa z drzwiczkami.

6.4. Moduł dodatkowe współpracujące z centralą (wyposażenie dodatkowe centrali):

Moduł GSM z anteną– moduł może pracować w dowolnej sieci GSM przy zastosowaniu odpowiedniej karty SIM. Każda z central posiada odpowiednie gniazdo przeznaczone do podłączenia tego modułu. Jego wyposażenie stanowi antena zewnętrzna , dostosowana do obudowy. Umożliwia raportowanie zdarzeń do stacji monitorowania alarmów z wykorzystaniem ogólnie stosowanych formatów (SIA, Contact ID), a także zdalne połączenie z wykorzystaniem programu celu przeprowadzenia konfiguracji i diagnostyki systemu. Ponadto, wysyła SMS-y do użytkownika lub instalatora w formie ściśle zdefiniowanych tekstów,

informujących o zdarzeniach zachodzących w systemie. Może również odbierać SMS-y sterujące pracą centrali. Moduł GSM może zapewniać połączenia kanałem komunikacyjnym podstawowym lub zapasowym dla IP lub PSTN.

Parametry techniczne:

- Protokół komunikacyjny: protokoły SIA, Contact ID, up/download, dostęp do webserwera, SMS.
- Interfejsy: gniazdo kontrolera 1 x 16, gniazdo anteny.
- LED stanu: 2.
- Typ połączenia: GSM (pasmo 900/1800MHz).
- Pobór prądu: min 50mA (12VDC), max 60mA (12VDC).
- Temperatura pracy: 5 – 40 °C.
- Wilgotność względna: maks. 90% (bez kondensacji).
- Montaż: podłączenie do płyty kontrolera.

6.5. Programator –

Programator udostępnia prostą metodę transferu plików konfiguracyjnych z PC (USB) do centrali z wykorzystaniem programu i magazynowanie kopii konfiguracji do programatora bez korzystania z połączenia z PC. Pamięć programatora posiada pojemność 1MB, co umożliwia zmagazynowanie do 100 typowych plików konfiguracyjnych lub plików firmware'u służących do aktualizacji oprogramowania fabrycznego.

6.6. Elementy zewnętrzne systemu SSWiN:

6.6.1. Klawiatura LCD, 2x16 znaków:

Przewodowa klawiatura umożliwiająca obsługę systemu. Posiada 32 znakowy wyświetlacz podświetlany podobnie jak jej przyciski niebieskim światłem. Proste i intuicyjne menu systemu obsługiwane jest przez centralny przycisk nawigacyjny. Klawiatura posiada również przyciski funkcyjne i alfanumeryczne umożliwiające dokonywanie operacji kontekstowych a także wprowadzanie danych z klawiatury.

6.6.2. Zasilacz z ekspanderem 8 wejść / 2 wyjść:

Zasilacz jest podłączony do magistrali jest monitorowanym źródłem dodatkowego zasilania 12V / 2.6A urządzeń wchodzących w skład systemu, obsługuje akumulator, a także posiada 8 wejść i 2 w pełni programowalne wyjścia przekaźnikowe. Funkcje realizowane przez wyjścia i wejścia ekspandera i znajdujące się na płycie centrali są identyczne. Każde z wejść może zostać indywidualnie zaprogramowane w sposób zgodny z wymaganymi zasadami monitorowania ich stanów. System umożliwia wybór szerokiej gamy wartości rezystorów końca linii. Bezpotencjałowe wyjścia przekaźnikowe o wyprowadzeniach NO i NC zapewniają możliwość elastycznego sterowania urządzeniami dołączonymi do systemu. Zastosowana w module dioda LED informuje o stanie komunikacji z procesorem, a brzęczyk ułatwia identyfikację i lokalizację modułu. Moduł posiada ponadto rozbudowane funkcje diagnostyczne. Zasilacz i ekspander umieszczone w obudowie metalowej, zabezpieczonej przed sabotażem, z miejscem na akumulator o pojemności 17Ah i 3 dodatkowe ekspandery, spełniają wymagania normy EN50131 klasa 3.

6.6.3. Czujka dualna ruchu i zbitcia szkła:

Inteligentna czujka skutecznie wykrywa intruza dzięki wyrafinowanej, cyfrowej obróbce sygnału oraz powiązaniu sposobów detekcji, wykorzystujących pasywną podczerwień i mikrofałe. W obu torach sygnałowych zastosowano wielokryteriową analizę sygnału, która umożliwia skuteczne rozpoznanie i eliminację niepożądanych zakłóceń. Zastosowane rozwiązania konstrukcyjne czynią czujkę niewrażliwą nawet na silnie niekorzystne wpływy otoczenia takie jak przeciągi, zmiany temperatury, zakłócenia elektromagnetyczne, penetrację przez owady czy światło zewnętrzne.

Charakterystyczne parametry:

- Cyfrowa obróbka sygnału,
- Promień charakterystyki szerokokątnej 12 m ze strefą obserwacji pod czujką lub szczelna charakterystyka kurtynowa 12 m,
- Odporność na zwierzęta do 20 kg,
- Doskonała filtracja światła białego dzięki zastosowaniu czarnego lustra,
- Możliwość wyboru czterech ustawień zależnie od warunków pracy.

6.6.4. Czujka magnetyczna:

Czujka magnetyczna składa się z dwóch elementów: czujnika magnetycznego (kontaktronu) i magnesu. Kontaktron umieszczony w pobliżu magnesu zamyka obwód elektryczny.

Czujka magnetyczna może być stosowana wszędzie tam, gdzie występuje potrzeba kontroli stanu drzwi, okien lub innych elementów ruchomych, np. w celu ochrony lub kontroli dostępu do określonych obiektów, pomieszczeń, urządzeń; w systemach automatyki itd.

System SSWiN jest odporny na wypadek prób uszkodzenia czy demontażu przez osoby niepowołane – jest on wyposażony w styki sabotażowe – jakkolwiek nieautoryzowana. Próba

demontażu urządzeń czy przerwania ciągłości instalacji SSWiN spowoduje wszczęcie alarmu wraz z lokalizacją miejsca jego powstania.

Zmiany programowe systemu winny być dokonywane w uzgodnieniu z Użytkownikiem przez autoryzowaną obsługę serwisową.

System został zaprojektowany pod kątem podziału na strefy dozoru. Na życzenie Inwestora można zastosować inny podział na dowolne strefy dozoru. Podział taki należy zlecić firmie posiadającej odpowiednie świadectwa kwalifikacyjne producenta oraz uprawnienia pracowników ochrony technicznej mienia oraz sprzęt serwisowy.

Do rozbijania i uzbrajania systemu zaprojektowano manipulatory z wyświetlaczem LCD. Możliwość rozbijania / uzbrojenia systemu uzależniona jest od przypisania kodów.

Centrala może przekazywać informacje o swoim stanie (uzbrojenie, rozbijanie, niski stan akumulatora, zanik napięcia sieciowego, sabotaż, alarm włamaniowy) poprzez np.: nadajnik GSM do agencji ochrony.

Uwaga: urządzenie pośredniczące w przekazaniu sygnałów do agencji ochrony dostarcza agencja, z którą zostanie podpisana umowa o świadczenie usług ochrony obiektu.

6.7. Opis instalacji systemu sygnalizacji włamania:

W pomieszczeniu technicznym na parterze zamontować centrale systemu sygnalizacji włamania CA. Centralę CA należy zamontować na wysokości $h=1,7m$ (dół obudowy).

Centrale alarmową należy połączyć z ekspanderami, klawiaturami i modułami radiowymi za pomocą kabla magistrali U/UTP, kat.5e, wewnętrzny, 4x2x24 AWG. Połączenie wszystkich elementów systemu należy wykonać jako pętle.

Na korytarzach i w pomieszczeniach zamontować czujki ruchu PIR. Czujki PIR montować na wysokości $h=2,0-2,5m$ (wysokość montażu dla czujki z lustrem kurtynowym 2,0-3,5m). Stosować czujki z funkcją antymaskingu. Czujki PIR, przyciski i czujki magnetyczne (połączyć podcentralami kablami typu YTDY 6x0,5mm²). W pomieszczeniach należy w czujkach ustawić obszar pokrycia jako lustro szerokokątne, a na korytarzach jako lustro kurtynowe. Połączenia wykonać typu 2EOL.

Przy wejściach głównych i w miejscach zaznaczonych na rysunku zamontować na wysokości $h=1,4m$ (dół obudowy) manipulatory. Na zewnątrz na budynku na wysokości $h=3,0m$ zamontować sygnalizator optyczno-akustyczny.

Sygnalizator połączyć z zasilaczem (wyjście nadzorowane) kablem typu YTDY 6x0,5mm². Sygnalizatory wewnętrzne montować na wysokości 2,5m. Zasilacze systemu na wysokości $h=2,5m$.

W ciągach komunikacyjnych kable układać w korytkach kablowych instalacji teletechnicznych.

W pomieszczeniach kable układać w rurach elektroinstalacyjnych 28 podtynkowo.

Przepusty kablowe między strefami pożarowymi uszczelnić pianą ogniochronną.

6.8. BILANS MOCY I OBLICZENIE POJEMNOŚCI PĘTLI

Obliczenia wykonano celem doboru akumulatorów podtrzymujących pracę systemu przez okres 24 godzin od momentu zaniku zasilania.

Rodzaj urządzenia	Ilość	Pobór prądu w spoczynku (mA)	Pobórprądu w alarmu (mA)	Suma prąd Czuwania (A)	Suma prąd alarm (A)	BILANS Ah
Centrala CSW	1	150	150	0,150	0,150	3,6
Koncentrator	16	15	15	0,195	0,195	4,68
Manipulator	3	17	17	0,051	0,051	2,461
Czujka ruchu+zbicia szkła	82	7,5	7,5	0,615	0,615	14,76
Sygnalizator	11	0	120	0	1,32	31,68
Czujka magnt.	18	0,5	0,5	0,0045	0,0045	0,108

Dobrano akumulator 60 Ah

W SSWiN, jeżeli występuje zespół zasilacza zawierający baterię akumulatorów i urządzenie ładujące, Polska Norma definiuje sposób określania minimalnej pojemności akumulatora Q_{min} wyrażoną w2 amperogodzinach [Ah], jako:

$$Q_{\min} = 1,25 * (I_S * t_S + I_A * t_A)$$

gdzie:

I_S – całkowity prąd obciążenia zasilaczy systemu alarmowego, pobierany przez system alarmowy ze źródła rezerwowego w przypadku uszkodzenia zasilania podstawowego 230 VAC, liczony dla warunków, w których system nie jest w stanie alarmu, a jedynym sygnalizowanym uszkodzeniem jest awaria zasilania 230 VAC, wyrażony w amperach [A]

t_S – wymagany czas trwania obciążenia systemu alarmowego w stanie gotowości (dozoru), wyrażony w godzinach [h]

I_A – całkowity prąd obciążenia zasilaczy systemu alarmowego, pobierany przez system alarmowy ze źródła rezerwowego w przypadku uszkodzenia zasilania podstawowego 230 VAC, liczony dla warunków, w których system jest w stanie alarmu, wyrażony w amperach [A]

t_A – wymagany czas trwania obciążenia systemu w stanie alarmu

6.9. Czas działania systemu:

Czas pracy SSWiN na zasilaniu awaryjnym – 24 godzin.

Czas pracy SSWiN na zasilaniu awaryjnym w czasie alarmu – 0,4 godziny (24 minut).

6.10. Uwagi końcowe:

- montaż, uruchomienie oraz stały serwis (nadzór) nad systemami sygnalizacji włamania należy zlecić jednostce (firmie) posiadającej odpowiednie uprawnienia i certyfikaty.
- przed rozpoczęciem instalacji oraz uruchomieniem systemu należy zapoznać się z instrukcjami montażu dostarczonymi przez producenta wraz z urządzeniami. Podczas montażu i programowania urządzeń należy bezwzględnie przestrzegać zaleceń producenta,
- wszystkie roboty objęte niniejszym projektem należy wykonać zgodnie z obowiązującymi normami, przepisami i warunkami na roboty teletechniczne,
- przy pracach wykonawczych należy bezwzględnie przestrzegać przepisów BHP,
- przed rozpoczęciem instalacji oraz uruchomieniem systemu należy zapoznać się z instrukcjami montażu dostarczonymi przez producenta wraz z urządzeniami. Podczas montażu i programowania urządzeń należy bezwzględnie przestrzegać zaleceń producenta,
- do wykonania instalacji wg niniejszego opracowania należy użyć materiałów wymienionych w zestawieniu poniżej lub równoważnych o nie gorszych parametrach technicznych,
- wszystkie zmiany wprowadzone na budowie w trakcie realizacji należy uzgodnić z projektantem i Inwestorem.
- po wykonaniu instalacji należy opracować dokumentację powykonawczą.

7. Zintegrowany System Zarządzania Bezpieczeństwem

Wszystkie systemy bezpieczeństwa zainstalowane w obrębie budynku Centrum Symulacji Medycznej w Sanoku muszą być w pełni monitorowane i zarządzane z poziomu centralnej platformy Systemu Zarządzania Bezpieczeństwem (SMS). Do najważniejszych funkcjonalności realizowanych przez platformę SMS można zaliczyć:

- zarządzanie elementami sprzętowymi i logicznymi poszczególnych podsystemów;
- konfiguracja parametrów urządzeń wchodzących w skład poszczególnych podsystemów;
- pełna wizualizacji stanu elementów sprzętowych i logicznymi poszczególnych podsystemów;
- korelacja zdarzeń występujących w kilku podsystemach w oparciu o funkcje logiczne;
- jedna baza danych użytkowników i zdarzeń dla wszystkich podsystemów.

Projektowany system bezpieczeństwa CSM opracowany został w celu zapewnienia bezpieczeństwa osób i mienia znajdujących się na terenie obiektu oraz terenu zewnętrznego wokół obiektu.

Podstawą poniższego opracowania są:

- Wytczne inwestora w zakresie aranżacji i wykorzystania poszczególnych

- pomieszczeń;
- Podkłady budowlane oraz architektura budynku;
- Ogólne założenia wynikające z odpowiednich norm i przepisów:
 - PN-EN 50131 – w zakresie Systemów Sygnalizacji Włamania i Napadu;
 - PN-EN 50133 – w zakresie Kontroli Dostępu;
 - PN-EN 50136 – w zakresie Dystrybucji Alarmów;
 - PN-EN 50132 – w zakresie Systemów Telewizji Dozorowej.

Platforma zarządzania SMS musi umożliwiać wzajemne współdziałanie poniższych podsystemów za pomocą interfejsów programowych:

- Kontroli Dostępu,
- Sygnalizacji Włamania i Napadu,
- Monitoringu Wizyjnego CCTV IP,
- Interkomowego.

Dodatkowo system SMS integrować systemy zewnętrzne m.in.:

- System OPTICAMP obecny na PWSZ w Sanoku,

Każda z funkcjonalności musi być dostępna zarówno na etapie projektu i wdrażania, jak i ewentualnej rozbudowy działającego systemu. Dodatkowo każdą z funkcjonalności oraz każdy z modułów będzie można płynnie rozbudowywać w przyszłości.

System Zarządzania Bezpieczeństwem (SMS) powinien być oparty na strukturze sieci IP z centralnym serwerem SMS oraz rozproszoną strukturą elementów sterujących, wykorzystującą standardowe łącza okablowania strukturalnego, zarówno miedzianego jak i światłowodowego. Taka konfiguracja daje możliwość łatwej i bezproblemowej rozbudowy, bez ingerencji w resztę pracującego systemu. Każdy sterownik musi posiadać możliwość nadzorowania prawidłowego działania za pomocą sieci LAN i musi działać w trybie Plug-Play, wymiana uszkodzonego kontrolera powoduje pobranie automatyczne konfiguracji z serwera.

Aplikacja kliencka SMS musi być oparta na technologii Web i umożliwiać dostęp użytkownikom do interfejsu systemu za pomocą przeglądarek internetowych Internet Explorer, Chrome lub Firefox z dowolnej stacji operatorskiej podłączonej do sieci bezpieczeństwa (lokalnie lub zdalnie, np. za pomocą wirtualnej sieci lokalnej VPN). Ze względu na kwestie bezpieczeństwa, dostęp nie może wymagać instalacji jakiegokolwiek oprogramowania lokalnie na stacji operatorskiej. Musi działać zarówno w środowisku Unix, jak i Windows bez żadnych ograniczeń funkcjonalnych.

Platforma SMS musi dać możliwość diagnostyki zdalnej (przez sieć Internet) i lokalnej przez komputer w sieci, lub komputer podłączony do sterownika z hiperterminalem. Informacja o błędach w komunikacji jest także odzwierciedlana diodami sygnalizacyjnymi umieszczonymi na sterowniku lokalnym.

Zastosowanie Systemu Zarządzania Bezpieczeństwem (SMS) ma skutkować znaczącym obniżeniem kosztów utrzymania i eksploatacji systemu bezpieczeństwa przez:

- Zautomatyzowanie procesu detekcji sytuacji alarmowej;
- Ograniczenie liczby kadry pracowniczej wewnętrznej lub zewnętrznej odpowiedzialnej za monitorowanie systemów bezpieczeństwa;
- Optymalizację procesu konfiguracji poszczególnych podsystemów przez administratora systemów;
- Ograniczenie kosztów ewentualnych działań serwisowych przez możliwość rekonfiguracji zdalnej;

Aby zabezpieczyć bezproblemowe działanie systemu, na wypadek braku komunikacji lub uszkodzenia serwera inteligencja musi zostać rozproszona do poziomu lokalnych sterowników. Sterowniki muszą być wyposażone w moduły pamięci pozwalające na buforowanie transakcji w przypadku braku komunikacji z serwerem centralnym. Dodatkowo muszą przechowywać informację na temat uprawnień poszczególnych użytkowników, dzięki czemu mogą sterować elementami wykonawczymi (np. czytnikami) całkowicie samodzielnie.

W momencie, gdy sterowniki ponownie otrzymają połączenie z serwerem, muszą zsynchronizować swoją bazę danych lokalną z serwerem centralnym (przesłanie buforowanych zdarzeń, aktualizacja uprawnień).

Dane przesyłane w systemach zabezpieczeń są kluczowe dla zachowania bezpieczeństwa. Z tego względu system SMS musi wykorzystywać najwyższej klasy protokoły kryptograficzne. Komunikacja między serwerem a stacją roboczą (stanowisko wizualizacji, punkt zdalnego zarządzania, terminal modyfikacji parametrów) musi się odbywać przez sieć TCP/IP z wykorzystaniem protokołu SSL, ze 128-bitowym kluczem.

Platforma SMS musi być skalowalna i umożliwiać realizacji rozbudowanych instalacji. Ze względu na to platforma SMS:

- musi umożliwiać dodanie co najmniej 150 000 użytkowników do systemu przypisanych do co najmniej 1024 grup użytkowników;
- musi pozwalać na zapisanie w systemie co najmniej 7 000 000 zdarzeń;
- musi umożliwiać dodanie co najmniej 3200 map synoptycznych oraz 32 000 obiektów;
- nie może ograniczać liczby stanowisk operatorskich.

Platforma SMS musi dawać możliwość kontroli zdarzeń, przez listę zdarzeń. Zdarzenia muszą mieć przypisany stopień priorytetyzacji oraz muszą być wyświetlane w kolorze wskazującym ich charakter (np. zdarzenia alarmowe – kolor czerwony). Lista zdarzeń może być filtrowana i w konsekwencji wyświetlane będą tylko zdarzenia określonego rodzaju. Pozwala to operatorowi wyświetlać wyłącznie wybrany typ zdarzeń. Platforma SMS musi mieć również możliwość zapisywania w systemie wszystkich ruchów wykonanych w systemie przez operatora w trakcie jego pracy na stacji operatorskiej,

Platforma SMS musi również umożliwiać definiowanie jakie rodzaje alarmu mają trafiać do konkretnego operatora, przykładowo pracownik ochrony ma otrzymywać zdarzenia alarmowe, pracownik administracyjny – zdarzenia związane z przemieszczaniem się pracowników, a administrator tylko zdarzenia techniczne związane z pracą urządzeń.

Dodatkowo można ustalać sekwencje zdarzeń dla różnych operatorów (np. jeden dozorca zajmuje się alarmami z jednej części budynku, a po odpowiednio długim czasie zwłoki może także obsługiwać alarmy przekierowane z innej części budynku, inny użytkownik otrzymuje alarmy wyłącznie techniczne).

System musi pozwalać na pisanie procedur programowych pozwalając na reagowanie w zależności od kilku zmiennych (algebra Boole'a dla co najmniej dwóch warunków). Działania mogą dotyczyć zdarzeń występujących w różnych podsystemach.

Platforma SMS musi umożliwiać pełne raportowanie i archiwizację danych. System musi mieć wbudowane predefiniowane raporty, m.in:

- Raport zdarzeń i częstotliwości występowania zdarzeń;
- Raport listy użytkowników z danymi osobowymi;
- Raport obecności dla danego użytkownika i dla danego obszaru;
- Raport praw dostępu dla użytkownika i czytelnika;
- Raport ścieżki użycia karty na obiekcie;
- Raport stanu sterowników i podłączonych do nich urządzeń;
- Raport stanu błędów występujących w systemie.

Dodatkowo system musi umożliwiać przygotowanie dowolnych raportów według wymogów użytkownika, przez definiowanie jaki typ danych ma znajdować się w konkretnej kolumnie raportu. System musi umożliwiać eksport raportów do plików PDF, XML, CSV.

W momencie wystąpienia zdarzenia alarmowego z każdego z podsystemów, platforma SMS musi wyświetlić dodatkowe okno alarmowe, zasłaniając jednocześnie wszystkie inne okna wyświetlone na stacji operatorskiej. System musi umożliwiać priorytetyzację alarmów i

przypisanie ich do jednej z 27 poziomów. Okno alarmów musi prezentować listę kroków, które operator musi wykonać. Każdy krok działania może mieć charakter informacyjny (np. „Zadzwoń na policję”), jak również aktywny, który zmienia stan urządzenia (np. otwarcie drzwi). Dodatkowo musi być prezentowana operatorowi mapa synoptyczna z zaznaczonym elementem systemu, który wywołał alarm. Jeżeli do danego elementu systemu jest przyporządkowana kamera, automatycznie musi być prezentowany również obraz z danej kamery.

Zarządzanie uprawnieniami i personalizacja stanowiska pracy musi być przypisywana poszczególnym profilom użytkownika. Musi istnieć możliwość przypisywania dostępu do poszczególnych modułów poszczególnym operatorom w zależności od ich uprawnień. Po wprowadzeniu zmian konfiguracyjnych system nie może wymagać resetowania poszczególnych jednostek, wystarczające jest zapisanie zmian na serwerze głównym.

Kluczowy z punktu widzenia bezpieczeństwa i samej obsługi systemu jest interfejs użytkownika. Platforma musi oferować czytelny i intuicyjny interfejs użytkownika GUI znany wszystkim użytkownikom Internetu i Eksploratora Windows. W ustawieniach parametrów systemowych, każdy moduł obsługi poszczególnych systemów (kontroli dostępu, SSWiN itp.) musi mieć odmienny kolor tła, co podpowiada jednoznacznie użytkownikowi, w której części menu się znajduje.

System musi umożliwiać przypisanie w bazie danych do użytkownika następujących danych:

- imienia i nazwiska
- numeru karty dostępowej
- sklasyfikowania do grupy użytkowników – np. pracownik, serwisant, gość, dział kadr,
- bloku parkingowego
- samochodu
- numerów rejestracyjnych pojazdu
- telefonu
- adresu

Dodatkowo istnieje możliwość zdefiniowania dowolnych pól dodatkowych, których wymaga inwestor.

Każdy z użytkowników po zalogowaniu się do systemu może korzystać z okienek w wybranym języku: holenderski, niemiecki, angielski, polski, rosyjski. Interfejs językowy przypisany jest do użytkownika, a nie do urządzenia. Hasło dostępowe do systemu ma składać się przynajmniej z 6 znaków, z których przynajmniej jeden to cyfra a inny to wielka litera.

System musi mieć wbudowaną mapę synoptyczną (wizualizację) za pomocą, której będzie istnieć możliwość pełnej wizualizacji stanu i zarządzania wszystkimi podsystemami. Funkcje, które muszą być realizowane przez system wizualizacji:

- System Kontroli dostępu – wizualizacja stanów czytnika, kontaktronu, elektrorygla i wszystkich elementów dodatkowych. Po kliknięciu ikony czytnika powinna zostać wyjustowana lista wyboru trybów pracy czytnika (m.in. stan otwarty, stan normalny, stan z potwierdzeniem operatora).
- System Sygnalizacji Włamania i Napadu – wizualizacja stanów poszczególnych elementów detekcyjnych (np. czujek ruchu PIR). Zazbrajanie i rozbrajanie poszczególnych stref SSWiN.
- System Monitoringu wizyjnego – kliknięcie ikony kamery ma spowodować wyświetlenie obrazu z danej kamery. Dla kamer PTZ, pełna możliwość sterowania kamerą z poziomu mapy synoptycznej. Możliwość umiejscowienia na mapie synoptycznej przycisków, wymuszających obrót kamery PTZ w konkretne miejsce.
- System Interkomowy – kliknięcie ikony interkomu ma skutkować wywołaniem połączenia z danym interkomem oraz prezentację obrazu z kamery skierowanej na interkom.

- System OPTICamp – synchronizacja danych między OPTIcamp-em a SKD opierać się będzie o replikę bazy danych OPTIcamp. Replika bazy danych zostanie udostępniona przez Zamawiającego

Dodatkowo mapa synoptyczna musi wspierać system widgetów, który umożliwia umieszczenie na niej dowolnych elementów, m.in.:

- Listę osób znajdujących się w danym pomieszczeniu (przy kontroli dwustronnej);
- Wykresy zawierające liczby osób przechodzących przez dane przejście;
- Listę stref SSWiN z informacją o ich stanie, umożliwiającą zazbrajanie i rozbrajanie poszczególnych stref;
- Skrót do konkretnych pozycji w menu, szczególnie często używanych przez operatora;
- Listę urządzeń z informacją o ich stanie połączenia z serwerem.

Kliknięcie każdej z ikon urządzenia prawym przyciskiem myszy, ma spowodować wyświetlanie wszystkich zdarzeń związanych z danym urządzeniem. Umożliwia to szybkie odwołanie do zdarzeń w obrębie każdego z systemów. Dodatkowo musi istnieć możliwość umiejscowienia bezpośrednio na mapie synoptycznej odnośnika do innej mapy synoptycznej (innego piętra budynku).

Platforma SMS musi umożliwiać realizację następujących funkcjonalności międzystemowych:

1. Podsystemy SSWiN i Kontroli dostępu:

- Zarządzanie systemami kontroli dostępu i SSWiN z poziomu jednego urządzenia – czytnika kontroli dostępu (m.in. zazbrajanie i rozbrajanie stref SSWiN).
- Wykorzystanie automatycznych funkcji zliczania osób wchodzących i wychodzących w obrębie stref kontroli dostępu po których strefa SSWiN zmieni swój stan oraz wykorzystanie zazbrajania czasowego;

2. Podsystem monitoringu wizyjnego:

- Wywołanie okna widoku kamery CCTV w sytuacjach alarmowych wywołanych przez system KD lub SSWiN (obraz wideo wspiera procesy decyzyjne w systemie) w platformie SMS.
- Rozpoczęcie zapisu materiału wideo z kamer systemu CCTV, w momencie wystąpienia określonych zdarzeń w pozostałych systemach (KD, SSWiN, Interkomowym). Zapisany materiał jest przypisany do konkretnego zdarzenia.
- Integrację funkcji analitycznych rozpoznawania numerów rejestracyjnych aut realizowaną przez system CCTV, czy rozpoznawania twarzy z systemem kontroli dostępu. Numer rejestracyjny lub wzór twarzy pełni rolę karty dostępowej w systemie kontroli dostępu.
- Przesłanie informacji o przekroczeniu wirtualnej linii i detekcji ruchu do systemu SMS oraz rozpoczęcie określonej procedury alarmowej.
- Prezentację bezpośrednio na mapie synoptycznej obrazu z kamer. Dodatkowo możliwość wysterowania kamer PTZ oraz realizację „Presetu” bezpośrednio z mapy synoptycznej.

3. Podsystem interkomowy:

- Interkomy podłączony do lokalnej centrali telefonicznej uczelni.
- Wyświetlenie kamery skierowanej na szlaban, przy którym będzie zamontowany interkom wywoławczy
- Funkcjonalność centrali telefonicznej

4. Podsystem Sygnalizacji pożarowej

- Przesyłanie informacji o zdarzeniach alarmowych z centrali SSP do systemu SMS i rozróżnienie rodzaju alarmu, np. alarm pożarowy czujki, alarm pożarowy strefy, alarm tampera, brak połączenia między centralą a serwerem itp.

- definiowanie dowolnych procedur działania alarmowego w platformie SMS i kroków, które operator systemu musi wykonać (np. wywołanie komunikatu z systemu interkomowego itp.).
- wizualizacja na mapie synoptycznej stanu poszczególnych detektorów i/lub stref SSP; prezentacja stanu stref może być przedstawiona jako dynamiczna ikona umieszczona w danym pomieszczeniu lub jako pozycja w tabeli na dedykowanej mapie synoptycznej.

5. Podsystem OptiCamp

Synchronizacja danych między OPTIcamp-em a SKD opierać się będzie o replikę bazy danych OPTIcamp. Replika bazy danych zostanie udostępniona przez Zamawiającego. Konto użytkownika dostępowego do repliki bazy OPTIcamp, będzie w trybie tylko do odczytu.

Dodatkowo platforma SMS musi mieć możliwość integracji innych zewnętrznych systemów w oparciu o protokoły JDBC, XML SQL, LDAP.

Komunikacja między serwerem centralnym a sterownikiem kontroli dostępu musi się odbywać w oparciu o protokół TCP/IP. Przesyłane dane muszą być szyfrowane za pomocą standardu AES-CBC (256 bit). Dla każdej sesji musi być generowany nowy klucz, aby zapobiec powtórzeniu kluczy. Klucze muszą być zapisane w pliku XML, który musi być zabezpieczony za pomocą szyfrowania AES-256. Aby zapewnić bezproblemową transmisję danych każda wiadomość przesyłana między serwerem a kontrolerem musi być poprzedzona 8-bajtowym nagłówkiem. Nagłówek musi zawierać 32 bitowe pole flag oraz 32 bitowe pole CRC, wykorzystywane do weryfikowania poprawności danych.

Komunikacja między serwerem centralnym a serwerem interkomowym musi się odbywać w oparciu o protokół komunikacji interkomowej ICX over IP/RS-232 lub analogiczny oferujący co najmniej taki zakres funkcjonalności integracyjnych. Wymagane jest połączenie logiczne serwera centralnego i serwera interkomowego w sieci TCP/IP.

Komunikacja między serwerem centralnym a serwerem monitoringu wizyjnego CCTV IP musi się odbywać w oparciu o protokół komunikacji HTTP over IP. Wymagane jest połączenie logiczne serwera centralnego i serwera CCTV w sieci TCP/IP.

Komunikacja między serwerem centralnym a centralą SSWiN musi się odbywać przez sterownik sieciowy (wymagane tylko połączenie logiczne). Komunikacja odbywa się w oparciu o protokół TCP/IP.

System musi być zaimplementowany w systemie wirtualizacyjnym min. Vmware. Cecha ta zapewnia możliwość wykorzystania infrastruktury serwerowej przy optymalizacji kosztowej wdrażanie systemu bezpieczeństwa oraz wykorzystanie dodatkowych oferowanych przez środowisko wirtualizacyjnej funkcjonalności jak min. łatwa przywracanie systemów po awarii czy dynamiczna lustrzana kopia danych.

System ma być oparty o środowisko UNIX. System musi instalować tylko ten fragment jądra UNIX, który jest wymagany do realizacji zadań SMS, aby zminimalizować ryzyko włamania się do systemu użytkowników zewnętrznych.

Elementami wykonawczymi platformy SMS muszą być inteligentne sterowniki sieciowe pozwalające na podłączenie elementów wykonawczych systemu Kontroli Dostępu, SSWiN.

System Kontroli dostępu

W Centrum Symulacji Medycznej PWSZ, w wybranych grupach pomieszczeń przewiduje się wykonanie instalacji systemu kontroli dostępu (KD). System KD musi posiadać certyfikat zgodności z normą PN-EN 50133-1: 2007 dla klasy dostępu B i klasy rozpoznania 3.

Głównym zadaniem systemu kontroli dostępu jest zarządzanie kontrolą dostępu do poszczególnych obszarów zlokalizowanych na terenie obiektu. System KD ma uniemożliwić wejście do konkretnej strefy KD osobom nieuprawnionym. System KD musi mieć możliwość definiowania harmonogramu terminowego dostępu do stref KD dla poszczególnych użytkowników lub grup użytkowników. Harmonogramy muszą mieć możliwość działania w

pętli. Dodatkowo system KD musi umożliwiać definiowania harmonogramów czasowych definiujących prawa dostępu w konkretnym dniu z dokładnością do jednej minuty.

System kontroli dostępu musi mieć możliwość podłączenia czytników w oparciu o dwie architektury. W pierwszej architekturze - gwiazdy, serwer musi komunikować się z dedykowanymi sterownikami sieciowymi przez sieć TCP/IP. Każdy ze sterowników musi obsługiwać co najmniej 4 kontrolery drzwiowe, a każdy kontroler drzwiowy co najmniej 2 czytniki. Sumarycznie w architekturze gwiazdy, sterownik musi obsługiwać co najmniej 8 czytników.

W drugiej architekturze – magistralowej, sterownik sieciowy musi komunikować się z serwerem przez sieć TCP/IP i posiadać możliwość rozbudowy o co najmniej 4 interfejsy magistral RS-485. Do każdej magistrali musi istnieć możliwość podłączenia co najmniej 8 kontrolerów drzwiowych. Sumarycznie w architekturze magistrali, sterownik musi obsługiwać co najmniej 32 czytniki podłączone do kontrolerów drzwiowych.

Powyższe architektury można używać w jednym systemie. We wszystkich przypadkach czytnik kontroli dostępu komunikuje się w czasie rzeczywistym z serwerem zarządzającym, dzięki czemu ewentualne zmiany wprowadzone w systemie (np. uprawnień) są bez opóźnień realizowane na obiekcie.

System KD musi umożliwiać podłączenie szerokiego zakresu czytników kontroli dostępu.

System kontroli dostępu musi mieć możliwość komunikacji z czytnikiem za pomocą protokołów Wiegand, Clock&Data lub RS-422 w zależności od stosowanego sterownika.

System będzie obsługiwać czytniki wspierające technologię zbliżeniowych, m.in. krótkiego zasięgu Mifare – karty z pamięcią 4K, jak i dalekiego zasięgu – HyperX, czy UHF.

Dodatkowo system musi mieć możliwość podłączenia czytników kart z klawiaturą numeryczną oraz czytników biometrycznych linii papilarnych. Wymagane jest, aby wszystkie informacje na temat wzorców linii papilarnych były przechowywane na karcie dostępu, a nie w centralnej bazie systemu zabezpieczeń ze względu na ochronę danych osobowych. Wzorce biometryczne muszą być zbiorem wybranych punktów charakterystycznych, a nie całościowym obrazem analizowanej cechy, aby nie było możliwości odtworzenia oryginalnego obrazu cechy.

System KD musi mieć również możliwość obsługi gości. System musi umożliwiać dodanie przez użytkowników do systemu informacji o przyjeździe gościa, którą otrzymuje operator systemu. Dodatkowo musi być możliwość przypisania do danej osoby numeru rejestracyjnego samochodu. Operator musi mieć możliwość przygotowania dla gościa specjalnej, spersonalizowanej karty z tymczasowymi prawami dostępu do wyznaczonych pomieszczeń, gdzie mają miejsce spotkania.

System KD musi zabezpieczać przed niewłaściwym użyciem karty przez użytkowników oraz sygnalizować sytuacje alarmowe. W tym celu musi realizować poniższe funkcjonalności:

- Funkcję globalnego Anti-Pass Back z podziałem na strefy (wsparcie dla Anti-Pass Back globalnie, punktowo, czasowo, rewersyjnie).
- Funkcję służowości obsługującą do 16 wejść.
- Funkcję unieważniania kart zbyt długo nie używanych zabezpieczającą przed użyciem zagubionej karty, np. karta nie użyta na jednym z czytników w ciągu 24 godzin traci swoje prawa dostępowe.
- Funkcję kwarantanny, która zabrania użytkownikom wejście do określonych stref, jeżeli wcześniej znajdowali się w innej, ściśle zdefiniowanej strefie.
- Funkcję nadawania praw użytkownikom, w momencie gdy znajdowali się w innej strefie, np. karta jest ważna na terenie magazynu, tylko w momencie gdy wcześniej została użyta w portierni.
- Element ryglujący musi dokonywać zaryglowania przejścia niezwłocznie po zamknięciu drzwi przez osobę wchodzącą do pomieszczenia (element ryglujący nie czeka, aż skończy się czas odryglowania ustawiony w systemie).

- Funkcję wzbudzenia alarmu w momencie gdy drzwi na zbyt długi czas pozostają otwarte.
- Funkcję wejścia pod przymusem polegającą na zapisaniu dla danego użytkownika dwóch haseł pin. W momencie gdy dany użytkownik wchodzi pod przymusem do strefy, przykładą kartę i wpisuje hasło dedykowane dla wejścia pod przymusem. Uzyskuje on dostęp do danej strefy, jednocześnie operator zostaje powiadomiony o fakcie wejścia pod przymusem.
- Funkcję rozbudowanych alarmów kontroli dostępu, w których alarm jest wzbudzony w momencie gdy karta zostaje uznana jako skradziona, lub użytkownik przyłoży do kartę do czytnika do którego nie ma uprawnień.

System musi umożliwiać zmianę stanu przejścia. W systemie muszą być wyróżnione następujące tryby pracy przejścia kontroli dostępu:

- Otwarte – element ryglujący jest nieaktywny;
- Normalny – kontrola dostępu zgodna z harmonogramem i uprawnieniami użytkowników;
- Zablokowany – element ryglujący zaryglowany, czytnik zablokowany i nie odczytuje kart dostępowych;
- Z potwierdzeniem – W momencie gdy użytkownik przykładą kartę dostępową operatorowi prezentowane jest okno w którym widoczne jest zdjęcie właściciela karty z bazy systemowej oraz obraz z kamery (w przypadku integracji systemu CCTV). Operator potwierdza czy dana osoba może wejść do danej strefy kontroli dostępu.

Uprawniony operator musi mieć możliwość zmiany w czasie rzeczywistym trybu pracy danego czytnika kontroli dostępu z poziomu mapy synoptycznej. System musi dodatkowo mieć możliwość zmiany trybu pracy czytnika w zależności od stanu systemu (stan systemu normalny, alarmowy itp.).

System kontroli dostępu powinien być również dostosowany do obsługi przez osoby niepełnosprawne, przez wydłużenie czasu zwolnienia elementu ryglującego w momencie przyłożenia karty przez osobę niepełnosprawną. Dzięki temu osoba niepełnosprawna może bez problemów przemieszczać się po obiekcie.

Opis kluczowych elementów systemu Kontroli dostępu

Sterownik sieciowy

Elementami wykonawczymi systemu kontroli dostępu muszą być inteligentne sterowniki sieciowe pozwalające na podłączenie kontrolerów drzwiowych. Sterownik musi komunikować się z serwerem za pomocą standardu TCP/IP. W przypadku zerwania łączności kontrolera sieciowego z serwerem, musi on nadal zarządzać elementami do niego podłączonymi. Dodatkowo musi zarejestrować w pamięci, co najmniej 5000 zdarzeń. Po ponownym podłączeniu go do serwera musi nastąpić automatyczna, wzajemna synchronizacja.

Sterownik sieciowy musi umożliwiać bezpośrednie podłączenie 4 kontrolerów drzwiowych w obrębie 1 wspólnej obudowy. Do każdego z podłączonych w ten sposób kontrolerów drzwiowych można podłączyć bezpośrednio czytniki oraz / lub wyprowadzić maksymalnie 4 magistrale RS485 do podłączenia kolejnych, w sumie 32 kontrolerów drzwiowych. Jeden sterownik sieciowy musi obsłużyć do 32 czytników kontroli dostępu za pomocą podłączonych kontrolerów drzwiowych.

Sterownik sieciowy musi umożliwiać podłączenie kontrolerów drzwiowych w gwiazdę, lub magistralę oraz użycie interfejsów RS232, RS485, Clock/Data, Wiegand. Rozwiązanie musi zapewnić najwyższy poziom bezpieczeństwa poprzez możliwość szyfrowania od karty do serwera metodą AES.

Sterownik sieciowy powinien spełniać poniższe wymagania:

- Szyfrowana komunikacja AES256 między sterownikiem sieciowym a serwerem SMS

- Stabilny system operacyjny LINUX
- Montaż na szynę DIN 35 mm
- Niski pobór mocy (średnio 2.5W)
- Zasilanie 12 – 24 V DC
- Możliwość podłączenie do 4 kontrolerów drzwiowych w trybie End To End Security (szyfrowanie od karty do serwera)
- Obsługa wielu interfejsów i topologii: Wiegand, RS232, RS485, Clock/Data, TCP/IP, gwiazda i magistrala
- Temperatura pracy od -10 do + 60°C
- Złącza SD(SDHC), SAM (opcja), USB
- Ethernet Gigabit RJ-45

Kontroler drzwiowy

Kluczowym urządzeniem wykonawczym systemu kontroli dostępu musi być kontroler drzwiowy odpowiedzialny za zabezpieczenie dwóch przejść pojedynczych lub jednego przejścia podwójnego.

W zależności od charakterystyki poszczególnych obiektów, kontroler drzwiowy musi działać zarówno w topologii gwiazdy, jak i magistrali w zależności od stosowanego typu sterownika sieciowego. Musi istnieć możliwość stosowania obu topologii jednocześnie w ramach pojedynczej instalacji, dzięki czemu istnieje możliwość dostosowania sposobu instalacji do wymogów poszczególnych pomieszczeń. Elastyczność topologii umożliwia również wykorzystanie dotychczasowego okablowania zainstalowanego już na obiekcie.

Kontroler musi obsługiwać 2 czytniki kontroli dostępu i komunikować się z nimi za pomocą protokołów Clock/Data / Wiegand. W zależności od typu architektury kontroler musi oferować 8 wejść i 4 wyjścia (gwiazda) lub 8 wejść i 8 wyjść (magistrala) do podłączenia elementów wykonawczych (kontaktronów, zwór, elektrozaczepów, przycisków wyjścia, czy przycisków ewakuacyjnych).

Kontroler musi być wyposażony w specjalny system monitorowania stanu kontrolera (autotest), umożliwiający ciągły pomiar m.in.: wewnętrznej temperatury, parametrów zasilania kontrolera i czytników oraz stanu komunikacji z czytnikami. Stan urządzenia powinien być sygnalizowany wielokolorową diodą oraz przesyłany do oprogramowania zarządzającego w czasie rzeczywistym.

Sterownik drzwiowy powinien spełniać poniższe wymagania:

- Praca w architekturze gwiazdy lub magistrali
- Obsługa 2 czytników kontroli dostępu
- Wbudowany moduł Wejść / Wyjść – 6 wejść / 8 wyjść
- Obsługa 2 mierników temperatury / wilgotności
- Funkcja „Autotestu”
- Wysoka gęstość instalacji (montaż DIN)
- Wyjście cyfrowe 6 x - max. 28V; OC; Max. natężenie 300mA
- Wyjście mocowe 2; max. 2.5A
- Wejścia cyfrowe 6
- Temperatura / Wilgotność pracy -35°C do +70°C / 20 ~ 90% nieskondensowana
- Napięcie 12,0 – 24V DC
- Moc 0,48 W (Średnia)

Czytniki kontroli dostępu

W ramach infrastruktury systemu kontroli dostępu na obiekcie muszą zostać zainstalowane czytniki oraz karty w standardzie zbliżeniowym Mifare sektorowe karty kontroli dostępu.

Wykorzystywane w kartach chipy, 32 sektory pamięci, w zależności od stosowanego rodzaju karty (1K lub 4K). Pierwszy sektor jest wykorzystywany do zapisu informacji charakterystycznej dla danej karty (m.in. numer seryjny). Pozostałe sektory mogą być dowolnie wykorzystywane. Karty są w pełni zgodne ze standardem ISO 7810–Transpondery

typ transmisji ISO/IEC 14443A-3 / Mifare / Zbliżeniowa Częstotliwość pracy 13.56 MHz Karta z pamięcią 4K 4096 x 8 bit EEPROM. 3456 bajtów podzielonych na 32 sektory po 4 bloki i 8 sektorów po 16 bloków.

Czytniki powinny być dostępne w wersji natynkowej i podtynkowej. W przypadku wersji podtynkowej ich rozmiar musi umożliwić montaż w standardowej puszcze dostosowanej do montażu gniazd elektrycznych.

Czytniki kontroli dostępu muszą mieć możliwość odczytu szerokiego spektrum technologii zbliżeniowych: Mifare 1K, Mifare 4K, Mifare DESFire, Mifare DESFire EV1. Dodatkowo muszą mieć możliwość komunikacji za pomocą różnych protokołów transmisyjnych: Wiegand, Clock / Data, RS-485.

Czytnik musi być wyposażony w czujnik ruchu, który wzbudzi czytnik w stan odczytu karty tylko w momencie, gdy zbliżona zostanie do niego karta dostępową. Dzięki temu możliwa jest znaczna redukcja zużycia energii.

Czytnik musi być wyposażony w wielotonowy brzęczyk, który realizuje sygnalizację dźwiękową o różnych tonach w zależności od rodzaju reakcji czytnika (przejście otwarte, brak dostępu itp.). Jest to funkcjonalność szczególnie pomocna dla osób niewidomych. Czytnik musi być również wyposażony w diodę sygnalizacyjną, mogącą wyświetlić 4096 kolorów w zależności od stanu i reakcji czytnika.

Wszystkie elementy elektroniczne znajdujące się wewnątrz obudowy czytnika muszą być zalewane żywicą epoksydową. Dzięki temu czytniki są odporne na niekorzystne warunki atmosferyczne. Czytniki muszą posiadać normę szczelności IP64.

Czytnik z klawiaturą PIN, musi być wyposażony w klawiaturę pojemnościową i nie posiadać przycisków ruchomych. Dodatkowo musi być wyposażony w mechanizm autokalibracji, który dostosowuje czułość klawiatury w zależności od warunków temperaturowych.

System Sygnalizacji Włamania i Napadu

Zakłada się instalację sygnalizacji włamania oraz instalację sygnalizacji napadu obejmującą wybrane pomieszczenia Centrum Symulacji Medycznej.

Instalacje te mają za zadanie ochronę wybranych pomieszczeń przed włamaniem lub wejściem niepożądanych osób oraz zapewnić bezpieczeństwo obsługi w przypadku napadu.

Ochrona pomieszczeń przed włamaniem będzie realizowana poprzez zastosowanie detektorów:

- kontaktronów magnetycznych w oknach i drzwiach w pomieszczeniach;
- czujek ruchu dualnych pasywnych podczerwieni i mikrofalowych w pomieszczeniach;
- czujek ruchu dualnych pasywnych podczerwieni i mikrofalowych z funkcją antymaskingu w pomieszczeniach;

Ochrona przed napadem będzie realizowana w oparciu o:

- ręczne przyciski napadowe przewodowe ;

Odpowiednie rozmieszczenie czujek zapewni wytworzenie stref ochronnych, które obejmują pomieszczenia określone przez Inwestora.

Zarządzanie systemem SSWiN musi być możliwe z poziomu:

- Mapy synoptycznej – zazbrajanie i rozbrajanie poszczególnych stref SSWiN oraz wizualizacja stanów poszczególnych stref i elementów detekcyjnych nawet w momencie gdy strefa nie jest zazbrojona.
- Czytnika kontroli dostępu – automatyczne zazbrajanie i rozbrajanie poszczególnych stref SSWiN po przyłożeniu uprawnionej karty dostępowej lub w momencie gdy wszystkie osoby wyjdą z pomieszczenia (realizowane w oparciu o czytniki kontroli dostępu). Wizualizacja stanu strefy SSWiN na diodzie czytnika kontroli dostępu.
- Manipulatora SSWiN – zazbrajanie i rozbrajanie po wpisaniu kodu autoryzacyjnego. Wizualizacja stanów poszczególnych stref. Konfiguracja systemu zgodnie z uprawnieniami.
- Aplikacji mobilnej – zazbrajanie i rozbrajanie po wpisaniu kodu autoryzacyjnego. Wizualizacja stanów poszczególnych stref. Konfiguracja systemu zgodnie z

uprawnieniami.

Centralnym punktem systemu jest centrala alarmowa. Centrala alarmowa musi mieć wbudowany na płycie głównej centrali interfejs TCP/IP. Centrala musi być w pełni skalowalna i domyślnie oferować jedną magistralę transmisyjną. W obrębie samej centrali musi być wbudowany moduł obsługi 16 linii dozorowych, 1 wyjścia przekaźnikowego i 4 wyjść OC. Pozostałe linie dozorowe powinny być podłączane do ekspanderów linii dozorowych, dołączonych do magistrali (maksymalnie 120 linii dozorowych na magistralę). Dodatkowo centrala musi umożliwiać rozbudowę o jedną lub cztery dodatkowe magistrale transmisyjne za pomocą dedykowanej płyty rozszerzeń magistral (instalowanej bezpośrednio na płycie głównej centrali). Pojedyncza centrala musi obsługiwać maksymalnie do 616 linii dozorowych. Centrala musi oferować możliwość podłączenia do każdej magistrali co najmniej 15 ekspanderów przewodowych lub bezprzewodowych, każdy wyposażony w 8 linii dozorowych. Do każdej centrali musi być możliwość podłączenia maksymalnie 40 klawiatur kodowych (manipulatorów) do zarządzania strefami.

Centrala SSWiN musi być zgodna z wymogami norm PN-EN 50131 dla systemu stopnia 3. Zgodność musi być potwierdzona certyfikatem akredytowanej europejskiej jednostki certyfikacyjnej oraz polskiego Zakładu certyfikacyjnego TECHOM. System SSWiN musi dawać możliwość rozbudowy systemu w przyszłości o kolejne centrale SSWiN oraz sieciowanie ich za pomocą interfejsu SMS.

Wymagane dodatkowe parametry centrali:

- Komunikacja:
 - dialer IP zintegrowany na płycie głównej centrali,
 - możliwość podłączenia dialera PSTN
 - możliwość podłączenia dialera GPRS
- Czujnik antysabotażowy
- Klasa (Grade): 3
- Kody użytkownika: 500 (9 poziomów)

Poniżej przedstawiono wymagania odnośnie kluczowych parametrów ekspanderów linii i manipulatora kontrolnego:

Ekspander 8 linii z zasilaczem

Moduł rozszerzenia centrali alarmowej umożliwiający podłączenie detektorów.

- Wejścia: 8x NO, NC, EOL, DEOL; 3x antysabotaż
- 9 wyjść:
 - 2 przekaźnikowe,
 - 6 OC (max 100mA),
 - 1 głośnikowe (8 om).
- Komunikacja: RS485.

Manipulator kontrolny

Służący do zazbrajania i rozbrajania stref SSWiN oraz

- Wymiary: 164 x 124 x 28 mm
- Napięcie: 12 VDC
- Temp./ Wilgotność: 0°C do +50°C, do 90% bez kondensacji
- Komunikacja: RS485
- Inne cechy: buczek, wyświetlacz LCD 2x16 znaków
- 8 diod LED sygnalizujących stan systemu

System inteligentnej platformy telewizji przemysłowej CCTV IP

System będzie oparty na technologii IP. Obraz z kamer będzie nagrywany przez serwery wideo. Obrazy z kamer będą obserwowane na dedykowanych stacjach operatorskich.

System będzie składał się z:

- 4 kamer zewnętrznych typu bullet 4MPX 2,8-12mm z motozoomem wyposażonych w obudowy z grzałką, promiennikiem
- 2 kamer zewnętrznych typu bullet 4MPX 2,8-12mm z motozoomem wyposażonych w obudowy z grzałką, promiennikiem na szlabanach bramy głównej
- 5 kamer zewnętrznych 4-obiektywowych x 5MPX 3,3-6,6 mm z motozoomem
- 7 kamer wewnętrznych kopułkowych 2,8-12mm z funkcją hallway view WDR 120dB
- 6 kamer 2-obiektywowe 2x2MPX, obiektyw 2,8-12mm z funkcją hallway view
- 2 kamery 360stopni 12MPX
- 1 Vmware server
- 1 stanowisko operatorskie (wspólnych dla platformy SMS) wyposażone w 2 monitory 32calowe.

System zbudowany musi być w architekturze klient- serwer w z zastosowaniem architektury rozproszonej serwerów z zasilaczami redundantnymi oraz macierzami DAS pracująca w trybie RAID 5 lub 6. Architektura taka minimalizuje ryzyko utraty rejestrowanych danych w przeciwieństwie do architektury z centralną macierzą rejestrującą

Aplikacja serwerowa platformy musi wspierać architekturę 64-bitową w celu zapewnianie maksymalizacji wykorzystanie zasobów serwerów np. zapewnić obsługę min. 200 kamer w rozdzielczości FullD w trybie zapisu ruchu na jednej jednostce serwerowej.

Platforma musi zapewnić obsługę kamer min 30 producentów. W przypadku braku wspierania dedykowanego protokołu dopuszcza się możliwość stosowanie protokołów generycznych takich jak Onvif oraz PSIA w celu połączenia urządzenia z platformą.

Wymagane jest obsługiwane wbudowanych w kamerę algorytmów badania, jakości obrazu kamery w celu ułatwienia zarządzanie wielokamerowymi poprzez automatyczne poinformowanie operatora, administratora o utracie jakości obrazu.

Serwer systemu CCTV musi zapewniać możliwość obsługi do 500 urządzeń w tym kamer , kanałów video z koderów video.

System musi być zaimplementowany w systemie wirtualizacyjnym min. Vmware. Cecha ta zapewnia możliwość wykorzystania infrastruktury serwerowej przy optymalizacji kosztowej wdrażanie systemu bezpieczeństwa oraz wykorzystanie dodatkowych oferowanych przez środowisko wirtualizacyjnej funkcjonalności jak min . łatwa przywracanie systemów po awarii czy dynamiczna lustrzana kopia danych.

System musi gwarantować najwyższy poziom bezpieczeństwa danych w warstwie sprzętowej serwera, usługi systemu operacyjnego, aplikacyjnej – przez możliwość wdrożenia w systemie serwera redundantnego, detekcję sabotażu punktu kamerowego, watchdog aplikacji oraz redundancję sprzętową.

W przypadku wykrycia nieprawidłowości usługa serwerowa jest restartowana w celu uniknięcia błędnego funkcjonowania części platformy w dłuższym czasie, co mogłoby spowodować brak możliwości nagrywania w przypadku serwerów rejestrujących lub braku możliwości podglądu obrazów na żywo, interaktywnej obsługi systemu w przypadku stacji operatorskich.

Anty-sabotaż punktu kamerowego - dla każdego punktu kamerowego możliwe będzie, bez konieczności wykupu dodatkowej licencji, detekcja sabotażu punktu kamerowego dokonywana przez serwer. Funkcje analizy obrazu są wspomagane ciągłym monitorowaniem zakresu obserwowanej przez kamerę sceny. W przypadku zmiany kąta obserwacji, zakrycia obiektywu, lub rozmycia obrazu system automatycznie informuje o tym fakcie operatora, co

gwarantuje poprawne działanie poszczególnych algorytmów wideo identyfikacji oraz wideo detekcji.

Serwer platformy CCTV zapewniać musi zabezpieczenie struktury danych video, audio oraz metadanych poprzez zastosowanie technologii RAID 6 w przypisanej do serwera macierzy dyskowej. W celu zapewnienia ciągłości pracy w przypadku uszkodzenia dysku twardego serwer ma zapewniać możliwość wymiany uszkodzonego podzespołu bez konieczności wyłączania serwera i przerywania pracy platformy zarządzającej.

Konieczne są do realizacji wszystkie poniższe profile transmisji:

a) unicast - w dwóch odmianach:

- nagrywanie i podgląd z wykorzystaniem jednego strumienia (cała transmisja odbywa się poprzez serwer)
- nagrywanie i podgląd z wykorzystaniem dwóch niezależnych strumieni (cała transmisja odbywa się poprzez serwer)

b) Multicast -nagrywanie i podgląd z wykorzystaniem jednego strumienia (niezależna transmisja do operatora oraz serwera)

c) Hybrydowe - nagrywanie i podgląd z wykorzystaniem dwóch niezależnych strumieni (przykładowo transmisja unicast do serwera oraz multicast do operatorów)

d) Transkodowanie dopasowanie strumieni wideo pomiędzy serwerem, a stacją operatora do szerokości dostępnego pomiędzy nimi pasmem transmisji

System musi zapewniać nieograniczoną licencyjnie ilość jednoczesnych połączeń klienckich z komputerów zdalnych, wyposażonych w aplikacje kliencką systemu , urządzeń mobilnych obsługiwanych przez system Android lub iOS oraz z dowolnej przeglądarki internetowej.

Ze względu na wrażliwe dane jakimi będą nagrania, system nie powinien umożliwiać operatorom dowolnego eksportu i kopiowania nagrań. Eksport i kopiowanie nagrań powinno być możliwe tylko w przypadkach uzasadnionych i powinno być autoryzowane przez dwóch użytkowników systemu, a mianowicie operatora i administratora (kierownika) przez tzw. Funkcjonalność dualnego logowania.

Możliwość tworzenie elastycznego interfejsu użytkownika szytego na miarę potrzeb zapewnia intuicyjną pracę oraz ekspresowy czas reakcji gwarantując tym samym najwyższy poziom bezpieczeństwa. Dlatego praca operatora musi być wspierana przez następujące cechy interfejsu systemu :

- w pełni edytowalne przyciski ekranowe rozmieszczane w dowolnym miejscu poszczególnych widoków zapewniające możliwość przełączania pomiędzy widokami lub wyzwalania zaawansowanych makr oferujących możliwość wielopoziomowych akcji w tym min wysterowanie presetu kamery PTZ , aktywacja wyjścia przekaźnikowego w kamerze , nadanie uprawnień rozpoznania tablic rejestracyjnych dla danej kamery , sterowanie modułami

- aktywowanie dowolnego makra w tym presetów kamer PTZ po kliknięciu kursorem myszy na predefiniowanym transparentnym regionie obrazu na dowolnym widoku powiązanej kamery stacjonarnej,

- zaawansowane zbliżenia cyfrowe – możliwość zbliżenia cyfrowego dla wielu fragmentów z danej kamery jednocześnie przy możliwości zachowanie podglądu na całą obserwowaną przez nią scenę

- wsparcie dla kontrolera USB z joystickiem do kontrolowania funkcji PTZ ruchomych punktów kamerowych oraz możliwość kontrolowanie kamer PTZ z poziomu panelu w oprogramowaniu

- obsługa cyfrowych modułów I/O aktywowanych z poziomu dedykowanych przycisków ekranowych lub automatycznie przez egzekucję reguł makr

- jednoczesny dostęp do 4 obrazów bieżących (w tym sterowanie funkcjami PTZ) z poziomu przeglądarki internetowej

- jednoczesny podgląd obrazu archiwalnego z minimum 48 kamer jednocześnie w jednym widoku

- dostęp do serwerów z poziomu urządzeń mobilnych (iOS, Android) pozwalający na oglądanie bieżących widoków z kamer, sterowanie funkcjami PTZ oraz przechwytywanie zdjęć ze wskazanych momentów obserwowanego obrazu

- swobodne nadawanie przez administratora systemu hierarchicznych uprawnień każdemu operatorowi lub grupie operatorów korzystających z odpowiednich dla nich zasobów systemu

takich jak dostęp grup użytkowników do urządzeń, funkcjonalności urządzeń, widoków, reguł makr domyślnego widoku wyświetlanie

- edytowalne reguły makr budowane w oparciu o instrukcje warunkowe aktywowane krzyżowo przez wszelkie zasoby oraz funkcjonalności systemu (np. rozpoznanie tablicy rejestracyjnej z tzw. białej listy automatycznie aktywuje przełączenie widoku na ekranie monitora oraz otworzenie bramy wjazdowej do garażu)

- wsparcie 4 i więcej monitorów o dowolnej przekątnej ekranu w ramach każdego stanowiska operatorskiego, w tym wirtualnego kontrolera z matrycą dotykową oraz klawiaturą numeryczną

- definiowanie widoków (wyświetlanie na pojedynczym monitorze) oraz multi-widoków (wyświetlanie na wielu monitorach) o różnej zawartości poszczególnych paneli (np. obraz na żywo, odtwarzanie, zegar, adres URL, lista zdarzeń, przycisk funkcyjny, mapa obiektu, sterowanie PTZ), dowolnym rozmiarze oraz położeniu w ekranie monitora

- obsługa funkcji tzw. videowall'a z możliwością zdalnego delegowania zawartości poszczególnych widoków wyświetlanego na ekranach monitorów podrzędnych stacji operatorskich

- zbliżenie cyfrowe wybranego fragmentu obrazu bez utraty podglądu na pierwotny zakres obserwowanej sceny

- wybór kamery do aktualnego podglądu przez przeciągnięcie ikony kamery z mapy synoptycznej

- wskazanie materiału blokowanego przed nadpisaniem

- rozpoczęcie nagrywania po detekcji ruchu definiowanej dla dowolnego obszaru kamery

- możliwość doboru czasu nagrania dla każdej z kamer indywidualnie

- zmiana atrybutów zapisu przypisana do aktywnego profilu

- odtwarzanie ostatnich kilkunastu sekund nagrania bezpośrednio z widoku kamery będącej aktualnie w trybie podglądu bieżącego obrazu po kliknięciu prawym przyciskiem myszy

- dynamiczna zmian trybów , parametrów nagrywanie poprzez makra jako reakcja na dowolne zdefiniowane przez użytkownika zdarzenie w systemie

- zmiana parametrów nagrywania w oparciu o kalendarz tygodniowy lub roczny dedykowane szczególnie dla wydarzeń niepowtarzalnych w terminarzu jak imprezy masowe

- eksport materiału z wielu serwerów jednocześnie do jednego pliku z materiałem archiwalnym

- wybór kamery do podglądu archiwalnego przez przeciągnięcie ikony kamery z mapy synoptycznej

- funkcjonalność zoomo`walnych map umożliwiających wykorzystanie w wizualizacji obiektów map wektorowych dzięki czemu na jednej tylko mapie wysokiej rozdzielczości można umieścić elementy znajdując się na całym chronionym obiekcie ,które będąc scrollowaną będą zapewniając bardzo szybkie przejście od podglądu ogólnego obrysu obiektu do wysokiego poziomu szczegółowości np. do poziomu danego pomieszczenia.

- programowa korekcja zniekształceń obrazu dla wszystkich obsługiwanych kamer w tym min dla kamer analogowych

- obsługa kamer 360 stopni typu rybie oko – odbywa się przez możliwość rozłożenia jednego strumienia kamery dowolnego producenta na trzy widoki w dedykowanych panelach umożliwiających : podgląd panoramiczny, sferyczny oraz podgląd na obszar wybrany przez obrót ePTZ i przez wskazanie przez operatora w poglądzie panoramicznym oraz sferycznym przy czym obserwowany na tym panelu obraz jest zaznaczany obwódką w celu łatwej

orientacji w obserwowanym materiale. Przetwarzanie kamer typu rybie oko musi być certyfikowane przez Immervision Enables®

- możliwość precyzyjnej lokalizacji zdarzenia na skorelowanej mapie synoptycznej np. poprzez wskazanie przez podświetlenie transparentnych wielopolygonowych obszarów wizualizujących miejsce wykrycia alarmu.

- możliwość korelacji dowolnej rekacji systemu np. przełączenie trybu nagrywanie, wyzwolenie presetu kamery, przesłanie sygnału do sytemu integrowanego, aktywacja analizy obrazu dla wybranej kamery lub grupy kamer, wyzwalanego poprzez transparentny wielopolygonowy obszar

- system ma dawać możliwość automatycznego wskazanie obrazu z kamer obserwujących dany interesujący obszar obiektu bez konieczności znajomości przez operatora nazw, grupy kamer oraz ich hierarchii – funkcjonalność ta zwiększa ergonomię i szybkość pracy operatora.

- możliwość wysłania emaila z dołączanym zdjęciem prezentującym zdarzenie alarmowe poprzez wykorzystanie przez silnik makr wraz z możliwością tworzenia generycznych makr – przechwytywanie wielu zdarzeń przez jedno generyczne makro

- alarmowanie o opóźnieniu w transmisji materiału z kamer – jest kluczowe w systemach wykorzystujących punkty kamerowe do: sterowania automatyką / weryfikacji procesów technologicznych, obsługi systemów rozproszonych. System musi alarmować operatora w przypadku wystąpienia opóźnieni w transmisji obrazu powyżej 500 ms.

System musi zapewniać możliwość rozszerzenie bezpieczeństwa obiektu poprzez implementację algorytmów inteligentnej analizy obrazu. System pozwoli na migrację funkcji analitycznych w obszarze zasobów systemu oznaczającą brak konieczności stosowania wyspecjalizowanych kamer dedykowanych do realizacji tejże analizy zawartości obrazu oraz możliwość wykorzystywania jednej kamery do wykonywania wielu analiz minimum 5 różnych typów analiz jednocześnie lub wdrożenie analizy obrazu dla istniejących analogowych lub sieciowych punktów kamerowych.

W celu sprawniejszego wyszukiwania zdarzeń algorytmy muszą:

- umożliwiać analizę danych post factum pozwalającą na wykonanie analizy zawartości obrazu już zarejestrowanego przez kamerę nawet dla kamery, dla której dana reguła analityczna nie była wcześniej aktywna. Usprawnia to znacznie proces poszukiwanie materiału video, gdyż system CCTV w ekspresowym tempie do np. do 300 sekund wyświetli listę znalezionych zdarzeń z wybranego zakresu czasowego odpowiadających wyrysowanej regule np. pojawienie się osoby w danym wyrysowanym obszarze z możliwością podglądu materiału video skorelowanego ze zdarzeniem z listy spełniających warunków zdarzeń. Powoduje to, iż wyszukanie poszukiwanego zdarzenia nie wymaga ręcznego, czasochłonnego przeszukiwania rejestrowanego materiału video.

- zapisywać meta dane w bazie danych zapewniającą szybkie wyszukiwanie archiwizowanych zdarzeń z wykorzystaniem do tego celu wielu kryteriów (np. egzekucja makra, wskazanie regionu obrazu, zmiana kąta obserwacji kamery, skorelowany indywidualnie tekst, tablice rejestracyjne, twarze, zdefiniowane reguły ruchu) definiowalnych dla wybranych zasobów we wskazanym okresie czasu.

Dla każdego punktu kamerowego możliwe będzie zaimplementowanie algorytmu inteligentnej analizy obrazu bazując na licencjach serwera dającej tym samym możliwość migracji wybranej funkcji wg harmonogramu. Dla wybranego punktu kamerowego możliwa będzie implementacja jednego, dwóch lub wszystkich algorytmów jednocześnie:

- rozpoznawanie tablic rejestracyjnych
- rozpoznawanie twarzy- algorytm wyodrębnia z bieżącego obrazu wideo twarze obserwowanych osób przekształcając je do postaci tzw. meta danych. Analizie podlegają punkty nanoszone na brwi, oczy, nos oraz usta. Każda rozpoznana twarz jest porównywana ze wzorcem przechowywanym w bazie danych i na tej podstawie automatycznie klasyfikowana do tzw. czarnej lub białej listy ściśle powiązanej z uprawnieniami dostępu do zasobów obiektu osób, których twarz podlega analizie. Na podstawie wyników tejże analizy,

system aktywuje odpowiednią regułę makr. Aktywacja dedykowanego profilu pozwala na weryfikowanie obecności osób we wskazanym miejscu obiektu z podaniem okresu czasu.

- rozpoznawanie reguł ruchu predefiniowane reguły ruchu izolują i klasyfikują obiekty wprost z bieżącego strumienia wideo.

- detekcja twarzy na dowolnej obsługiwanej przez platformę kamerze będzie możliwa bez konieczności wykorzystywania dodatkowych licencji lub wykorzystywania dedykowanych kamer.

System musi zapewniać komunikację programową ze zintegrowanym systemem bezpieczeństwa SMS umożliwiając poprzez synergę tych systemów następujące funkcjonalności:

- aktywację predefiniowanych ustawień kamer obrotowych kamer PTZ w wyniku otrzymania przez system SMS informacji alarmowej z systemu SSWiN, KD lub innych
- zdalne kontrolowanie funkcji PTZ z poziomu mapy synoptycznej systemu SMS
- generowanie zdarzeń w bazie danych systemu SMS z przypisaniem powiązanego obrazu
- import zdarzeń będących wynikiem działania algorytmów analizy obrazu
- wyświetlanie obrazu z kamer w trybie bieżącego podglądu np. z poziomu mapy synoptycznej systemu SMS
- odtwarzanie materiału archiwalnego przypisanego do zdarzeń w systemie SMS

Parametry kamer:

Kamery zewnętrzne 4 MPX 2,8-12mm z motozoomem wyposażonych w obudowy z grzałką, promiennikiem

Wielostrumieniowa wysoka rozdzielczość

umożliwia przesyłanie dwóch strumieni H.264/H.264 lub H.264/MJPEG. Istnieje możliwość połączenia wielu rozdzielczości i przepływności dla różnych scenariuszy oraz podglądów na żywo. Można użyć standardu H.264i aby zmniejszyć pasmo, przy jednoczesnym zachowaniu wysokiej jakości obrazu.

ONVIF

w pełni obsługuje międzynarodowy standard ONVIF, zapewniając zestandaryzowany dostęp oraz integrację z systemami zarządzania wideo, zgodnymi z ONVIF.

Smart Codec

Funkcje Smart Codec, w tym również Smart Recording z podwójnym VCA, tryby niskiej przepływności oraz niskich opóźnień, rozszerzenie ROI, przesyłanie wielostrumieniowe, tryb obrotu oraz Edge Recording.

Maski prywatności

Maski prywatności zakrywają obszary obrazu. Funkcja ta jest często wymagana w miejskim monitoringu lub w monitoringach w centrach handlowych.

Dzień / noc

W warunkach słabego oświetlenia, kamera automatycznie przełącza się na podświetlenie podczerwienią, dzięki filtrowi IR-cut. Funkcja ta zapewnia, iż nawet przy najmniejszym dostępie światła, kamera wciąż będzie przysyłać zdjęcia w wysokiej jakości. Kamera dostarczana jest w standardzie z diodami LED, odpowiedzianymi za podświetlanie IR.

WDR

W sytuacjach, gdy obserwowany obiekt jest niewyraźny z uwagi na niedostateczną lub nadmierną ilość światła (jak w przejściach lub w przypadku zbyt dużej liczby okien), wtedy funkcja WDR rozwiązuje ten problem poprzez wzięcie dwóch najlepszych zdjęć o różnym stopniu naświetlenia.

Wybór źródła zasilania

Kamera może być zasilana napięciem 12 Vdc (wtyczka DC) lub poprzez kabel sieciowy, dzięki zgodności ze standardem PoE.

Cechy:

- 1/3" przetwornik typu CMOS
- obiektyw elektryczny 2,8 do 12 mm
- 4 MP przy 20 kl./s (2688 x 1520)
- 2 MP przy przepływności 25/30 kl./s
- dwa strumienie H.264/H.264 lub H.264/MJPEG
- detekcja przekroczenia linii oraz wtargnięcia
- 3D DNR
- 120 dB WDR
- obsługa wbudowanej pamięci 128 GB
- IP67
- 12 Vdc / 802.3af PoE

Specyfikacja techniczna

Sensor obrazu przetwornik 1/3" typu CMOS

Minimalne naświetlenie 0,1 lux kolor, 0,01 lux (cz/b), 0 lux z podświetleniem IR

Szybkość migawki 1/3 s do 1/10 000 s

Migawka powolna obsługuje

Obiektyw elektrycznie sterowany, 2,8 do 12 mm, F1.4

Poziome pole widzenia 112° ~ 33.8°

Automatyczna przysłona zasilana prądem DC

Dzień/noc filtr IR-cut z automatycznym włącznikiem

Podświetlanie IR 42 el., 850 nm

Odległość skuteczna podświetlania IR do 30 m

WDR 120 dB

Udoskonalenie obrazu zaawansowane DNR / ROI / BLC

Ustawienia obrazu tryb obracania, nasycenie, jasność, kontrast, kolor oraz ostrość regulowane są z poziomu oprogramowania klienckiego lub przeglądarki internetowej

Korekcja odkształceń obrazu obsługuje

Balans bieli ręczny, AWB1, AWB2, blokada WB, lampa fluorescencyjna, lampa żarowa, ciepła barwa światła, światło naturalne

Wideo

Algorytm(y) kompresji H.264, MJPEG, H.264i

Typ H.264 profil główny

Przepustowość wideo 32 Kb/s - 16 Mb/s

Maks. rozdzielczość 2688x1520

Przepływność główna: 2688 x 1520 (20/20fps), 2304 x 1296 (20/20fps), 1920 x 1080 (25/30fps), 1280 x 720 (25/30fps) podrzędna: 1280 x 720(25/30fps), 640 x 480(25/30fps),

352 x 288(25/30fps), 320 x 240(25/30fps)

Położenie odwrócone normalne, flip, odbicie lustrzane, tryb pionowy, 180 stopni

Warstwa tekst / wideo łańcuch tekstowy (28 znaków), napisy (1 linia o długości 44 znaków)

Strumieniowanie wideo strumień podwójny H.264 + H.264 lub H.264 + MJPEG

Parametry dźwiękowe

Interfejs dźwiękowy 1-ch 3,5 mm wejścia audio / wyjście audio

Wejścia/Wyjścia dźwiękowe obsługa podwójnej ścieżki audio w stereo

Kompresja audio G.711/G.722.1/G.726/MP2L2

Przepustowość dźwiękowa

64 Kb/s (G.711) / 16 Kb/s (G.722.1) / 16 Kb/s (G.726) /

32-128 KB/s (MP2L2)

Filtrowanie szumów z otoczenia obsługuje

Zestaw funkcji inteligentnych

Wykrycie przekroczenia linii przekroczenie wstępnie określonej linii wirtualnej

Wykrycie wtargnięcia wtargnięcie na wstępnie określony obszar wirtualny

Detekcja ruchu 8 zdefiniowanych przez użytkownika, prostokątna maska, nastawne poziomy wykrycia, czułość oraz interwały czasowe

Sygnalizacja sabotażu wł./wyl./zaprogramowana

Magazyn danych

Magazyn wbudowany wbudowane gniazdo SD/SDHC/SDXC, pojemność do 128 GB

Magazynowanie sieciowe NAS

Kamery 4-obiektywowych x 5MPX 3,3-6,6 mm z motozoomem

Kamery kopułkowe IP typu all-in-one do zastosowań zarówno wewnątrz jak i na zewnątrz z funkcją dzień / noc, zdalnie konfigurowalnym wielokierunkowym multisensorem, działające w trybie 20 megapikseli z modelami SNAPstream™ (Smart Noise Adaptation and Processing) oraz WDR (Wide Dynamic Range).

- konfiguracja bezdotykowa: 4 oddzielne kamery Gimbals, każda z mechanicznym obiektywem ze zmienną ogniskową, które można ustawiać zdalnie w dowolnej pozycji w ramach ścieżki 360 stopni

- wstępne położenia, pozwalające osiągnąć kąt patrzenia 360°, 270° lub 180° - można też zapisać własne ustawienia

- technologia SNAPstream™ zaawansowanego algorytmu kompresji redukuje pasmo bez utraty jakości obrazu

- Forensic Zooming – zoom na żywo lub po wystąpieniu zdarzenia podczas nagrywania z pełnym polem w jakości

HD – zastąpienie urządzeń PTZ

- tryb dzień/noc z mechanicznym filtrem IR

- funkcja True WDR o mocy do 100dB przy pełnej rozdzielczości: wyraźna widoczność przy jednocześnie jasnych

i zaciemnionych warunkach oświetlenia w wybranych modelach 12 MP

- tryb Binning umożliwiający zachowanie doskonałych parametrów w warunkach słabego oświetlenia

- maski prywatności, wykrywacz ruchu, elastyczne przycięcie, kontrola przepływności, wielostrumieniowe przesyłanie

danych oraz funkcja grupowego rozsyłania

- podwójny koder H.264/MJPEG

- protokoły internetowe, w tym: 802.1x, IPv6, QoS, DHCP i wiele innych

- zasilanie PoE oraz zasilanie zapasowe: 18–48V DC / 24V AC

- obudowa zewnętrzna o klasie szczelności IP66 i odporności na zniszczenia IK-10

Transmisja danych

Typ kompresji

H.264 (MPEG-4, Part 10)/ruchomy JPEG

21 poziomów jakości

Protokoły sieciowe RTSP, RTP/TCP, RTP/UDP, HTTP, DHCP, TFTP, IPv4, IPv6, QoS, 802.1x

Interfejs sieciowy 100 Base-T Ethernet

Wielo-strumieniowość 8 różnych strumieni

Parametry środowiskowe

Temperatura robocza

-40°C do 50°C

0°C to 50°C wyl. grzałka

Wilgotność 0% to 90% (bez skroplenia)

Temperatura przechowywania -40°C do 60°C

Parametry elektryczne

Wejścia / wyjścia alarmowe 1 wejście/ 1 wyjście

Power Over Ethernet PoE 802.3af, Klasa 3

Zasilanie pomocnicze 18-48V DC, 24V AC

Maksymalny pobór mocy 12 W

Parametry fizyczne

Obudowa

obudowa z odlewane aluminium z poliwęglanową bańką kopułkową

klasa szczelności dla odporności pogodowej – IP66

znamionowa odporność uderzeniowa – IK-10

Gimbal regulacja ręczna, 3-osiowa w zakresie obrotu 360° pan i pochylenia 135°

Wymiary

Zespół Ø 223,4 mm x wys. 125,4 mm

Tylko bańka Ø 183,3 mm x wys. 59,3 mm

Waga Zespół 2.36 kg

Kamer 2-obiektywowa 2,8mm 4MPX

- Technologia SNAPstream redukująca przepustowość bez wpływania na jakość obrazu
- Bardzo wysoka czułość świetlna z trybem Binning dla modeli MicroDome Duo 6- i 10-megapikselowych
- Prawdziwy tryb dzień/noc z mechanicznym filtrem IR
- WDR aż do 100dB dla pełnej rozdzielczości dla model MicroDome Duo
- CorridorView pozwala na obrót obrazem o 90°, co zapewnia lepsze wrażenia wizualne na deptakach oraz korytarzach
- Podwójny enkoder H.264 / MJPEG
- Zdalne sterowanie ostrością
- Maski prywatności, detekcja ruchu, rozdzielczość kadrowania, kontrola przepływności, wielokrotne-strumieniowanie, przybliżanie śledcze
- Łatwość regulowania trzech osi kamery
- Odporność na uderzenia IK-10
- Odporność IP66

Wielkość sensora: 1/3.2"

Kolor (Tryb dzienny): 0.2 Lux

B/W (Tryb nocny): 0.03 Lux, IP czułości

WDR: WDR aż do 100d

Cechy:

- przetwornik 1/1.7" typu CMOS
- obiektyw - 1,65 mm, F2.8
- 12 MB przy 20 kl./s.
- jednoczesny strumień wideo w standardzie H.264 oraz MJPEG
- tryb dzień / noc z filtrem IR-cut
- wbudowane podświetlenie podczerwienią (odległość efektywna: 5 m)
- 24 Vac / 24 Vdc / 12 Vdc / 802.3af PoE
- zgodność ze standardem ONVIF Profile S
- minimalne naświetlenie: 0.01lux @ F2.8 kolor, 0.01 lux @ F2.8 (cz./b.), 0 lux z podświetleniem IR
- klasa szczelności IP66
- odporność uderzeniowa IK10

Integracja OPTicamp z SKD

Na potrzeby aplikacji projektowanego systemu integrującego OPTicamp z SKD do obsługi użytkowników PWSZ oraz Centrum Symulacji Medycznej wykorzystane zostanie wyodrębniony zasób w środowisku wirtualnym o parametrach nie gorszych niż:

Procesor – min. 2 core

Pamięć RAM – 6 GB

Dysk twardy – 120 GB min. RAID 1

Karta sieciowa - 1 interfejs 100MB/s

Połączenie sieciowe serwera powinny zapewnić dostęp zarówno do sieci wewnętrznej (serwer SKD), sieci SELS (dostęp do bazy danych OPTIcamp)

Adresacja IP poszczególnych usług i aplikacji zostanie ustalona z Zamawiającym na etapie wdrożenia.

Moduł synchronizacji zostanie zrealizowany w technologii Microsoft .NET.

Synchronizacja danych między OPTIcamp-em a SKD opierać się będzie o replikę bazy danych OPTIcamp. Replika bazy danych zostanie udostępniona przez Zamawiającego. Konto użytkownika dostępowego do repliki bazy OPTIcamp, będzie w trybie tylko do odczytu. Moduł synchronizacji danych będzie łączył się tylko z punktem dostępowym do sieci SELS. W podobny sposób będzie komunikował się z aplikacją SKD

Synchronizacja użytkowników w systemie odbywa się na dwa sposoby:

- pojedynczo – przy logowaniu
- zbiorowo – różnicowa synchronizacja nocna

Pierwszy sposób wykonuje się po zalogowaniu się użytkownika do systemu. Za każdym razem z SELS OPTIcamp pobierany jest rekord z danymi użytkownika, porównywany z danymi znajdującymi się w systemie SKD. i w momencie, gdy zostanie wykryta różnica na kluczowych danych^[1], wykona się aktualizacja danych w SKD.

Status konta użytkownika zapisywany w SKD jest kombinacją dwóch pól pobieranych z bazy danych OPTIcamp (status karty oraz data ważności karty). W przypadku, gdy karta straciła ważność lub jej status jest większy od 7 (karta straciła ważność, jest zablokowana, itp.), konto użytkownika zostanie zablokowane. Jest to równoznaczne z odebraniem dostępu do budynku oraz utratą możliwości otwierania szlabanów na parkingach. W dalszym ciągu użytkownik może korzystać do portalu WWW.

Przebieg procesu logowania:

- autentykacja użytkownika w systemach AD/OpenLDAP

Następnie dane pobierane są z bazy SELS i po wykonaniu na nich pewnych przekształceń zapisane do bazy danych systemu SKD. Po zakończeniu synchronizacji użytkownik zostaje przekierowany na stronę główną.

Z systemu SELS obierana jest informacja o przynależności użytkownika do grupy.

Wszystkie przekazywane dane opisane zostały w poniższej tabeli.

Nazwa pola	Opis
ID	Identyfikator użytkownika
LoginName	Login do systemu SELS/IPProtect
FirstName	Imię użytkownika
LastName	Nazwisko użytkownika
Email	Adres e-mail zapisany w AD/OpenLDAP
UserNumber	Numer indeksu/numer pracowniczy
VehicleRegistrationNumber	Numer rejestracyjny (nie jest mapowany z SELS)
PinCode	PIN do karty (nieużywany)
SmartCardSerialNumber	Zbliżeniowy identyfikator legitymacji
State	Status konta (aktywne/nieaktywne)
CardType	Typ karty (zawsze wartość MIFARE)
CardExpirationDate	Data ważności legitymacji
GroupCode	Grupa (pracownik, doktorant, student)

Drugi typ synchronizacji polega na cyklicznym uruchamianiu procesu w większości przypominającego synchronizację pojedynczego użytkownika. Najpierw wyznaczany jest zestaw użytkowników, którzy powinni zostać zsynchronizowani. Są to osoby, których rekordy w bazie danych OPTIcamp zostały zmodyfikowane od wykonania poprzedniej

^[1] Jako kluczowe dane rozumiane są: imię, nazwisko, status karty oraz zbliżeniowy identyfikator karty

synchronizacji. Następnie odrzucane są osoby, które nie znajdują się w systemie SKD i nie są pracownikami. Na pozostałej puli rekordów wykonywana jest operacja porównania, a aktualizacja danych następuje dopiero przy wykryciu zmian kluczowych dla systemu. Obydwa typy synchronizacji kończą się przydzieleniem domyślnych uprawnień dla użytkownika.