#  CZĘŚĆ OGÓLNA

## Przedmiot opracowania

Przedmiotem opracowania jest opis szczegółowy wymagań branży **Teletechnicznej**.

W ramach opracowań instalacji teletechnicznych ujęte będą:

* System przyzywowy,
* System sygnalizacji pożaru - SSP,
* dźwiękowy system ostrzegawczy – DSO,
* System Interkomowy,
* System kontroli dostępu
* System monitoringu CCTV
* System sygnalizacji włamania i napadu
* Platforma integracyjna z wizualizacją

## Podstawa opracowania

* projekt architektury
* projekt technologii
* uzgodnienia z Inwestorem
* Rozporządzenie Ministra Infrastruktury z dn. 12-04-2002r. DzU Nr 75 poz. 690 "W sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie" z późniejszymi zmianami
* Rozporządzenie MSWiA z dn.07-06-2010r. DzU Nr 109 poz. 719 "W sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów"
* [PN-EN 50173-1:2011](http://sklep.pkn.pl/pn-en-50173-1-2011e.html) - Technika informatyczna -- Systemy okablowania strukturalnego -- Część 1: Wymagania ogólne
* [PN-EN 50173-2:2008/A1:2011](http://sklep.pkn.pl/pn-en-50173-2-2008-a1-2011e.html) - Technika informatyczna -- Systemy okablowania strukturalnego -- Część 2: Pomieszczenia biurowe
* [PN-EN 50174-1:2010/A2:2015-02](http://sklep.pkn.pl/pn-en-50174-1-2010-a2-2015-02e.html) - Technika informatyczna -- Instalacja okablowania -- Część 1: Specyfikacja instalacji i zapewnienie jakości
* [PN-EN 50174-2:2010/A2:2015-02](http://sklep.pkn.pl/pn-en-50174-2-2010-a2-2015-02e.html) - Technika informatyczna -- Instalacja okablowania -- Część 2: Planowanie i wykonywanie instalacji wewnątrz budynków
* [PN-EN 50346:2004/A2:2010](http://sklep.pkn.pl/pn-en-50346-2004-a2-2010p.html) - Technika informatyczna -- Instalacja okablowania -- Badanie zainstalowanego okablowania
* [PN-EN 50310:2012](http://sklep.pkn.pl/pn-en-50310-2012p.html) - Stosowanie połączeń wyrównawczych i uziemiających w budynkach z zainstalowanym sprzętem informatycznym
* BN-88/8994-19 Telekomunikacyjne sieci wewnątrzzakładowe przewodowe. Linie kablowe. Ogólne wymagania i badania.
* PN-T-06800 Sygnały: Wizyjny i foniczny
* PN-IEC 574-2 Urządzenia i systemy audiowizualne, wizyjne i telewizyjne
* zestaw norm PN-EN 50132 Systemy alarmowe. Systemy dozorowe CCTV stosowane w zabezpieczeniach
* właściwe normy krajowe dotyczące instalacji elektrycznych
* właściwe normy branżowe i zalecenia dotyczące instalacji teletechnicznych
* katalogi urządzeń i materiałów

**WYSTĘPUJĄCE W OPRACOWANIU URZĄDZENIA ZAOPATRZONE W NAZWY WŁASNE ZOSTAŁY WYBRANE W CELU DOKONANIA WŁAŚCIWYCH OBLICZEŃ. ZGODNIE Z PZP ART.29 P.3 DOPUSZCZA SIĘ MOŻLIWOŚĆ ZAMONTOWANIA/ZASTOSOWANIA URZĄDZEŃ O PARAMETRACH RÓWNOWAŻNYCH PO UZGODNIENIU Z INWESTOREM ORAZ INŻYNIEREM KNTRAKTU.**

# 2. CZĘŚĆ TECHNICZNA

* 1. **System Kontroli Dostępu**
		1. **Wymagania ogólne**

Projekt przewiduje instalację na obiekcie Systemu Kontroli Dostępu (KD), którego głównym zadaniem jest kontrola przepływu osób poruszających się w ramach wyznaczonych obszarów. System musi umożliwiać nadawanie uprawnień poszczególnym osobom, w zakresie ich dostępu w określonych porach dnia, do określonych części budynku. Możliwość decydowania, kto, gdzie i kiedy może wejść ma kluczowe znaczenie dla ochrony budynku, pracujących w nim osób oraz znajdujących się tam informacji i mienia.

Jako sposób identyfikacji osób zakłada się wykorzystanie kart zbliżeniowych. Czytniki zlokalizowane będą przy wejściach do wyznaczonych stref oraz do pomieszczeń technicznych, lub innych wymagających szczególnego zabezpieczenia. Zaprojektowany system pozwala na sieciową pracę urządzeń (zarządzanie, konfiguracja i rejestracja zdarzeń) oraz na sukcesywną rozbudowę. Poprawna identyfikacja osoby pozwala na otwarcie drzwi automatycznych lub zwolnienie elektrozaczepu drzwi „tradycyjnych”. Z uwagi na uniwersalność i izolację galwaniczną obwodów elektrycznych instalacji współpracujących z instalacją kontroli przejścia, do przekazania sygnału identyfikacji wykorzystuje się bezpotencjałowe styki (NO/NC) przekaźników wyjściowych kontrolerów. Jako element wykonawczy do blokowania drzwi nieautomatycznych zaprojektowano elektrozaczepy rewersyjne NO z mikroprzełącznikiem (informacja o otwarciu drzwi przy użyciu klamki lub klucza). Wejście do pomieszczenia lub strefy objętej jednostronną kontrolą dostępu jest możliwe po poprawnej identyfikacji (od strony wejścia drzwi wyposażone są w uchwyt), wyjście po naciśnięciu klamki od wewnątrz. W przypadku kontroli dostępu dwustronnej otwarci drzwi możliwe jest wyłącznie po poprawnej identyfikacji karty przyłożonej do czytników zaprojektowanych po obu stronach drzwi. W miejscach, gdzie projekt przewiduje dwustronną kontrolę przejścia, w kierunku drogi ewakuacyjnej, poza czytnikiem przy drzwiach należy zainstalować przycisk wyjścia ewakuacyjnego, a zasilanie elektrozaczepu zintegrować z SAP w taki sposób, aby w przypadku alarmu pożarowego II-go stopnia, w strefie, w której znajduje się przejście, nastąpiło jego zwolnienie.

Każde drzwi objęte systemem kontroli dostępu muszą być wyposażone w kontaktrony zintegrowane ze stolarką.

Zaprojektowany system oparty jest o kontrolery przystosowane do funkcjonowania w środowisku sieciowym, przeznaczonym dla systemów ochrony. Kontrolery komunikują się z serwerem za pośrednictwem sieci strukturalnej, z wykorzystaniem protokołu TCP/IP. Na serwerze będzie zainstalowane oprogramowanie służące do zarządzania systemem. Utrata zasilania lub awaria serwera nie może wpływać w żaden sposób na bieżące działanie Systemu Kontroli Dostępu, gdyż zaprojektowany system jest systemem rozproszonym (każdy kontroler ma zapisaną bazę użytkowników i działa niezależnie).Każdy z zaprojektowanych kontrolerów należy wyposażyć w akumulatory umożliwiające, w przypadku awarii zasilania w budynku, funkcjonowanie systemu przez czas minimum 4 godzin.

System kontroli dostępu należy zintegrować z przewidzianą w ramach niniejszego projektu Platformą PSIM w taki sposób, aby z poziomu interfejsu platformy możliwe było sterowanie przejściami, zarządzanie użytkownikami, pełna wizualizacja stanu przejść oraz monitoring techniczny systemu.

W ramach realizacji niniejszego zakresu należy dostarczyć 300 kart zbliżeniowych Mifare oraz drukarkę z oprogramowaniem do zadrukowywania kart.

* + 1. **Charakterystyka systemu**

Program zarządzający systemem kontroli dostępu ma być zainstalowany na dostarczonym serwerze typu RACK, musi pracować w topologii Klient – Serwer i być dostępny przez przeglądarkę WWW. Jednocześnie musi być to w pełni autonomiczne oprogramowanie, pozwalające na pracę bez ciągłego połączenia elementów systemu z serwerem, realizujące ideę „rozproszonej inteligencji”. Obsługa systemu przez operatorów może odbywać się z niezależnych stanowisk z dowolnego punktu sieci. Projekt przewiduje 3 niezależne stanowiska operatora oraz dodatkowe stanowisko dla głównego administratora systemu zintegrowane z serwerem.

Oprogramowanie musi umożliwiać tworzenie modeli czasowych dostępu zdefiniowanych na poszczególne dni tygodnia łącznie z konfiguracjami obejmującymi dni wolne, święta itp. Modele takie umożliwiają automatyczne uaktywnianie / blokowanie ustawień karty, np. zasad dostępu, kodów PIN itp.

Ze względu na przyszłą rozbudowę systemu, zaprojektowane rozwiązanie nie posiada ograniczeń w zakresie ilości kontrolerów możliwych do połączenia. Struktura systemu umożliwia zbudowanie i podłączenie magistrali sterowników (kontrolerów) w „gwiazdę”, co gwarantuje możliwość prowadzenia poszczególnych magistrali z jednego centrum w różnych kierunkach. Zaprojektowany system musi umożliwiać wyprowadzenia min. 32 niezależnych magistral.

Ze względu na przyszłą rozbudowę wymaga się, by system zapewniał następującą minimalną pojemność: co najmniej 50 000 użytkowników kart, co najmniej 2000 czytników (lub 1000 dwustronnie kontrolowanych przejść) w ramach jednego podsystemu.

System musi umożliwiać pogląd stanu aktualnego oraz pełne raportowanie - dowolne filtrowanie odczytów umożliwiające sprawdzenie historii każdego użytkownika karty lub wybranego pomieszczenia (kto, gdzie i kiedy przebywał), przeglądanie ścieżek przejścia pracowników, lokalizację pracowników.

**Kontroler drzwiowy**

Zaprojektowany kontroler przeznaczony jest do pracy w systemach kontroli dostępu pracujących pod programami opisanym powyżej. Kontroler musi posiadać 4 porty czytników, umożliwiając kontrolę 4 drzwi jednostronnie lub 2 drzwi dwustronnie.

W procesie komunikacji kontrolera z oprogramowaniem nadzorczym wykorzystywane jest kodowanie AES 128 bitowe. Na płycie kontrolera znajduje się 16 wejść linii dozorowych, do których zostaną podłączone elementy bezpieczeństwa (tj. kontaktrony). Kontroler musi być monitorowany przez specjalne wejście linii dozorowej do podłączenia czujnika sabotażowego obudowy kontrolera. Kontroler ciągle monitoruje stan zasilania sieciowego i akumulatora. Wszystkie zmiany stanu są raportowane komunikatami wysyłanymi do programu nadzorczego oraz Platformy PSIM. Są to komunikaty typu: „Zasilanie AC utracone”, „Niski poziom zasilania z akumulatora”, „Brak zasilania z akumulatora” itp. Wyjścia napięć zasilających są zabezpieczone przed uszkodzeniem na wypadek zwarcia i kontrolowane. Podobnie jest z wyjściami do sterowania zamków. Kontroler posiada sygnalizację stanu na płycie głównej w postaci diod LED, które pokazują stan aktywności sieci Ethernet, zasilania, wyjść sterujących itp.

Wymagania techniczne dla kontrolera systemu KD:

* + 1 x port sieciowy Ethernet 10/100 do połączenia z programem bramki
	+ 1 x RS-232 (COM3) do bezpośredniego połączenia z komputerem lub z konwerterem transmisji na RS-485 obsługującym magistralę kontrolerów
	+ 1 x RS-485 (COM1) do połączenia z magistralą kontrolerów
	+ 1 x SPI (interfejs szeregowy peryferii) do podłączenia modułów rozszerzeń wejść linii dozorowych i wyjść bezpotencjałowych oraz przekaźnikowych
	+ zasilanie sieciowe AC: 230 - 240 VAC, 100VA
	+ zasilanie na wyjściu transformatora: 16,5 VAC
	+ zasilanie z akumulatora: akumulator 12V / 7Ah, monitorowany, czas pracy minimum 4 godziny
	+ typy czytników: Wiegand, ABA Track II, zintegrowane z klawiaturami
	+ wyjścia do czytników: 12 VDC i 5 VDC @ 400 mA max. każde, zabezpieczone i monitorowane
	+ wejścia linii dozorowych: 16 wejść linii dozorowych (Z1 do Z16), bez rezystora EOL, z pojedynczym rezystorem EOL lub podwójnym oraz 1 wejście do czujnika drzwi obudowy
	+ typ przewodu/maksymalna długość do czujnika na końcu linii: AWG #22 - 600 m
	+ monitorowane wyjścia do zamków: 625 mA każde lub 2.5 Amps razem
	+ wyjścia sterujące do sygnalizatorów w czytnikach: dla diod LED (LED, OUT1, OUT2) oraz dla buzera - każde o 25 mA, tranzystorowe, typu „otwarty kolektor”
	+ przekaźniki na płycie: 4 szt., typu „C”, obciążalność zestyków: 30 VDC/3 Amp każde
	+ pojemność pamięci FLASH: 16 MB
	+ pojemność pamięci SDRAM: 64 MB, zabezpieczona baterią litową przez 75 godzin po utracie zasilania
	+ dodatkowe wyjście zasilające: 12VDC, 250mA, zabezpieczone pozystorem
	+ certyfikaty: CE (EN50133-1, EN55022, EN60950, EN61000-6-1, EN61000-6-2).

**Czytnik zbliżeniowy kart**

Wymagania techniczne dla czytnika zbliżeniowego kart systemu KD:

* + montaż do 60 m od kontrolera
	+ zasięg odczytu do 10 cm
	+ format kodowania 34 bit Wiegand
	+ warunki pracy wewnętrzne/zewnętrzne
	+ 2- kolorowe diody LED sygnalizujące pozytywną weryfikację numeru karty i otwarcie drzwi, błąd odczytu karty
	+ wbudowany sygnalizator akustyczny
	+ typ karty: MIFARE
	+ częstotliwość pracy 13,56 MHz.

**Przycisk wyjścia awaryjnego**

Dla miejsc, gdzie w projekcie przewidziano dwustronną kontrolę dostępu zaprojektowano przycisk wyjścia awaryjnego resetowany przy użyciu kluczyka. Obudowa wykonana jest z plastiku w kolorze zielonym. Przycisk posiada 2 pary zestyków NO/NC – jeden do otwarcia przejścia, a drugi do monitorowania stanu przycisku.

Wymagania techniczne dla przycisku wyjścia awaryjnego systemu KD:

* + przeznaczony do montażu nawierzchniowego
	+ kolor: zielony
	+ obciążalność zestyków: 30VDC 2A
	+ zakres temperatur: -30 do +70 st. Celsjusza
	+ IP24

**Drukarka do kart**

W ramach realizacji niniejszego zakresu należy dostarczyć drukarkę do kart zbliżeniowych.

Wymagania techniczne dla drukarki do kart systemu KD:

* + rodzaj nadruku: kolor / mono
	+ typ nadruku: jednostronny lub dwustronny
	+ charakterystyka: średnie i duże nakłady
	+ rozdzielczość druku: 300 dpi
	+ prędkość druku kolor (YMCKO): powyżej 190 kart/godz.
	+ druk monochromatyczny: powyżej 600 kart/godz.,
	+ druk dwustronny (MCKO-K): minimum 140 kart/godz.
	+ podajnik i odbiornik kart: na 100 kart o grubości 0,76 mm (30 mil)
	+ odbiornik kart odrzuconych: na 30 kart o grubości 0,76 mm (30 mil)
	+ grubość kart: 0,25 - 1,25 mm (10-50 mil)
	+ możliwość nadruku na foliach.

Do drukarki należy dostarczy materiały eksploatacyjne umożliwiające nadruk w kolorze na minimum 1000-ukartach.

* 1. **System Interkomowy**

### **2.2.1. Charakterystyka systemu**

Dla kontroli osób trzecich poruszających się po budynku oddziałów szpitalnych projektuje się zainstalowanie systemu interkomowego.

System będzie nadzorował wejścia do budynku, wejścia na oddziały oraz do wyznaczonych stref z ograniczonym dostępem.

System będzie oparty o urządzenia IP zasilane zgodnie ze standardem 802.3af (PoE). Kasety zainstalowane na ścianach, przy drzwiach, będą podłączone do sieci LAN i będą zalogowane przy wykorzystaniu otwartego protokołu SIP do bramy głosowej, do której zalogowane będą urządzenia systemu przyzywowego oraz telefony bezprzewodowe.

 Urządzeniami końcowymi odpowiedzialnymi za odbieranie zgłoszenia oraz zwalnianie elektrorygla będą telefony IP zalogowane do tej samej bramy głosowej co kasety. Telefony IP systemu interkomowego docelowo będą mogły służyć jako część systemu komunikacji głosowej szpitala. Sterowanie elektroryglem ma odbywać się za pośrednictwem kontrolera SKD obsługującego odpowiednie drzwi do którego należy doprowadzić kabel typu OMY 2x1.

Dla wszystkich urządzeń korzystających z protokołu IP należy zapewnić połączenie z siecią LAN wykonując okablowanie zgodnie z wytycznymi dotyczącymi systemu okablowania strukturalnego dla obiektu.

* + 1. **Elementy systemu**

**Kaseta**

Kaseta przeznaczona poza obszary sterylne i sale operacyjne. Stacja posiada trzy przyciski szybkiego wybierania – będą podświetlone w celu łatwiejszej ich identyfikacji. Posiada klasę szczelności IP53 oraz zasilany jest POE w standardzie 802.3af. Obudowa (wykonana ze stali nierdzewnej) i konstrukcja mechaniczna, gwarantują dużą odporność na warunki klimatyczne i zapewniającą należytą ochronę urządzenia.

Charakterystyka:

* Protokoły sygnalizacji SIP 2.0 (RFC - 3261)
* Przyciski szybkiego wyboru :stal nierdzewna
* Liczba przycisków 1, 3, 6 i rozbudowa modułami do 54
* Klawiatura numeryczna opcjonalna
* Strumień audio Kodeki G.711, G.729, G.722
* Kamera - rozdzielczość 640 (Poziomo) x 480 (Pionowo)
* Kamera - kąt widzenia 55° (Poziomo), 39° (Pionowo)
* Strumień wideo Kodeki H.263+, H.263, H.264, MJPEG
* Zasilanie 12V±15%/2A DC lub PoE
* PoE PoE 802.3af (Class 0 - 12.95W)
* LAN Złącze śrubowe 10/100 BASE-T z Auto-MDIX
* Wyjście przekaźnika styki NC/NO, maks. 30V/1A AC/DC
* Wyjście aktywne 10V – 14V DC / 700mA
* Czytnik kart zbliżeniowych RFID EM-40XX (125Khz) HID Proximity (125kHz, 26/37bit)
* Temperatury pracy -20°C – +55°C
* Temperatury maksymalne -40°C – +70°C
* Wilgotność otoczenia 10% - 95% (bez kondensacji)
* Wymiary 210x100x29 mm
* Poziom odporności IP 53, IK07

Cechy:

* **Strumień wideo w czasie rzeczywistym**

Jest to podgląd kamery interkomu przez 24/7. To ciągła transmisja głosu i wideo za pośrednictwem sieci LAN, która może być odbierana przez 4 różne urządzenia wspierające RTSP jednocześnie i niezależnie od połączenia VoIP.

* **Profile czasowe**

Profil czasowy określa, kiedy numer telefonu lub kod dostępu jest aktywny, a kiedy nie. Każdy profil może być przypisany do danego zamka lub kontaktu w książce telefonicznej. Maksymalnie można utworzyć 20 profili.

* **Sterowanie zamkiem poprzez HTTP**

Przełącznik wewnątrz może być sterowany z innego urządzenia za pomocą komendy http w pełni niezależnie od połączeń przychodzących/wychodzących.

* **Komunikaty słowne**

Funkcja ta umożliwia ustawienie dowolnych komunikatów głosowych zdefiniowanych przez użytkownika, zamiast domyślnych dźwięków. Ta funkcja umożliwia personalizacje urządzenia i czyni go bardziej przyjaznym dla gości.

* **Serwer TFTP**

Funkcja ta umożliwia automatyczna aktualizacje oprogramowania i konfiguracji z serwera TFTP i zapewnia znaczne oszczędności czasu działu IT, gdy wiele domofonów musi być zarządzanych jednocześnie.

* **Zewnętrzny przekaźnik sterowany poprzez IP**

Moduł może sterować innymi urządzeniami za pomocą komend przesyłanych poprzez sieć IP. Odbywa się to identycznie jak w przypadku wbudowanego przełącznika, wystarczy podać adres IP i komendę sterującą.

* 1. **System Przyzywowy**
		1. **Informacje ogólne**

Wymaga się zaprojektowania i wykonania cyfrowego systemu przyzywowego z optyczną i akustyczną sygnalizacją wezwań, priorytetyzacją i wizualizacją zdarzeń na stanowisku pielęgniarskim oraz raportowaniem obsługi zdarzeń i błędów.

Zaprojektowany i wykonany system ma być zgodny z normą DIN VDE 0834 część 1 oraz 2: 2000-04, jak również PN-EN 60601-1:2011 oraz charakteryzować się rozproszoną topologią opartą na sieci LAN. System ma realizować funkcje automonitoringu, co w przypadku uszkodzenia modułu lub okablowania będzie skutkować sygnalizacją na odpowiedniej lampce korytarzowej i telefonie bezprzewodowym. Dodatkowo zaprojektowany system przyzywowy ma umożliwiać pełną integrację z systemem komunikacji bezprzewodowej zarówno w zakresie głosu, jak wiadomości tekstowych (przewidzianego w ramach niniejszego zakresu) oraz Platformą PSIM zapewniającą funkcję wizualizacji wezwań i alarmów na stanowiskach pielęgniarskich.

 System nie może posiadać centralnych elementów sterujących, których uszkodzenie spowoduje brak działania lub niewłaściwe działanie przynajmniej podstawowych funkcjonalności systemu. Zarządzanie i programowanie systemu ma odbywać się przez przeglądarkę internetową i nie może wymagać instalowania dodatkowego (dedykowanego) oprogramowania.

Każde wezwanie z systemu przyzywowego musi być sygnalizowane przez lampkę salową oraz ma trafiać na wizualizację w punkcie pielęgniarskim oraz na telefon bezprzewodowy odpowiedniej osoby/grupy osób odpowiedzialnych za obsługę danego typu wezwania pochodzącego z określonej grupy pomieszczeń lub oddziału. Powiadomienie wyświetlane na telefonie bezprzewodowym musi być oznaczone odpowiednim kolorem, w zależności od typu/priorytetu wezwania. Powiadomienie na telefonie ma zapewniać możliwość jego zaakceptowanie lub odrzucenie. Odrzucenie lub brak akceptacji powiadomienia w zdefiniowanym czasie musi powodować automatyczne przesłanie powiadomienia do kolejnej osoby lub grupy osób. W przypadku akceptacji zdarzenie nie będzie eskalowane oraz zniknie z innych telefonów do których zostało wysłane. Jeżeli wezwanie wygenerowano z modułu wyposażonego w moduł głosowy, po akceptacji wezwania na telefonie musi pojawić się opcja pozwalająca na zestawienie połączenia głosowego z pacjentem. Po odbyciu rozmowy personel musi mieć możliwość zdalnego skasowania wezwania za pomocą telefonu lub zakończenia połączenia bez kasowania alarmu. Opcja zdalnego kasowania nie może być dostępna przed wykonaniem połączenia głosowego.

Do wizualizacji działań systemu przyzywowego ma zostać wykorzystana, przewidziana w ramach projektu, Platforma PSIM, do której będzie dostęp przez przeglądarkę WWW. Wizualizacja musi być spójna dla całego obiektu tzn. dostępna pod jednym adresem sieciowym, a rozgraniczenie, jaki użytkownik ma dostęp do jakich funkcjonalności oraz których zdarzeń, musi być uzależnione wyłącznie od uprawnień nadanych przez administratora systemu.

* + 1. **Założenia projektowe**

W zaprojektowanym systemie przyzywowym na korytarzu nad drzwiami do pomieszczeń objętych elementami przyzywowym należy przewidzieć lampki wyposażone w trzy niezależne, różnokolorowe źródła światła oparte na technologii LED.

Przy drzwiach sal łóżkowych, przewidzieć moduły trzyprzyciskowe, w których istnieje możliwość wykorzystania każdego z przycisków na dwa sposoby: przez naciśnięcie oraz przez naciśnięcie i przytrzymanie przez przynajmniej 2 sekundy. Funkcje przycisków mają być dowolnie konfigurowane w zakresie generowanego zdarzenia i jego priorytetu.

Przy łóżkach pacjentów zaprojektować i zamontować moduły przyłóżkowe trzyprzyciskowe z manipulatorem trzyprzyciskowym na przynajmniej dwumetrowym kablu służącym do wezwania pielęgniarki oraz sterowania dwoma źródłami światła. Do każdego przycisku modułu przyłóżkowego, podobnie jak w modułach trzyprzyciskowych ma być możliwość przypisania przynajmniej dwóch funkcji. Przy każdym łóżku zestaw musi być wyposażony w zintegrowany z nim moduł rozmówny umożliwiający dwukierunkową komunikację głosową personelu z pacjentem. Manipulator do modułu przyłóżkowego musi być podłączony przez złącze, którego konstrukcja, w przypadku silnego, nagłego pociągnięcia w dowolnej płaszczyźnie, jest odporna na uszkodzenie tzn. nie powoduje trwałego uszkodzenia zarówno po stronie modułu jak i manipulatora, a jedynie rozłączenie elementów. W przypadku odłączenia manipulatora od modułu system musi wygenerować alarm sygnalizowany na tych samych urządzeniach co w przypadku wezwania wygenerowanego przez pacjenta. W projekcie przewidzieć doposażenie manipulatorów w uchwyty montowane na ścianie umożliwiające przyczepienie manipulatora w momencie sprzątania łóżka i gdy na łóżku nie leży pacjent oraz klipsy umożliwiające przyczepienie manipulatora np. do pościeli.

W łazienkach dla pacjentów przy drzwiach zaprojektować i zamontować dwuprzyciskowy kasownik łazienkowy oraz przy toalecie i w prysznicu moduły pociągowe. Linki w modułach pociągowych mają mieć budowę zabezpieczającą moduł przed trwałym uszkodzeniem przy zbyt silnym pociągnięciu (przywrócenie poprawnego działania elementu musi być możliwe bez użycia jakiegokolwiek narzędzia i wiedzy technicznej). Urządzenia zainstalowane w łazienkach/wc są przypisane do konkretnego pomieszczenia, co pozwala na podanie dokładnej lokalizacji zdarzenia w momencie wygenerowania alarmu. Wymaga się, aby moduły montowane pod prysznicem posiadały klasę szczelności przynajmniej IP44.

W gabinetach zabiegowych zależy przewidzieć na ścianie moduł przywoławczo-kasujący wraz z modułem rozmównym, a nad drzwiami lampę salową. Zapewni to możliwość szybkiej reakcji personelu na nagłe pogorszenie się stanu zdrowia pacjenta znajdującego się w trakcie czynności zabiegowych np. poprzez wezwanie zespołu resuscytacyjnego. Specyfikacja funkcjonalna identyczna jak dla odpowiednich modułów przeznaczonych dla sal chorych.

System ma umożliwiać programowanie przycisków w modułach przyzywowych w sposób elastyczny tzn. dla danego modułu lub grupy modułów umożliwia przypisanie indywidualnego zdarzenia zarówno przy naciśnięciu, naciśnięciu i przytrzymaniu oraz pozwala uzależnić przypisanie zdarzenia od stanu modułu – po uaktywnieniu jednego z przycisków drugi może zachowywać się inaczej aniżeli w przypadku, gdy żaden z przycisków wcześnie nie został wciśnięty - możliwość wygenerowania wezwania lekarza możliwe jest wyłącznie w przypadku wcześniejszego zaznaczenia obecności pielęgniarki.

System przyzywowy oraz zintegrowany z nim system IP-DECT musi być w pełni monitorowany pod względem poprawnego działania. Zarówno pojedyncze moduły jak i cały system wraz z infrastrukturą (włączając w to stacje bazowe, przełączniki sieciowe i zasilanie) muszą podlegać ciągłej i automatycznej kontroli przez Platformę PSIM. W przypadku wykrycia jakiejkolwiek nieprawidłowości informacja taka powinna być widoczna na wizualizacji dostępniej dla działu technicznego z pełną informacją o miejscu i typie awarii. Dodatkowo informacja o awarii musi być również wyświetlana na wizualizacji systemu przyzywowego w odpowiednim punkcie pielęgniarskim.

Dla celów komunikacji bezprzewodowej muszą być zainstalowane stacje bazowe IP-DECT posiadające przynajmniej 8 kanałów rozmównych oraz niezależny (nieblokowalny) kanał dla przesyłania wiadomości o alarmach. Ilość stacji bazowych DECT musi zapewniać możliwość komunikacji głosowej i tekstowej na terenie całego obiektu.

Dla celów dystrybucji informacji oraz komunikacji głosowej w całym obiekcie zaprojektować oraz wykonać łączność bezprzewodową IP-DECT. Dla projektu przewiduje się dostarczenie 12 telefonów bezprzewodowych. Telefony bezprzewodowe DECT poza funkcją terminali zdarzeń z systemu przyzywowego muszą zapewniać pełną komunikację głosową pomiędzy personelem szpitala (zarówno tym wyposażonym w telefony bezprzewodowe jak i używającym dowolnego telefonu podłączonego do centrali telefonicznej szpitala). Telefony bezprzewodowe muszą również być zintegrowane z systemem interkomowym oraz systemem kontroli dostępu w taki sposób, aby wywołania z poszczególnych interkomów można było odbierać na telefonach bezprzewodowych oraz bezpośrednio z telefonu otwierać drzwi zabezpieczone systemem kontroli dostępu.

Do realizacji funkcji komunikacji głosowej system musi uwzględniać bramę głosową, która ma być zintegrowana z istniejącym systemem komunikacji głosowej w szpitalu poprzez łącze SIP Trunk lub trakt ISDN PRA oraz musi umożliwiać zalogowanie innych elementów komunikacyjnych dostarczonych przy realizacji niniejszego projektu.

Elementy systemu przyzywowego i komunikacji bezprzewodowej mają być zasilane przy wykorzystaniu standardu PoE, co umożliwi ich pełne monitorowanie oraz centralne podtrzymanie przy braku zasilania.

Wymagania funkcjonalne Platformy PSIM dla systemu przyzywowego:

* wizualizacja wezwań / alarmów na podkładzie oddziału
* wizualizacja kolejki wezwań / alarmów do obsługi z opisem miejsca, typu, czasu wygenerowania oraz czasu, jaki upłynął od momentu jego wygenerowania
* generowanie zdarzeń obsługiwanych identycznie jak zdarzenia pochodzące z samego systemu przyzywowego
* wysyłanie powiadomień na telefony IP-DECT
* podgląd obrazu z kamer zainstalowanych na oddziale oraz możliwość włączania / wyłączania rejestracji obrazu wybranej kamery (wymagane odpowiednie uprawnienia)
* raportowanie z możliwością wykonywania zestawień ilościowych (m.in. ilość odpowiedniego typu wezwań dla danej lokalizacji) oraz jakościowych (analiza czasowa reakcji personelu, czasu obsługi, łącznego czasu alarmu)

Wymagania techniczne dla elementów systemu przyzywowego i komunikacji bezprzewodowej:

Moduł przyłóżkowy:

* minimum 3 różnokolorowe przyciski, podświetlane oraz sygnalizujące wciśnięcie
* unikalny adres oraz jednoznaczna identyfikacja w skali całego systemu przywoławczego
* wbudowane szybkozłącze umożliwiające podłączenie manipulatora
* wbudowane złącze umożliwiające podłączenie modułu głosowego
* klasa szczelności minimum IP40.

Moduł głosowy:

• minimum 2 wbudowane głośniki, wzmacniacz oraz mikrofon

• dwukolorowa dioda wskazująca kierunek transmisji

• klasa szczelności minimum IP40.

Moduł przywoławczo – kasujący:

* minimum 3 różnokolorowe przyciski, podświetlane oraz sygnalizujące wciśnięcie
* unikalny adres oraz jednoznaczna identyfikacja w skali całego systemu przywoławczego
* wbudowane złączę umożliwiające podłączenie modułu głosowego
* klasa szczelności minimum IP40.

Moduł toaletowy pociągowy:

* unikalny adres oraz jednoznaczna identyfikacja w skali całego systemu przywoławczego
* linka o długości minimum 2 m umożliwiająca wezwanie personelu poprzez pociągnięcie
* klasa szczelności minimum IP44.

Lampka salowa:

* 3 niezależne, różnokolorowe źródła światła oparte na technologii LED
* niezależnie programowany sygnał dźwiękowy
* unikalny adres oraz jednoznaczna identyfikacja w skali całego systemu przywoławczego.

Manipulator:

* 1 przycisk (wezwanie), podświetlany, sygnalizujący wciśnięcie
* 2 przyciski umożliwiające sterowanie 2 niezależnymi źródłami światła
* złącze odporne na wyrwanie
* 2 metrowy przewód
* klasa szczelności minimum IP67
* możliwość dezynfekowania poprzez zanurzenie w płynie dezynfekującym.

Kasownik toaletowy:

* minimum 2 różnokolorowe przyciski, podświetlane oraz sygnalizujące wciśnięcie
* unikalny adres oraz jednoznaczna identyfikacja w skali całego systemu przywoławczego
* klasa szczelności minimum IP40.

Stacje bazowe IP-DECT:

* + Protokoły

Obsługa protokołu SIP

Obsługa protokołu H.323 wersja 4 (z H.223, H.235, H.245)

Obsługa protokołu SRTP

* + Zasilanie

PoE (Power over Ethernet)

48V DC

* + Standardy i normy

DECT GAP/CAP

EN 300 444 N.35

EN 301 406

EN 60950-1

EN 301 489-6

* + Kodowanie

G.711 A-law

G.723.1

G729A i AB

* + Funkcjonalności

8 kanałów rozmównych

1 dedykowany kanał do przesyłania wiadomości i alarmów

Konfiguracja i administracja przez przeglądarkę internetową

Podłączenie do centrali telekomunikacyjnej IP PBX poprzez sieć LAN

Obsługa powiadomień interaktywnych

Telefony bezprzewodowe DECT:

* + Parametry fizyczne

Kolorowy wyświetlacz TFT min. 30×40mm

Waga max. 120g (z baterią)

Bateria typu Li-Po

Klawiatura numeryczna

3 programowalne klawisze funkcyjne

Bluetooth

* + Zasilanie

Ładowarka biurkowa

* + Standardy i normy

DECT GAP/CAP

EN 300 444 N.35

EN 301 406

EN 60950-1

EN 301 489-6

* + Parametry środowiskowe

Szczelność IP44

Odporność na działanie pól elektromagnetycznych: 3 V/m EN61000-4-3.

Odporność na wyładowania elektrostatyczne:

wyładowanie kontaktowe 4 kV, wyładowanie w powietrzu 8 kV (EN61000-4-2).

Odporność na upadki z wys. 1,5m (zgodnie z normą IEC 60068-2-32)

* + Funkcjonalności

MENU w języku polskim

Centralne zarządzanie przez przeglądarkę WWW (konfiguracja oraz upgrade)

Centralna książka telefoniczna (bez ograniczeń)

Lista połączeń (min. 25)

Pełen roaming i handover (płynne przełączanie pomiędzy stacjami bazowymi IP-DECT bez utraty połączenia)

Obsługa powiadomień interaktywnych (wiadomości tekstowych z funkcją odbioru lub odrzucenia oraz priorytetyzacji).

Brama głosowa :

Wysokość 1U

Montaż w szafie 19’’

Zasilanie PoE – 802.3af

Brak elementów ruchomych, mechanicznych – wiatraki

5 x Interfejs BRI

2 x Gigabit-Ethernet: 1000-BASE-T

Zasilanie PoE zgodnie z IEEE 802.3af, Class 3

Energy Efficient zgodnie z IEEE 802.3az

Obsługa G.711 A-law / µ-law,

Obsługa G.722,

Obsługa G.723.1 (5.3),

Obsługa G.729A

Opus-NB z VAD (Voice Activity Detection), CNG (Comfort Noise Generation)

Dynamic Jitter Buffering,

Kompensacja echa: G.168

Wsparcie dla modemu

Czas restartu nie dłuższy niż 20 sekund

Protokół PPPoE, manualne/automatyczne nawiązanie połączenia po Start

PPTP do 4 tuneli jednocześnie, Szyfrowanie MPPE

NAT, H.323-NAT, STUN, TURN

RSTP, EAP-TLS/EAP-MD5 zgodnie z IEEE 802.1x

W celu zapewnienia maksymalnego bezpieczeństwa system komunikacji bezprzewodowej IP-DECT musi zapewniać łączność pomiędzy użytkownikami telefonów bezprzewodowych oraz przesyłanie wiadomości interaktywnych również w przypadku niedostępności lub awarii centrali telefonicznej.

System komunikacji bezprzewodowej IP-DECT należy zintegrować z systemem przyzywowym w taki sposób, aby możliwe było odbieranie alarmów i powiadomień interaktywnych generowanych przez pacjentów na zaawansowanych telefonach bezprzewodowych oraz realizowanie połączeń głosowych pomiędzy pacjentem a personelem wyposażonym w telefon bezprzewodowy.

System komunikacji bezprzewodowej należy zintegrować z przewidzianą w ramach realizacji projektu Platformą Integracyjną w celu zarządzania zdarzeniami (odbierania i potwierdzania obsługi) pochodzącymi z systemów zintegrowanych na tej platformie.

Telefony bezprzewodowe systemu IP-DECT mają być docelowo zalogowane do bramy głosowej przewidzianej w ramach systemu przyzywowego.

* 1. **System monitoringu wizyjnego CCTV**

Dla obserwacji ciągów komunikacyjnych oraz terenu zewnętrznego obiektu zaprojektowano system monitoringu wizyjnego CCTV w oparciu o technologię TCP/IP. System do transmisji sygnałów wizyjnych będzie wykorzystywał okablowanie sieci LAN.

System telewizji dozorowej CCTV objęte zostaną:

- wejścia do budynku, wjazd na teren,

- elewacja budynku,

- ciągi komunikacyjne.

Kamery zasilane będą poprzez PoE. Dotyczy to zarówno kamer wewnętrznych jak i zewnętrznych. W tym celu przewiduje się umieszczenie w punktach dystrybucyjnych, przełączników z odpowiednią mocą do zasilania kamer.

System będzie składał się z następujących elementów:

• rejestrator sieciowy IP

• kamery kopułkowe wewnętrzne IP

• kamery tubowe IP z obiektywami

• kamery IP 360 stopni.

Rejestratory systemu telewizji dozorowej mają zostać umieszczone w szafie SER w serwerowni. Wszystkie kamery podłączone zostaną do najbliższych punktów dystrybucyjnych, do przełączników 1Gbit z zasilaniem PoE. Połączenia szkieletowe pomiędzy przełącznikami, a rejestratorami muszą być wykonane w technologii 1Gbit lub więcej i powinny stanowić oddzielną logiczną lub fizyczną podsieć. Połączenia rejestratorów ze stacjami podglądowymi muszą być również wykonane w technologii 1Gbit.

Zaprojektowane oprogramowanie zarządzające posiada interfejs graficzny składający się z odrębnych paneli umożliwiających elastyczne dostosowanie GUI do potrzeb użytkownika o następującej minimalnej funkcjonalności: włączanie/wyłączanie dowolnych paneli w widoku, autoukrywanie nieaktywnych paneli, łączenie paneli, dokowanie do krawędzi, zagnieżdżanie paneli w jeden złożony panel z subpanelami dostępnymi w formie zakładek, przypisywanie układu paneli do konkretnego konta użytkownika.

Oprogramowanie zarządzające ma umożliwiać pracę w rozproszonej architekturze klient-serwer umożliwiającej rozdzielenie funkcji nagrywania i podglądu strumieni.

Wymaga się, by oprogramowanie zarządzające zapewniało możliwości konfiguracji dostępnych funkcji i ich działania. Wymagana jest, co najmniej następująca funkcjonalność:

* tworzenie nieograniczonej programowo liczby grup użytkowników z możliwością nadania odrębnych uprawnień każdej z grup
* tworzenie nieograniczonej programowo liczby kont użytkowników w ramach każdej grupy, zabezpieczonych odrębnymi hasłami
* tworzenie nieograniczonej programowo liczby kont użytkowników domenowych w oparciu o usługę Active Directory, przypisanie do każdej grupy użytkowników (w szczególności do każdego konta użytkownika) układu (widoku) paneli programu
* przypisanie do każdej grupy użytkowników (w szczególności do każdego konta użytkownika) dostępnych urządzeń IP (kamer i serwerów) spośród wszystkich zdefiniowanych
* przypisanie do każdej grupy użytkowników (w szczególności do każdego konta użytkownika) uprawnień do używania poszczególnych modułów (paneli) programu
* przypisanie do każdej grupy użytkowników (w szczególności do każdego konta użytkownika) uprawnień do otrzymywania informacji (logów) systemowych o zdarzeniach pochodzących od samej aplikacji jak i urządzeń
* przypisanie do każdej grupy użytkowników nieograniczonej programowo liczby masek prywatności definiowanych dla każdego strumienia wideo
* przypisanie do każdej grupy użytkowników uprawnień do cyfrowego zbliżenia obrazu, definiowanych dla każdego strumienia wideo
* przypisanie do każdej grupy użytkowników maksymalnej prędkości kopiowania strumieni do formatu avi
* przypisanie do każdej grupy użytkowników okresu, z jakiego dostępne będą nagrania w trybie odtwarzania
* przypisanie grupie użytkowników prawa do wybranych okien wideo.

Oprogramowanie powinno zapewniać możliwość automatyzacji reakcji systemu w przypadku wystąpienia zdarzeń oraz zarządzania informacjami o zdarzeniach zaistniałych w systemie. Wymagana jest co najmniej następująca funkcjonalność:

* definiowanie nieograniczonej programowo ilości scenariuszy automatycznych reakcji systemu na zdarzenia z możliwością zdefiniowania, które zdarzenia wywołują reakcję
* zdefiniowanie harmonogramu zdarzeń systemowych
* przechwytywanie, zapisywanie oraz wyświetlanie informacji (logów) pochodzących z urządzeń IP (kamer i serwerów), jak również pochodzących od samej aplikacji lub informujących o stanie platformy komputerowej, na której zainstalowana jest aplikacja
* wyświetlanie zdarzeń na bieżąco w specjalnie przeznaczonym do tego oknie programu
* zapisywanie logów do bazy
* przeszukiwanie listy logów zapisanych w bazie.

System rejestracji obrazu musi być zintegrowany z Platformą PSIM w celu zarządzania zdarzeniami za pomocą protokołu umożliwiającego sterowanie, monitorowanie oraz pobieranie zdarzeń.

Minimalne wymagania dla kamer 360 stopni:

• kamera sieciową (kamerą IP) wandaloodporna z obiektywem „rybie oko” (360 stopni) o ogniskowej 1,6mm i aperturze F2.0.

• moduł kamerowy zintegrowany z obiektywem ze stałą ogniskową

• przetwornik SONY CMOS 1/1.8” o rozdzielczości 6Mpx

• dwa tryby pracy: kolorowy i czarno-biały -zmiana trybu ma być realizowana za pomocą mechanicznie przesuwanego filtru podczerwieni

• zintegrowany oświetlacz podczerwieni wykorzystujący diody LED o zasięgu co najmniej 10m

• transmisja obrazu oraz dźwięku w sieci Ethernet z możliwością jego podglądu na standardowej przeglądarce internetowej oraz dedykowanym oprogramowaniu klienckim

• przetwornik obrazu typu CMOS o rozdzielczości 6Mpx z generowanym obrazem o rozdzielczości nie mniejszej niż 3072x2048 pikseli

• czułość nie gorsza niż:

o lx/F2.0 - tryb kolorowy (DSS 0,2s)

o 0lx/F2.0 – tryb cz/b (1/50 s) (Z włączonym IR)

• funkcja wydłużonej migawki z możliwością regulacji w zakresie do 0,2s

• funkcja cyfrowego filtru szumu 2D i 3D

• regulacja następujących parametrów obrazu: jasność, kontrast, ostrość, nasycenie koloru

• transmisja dwóch niezależnych strumieni sieciowych wideo z możliwością regulacji ich parametrów

• wybór algorytmu kompresji wideo spośród: H.264, MJPEG(w przypadku pracy wielostrumieniowej powinna być możliwość ustawienia różnych algorytmów kompresji dla przynajmniej dwóch strumieni)

• transmisja: minimum 15 kl/s dla rozdzielczości 3072 X 2048, dla pierwszego strumienia przy jednoczesnych 25 kl/s w rozdzielczości D1 (704 x 480) dla strumienia drugiego.

Minimalne wymagania dla kamer tubowych:

• moduł kamerowy zintegrowany z obiektywem ze zmienną ogniskową

• przetwornik CMOS 1/3” o rozdzielczości 4 MPX - dwa tryby pracy: kolorowy i czarno-biały (zmiana trybu ma być realizowana za pomocą mechanicznie przesuwanego filtru podczerwieni)

• zintegrowany oświetlacz podczerwieni wykorzystujący diody LED o zasięgu co najmniej 20m

• transmisja obrazu w sieci Ethernet z możliwością jego podglądu na standardowej przeglądarce internetowej oraz dedykowanym oprogramowaniu klienckim

• przetwornik obrazu typu CMOS o rozdzielczości 4 MPXz generowanym obrazem o rozdzielczości nie mniejszej niż 2688x1520 pikseli

• minimalna czułość nie gorsza niż

o 0.27 lx/F1.4 - tryb kolorowy

o 0.14 lx/F1.4 - tryb kolorowy (DSS)

o 0lx/F1.4 – tryb cz/b, włączony oświetlacz podczerwieni

• przełączanie się między trybami kolor i czarno-biały:

o automatycznie, w zależności od poziomu oświetlenia i ustawień poziomu przełączania

o ręcznie, przez operatora

o czasowo, według harmonogramu

• funkcja szerokiego zakresu dynamiki (WDR) z możliwością jej wyłączenia

• funkcja cyfrowego filtru szumu (DNR)

• ręczne i automatyczne sterowanie migawką

• obiektyw o ogniskowej od 3.0 do 12mm i aperturze F1.4

• transmisja dwóch strumieni sieciowych wideo z możliwością regulacji ich parametrów

• kompresja wideo: H.264 i MJPEG (w przypadku pracy wielostrumieniowej powinna być możliwość ustawienia różnych algorytmów kompresji dla przynajmniej dwóch strumieni)

• transmisja:

o w trybie jednostrumieniowym: minimum 20 kl/s dla rozdzielczości 2688x1520, 2560x1440

o w trybie jednostrumieniowym: minimum 25 kl/s dla rozdzielczości 2304x1296

o w trybie wielostrumieniowym: minimum 30 kl/s dla rozdzielczości 1920x1080 dla pierwszego strumienia przy jednoczesnych 30 kl/s w rozdzielczości 1280x720 dla strumienia drugiego

• strumień w trybie VBR oraz CBR z możliwością regulacji rozdzielczości, ilości klatek, wielkości strumienia, wartości GOP

• transmisja w protokole RTP/RTSP

• autoryzacja hasłem dostępu do podglądu strumienia wideo i ustawień kamery przez przeglądarkę

• detekcja ruchu o funkcjonalności:

o możliwość elastycznego zdefiniowania strefy detekcji w oparciu o siatkę 18 x 22

o możliwość zdefiniowania poziomu czułości

o możliwość ustawienia czasu braku reakcji na kolejno pojawiające się naruszenia (detekcje)

o możliwość wysłania emaila z załącznikiem po wystąpieniu detekcji

o możliwość uruchamiania funkcji w oparciu o zdefiniowane wcześniej harmonogramy czasowe

• interfejssieciowy Ethernet 10/100Mbit/s, złącze RJ-45

• zasilanie kamery: 12VDC, 24VAC lub PoE

• obudowa aluminiowa, klasa szczelności IP66

Minimalne wymagania dla kamer kopułkowych:

• moduł kamerowy zintegrowany z obiektywem ze zmienną ogniskową

• przetwornik CMOS 1/3” o rozdzielczości 4 MPX - dwa tryby pracy: kolorowy i czarno-biały (zmiana trybu ma być realizowana za pomocą mechanicznie przesuwanego filtru podczerwieni)

• oświetlacz podczerwieni wykorzystujący diody LED o zasięgu co najmniej 15m

• transmisja obrazu w sieci Ethernet z możliwością jego podglądu na standardowej przeglądarce internetowej oraz dedykowanym oprogramowaniu klienckim

• autoryzacja hasłem dostępu do podglądu strumienia wideo i ustawień kamery przez przeglądarkę

• przetwornik obrazu typu CMOS o rozdzielczości 4 MPX generujący obraz o rozdzielczości nie mniejszej niż 2688x1520 pikseli

• czułość nie gorszą niż:

o 0.27 lx/F1.4 - tryb kolorowy

o 0.14 lx/F1.4 - tryb kolorowy (DSS)

o 0lx/F1.4 – tryb cz/b, włączony oświetlacz podczerwieni

• możliwość przełączania się między trybami kolorowym i czarno-białym:

o automatycznie, w zależności od poziomu oświetlenia i ustawień poziomu przełączania

o ręcznie, przez operatora

o czasowo, według harmonogramu

• szeroki zakres dynamiki (WDR)z możliwością jego wyłączenia

• funkcja cyfrowego filtru szumu (DNR)

• ręczne i automatyczne sterowanie migawką

• obiektyw o ogniskowej od 3.0 do 12mm i aperturze F1.4

• transmisja dwóch strumieni sieciowych wideo z możliwością regulacji ich parametrów

• algorytmy kompresji wideo: H.264 i MJPEG (w przypadku pracy wielostrumieniowej możliwość ustawienia różnych algorytmów kompresji dla przynajmniej dwóch strumieni)

• transmisja:

o w trybie jednostrumieniowym: minimum 20 kl/s dla rozdzielczości 2688x1520, 2560x1440

o w trybie jednostrumieniowym: minimum 25 kl/s dla rozdzielczości 2304x1296

o w trybie wielostrumieniowym: minimum 30 kl/s dla rozdzielczości 1920x1080 dla pierwszego strumienia przy jednoczesnych 30 kl/s w rozdzielczości 1280x720 dla strumienia drugiego

• strumienie w trybie VBR oraz CBR z możliwością regulacji rozdzielczości, ilości klatek, wielkości strumienia, wartości GOP

• transmisja w protokole RTP/RTSP

• możliwość zdefiniowania co najmniej 5 stref prywatności

• detekcja ruchu o funkcjonalności:

o możliwość elastycznego zdefiniowania strefy detekcji w oparciu o siatkę 18 x 22

o możliwość zdefiniowania poziomu czułości

o możliwość ustawienia czasu braku reakcji na kolejno pojawiające się naruszenia (detekcje)

o możliwość wysłania emaila z załącznikiem po wystąpieniu detekcji

o możliwość uruchamiania funkcji w oparciu o zdefiniowane wcześniej harmonogramy czasowe

• analiza obrazu: wykrywanie sabotażu kamery, wykrywanie zniknięcia obiektu, wykrywanie przekroczenia linii przez obiekt, wykrywanie wkroczenia obiektu do określonej strefy, wykrywanie przekroczenia określonych dwóch linii przez obiekt, wykrywanie wałęsania, wykrywanie tłumu, wykrywanie poruszania się z niedozwoloną prędkością, wykrywanie poruszania się w niedozwolonym kierunku, wykrywanie niedozwolonego parkowania

• interfejsy wejść/wyjść:

o Ethernet 10/100Mbit/s, złącze RJ-45

o wejścia alarmowe: 1 wejście, zwarcie lub rozwarcie wykrywane jako zadziałanie; wybór trybu NO/NC z poziomu menu kamery

o wyjścia alarmowe: 1 wyjście przekaźnikowe

o gniazdo kart pamięci: 1 gniazdo kart microSD/SDHC/SDXC

• zasilanie kamery: 12VDC, 24VAC lub PoE

• obudowa o podwyższonej wytrzymałości mechanicznej (IK 10), aluminiowa, stopień ochrony IP66

• możliwość 3-osiowej regulacji położenia modułu kamerowego względem obudowy

Dla potrzeb bieżącego podglądu wraz z systemem monitoringu projekt przewiduje stacje wyposażone w 2 monitory min. 24”. Na stacji musi zostać zainstalowane oprogramowanie umożliwiające podgląd z kamer oraz sterowanie systemem.

Minimalne wymagania techniczne dla stacji poglądowej:

• procesor: min. klasy Intel Core i5 4460 3,2 GHz 6 MB

• pamięć RAM: zainstalowane min. 8 GB DDR3 1600 MHz z możliwością rozszerzenia do 16 GB

• dysk twardy: min. 1x1000 GB

• karta graficzna: nVIDIA® GeForce GTX750 Ti 2048 MB lub lepsza

• napęd optyczny - Tak Multi DVD+/-RW/RAM SATA

• karta dźwiękowa zintegrowana

• karta sieciowa: zintegrowana 10/100/1000 Mbit/s

• liczba złączy HDMI - 2 sztuki

• zainstalowany system operacyjny WIN 7 Pro PL

Minimalne wymagania techniczne dla stacji roboczej:

• procesor: min. klasy Intel Core i5 4460 3,2 GHz 6 MB

• pamięć RAM: zainstalowane min. 8 GB DDR3 1600 MHz z możliwościąrozszerzenia do 16 GB

• dysk twardy: min. 2x1000 GB SSHD w RAID1

• karta graficzna: nVIDIA® GeForce GTX750 Ti 2048 MB lub lepsza

• napęd optyczny - Tak Multi DVD+/-RW/RAM SATA

• karta dźwiękowa zintegrowana

• karta sieciowa: zintegrowana 10/100/1000 Mbit/s

• liczba złączy HDMI - 2 sztuki

• zainstalowany system operacyjny WIN 7 Pro PL.

Minimalne wymagania techniczne dla serwera rejestrującego:

• obudowa typy RACK

• 1 dysk 2,5” SATA SSD systemowy

• 12 dysków HDD 3,5” 4TB SAS Serwerowe, przeznaczone do rejestracji 24/7

• wyjścia monitorowe: 1x Micro HDMI (przejściówka w zestawie), 1 x DVI, 1 x Mini-Display Port

• wyjścia audio: 1 x liniowe (jack 3,5mm), 1 x HDMI

• 2 x Ethernet - złącze RJ-45, 10/100/1000 Mbit/s

• przepustowość do 250Mb/s łącznie ze wszystkich kamer

• przepustowość do 250Mb/s łącznie do wszystkich stacji klienckich

• 2 x USB 3.0 i 8 x USB 2.0

• wbudowane 2 redundantne zasilacze 230VAC/920W (Platinium Level 94%+)

• obudowa RACK 19“ 2U 89(wys)x437(szer)x648(gł)

• klawiatura i mysz komputerowa

• temperatura pracy 10 °C ~ 35 °C.

## Platforma PSIM

* + 1. **Opis ogólny**

W celu integracji systemów bezpieczeństwa (tj. SSP,DSO, SKD, SSWiN, CCTV IP, DSO) , systemu przyzywowego z komunikacją bezprzewodową, systemu interkomowego, urządzeń aktywnych oraz systemu automatyki budynkowej projekt przewiduje dostarczenie i wdrożenie Platformy PSIM (Physical Security Information Management), która będzie umożliwiała zarządzanie zdarzeniami pochodzącymi ze wszystkich zintegrowanych systemów oraz infrastruktury IT.

Platforma ma działać w architekturze Klient – Serwer, a interfejs użytkownika ma być w pełni polskojęzyczny.

Serwer Platformy Integracyjnej ma być zainstalowany w GPD,a jego głównymi zadaniami mają być:

* zbieranie i archiwizowanie danych z systemów podlegających integracji
* zarządzanie i dystrybuowanie zebranych i przetworzonych informacji zgodnie ze zdefiniowanymi schematami obsługi
* zarządzanie użytkownikami
* komunikacja przez kanały WWW, IP-DECT, e-mail i SMS
* generowanie raportów oraz udostępnianie informacji dla aplikacji Klienta

Zarówno kanał WWW, jak i IP-DECT muszą być kanałami interaktywnymi tzn. muszą umożliwiać akceptację/odrzucenie zdarzenia (przyjęcie lub odrzucenia zdarzenia do obsługi) oraz sterowanie zintegrowanymi systemami. Interaktywność ma umożliwiać eskalację (przesłanie) zdarzenia wymagającego reakcji do innego użytkownika lub grupy użytkowników w przypadku braku obsługi w zdefiniowanym czasie.

Zakres funkcjonalny Platformy można podzielić na następujące moduły:

|  |  |  |
| --- | --- | --- |
| **Moduł** | **Zakres** | **Główny użytkownik** |
| Bezpieczeństwo mienia | Wizualizacja i zarządzanie zdarzeniami z systemów bezpieczeństwa. | Pracownicy ochrony |
| Techniczny | Zbieranie informacji, wizualizacja i obsługa zdarzeń związanych z poprawnością działania urządzeń i systemów zintegrowanych w ramach Platformy. | Dział techniczny |
| Medyczny | Wizualizacja i zarządzanie zdarzeniami z systemu przyzywowego, obsługa przejść objętych systemem KD oraz podgląd z wyznaczonych kamer. | Personel medyczny |
| Infrastruktura | Monitorowanie i obsługa zdarzeń związanych z infrastrukturą i urządzeniami IP. | Dział IT |

Aplikacja Klienta musi być w pełni polskojęzyczna, dostępna przez przeglądarkę WWW i nie może wymagać instalowania żadnego dedykowanego oprogramowania na stanowiskach końcowych. Musi umożliwiać dostęp do wszystkich funkcji Platformy PSIM:

• wizualizacji

• generowania zdarzeń

• sterowania

• zarządzania

• raportowania.

* + 1. **Komunikacja z systemami**

 Projekt zakłada, że Platforma PSIM będzie się komunikowała z systemami: kontroli dostępu, SSWiN, CCTV, SAP, IP-DECT, systemem przyzywowym, interkomowym przy wykorzystaniu dedykowanych protokołów, a z systemem BMS za pomocą protokołu OPC. Komunikacja z infrastrukturą IP ma się odbywać z wykorzystaniem protokołu SNMP. Projekt, dla realizacji założonej funkcjonalności, dodatkowo przewiduje wykorzystanie otwartych protokołów jak ICMP, SIP, LDAP oraz integrację z bazami danych. Dla przyszłej integracji z istniejącym na obiekcie oprogramowaniem HIS Platforma musi umożliwiać integrację przy pomocy protokołu HL7.

* + 1. **Wizualizacja**

Projekt przewiduje, że Platforma będzie umożliwiała wizualizację na podkładach budynku 2D i 3D (w zależności od zaimplementowanego podkładu) oraz na schematach logicznych systemów. W przypadku wizualizacji na podkładzie budynku, aplikacja musi umożliwiać wizualizację zarówno pojedynczego elementu danego systemu (np. w formie ikony) jak i obszaru/strefy, w której pojawiło się zdarzenie. Prezentowane na podkładach treści muszą być dostępne na wielu poziomach szczegółowości (budynek/piętro/oddział) z możliwością przejścia do schematu logicznego systemu, na którym będzie zaznaczone urządzenie, z którego zdarzenie zostało wygenerowane. Dodatkowo, wszystkie aktywne zdarzenia mają być prezentowane w formie listy. Lista ta ma zawierać: typ i status zdarzenia (nowe, w obsłudze, zakończone), datę i godzinę jego wygenerowania, opis lokalizacji lub urządzenia, priorytet, czas i szczegóły związane ze zmianą statusu zdarzenia. Z poziomu listy ma być również możliwość przejścia do interfejsu prezentującego wszystkie informacje związane ze zdarzeniem, jego obsługą i dystrybucją (przyjęcie, akceptacja(wraz z ich czasami), treści wysłane na poszczególne kanały komunikacyjne oraz użytkownicy (jeżeli są zidentyfikowani) biorący udział w obsłudze zdarzenia itp.). Z poziomu interfejsu wizualizacji oraz listy zdarzeń użytkownik będzie miał dostęp do takich funkcji jak przyjęcie zdarzenia do obsługi, zakończenie obsługi i archiwizacja w zależności od przydzielonych mu wcześniej uprawnień. Na każdym z etapów będzie możliwość dopisania komentarza oraz przydzielenia zdarzenia do odpowiedniej wcześniej zdefiniowanej kategorii (alarm, błąd użytkownika, działanie serwisowe itd), która będzie wykorzystywana podczas raportowania i widoczna w historii wszystkich zdarzeń (wraz z możliwością odpowiedniego odfiltrowania). Na każdym etapie obsługi zdarzenia zaprojektowane rozwiązanie umożliwia załączenie indywidualnej instrukcji postępowania.

* + 1. **Generowanie zdarzeń / sterowanie**

Projekt zakłada, że z poziomu aplikacji Klienta możliwe będzie:

* generowanie wcześniej zdefiniowanych zdarzeń, których obsługa będzie przebiegała zgodnie z zaprojektowanym schematem obsługi
* wysyłanie wiadomości tekstowych do użytkownika/grupy użytkowników na telefony GSM oraz DECT w formie interaktywnych wiadomości tekstowych z możliwością ich akceptacji lub odrzucenia, co będzie widoczne na aplikacji.

 Funkcjonalność sterowania ma dawać możliwość m.in. uzbrajania/rozbrajania stref, załączania/wyłączania urządzeń, zwalniania drzwi objętych SKD, itp.

* + 1. **Zarządzanie**

Zarządzanie (administracja) musi być możliwe w następujących obszarach:

Zarządzanie użytkownikami i grupami użytkowników. Dla każdego użytkownika system musi umożliwiać zdefiniowanie przynajmniej następujących parametrów: imię, nazwisko, dział/oddział, stanowisko/funkcję, numer karty identyfikacyjnej systemu kontroli dostępu, dostępne kanały komunikacji (numer telefonu DECT, numer telefonu GSM, e-mail), login i hasło do aplikacji WWW, zakres dostępnych funkcji (podgląd, przyjmowanie do obsługi, archiwizacja, raportowanie), systemów i lokalizacji. System musi umożliwiać przypisanie każdego użytkownika do grupy lub grup użytkowników. Oprócz synchronizacji użytkowników z zaprojektowanymi systemami, serwer ma umożliwiać synchronizację z wykorzystaniem mechanizmów ODBC lub OLE DB oraz z wykorzystaniem protokołu LDAP. Z wykorzystaniem zgromadzonych danych aplikacja musi umożliwiać przygotowywanie i przechowywanie widoków identyfikatorów, które następnie mogą być wydrukowane przy pomocy drukarki dostarczonej w ramach realizacji zakresu SKD.

Zarządzanie komunikacją z systemami podlegającymi integracji. System ma zapewniać interfejs umożliwiający zdefiniowanie parametrów niezbędnych do nawiązania połączenia i komunikacji dla każdego z systemów podlegających integracji. Przebieg komunikacji ma być dostępny w formie logów, wraz z możliwością odfiltrowania systemu, czasu, lub kluczowych ciągów z odebranych informacji.

Zarządzanie schematami obsługi zdarzeń. Dla każdego ze zdefiniowanych zdarzeń pochodzących z systemów podlegających integracji, Platforma PSIM musi umożliwiać: zdefiniowanie sposobu wizualizacji, określenie priorytetu, maksymalnego akceptowalnego czasu reakcji i obsługi, zdefiniowanie grupy/grup użytkowników odpowiedzialnych za reakcję, zdefiniowanie grupy/grup eskalacyjnych oraz czasu po jakim eskalacja nastąpi w przypadku braku reakcji, zdefiniowanie treści wiadomości, jaka trafi do użytkowników danych grup określonym kanałem komunikacyjnym (DECT, e-mail, SMS), określenie czy, i w jaki sposób zdarzenie ma mieć wpływ na systemy umożliwiające zewnętrzne sterowanie oraz czy, i do kogo ma trafić raport z obsługi zdarzenia po jego zakończeniu. Wymagane jest, aby do każdego ze zdarzeń istniała możliwość przypisania znacznika, który można wykorzystywać przy wykonywaniu raportów lub filtrowaniu.

Zarządzanie raportami. W tym obszarze projekt zakłada możliwość zdefiniowania dla każdego z raportów harmonogramu automatycznego wysyłania oraz listy odbiorców.

* + 1. **Raportowanie**

Raportowanie ma umożliwiać wykonywanie zestawień czasowych oraz ilościowych. Pod pojęciem zestawień czasowych należy rozumieć m.in. takie raporty, które pokazują czasy reakcji i zakończenia obsługi zdarzenia, porównują je z wcześniej zdefiniowanymi maksymalnymi wartościami.  Raporty ilościowe mają m.in. pokazywać liczbę wystąpień poszczególnych zdarzeń w określonym przedziale czasowym, liczbę zdarzeń obsłużonych zgodnie/niezgodnie z założeniami. Dostęp do generowania i przeglądania raportów musi być zgodny z uprawnieniami nadanymi każdemu z użytkowników (np. pielęgniarka oddziałowa może wykonać raport wyłącznie ze zdarzeń pochodzących z systemu przyzywowego z jej oddziału, a pracownik techniczny ze zdarzeń z wszystkich systemów, ale wyłącznie w zakresie ich właściwego funkcjonowania).

* + 1. **Generowanie zdarzeń / sterowanie**

Projekt zakłada, że z poziomu aplikacji Klienta możliwe będzie:

generowanie wcześniej zdefiniowanych zdarzeń, których obsługa będzie przebiegała zgodnie z zaprojektowanym schematem obsługi

wysyłanie wiadomości tekstowych do użytkownika/grupy użytkowników na telefony GSM oraz DECT w formie interaktywnych wiadomości tekstowych z możliwością ich akceptacji lub odrzucenia, co będzie widoczne na aplikacji.

* + 1. **Moduły Platformy PSIM**

Zaprojektowana Platforma z jednej strony daje umożliwia jednolite i spójne administrowanie użytkownikami i zarządzanie komunikacją z systemami podlegającymi integracji, z drugiej strony umożliwia wydzielenie spójnych funkcjonalnie modułów przez nadanie użytkownikom uprawnień dostępu do odpowiednich zakresów (map wizualizacji, systemów i raportów) i dostosowanie wizualizacji do prezentowanej treści. Projekt zakłada podział Platformy na 3 główne obszary działania (moduły) wspierające pracę: pracowników ochrony mienia (A), personelu technicznego/administracyjnego (B) oraz personelu białego (C).

Moduł (A) będzie dedykowany głównie dla pracowników ochrony i dla niego przewidziano stanowisko komputerowe wyposażone w 27’’ monitor LCD zainstalowany w tym samym miejscu, co stanowiska poglądowe systemu CCTV. Będzie dawał dostęp do zarządzania i wizualizacji wszystkich systemów bezpieczeństwa. Do modułu tego będzie również dostęp z każdego innego komputera podłączonego do właściwej podsieci dzięki przeglądarce WWW i autoryzacji użytkownika z odpowiednimi uprawnieniami. Projekt zakłada integrację Platformy z systemem monitoringu wizyjnego w taki sposób, aby zdarzenia odebrane przez Platformę mogły wpływać na stację poglądową systemu CCTV (znajdującą się w tym samym pomieszczeniu) np. poprzez sposób prezentowania treści. Dodatkowo z poziomu aplikacji WWW przewiduje się możliwość sterowania systemami alarmowym i kontroli dostępu w zakresie uzbrajania/rozbrajania stref, izolowania i blokowania czujek, sterowania przejściami itd.

Moduł monitoringu technicznego (B) jest przeznaczony dla monitorowana istotnych i krytycznych parametrów technicznych systemów podlegających integracji. Będzie on zarządzał i prezentował treści pochodzące ze wszystkich systemów podlegających integracji, głównie w zakresie związanym z ich właściwym funkcjonowaniem. Monitorowanie infrastruktury IP musi umożliwiać zarówno monitorowanie urządzeń przy pomocy protokołu ICMP (ping) jak i SNMP (Trap i Get). Dodatkowo system musi zapewnić integrację za pomocą mechanizmów ODBC lub OLE DB z bazami danych przechowującymi identyfikatory OID urządzeń przynależnych do infrastruktury IP. Aplikacja ma również umożliwiać budowanie zależności pomiędzy urządzeniami w formie hierarchicznej (drzewiastej) odzwierciedlających ich fizyczne połączenia.

Moduł personelu białego (C) jest w głównej mierze przeznaczony dla personelu pielęgniarskiego. Moduł ma za zadanie wspierać ich pracę przez wizualizację i zarządzanie zdarzeniami pochodzącymi z systemu przyzywowego oraz umożliwiać dostęp do kamer monitoringu wizyjnego znajdujących się na danym oddziale. Dostęp do modułu jest przewidziany na każdym oddziale w dyżurce pielęgniarskiej przez przeglądarkę WWW na komputerze dostarczonym w ramach dostawy inwestorskiej .Dla celów raportowych dostęp jest możliwy przez dowolny komputer podłączony do odpowiedniej podsieci, na którym do aplikacji Klienta zaloguje się osoba posiadająca odpowiednie uprawnienia. Bardziej szczegółowy opis tego modułu znajduje się w rozdziale opisującym system przyzywowy i system komunikacji bezprzewodowej.

* + 1. **Redundancja**

Dostarczone rozwiązanie musi zapewniać generowanie kopii zapasowej baz danych, obejmujących konfigurację, oraz zdarzeń i odebranych informacji ze zintegrowanych systemów na niezależnej przestrzeni dyskowej.

Musi mieć zaimplementowane mechanizmy samokontroli oraz raportowania błędów i wysyłania informacji o ich wystąpieniu na telefony DECT, GSM oraz pocztę e-mail. Dodatkowo, serwer musi być monitorowany przez niezależne rozwiązanie sprzętowe z niezależnym podtrzymaniem zasilania przez minimum 24 godziny. Rozwiązanie ma sprawdzać poprawność pracy serwera i przy jego awarii (powodującej niewłaściwe jego działanie lub wręcz przerwanie pracy) umożliwiać wysłanie odpowiedniej informacji na telefony DECT i GSM oraz na e-mail.

**2.6 System sygnalizacji włamania i napadu**

Projekt przewiduje instalację na obiekcie Systemu Sygnalizacji Włamania i Napadu (SSWiN), którego zadaniem jest ochrona wybranych pomieszczeń przed włamaniem lub wejściem osób niepożądanych. Ochrona pomieszczeń będzie realizowana przez zastosowanie dualnych czujek ruchu (podczerwień + mikrofale) oraz manipulatora z wyświetlaczem LCD umożliwiającego uzbrajanie i rozbrajanie strefy. Centrala systemu SSWiN musi być zainstalowana w głównym punkcie dystrybucyjnym i zintegrowana z Platformą PSIM umożliwiając z poziomu interfejsu platformy PSIM uzbrajanie i rozbrajanie poszczególnych stref SSWiN oraz wizualizację stanów poszczególnych stref i elementów detekcyjnych. Dodatkowo Platforma PSIM musi w sposób ciągły monitorować pracę systemu w zakresie monitorowania zasilania, błędów systemowych oraz dostępu to wszystkich zdarzeń. Dzięki integracji SSWiN z SKD projekt zakłada automatyczne uzbrajanie 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).