

**„Warmia i Mazury regionem zjednoczonej Europy”**

**Projekt dofinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Warmia i Mazury na lata 2007-2013 oraz budżetu państwa**

**Załącznik nr 1.1 A do SIWZ**

**Minimalne wymagania techniczne dotyczące budowy systemu ochrony obwodowej dla Portu Lotniczego Olsztyn-Mazury w Szymanach.**

**1. System ochrony obwodowej – opis ogólny**

Należy wykonać system składający się z minimum 14 kamer obrotowych. Należy dobrać takie kamery obrotowe, które zapewnią rozpoznanie z odległości min 150 metrów oraz detekcje z min 400 metrów od miejsca instalacji kamery wg tablic z załącznika C zawartych w PN-EN 50132-7. Wszystkie kamery należy umieścić na słupach o wysokości 6 metrów.

**Kamery należy rozmieścić zgodnie z Rysunkiem nr S001 załączonym do specyfikacji. Słupy dla montażu kamer oraz kanalizacja teletechniczna dla okablowania zostały wykonane na terenie lotniska przez zamawiającego.**

Czas archiwizacji materiału wideo powinien wynosić 30 dni dla wszystkich kamer i zdarzeń oraz 60 dni dla zdarzeń alarmowych. Rejestracja do 30 dni 12,5kl/s dla zdarzeń alarmowych i 1kl/s dla normalnej pracy kamer.

Centrum monitoringu należy zlokalizować w budynku nr 2 (pomieszczenia administracyjne SOL). Zamawiający przygotował pomieszczenie serwerowni W pomieszczeniu należy zainstalować klimatyzację dla utrzymania temperatury wewnętrznej < 25 °C.

W pomieszczeniu serwerowni należy również zamontować:

- a) szafę RACK o wysokości 42U, wyposażoną w panele wentylacyjne. W szafie należy zainstalować UPS minimum 5000VA rejestrator oraz jeden monitor z serwerem dedykowanym dla oprogramowania integrująco-wizualizacyjnego
- b) tablicę rozdzielczą do zasilania szafy RACK i systemu kamer podzielonych na segmenty zasilania

W centrum monitoringu należy zainstalować dwie stacje klienckie, dwie konsole sterujące kamerami 2 monitory o przekątnej ekranu min 42 cale oraz dwa o przekątnej min 24 cale. Monitory muszą być wykonane w standardzie pozwalającym na ich pracę przez 24 godziny 7 dni w tygodniu (wraz z meblami).

System ochrony obwodowej musi zostać zintegrowany z systemem kamer w taki sposób aby naruszenie strefy (maksimum 50 metrowej) ochrony obwodowej spowodowało automatyczne skierowanie najbliższych kamer na odcinek, który wywołał alarm. Obraz alarmowy winien zostać wyświetlony w oknie alarmowym. System musi obsługiwać kolejowanie zdarzeń alarmowych.

Dodatkowo oprogramowanie integrująco-wizualizacyjne powinno graficznie wyznaczyć miejsce naruszenia strefy. Oprogramowanie to również powinno umożliwiać (poprzez wybór kamery na grafice) zarządzanie obrazem z poszczególnych kamer na monitorach systemu CCTV i w razie potrzeby (decyzje podejmie operator) wywołanie dodatkowych zdarzeń w systemie CCTV jak i pozostałych systemach bezpieczeństwa zainstalowanych w obiekcie (np. kontrola dostępu i system sygnalizacji włamania i napadu). Zdarzenia te powinny być realizowane na poziomie programowym.

System ochrony obwodowej należy zbudować w oparciu o czujniki sensoryczne montowane na ogrodzeniu z dokładnością rozpoznania strefy detekcji wynoszącej **maksimum 50 metrów**. Każdy ze sterowników systemu ochrony obwodowej musi posiadać interfejs sieciowy, celem komunikacji w sieci IP.

System musi wykrywać wspinanie się na ogrodzenie oraz jego przecinanie.

System musi wykrywać także zmianę położenia czujników względem powierzchni ziemi w celu wykrycia próby sabotażu polegającej na odchyłaniu lub zdjęciu czujników z ogrodzenia.

System musi być odporny na warunki atmosferyczne takie jak wiatr, deszcz oraz zakłócenia środowiskowe wywoływane np. przez przejeżdżające samochody lub zakłócenia wywołane przez małe zwierzęta.

System powinien być w pełni zintegrowany z systemem CCTV na poziomie programowym.

Przy każdej z kamer należy posadzić na fundamencie betonowym hermetyczną szafę zawierającą wyłączniki nad prądowe, zabezpieczenia przepięciowe, osprzęt światłowodowy oraz switche.

Rozdzielnia winna być wyposażona w wentylację. Instalowane switche muszą posiadać charakterystykę przemysłową. Należy wykonać instalację odgromową i uziemienia słupów.

Do budowy infrastruktury teletechnicznej oraz zasilania należy wykorzystać istniejącą kanalizację teletechniczną. Światłowody należy ułożyć w dodatkowej rurze HDPE.

W ramach zadania należy wykonać projekt wykonawczy.

**Nie przewiduje się integracji ww. systemu z systemem ochrony Terminala, tym nie mniej zamawiający dopuszcza takie rozwiązanie.**

## **2. System ochrony obwodowej – wymagania minimalne dotyczące zastosowanych urządzeń.**

### **2.1 Kamera obrotowa**

Kamera powinna być urządzeniem produkowanym seryjnie przeznaczona do ciągłej pracy w aplikacjach komercyjnych i przemysłowych.

Kamera powinna posiadać minimalną 3 letnią gwarancję producenta.

Produkt powinien zostać wyprodukowany zgodnie z ISO 9001 / EN 29001 oraz ISO 14000.

Urządzenie powinno spełniać standardy elektromagnetyczne: EN55022, EN55024 oraz FCC część 15 – część B.

Kamera powinna posiadać zdolność do bezpiecznego uruchomienia się i pracy w zakresie temperatur od -40 C do +50 C, powinna posiadać klasę obudowy minimum IP66.

Kamera powinna być wyposażona w przetwornik obrazu "full HD" 1920x1080 (2 MP/HDTV 1080p). z sensorem High Definition 16:9 z progresywnym skanowaniem czuły na zakres podczerwieni, obiektów z minimalnie 32-krotnym zoomem optycznym o jasności w zakresie F1.6 – F2.9 DC-iris, funkcjonalność umożliwiającą pracę w trybie dzień/noc i światłoczułość minimalnie 0,2 luksa w trybie dziennym (przy F1.6) i minimalnie 0,04 luksa w trybie nocnym (przy F 1.6 i usuniętym filtrem odcinającym podczerwień).

Kamera powinna być wyposażona w mechaniczny filtr odcinający promieniowanie podczerwone, sterowany automatycznie lub manualnie.

Kamera powinna zapewnić precyzyjny, szybki obrót i pochylenie, ciągły obrót w zakresie 360 i pochylenie w zakresie minimalnie 220.

Kamera powinna być wyposażona w port sieci Ethernet 10BASE-T/100BASE-TX.

Kamera powinna dostarczać jednocześnie strumienie wideo w formatach Motion JPEG i H.264 i obsługiwać przynajmniej indywidualnie konfigurowalne strumienie w rozdzielczości HDTV 1080p (1920x1080) przy pełnej prędkości 30/25 kl/s.

Kamera powinna posiadać automatyczny i manualny balans bieli i być wyposażona w funkcjonalność rozszerzonej dynamiki WDR, możliwość odwrócenia obrazu oraz kompensacji tylnego oświetlenia.

Kamera powinna posiadać funkcję automatycznego odwrócenia obrazu w celu utrzymania ciągłości obserwacji obiektu przemieszczającego się pod kamerą.

Kamera powinna być wyposażona w możliwość zapamiętania trasy polegającej na przemieszczaniu się po wcześniej zaprogramowanych pozycjach jak i trasy użytkownika polegającej na zapamiętaniu ruchów głowicy i wartości zoom.

Kamera powinna posiadać funkcje detekcji ruchu w scenie, automatyczne śledzenie obiektów przemieszczających się w dozorowanej scenie oraz funkcję powrotu do wcześniej zaprogramowanej pozycji po ustaniu ruchu w scenie.

Kamera powinna reagować na określone zdarzenia w oparciu o wbudowane inteligentne funkcje takie jak wideo detekcja ruchu, pozycja mechanizmu PTZ, automatyczne śledzenie.

Kamera powinna być wyposażona w bufor do zapisu zdarzeń przed- i po alarmowych i powinna mieć wbudowane gniazdo kart pamięci SD/SDHC, umożliwiając korzystanie z lokalnego przechowywania materiału wideo.

Dla zapewnienia bezpiecznego dostępu do kamery i przesyłanej zawartości, kamera powinna obsługiwać szyfrowanie HTTPS, SSL/TLS i uwierzytelnianie IEEE802.1X. Kamera powinna także obsługiwać filtrowanie adresów IP i przynajmniej trzy różne poziomy zabezpieczenia hasłem.

Dla celów diagnostycznych kamera powinna posiadać możliwość logowania min. ostatnich 50 połączeń od uruchomienia urządzenia (adres IP z którego doszło do połączenia oraz czas utworzenia połączenia) oraz wygenerowania listy aktywnych połączeń.

## 2.2 Kamera stałopozycyjna

Kamera musi posiadać minimum 3 letnią gwarancję producenta

Kamera musi być fabrycznie wyposażona w obudowę w całości wykonaną z metalu.

Kamera musi poprawnie pracować w zakresie temperatur od -40°C do +50°C

Kamera musi poprawnie pracować w środowisku o wilgotności powietrza od 10% do 100% RH (z kondensacją).

Kamera musi posiadać przetwornik o przetwarzaniu progresywnym.

Kamera musi być fabrycznie wyposażona w obiektyw zmienneogniskowy z przesłoną P-iris i korekcją aberracji chromatycznej w zakresie widma podczerwieni.

Kamera musi posiadać mechaniczny filtr odcinający promieniowanie podczerwone, zapewniający poprawne odwzorowanie kolorów w ciągu dnia oraz zwiększający czułość kamery w zakresie promieniowania podczerwonego.

Kamera musi dostarczać poprawny obraz kolorowy sceny o poziomie oświetlenia nie większym niż 0.2lx i obraz czarno-biały dla scen o poziomie oświetlenia nie wyższym niż 0.04lx

Urządzenia musi posiadać wbudowany mechanizm balansu bieli pracujący w trybie automatycznym i manualnym.

Kamera musi być wyposażona w elektroniczną migawkę.

Kamera musi posiadać kontrolę obrazu dla obszarów zdefiniowanych przez użytkownika jak i automatyczną do całości obrazu.

Kamera musi posiadać funkcjonalność rozszerzonej dynamiki, zwiększania kontrastu obrazu.

Kamera musi umożliwiać manualne ustawienie prędkości migania migawki od 2s do 1/28000 dla tryby pracy migawki 50Hz i od 2s do 1/33500 dla tryby pracy migawki 60Hz

Kamera musi być wyposażona w funkcję kompensacji tylnego oświetlenia.

Kamera musi mieć możliwość dopasowania jakości obrazu w zakresie:

- Intensywności koloru
- Jasności
- Wyrazistości
- Kontrastu

Kamera musi być wyposażona w funkcjonalność optymalizacji parametrów (poziom wzmocnienia i prędkość migawki) wpływających na jakość obrazu dla scen słabo oświetlonych.

Kamera powinna dostarczać jednocześnie indywidualnie konfigurowane strumienie wideo w formatach Motion JPEG i H.264.

Kamera musi dostarczać przynajmniej dwa niezależne strumienie o rozdzielczości HDTV 1080p (1920x1080) przy 30 obrazach na sekundę (w trybie pracy migawki 60Hz) lub 25 obrazach na sekundę (w trybie pracy migawki 50Hz) w kompresji H.264 i/lub Motion JPEG.

Kamera musi być wyposażona w interfejs sieci Ethernet RJ45 10BASE-T/100BASE-TX PoE.

Kamera musi być wyposażona w zintegrowaną funkcjonalność zarządzania alarmami/zdarzeniami, które mogą być wywołane przez:

- Naruszenie wejścia alarmowego
- Detekcję ruchu
- Detekcję dźwięku
- Harmonogram
- Naruszenie zabezpieczenia antysabotażowego kamery
- Aplikację uruchomioną w kamerze
- Awarię lub zapełnienie pamięci lokalnej

W następstwie wywołania zdarzenia alarmowego kamera:

- Wyśle powiadomienie wykorzystując zapytania po protokołach TCP, SMTP lub HTTP
- Wyśle obrazy za pomocą protokołów FTP, SMTP lub HTTP
- Aktywuje wyjście/wyjścia alarmowe
- Rozpocznie zapis na pamięci lokalnej lub sieciowej

### **Pamięć do zapisu**

Kamera musi być wyposażona w bufor zapisu alarmowego zapewniający zapis obrazu z obserwowanej sceny poprzedzający wystąpienie alarmu oraz po zakończeniu alarmu. Musi również posiadać slot na kartę pamięci MicroSD w celu lokalnego przechowywania materiału wizyjnego.

Kamera musi być wyposażona w karty pamięci typów microSD/microSDHC/microSDXC, o pojemności do 64 GB.

### **Pozostała funkcjonalność**

Kamera musi być wyposażona w funkcję zdalnego ustawiania, np. przez stronę www, pozycji przetwornika w celu uzyskania optymalnego punktu ostrości.

Kamera musi posiadać wbudowaną funkcjonalność licznika pikseli w obrazie w celu określenia wielkości obiektu w scenie do liczby pikseli w obrazie.

Kamera musi posiadać funkcjonalność nanoszenia obrazów graficznych na strumień wizyjny.

### **Sieć**

Kamera musi wspierać zarówno adresację statyczną IP oraz dynamiczną w oparciu o serwer DHCP .

Kamera musi wspierać protokoły IPv4 oraz IPv6.

Kamera musi obsługiwać Quality of Service (QoS).

W celu zabezpieczenia transmisji przed nieautoryzowanym dostępem, urządzenie musi wspierać protokoły HTTPS, SSL/TLS oraz wspierać autentykację w ramach IEEE802.1X.

Kamera musi wspierać filtrowanie adresów IP i posiadać przynajmniej 3 różne poziomy zabezpieczenia hasłem.

Kamera musi wspierać synchronizację z serwerem czasu NTP.

Kamera musi obsługiwać Power over Ethernet zgodny z IEEE 802.3af.

### **Utrzymanie i serwis**

Kamera musi posiadać plik logów, zawierający informację o wszystkich połączeniach hostów od ostatniego restartu. Plik logów musi zawierać również informację, z jakiego adresu IP doszło do połączenia i czasie, kiedy ustanowiono połączenie.

Kamera musi posiadać wbudowaną funkcję Watchdog, która automatycznie zainicjuje proces restartu usługi lub kamery w przypadku wykrycia błędu.

Kamera musi obsługiwać w pełni otwarty i opublikowany interfejs API (Application Programmers Interface), zapewniając informacje niezbędne do integracji funkcjonalności aplikacji różnych producentów.

## 2.3 System rejestracji

Użyty sprzęt i materiały powinny być komponentami standardowymi dostępnymi w stałej ofercie danego producenta. Wszystkie systemy powinny być przetestowane i wdrożone w istniejących instalacjach.

Gwarancja wykonawcy nie powinna być krótsza niż 36 miesiące od daty dostawy.

System powinien pozwalać na rozszerzenie funkcjonalności poprzez uaktualnienie oprogramowania bez potrzeby zmian w strukturze sprzętowej.

System powinien obsługiwać połączenie sieciowe z obsługą protokołu TCP/IP i prędkością połączenia 1 GBit/sekundę.

System powinien umożliwiać tworzenie wielopoziomowego systemu zabezpieczeń dostępu w oparciu o hasła. System powinien umożliwiać tworzenie kont pojedynczych użytkowników oraz grup użytkowników z przypisanymi uprawnieniami dostępu. Prawa dostępu powinny co najmniej umożliwić rozróżnienie grup administracyjnych (z dostępem do opcji konfiguracji systemu) oraz grup użytkowych (dostęp do poszczególnych rejestratorów i kamer, podgląd "na żywo" oraz dostęp do archiwum, definiowanie akcji takich jak przetwarzanie i wyświetlanie stanów alarmowych, tworzenie kopii zapasowych, drukowanie, eksport sekwencji obrazów).

System powinien udostępniać otwarte i udokumentowane interfejsy komunikacyjne. Producent systemu na żądanie powinien bezpłatnie udostępniać zestaw narzędzi programistycznych (z ang. *Software Development Kit, SDK*) umożliwiający stworzenie oprogramowania integrującego z innymi systemami.

Rejestrator / serwer powinien posiadać moduł macierzy dyskowej z obsługą min. 8 kieszeni dyskowych hot-swap z możliwością obsługi dysków z interfejsem SATA o pojemności minimum 4TB i konfiguracji trybów RAID.

Możliwe powinno być automatyczne tworzenie kopii zapasowych całości lub wybranej części materiału. System powinien zarządzać zapisanymi kopiami nagrań udostępniając co najmniej opcje: dzielenie dużych plików na części przy ich tworzeniu, szyfrowanie tworzonych plików (hasło), limitowanie pasma zajmowanego przez proces backupu, autousuwanie najstarszych nagrań po zdefiniowanym czasie lub przekroczeniu wielkości zdefiniowanej przestrzeni dyskowej.

System umożliwiający tworzenie kopii fragmentów lub całości zarejestrowanego materiału. Konfiguracja tworzenia kopii zapasowych powinna pozwolić użytkownikowi wskazywać różne katalogi dla przechowywania kopii zapasowych na nośnikach magazynujących połączonych lokalnie lub poprzez sieć, dla różnych zdarzeń dotyczących tworzenia kopii zapasowych.

Tworzenie kopii zapasowych powinno być możliwe regularnie, we wcześniej określonych godzinach lub dniach jak również wywoływać je powinien dowolny alarm lub zdarzenie systemowe.

Dostępna przestrzeń dyskowa zespołu rejestratorów powinna być zorganizowana logicznie w formie odrębnych segmentów (pierścieni, z ang. ring). Pozwoli to na prowadzenie zapisu z różnymi parametrami odnośnie czasu i priorytetu przechowywania zapisu z poszczególnych kamer i zdarzeń. System powinien udostępniać co najmniej 5 pierścieni zapisu i 5 poziomów (priorytetów) zapisu. Zapis na pierścieniach powinien odbywać się poprzez automatyczne nadpisywanie i zastępowanie najstarszych nagrań.

System powinien obsługiwać dynamiczną transmisję strumieniową, w celu optymalizacji obciążenia sieci, obniżenia wymagań dla dekompresji obrazu i zwiększenia wydajności wyświetlania na stacjach podglądowych. W tym celu rozdzielczość transmitowanych "na żywo" obrazów powinna automatycznie dostosowywać się do rozmiaru (rozdzielczości) okien podglądu, w których wyświetlane są obrazy z poszczególnych kamer na stacji podglądowej. Dopasowanie to zależne powinno być od typu zastosowanej kamery, jednak system przy współpracy z wybranymi kamerami umożliwiać powinien automatyczne dopasowanie minimum do rozdzielczości: QCIF, QVGA, VGA, SVGA, WXGA, 720p, 1080p, 3MPix, 5MPix.

Użytkownik powinien mieć możliwość ustawiania takich parametrów, jak rozmiar, kolor, kolor tła oraz czcionka, przy pomocy których informacje te są wyświetlane.

Zarządzanie zdarzeniami i alarmami powinno pozwalać na efektywną adaptację reakcji systemu na stany alarmowe oraz inne zdarzenia, zgodnie z wymaganiami użytkownika.

Reakcje systemu powinny uwzględniać:

- Zdefiniowane przez użytkownika dowolnego czasu trwania sekwencji wideo przed i po wystąpieniu alarmu;
- Parametry rejestracji (jakość i prędkość niezależne (indywidualne) dla wszystkich kamer;
- Automatyczne wyświetlanie obrazów alarmowych zdefiniowanych przez użytkownika (na żywo i/lub w trybie odtwarzania) na predefiniowanych stacjach roboczych;
- Zmiana stanu jednego lub kilku styków wyjściowych przekaźników;
- Wysyłanie informacji o alarmach lub zdarzeniach do zalogowanych użytkowników;
- Obsługa interfejsów do systemów innych producentów;
- Ustawienie jednej lub wielu kamery PTZ w zaprogramowanej pozycji;
- Rozpoczęcie tworzenia automatycznych kopii zapasowych predefiniowanych sekwencji w razie wystąpienia alarmu, bądź innego zdarzenia;

Generowanie alarmów powinno następować co najmniej na skutek następujących zdarzeń: wewnętrzna analiza obrazu, zewnętrzne wejścia alarmowe oraz interfejsy z systemów innych producentów (szeregowo lub łącznie TCP/IP).

System udostępniać powinien harmonogramy czasowe do kontroli przetwarzanych zdarzeń oraz parametrów rejestracji. Pozwala to na całkowicie bezobsługowe działanie systemu, np. włączenie funkcji detekcji (wykrywania) ruchu w określonym przedziale czasowym, lub sprawdzanie stanu styków wyjściowych w określonych przedziałach czasowych.

Podgląd i przeglądanie zarejestrowanych obrazów i dźwięku powinno być możliwe przy użyciu oprogramowania, dostarczonego przez dostawcę cyfrowego systemu CCTV na nośnikach CD-ROM lub DVD-ROM, pracującego na komputerze klasy PC. Oprogramowanie musi być kompatybilne co najmniej z systemami operacyjnymi w wersjach 64 bitowych. Oprogramowanie ma być instalowane bezpłatnie na dowolnej ilości stacji podglądowych.

Każda stacja robocza użytkownika powinna mieć nieograniczony dostęp do wielu jednostek DVR/NVR jednocześnie. Oprogramowanie do podglądu obrazów (na żywo i zarejestrowanego materiału) może być instalowane bezpłatnie na dowolnej ilości stacji podglądowych, przy czym każda z tych stacji może w dowolnym momencie połączyć się z rejestratorem (o ile nie został wykorzystany w tym konkretnym momencie limit dostępnych sesji na rejestratorze, który można zwiększyć za pomocą licencji)

Interfejs użytkownika powinien umożliwiać jednoczesne wyświetlanie obrazu z tej samej kamery w wielu oknach w różnych trybach (na żywo, odtwarzanie w przód, odtwarzanie wstecz, odtwarzanie poklatkowe) jak również odtwarzanie obrazów z różnych kamer w wielu oknach podglądu.

Użytkownik powinien mieć możliwość ustawienia dowolnego rozmiaru, proporcji i pozycji każdego okna podglądu dzięki czemu możliwe będzie wyświetlanie niezniekształconego obrazu z dowolnej kamery zainstalowanej w systemie.

Dostępny powinien być zestaw narzędzi ulepszających podgląd obrazu, w tym regulacja jasności, kontrastu, nasycenia barw oraz poziom powiększenia. Zmiany wprowadzone na podglądzie nie mają wpływu na zapisane dane.

Podgląd alarmowy (wywołanie sceny po wystąpieniu alarmu) powinien umożliwiać wyświetlenie pojedynczych obrazów przed- i po-alarmowych oraz całych sekwencji obrazów w pętli, dla jednej lub wielu kamer.

Funkcja szybkiego wyszukiwania obrazu powinna być definiowana poprzez określenie takich kryteriów wyszukiwania jak czas, data, numer kamery, typ zdarzenia, data zdarzenia.

Powinna istnieć możliwość wyszukiwania po detekcji ruchu na zarejestrowanym obrazie.

Analiza alarmów lub zdarzeń powinna umożliwiać bezpośredni dostęp do obrazów związanych z tymi zdarzeniami, poprzez przeglądanie globalne wszystkich zdarzeń w systemie, zdarzeń przetwarzanych poprzez wybrany serwer lub zdarzeń związanych wyłącznie z wybraną kamerą.

Wyszukiwanie obrazu w grupie kamer powinno umożliwiać późniejsze zsynchronizowane wyświetlanie wszystkich lub wybranych obrazów (za pomocą jednej komendy ustawienie kamer na ten sam czas) odpowiadające danym kryteriom wyszukiwania z różnych kamer, w różnych oknach podglądu, bez względu na liczbę jednostek DVR/NVR, z którymi połączone są kamery z danej grupy.

W przypadku wyszukiwania dotyczącego wybranej kamery, operator powinien mieć możliwość dokonania wyboru spośród listy dostępnych nagrań oraz punktu na wskaźniku czasu. Lista nagrań

powinna zawierać wszystkie kamery, również te, które w obecnej chwili nie przekazują obrazu „na żywo”, a nadal posiadają obrazy wideo przechowywane w bazie danych urządzenia DVR/NVR.

W celu odnalezienia określonego nagrania wideo, operator nie musi wybierać odpowiedniego urządzenia nagrywającego. Użytkownikowi powinna być udostępniona jednolita lista wszystkich dostępnych kamer, niezależnie od tego, do jakiego rejestratora DVR/NVR kamery te są podłączone.

Przy wybieraniu kamery, lista kamer do wyboru powinna być przedstawiona jako struktura drzewa katalogowego. Różne typy kamer (stacjonarne, obrotowe, IP i inne) powinny być wyróżnione w widoku drzewa odpowiednim symbolem lub kolorem.

Oprogramowanie konfiguracyjne powinno być oddzielone od oprogramowania podglądu. Powinno się je uruchomić na standardowym komputerze klasy PC z systemem operacyjnym w wersji 64 bitowej.

Połączenie oprogramowania konfiguracyjnego z jednostkami systemu powinno być możliwe lokalnie, jak również poprzez sieć (przy użyciu protokołu TCP/IP).

System powinien posiadać opcję szyfrowania zgrywanego na nośniki zewnętrzne materiału.

Oprogramowanie rejestratora i stacji podglądu umożliwiać powinno weryfikację autentyczności zarejestrowanych obrazów.

W trakcie procesu eksportowania lub tworzenia kopii zapasowych, oprogramowanie odczytujące kopię nagrań powinno zostać automatycznie umieszczone razem z sekwencjami wideo na nośniku magazynującym, aby umożliwić przegląd wyeksportowanych obrazów na standardowym komputerze klasy PC z systemem Windows 7 w wersji 64 bitowej lub nowszym, dzięki czemu można uniknąć naruszenia ich integralności oraz unika się potrzeby dodatkowego instalowania oprogramowania przeglądającego.

Powinna istnieć możliwość wyeksportowania materiału do formatu DVD-Video, dzięki czemu będzie można odtwarzać materiał na standardowych odtwarzaczach DVD (brak konieczności używania komputera PC oraz jakiegokolwiek programowania)

Dostępna jest możliwość wydruku (na drukarce podłączonej do komputera PC) obrazów bezpośrednio z poziomu aplikacji podglądu wraz ze szczegółowymi danymi o tym obrazie (data, czas, nazwa kamery) oraz z możliwością dołączenia komentarza wpisywanego przez użytkownika.

Aplikacja operatora systemu powinna być w języku polskim

Możliwość kopiowania do pliku wszystkich ustawień systemu oraz możliwość przesłania wszystkich ustawień z pliku do systemu lub jego poszczególnych części .

System udostępniać pełną funkcjonalność krosownicy wizyjnej z możliwością:

- krosowania sygnałów na żywo oraz obrazów zapisanych w bazie danych
- grupowe przełączanie kamer na poszczególne monitory
- sterowanie kamerami obrotowymi
- wyświetlanie komunikatów alarmowych
- ustawienie sekwencji dla poszczególnych kamer
- podgląd na poszczególnych monitorach w trybach wieloekranowych (wiele kamer obserwowanych jednocześnie w podziale ekranu na pojedynczym monitorze)
- powinna istnieć możliwość modernizacji oprogramowania sprzętowego
- możliwość zaprogramowania do 50 niezależnych sekwencji

Klawiatura winna posiadać możliwość :

- sterowania funkcjami rejestratorów oraz krosownicy wizyjnej
- sterowania kamer obrotowych przy pomocy drążka sterującego
- możliwość definiowania min. 5 przycisków na klawiaturze, umożliwiając wykonywanie poleceń zaprogramowanych w systemie
- możliwość sterowania wieloma rejestratorami z pozycji jednej klawiatury (min. do 32 rejestratorów)
- możliwość podłączenia do systemu poprzez sieć LAN. Ze względu na architekturę systemu port LAN jest wymaganiem koniecznym.

## 2.4 System ochrony obwodowej

System ochrony obwodowej powinien być podzielony na strefy i nadzorowany.

System ochrony obwodowej powinien wykorzystywać akcelerometry w 3-osiowej technologii MEMS i stosować analizę logiki rozmytej. Czujniki powinny być połączone ze sobą w systemie Plug & Play, za pomocą dostarczonego z systemem, wodoszczelnego i odpornego na promieniowanie UV, okablowania zakończonego złączami RJ45.

Zapis pozycji przestrzennych i adresów każdego sensora zainstalowanego na ogrodzeniu powinien być wykonany automatycznie podczas konfiguracji parametrów.

Długość strefy powinna być selektywna i wynosić od 1m do 700 m.

Dokładność identyfikacji alarmu z danej strefy winna wynosić maksymalnie 50 metrów.

Pojedyncza linia powinna zapewniać ochronę dla ogrodzenia o wysokości do 6 m.

System powinien być wyposażony w cyfrową analizę sygnału wykorzystującą logikę rozmytą.

System powinien posiadać inteligencję rozproszoną pozwalającą na osobną analizę sygnału każdej z czujek. Wykorzystanie takiej technologii powinno pozwolić na dobranie parametrów pracy indywidualnie dla stref lub pojedynczych czujek.

Temperatura pracy systemu powinna się zawierać w zakresie od – 40 °C do + 70 °C.

Wilgotność względna pracy systemu powinna zawierać się w zakresie od 0% do 100%.

Powinna istnieć możliwość konfiguracji systemu przy pomocy oprogramowania.

System powinien być w stanie, w odniesieniu do przyspieszenia ziemskiego, zapamiętać informacje na temat pozycji akcelerometru w przestrzeni. Zapamiętanie pozycji każdego czujnika podczas konfiguracji pozwoli, na podstawie analizy kąta nachylenia, na rozpoznanie próby przechylenia lub zmiany położenia płotu.

System powinien być natywny dla IP i posiadać wyjście Ethernet pozwalające na połączenie komputera lokalnie lub zdalnie za pomocą sieci IP.

Za pomocą oprogramowania producenta do konfiguracji/zarządzania/monitoringu powinno możliwe być wykonanie zaawansowanych ustawień systemu i odczyt rejestru alarmu i zdarzeń.

Oprogramowanie konfiguracyjne połączone do systemu powinno pozwolić instalatorowi na:

- Ustawienie i zarządzanie ustawieniami parametrów dla systemu / strefy / czujki.
- Ustawienie i zarządzenia analizą przecięcia ogrodzenia dla systemu / strefy / czujki.
- Wybór rodzaju ogrodzenia dla systemu / strefy / czujki.
- Zdefiniowanie rozmiarów i pozycji stref dla systemu.
- Ustawienie alarmu przechylenia czujki dla systemu / strefy / czujki.
- Zabezpieczenie hasłem
- Odczyt sygnałów z pojedynczych czujek w czasie rzeczywistym.
- Przegląd archiwum rejestru zdarzeń i poziomów sygnałów, przechowywany przez system przez ponad rok.

Analiza sygnału z każdej czujki lub całych stref musi odbywać się przy wykorzystaniu logiki rozmytej, co pozwala na dokładne ustalenie czy odebrany sygnał jest zakłóceniem generowanym przez środowisko czy próbą przejścia człowieka przez strefę detekcji.

Silne warunki pogodowe takie jak: wiatr, deszcz, śnieg itp. powinny być odrzucane przez system bez wykorzystywania jakichkolwiek dodatkowych stacji pogodowych

System powinien rozpoznać intruza próbującego przejść przez strefę detekcji w następującymi sposobami:

- Przejście przez płot
- Podniesienie płotu
- Przecięcie ogrodzenia

Słupy betonowe o wysokości 6m na których zamontowane zostaną kamery należy zabezpieczyć w taki sposób, aby wykryć podejście do słupa przez intruza na odległość nie mniejszą niż 6 m od strony zewnętrznej ogrodzenia.

## 2.6. Oprogramowanie integrujące systemy bezpieczeństwa



Interfejs zarządzający systemami bezpieczeństwa bazującymi na sieci IP powinien zostać zaprojektowany w celu gromadzenia i integracji danych z czujek/stref alarmowych poprzez połączenie Ethernet, a także transmisji danych do systemów zewnętrznych. System powinien składać się z Serwera z zainstalowanym oprogramowaniem, zdolnym do zarządzania nie mniej niż 1280 różnych czujek/stref.

Interfejs zarządzający systemami bezpieczeństwa bazującymi na sieci IP, powinien wykorzystywać bezpieczne protokoły komunikacyjne w połączeniach z czujkami/strefami alarmowymi.

W razie usterki serwera głównego, powinien być dostępny serwer zapasowy w trybie „Hot Backup”, pozwalający na natychmiastowe przejście funkcji serwera głównego. Serwer zapasowy powinien automatycznie uruchomić się z włączonymi wszystkimi ustawieniami z serwera głównego i rozpocząć monitorowanie systemu. Serwer zapasowy, po naprawie i ponownym uruchomieniu serwera głównego, powinien przekazać funkcję nadzoru wraz zapisanymi plikami rejestru zdarzeń do serwera głównego.

Interfejs zarządzający systemami bezpieczeństwa bazującymi na sieci IP, powinien zostać wyposażony w funkcję analizy sygnału QoS (Quality of Signal), która pomaga w monitorowaniu i ocenie transmisji danych w danej infrastrukturze.

Interfejs zarządzający systemami bezpieczeństwa bazującymi na sieci IP, powinien być w stanie wykonać analizę sygnatur każdej z czujek/stref, pozwalającą na detekcję blokowania lub bezprawnego podmienienia czujki/strefy.

Główny i zapasowy serwer powinny być zabezpieczone hasłem, w celu ochrony systemu przeciwko próbom włamania/sabotażu.

System powinien być wyposażony w funkcję ciągłego odpytywania czujek/stref połączonych do serwera poprzez połączenie Ethernet wykorzystujące rodzaj transmisji TCP/IP. Serwer powinien być w stanie odpytać nie mniej niż 1280 czujek/stref dostarczając informację o statusie urządzeń w czasie mniejszym niż 0,5 sekundy od generacji stanu na urządzeniu.

System powinien posiadać do 10 różnych grup wyjść, każda grupa zdolna do komunikacji za pomocą 5 różnych protokołów w tym samym czasie.

W pełni wyposażony system, powinien zajmować kanał nie większy niż 20 kilobitów. Praca serwera nie powinna zakłócać istniejącej sieci IP, pozwalając na pracę w tej samej sieci LAN zarówno czujek/stref alarmowych i kamer IP.

System, powinien być w stanie wykonać analizę sygnatur każdej z czujek/stref, pozwalającą na detekcję blokowania lub bezprawnego podmienienia czujki/strefy.

System powinien być wyposażony w funkcję automatycznej akwizycji i konfiguracji. Pozwoli to na szybkie i proste uruchomienie jego pełnej funkcjonalności.

System powinien być wyposażony w tryb zaawansowany. Funkcja ta, powinna pozwolić na wykonanie konserwacji i obsługi systemu, a także ustawień czujek/stref bez wpływu na stabilność pracy, w sensie opóźnienia odpowiedzi serwera, gwarantując tym samym nieprzerwaną ochronę. Tryb ten powinien pozwolić na pobranie rejestrów zdarzeń bez przerywania statusu odpytywania czujek/stref.

System powinien posiadać oprogramowanie konserwacyjne, testowe i synoptyczne, które połączone w dowolnym punkcie w sieci LAN, może pracować nieprzerwanie lub może wykonać funkcję konserwacji lub testu systemu.

System powinien być w stanie wykonać raz dziennie automatyczną synchronizację daty i czasu wszystkich połączonych do niego urządzeń: czujek/stref, serwera zapasowego i terminali synoptycznych.

Serwer powinien być skonfigurowany w taki sposób aby w razie wystąpienia zaniku i przywrócenia zasilania, uruchamiał automatycznie OS, aplikację zarządzającą wraz z ostatnio wykorzystywaną konfiguracją.

## **2. System ochrony budynku administracyjnego oraz zaplecza warsztatowo-technicznego**

Na budynku administracyjnym (wokół jego obwodu ) należy zamontować co najmniej 6 kamer IP o rozdzielczości minimum 720P stałopozycyjnych. W budynku nr 1 przy wejściu na wieże i na

kondygnacji 3 wieży po jednej kamerze o rozdzielczości minimum 720P stałopozycyjnych. Wewnątrz budynku na kondygnacji -1, parterze i kondygnacji +1 korytarze do części administracyjnej należy zabezpieczyć systemem alarmowym.

Na zewnątrz budynku nr 1 należy zamontować co najmniej 2 kamery IP o rozdzielczości minimum 720P obserwujące stacje transformatorowo oraz agregat prądowórczy zasilający budynek.

Na budynku warsztatowo technicznym nr 9 należy zamontować co najmniej 4 kamery IP o rozdzielczości minimum 720P obserwujące plac przed budynkiem z tym, że jedna ma służyć obserwacji budynku nr 5 hydrofornia.

Dodatkowo przy bramie nr 1 i bramie nr 2 należy zamontować po 3 kamery stałopozycyjne dla podglądu:

- Podjeżdżającego pojazdu.
- Kontrolowanego pojazdu z przodu
- Kontrolowanego pojazdu z boku.

W punktach kontroli Wartowania i budynek nr 3 należy zamontować po 1 kamerze stałopozycyjnej. Wszystkie ww. kamery mają pracować w jednym systemie a sygnał ma być przesyłany do centrum monitoringu.

Pomiędzy wieżą a budynkiem administracyjnym, w kanalizacji teletechnicznej, należy ułożyć światłowód oraz zamontować niezbędne urządzenia do przesyłu obrazów oraz sygnałów systemu alarmowego do centrum monitoringu. Kamery należy podłączyć do rejestratora cyfrowego IP nadzorującego pracę kamer systemu ochrony obwodowej. Stany alarmowe oraz informacje o uzbrojeniu obiektu winne być wizualizowane programowo w pomieszczeniu centrum monitoringu.

#### **Wymagania techniczne dla kamer, za wyjątkiem rozdzielczości, takie same jak dla kamer Systemu ochrony obwodowej w pkt 2.2.**

Kamery należy podłączyć do systemu ochrony obwodowej- centrum monitoringu.

Kanalizację teletechniczną jednonotworową wykonać w oparciu o studnie SK1, SK2 oraz rury typu AROT 100.

#### **4. Na potwierdzenie wymagań opisanych w pkt 2.1-2.6 do oferty muszą być dołączone karty katalogowe celem potwierdzenia parametrów oferowanego sprzętu.**