**SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA**

**Wdrożenie i zakup platformy integrującej techniczne systemy bezpieczeństwa na rzecz Zamawiającego PGNiG TERMIKA S.A.**

**Załącznik nr 3**

**Opis Przedmiotu Zamówienia**

Spis treści /

[**1.** **Wstęp** 3](#_Toc534613339)

[**2.** **System ochrony perymetrycznej** 6](#_Toc534613340)

[**2.1. Istniejący system aktywnych barier podczerwieni** 6](#_Toc534613341)

[**2.2. Podsystem kamer stałopozycyjnych termowizyjnych** 7](#_Toc534613342)

[**2.3. Podsystem kamer stałopozycyjnych światła widzialnego.** 7](#_Toc534613343)

[**2.4. Podsystem głowic szybkoobrotowych** 9](#_Toc534613344)

[**3.** **System nadzoru nad ruchem osobowym.** 9](#_Toc534613345)

[**3.1. System Kontroli Dostępu.** 9](#_Toc534613346)

[**3.2. Elektroniczne depozytory kluczy** 11](#_Toc534613347)

[**3.3. System Telewizji Dozorowej.** 11](#_Toc534613348)

[**4.** **System nadzoru nad ruchem pojazdów.** 14](#_Toc534613349)

[**4.1. System Kontroli Dostępu.** 14](#_Toc534613350)

[**4.2. System Telewizji Dozorowej.** 14](#_Toc534613351)

[**4.2.1. Parkingi zakładowe.** 14](#_Toc534613352)

[**4.2.2. Bramy i wagi samochodowe.** 15](#_Toc534613353)

[**4.2.3. Bramy kolejowe** 15](#_Toc534613354)

[**4.2.4. Stacja paliw** 15](#_Toc534613355)

[**4.2.5. Drogi wewnętrzne przeznaczone do ruchu samochodów dostawców i podwykonawców.** 16](#_Toc534613356)

[**5.** **Infrastruktura kablowa** 17](#_Toc534613357)

[**5.1. Okablowanie strukturalne dla potrzeb CCTV** 17](#_Toc534613358)

[**5.2. Linie zasilające** 17](#_Toc534613359)

[**6.** **Podsystemu ochrony technicznej wybranych budynków** 17](#_Toc534613360)

[**7.** **Platformy systemu zarządzania bezpieczeństwem** 17](#_Toc534613361)

[**7.1. Integracja z systemem telewizji dozorowej.** 18](#_Toc534613362)

[**7.2. Integracja z systemem kontroli dostępu** 18](#_Toc534613363)

[**7.3. Integracja z systemem sygnalizacji włamania i napadu** 19](#_Toc534613364)

[**7.4. Integracja z podsystemem zarządzania kluczami** 20](#_Toc534613365)

[**7.5. Aplikacja Mobilna.** 21](#_Toc534613366)

[**8.** **Zabezpieczenie przeciwprzepięciowe.** 22](#_Toc534613367)

[**9.** **Zasilanie podstawowe i awaryjne systemu** 23](#_Toc534613368)

[**10.** **Opis wymagań zamawiającego w stosunku do przedmiotu zamówienia** 23](#_Toc534613369)

[**10.1. Wymagania ogólne** 23](#_Toc534613371)

[**10.2. Dokumentacja projektowa.** 25](#_Toc534613372)

[**10.2.1. Forma dokumentacji projektowej.** 28](#_Toc534613373)

[**10.2.2. Prawa autorskie.** 29](#_Toc534613374)

[**10.3. Minimalne wymagania techniczno-użytkowe wobec urządzeń.** 29](#_Toc534613375)

[**10.3.1. Wymagania dla urządzeń i oprogramowania systemu CCTV:** 29](#_Toc534613377)

[**10.3.2. Wymagania dla Centrum Monitoringu i Zarządzania.** 38](#_Toc534613378)

[**10.3.3. Wymagania dla stanowisk Biura Bezpieczeństwa.** 40](#_Toc534613379)

[**10.3.4. Wymagania dla stanowisk w posterunkach ochrony.** 40](#_Toc534613380)

[**10.3.5. Urządzenia aktywne** 40](#_Toc534613381)

[**10.3.6. Wymagania dla urządzeń systemu SSWiN:** 42](#_Toc534613382)

[**10.3.7. Wymagania dla PSIM.** 44](#_Toc534613383)

[**10.3.8. Wymagania dla okablowania strukturalnego** 48](#_Toc534613384)

[**10.3.9. Pomiary okablowania miedzianego** 51](#_Toc534613385)

[**10.3.10. Pomiary okablowania światłowodowego** 52](#_Toc534613386)

[**11.** **Wymagania serwisowe w okresie gwarancyjnym** 52](#_Toc534613387)

1. **Wstęp**

Przedmiotem opracowania jest opis przedmiotu zamówienia stanowiący załącznik nr 2 do umowy na zakup, wdrożenie, realizację szkoleń i wsparcie techniczne w ramach modernizacji systemów zabezpieczeń technicznych (SZT) w PGNiG Termika SA obejmujących systemy KD, SWiN i CCTV, które powinny zostać zintegrowane w jednej platformie systemu zarządzania bezpieczeństwem (SZB).

Modernizacja będzie dotyczyć głównie Zakładu nr 1 – Elektrociepłownia Siekierki (ECS) i Zakładu nr 2 – Elektrociepłownia Żerań (ECZ), w których mają zostać zmodernizowane wszystkie w/w systemy zabezpieczeń technicznych. W przypadku Zakładów nr 3, 4 i 5, czyli odpowiednio Ciepłownia Kawęczyn (CK), Ciepłownia Wola (CW) i Elektrociepłownia Pruszków (ECP), modernizacji i ujednoliceniu podlega przede wszystkim system KD.

Celem niniejszego dokumentu jest określenie wymagań funkcjonalnych i technicznych, które powinny spełniać zaprojektowane i wykonane systemy zabezpieczeń technicznych wraz z platformą zarządzania bezpieczeństwem, zgodnie z zasadą „projektuj i buduj”.

System ochrony technicznej na terenie zakładów ECS i ECZ składać się będzie z:

* Podsystemu ochrony perymetrycznej obiektu,
* Podsystemu nadzoru nad ruchem osobowym,
* Podsystemu nadzoru nad ruchem pojazdów,
* Podsystemu ochrony technicznej wybranych budynków,
* Platformy systemu zarządzania bezpieczeństwem klasy PSIM,

zbudowanych na bazie współdziałających i zintegrowanych systemów CCTV, KD i SWiN wraz z oprogramowaniem zarządzającym. Całość systemu powinna być tak zaprojektowana i wykonana aby zapewnić pełną ochronę antysabotażową oraz pełną informację o stanie pracy/awarii/sabotażu wszystkich podstawowych urządzeń systemu.

Obecnie zainstalowane są systemy:

* System telewizji dozorowej firmy Siemens oparty o kamery analogowe, przeznaczony do demontażu;
* System Sygnalizacji Włamania i Napadu firmy Siemens. Centrale, moduły rozszerzeń urządzenia obsługi (klawiatury, stanowiska obsługi) przeznaczone do demontażu, urządzenia detekcyjne do dalszego użytkowania;
* System Kontroli Dostępu firmy EDPS oparty o rozwiązania techniczne firmy KABA, który może być przeznaczony w części lub w całości do dalszego użytkowania. Przewiduje się konieczność pełnej integracji istniejącego systemu KD z platformą zarządzania bezpieczeństwem SZB zgodnie z opisem w dalszej części opracowania. Wykonawca może zaproponować wymianę sytemu na inny pod warunkiem odtworzenia wszystkich istniejących funkcji systemu oraz zapewnieniu nowych funkcjonalności opisanych w dalszej części opracowania.

Przewidywany zakres prac obejmuje zaprojektowanie, wykonanie, dostawę, montaż, uruchomienie i zaprogramowanie Systemów SZT i SZB wraz z pracami towarzyszącymi, w tym:

* wykonanie weryfikacji inwentaryzacji istniejących systemów i posiadanej dokumentacji, opracowanie niezbędnych analiz, koncepcji, symulacji i ekspertyz;
* przeprowadzenie analizy zagrożeń;
* opracowanie i wykonanie zgodnie z obowiązującymi przepisami i normami dokumentacji projektowej w uzgodnieniu z Zamawiającym oraz z rzeczoznawcą ds. zabezpieczeń ppoż. (koncepcja, projekt wykonawczy i dokumentacja powykonawcza);
* demontaż i przekazanie do magazynu Zamawiającego istniejących urządzeń Systemu, które Zamawiający wskaże jako przeznaczone do zachowania.
* demontaż i utylizacja pozostałych urządzeń Systemu (nieprzewidzianych przez Zamawiającego do dalszego użytkowania lub zachowania), zdemontowanego zbędnego okablowania i tras kablowych.
* podwyższenia istniejącego ogrodzenia o ok. 1,5m wraz zabezpieczeniem go drutem żyletkowym (ostrzowym) concertina w miejscach wskazanych przez zamawiającego (łącznie ok. 100m);
* wykonanie pomiarów potwierdzających możliwość wykorzystania istniejącego okablowania;
* przeprowadzenie testów potwierdzających możliwość dalszego użytkowania urządzeń wskazanych przez Zamawiającego jako przeznaczonych do wykorzystania;
* wykonanie na podstawie projektu wykonawczego sporządzonego przez Wykonawcę i zaakceptowanego przez Zamawiającego nowego systemu chroniącego obiekt;
* budowa nowego okablowania, tam gdzie brak możliwości wykorzystania istniejącego;
* dostawa, zainstalowanie, zaprogramowanie, uruchomienie i testy nowych urządzeń;
* podłączenie i integracja z nowym systemem SZT i SZB istniejących urządzeń wskazanych przez Zamawiającego jako przeznaczonych do wykorzystania;
* odtworzenie pomieszczeń i terenu do stanu poprzedniego;
* dostosowanie istniejących pomieszczeń Centrum Monitoringu w ECS i ECZ do aktualnych wymogów dla tego typu pomieszczeń przy uwzględnieniu dodatkowych wymagań Zamawiającego;
* podłączenie systemów CCTV nowego Bloku Gazowo-Parowego i Kotłowni Szczytowej ECZ do nowych serwerów SZB i ich integracja (ok. 50 punktów kamerowych);
* podłączenie systemów SWiN i KD nowego Bloku Gazowo-Parowego oraz Kotłowni Szczytowej ECZ do SZB i ich integracja (ok. 20 sygnałów);
* zintegrowanie systemu z istniejącym systemami związanymi z ochroną przeciwpożarową obiektu (informacje w postaci komunikatów o wystąpieiu pożaru w danej strefie, otwarcie drzwi objętych systemem kontroli dostępu w danej strefie, wyświetlenie w trybie alarmowym obrazów z kamer zainstalowanych w obszarze, gdzie wykryto pożar, itp) ;
* przetestowanie systemu pod kątem poprawności działania;
* wykonanie pełnej wizualizacji systemu na stanowiskach komputerowych przeznaczonym dla ochrony wraz z dostawą tych stanowisk;
* zainstalowanie i konfiguracja oprogramowania zarządzającego systemem dla administratorów systemu, na stanowiskach komputerowych wraz z dostawą tych stanowisk;
* dostawa stacji inżynierskiej wraz z aplikacjami administratora systemu;
* przekazanie Zamawiającemu wszystkich licencji, kluczy, haseł do zainstalowanego oprogramowania, central, rejestratorów, stacji roboczych, serwerów itp., kodów źródłowych do modyfikacji oprogramowania;
* serwisowanie i konserwacja systemu w okresie gwarancji, przy czym przeglądy serwisowe winny się odbywać nie rzadziej niż raz na kwartał, chyba, że producent urządzeń zaleca częstsze przeglądy;
* bezpłatna aktualizacja oprogramowania zarządzającego oraz firmware urządzeń do najnowszych przetestowanych wersji w całym okresie gwarancji;
* przeszkolenie pracowników Zamawiającego z zakresu obsługi, eksploatacji i administracji nowego Systemu;
* opracowanie i przekazanie dokumentacji powykonawczej.

Wszystkie dane ilościowe podane są jedynie informacyjnie. Obowiązkiem Wykonawcy jest własnym kosztem i staraniem dokonać na własną odpowiedzialność weryfikacji tychże informacji. Obowiązkiem Wykonawcy będzie, niezależnie od precyzji zawartych w koncepcji danych, zaprojektowanie i wykonanie kompletnego systemu zabezpieczeń technicznych (SZT) wraz z platformą systemu zarządzania bezpieczeństwem (SZB), zapewniającego ochronę całkowitej powierzchni zajmowanych przez zakłady ECZ i ECS zgodnie z obowiązującymi przepisami, normami i najnowszymi zasadami wiedzy technicznej przy założeniu wykorzystania wszystkich dostępnych funkcji systemów w celu osiągnięcia optymalnego stosunku „koszt/efekt”.

1. **System ochrony perymetrycznej**

Pod pojęciem systemu ochrony perymetrycznej należy rozumieć zestaw urządzeń elektronicznych i optoelektronicznych przeznaczonych do ochrony terenu zewnętrznego, system zobrazowania sytuacji alarmowej we wskazanym pomieszczeniu oraz systemy i urządzenia pomocnicze.

W skład elementów ochrony perymetrycznej i systemów pomocniczych wchodzą:

1. Aktywne bariery podczerwieni do detekcji forsowania ogrodzenia.
2. Zewnętrzne czujki ruchu.
3. Podsystem stałopozycyjnych zewnętrznych kamer CCTV do nadzorowania ogrodzenia (identyfikacja zagrożeń) oraz weryfikacji zdarzeń alarmowych, uwzględniający monitoring bram wjazdowych.
4. Podsystem głowic szybkoobrotowych składający się z dalekozasięgowych zespołów optoelektronicznych (głowica szybkoobrotowa z doświetleniem laserowym) o dużym zasięgu do identyfikacji i śledzenia intruza.
5. Okablowanie światłowodowe dla zapewnienia transmisji sygnałów.
6. Zobrazowanie sygnałów z wykonanych czujników i kamer oraz integracja w Centrum Monitoringu.
7. Kanalizacja teletechniczna i kable światłowodowe na potrzeby systemu.

Projektowany system ochrony perymetrycznej powinien zapewniać 2 niezależne sposoby detekcji wtargnięcia intruza na obszar chroniony oraz wideo weryfikację zdarzeń alarmowych. Wyjątek stanowią specyficzne obszary, gdzie detekcja oparta będzie jedynie na analityce w kamerach:

- wydzielany obecnie obszar Rozdzielni 110kV w ECZ,
- wydzielony obszar pod stację gazową w ECZ,
- ujęcie wody z rzeki Wilanówki (ECS).
- pompownia nad Wisłą (ECS).

 W pozostałych obszarach, detekcja zostanie zapewniona poprzez:

- wykorzystanie istniejącego system aktywnych barier podczerwieni;
- wykorzystanie istniejącego podsystemu kamer termowizyjnych (ECS);
- wykonanie podsystemu kamer stałopozycyjnych światła widzialnego z uruchomionymi analitykami.

* 1. **Istniejący system aktywnych barier podczerwieni**

należy podłączyć do nowych urządzeń systemu SWiN oraz uzupełnić w następującym zakresie:

1. EC Żerań:
* bariery podczerwieni chroniące ogrodzenie w rejonie:

- pompowni wody pitnej (ok. 100m);

- sprężarkowni (ok. 100m);

- bud. odprowadzenia wody (2x ok. 20m);

- bud. warsztatów i zaplecza technicznego (ok. 300m).

* Zewnętrzne dualne czujki ruchu:

- bramy wjazdowe i ewakuacyjne;

- teren wydzielony.

1. EC Siekierki
* bariery podczerwieni chroniące ogrodzenie w rejonie:

- budynku rozdzielni 15kV (4 odcinki, ok. 150 m);

- bramy nr 2 (ok. 60m);

- bramy kolejowej (ok. 120m).

* Zewnętrzne dualne czujki ruchu:

- bramy wjazdowe i ewakuacyjne.

W EC Żerań przewiduje się konieczność wymiany centralnych urządzeń firmy Siemens (centrala szt. 1, ekspander 8 we/wy z zasilaczem i akumulatorami 10 szt., klawiatura systemowa 3 szt.).

W EC Siekierki przewiduje się konieczność wymiany centralnych urządzeń firmy Siemens (centrala szt. 2, ekspander 8 we/wy z zasilaczem i akumulatorami 17 szt., klawiatura systemowa 3 szt.).

* 1. **Podsystem kamer stałopozycyjnych termowizyjnych**

zainstalowany w EC Siekierki, zapewnia detekcję intruza w części rejonu ogrodzenia od strony ul. Kobylańskiej. Należy rozbudować go o kamery termowizyjne zapewniające niezawodną detekcję w następujących obszarach:

* pozostała część ogrodzenia od ul. Kobylańskiej;
* ogrodzenie w rejonie kanału wody chłodzącej;
* ogrodzenie w rejonie ul. Łuczniczej;

łącznie ok. 8 kamer.

* 1. **Podsystem kamer stałopozycyjnych światła widzialnego.**

Podsystem kamer stałopozycyjnych będzie pełnił podwójną rolę: detekcji intruza oraz wideo weryfikacji zdarzeń. Należy tak zaprojektować i wykonać ww. podsystem aby jednocześnie spełniał oba zadania.

Detekcja intruza będzie zapewniona przez system kamer pracujących w świetle widzialnym. Wybrane kamery wyposażone będą w analityki w zakresie detekcji intruza, czyli wejścia/ wyjścia w rejon, przekroczenia linii. Efekt działania analityki w postaci metadanych zapisywany będzie w systemie rejestracji wideo. Wymagane jest zapewnienie funkcji detekcji na całej długości ogrodzenia (wraz z elewacjami budynków stanowiących granicę obiektu). Zapewnienie funkcji detekcji wymaga odwzorowania obiektu 1m przez min 80 pikseli rozdzielczości. Do spełnienia w/w wymagań należy zastosować kamerę pracującą np. w trybie korytarzowym, o przetworniku z rozdzielczością min. 1080p z odpowiednio dobranym obiektywem do obserwowanej sceny (kamera typ 1). Tak zdefiniowany tor optyczny zapewnia funkcję detekcji dla przewidywanego rozmieszczenia kamer. Należy stosować kamery z mechanicznym filtrem IR i z wysoką dynamiką przetwornika WDR min. 120dB. Maksymalne odległości masztów kamerowych ok. 80m. Szerokość pasa detekcyjnego przyjęto, jako min. 4-4.5m. Kamery na masztach mają być instalowane w taki sposób, aby na końcu pola zasięgu można było zarejestrować obiekt o wysokości 2m. Rozmieszczenie urządzeń musi zapewnić pełne pokrycie nadzorowanego obszaru. Martwe pole wynikające z graniastosłupowego widzenia kamery nadzorowane musi być przez kamerę poprzednią. Maszty należy rozmieścić tak, aby pola dozoru pokrywały się oraz w taki sposób, aby system był odporny na utratę ostrości i szczegółów widzenia wynikające z utraty głębi ostrości pod wpływem zmieniających się warunków oświetleniowych. Dopuszcza się zastosowanie kamer o lepszych parametrach technicznych.

Podsystem kamer stałopozycyjnych światła widzialnego ma zapewnić również na całej długości ogrodzenia (wraz z elewacjami budynków stanowiących granicę obiektu) weryfikację wideo zdarzeń alarmowych. Szerokość pasa weryfikacji wideo przyjęto, jako min. 2-2.5m.

W przypadku alarmu operator w pomieszczeniu Centrum Monitoringu ma otrzymać sygnał alarmowy w systemie prezentacji obrazu w formie okienka (popup), gdzie ma pojawić się obraz z kamery, która wygenerowała alarm.

W celu zapewnienia odpowiedniej jakości obrazu do weryfikacji zdarzeń, wymagany jest taki dobór i rozmieszczenie kamer stałopozycyjnych, aby zapewnić odwzorowanie min. 125 px/m na granicy zasięgu kamery. Należy zastosować kamery zapewniające efektywne i równomierne podświetlenie sceny w całym przyjętym zasięgu kamery.

Przewidywana min. ilość kamer typu 1:

EC Żerań - 39 szt.,

EC Siekierki - 58 szt.

W obszarach, gdzie skomplikowany przebieg ogrodzenia wymusza zastosowanie w jednym miejscu kilku kamer zamawiajacy dopuszcza wykorzystanie zintegrowanych zespołów kamerowych o parmetrach nie gorszych niż kamera typu 1 umożliwiających pokrycie pola obserwacji o kącie do 360o (kamera typ 2).

Przewidywana możliwość zastosowania kamer typu 2:

EC Żerań – 5 szt.,

EC Siekierki - 6 szt.

* 1. **Podsystem głowic szybkoobrotowych**

Podsystem głowic szybkoobrotowych ma zapewnić na całej długości ogrodzenia (wraz z elewacjami budynków stanowiących granicę obiektu) weryfikację wideo zdarzeń alarmowych oraz identyfikację i możliwość śledzenia intruza. Wymagany jest taki dobór i rozmieszczenie głowic szybkoobrotowych (kamera typ 3), aby zapewnić odwzorowanie min. 250 px/m na granicy zasięgu kamery. Należy zastosować dalekozasięgowe zespoły optoelektroniczne (głowica szybkoobrotowa z optyczną stabilizacją obrazu doświetleniem IR lub laserowym) o dużym zasięgu do identyfikacji i śledzenia intruza.

Przewidywana min. ilość kamer typu 3:

EC Żerań - 8 szt.,

EC Siekierki - 9 szt.

1. **System nadzoru nad ruchem osobowym.**

Nadzór nad ruchem osobowym na terenie zakładów Zamawiającego odbywać się będzie z wykorzystaniem:

* Systemu kontroli dostępu;
* Depozytorów kluczy;
* Telewizji dozorowej.
	1. **System Kontroli Dostępu.**

Przewiduje się konieczność pełnej integracji istniejącego systemu KD z platformą zarządzania bezpieczeństwem SZB zgodnie z opisem w dalszej części opracowania. Wykonawca może zaproponować wymianę sytemu na inny pod warunkiem odtworzenia wszystkich istniejących funkcji systemu oraz zapewnieniu nowych funkcjonalności opisanych w dalszej części opisu. SKD powinien umożliwiać zapisanie danych osobowych (imię, nazwisko, typ i numer dokumentu tożsamości). Wszystkie dane (logi) w bazie SKD nie powinny być przechowywane dłużej niż 5 lat. Wszystkie odczyty/dane starsze niż 4 lata i 11 miesięcy powinny być automatycznie usuwane po tym okresie.

Przewiduje się rozbudowę istniejących autonomicznych systemów KD firm Roger, KABA i Siemens poprzez wymianę ich na jednolite urządzenia współpracujące z systemem głównym. Po przeprowadzeniu niezbędnych prób i testów elementy wykonawcze i detekcyjne mogą pozostać bez zmian. Do wymiany mogą zostać zakwalifikowane jedynie kontrolery i czytniki.

Urządzenia Roger

• 8 czytników (w dwóch Zakładach)

Urządzenia Siemens:

• 14 czytników (w dwóch Zakładach)

Urządzenia Kaby:

• 26 kontrolerów (w pięciu Zakładach),

• 132 czytników (w pięciu Zakładach),

EC Żerań - 8 przejść jednostronnych,

EC Siekierki - 6 przejść jednostronnych,

Należy przyjąć konieczność objęcia bezprzewodową kontrolą dostępu (zamki typu hotelowego, online, zintegrowane z systemem kontroli dostępu):

EC Żerań - ok. 30 przejść w budynku biurowym

EC Siekierki – ok. 3 przejść.

System SKD powinien posiadać funkcję:

* Tworzenia kart dostępowych ze zdjęciem osoby (drukowania naklejek na karty magnetyczne) i dodawania schematów dostępowych przez uprawnionego Operatora.
* „Anty passback” na wszystkich wejściach i bramach głównych (ochrona obwodowa). Karty wydane Służbie ochrony oraz upoważnionym przedstawicielom PGNiG TERMIKA SA (np. Specjaliści ds. Bezpieczeństwa) powinny być wyłączone z tej funkcji.
* raportu „Monit o zwrot kart” – jeżeli termin ważności nadanych uprawnień upłynął (lista niezwróconych kart po 48 godz. od terminu upływu ich ważności z podziałem na firmy oraz informacjami o osobach, którym została wydana karta i jej numerze).
* „Alarm naruszenia strefy” – siłowe próby wejścia bez kart.
* „Raport o obecności” (zaawansowane raportowanie o osobach, firmach, przejściach przez terminale, pojazdach na terenie itp. z możliwością eksportu danych do np. xls.).
* SKD musi posiadać integrację z systemem SAP ERP (HR), w zakresie pobierania (odczytu) z bazy SAP ERP nowych użytkowników (nowych pracowników) i automatycznego dodania do SKD zgodnie z nadanymi uprawnieniami dostępowymi (z automatu pracownik PGNiG TERMIKA SA powinien otrzymać podstawowy dostęp do wszystkich Zakładów przez 24h/dobę – wszystkie podstawowe wejścia/wyjścia osobowe) oraz odbierania uprawnień osobom, z którymi rozwiązano umowę o pracę. Nowy system powinien umozliwić “płynne” przejście ze starego systemu, bez zakłóceń wynikających z braku mozliwości dostania się pracowników obiekt oraz powinien poprawnie funkcjonować w przypadku autoryzowanych aktualizacji wykonywanych w systemie SAP ERP.
	1. **Elektroniczne depozytory kluczy**

W celu prawidłowego zarządzania obiegiem kluczy, terenie ECZ i ECS przewidziano zainstalowanie elektroniczne depozytory kluczy. Zastosowane depozytory mają pozwolić na płynną konfigurację parametrów pracy, dzięki czemu administrator systemu będzie miał możliwość decydowania o tym, kto, kiedy i do jakich kluczy lub skrytek będzie miał dostęp. W ramach konfiguracji będzie też można zdecydować, czy dany klucz lub dokument zawsze musi trafić do tego samego depozytu czy też do dowolnego, wolnego miejsca w depozytorze.

Przyjęto, że pobieranie oraz deponowanie kluczy możliwe będzie przy użyciu tych samych kart zbliżeniowych (obecnie stosowanych), którymi pracownicy będą posługiwali się w systemie SKD do codziennego poruszania się po terenie obiektów. Zintegrowanie depozytorów z SKD, CCTV oraz z systemem zarządzania bezpieczeństwem pozwoli na automatyczną aktualizację uprawnień dysponowania kluczami stosownie do zmian uprawnień dostępu w SKD oraz na podgląd obrazu z kamery CCTV w czasie pobierania lub zdawania kluczy. System powinien posiadać funkcjolanlość ochrony przed kopiowaniem kluczy, np. poprzez uniemożliwienie opuszczenia obiektu bez pozostawienia kluczy w dyspozytorze.

Na terenie ECZ przewidziano montaż depozytorów w trzech skrzydłach budynku biurowego na pięciu kondygnacjach. Przewiduje się zamontowanie do 15 depozytorów o różnych pojemnościach kluczy oraz 1 depozytor wyposażony w 20÷30 skrytek pozwalających zdeponować kasetki z kluczami i dokumenty. Łącznie depozytory powinny umożliwić zdeponowanie 350÷400 kluczy oraz min. 20 kasetek z kluczami i dokumentami.

Na terenie ECS zaplanowano instalację 3 depozytorów kluczy, dających możliwość zdeponowania do 150 kluczy (ilość do zweryfikowania).

* 1. **System Telewizji Dozorowej.**

Na potrzeby kontroli ruchu osobowego na terenie obiektu przewiduje się zainstalowanie:

1. portiernie, teren budowy EC - automatyczne zespoły kamerowe wyposażone w kamerę ogólną o stałej ogniskowej pracującą z kamerą PTZ automatycznie przechwytującą cechy osobowe posiadające integracje z systemem, który potrafi odbierać odpowiednie dla tego typu analizy metadane (kamera typ 4)

Przewidywana min. ilość kamer typu 4:

* EC Żerań - 3 szt.,
* EC Siekierki - 2 szt.
1. wejścia osobowe przez kołowroty - kamery stało pozycyjne automatycznie przechwytujące cechy osobowe posiadające integrację z systemem, który potrafi odbierać odpowiednie dla tego typu analizy metadane (kamery typ 5)

Przewidywana min. ilość kamer typu 5:

* EC Żerań - 3 szt.,
1. przy wejściach osobowych inteligentne kamery stereoskopowe służące do identyfikacji twarzy (kamera typ 6).

Przewidywana min. ilość kamer typu 6:

* EC Żerań - 4 szt.,
* EC Siekierki - 2 szt.
1. wszystkie ciągi komunikacyjne w budynku biurowym ECZ i ECS - kamery kopułkowe, min. 2 MPx, pracujące w trybie korytarzowym, zapewniające min. 125px/m, z obudową antyrefleksyjną (kamery typ 7).

Przewidywana min. ilość kamer typu 7:

* EC Żerań - 68 szt.,
* EC Siekierki - 26 szt.
1. drogi wewnętrzne. W celu zapewnienia odpowiedniej jakości obrazu do weryfikacji zdarzeń, wymagane jest taki dobór i rozmieszczenie kamer stałopozycyjnych, aby zapewnić odwzorowanie min. 125 px/m na granicy zasięgu kamery. Należy zastosować kamery, których moduł IR zapewnia efektywne i równomierne podświetlenie sceny w całym przyjętym zasięgu kamery. Kamery swoim zasięgiem powinny pokrywać cały obszar wyznaczonych dróg. Obszary dróg, które należy objąć nadzorem kamer pokazano w załącznikach graficznych: załącznik nr 1 - EC Żerań i załącznik nr 2 EC Siekierki. Do spełnienia w/w wymagań dobrano kamerę o przetworniku pracującym w rozdzielczości min. 1080p pracującą w trybie korytarzowym, aby zapewnić rozdzielczość pionową min. 1920pix. (kamera typ 1). Należy stosować kamery z mechanicznym filtrem IR i z wysoką dynamiką przetwornika WDR min. 120dB. Kamery zainstalowane na drogach wewnętrznych służyć będą również do nadzoru ruchu samochodów.

Przewidywana min. ilość kamer typu 1:

* EC Żerań - ok. 26 szt.,
* EC Siekierki – ok. 58 szt.

Dopuszcza się w uzgodnieniu ze Zleceniodawcą wykorzystanie zintegrowanych zespołów kamerowych umożliwiających pokrycie pola obserwacji o kącie do 360O (kamera typ 2).

1. hale maszyn ECZ i ECS - przewiduje się wykorzystanie zintegrowanych zespołów kamerowych umożliwiających pokrycie pola obserwacji o kącie do 360 st. (kamera typ 2) zapewniających monitoring całości powierzchni najwyższego poziomu hali maszyn.

Przewidywana min. ilość kamer typu 2:

* EC Żerań - 2 szt.,
* EC Siekierki - 3 szt.

Kamery, które wyposażone są w algorytmy detekcji i przechwytywania twarzy, przechwytywania obiektów i tryb pracy perymetrycznej w obrazie wideo powinny być zbudowane są z dwóch urządzeń, czyli kamery panoramicznej i PTZ pracujących w oparciu o wspólny firmware. Szacowane prawdopodobieństwo rozpoznania musi wynosić nie mniej niż 90%.

Podsystem nadzoru CCTV nad ruchem osobowym musi zapewnić następujące funkcje:

* detekcja obiektu z rozróżnieniem na pojazd, sylwetka ludzka, twarz, przy czym wszystkie typy obiektów mogą być rozróżniane jednocześnie z zaznaczeniem typu obiektu
* detekcja twarzy wraz z zapewnieniem zrzutu zdjęcia
* ochrona perymetryczna, jako funkcja kamery panoramicznej ze wspomaganiem kamery PTZ, która po wykryciu obiektu zapewnia automatyczne zbliżenie na obiekt.
* wyszukiwanie w zarejestrowanym materiale we wskazanym przedziale czasowym, na wybranym obszarze osób o określonych cechach (np: kobieta/mężczyzna, w okularach/bez, kolor ubrania, z torbą, plecakiem, w kasku, poruszających się we wskazanym kierunku)
* wyszukiwanie online w obszarze pokrytym kamerami osób wskazanych na materiale archiwalnym lub osób i określonych cechach (np: kobieta/mężczyzna, w okularach/bez, kolor ubrania, z torbą, plecakiem, w kasku)
* system rozpoznawania twarzy połączony z systemem kontroli dostępu i dopiero po podwójnej weryfikacji przez system KD i VCA użytkownik ważnej przepustki zostanie wpuszczony do obiektu. W przypadku negatywnej weryfikacji przez którykolwiek system operator dyżurny otrzyma sygnał alarmowy.

System w trakcie pracy wraz z zapisanym materiałem wideo buduje bazę danych, tagowanych zdjęć, które posłużyć mogą do dalszej analizy. Algorytm wykorzystywany będzie w dwojaki sposób:

* Analityka w czasie rzeczywistym pracująca z predefiniowaną bazą danych w systemie nadzoru. System posiada zaimplementowaną bazę danych uprawnionych użytkowników i na podstawie porównania obrazu z kamery ze zdjęciem z bazy danych wypracowywana jest decyzja o dalszej akcji przewidzianej w wymogach operacyjnych systemu. W przypadku, kiedy system nie znajdzie użytkownika generuje „alarm obcego”.
* Analityka wsteczna materiału nagranego. W tym przypadku system na podstawie wprowadzonego z zewnątrz zdjęcia/obrazu wyszukuje twarz, która z określonym przez użytkownika prawdopodobieństwem odpowiada twarzy referencyjnej. Wynik podawany jest z określonym prawdopodobieństwem, a obrazy umożliwiają szybki podgląd nagranego materiału. Dodatkowo w przypadku pracy z bazą danych możliwe jest wyszukiwanie użytkowników nie tylko po zdjęciach, ale po zapisanych danych typu imię, nazwisko, dział itd.
1. **System nadzoru nad ruchem pojazdów.**

Nadzór nad ruchem pojazdów na terenie zakładów Zamawiającego odbywać się będzie z wykorzystaniem:

* Systemu kontroli dostępu;
* Telewizji dozorowej;
* Analityki obrazu.
	1. **System Kontroli Dostępu.**

System kontroli dostępu będzie realizował automatyczne podnoszenie szlabanów na bramach wjazdowych na teren parkingów. Wjazd dostaw na teren zakładów odbywać się będzie po rozpoznaniu numerów rejestracyjnych pojazdów przez system LPR.

* 1. **System Telewizji Dozorowej.**

Na potrzeby nadzoru nad ruchem pojazdów na terenie obiektu zainstalowane zostaną kamery w następujących obszarach:

* + 1. **Parkingi zakładowe.**

W celu zapewnienia odpowiedniej jakości obrazu do weryfikacji zdarzeń, proponowane jest zastosowanie zintegrowanych zespołów kamerowych umożliwiających pokrycie pola obserwacji o kącie 360O (kamer typu 2) i kamer PTZ z głowicą szybkoobrotową (kamera typu 3), panoramicznych zespołów kamerowych zintegrowanych z głowicą szybkoobrotową (kamery typ 8) lub (po uzgodnieniu ze Zleceniodawcą) kamer stałopozycyjnych (kamera typ 1), które swoim zasięgiem powinny stale pokrywać cały obszar parkingu. Przyjęte rozwiązanie powinno zapewnić jakość obrazu min. 125px/m i zapewniać efektywne i równomierne podświetlenie sceny w całym przyjętym zasięgu kamery. Obszary parkingów które należy objąć nadzorem kamer pokazano w załącznikach graficznych: załącznik nr 1 - EC Żerań i załącznik nr 2 EC Siekierki.

Przewidywana min. ilość kamer przy zastosowaniu zintegrowanych zespołów kamerowych 360 O z kamerą PTZ (kamera typ 8):

* EC Żerań (wraz nowoprojektowanymi parkingami) – ok. 6 szt.,
* EC Siekierki – ok. 4 szt.
	+ 1. **Bramy i wagi samochodowe.**

W celu zapewnienia odpowiedniej jakości obrazu do weryfikacji zdarzeń, wymagane jest taki dobór i rozmieszczenie kamer stałopozycyjnych, aby zapewnić prawidłowe odczytywanie nr rejestracyjnych z tablic wjeżdżających i wyjeżdżających pojazdów. Kamery swoim zasięgiem powinny pokrywać cały obszar bramy/wagi, oraz umożliwić weryfikację zawartości otwartych naczep samochodów wjeżdżających i wyjeżdżających. Bramy które należy objąć nadzorem kamer pokazano w załącznikach graficznych: załącznik nr 1 - EC Żerań i załącznik nr 2 EC Siekierki.

Do spełnienia w/w wymagnia należy zastosować kamerę przeznaczoną do nadzoru ruchu drogowego (kamera typ 9), o przetworniku pracującym w rozdzielczości min. 1080p. Należy stosować kamery z mechanicznym filtrem IR i z wysoką dynamiką przetwornika WDR min. 120dB. i bardzo wysoką czułością przetwornika

Przewidywana min. ilość kamer typu 9:

* EC Żerań – ok. 11 szt.;
* EC Siekierki – ok. 7 szt.
	+ 1. **Bramy kolejowe**

W celu zapewnienia odpowiedniej jakości obrazu do weryfikacji zdarzeń, wymagane jest taki dobór i rozmieszczenie kamer stałopozycyjnych (kamera typ 5), aby umożliwić weryfikację zawartości otwartych wagonów kolejowych wjeżdżających i wyjeżdżających. Kamery swoim zasięgiem powinny pokrywać cały obszar bramy. Bramy które należy objąć nadzorem kamer pokazano w załącznikach graficznych: załącznik nr 1 - EC Żerań i załącznik nr 2- EC Siekierki.

Przewidywana min. ilość kamer typu 5:

* EC Żerań – ok. 3 szt.,
* EC Siekierki –1 szt.
	+ 1. **Stacja paliw**

W celu zapewnienia odpowiedniej jakości obrazu do weryfikacji zdarzeń w rejonie stacji paliw, wymagane jest taki dobór i rozmieszczenie kamer stałopozycyjnych, aby zapewnić odwzorowanie min. 125 px/m na granicy zasięgu kamery. Należy zastosować kamery, których moduł IR zapewnia efektywne i równomierne podświetlenie sceny w całym przyjętym zasięgu kamery.

Przewidywana min. ilość kamer typu 5:

* EC Żerań - 1 szt.,
* EC Siekierki - 1 szt.
	+ 1. **Drogi wewnętrzne przeznaczone do ruchu samochodów dostawców i podwykonawców.**

Nadzór nad wyznaczonym obszarem dróg wewnętrznych prowadzony będzie przez podsystem kamer stałopozycyjnych do nadzoru ruchu osobowego (patrz pkt. 3.3 e). Dodatkowo aby zapewnić odpowiednią kontrolę nad ruchem pojazdów należy uzupełnić ww. podsystem o tak dobrane i rozmieszczone kamery stałopozycyjne, aby zapewnić odczyt tablic rejestracyjnych i kontrolę prędkości pojazdu na każdym wyznaczonym do nadzoru odcinku drogi. Obszary dróg, które należy objąć nadzorem kamer pokazano w załącznikach graficznych: załącznik nr 1 - EC Żerań i załącznik nr 2 EC Siekierki.

Do spełnienia w/w wymagań dobrano kamerę przeznaczoną do nadzoru ruchu drogowego, o przetworniku pracującym w rozdzielczości min. 1080p pracującą w trybie korytarzowym, aby zapewnić rozdzielczość pionową min. 1920pix. (kamera typ 9). Tak zdefiniowany tor optyczny zapewnia funkcję identyfikacji tablic rejestracyjnych dla przewidywanego rozmieszczenia kamer. Należy stosować kamery z mechanicznym filtrem IR i z wysoką dynamiką przetwornika WDR min. 120dB i bardzo wysoką czułością przetwornika, zapewniającą odczyt tablic rejestracyjnych do prędkości pojazdu min. 80km/h. Należy zastosować kamery, których moduł IR zapewnia efektywne i równomierne podświetlenie sceny w całym przyjętym zasięgu kamery.

Przewidywana min. ilość kamer typu 9:

* EC Żerań - 10 szt.,
* EC Siekierki - 20 szt.

Podsystem kamer do nadzoru ruchu pojazdów musi zapewnić:

* automatyczny odczyt tablic rejestracyjnych (wszystkie bramy, wagi samochodowe, każdy wskazany odcinek drogi)
* śledzenie trasy przejazdu,
* wykrycie wjazdu pojazdu do strefy niedozwolonej,
* wykrycie przekroczenia dopuszczalnej szybkości,
* zatrzymanie/postój pojazdu w miejscu niedozwolonym,
* wyszukiwanie w zarejestrowanym materiale pojazdów o wskazanych parametrach np.: numerach rejestracyjnych, kolorze, rodzaju pojazdu.

Zleceniodawca dopuszcza w uzgodnionych z nim miejscach zastosowanie kamer wielosensorycznych (kamery typu 2).

1. **Infrastruktura kablowa**
	1. **Okablowanie strukturalne dla potrzeb CCTV**

W ramach niniejszego zadania przewidywana jest rozbudowa istniejącej sieci światłowodowej oraz miedzianej o dodatkowe linie kablowe wynikających z budowy nowych punktów kamerowych, oraz wymiana części okablowania jeżeli zajdzie taka konieczność. Do okablowania transmisyjnego nowych szafek rozdzielczych SR należy użyć zewnętrznych kabli światłowodowych FO-4G-OM3. Okablowanie pomiędzy szafkami SR, a kamerami należy wykonać zewnętrznymi kablami typu FTP kat.6.

Dopuszcza się wykorzystanie istniejącego okablowania światłowodowego po wykonaniu pomiarów sprawdzających.

* 1. **Linie zasilające**

Linie zasilające skrzynki rozdzielcze SR należy wykonać kablami typu YKYżo o odpowiednim przekroju żył z istniejących rozdzielnic dedykowanych do zasilania systemów bezpieczeństwa. Po wykonaniu bilansu mocy dla projektowanych systemów bezpieczeństwa należy przebudować rozdzielnice zasilające systemy bezpieczeństwa.

Dopuszcza się wykorzystanie istniejącego okablowania zasilającego po wykonaniu pomiarów sprawdzających.

1. **Podsystemu ochrony technicznej wybranych budynków**

Z projektowanym systemem PSIM należy zintegrować istniejące lokalne systemy alarmowe w obiekcie EC Żerań oraz istniejące systemy alarmowe w obiekcie EC Siekierki (ok. 10 systemów).

1. **Platformy systemu zarządzania bezpieczeństwem**

Physical Security Information Management (PSIM) jest nowym standardem integrującym różnorodne systemy i aplikacje bezpieczeństwa, pozwalającym na ich kontrolę przez spójny, przejrzysty i jednorodny interfejs użytkownika. Interfejs ten umożliwia zabieranie i korelację zdarzeń z wielu urządzeń, rozproszonych systemów bezpieczeństwa, takich jak system telewizji dozorowej (CCTV) z analizą wizyjną, system kontroli dostępu (SKD), system sygnalizacji włamania i napadu (SSWiN) oraz system depozytorów kluczy.

Platforma powinna być w pełni zintegrowana z SKD, SSWiN, CCTV, LPR, depozytorami kluczy, modułem awizacji dostaw (system bazodanowy Zamawiajacego oparty o MS SQL server). Powinna posiadać możliwość zarządzania uprawnieniami Operatorów przez Administratora (dodawanie/odbieranie dostępu do wybranych modułów i funkcji), jak również podglądu wykonywanych przez nich czynności. Platforma musi posiadać moduł procedur postępowania w przypadku pojawienia się alarmu lub wystąpienia nieprzewidzianego zdarzenia – umożliwiający tworzenie procedur postępowania zgodnie z przyjętym przez PGNiG TERMIKA SA schematem przepływu informacji. PSIM musi posiadać moduł awizacji dostaw zintegrowany z obecnym SKD, CCTV i LPR.

* 1. **Integracja z systemem telewizji dozorowej.**
* Wywołanie okna widoku kamery CCTV w sytuacjach alarmowych wywołanych przez system KD lub SSWiN (obraz wideo wspiera procesy decyzyjne w systemie).
* Rozpoczęcie zapisu materiału wideo z kamer systemu CCTV, w momencie wystąpienia określonych zdarzeń w pozostałych systemach (KD, SSWiN,). Zapisany materiał jest przypisany do konkretnego zdarzenia.
* Integracja funkcji analitycznych rozpoznawania numerów rejestracyjnych aut realizowaną przez system CCTV, identyfikacji twarzy z systemem kontroli dostępu, analiza obrazu bezpośrednio z kamer lub z nagranego materiału (wyszukiwanie osób, trasy przejścia z kilku kamer, wyszukiwanie cech charakterystycznych – koloru ubioru, płci, posiadania kamizelek odblaskowych, toreb, kasków). Numer rejestracyjny lub cechy charakterystyczne twarzy mogą pełnić rolę karty dostępowej w systemie kontroli dostępu.
* Przesłanie informacji o przekroczeniu wirtualnej linii i detekcji ruchu do systemu SMS oraz rozpoczęcie określonej procedury alarmowej.
* Prezentacja bezpośrednio na mapie synoptycznej obrazu z kamer. Dodatkowo możliwość wysterowania kamer PTZ oraz realizację „presetu” bezpośrednio z mapy synoptycznej.
* Odtworzenie materiału z kamer w trybie “na żywo” oraz materiału nagranego.
* Sterowanie kamerami PTZ przy pomocy pulpit programowego.
* Wykonanie tzw. “stop klatki” z kamery oraz podpięcie jej do raportu ze zdarzenia (wysyłanego zgodnie z opracowaną procedurą).
	1. **Integracja z systemem kontroli dostępu**

W systemie mają zostanć przedstawione stany przejść, a także czujników zamknięcia drzwi, czytników i przycisków w miejscach ich lokalizacji na planach sytuacyjnych (architektonicznych) oraz na schematach zbiorczych. Operator musi otrzymać nie tylko informacje o stanie urządzeń systemu kontroli dostępu, ale także informacje o numerze identyfikatora osobistego. Z poziomu systemu operator będzie mógł sterować drzwiami kontroli dostępu np. otworzyć na chwilę , odtworzyć na stałe, zablokować drzwi. Dla każdych drzwi z czytnikami i przyciskami ma być zdefiniowana procedura działania, plan sytuacyjny. Sygnały z systemu kontroli dostępu poprzez zdefiniowanie automatycznych procedur działania i automatycznych sterowań będą mogły wywoływać działania innych zintegrowanych systemów np. identyfikacja twarzy osoby wchodzącej ma spowodować automatyczne zapewnienie dostepu do budynku lub przyłożenie karty do czytnika ma powodować, że w systemie pokazywane jest zdjęcie danej osoby, a następnie dzięki integracji z systemem CCTV na monitorze wywoływany jest obraz z najbliższej kamery powiązanej z danym czujnikiem.

Platforma PSIM musi posiadać przetestowany i wdrożony interfejs komunikacyjny do integracji z SKD. Moduł SKD musi posiadać narzędzie raportowania o ilości osób na terenie Zakładów PGNiG TERMIKA z podziałem na firmy, Departamenty, Wydziały itd. Moduł powinien posiadać bazę osób niepożądanych.

Moduł SKD musi pozwalać na automatyczne porównanie aktualnego zdjęcia osoby wchodzącej do obiektu ze zdjęciem z bazy danych w chwili zbliżeniu karty magnetycznej (przepustki-identyfikatora) przez tą osobę do czytnika. Funkcja ta musi działać również po fakcie wraz z funkcją nagranego materiału (wyszukiwanie odczytu z danego przejścia w wybranym przedziale czasowym z identyfikacją osoby wchodzącej).

Integracja ma umożliwić nadzorowanie następujących stanów systemu KD :

* stany kontrolerów,
* stany wszystkich wejść cyfrowych w kontrolerach (spoczynek, alarm),
* stany wszystkich przekaźników w kontrolerach (wyłączony, włączony),
* stany logiczne drzwi (otwarte, otwarte na stałe, zamknięte,
* zablokowane),
* alarmy drzwi (drzwi za długo otwarte, drzwi otwarte bez autoryzacji),
* stany logiczne czytników (aktywny, zablokowany).
* próba użycia nieważnej lub nieznanej karty o danym numerze,
* próba podwójnego wejścia przy pomocy karty o danym numerze,
* użycie aktywnej karty o danym numerze.

Integracja ma umożliwić następujące sterowanie systemem KD :

* wysterowanie dowolnego przekaźnika w dowolnym kontrolerze na
* określony czas lub na stałe,
* zezwolenie na jednorazowe wejście,
* otwarcie drzwi na stałe,
* zablokowanie drzwi,
* zablokowanie czytnika.
	1. **Integracja z systemem sygnalizacji włamania i napadu**

W systemie muszą zostanć przedstawione stany stref, a także wszystkich czujników podłączonych do linii wejściowych (czujki PIR, kontaktrony, przyciski napadowe, czujniki zaryglowania itp.) w miejscach ich lokalizacji na planach sytuacyjnych (architektonicznych) oraz na schematach zbiorczych. Z poziomu systemu operator będzie mógł sterować strefami SSWiN np. uzbroić, rozbroić (w trybie szybkim i zwłocznym), wygenerować alarm włamaniowy, załączać wyjścia cyfrowe i sygnalizację, potwierdzać i kasować alarmy. Dla każdego komponentu stref zostanie zdefiniowana procedura działania, plan sytuacyjny. Sygnały z systemu sygnalizacji włamania i napadu poprzez zdefiniowanie automatycznych procedur działania i automatycznych sterowań będą mogły wywoływać działania innych zintegrowanych systemów np. uzbrojenie lub rozbrojenie strefy powoduje, że w systemie pokazywane jest zdjęcie danej osoby, a następnie dzięki integracji z systemem CCTV na monitorze wywoływany będzie obraz z najbliższej kamery powiązanej z danym czujnikiem.

Integracja ma umożliwić nadzorowanie następujących stanów systemu SWiN :

* stany centrali,
* stany wszystkich wejść cyfrowych w centrali (spoczynek, alarm),
* stany wszystkich przekaźników w centrali (wyłączony, włączony),
* stany stref (uzbrojona, rozbrojona),
* alarmy stref (włamanie, napad, sabotaż, awaria),
* stany klawiatur (praca, awaria, sabotaż),

Integracja ma umożliwić następujące sterowanie systemem SWiN :

* uzbrojenie i rozbrojenie strefy
* wysterowanie dowolnego przekaźnika w centrali na określony czas lub na stałe,
* potwierdzenie alarmu,
* kasowanie alarmu,
* zablokowanie strefy,
* zablokowanie dowolnego urządzenia wejściowego.

Moduł SSWiN musi posiadać możliwość odebrania sygnału alarmowego i pozwalać na automatyczne wyświetlenie miejsca zdarzenia na mapie synoptycznej monitora alarmowego oraz funkcję weryfikacji podglądu CCTV (z najbliższych kamer) obrazu aktualnego i materiału nagranego (na chwilę przed pojawieniem się alarmu).

* 1. **Integracja z podsystemem zarządzania kluczami**

Moduł obsługujący dystrybuowanie kluczy powinien być zintegrowany z SKD i CCTV. Powinien wskazać czas pobrania/zdania klucza przez uprawnionego oraz nagrany materiał video skorelowany z tym zdarzeniem. Moduł ten powinien posiadać bazę pobrań kluczy przez okres min. 31 dni (zalecane 90 dni). Pobieranie klucza z depozytora powinno następować po zbliżeniu karty dostępowej, a w przypadku pomieszczeń o szczególnym znaczeniu również po wprowadzeniu kodu PIN na klawiaturze szyfrowej. Integracja ma umożliwiać:

* Przesyłanie informacji między depozytorami i platformą PSIM w czasie rzeczywistym.
* Wizualizację stanu depozytora i kluczy na mapie synoptycznej. Statusy obiektów reprezentowane będą za pomocą dowolnie skonfigurowanych ikon.
* Wyświetlanie informacji o zdarzeniach dotyczących depozytorów oraz kluczy.
* Konfigurację zdarzeń w systemie SMS w odpowiedzi na pojawienie się określonego zdarzenia, np. wyzwolenie widoku kamery CCTV; stworzenie procedur postępowania, które musi zrealizować operator na wypadek zdarzenia.
* Tworzenie użytkowników w bazie danych depozytora z poziomu systemu SMS.
* Synchronizację danych użytkowników między systemami.
* Nadanie uprawnień do danych kluczy depozytora z poziomu systemu SMS. Następnie automatyczne wysłanie do depozytora.

Moduł powinien być tak zintegrowany z SKD, aby uniemożliwić opuszczenie terenu PGNiG TERMIKA SA użytkownikowi, który pobrał klucz i nie zdał go do depozytora. W sytuacji kiedy jest kilku użytkowników jednego pomieszczenia z uprawnieniami do pobierania kluczy, to system powinien uniemożliwić wyjście ostatniego użytkownika pomieszczenia, jeśli nie zdał klucza. Jednocześnie Operator systemu powinien mieć możliwość odblokowania możliwości wyjścia takiego użytkownika po wyjaśnieniu zdarzenia.

* 1. **Aplikacja Mobilna.**

W celu weryfikacji zdarzeń generowanych przez systemy bezpieczeństwa oraz ochrony obwodowej należy przewidzieć zastosowanie dedykowanej aplikacji mobilnej instalowanej na urządzeniach przenośnych (typu Smartfon-PDA). Funkcjonalność ta ma być wdrożona, przetestowana i wyłączona. Zmawiający ma mieć możliwość uruchomienia jej w przyszłości samemu bez konieczności dodatkowych opłat technicznych i licencyjnych.

System ma umożliwiać przekazywanie zdarzeń w celu obsługi operatorom mobilnym wyposażonym w PDA (ang. Personal Digital Assistant) w formie urządzeń przenośnych bazujących na systemie Android w wersji 4.1 lub nowszej.

Aplikacja mobilna ma pozwalać na przekazywanie informacji od operatora PSIM do użytkownika mobilnego (np. Patrol) wraz z opisem zdarzenia, mapką z zaznaczonym miejscem wystąpienia oraz aktualnym zrzutem obrazu z kamery, a także zgłoszenie zdarzenia alarmowego przez operatora mobilnego do centrum dowodzenia wraz ze zdjęciem wykonanym przez PDA (wybór z galerii lub aparatu).

Informacje dla dyspozytora przesyłane mają być przy wykorzystaniu transmisji danych. Operator może przypisać strażnika przez aplikację. Strażnicy muszą odpowiadać z wykorzystaniem aplikacji na PDA, aktualizować jego stan oraz dodatkowe informacje i dalej informacje te są wysyłać do operatora. Stany zdarzeń i sytuacji strażników mają być wyświetlane na mapach.

Dyspozytor w systemie ma mieć możliwość przydzielania zdarzeń operatorom mobilnym i kontrolowania statusu poszczególnych zadań oraz strażników.

W przypadku obsługi zdarzeń za pomocą urządzenia mobilnego, zarówno strażnik jak i operator mają mieć do dyspozycji mapę z zaznaczonymi lokalizacjami i stanami zdarzeń oraz pozostałych PDA. Strażnicy mogą podejmować zadania z listy zdarzeń lub otrzymywać zadania przydzielone im przez dyspozytora. Użytkownik PDA ma mieć możliwość dodawania do zadań krótkich komentarzy, załączania zdjęć oraz zmiany statusu zdarzenia.

Aplikacja mobilna musi pozwalać również na zgłaszanie problemów. Definiowanie zdarzenia odbywać się może poprzez określenie jego typu, zamieszczenie krótkiego opisu, przypisanie priorytetu. Lokalizacja wyznaczana będzie na podstawie sygnału GPS lub koordynat wifi. Opcjonalnym jest dodanie zdjęcia z miejsca zdarzenia. Po wysłaniu zdarzenie zostaje automatycznie dodane do listy zdarzeń.

1. **Zabezpieczenie przeciwprzepięciowe.**

Należy zaprojektować i wykonać system ochrony przed przepięciami instalacji i urządzeń CCTV składający się z układów zabezpieczających zarówno poszczególne punkty kamerowe, jak i urządzenia umieszczone w centrum nadzoru wizyjnego (rejestratory, monitory itp.). Ochrona przed przepięciami powinna być zapewniona zarówno od strony zasilania jak i wszelkich linii sygnałowych (tory wizji, sterowanie kamer, itp.).

Ochrona przed przepięciami powinna być projektowana zgodnie ze strefową koncepcją ochrony opisaną w serii norm PN-EN 62305.

LPZ 0 – strefa zewnętrzna z wyróżnieniem LPZ 0A gdzie występuje zagrożenie wyładowaniem bezpośrednim i LPZ 0B tworzona przez układ zwodów instalacji odgromowej, LPZ 1 – wnętrze budynku, LPZ 2 – pomieszczenie centrum nadzoru wizyjnego (LPZ 2 zawiera się w LPZ 1).

Złącza ochrony przed przepięciami należy stosowac na granicach wydzielonych stref LPZ.

Należy stosować ograniczniki przepięć dedykowane do ochrony sieci Ethernet oraz systemów CCTV IP kompatybilny z wszystkimi standardami PoE.

• Napięcie znamionowe – 60 V DC

• Największe napięcie trwałej pracy – 65 V DC/ 45 V AC

• Maksymalny prąd obciążenia – 1,5 A

• Znamionowy prąd piorunowy (10/350 µs)/ linię - ≤1,0 kA

• Maksymalny prąd wyładowczy (8/20 µs) - ≤2,5 kA

• Napięciowy poziom ochrony żyła-żyła - ≤ 120 V

• Napięciowy poziom ochrony żyła-PE - ≤ 700 V

• Maksymalna częstotliwość pracy (3dB) – typ. 250 kHz

1. **Zasilanie podstawowe i awaryjne systemu**

Projektowane urządzenia systemów zabezpieczenia technicznego należy zasilić z istniejącej infrastruktury zasilającej systemy bezpieczeństwa i rozdzielnic dedykowanych do zasilania systemów bezpieczeństwa (napięcie gwarantowane). Po wykonaniu bilansu mocy dla projektowanych systemów bezpieczeństwa, jeśli zajdzie taka konieczność, należy przebudować rozdzielnice zasilające systemy bezpieczeństwa.

Dla zasilania awaryjnego należy przyjąć:

* 24 godzinny czas podtrzymania pracy systemu SSWiN w wypadku utraty zasilania podstawowego.
* 4 godzinny czas podtrzymania pracy systemu SKD w wypadku utraty zasilania podstawowego.
* 4 godzinny czas podtrzymania pracy urządzeń w centrach monitoringu.
* 4 godzinny czas podtrzymania pracy kamer w wypadku utraty zasilania podstawowego.

Wszystkie zasilacze i UPSy w systemach bezpieczeństwa powinny być monitorowane przez nadrzędny system PSIM.

1. **Opis wymagań zamawiającego w stosunku do przedmiotu zamówienia**
2. 1. **Wymagania ogólne**

Wszystkie prace powinny być wykonywane w taki sposób, aby nie były uciążliwe dla pracowników PGNiG Termika SA oraz nie utrudniały im czynności służbowych. Wykonawca będzie prowadził modernizację w reżimie pracy ciągłej istniejącego systemu zabezpieczeń technicznych. Ewentualne odstępstwa (częściowe wyłączenia) możliwe będą po uzyskaniu zgody Zamawiającego.

Wykonawca powinien zabezpieczyć systematyczny wywóz odpadów powstałych w trakcie realizowanych robót uwzględniając koszty z tym związane w ofercie.

Wykonawca będzie zobowiązany do przyjęcia odpowiedzialności cywilnej za wyniki działalności w zakresie:

* organizacji robót,
* zabezpieczenia interesów osób trzecich,
* ochrony środowiska,
* warunków bezpieczeństwa pracy oraz ochrony przeciwpożarowej
* warunków bezpieczeństwa ruchu pieszego.

Koszty naprawy ewentualnych uszkodzeń wewnątrz obiektu oraz na zewnątrz, w tym nawierzchni dróg, chodników, posadzek, powierzchni ściennych lub sufitowych ponosi Wykonawca i powinien uwzględnić je w cenie oferty.

Wyroby stosowane w trakcie wykonywania robót mają spełniać wymagania polskich przepisów, a Wykonawca będzie posiadał dokumenty potwierdzające, że zostały one wprowadzone do obrotu zgodnie z odpowiednimi przepisami i posiadają wymagane parametry.

Zamawiający przewiduje bieżącą kontrolę wykonywanych robót.

Kontroli zamawiającego będą poddane w szczególności:

* rozwiązania projektowe zawarte w koncepcji i projekcie wykonawczym przed ich skierowaniem do realizacji – w aspekcie ich zgodności z niniejszą koncepcją oraz warunkami umowy,
* stosowane materiały i urządzenia, w odniesieniu do dokumentów potwierdzających ich dopuszczenie do obrotu oraz zgodności parametrów z danymi zawartymi w specyfikacjach technicznych,
* sposób wykonania robót w aspekcie zgodności wykonania z projektem wykonawczym, planem BIOZ i specyfikacjami technicznymi.

Dla potrzeb zapewnienia współpracy z Wykonawcą i prowadzenia kontroli wykonywanych robót oraz dokonywania odbiorów, Zamawiający przewiduje ustanowienie inspektorów nadzoru inwestorskiego w zakresie wynikającym z ustawy Prawo budowlane i postanowień umowy.

Zamawiający ustala następujące rodzaje odbiorów:

* odbiory częściowe,
* odbiory techniczne,
* odbiór końcowy.

Do robót tymczasowych będą zaliczone m.in.: organizacja robót ogólnobudowlanych, zabezpieczenia interesów osób trzecich, ochrony środowiska, tymczasowa organizacja ruchu na czas wykonywania robót, spełnienie warunków bezpieczeństwa i higieny pracy, warunków bezpieczeństwa ruchu pieszego, zabezpieczenia robót przed dostępem osób trzecich, zabezpieczenia terenu robót od następstw związanych z budową itp.

Przed przystapieniem do montażu należy przeprowadzić odbiór techniczny oferowanego sprzętu (FAT – Fabryczne Testy Akceptacyjne). Zalecane jest by odbiór odbywał się w laboratorium producenta i obejmował testy parametrów wizyjnych, rejestracji i oferowanej analityki.

Do odbioru końcowego Wykonawca przekaże Zamawiającemu dokumentację powykonawczą.

* 1. **Dokumentacja projektowa.**

Wykonawca dostarczy wykonany według norm branżowych i państwowych techniczny projekt budowlano – wykonawczy w zakresie systemu ochrony technicznej oraz instalacji zasilania urządzeń, zasilaczy UPS oraz ich monitorowania przez PSIM do zaakceptowania przez Zamawiającego. W szczególności należy uwzględnić normy:

W zakresie instalacji elektrycznej:

* PN-EN 62305-1:2011 - Ochrona odgromowa - Część 1: Zasady ogólne (oryg.)
* PN-EN 62305-4:2011 - Ochrona odgromowa - Część 4: Urządzenia elektryczne i elektroniczne w obiektach (oryg.)
* PN-IEC 60364-5-52:2002 - Instalacje elektryczne w obiektach budowlanych - Dobór i montaż wyposażenia elektrycznego – Oprzewodowanie

W zakresie systemów dozorowych CCTV stosowane w zabezpieczeniach

* PN-EN 50132-1:2010 - Systemy alarmowe - Systemy dozorowe CCTV stosowane w zabezpieczeniach - Część 1: Wymagania systemowe (oryg.)
* PN-EN 50132-5:2002 - Systemy alarmowe - Systemy dozorowe CCTV stosowane w zabezpieczeniach - Część 5: Teletransmisja (oryg.)
* PN-EN 50132-7:2003 - Systemy alarmowe - Systemy dozorowe CCTV stosowane w zabezpieczeniach - Część 7: Wytyczne stosowania.

W zakresie systemów i urządzeń transmisji alarmu

* PN-EN 50136-1-1:2007 - Systemy alarmowe - Systemy i urządzenia transmisji alarmu - Część 1-1: Wymagania ogólne dotyczące systemów transmisji alarmu

W zakresie systemów kontroli dostępu w zabezpieczeniach

* PN-EN 50133-1:2007 - Systemy alarmowe - Systemy kontroli dostępu w zastosowaniach dotyczących zabezpieczenia - Część 1: Wymagania systemowe
* PN-EN 50133-2-1:2002 - Systemy alarmowe - Systemy kontroli dostępu stosowane w zabezpieczeniach -- Część 2-1: Wymagania dla podzespołów (oryg.)
* PN-EN 50133-7:2002 - Systemy alarmowe - Systemy kontroli dostępu stosowane w zabezpieczeniach -- Część 7: Zasady stosowania (oryg.)

W zakresie systemów sygnalizacji włamania

* PN-EN 50131-1:2009 - Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Część 1: Wymagania systemowe
* PN-EN 50131-3:2010 - Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Część 3: Urządzenia sterujące i obrazujące (oryg.)
* PN-EN 50131-4:2010 - Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Część 4: Sygnalizatory (oryg.)
* PN-EN 50131-6:2009 - Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Część 6: Zasilanie

W zakresie okablowania strukturalnego

* ISO/IEC 11801:2011 “Information technology. Generic cabling for customer premises”.
* EN 50173-1:2011 „Information technology. Generic cabling systems Part 1:
General requirements”.
* TIA/EIA 568-C.2:2009 “Generic Telecommunications Cabling for Customer Premises Part 2”.
* PN-EN 50173-1:2011 „Technika informatyczna. Systemy okablowania strukturalnego. Część 1: Wymagania ogólne”.
* PN-EN 50174-1:2010 „Technika informatyczna. Instalacja okablowania. Część 1: Specyfikacja i zapewnienie jakości.”
* PN-EN 50174-2:2010 „Technika informatyczna. Instalacja okablowania. Część 2: Planowanie i wykonawstwo instalacji wewnątrz budynków.”
* PN-EN 50174-3:2005 „Technika informatyczna. Instalacja okablowania. Część 3: Planowanie i wykonawstwo instalacji na zewnątrz budynków.”
* PN-EN 50346:2009 „Technika informatyczna. Instalacja okablowania - Badanie zainstalowanego okablowania”

Wykonawca sporządzi analizę zagrożeń i wstępną koncepcję, którą zatwierdzi Zamawiający (koncepcja ma zawierać w szczególności: obliczenia dot. doboru rozdzielczości kamer i obiektywów, wynikające z nich rozmieszczenie urządzeń, tras kablowych, przyjęte systemy i urządzenia wraz ze specyfikacjami technicznymi), projekt wykonawczy dla którego uzyska akceptacje Zamawiającego oraz sporządzi dokumentację powykonawczą.

Do obowiązków Wykonawcy należy pozyskanie i weryfikacja wszystkich danych niezbędnych do prawidłowego zaprojektowania i wykonania przedmiotu Zamówienia, a w szczególności wykonanie inwentaryzacji istniejących pomieszczeń, urządzeń i sieci w zakresie potrzebnym dla sporządzenia projektu wykonawczego.

Dokumentacja projektowa winna być opracowana przez wykwalifikowanych projektantów zgodnie z polskim prawem budowlanym i polskimi normami lub odpowiednimi standardami międzynarodowymi lub Unii Europejskiej, posiadających uprawnienia do pełnienia samodzielnych funkcji technicznych w budownictwie, poświadczenia bezpieczeństwa, zgodnie z najnowszą praktyką inżynierską i najlepszą dostępną techniką. Wykonawca zapewni nadzór autorski w całym okresie realizacji Zamówienia.

Wykonawca zobowiązany jest zapewnić, że projektanci będą do dyspozycji Zamawiającego aż do daty upływu okresu zgłaszania wad.

Przedmiot zamówienia obejmuje opracowanie kompletnej dokumentacji projektowej, wykonanej zgodnie z przepisami prawa polskiego, a w tym:

* Wykonanie prac przedprojektowych takich jak sporządzenie inwentaryzacji , ekspertyz itp.;
* Opracowanie analizy zagrożeń;
* Opracowanie koncepcji;
* Opracowanie Projektu Wykonawczego, przedstawiającego szczegółowe usytuowanie wszystkich urządzeń i ich parametry wymiarowe i techniczne, szczegółową specyfikację (ilościową i jakościową) urządzeń i materiałów. Projekt wykonawczy musi uwzględniać całość prac, a w szczególności Proces migracji i przełączenia systemu.
* Zamawiający wymagał będzie przedłożenia do akceptacji Projektu Wykonawczego przed skierowaniem do realizacji.
* Opracowania Specyfikacji Wykonania i Odbioru Robót;
* Wykonanie dokumentacji powykonawczej zawierającej wszystkie powstałe w czasie realizacji zmiany względem zatwierdzonej dokumentacji wykonawczej, oraz wszystkie konieczne i wymagane przepisami testy urządzeń, systemów, przewodów, atesty na wbudowane urządzenia i materiały, ich instrukcje obsługi, protokoły uruchomieniowe określone przez instalatora, dostawcę lub producenta. Dokumentacja powykonawcza ma zawierać oświadczenie Wykonawcy i Kierownika Robót z właściwymi uprawnieniami budowlanymi dla wykonywanych prac o zgodności wykonania robót z dokumentacją powykonawczą oraz zgodnie ze sztuką budowlaną oraz obowiązującymi przepisami i warunkami technicznymi. Dokumentacja powykonawcza musi zawierać także pomiary wykonanych instalacji i sieci, w szczególności: protokoły pomiarów ciągłości instalacji, stanów izolacji oraz rezystancji linii, protokoły z pomiarów uziemień oraz świadectwa dopuszczenia na elementy systemu.

Wszelkie opłaty administracyjne ponoszone w wyniku prowadzonych działań związanych z uzyskiwaniem uzgodnień, opinii i decyzji Wykonawca winien wliczyć do ceny opracowania dokumentacji projektowej.

Dodatkowo dokumentacja projektowa powinna zwierać:

* szczegółowy harmonogram rzeczowo-finansowy robót dla zadania,
* organizację robót z uwzględnieniem jak najmniejszego zakłócenia pracy w obiekcie.

Dokumentacja musi być na bieżąco konsultowana z Zamawiając i dostarczona do zatwierdzenia Zamawiającemu w terminie umożliwiającym jej sprawdzenie i uwzględniającym czas na ewentualne korekty i poprawki.

Dokumentacja wykonawcza i powykonawcza musi zostać wykonana jako dokumentacja stanowiąca tajemnicę spółki.

* + 1. **Forma dokumentacji projektowej.**

Wykonawca dostarczy dokumentację w formie papierowej i elektronicznej.

**Forma papierowa**

Wykonawca dostarczy rysunki i pozostałe Dokumenty Zamawiającemu wchodzące w zakres dokumentacji projektowej w znormalizowanym rozmiarze (format A4 i jego wielokrotność). Obliczenia i opisy powinny być dostarczone na papierze w formacie A4. Wykonawca opracuje i dostarczy w ramach zamówienia 5 egzemplarzy kompletnej dokumentacji wraz ze spisem opracowań i oświadczeniem, że dokumentacja projektowa wykonana jest zgodnie z obowiązującymi normami, przepisami techniczno-budowlanymi jest w stanie kompletnym z punktu widzenia jej przydatności do zrealizowania celu, któremu ma służyć.

Dokumentację należy opracować w oparciu o przekazaną specyfikację, inwentaryzację przedprojektową i wytyczne uzyskane podczas wizji lokalnej w Zakładach Zleceniodawcy.

**Forma elektroniczna**

Dokumentacja w wersji elektronicznej wykonana zostanie z zastosowaniem następujących formatów elektronicznych:

* Rysunki - format dwg (ACAD wersja 2004) i pdf.
* Tekst - format doc i pdf,
* Arkusze kalkulacyjne - format xls i pdf - arkusze kalkulacyjne muszą posiadać

aktywne formuły,

* Harmonogramy - format xls , mpp i pdf,
* Układ dokumentacji w wersji elektronicznej w formacie PDF jak w wersji papierowej.

Rysunki w formacie pdf powinny zostać tak skonwertowane, aby umożliwiały korzystanie z funkcji „wyszukaj” całej zawartej w nich treści.

Wykonawca dostarczy wersję elektroniczną na nośniku CD/DVD w 2 egzemplarzach.

Dokumentacja projektowa będzie kompletna z punktu widzenia celu, któremu ma służyć. Zawierać będzie wymagane potwierdzenia sprawdzeń rozwiązań projektowych w zakresie wynikającym z przepisów, a także spis opracowań dokumentacji składających się na jej komplet. Posiadać będzie oświadczenie Wykonawcy o jej wykonaniu zgodnie z umową, obowiązującymi przepisami techniczno-budowlanymi, normami oraz zasadami wiedzy technicznej, podpisane przez projektantów odpowiedzialnych za spełnienie tych wymagań.

* + 1. **Prawa autorskie.**

Wykonawca przeniesie na ZAMAWIAJĄCEGO autorskie prawa majątkowe do utworów powstałych w ramach dokumentacji w zakresie następujących pól eksploatacyjnych:

* utrwalania i zwielokrotniania utworu – wytwarzanych każdą techniką egzemplarzy utworu, w tym techniką drukarską, reprograficzną , zapisu magnetycznego oraz techniką cyfrową (w tym dyskietki, CD-ROM-y, DVD, taśmy magnetyczne, nośniki magnetooptyczne, poprzez druk oraz urządzenia elektroniczne, w tym tzw. Papier elektroniczny );
* wprowadzanie do pamięci komputera;
* prawo do wykorzystywania w każdy sposób i w każdej formie w Internecie lub innej sieci komputerowej;
* modyfikacja i uaktualnianie.
	1. **Minimalne wymagania techniczno-użytkowe wobec urządzeń.**

**Uwaga: wszystkie wymagania podano jako minimalne i należy przez to rozumieć, że Wykonawca ma dostarczyć urządzenia o parametrach nie gorszych niż podane. Urządzenia te powinny zapewnić poprawną i ciągłą pracę całości systemu w trudnych warunkach atmosferycznych i przy zmiennym oświetleniu. Muszą swoją wydajnością i odpowiednio dobranymi parametrami technicznymi zapewnić spełnienie wszystkich wymaganych przez Zamawijącego funkcjonalności wdrażanego systemu.**

* + 1. **Wymagania dla urządzeń i oprogramowania systemu CCTV:**

**Wymagania dla monitorów:**

* Wszystkie monitory muszą być przeznaczone do pracy ciągłej w trybie 24/7/365 (dwadzieścia cztery godziny na dobę, siedem dni w tygodniu, trzysta sześćdziesiąt pięć dni w roku).
* Należy dostarczyć monitory o rozdzielczości minimum Full HD oraz przekątnej minimum 50" do ściany wizyjnej w pomieszczeniu ochrony CM
* Do stacji operatorskich należy dostarczyć monitory o rozdzielczości minimum Full HD oraz przekątnej minimum 32"

**Minimalne wymagania dotyczące kamer ochrony obwodowej (kamera typ 1):**

* Czułość przetwornika min. 0,04 lux (kolor) przy AGC ON, 0 lux z podświetleniem
* Podświetlenie IR, zasięg podświetlenia IR równomierne w całym zasięgu obserwacji kamery
* Rozdzielczość min. FullHD 1080p
* Kompresja min. H.264, min. 4 strumienie
* Mechaniczny filtr IR
* Dynamika przetwornika; Wide Dynamic Range min. 120dB
* Obiektyw o odpowiedniej ogniskowej do obserwowanej i wymaganej sceny z funkcją autofocus i motorzoom,
* Detekcja sabotażu w zakresie utraty ostrości, zmiany sceny, zasłonięcie
* Analityka w zakresie; przekroczenie wirtualnej linii, wejście/wyjście intruza w rejon, pozostawienie/usunięcie obiektu, wałęsanie w obszarze.
* Klasa wandaloodporności min. IK10
* Klasa szczelności min. IP66
* Temperatura pracy min. -30oC do +50oC (wbudowana grzałka)
* Obudowa typu bullet z uchwytem montażowym i dedykowaną puszką montażową.

**Minimalne wymagania dla zintegrowanych panoramicznych (360°) stałopozycyjnych zespołów kamerowych (kamera typ 2):**

* zespół kamerowy wyposażony w 3 lub 4 przetworniki
* Czułość przetwornika min. kolor 0,04 lux (kolor) przy AGC ON, 0,01 lux (czarno/biały) przy AGC ON
* Podświetlenie IR, zasięg podświetlenia IR równomierne w całym zasięgu obserwacji kamery
* Rozdzielczość jednego sensora min. 2048x1536
* Kompresja min. H.264 min. 2 strumienie
* Mechaniczny filtr IR
* Dynamika przetwornika; Wide Dynamic Range min. 120dB
* Obiektyw o odpowiedniej ogniskowej
* Detekcja sabotażu w zakresie utraty ostrości, zmiany sceny, zasłonięcie
* Analityka w zakresie; przekroczenie wirtualnej linii, wejście/wyjście intruza w rejon, pozostawienie/usunięcie obiektu
* Możliwość definiowania ROI dla każdego strumienia
* Klasa wandaloodporności min. IK10
* Klasa szczelności min. IP66
* Temperatura pracy min. -30oC do +50oC
* Obudowa kopuła wyposażona w 3 lub 4 moduły kamerowe umożliwiająca dowolne przesunięcie kamer po obwodzie.

**Minimalne wymagania dla punktów kamerowych PTZ (kamery typ 3):**

* Rozdzielczość min. 1080p
* Czułość min. 0,05 Lux (kolor) przy AGC ON, 0,0 Lux z podświetleniem IR
* WDR min. 120dB
* Zoom optyczny min. 40x
* Mechaniczny filtr IR
* Podświetlenie IR lub laserowe, zasięg podświetlenia równomiernie w całym zasięgu obserwacji kamery
* Analityka w zakresie; przekroczenie wirtualnej linii, wejście/wyjście intruza w rejon, pozostawienie/usunięcie obiektu, wałęsanie się w obszarze
* Temperatura pracy -30oC do +50oC (wbudowana grzałka)
* Min. IP66
* Min. IK10

**Minimalne wymagania dla automatycznych zespołów kamerowych wyposażonych w algorytmy detekcji i przechwytywania twarzy, przechwytywania obiektów i tryb pracy perymetrycznej w obrazie wideo (kamera typ 4):**

* Kamera szerokokątna
* Rozdzielczość min. 1080p
* Obiektyw ogniskowej zapewniającej kąt horyzontalny obejmujący całość obserwowanej sceny
* Analityka; detekcja ruchu, sabotaż,
* Moduł PTZ
* Rozdzielczość min. 1080p
* Mechaniczny filtr IR
* Inteligencja; śledzenie wielu obiektów, detekcja i kategoryzacja obiektów w zakresie człowiek/pojazd, detekcja twarzy

**Minimalne wymagania dla kamer wyposażonych w algorytmy detekcji i przechwytywania twarzy, przechwytywania obiektów (kamery typ 5):**

* Czułość przetwornika min. 0,04lux (kolor) przy AGC ON, 0 lux z podświetleniem
* Podświetlenie IR, zasięg podświetlenia IR min. do 50m
* Rozdzielczość min. FullHD 1080p
* Mechaniczny filtr IR
* Dynamika przetwornika; Wide Dynamic Range min. 120dB
* Obiektyw o odpowiedniej ogniskowej z funkcją autofocus i motozoom,
* Detekcja sabotażu w zakresie utraty ostrości, zmiany sceny, zasłonięcie
* Przechwytywanie cech osobowych
* Zliczanie obiektów
* Możliwość definiowania obszarów ROI
* Klasa wandaloodporności min. IK10
* Klasa szczelności min. IP66
* Temperatura pracy min. -30oC do +50oC (z grzałką)
* Obudowa typu bullet z uchwytem montażowym i dedykowaną puszką montażową

**Minimalne wymagania dla kamer systemu rozpoznawania twarzy (kamera typ 6):**

* Czułość przetwornika min. 0,01lux (kolor) przy AGC ON, 0 lux z podświetleniem
* Podświetlenie IR, zasięg podświetlenia IR w założonej scenie
* Rozdzielczość min. FullHD 1080p
* Kompresja H.265 lub H.264, min. 2 strumienie
* Dynamika przetwornika; Wide Dynamic Range min. 120dB
* Mechaniczny filtr IR
* 2 obiektywy o odpowiedniej ogniskowej z funkcją autofocus
* Klasa wandaloodporności min. IK10
* Detekcja sabotażu, detekcja ruchu, zasłonięcie
* Analityka w zakresie; porównywanie twarzy obiektu w kadrze z predefiniowanym wzorcem w bazie danych, automatyczne zapisywanie zdjęcia twarzy w celu wstecznego przeszukania bazy danych.

**Minimalne wymagania dla kamer kopułowych budynku biurowym na potrzeby kontroli ruchu osobowego (kamery typ 7):**

* Czułość przetwornika min. 0,04lux (kolor) przy AGC ON, 0 lux z podświetleniem
* Podświetlenie IR, zasięg podświetlenia IR w całym przyjętym zakresie sceny
* Rozdzielczość min. FullHD 1080p
* Kompresja H.264 min.5 strumieni (?)
* Mechaniczny filtr IR
* Dynamika przetwornika; Wide Dynamic Range min. 120dB
* Obiektyw o z funkcją motorzoom, autofocus
* Detekcja sabotażu w zakresie utraty ostrości, zmiany sceny,
* Analityka w zakresie; przekroczenie wirtualnej linii, wejście/wyjście intruza w region, pozostawienie/usunięcie obiektu,

**Minimalne wymagania dla automatycznych zespołów kamerowych (kamera panoramiczna 360° + głowica PTZ) wyposażonych w algorytmy detekcji i przechwytywania twarzy, przechwytywania obiektów i tryb pracy perymetrycznej w obrazie wideo (kamera typ 8):**

Kamera panoramiczna:

* Czułość przetwornika min. 0,04lux (kolor) przy AGC ON
* Rozdzielczość min. 2x4096x1800
* Kompresja H.265+/H.265/H.264+/, min. 2 strumienie
* Kąty widzenia min.: horyzontalny 360°, wertykalny 80°

Głowica PTZ

* Rozdzielczość min. 1080p
* Czułość min. 0,04 Lux (kolor) przy AGC ON, 0,0 Lux z podświetleniem IR
* WDR min. 120dB
* Zoom optyczny min. 25x
* Mechaniczny filtr IR
* Oświetlacz IR w całym przyjętym zasięgu sceny,
* Analityka w zakresie; przekroczenie wirtualnej linii, wejście/wyjście intruza w rejon, pozostawienie/usunięcie obiektu, dynamiczne śledzenie twarzy w obszarze
* Rozróżnienie typu obiektu na człowiek/pojazd i możliwość filtrowania zdarzeń po typie obiektu
* Detekcja twarzy
* Temperatura pracy min. -30oC do +50oC
* Klasa szczelności min. IP66

**Minimalne wymagania dla kamer LPR (kamera typ 9)**

* Czułość przetwornika min. 0,04 lux (kolor) przy AGC ON, 0 lux z podświetleniem
* Podświetlenie IR, zasięg podświetlenia IR w całym zasięgu sceny
* Rozdzielczość min. FullHD 1080p
* Kompresja min. H.264, min. 2 strumienie
* Mechaniczny filtr IR
* Dynamika przetwornika; Wide Dynamic Range min.120dB
* Obiektyw o odpowiedniej ogniskowej do obserwowanej sceny
* WDR w zakresie czytania tablic rejestracyjnych; skuteczność przechwytywania >95%, skuteczność rozpoznania >95%, pomiar prędkości pojazdu do min. 80km/h, ilość obsługiwanych pól przechwytywania min. 2, ilość wpisów na czarnej liście min. 2048,
* Zgrubny pomiar prędkości na podstawie analizy przemieszczania się obiektu w polu obserwacji
* Klasa szczelności min. IP66
* Temperatura pracy min. -30oC do +50Oc (wbudowana grzałka)

**Wymagania dla serwerów (urządzeń rejestrujących):**

Na potrzeby systemu monitoringu wizyjnego należy przewidzieć serwery w ilości niezbędnej do realizacji przedmiotu zamówienia, zamontowane w trzech lokalizacjach, spełniające poniższe wymagania:

* montowane w szafach technicznych,
* w zależności od oferowanego oprogramowania PSIM i CCTV:
	+ system operacyjny Microsoft Windows Server 2012R2 lub 2016 – w gestii Zamawiającego
	+ system operacyjny Red Hat® Enterprise Linux lub inny wraz z licencjami – dostarcza Wykonawca
	+ oprogramowanie wraz licencjami do wirtualizacji VMware lub inne – dostarcza wykonawca
* min. 2 procesory klasy Intel Xeon E5-2600 v4 lub równoważne
* min. 64 GB RAM DDR4,
* wbudowana karta graficzna,
* min. 2 dyski SSD 400GB każdy,
* RAID 0, 1
* min. 4 x 1Gb/s
* wsparcie do VMWare i Hyper-V
* redundantne zasialnie
* niezbędne okablowanie

**Macierze dyskowe dołączone do serwerów**

* montowane w szafach technicznych,
* dwa kontrolery iSCSI (min. 4GB pamięci na kontroler) wraz z okablowaniem
* redundantne zasilanie,
* obsługa min. 8 serwerów,
* obsługa RAID 0, 1, 10, 5, 6
* obsługa minimum 12 dysków HDD
* zainstalowane dyski min. 4TB (3.5’’ SAS)
* ilość dostarczonyc dysków musi zapewnić określony czas rejestracji z wymaganymi parametrami
* obsługa dysków o pojemności do nie mniej niż 8TB
* minimum 4 porty sieciowe
* niezbędne okablowanie
* dodatkowe 3 HDD do każdej z macierzy

**UWAGA! Wykonwaca będzie miał możliwość inastalacji systemu tylko w jednej szafie technicznej 42U w każdej z lokalizacji. Do lokalizacji ECS dostracza szafę we własnym zakresie.**

**Stacje Operatorskie**

Stacje operatorskie muszą posiadać odpowiednią wydajność, zapewnić płynną pracę systemu i muszą spełniajać poniższe minimalne wymagania:

* Procesor Intel Core i5-8500, 3GHZ, 9MB (lub równoważny) lub nowszy
* min. 8GB RAM DDR4
* 2 porty sieciowe 1000Mb/s,
* 1 lub dwie karty graficzne klasy Nvidia Quadro, każda obsługująca po 2 monitory,
* wsparcie sprzętowe dla dekodowania obrazu wideo,
* gwarancja oraz naprawa na miejscu (Next Bussines Day),
* stacja przewidziana do pracy ciągłej.

**Oprogramowanie**

* Praca w architekturze klient – serwer.
* Otwarta architektura umożliwiająca podłączenie do systemu nielimitowanej liczby nowych urządzeń.
* Możliwość podłączenia kamer IP o rozdzielczości min. FullHD różnych producentów przy wykorzystaniu protokołu ONVIF.
* Wsparcie dla kamer obsługujących kompresje H.265, H.264, MJPEG, MPEG4.
* Lista kamer zintegrowanych w sposób natywny zawierająca głównych producentów.
* Zapisywany materiał z kamer wideo musi być zaszyfrowany.
* Obsługa strumieni multicast.
* Obsługa dwóch strumieni wideo, zapisywany materiał zawsze musi być w jakości przyjętej do kalkulacji powierzchni dyskowej.
* Ustawianie innych parametrów rejestracji dla każdej podłączonej kamery.
* Wyposażenie systemu w zegar i kalendarz synchronizowany czasem NTP.
* Wsparcie dla analityk wideo serwerowych oraz zaimplementowanych na kamerach. System musi umożliwiać przechwycenie sygnału alarmowego z analityki wideo.
* W przypadku alarmu z analityki wideo równoczesne wyświetlenie obrazu z kamery generującej alarm oraz przemieszczenie zdefiniowanej kamery obrotowej do określonego położenia. Wszystkie czynności muszą odbywać się w sposób automatyczny i wyświetlać obraz dla operatora.
* Sygnalizacja o sabotażu kamery.
* Nadawanie przez administratora systemu hierarchicznych uprawnień każdej osobie lub grupom osób korzystających z systemu.
* Zapisywanie zdarzeń wykonywanych w systemie, m.in.: logowanie \ wylogowanie użytkownika, podłączenie \ odłączenie urządzenia, eksport materiału wideo, dodanej \ zaktualizowanie mapy, dodanie \ zaktualizowanie widoku, \ serwer zmienił ustawienie, \ zmieniono ustawienie urządzenia \ wykonano eksport materiału wideo, \ wyjście cyfrowe wyzwolono, \ położenie kamery PTZ zmieniono.
* Możliwość wykorzystania wielopoziomowych map nadzorowanego obszaru obiektu i umieszczenia na tych mapach punktów kamerowych.
* Nadawanie nazw wybranych przez użytkownika systemu poszczególnym kamerom
* Interfejs użytkownika i pomoc wbudowana w języku polskim.
* Wyszukiwanie zarejestrowanych zdarzeń, z podziałem na źródła sygnału i z uwzględnieniem kalendarza w zadanych przez użytkownika przedziałach czasowych.
* Możliwość współpracy z systemami kontroli dostępu, systemami sygnalizacji włamania i napadu, innymi systemami sygnalizacji zagrożeń oraz systemem rozpoznawania tablic rejestracyjnych.
* Transmisja danych wizyjnych przy użyciu protokołu TCP/IP.
* Automatyczne nadpisywanie najstarszego materiału po zapełnieniu przestrzeni dyskowej.
* Ustawianie harmonogramów nagrywania wideo dla każdej kamery niezależnie.
* Możliwość podłączenia nieograniczonej liczby stacji klienckich.
* System musi umożliwiać zarządzanie prawami dostępu dla każdego z osobna użytkownika systemu. Musi istnieć możliwość nadzoru nad użytkownikami, którzy mają prawo dostępu do zgrywania materiałów.
* Możliwość zdefiniowania funkcji, które umożliwiają wykonanie akcji według zadanego zdarzenia.
* Tworzenie programowalnych ustawień położenia dla kamer obrotowych, co najmniej 6 dla każdej kamery.
* Możliwość konfigurowania tras patrolowych dla dowolnej kamery obrotowej podłączonej do systemu.
* Zintegrowany pulpit sterowniczy umożliwiający wyświetlanie obrazu z kamer na monitorze, odtwarzanie nagranego materiału, sterowanie kamerami obrotowymi.
* Moduł SDK umożliwiający późniejszą integrację z innymi systemami obiektowymi.
* Funkcjonalność wirtualnej ściany wideo.
* Współpraca z wielomonitorowymi stacjami klienckimi - co najmniej 4 monitory na 1 stację.
* Stacja robocza musi zostać tak dobrana aby jej wydajność umożliwiła równoczesne wyświetlenie materiału na co najmniej 4 monitorach (z minimum 64 kamer).
* Możliwość wyświetlania map obiektu na dowolnym podłączonym monitorze.
* Aplikacja producenta do odtwarzania eksportowanego materiału.
* Nanoszenie pola widzenia kamer stałych na mapach.
* Możliwość wyświetlenia obrazu z kamery poprzez wskazanie jej na mapie.
* Opcja podłączenia tzw. klienta mobilnego współpracującego z co najmniej dwoma z wymienionych systemów operacyjnych: Android, iOS, Windows Mobile.
* Oprogramowanie musi umożliwiać aktualizację do najnowszej wersji bez konieczności istotnych ingerencji w konfigurację systemu oraz kształtu i zawartości bazy danych.
* Jednoczesne oglądanie materiału w trybie "na żywo" oraz materiału odtwarzanego na jednej stacji roboczej.
* Oprogramowanie musi zapewnić możliwość planowania kopii zapasowych z nagraniami wideo i zdarzeń do folderu lokalnego lub na zmapowany dysk sieciowy.
* Oprogramowanie na serwerze musi prowadzić log systemowy pozwalający na zapisanie następujących informacji: uruchomienie \ zamknięcie aplikacji na serwerze, \ połączenie sieciowe nawiązane \ utracone, \ problem z wydajnością systemu, \ błąd bazy danych, \ błąd dysku \ partycji.
* Sterowanie kamerami obrotowymi za pomocą myszy komputerowej lub joysticka.
* Oprogramowanie musi zapewnić możliwość ustawienia limitu maksymalnego pasma dla danych przesyłanych z aplikacji serwerowej do aplikacji klienckiej.
* Oprogramowanie musi umożliwiać tworzenie zakładek na nagraniach wideo na osi czasu, wraz z możliwością blokady przed nadpisaniem materiału wideo.
* Oprogramowanie musi umożliwiać przeszukiwanie nagrań wideo na podstawie ruchu w obszarach zdefiniowanych przez użytkownika.
* Oprogramowanie musi umożliwiać konwersję materiału wideo, który został wyeksportowany w natywnym formacie do innych popularnych formatów.
* Oprogramowanie musi pozwalać na kontrole zajętości pasma pomiędzy serwerem a stacjami klienckimi.

**Analityki Wideo**

Dopuszcza się analityki na serwerach bądź kamerach. W momencie korzystania z kamer z wbudowaną analizą obrazu, system musi pozwalać na konfigurację reguł analityki z poziomu aplikacji klienckiej.

Należy założyć w przypadku analizy obrazu na terenie zewnętrznym, optymalizację jakości działania w zależności od pory roku. Wykonawca zobowiązany jest do wykonywania raportów raz na kwartał, odnośnie jakości i skuteczności działania reguł.

W określonych miejscach wskazanych przez klienta, takich jak ochrona perymetryczna, ruch osobowy oraz samochodowy, analiza obrazu powinna pozwalać na klasyfikowanie obiektów na osoby oraz pojazdy, a dane zebrane przez system powinny być skorelowane w postaci metadanych i pozwalać na wyszukiwanie obiektów na nagranym materiale wideo.

**Rejestracje archiwalnego materiału wideo**

Do obliczeń wymaganej przestrzeni dyskowej dla rejestracji archiwalnego materiału wideo przyjęto następujące założenia:

* Czas przechowywania archiwalnego materiału wideo: min. 31 dni w każdej z lokalizcji
* Min. 15 kl/s.
* Zapis ciągły 24h.
* Kodowanie H.264 lub H.265.
* bitrate, zapewniający bardzo wysoką jakość .

Wykonawca przy wyliczaniu odpowiedniej wielkości pojemości proponowanych serwerów musi wziąć pod uwagę ilość kamer:

* obecnie użytkowanych,
* nowo projektowanych,
* dodatkowych zainstalowanych lub projektowanych w ramach odrębnych Projektów Inwestycyjnych (w szczególności Blok parowo-gazowy i Kotłownia gazowa), które zostaną podłączone do tych serwerów (wielkość należy uzgodnić ze Zleceniodawcą).

Należy zapewnić backup online (korzystająć z istniejących łączy 10 Gb Zamawiającego) materiału wideo zarejstrowanego w ECS i ECZ w na urządzeniu rejestrującym (wraz z dostawą tego urządzenia i niezbędnego oprogramowania) w serwerowni Zamawiającego zlokalizowanej w EC Kawęczyn. Należy zapewnić możliwość przechowywania archiwalnego materiału wideo z ECS i ECZ przez 31 dni, materiał powinien być rejestrowany z maksymalną dostępną jakością wynikającą z przepustowości istniejących łącz.

Należy zapewnić we wszystkich lokalizacjach redundancję urządzeń rejestrujących min. w konfiguracji N+1, urządzenie zapasowe, musi zapewnić możliwość przejęcia wszystkich funkcji urządzenia uszkodzonego.

* + 1. **Wymagania dla Centrum Monitoringu i Zarządzania.**

Przeiduje się adaptację trzech pomieszczeń na potrzeby Centrum Monitoringu i Zarządzania. W pomieszczeniach centrum monitoringu (2xECZ i 1xECS) proponuje się instalację min. 2 stacji roboczych (oglądowo-zarządzających), wyposażonej w dwa monitory LCD min. Full HD o przekątnych co najmniej 32 cali.

Dodatkowo przewiduje się zastosowanie jednej ściany wideo złożonej z monitorów bezramokowych o przekątnych co najmniej 50 cali i zdalnie sterowanej ze stacji roboczych poprzez funkcję wirtualnej krosownicy. Monitory powinny maksymalnie i ergonomicznie wykorzystywać dostępną przestrzeń ściany (4x4 lub 3x3).

Dodatkowo należy przewidzieć wykonanie następujących prac w pom. monitoringu:

EC Żerań 1:

* wyburzenie ścian magazynu broni,
* wyburzenie ściany pomiędzy pom. monitorignu a serwerownią,
* wymianę okien w obecnym pom. serwerowni na okna przeciwwłamaniowe,
* wyklejenie wszystkich okien folią przeciwsłoneczną zewnętrzną,
* wyrównanie ubytków w ścianach,
* wykonanie wentylacji mechnicznej,
* wykonanie instalacji klimatyzacji, zapewniającej utrzymanie temp. ok 20 st. C ,
* malowanie ścian,
* wymianę oświetlenia wraz z zapewnieniem oświetlenia awaryjnego,
* dostawę i instalację wyposażenia:
* 2x stół dla stacji operatorskich (wym. min. 180 cm x 80, regulacja wysokości, podwyższona odporność na ścieralność okładziny blatu),
* 2x kontener na kółkach pod biurko z szufladami,
* 1x stół do przeglądania dokumentacji (wym. min. 180 cm x 80, regulacja wysokości, podwyższona odporność na ścieralność okładziny blatu),
* 3x krzesło biurowe (wielopłaszczyznowa regulacja zagłówka, oparcia, siedziska oraz podłokietników, blokasa oparcia w co najmniej 3 pozycjach),
* 1x szafa na dokumentację (metalowa, drzwi przesuwne z zamkiem, min. wymiary 190x200x45)

EC Żerań 2:

* wyburzenie ściany,
* wymianę okien w obecnym pom. serwerowni na okna przeciwwłamaniowe o klasie odporności RC4,
* podłączenie pomieszczenia do istaniejącej instalacji SKD i SSWiN,
* wymianę i montaż drzwi o klasie odporności RC4
* wyklejenie wszystkich okien folią przeciwsłoneczną zewnętrzną,
* wyrównanie ubytków w ścianach,
* wykonanie wentylacji mechnicznej,
* wykonanie instalacji klimatyzacji, zapewniającej utrzymanie temp. ok 20 st. C ,
* malowanie ścian,
* wymianę oświetlenia wraz z zapewnieniem oświetlenia awaryjnego,
* dostawę i instalację wyposażenia:
* 4x stół dla stacji operatorskich (wym. min. 180 cm x 80, regulacja wysokości, podwyższona odporność na ścieralność okładziny blatu),
* 4x kontener na kółkach pod biurko z szufladami,
* 1x stół do przeglądania dokumentacji (wym. min. 180 cm x 80, regulacja wysokości, podwyższona odporność na ścieralność okładziny blatu),
* 4x krzesło biurowe (wielopłaszczyznowa regulacja zagłówka, oparcia, siedziska oraz podłokietników, blokasa oparcia w co najmniej 3 pozycjach),
* 1x szafa na dokumentację (metalowa, drzwi przesuwne z zamkiem, min. wymiary 190x200x45)

EC Siekierki:

* wyburzenie pozostałości ścianek działowych,
* wyrównanie ubytków w ścianach,
* wyklejenie wszystkich okien folią przeciwsłoneczną zewnętrzną,
* wykonanie wentylacji mechnicznej,
* wykonanie instalacji klimatyzacji, zapewniającej utrzymanie temp. ok 20 st. C ,
* malowanie ścian,
* wymianę oświetlenia wraz z zapewnieniem oświetlenia awaryjnego,
* dostawę i instalację wyposażenia:
* 2x stół dla stacji operatorskich (wym. min. 180 cm x 80, regulacja wysokości, podwyższona odporność na ścieralność okładziny blatu),
* 2x kontener na kółkach pod biurko z szufladami,
* 1x stół do przeglądania dokumentacji (wym. min. 180 cm x 80, regulacja wysokości, podwyższona odporność na ścieralność okładziny blatu),
* 3x krzesło biurowe (wielopłaszczyznowa regulacja zagłówka, oparcia, siedziska oraz podłokietników, blokada oparcia w co najmniej 3 pozycjach),
* 1x szafa na dokumentację (metalowa, drzwi przesuwne z zamkiem, min. wymiary 190x200x45).
	+ 1. **Wymagania dla stanowisk Biura Bezpieczeństwa.**

Należy skonfigurować i dostarczyć (po jednym dla każdej lokalizacji) stanowiska nadzoru przeznaczone dla pracowników Biura Bezpieczeństwa. Stanowiska powinny zapewniać możliwość pełnego korzystania ze wszystkich funkcji systemu SZT i SZB i być wyposażone w odpowiednio wydajny komputer klasy PC oraz monitory min. 32’’. Dodatkowo stanowisko w ECZ należy wyposażyć w dodatkowy monitor min. 65’’ (zamontowany na ścianie).

* + 1. **Wymagania dla stanowisk w posterunkach ochrony.**

Należy skonfigurować i dostarczyć stanowiska nadzoru przeznaczonego dla posterunków ochrony (łącznie ok. 9 stanowisk). Stanowisko powinno zapewniać możliwość korzystania z wybranych przez Zamawiającego, funkcji systemu SZT i SZB i być wyposażone w odpowiednio wydajny komputer klasy PC oraz 1 monitor min. 22’’.

* + 1. **Urządzenia aktywne**

Transmisja danych z kamer odbywać się będzie w oparciu o wydzieloną sieć Ethernet. Sieć transmisyjna powinna zostać wykonana w topologii gwiazdy z centralnym węzłem w postaci Głównego Punktu Dystrybucyjnego (GPD-CCTV) oraz punktami pośrednimi w postaci szafek nasłupowych. Połączenie urządzeń aktywnych pomiędzy Punktami LPD i Głównym Punktem Dystrybucyjnym (GPD) powinno zostać wykonane za pomocą światłowodów wielomodowych.

Głównymi elementami aktywnymi sieci transmisyjnej zarówno w LPD jak również w GPD będą zarządzalne przełączniki sieciowe.

Przełączniki sieciowe w projektowanych punktach LPD-CCTV powinny charakteryzować się następującymi minimalnymi parametrami:

* Minimum 4 porty 10/100/1000Base-T RJ-45 z funkcją PoE+
* min. 2 porty SFP+ współdzielone
* Funkcja Routing Statyczny
* Matryca przełączająca min. 20Gbps
* Tablica adresów MAC 9K
* Pełne wsparcie transmisji Multicast dla IP Video (do 255 grup multicastowych)
* Wsparcie do 255 grup VLAN
* Power over Ethernet (PoE) (zgodne z IEEE 802.3at)
* Zabezpieczenie zwarciowe portów RJ-45.
* Automatyczna detekcja urządzeń zasilanych za pośrednictwem PoE
* Quality of Service (QoS)
* IP30 metalowa obudowa, montaż na szynie DIN
* Temperaturowy zakres pracy -40ºC ~ +70ºC

Przełączniki sieciowe w projektowanym w szafach CCTV powinny charakteryzować się następującymi minimalnymi parametrami:

* 24 porty SFP o prędkości min. 1Gbps / min. 24 porty Gigabit Ethernet RJ-45
* min.4 współdzielone porty RJ45 10/100/1000
* min. 4 porty SFP+ o prędkości min. 10Gbps
* Funkcja Routing statyczny
* Matryca przełączająca min. 128Gbps
* Współdzielony bufor danych o wielkość 32Mb
* Tablica adresów MAC 16K
* Pełne wsparcie transmisji Multicast dla IP Video (do 255 grup multicastowych)
* Wsparcie do 256 grup VLAN
* Zaawansowane mechanizmy bezpieczeństwa, oparte o IP lub ACL/MAC listy po 256 wpisów
* Wsparcie QoS w oparciu o klasy, konkretny priorytet lub WRR, 4-poziomy priorytetów
* Redundancja zasilania

Podłączenie światłowodów powinno zostać wykonane poprzez odpowiednie interfejsy światłowodowe SFP (MiniGBIC) o szybkości co najmniej 1Gbps.

Do przełączników w GPD zostaną podłączony redundantnie rejestratory oraz stacja robocza służąca do zarządzania i obsługi systemu CCTV IP.

Podstawowe wytyczne konfiguracji sieci;

* Dostęp administracyjny powinien być zapewniony tylko poprzez port konsoli zarządzającej lub poprzez wydzielony port znajdujący się w innej podsieci niż urządzenia CCTV. Wydzielony port zapewni dostęp do wszystkich urządzeń aktywnych oraz uniemożliwi podpięcie się do funkcji zarządzających osobom niepowołanym.
* Wszystkie urządzenia muszą mieć ten sam czas pracy. Należy użyć serwera NTP do synchronizacji czasu.
* Wszystkie urządzenia CCTV muszą pracować we wspólnej dla siebie, wydzielonej podsieci. Żadne inne urządzenie nie może wykorzystywać danej podsieci. W przypadku integracji z innymi systemami bezpieczeństwa dopuszcza się pracę we wspólnej podsieci.
* Stanowiska nadzoru pracowało będzie we wspólnym VLANie ze wszystkimi urządzeniami. W celu połączenia z siecią LAN Zamawiającego i przekazywania informacji min. do systemu Zamawiającego SIEM IBM QRadar, stacji nadzoru, konsoli Biura Bezpieczeństwa, Wykonawca dostarczy i skonfiguruje urządzenie firewall firmy Check Point min. 1430/50.
* Funkcję QoS należy włączyć przynajmniej w wartościach domyślnych.
* Nieużywane porty przełączników muszą być wyłączone.

Praca przełączników musi być nadzorowana przez system PSIM. Wymagane jest przekazywanie minimum następujących informacji:

* aktywacja / podpięcie wybranego portu
* dezaktywacja / odpięcie wybranego portu
* aktywacja funkcji PoE na wybranym porcie
* dezaktywacja funkcji PoE na wybranym porcie
* filtracja adresów MAC zgodnie z ACL ( detekcja aktywności „obcego” urządzenia )
* przekroczenie definiowalnego zużycia pamięci ( wartość min. oraz max. wyrażana w procentach )
* przekroczenie definiowalnego obciążenia CPU ( wartość min. oraz max. wyrażana w procentach )
* informacja o wykonywanym logowaniu do przełącznika
* dokonanie zmiany w pliku konfiguracji przełącznika
	+ 1. **Wymagania dla urządzeń systemu SSWiN:**

Centrala SSWiN powinna spełniać poniższe wymagania:

* pełna zgodność z normami serii EN50131 dla urządzeń Stopnia 3 (Grade 3)
* wbudowany zaawansowany zasilacz 2 A+1,5 A z rozbudowaną diagnostyką
* obsługa do 256 wejść z możliwością programowania rezystancji parametrycznej oraz obsługą linii 3EOL (tylko wejścia płyty głównej)
* port USB do programowania za pomocą PC
* możliwość podziału systemu na 32 strefy oraz 8 partycji
* rozbudowa do 256 programowalnych wyjść
* magistrale komunikacyjne do podłączania manipulatorów i modułów rozszerzeń
* wbudowany komunikator telefoniczny z funkcją monitoringu, powiadamiania głosowego i zdalnego sterowania
* obsługa systemu przy pomocy manipulatorów LCD, klawiatur strefowych, pilotów i kart zbliżeniowych oraz zdalnie z użyciem komputera lub telefonu komórkowego
* 64 niezależne timery do automatycznego sterowania
* pamięć 24 575 zdarzeń z funkcją wydruku
* obsługa do 240+8+1 użytkowników
* możliwość aktualizacji oprogramowania za pomocą komputera

Moduły rozszerzeń SSWiN powinny spełniać poniższe wymagania:

* obsługa konfiguracji:
* NO, NC
* EOL, 2EOL/NO, 2EOL/NC (tylko centrale alarmowe)
* 3EOL (tylko INTEGRA Plus)
* obsługa czujek roletowych i wibracyjnych (tylko centrale alarmowe)
* rozbudowa systemu o 8 wejść
* rozbudowa systemu o 8 wyjść:
* 4 wyjścia typu OC
* 4 wyjścia przekaźnikowe
* możliwość podłączenia do magistrali RS-485 (aktualizacja oprogramowania za pośrednictwem magistrali).

Aktywne bariery podczerwieni powinny spełniać poniższe wymagania:

* Min. 4 wiązki podczerwieni
* Zasięg do 100m
* Styk sabotażowy
* Przekaźnik wyjścia alarmowego typu NO/NC
* Temperatura pracy -25°C - 60°C
* Dopuszczalna wilgotność do 95% bez kondensacji
* Klasa ochrony obudowy IP65

Czujki zewnętrzne powinny spełniać poniższe wymagania:

* Czujka dualna PIR +MW z funkcją antymaskingu i ochroną strefy podejścia
* Zasięg 2,5 - 12m
* Styk sabotażowy
* Przekaźnik wyjścia alarmowego typu NO/NC
* Regulacja czułości
* Temperatura pracy -25°C - 60°C
* Dopuszczalna wilgotność do 95% bez kondensacji
* Klasa ochrony obudowy IP55
	+ 1. **Wymagania dla PSIM.**
* System zarządzania musi być neutralny wobec producentów integrowanych systemów i urządzeń.
* Oprogramowanie musi mieć budowę modułową. Wymiana dowolnego modułu programowego nie może wstrzymywać pracy pozostałych funkcji.
* W systemie wymagane są następujące sposoby połączeń :
	+ Wyjścia przekaźnikowe różnych urządzeń i systemów do wejść systemu integracyjnego,
	+ Przekaźniki systemu integracyjnego do wyjść sterujących różnych urządzeń i systemów,
	+ Port komunikacyjny centrali integrowanego systemu do sterownika systemu integrującego
	+ Port komunikacyjny integrowanych urządzeń do sterownika będącego elementem systemu integracyjnego. Dodatkowo wymaga się aby sterowniki systemu integracyjnego mogły pracować w sieci.
	+ Port komunikacyjny integrowanego systemu do portu szeregowego lub gniazda Ethernet komputera systemu integracyjnego.
* System musi pracować w sieci komputerowej oraz umożliwiać obsługę za pomocą przeglądarki internetowej z dowolnego miejsca w budynku.
* Wymagana jest możliwość pomiaru wielkości fizycznych typu ciągłego (np. prąd ładowania baterii, wartość napięcia, temperatury, ciśnienia itp.) Wymagana jest możliwość generowania alarmów na podstawie przekroczenia progów alarmowych
* Monitorowanie (wraz z obsługą sytuacji alarmowych) i raportowanie (w postaci tabel i wykresów):

- pracy serwerów (temperatury, wentylatory, macierze)

- zasilania (inteligentne listwy zasilające)

- warunków panujących w serwerowni (temperatura, wilgotność, światło, otwarcie drzwi, ruch)

- pracy zarządzalnych przełączników sieciowych

* Oprogramowanie musi mieć możliwość pracy w środowiskach wirtualnych
* Zdarzenia i reakcje na zdarzenia muszą być zapamiętywane w logu działań.
* Wymagane są rozbudowane systemy poziomów dostępu dla poszczególnych grup użytkowników z możliwością zróżnicowania uprawnień dostępu do:
* Raportów.
* Procedur alarmowych.
* Planów sytuacyjnych.
* Ustawień ogólnych.
* Opracowywania i zamykania zdarzeń alarmowych, zamykania zdarzeń nieopracowanych.
* Przekazywania zdarzeń do innych stacji obsługi ze zróżnicowaniem uprawnień na: brak dostępu, tylko odczyt, edycję, wprowadzanie nowych, kasowanie.
* System powinien posiadać możliwość przypisywania uprawnień dla operatorów z możliwością tworzenia indywidualnych stanowisk obsługi przypisanych do operatora bądź grupy.
* Wymagana jest możliwość skonfigurowania systemu z wieloma stanowiskami roboczymi.
* Wymagana możliwość skonfigurowania automatycznego kierowania zdarzeń alarmowych na odpowiednie stanowiska robocze. Dodatkowo wymagana jest możliwość przekazania zdarzenia przez użytkownika. Wymagany jest przy tym mechanizm weryfikacji czy wybrane stanowisko jest aktywne. Przy przekazywaniu zdarzenia wyświetlane są tylko aktywne stanowiska z identyfikatorem (loginem) użytkownika.
* Wymagana jest możliwość dowolnego ustawiania kategorii zdarzeń połączona z możliwością kierowania zdarzeń na stanowiska robocze. Wymagane jest zróżnicowanie kolorów zdarzeń poszczególnych kategorii.
* Zdarzenia muszą być prezentowane na liścia zdarzeń w jednowierszowej postaci zwięzłej. Musi istnieć możliwość edycji postaci zwięzłej – wymagana jest możliwość wyboru wyświetlanych danych spośród: lp. czas i data, nazwa (lokalizacja), zdarzenia, stan obecny, priorytet, kategoria, status, użytkownik.
* Wymagana jest możliwość ustawienia kolejności wyświetlania zdarzeń alarmowych przynajmniej według (lp., czasu, identyfikatora czujnika, zdarzenia, priorytetu, kategorii) rosnąco lub malejąco.
* Wymagane są liczniki zdarzeń oddzielne dla zdarzeń wszystkich kategorii. Musi istnieć możliwość filtrowania widoku zdarzeń na liście (stosie) alarmów na zdarzenia wybranej kategorii poprzez prostą operację (np. kliknięcie).
* Z widoku, w którym prezentowane są tylko zdarzenia wybranej kategorii (widok filtrowany) system musi powracać automatycznie do widoku zdarzeń wszystkich kategorii (widok nie filtrowany) po upływie zadanego czasu.
* Wymagana jest możliwość korelacji zdarzeń i generowania zdarzenia dodatkowego
* Wymagana jest możliwość wykonywania backupu online oraz backupu przyrostowego. Możliwość backupu bazy danych. Możliwość odtworzenia systemu z backupu.
* Wymagana jest sygnalizacja przerwy komunikacji z każdym integrowanym systemem poprzez wyświetlenie odpowiedniego komunikatu alarmowego.
* Wymagane jest, że PSIM musi automatycznie powrócić do stanu pracy. Niezbędne składniki oprogramowania (moduły) muszą być uruchamiane automatycznie (np. usługi systemu operacyjnego).
* Powinien posiadać plany w formacie wektorowym z możliwością skalowania obrazu dla całego obszaru jak i poszczególnych budynków, stref.
* Obsługa interaktywnych offlinowych map georeferencyjnych; możliwość nanoszenia elementów systemów podrzędnych na podkłady graficzne
* Czujniki na planie powinny być wyświetlane warstwowo dla poszczególnych systemów z możliwością wygaszania warstw i zdefiniowanych widoków (wycinków) na wypadek zdarzenia z danego systemu.
* System powinien posiadać możliwość tworzenia raportów dziennych, miesięcznych, kwartalnych ze sprawności integrowanych systemów.
* System powinien posiadać możliwość tworzenia indywidualnych procedur działania na wypadek zdarzenia w budynku z możliwością rozgałęzienia procedur na kolejne etapy w zależność od działań podjętych przez operatora.
* System powinien posiadać możliwość załączania dowolnych dokumentów takich jak karty katalogowe, instrukcje, przypisanych do konkretnych procedur działania, czujników lub urządzeń.
* System powinien mieć możliwość podłączenia dowolnego systemu za pomocą protokołu komunikacyjnego.
* System powinien mieć możliwość tworzenia indywidualnych stanowisk obsługi dla poszczególnych budynków jak i możliwość nadzorowania wszystkich budynków z jednej stacji operatorskiej.
* Należy zapewnić bezpieczne połączenie z serwerem za pomocą SSL.
* System musi umożliwiać filtrowanie aktywnych alarmów dla dowolnego zdarzenia,
* Wymagany jest mechanizm automatycznego wykonywania kopii zapasowych zgodnie z harmonogramem, na żądanie i z podziałem na kopiowane fragmenty systemu takie jak baza danych, logi, usługi, pliki konfiguracyjne, dokumentacje, instrukcje, zagnieżdżone elementy.
* Musi być obsługiwany w języku polskim.
* Możliwość biometrycznego zalogowania się operatora do systemu (np. przy użyciu odcisku palca, skanera tęczówki oka, itp).
* Wymaga się, aby system umożliwiał obsługę przygotowanych procedur reagowania na incydenty (zdarzenia). Musi umożliwiać zdefiniowanie procedur, które będą przypisane do każdego typu zdarzenia, przyczym każda przypisana procedura musi się składać z listy kroków wykonywanych przez (zdefiniowanego) użytkownika (Operatora). Każdy krok użytkownika (w zalezności od rodzaju zdarzenia) musi być poprzedzony pytaniem opisowym i wymuszającym odpowiedź “Tak” lub “Nie”.
* Operator w ramach obsługi konkretnej procedury musi mieć możliwość wysłania z poziomu system wiadomości SMS lub e-mail do zdefiniowanego w procedurze odbiorcy. Jednocześnie musi mieć możliwość wygenerowania krótkiego raportu (w formacie pdf.) podsumowującego zdarzenie i podjęte kroki (działania). Musi mież również możliwość wygenerowania alarmu skorelowanego z konkretną kamerą system CCTV a każdy jego krok musi być rejestrowany w baize danych.
* Operator musi mieć możliwość ręcznego uruchomienia procedury alarmowej w sytuacji gdy zauważy np. zdarzenie wymagające natychmiastowej interwencji (wypadek, zagrożenie życia lub zdrowia, pożar itp.). System musi również aktywować procedure alarmową automatycznie gdy wystąpił alarm np. z analityki video.
* Administartor systemu musi posiadać narzędzie (moduł) do edytowania I tworzenia (projektowania) odpowiednich procedur. Przy czym każda z tych procedur musi się składać z dowolnej ilości kroków, a każdy krok z dowolnej listy zdefiniowanych typów (np. polecenie: tekstowe, z dołaczonym przyciskiem akcji, pytaniem otwartym, pytaniem zamkniętym).
* Procedury muszą być uruchamiane w taki sposób, aby obejmowały (generowane przez użytkowników lub systemy) ujednolicone logiczne czynności sposobu reagowania na zaistniałe zdarzenie oraz prowadzić użytkownika (Operatora) “krok po kroku”.
* Moduł systemu zawierający procedury musi zapewniać użytkownikowi (Operatorowi) interreakcję z PSIM, która będzie umożliwiać obsługę przycisków np. “Tak”, “Nie” lub checkboxy oraz przycisków zdefiniowanych w procedurze akcji np. wysłanie SMS, uzbrojenie lub rozbrojenie strefy. Jednocześnie musi mieć pola tekstowe umożliwiające wpisanie dowolnego tekstu (komentarza) w każdym kroku procedury. Możliwość integracji z bramką SMS umożliwiająca wysyłanie i odbiór wiadomości tekstowych.
* System musi posiadać panel administracyjny umożliwiający upoważnionemu przedstawicielowi Zamawiającego dokonywanie samodzielnych modyfikacji systemu bez ponoszenia dodatkowych kosztów z tym związanych. Panel ten musi spełniać poniższe wymagania dotyczące:
	+ Użytkowników:
		- dodawanie nowych kont dla użytkowników,
		- przypisywanie kont dla grup użytkowników,
		- samodzielne definiowanie grup/ról użytkowników z przypisywaniem do nich uprawnień,
		- określanie polityki dotyczącej haseł (wymuszanie ilości znaków),
		- określanie czasu (daty) ważności konta użytkownika,
		- wprowadzanie danych użytkownika (imię, nazwisko, tel. kontaktowy, e-mail, jednostka organizacyjna),
		- czasowa blokada konta (od-do).
	+ Procedur:
		- tworzenie nowych procedur,
		- tworzenie kroków procedur,
		- zagnieźdżanie jednej procedury w drugiej,
		- wybór typu procedury (uruchamianie ręczne, uruchamianie automatyczne),
		- wybór typu kroku procedury (polecenie, warunek “Tak” lub “Nie”, automatyczna wysyłka wiadomości SMS lub e-mail, zablokowanie przejścia SKD).
	+ Mapy:
		- dodawanie nowych map,
		- zmiana dotychczasowych map,
		- dodawanie / zmiana lokalizacji/ usuwanie elementów zintegrowanych systemów z map (np. czujek),
		- wyświetlanie elementów, które nie zostały naniesione na mapy,
		- import nowo dodawanych elementów,
		- dodawanie i zmiana wyświetlanych nazw warstw mapy.
		1. **Wymagania dla okablowania strukturalnego**

System okablowania strukturalnego ma zapewnić niezawodną i wydajną warstwę fizyczną sieci teleinformatycznej, która zagwarantuje wystarczający zapas parametrów transmisyjnych dla działanie dzisiejszych i przyszłych aplikacji transmisyjnych. W celu spełnienia najwyższych wymogów jakościowych i wydajnościowych należy zapewnić:

* Okablowanie miedziane przewyższające wymagania kategorii 6 (klasy E).
* Okablowanie skrętkowe w wersji ekranowanej.
* Certyfikaty wydane przez międzynarodowe, renomowane niezależne laboratorium badawcze np. Delta, potwierdzające zgodność okablowania miedzianego z najnowszymi, aktualnymi normami okablowania strukturalnego ISO/IEC 11801:2011 (która zastępuje normy ISO/IEC 11801:2002, ISO/IEC 11801 AMD1:2006, ISO/IEC 11801 AMD2:2010), EN 50173-1:2011, TIA-568-C.2. Należy zapewnić certyfikaty potwierdzające zgodność z normami w zakresie testu całego łącza oraz niezależnych komponentów (kabel, panel, złącze RJ45). Nie dopuszcza się certyfikatów z lokalnych instytutów łączności, ponieważ nie posiadają one wystarczających akredytacji do testów wszystkich parametrów wymienionych w powyższych normach.
* Okablowanie światłowodowe wielodomowe OM3.
* Wszystkie produkty muszą być fabrycznie nowe.
* Celem idealnego dopasowania komponentów, wszystkie produkty okablowania strukturalnego muszą pochodzić z oferty jednego producenta i być oznaczone jego nazwą lub logo.
* Należy zastosować renomowany i sprawdzony w wielu instalacjach, nie tylko w Polsce, ale i w innych krajach Unii Europejskiej, system okablowania strukturalnego. Należy zastosować przetestowany system, którego producent ma, co najmniej 15-letnie doświadczenie w produkcji okablowania strukturalnego.
* Producent okablowania strukturalnego musi spełniać wymagania międzynarodowej normy odnośnie standardów jakości ISO 9001, należy przedłożyć odpowiedni certyfikat.
* Producent okablowania musi objąć zainstalowany system bezpłatną, 25-letnią systemową gwarancją niezawodności, która obejmie tory transmisyjne miedziane i światłowodowe w zakresie łącza Channel (kable instalacyjne, panele 19”, złącza, kable krosowe i przyłączeniowe). Gwarancja musi być trójstronną umowa podpisana pomiędzy Użytkownikiem, Wykonawcą okablowania oraz Producentem.
* Producent okablowania jest zobligowany do reasekuracji zobowiązań gwarancyjnych Wykonawcy, w przypadku niemożności wywiązania się Wykonawcy z tych zobowiązań. Reasekuracja obejmuje okres, na jaki została udzielona gwarancja.
* Warunkiem udzielenia systemowej gwarancji niezawodności jest wykonanie instalacji zgodnie z obowiązującymi normami okablowania strukturalnego oraz zgodnie z zaleceniami producenta. Instalacja musi być wykonana przez Certyfikowanego Instalatora systemu okablowania.

Zadaniem okablowania poziomego jest zapewnienie wydajnej i niezawodnej transmisji danych pomiędzy punktami dystrybucyjnymi, a punktami przyłączeniowymi użytkowników. Długość kabla instalacyjnego, pomiędzy gniazdem RJ45 w panelu rozdzielczym a gniazdem (nie licząc kabli krosowych i przyłączeniowych) nie może przekraczać 90m. Celem zapewnienia wysokiej przepływności nie tylko dzisiaj ale i w przyszłości należy zastosować okablowanie co najmniej klasy E (kategorii 6) wg najnowszych aktualnych standardów okablowania strukturalnego ISO/IEC 11801:2011, EN 50173-1:2011, TIA-568-C.2. Zagwarantuje to odpowiedni zapas parametrów transmisyjnych dla transmisji danych Ethernet 10Gb/s zgodnie ze standardem IEEE 802.3an. Zgodność z powyższymi normami należy udokumentować certyfikatami wydanymi przez laboratorium badawcze np. Delta, w zakresie całego łącza oraz niezależnych komponentów (kabel, panel, złącze RJ45).

Celem zapewnienia zasilania urządzeniom końcowym, należy zastosować komponenty okablowania strukturalnego zapewniające przesył energii zgodnie ze standardem PoEP (ang. Power over Ethernet Plus) wg IEEE 802.3at o mocy do 30W.

W połączeniach szkieletowych, pomiędzy głównym a pośrednimi punktami dystrybucyjnymi, należy zastosować kable światłowodowe spełniające poniższe wymagania (nie gorsze niż):

* Pojemność 4 włókna
* Włókna wielomodowe MM OM3 50/125µm o parametrach:

|  |  |
| --- | --- |
| **Parametr** | **Wartość** |
| Szerokość pasma przy 850 nm | 1500 MHz/km |
| Szerokość pasma przy 1300 nm | 500 MHz/km |
| Tłumienność przy 850nm | 2.5 dB/km |
| Tłumienność przy 1300nm | 0.7 dB/km |

* Konstrukcja kabla typu uniwersalna z możliwością układania wewnątrz budynku i na zewnątrz budynku(w rurach osłonowych).
* Wzmocniona` konstrukcja w postaci luźnej centralnej tuby, wypełnionej żelem chroniącym przed wilgocią oraz zmniejszającym tarcie pomiędzy włóknami w czasie układania.
* Konstrukcja kabla musi zawierać wzmocnienie w postaci włókien szklanych, które dodatkowo muszą zapewniać ochronę antygryzoniową.
* W celu spełnienia wymogów przeciwpożarowych należy zastosować kabel w powłoce zewnętrznej LSZH (ang. Low Smoke Zero Halogen), czyli wykonanej z materiału bezhalogenowego emitującego ograniczoną ilość szkodliwych substancji w czasie pożaru.
* Wymagane parametry kabla światłowodowego

|  |  |
| --- | --- |
| **Parametr** | **Wartość** |
| Siła ciągnienia (maksymalna) | 1600 N |
| Promień gięcia (minimalny) | 105 mm |
| Odporność na zgniatanie(maksymalna) | 1500 N/dm |
| Zakres temperatury instalacji | -15 /+50 °C |
| Zakres temperatury pracy | -40 /+70 °C |

Po wykonaniu instalacji okablowania strukturalnego wykonawca musi przeprowadzić odpowiednie pomiary sprawdzające (certyfikacyjne), wszystkich łączy miedzianych skrętkowych i światłowodowych, potwierdzające, iż wykonane okablowanie strukturalne spełnia wymagania norm. Pomiary należy przeprowadzić zgodnie z wartościami granicznymi zdefiniowanymi w ISO 11801 lub EN 50173. Wyniki wszystkich pomiarów muszą być pozytywne. Pomiary należy wykonać przyrządem w pełni sprawnym, posiadającym ważny certyfikat potwierdzający przejście procesu kalibracji u producenta, co będzie potwierdzeniem poprawności jego wskazań. Do dokumentacji powykonawczej należy dołączyć wymieniony certyfikat kalibracji oraz raport z wynikami pomiarów wszystkich łączy okablowania skrętkowego i światłowodowego.

* + 1. **Pomiary okablowania miedzianego**

Wszystkie łącza skrętkowe w systemie należy przetestować pod kątem spełniania wymogów klasy E / kategorii 6 wg ISO 11801 lub EN 50173:

* Należy przeprowadzić pomiary w układzie pomiarowym typu „Permanent Link” (bez kabli krosowych).
* Pomiary należy wykonać miernikiem o poziomie dokładności, co najmniej „Level IV”. Zalecane typy mierników: DSX-5000, DTX-1800 lub DTX-1200 firmy Fluke Networks.
* Należy wykonać pomiary certyfikacyjne, w których po zmierzeniu rzeczywistych wartości parametrów łącza, miernik automatycznie porówna je z granicznymi wartościami definiowanymi przez aktualne normy okablowania i określi wynik porównania.
* Wyniki pomiarów certyfikacyjnych wszystkich łączy musza być prawidłowe.
* Pomiary należy wykonać zgodnie z wymaganiami normy PN-EN 50346.
* Wymagany zakres mierzonych parametrów dla każdej z par (kombinacji par):
	+ Mapa połączeń - poprawność i ciągłość wykonanych połączeń
	+ Straty odbiciowe (ang. RL - Return Loss)
	+ Straty wtrąceniowe - tłumienie (ang. IL - Insertion Loss)
	+ Straty przesłuchów zbliżnych (ang. NEXT - Near End Crosstalk Loss)
	+ Sumaryczny parametr NEXT (ang. PSNEXT – Power Sum NEXT)
	+ Współczynnik tłumienia w odniesieniu do straty przesłuchu na bliskim końcu (ang. ACR-N – Attenuation to Crosstalk Ratio at the Near end)
	+ Sumaryczny współczynnik ACR-N (ang. PSACR-N – Power Sum ACR-N)
	+ Współczynnik tłumienia w odniesieniu do straty przesłuchu na dalekim końcu (ang. ACR-F – Attenuation to Crosstalk Ratio at the Far end)
	+ Sumaryczny współczynnik ACR-F (ang. PSACR-F – Power Sum ACR-F)
	+ Rezystancja pętli dla prądu stałego (ang. DC current loop)
	+ Opóźnienie propagacji (ang. Propagation delay)
	+ Różnica opóźnień propagacji (ang. Delay skew)
		1. **Pomiary okablowania światłowodowego**

Wszystkie łącza światłowodowe w systemie należy przetestować pod kątem spełniania wymogów norm ISO 11801 lub EN 50173:

* Należy przeprowadzić pomiary dwukierunkowe, w których źródło świetlnego sygnału referencyjnego będzie umieszczone w pierwszym kroku na jednym końcu łącza, a w kolejnym kroku na drugim końcu łącza.
* Łącza wielomodowe (MM) należy przetestować w dwóch oknach transmisyjnych, dla długości fali: 850 nm i 1300 nm.
* Należy wykonać pomiary certyfikacyjne, w których po zmierzeniu rzeczywistych wartości parametrów łącza, miernik automatycznie porówna je z granicznymi wartościami definiowanymi przez aktualne normy okablowania i określi wynik porównania.
* Wyniki pomiarów certyfikacyjnych wszystkich łączy musza być prawidłowe.
* Pomiary należy wykonać zgodnie z wymaganiami normy PN-EN 50346.
* Wymagany zakres mierzonych parametrów:
	+ Ciągłość łącza.
	+ Długość łącza.
	+ Tłumienie włókien dla dwóch długości fali.
1. **Wymagania serwisowe w okresie gwarancyjnym**
2. Do dostarczonych urządzeń, będących przedmiotem umowy Wykonawca, dołączy zbiorczy ich wykaz zawierający: numery seryjne, terminy i warunki ważności gwarancji i rękojmi (które nie mogą być w żaden sposób sprzeczne z zapisami OPZ), adresy, numery telefonów, faksów punktów serwisowych świadczących usługi gwarancyjne.
3. Zamawiający dysponuje urządzeniami będącym w okresie gwarancyjnym, a moziliwymi do wykorzystania przez Wykonawcę: 20 kamer IP marki Avigilon oraz serwer wraz z półką dyskową i licencjami dedykowany do obsługi tych kamer.
4. Zamawiający wymaga, aby oferowany przedmiot zamówienia objęty był gwarancją Wykonawcy przez okres co najmniej 5 lat licząc od daty końcowego protokołu odbioru.
5. Dostarczone urządzenia wchodzące w skład przedmiotu umowy muszą spełniać wymagania techniczno-funkcjonalne opisane w niniejszej koncepcji oraz muszą być wolne od wad i zgodne z poziomem technologii istniejącym w momencie podpisania umowy.
6. O usterce Zamawiający powiadomi Wykonawcę poprzez dostarczoną i wdrożoną przez Wykonawcę, elektroniczną platformę obsługi zgłoszeń oraz w formie telefonicznej, mailowej lub pisemnej. Każde zgłoszenie telefoniczne wymaga potwierdzenia w formie pisemnej.
7. Pisemny raport z naprawy po każdej naprawie gwarancyjnej musi zawierać co najmniej następujące informacje:
* datę zgłoszenia usterki;
* datę odbioru sprzętu od Zamawiającego;
* rodzaj i opis usterki;
* opis wykonanych czynności serwisowych w tym wymienionych elementów;
* opis procedur weryfikacyjnych i ich wyniki;
* datę przekazania naprawionego urządzenia do Zamawiającego;
* podpisy przedstawicieli Wykonawcy i Zamawiającego.
1. Zamawiający przekaże Wykonawcy wzory formularzy, o których mowa w ppkt. d) i e) oraz określi procedurę zgłaszania usterek.
2. Wykonawca jest zobowiązany do zdemontowania i odebrania uszkodzonych urządzeń z miejsca ich instalacji i dostarczenia, zainstalowania i uruchomienia naprawionych urządzeń w miejscu ich instalacji na własny koszt. W wyjątkowych sytuacjach, po uzyskaniu pisemnej zgody od Zamawiającego, uszkodzone urządzenia mogą zostać dostarczone do siedziby Wykonawcy przez Zamawiającego na koszt Wykonawcy.
3. Czas naprawy nie może być dłuższy niż 14 dni licząc od dnia następującego po powiadomieniu Wykonawcy o usterce. Za dzień wykonania naprawy gwarancyjnej Zamawiający uzna dzień podpisania przez upoważnionych przedstawicieli Zamawiającego i Wykonawcy raportu z naprawy, o którym mowa w pkt. e).
4. Jeżeli naprawa uszkodzonego urządzenia nie będzie możliwa w wyznaczonym terminie (określonym w pkt. h)), wówczas Wykonawca jest zobowiązany do dostarczenia, zainstalowania i uruchomienia urządzenia zastępczego posiadającego, co najmniej takie same parametry i funkcjonalność, co urządzenia naprawiane).
5. W przypadku zgłoszenia przez Zamawiającego niesprawności/uszkodzenia urządzenia zastępczego Wykonawca jest zobowiązany do dostarczenia, zainstalowania i uruchomienia w czasie 1 dnia (licząc od dnia następnego po pisemnym powiadomieniu Wykonawcy o zaistnieniu powyższych okoliczności) kolejnego urządzenia zastępczego posiadającego co najmniej takie same parametry i funkcjonalność co urządzenia naprawiane. Niedostarczenie, niezainstalowanie i nieuruchomienie przez Wykonawcę sprawnego urządzenia zastępczego spełniającego wymagania Zamawiającego spowoduje naliczenie kar umownych za opóźnienie w naprawie gwarancyjnej.
6. Po wykonaniu naprawy oraz dostarczeniu, zainstalowaniu i uruchomieniu naprawionego urządzenia w miejscu instalacji Wykonawca dokona podmiany urządzenia i zabierze zdemontowane urządzenie zastępcze. Na wniosek Wykonawcy w szczególnych przypadkach zdemontowane urządzenie zastępcze może zostać na jego koszt odesłane przez Zamawiającego.
7. Zamawiający nie dopuszcza możliwości wykorzystania urządzeń będących w naprawie jako urządzeń zastępczych dla innych, równolegle prowadzonych napraw.
8. W przypadku, gdy czas naprawy, licząc od dnia następnego po powiadomieniu Wykonawcy o konieczności dokonania naprawy, przekroczy 180 dni, Wykonawca dostarczy, zainstaluje i uruchomi na własny koszt nowe urządzenie o co najmniej takich samych parametrach, jak urządzenie naprawiane.
9. Nowe urządzenie musi być dostarczone do Zamawiającego, zainstalowane i uruchomione najpóźniej w ciągu 4 dni od upływu terminu naprawy gwarancyjnej określonego.
10. W przypadku, gdy Wykonawca (po przekroczeniu 180 dni naprawy) nie dostarczy, nie zainstaluje i nie uruchomi nowego urządzenia, o którym mowa w pkt 15 w terminie określonym w pkt. 16 Zamawiający ma prawo zakupić od osób trzecich (zdemontować, zainstalować i uruchomić) na koszt Wykonawcy nowe urządzenie, o co najmniej takich samych parametrach, jaku rządzenie naprawiane. W takim przypadku Zamawiający nie traci praw do gwarancji i rękojmi za wady.
11. Gwarancja na naprawiony sprzęt zostanie przedłużona o czas naprawy.
12. W okresie gwarancyjnym Wykonawca zapewni stały kontakt ze swoimi przedstawicielami, którzy będą nie odpłatnie, udzielać Zamawiającemu informacji, konsultacji i pomocy technicznej (tzw. Hot-Line) w zakresie użytkowania sprzętu i oprogramowania, będącego przedmiotem zakupu. Językiem porozumiewania się stron będzie język polski.