**Opis Warunków Zamówienia**

**System Kontroli Dostępu, System Monitoringu Wizyjnego CCTV, System Awizacji w Enea Elektrownia Połaniec S.A. (dalej: „EEP”).**

Wykonawca ma obowiązek zaprojektować, dostarczyć oraz wdrożyć:

* System Kontroli Dostępu (dalej „SKD”),
* System Monitoringu Wizyjnego CCTV (dalej „CCTV”),
* System Awizacji (dalej „SA”)

na Platformie Integrującej w Enea Elektrownia Połaniec S.A, zgodne z poniżej określonymi wytycznymi. Wskazania Zamawiającego w zakresie funkcjonalności systemów należy traktować, jako priorytetowe.

1. **System Kontroli Dostępu („SKD”)**
2. Wymagania dotyczące SKD
	1. Dostarczony SKD musi zapewniać nieograniczoną rozbudowę w zakresie:
		1. Liczby przejść kontrolowanych przez SKD.
		2. Liczby identyfikatorów w SKD.
		3. Liczby rekordów bazy danych.
		4. Liczby filii zarządzanych z poziomu serwera centralnego.
		5. Liczby zdarzeń w SKD.
		6. Liczby użytkowników w SKD.
	2. Dostarczony SKD musi cechować się bardzo dużym stopniem stabilności (pkt 1.7.5.5) i redundancji (dyspozycyjność 24h/dobę, 365 dni/rok). Warunkiem koniecznym jest zapewnienie w SKD autonomicznego działania kontrolerów. Oznacza to, że:
		1. Kontrolery muszą być standardowymi urządzeniami sieciowymi (posiadającymi możliwość komunikacji z innymi urządzeniami w sieci TCP/IP, bez konieczności stosowania jakiejkolwiek formy konwersji sygnału.
		2. Kontrolery muszą posiadać dużą moc obliczeniową (CPU minimum 800MHz) i duże zasoby pamięci (min. 256 MB SDRAM, 2 GB pamięci typu Flash).
	3. Komunikacja w SKD musi odbywać się z wykorzystaniem protokołu TCP/IP w sposób szyfrowany i zabezpieczony protokołem SSL/TLS i szyfrem co najmniej 128 bitowym.
	4. Monitorowanie urządzeń powinno zostać zrealizowane poprzez protokół SNMP lub równoważny.
	5. Logowanie do SKD musi być zabezpieczone indywidualnym loginem i hasłem, przy czym SKD musi pozwalać na wymuszenie przez administratora stosowania haseł o określonej sile oraz ich zmianę po określonym interwale czasowym.
	6. SKD musi zapewniać swobodne programowanie funkcjonalności (na poziomie kontrolera) z poziomu prostej aplikacji graficznej za pomocą metod „drag and drop”.
	7. Minimalne wymagania dla projektowanego środowiska serwerowego:
		1. Serwer produkcyjny powinien działać w klastrze HA (w razie uszkodzenia 1 węzła zostaje uruchomiony drugi).
		2. Środowisko serwerowe musi składać się z:
			1. Serwera aplikacji umożliwiającego pracę w dowolnym systemie wspomaganym przez Java.
			2. Relacyjnej bazy danych (serwera bazodanowego) wykorzystującego język zapytań SQL.
		3. Projektowane środowisko serwerowe powinno spełniać następujące minimalne wymagania sprzętowe:
			1. Nowoczesna 64 bitowa maszyna serwerowa (zastosowane serwery będą serwerami wirtualnymi w środowisku VMWare.).
			2. Jeden z poniższych systemów operacyjnych:
* Linux CentOs w wersji minimum 7.
* Minimum Microsoft Windows Server 2016R2.
	+ - 1. Jedna z poniższych baz danych:
* Oracle® 12c Enterprise edition lub wyższą.
* Microsoft® SQL Server 2012 lub wyższej
* MySQL Enterprise Edition.
* PostgreSQL wersja 9.4
	+ 1. Aplikacja Kliencka/Operatorska musi:
			1. Umożliwiać dostęp do SKD dla Użytkownika (role typu: Administrator, Operator, Recepcja) z poziomu przeglądarki internetowej – brak konieczności instalowania dodatkowego, dedykowanego oprogramowania na stacjach roboczych.
			2. Wspierać minimum poniżej wskazane przeglądarki:
* Microsoft Internet Explorer lub nowsze wersje.
* Firefox.
* Chrome.
	+ 1. Wymagania dotyczące projektowanych kontrolerów:
			1. Kontrolery muszą zapewniać możliwość autonomicznego podejmowania decyzji o autoryzacji bez udziału serwera (informacje niezbędne do autoryzacji opcjonalnie mogą być przechowywane również w pamięci kontrolerów, a nie tylko na serwerze).
			2. Kontrolery muszą buforować co najmniej 1 000 000 zdarzeń pracując w trybie autonomicznym.
			3. Buforowane zdarzenia muszą być automatycznie przesyłane, po odzyskaniu łączności z serwerem.
			4. Kontrolery muszą mieć możliwość bieżącego przekazywania informacji o stanach czujników (np. kontaktronów drzwiowych) również podczas braku dostępu do serwera.
			5. Kontrolery SKD muszą posiadać możliwość pracy w trybie autonomicznym. Oznacza to, że w sytuacji braku dostępu do serwera z jednej strony będą one w stanie przejąć na siebie rolę bezpośredniej komunikacji między sobą i będą przesyłać na bieżąco informacje o stanach przejść (drzwi otwarte/drzwi zamknięte, drzwi otwarte zbyt długo, drzwi sforsowane itp.) do własnego systemu monitorującego lub do zewnętrznych zintegrowanych systemów monitorujących.
			6. Zmiana oprogramowania czy konfiguracji systemu musi być możliwa dla całego SKD z jednego centralnego punktu lub dla wybranych elementów/modułów lokalnie lub centralnie. Możliwe musi być zdalne sprawdzenie pełnej konfiguracji zapisanej w pamięci wybranego kontrolera (poprzez graficzne narzędzie pozwalające na monitorowanie działania SKD w trybie na żywo – np. przyłożenie identyfikatora do czytnika spowoduje zaznaczenie całej ścieżki sygnału w systemie od czytnika, poprzez moduł czytnika aż do kontrolera).
			7. SKD musi być zaprojektowany w oparciu o architekturę gwiazdy przy użyciu tylko kontrolerów, połączonych bezpośrednio do przełączników sieciowych. W architekturze SKD mogą być użyte tylko kontrolery, bez modułów rozszerzeń.
			8. Dostarczony SKD musi posiadać integracje z systemem Platformy Integrującej potwierdzoną przez producenta tego systemu w zakresie:
		- Wizualizacji stanów pracy: otwarcie przejścia za pomocą karty, udzielenia dostępu do KD przez administratora, zakluczenia drzwi których zamki wysyłają takie stany oraz stan awarii.
		- Sterowania przejściami: otwarcie, zamknięcia drzwi,
			1. Kontrolery muszą posiadać obok standardowego wejścia zasilającego 12-24 VDC, możliwość zasilania za pomocą standardu PoE+ (Power over Ethernet IEEE 802.3at).
	1. Wymagania dotyczące oprogramowania aplikacyjnego:
		1. SKD musi posiadać, co najmniej trzy rodzaje oprogramowania aplikacyjnego lub zapewniać, w zależności od uprawnień osoby zalogowanej do aplikacji uzyskanie co najmniej trzech poziomów zarządzania systemem:
* Poziom administratora.
* Poziom rozszerzony użytkownika (możliwość zarządzania alarmami, drzwiami, możliwość dodania komentarza dla poszczególnych alarmów).
* Poziom ograniczony użytkownika (informacja o stanie autoryzacji wraz z prezentacją miejsc w których autoryzacja bądź jej brak miała miejsce).
	1. Oprogramowanie najwyższego poziomu musi zawierać wbudowany moduł obsługi i monitorowania alarmów i stanów czujników SKD. W module tym musi być możliwość przypisywania do konkretnych alarmów/zdarzeń określonych procedur. W ramach procedur alarmowych wyświetlane muszą być przygotowane wcześniej instrukcje alarmowe, a w określonych przypadkach, SKD musi wymuszać opatrzenie alarmu komentarzem i zestawem komentarzy pracownika ochrony pełniącego służbę na stanowisku monitoringu obiektowego. SKD musi umożliwiać również automatyczne pokazanie podglądu z kamery wideo, która jest skojarzana z punktem alarmowym np. główne wejście do budynku.
	2. Oprogramowanie niższego poziomu musi wykorzystywać do komunikacji pomiędzy SKD a użytkownikiem przede wszystkim elementy graficzne takie jak ikony, okna i przyciski. SKD musi pozwalać na podłączanie skanerów dokumentów co najmniej kilku różnych producentów, dzięki którym możliwe będzie wprowadzanie danych osobowych poprzez skanowanie dokumentów potwierdzających tożsamość. Oprogramowanie musi posiadać możliwość obsługi czytników kart dla biur przepustek. Oprogramowanie musi zapewniać możliwość wprowadzania tzw. pól dowolnych (np. PESEL itp.) Oprogramowanie musi pozwalać na ograniczanie dostępnych funkcjonalności w zależności od uprawnień i obowiązków użytkownika logującego się do SKD.
	3. Wszelkie informacje wyświetlane w oprogramowaniu muszą być dostępne w języku polskim i zawierać polskie znaki diakrytyczne.
	4. Poza standardowymi funkcjami oprogramowania SKD dotyczącymi nadawania posiadaczom identyfikatorów i uprawnień dla poszczególnych przejść zgodnie z określonymi harmonogramami czasowymi, SKD musi pozwalać na realizację poniższych funkcjonalności:
		1. Kontrola obchodu strażników (z możliwością swobodnego kształtowania tras obchodu i okien czasowych dla poszczególnych punktów kontrolnych – czytników).
		2. Automatyczne blokowanie identyfikatorów po określonym czasie nieużywania.
		3. Tworzenie profili tymczasowych tzn. zmiana profilu na określony czas, po którym automatycznie zostanie przywrócony poprzedni profil.
		4. Blokowanie identyfikatorów w wyniku określonych naruszeń instrukcji ruchu osobowego np. złamanie zasady antypassback.
		5. SKD musi pozwalać na automatyczne usuwanie danych odwiedzających po definiowalnym okresie czasu.
		6. Tekstowy monitor zdarzeń – bieżące wyświetlanie wszystkich zdarzeń w SKD w formie tekstowej.
		7. Rozbudowany monitor zdarzeń – bieżące wyświetlanie zdarzeń w SKD z towarzyszącymi im zdjęciami (zdjęcia osób wyświetlane w tym samym momencie co zbliżenie identyfikatora do czytnika).
		8. Tworzenie tzw. czarnych list (list osób i pojazdów niepożądanych).
		9. Awizowanie wizyt gości/firm zewnętrznych przez pracowników posiadających dostęp do SKD.
		10. Zliczanie osób w określonej strefie i wprowadzanie ograniczeń liczby osób uprawnionych do przebywania w strefie.
		11. Tworzenie wydzielonych wirtualnie części SKD dla poszczególnych oddziałów, dzięki czemu użytkownicy w poszczególnych oddziałach będą mieli możliwość nadawania uprawnień jedynie osobom przypisanym do swojego oddziału. Wybrani użytkownicy SKD będą mogli kształtować uprawnienia wszystkich osób.
		12. Stosowanie filtrów przejść, dzięki czemu użytkownicy SKD w poszczególnych oddziałach będą mieli dostęp do przejść przypisanych jedynie do ich oddziału.
		13. Ograniczenie liczby zbliżeń identyfikatora do czytników, dzięki czemu możliwe musi być wymuszenie właściwej ścieżki poruszania się po obiekcie – jeżeli na drodze od wejścia głównego do pomieszczenia, które jest celem wizyty znajdują się 4 czytniki możliwe musi być ograniczenie tej liczby do 4, co wyeliminuje ryzyko nieuprawnionego poruszania się osoby po obiekcie.
		14. SKD musi mieć możliwość łączenia zdarzeń tekstowych (np. autoryzacja, otwarcie drzwi itp.) wraz ze zdjęciami poszczególnych użytkowników oraz ujęciem na żywo z kamery, aby móc w trybie rzeczywistym porównać prezentowane dane.
		15. Możliwość importu danych osobowych z innego zewnętrznego źródła (np. baza danych działu personalnego) w minimum standardzie pliku xlsx.
		16. SKD musi umożliwiać integracje z LDAP.
		17. SKD musi umożliwiać zastosowanie funkcjonalności ANTYPASSBACK - uniemożliwia dwukrotne wejście posiadacza do danej strefy bez jej opuszczenia albo użycia niedozwolonego przejścia. APB zapobiega autoryzowanemu wejściu do budynku, strefy lub obszaru przez osobę korzystającą z identyfikatora należącego do osoby już będącej w środku.
		18. SKD musi umożliwiać zastosowanie następujących trybów antypassback:
* Miękki APB (ANTYPASSBACK)– generuje zdarzenie alarmowe po naruszeniu zasady.
* Twardy APB (ANTYPASSBACK– nie wpuszcza karty z wewnątrz strefy do tej samej strefy
* Czasowy APB (ANTYPASSBACK) – możliwy reset osoby po określonym czasie od wejścia do wyjścia.
	+ 1. Infrastruktura IT GK ENEA oparta jest o platformę wirtualizacją VMware vSphere.
		2. Serwery SKD będą również zwirtualizowane na tej platformie, zarówno środowisko testowe i produkcyjne.
		3. SKD ma być zbudowany o klastry HA tak aby wyeliminować pojedyncze punkty awarii.
		4. SKD musi posiadać architekturę rozproszoną między CPD w GK ENEA ( Poznań - Kozienice - Połaniec)
		5. Pod instalację SKD zostanie udostępniona licencja Windows Server 2016 lub 2019.
		6. SKD musi być oparty o czytniki obsługujące karty w standardzie Desfire EV1
		7. W ramach projektu zostaną wymienione kołowroty na bramach wejściowych o przepustowości nie mniejszej niż 40 osób na minutę w pracy ciągłej oraz furtki sterowane przez służby ochrony w celu całkowitego zabezpieczenia wejścia na obiekt. Wymiana urządzeń po stronie wykonawcy.
		8. W ramach dostawy zostaną wymienione skanery do dowodów osobisty na czytniki pobierające dane z dokumentów oraz drukarki do wydawania przepustek w formie naklejek oraz nadruku na kartach stałych zgodnie z Instrukcją Ruchu Osobowego EEP.
		9. W związku z wymaganiami BHP i Ppoż, klamki od wewnątrz muszą być funkcjonalne.
		10. SKD musi obsługiwać :
* <20 tysięcy użytkowników.
* nadzorować < 1500 przejść.
* umożliwiać praca kontrolerów on line lub autonomiczną (w zakresie pamięci buforowej)
* pojemność zapisu zdarzeń w trybie ON-LINE min. na okres 12 miesięcy
* możliwość określenia 120 dni wolnych
* funkcja Anti-pass-back
* zakres temperatur pracy czytników – do -30 oC +60 oC
* monitorowane wejścia czujników drzwi, przycisków wyjścia, itd.
* współpraca z czytnikiem biometrycznym
* możliwość kontroli wind
	+ 1. Czas na czytnikach ma być uregulowany i zsynchronizowany z wewnętrznym serwerem NTP GK ENEA.
		2. SKD musi posiadać przejrzysty interfejs nadawania uprawnień (zatwierdzony przez EEP) do stref z poziomu widoku użytkownika.
		3. SKD powinien mieć możliwość blokowania wejścia dla wybranych osób zgodnie z harmonogramem lub całkowitego zablokowania możliwość wejścia na obiekt.
		4. SKD musi posiadać możliwość rozróżnienia użytkowników z dostępem do obiektu dla wszystkich firm realizujących dostawy, usługi lub roboty budowlane na terenie elektrowni lub mających siedzibę na terenie elektrowni.
		5. Umożliwienie zmiany karty Gościa na Tymczasową (Gościa powinna stracić uprawnienia analogicznie jak przy przepustkach stałych).
		6. Po zabraniu uprawnień danej karcie należy dawać możliwość zmiany statusu użytkownika na nieobecny w obiekcie – bez konieczności używania karty tego użytkownika na czytniku wyjściowym z obiektu
		7. Generowanie się sygnału alarmowego na stanowisku dowodzenia ochroną po nieprawidłowym odbiciu karty.
		8. Po wymianie czytnika i wysłaniu uprawnień, informowanie o zakończeniu przesyłania uprawnień i jego statusie.
		9. Umożliwienie zarządzanie kontami użytkowników i operatorów całego SKD z poziomu serwera.
		10. SKD musi umożliwiać nadawanie uprawnień dla operatorów do wybranej części logicznej/fizycznej SKD.
		11. Dysponowanie modułem typu wartownik – wyświetlanie zdjęć osób właśnie przechodzących przez dane przejście – w celu dodatkowej weryfikacji wzrokowej – porównywania przechodzącej osoby z jej zdjęciem zapisanym w bazie danych.
		12. SKD musi posiadać możliwość integracji z Active Directory.
		13. Autentykacja do aplikacji będzie następowała poprzez konto domenowe SKD.
		14. Wykonawca SKD powinien udostępnić wszystkie potrzebne aplikacje i sterowniki (wraz z udzieleniem niezbędnych licencji) potrzebne do ewentualnego ponownego zainstalowania SKD na stacji roboczej lub serwerze ( również sterowniki do drukarek, skanerów itp.)
		15. Przy zerwaniu etykiety z przepustki tymczasowej brak możliwości na podstawie kodu wewnętrznego ustalenia ostatniego użytkownika, kto miał wydaną przepustkę - chodzi o dołożenie czytnika USB na bramie gdzie wydawane są przepustki tymczasowe.
		16. Na formularzu przepustki tymczasowej w zakładce dane użytkownika należy usunąć dane pojazdu. Pole zablokować ma być dostępne dla Gościa. Na przepustkach tymczasowych pole ma być zablokowane
		17. Zablokować edycję numeru ewidencyjnego dla obsługi biur przepustek, podczas wystawiania przepustek rezerwowych. Nr ewidencyjny wprowadzony przy przepustkach stałych. Zablokować pole nr ewidencyjnego przy przepustkach stałych dla biur przepustek na bramach, zmiany wprowadza tylko administrator SKD.
		18. SKD nie może pozwalać na wystawienia więcej niż jednej przepustki na użytkownika.
		19. SKD ma zapewnić obsłużenie minimalnej przepustowości 2 co 5 minut wjeżdżających i wyjeżdżających samochodów na bramie samochodowej nr 3. Wyjeżdżające samochody będą opuszczać teren elektrowni tą samą bramą. Istnieje możliwość, że do czasu wdrożenia powstanie 4 brama która będzie obsługiwała tylko i wyłącznie wyjazdy dostaw biomasy, co zredukuje ilość wyjazdów bramą nr 3 ale nie zlikwiduje ich zupełnie. Sprawna i szybka obsługa pozostałych bram nr 1 i 2. Stanowiska na bramach nie ulegną zmianie.
		20. SKD musi posiadać możliwość tworzenia dedykowanych grup np. po nazwie firmy i pozwalać na nadawanie określonych uprawnieni dla kart tych grup ( grupy nie tylko mogły by być tworzone przy wprowadzeniu do SKD użytkowników ale też wyodrębniane z istniejących już w systemie użytkowników kart.)
1. Wymagania dotyczące bezpieczeństwa:
	1. System SKD musi zapewniać dedykowane zabezpieczenia chroniące przed atakami sieciowymi, polegające na wyposażeniu kontrolera drzwiowego w moduł, który umożliwia przechowywanie certyfikatów uwierzytelniających komunikację między serwerem zarządzającym Systemem Kontroli Dostępu a kontrolerami drzwiowymi. Takie rozwiązanie wymusza autentykacje nowych kontrolerów przez administratora zanim zostaną dodane do Systemu Kontroli Dostępu, a tym samym zabezpiecza przed nieautoryzowanym zmodyfikowaniem oprogramowania zarządzającego kontrolerem.
	2. Klucze Mifare Plus X oraz DESSFire EV1 odpowiadające za odczyt danych autoryzacyjnych z karty RFID, mają posiadać opcję przechowywania w tym samym dedykowanym module kontrolera drzwiowego co certyfikaty autentykacyjne. W takim scenariuszu czytnik staje się dla karty transparentny i deszyfracja następuje po stronie kontrolera.
	3. Zarządzanie certyfikatami autentykacyjnymi jak i kluczami Mifare Plus X oraz DESFire ma być możliwe z centralnego poziomu, jednej stacji roboczej. Certyfikaty i klucze mają posiadać możliwość automatycznego dystrybuowanania do kontrolerów drzwiowych z jednego punktu zarządzania do wszystkich elementów systemu KD.
	4. Zamawiający ma mieć możliwość zarządzania i wymiany certyfikatów autentykacyjnych w każdym momencie bez ingerencji dostawcy systemów.
	5. Wszystkie stany alarmowe przejść muszą być zobrazowane graficznie na rzutach pomieszczeń w systemie wizualizacji zdarzeń. Ponadto należy przygotować instrukcję/zestaw instrukcji dla niżej omówionych zdarzeń (otwarcie przy pomocy przycisku, otwarcie przy pomocy karty, otwarcie przy pomocy przycisku ewakuacyjnego, zbyt długo otwarte przejście, sforsowane przejście, przejście otwarte trwale, przejście zamknięte trwale, przejście otwarte z harmonogramu, przejście uszkodzone, sabotaż krańcówki przejścia, sabotaż przycisku wyjścia, brak stanu przejścia).
	6. W projekcie należy zaprojektować automatyczne otwieranie się przejść objętych Systemem Kontroli Dostępu na drogach ewakuacyjnych podczas wystąpienia alarmu II stopnia instalacji sygnalizacji pożaru. Ta funkcjonalność powinna być realizowana za pomocą central sterowniczych systemu aplikacji na platformie integrującej i w nim zwizualizowana.
	7. Dodatkowo administrator systemu ma mieć możliwość otwarcia wybranych przejść lub zdefiniowanych grup przejść na wypadek zdarzeń typu napad, ewakuacja.
	8. W związku z obsługiwaną przez Zamawiającego infrastrukturą krytyczną, dostarczony System Kontroli Dostępu musi mieć możliwość użycia systemu certyfikatów dla wszystkich urządzeń cyfrowych systemu KD, autoryzujący urządzenia i komunikację wewnątrz systemu KD (czytnik - kontroler - serwer - stacja operatorska). Dystrybucja certyfikatów na urządzenia systemu musi być w wyłącznym posiadaniu i z pełną możliwością zarządzania przez Zamawiającego i odbywać się z centralnego punktu do wszystkich urządzeń systemu KD (PKI Zamawiającego). Zastosowanie takiej architektury bezpieczeństwa spowoduje iż wszystkie wrażliwe klucze (w tym klucz odczytu numeru karty, ulokowany w standardowych rozwiązaniach na czytniku) znajdować się będą na kontrolerze w bezpiecznym module po chronionej stronie dostępu. Każdy projektowany element: czytnik, kontroler i karta muszą być gotowe do implementacji reguł end to end security w formule opisanej powyżej. Efektem implementacji mechanizmów end to end security ma być możliwość zmiany używanego klucza Mifare Plus X oraz DESFire zapisanego na karcie bez rekonfiguracji każdego czytnika kart dostarczonej infrastruktury z osobna. Ma to na celu umożliwienie prewencyjnej lub reaktywnej (w chwili podwyższonego zagrożenia) wymiany używanych kluczy oraz zmianę kluczy jeśli jest podejrzenie, że zostały skopiowane.
2. Raportowanie
	1. Uzyskanie niezbędnych raportów w dziale NS i ( DK – w zakresie ruchu osobowego pracowników GK ENEA ) przedstawią wzory. Możliwość wszelkiego rodzaju raportowania po wszelkich znamionach identyfikacji np. numer karty+ czasookres+ marka pojazdu +rodzaj ładunku+ Nazwisko+ imię+ nr rej. Samochodu i naczepy +data zdarzenia,+ określone godziny, + rodzaj zdarzenia, nazwa firmy, np. wjazd, wyjazd, wejście, wyjście z terenu lub ze strefy, rodzaj ładunku,
	2. Możliwość identyfikacji który z operatorów wydał daną przepustkę i kiedy.
	3. Umożliwienie tworzenia kombinacji filtra przejść - tak, aby można stworzyć filtr przejść dla poszczególnych rodzajów kart i czytników.
	4. Umożliwienie dodania firmy, marki pojazdu przez administratora, bez dodania karty.
	5. Umożliwienie wykonywania raportów po oznaczniku obecny na terenie zakładu tj. ile osób i pojazdów znajduje się w danej chwili na terenie zakładu.
	6. Umożliwienie automatycznego generowania i wysyłania raportów na e-maila zgodnie z zadanym harmonogramem.
	7. Umożliwienie sortowania zdarzeń po każdym parametrze zdarzenia.
	8. Umożliwienie przeglądu zdarzeń oraz raportowanie przy pomocy przeglądarki www. oraz pliku csv, xls, preferowane jest indywidualne znaczony format raportu.
	9. Dostęp do raportów powinien być potwierdzany przy pomocy indywidualnych kont użytkowników.
	10. Umożliwienie generowanie raportów przy pomocy przeglądarki www, tworzonych na podstawie ruchu osób na danym przejściu oraz ruchu danego użytkownika na wielu przejściach.
	11. Umożliwienie generowania raportów dla grup pracowników np. firma.
	12. Umożliwienie generowania list z przepustkami będącymi w dyspozycji użytkowników i datą ich ważności. Umożliwienie zmiany daty ważności przepustki w sposób uproszczony bez konieczności usuwania i nadawania uprawnień z nową datą.
	13. Umożliwienie zaznaczenie w karcie użytkownika zdania przepustki po terminie ważności oraz generowania raportów z wykazem przepustek, które utraciły ważność i nie zostały zdane. Proszę o możliwość wykonania raportu. Jeżeli firma XX miała wydane 10 przepustek tymczasowych. Na koniec umowy zdała 8 przepustek. Chcemy wygenerować raport, kto z firmy XX nie oddał przepustki.
	14. Możliwość wykonania raportu z poziomu przeglądarki www dostępu do konkretnego pomieszczenia np. Serwerownia, F12 itp., Możliwość wykonania raportu z poziomu przeglądarki www mówiący o tym gdzie dany użytkownik wchodził.
	15. Autentykacji dostępu do raportów przy pomocy przeglądarki www
	16. Przy wykonywaniu raportów za pomocą przeglądarki www powinny działać wszystkie filtry
	17. System musi przechowywać wszystkie dane gości z informacjami o datach wizyt, osobach odwiedzanych oraz historii przejść z wszystkich wizyt.
	18. Możliwość filtrowania i sortowania w zakładce „Karty stałe”.
	19. Powinien umożliwiać generowanie automatycznych raportów z wybranych stref dostępu w określonym czasookresie i przesyłać te raporty drogą elektroniczną z automatu do określonych odbiorców.
3. Przepustki
	1. W systemie muszą być obsługiwane następujące rodzaje przepustek :
* Stałe
* Jednorazowe
* Gość
* Gość Zarządu
* Rezerwowe
* Serwisowe/Kontrahent
* Tymczasowe
* Alarmowe.
	1. Tymczasowe muszą być wykonane w wersji plastikowej jednokrotnego użytku ze zdjęciem , również z chipem umożliwiającym zapisanie na nim danych z wykonanego skanu dokumentu tożsamości, tzn. że po upływie określonego przez operatora czasu przepustka staje się nie aktywna i nie może być przydzielona ponownie innemu nowemu użytkownikowi (ale wszystkie dane użytkownika pozostają w bazie zbioru). Zdjęcie do przepustki ma być wykorzystane z skanu dokumentu lub danych przekazanych na elektronicznym nośniku informacji, tak aby dane każdego kto wchodzi na teren zakładu znajdowały się w zbiorze systemu i w razie konieczności późniejszego wydania przepustki stałej lub tymczasowej nie będzie trzeba po raz wtóry wprowadzać danych i zdjęć do systemu.
	2. Przepustki stałe wydawane przez dział NS ENEA Połaniec , w wersji plastikowej wielokrotnego użytku ze zdjęciem, z chipem umożliwiającym zapisanie na nim danych z wykonanego skanu dokumentu tożsamości lub danych przekazanych na elektronicznym nośniku informacji mają mieć możliwość dodania uprawnień do stref zamkniętych jak również uprawnienia do wjazdu pojazdem na teren elektrowni.
	3. Przepustki Jednorazowe wydawana na pracę w firmach zewnętrznych z chipem umożliwiającym zapisanie na nim danych z wykonanego skanu dokumentu tożsamości lub danych przekazanych na elektronicznym nośniku informacji. Wykonane ze zdjęciem w wersji plastikowej jednokrotnego użytku tzn. że po odbiciu przepustki przy wychodzeniu po upływie ustalonego czasu ważności staje się nie aktywna i nie może być przydzielona ponownie innemu nowemu użytkownikowi. Przy przepustkach jednorazowych do pracy, po 4 dniach (ma blokować wejście poprzez wydanie z czytnika sygnału dźwiękowego), ponieważ tyle pracownik dostaje czasu na załatwienie spraw z wydaniem dla niego przepustki.
	4. Przepustka GOŚĆ, GOŚĆ z POJAZDEM w wersji plastikowej wydawana jest bez wydruku zdjęcia również z chipem umożliwiającym zapisanie na nim zdjęcia i danych z wykonanego skanu dokumentu tożsamości, maksymalnie ważna na 24h jeżeli nie została odbita przy wychodzeniu, system samodzielnie musi odebrać uprawnienia takiej karcie. Anulowana przepustka będzie powodować alarm w postaci sygnału dźwiękowego na bramach przy próbie użycia karty.
	5. Przewidzieć możliwość wprowadzenia GOŚCIA do bazy ale bez wydawania przepustki np. PIP , NIK, UDT,ABW itp. służby te – nie obowiązuje odbijanie przepustek ale dane w bazie maja być zapisane
	6. Przepustka GOŚĆ Zarządu wydawana w wersji plastikowej bez wydruku zdjęcia również z chipem. Okres aktywności to maksymalnie 24h po upływie tego czasu jeżeli nie została odbita przy wychodzeniu, system musi samodzielnie odebrać uprawnienia takiej karcie i będzie powodować alarm w postaci sygnału dźwiękowego na bramach przy próbie użycia karty.
	7. Przepustka rezerwowa wydawana w wersji plastikowej bez wydruku zdjęcia również z chipem umożliwiającym zapisanie na nim zdjęcia i danych z wykonanego skanu dokumentu tożsamości na bramach w przypadku gdy pracownik Enea lub spółki zapomni swojej stałej lub tymczasowej przepustki. Okres aktywności to maksymalnie 24h po upływie tego czasu jeżeli nie została odbita przy wychodzeniu, system musi samodzielnie odebrać uprawnienia takiej karcie i będzie powodować alarm w postaci sygnału dźwiękowego na bramach przy próbie użycia karty.
	8. Przepustka serwisant wydawana w wersji plastikowej jednokrotnego użytku bez zdjęcia lub wielokrotnego użytku ze zdjęciem , również z chipem umożliwiającym zapisanie na nim danych z wykonanego skanu dokumentu tożsamości, na bramach w przypadku konieczności wjazdu na teren elektrowni serwisu do urządzeń, maszyn, pojazdów itp. celem wykonania prac remontowych, przeglądu itp. Jest ważna maksymalnie na 24h z możliwością przedłużenia do 96 godzin, w przypadku nie opuszczenia zakładu po 13 godzinach włącza się alarm wyświetla kolorem na ekranie monitora i podaje sygnał dźwiękowy. Jeżeli przy wyjeździe przepustka nie została odbita system samodzielnie po upływie oznaczonego czasu musi odebrać uprawnienia takiej karcie i będzie powodować alarm w postaci sygnału dźwiękowego na bramach przy próbie użycia karty. Przepustki te mają mieć możliwość dodania uprawnień do stref zamkniętych.
	9. Przepustka Tymczasowa wydawana w wersji plastikowej jednokrotnego lub wielokrotnego użytku ze zdjęciem , również z chipem umożliwiającym zapisanie na nim danych z wykonanego skanu dokumentu tożsamości lub danych przekazanych na elektronicznym nośniku informacji . Przeznaczona na wykonanie prac krótkookresowych. Przepustki te mają mieć możliwość dodania uprawnień do stref zamkniętych jak również uprawnienia do wjazdu pojazdem na teren Elektrowni. Czasookres ważności Przepustek tymczasowych powinien być ustawiany dowolnie natomiast system samoczynnie powinien zabrać ważność dla przepustki której czasookres ustawiony przez operatora upłynął i powodować alarm w postaci sygnału dźwiękowego na bramach przy próbie użycia karty.
	10. Przepustka Alarmowa wydawana przez Kierownika Biura Bezpieczeństwa w sytuacjach zagrożenia uprawnionym osobom wykonana w wersji plastikowej wielokrotnego użytku bez zdjęcia.
	11. Przepustka Samochodowa nadawana jako uprawnienie do wjazdu na teren elektrowni przez pracowników NS na dowolny okres, natomiast dla firm zewnętrznych nie mających stałej siedziby na terenie elektrowni - nie dłuższy niż rok. Mają informować strażnika 5dni przed utratą ważności pozwolenia – komunikatem na monitorze o upływie terminu jej ważności. Po upływie okresu ważności system sam powinien odebrać uprawnienia i powodować alarm w postaci sygnału dźwiękowego na bramach przy próbie użycia karty. Podczas wprowadzania numerów rejestracyjnych pojazdów należy wykluczyć możliwość używania spacji i jakichkolwiek znaków. Przy poszukiwaniu pojazdu nie trzeba zabierać ważności karcie żeby pobudziła alarm na bramach podczas próby użycia. System powinien pozwalać na przypisanie uprawnień karty do danej bramy oraz w dni powszednie po godzinie 1800, w święta i dni wolne od pracy kierować uprawnienia dla wszystkich kart samochodowych na bramę numer 3.
1. Procedury
	1. Brama nr 1
		1. Obsługuje ruch osobowy i pojazdów osobowych, obciążenie 90% ruch osobowy oraz 10% ruch pojazdów wyłącznie osobowych. Wydaje przepustki typu, GOŚĆ ZARZĄDU, GOŚĆ, GOŚĆ z POJAZDEM, REZERWOWA, SERWIS, TYMCZASOWA.
		2. Wprowadzenie danych interesantów, poprzez pobranie danych z dokumentów tożsamości typu: Dowód Osobisty, Prawo Jazdy, Paszport.
	2. Brama nr 2
		1. Obsługuje ruch osobowy i pojazdów do 3,5 tony, obciążenie osobowy 50% oraz 50% ruch pojazdów. Wprowadzenie danych poprzez pobranie danych z dokumentów typu Dowód Osobisty, Prawo Jazdy, Paszport. Obsługa samochodów wjeżdżających - kierowcy posiadający stałe przepustki kierowcy i na samochód podjeżdżają do bramy, odbija przepustkę, strażnik identyfikuje kierowcę na monitorze na którym wyświetlą się info. oraz zdjęcie kierowcy . (zgodność samochodu , osoby dokumentów), przeprowadza kontrolę i wpisuje z czym wjeżdża. Po czynnościach sprawdzających strażnik podnosi szlaban. Kierowca przejeżdża. Sytuacja wyjeżdżającego samochodu jest taka sama. Kierowca odbija przepustkę – strażnik sprawdza zgodność i czynności kontrolne pojazdów następnie strażnik podnosi szlaban.
	3. Brama nr 3
		1. Obsługuje ruch głównie pojazdów o dużym tonażu typu TIR. Ruch osobowy 30% oraz ruch pojazdów 70% w tym 100% ruchu samochodów ciężarowych . Wprowadzenie danych poprzez pobranie danych z dokumentów typu Dowód Osobisty, Prawo Jazdy, Paszport oraz dowodu rejestracyjnego (jeżeli to możliwe).
		2. Należy obsłużyć kombinację kiedy wjeżdża:
* Kierowca + 1 Samochód + naczepa
* Dwóch kierowców +1 Samochód +naczepa
* Pojazdy samobieżne typu dźwig, ładowarka itp. + operator.
	1. Obsługa samochodów wjeżdżających - kierowcy posiadający stałe przepustki na kierowcę i na samochód podjeżdżają do bramy, odbija przepustkę, strażnik identyfikuje kierowcę na monitorze na którym wyświetlą się info. oraz zdjęcie kierowcy . (zgodność samochodu , osoby dokumentów), przeprowadza kontrolę i wpisuje w specyfikację wwozową z czym wjeżdża. Po czynnościach sprawdzających strażnik potwierdza wwóz i podnosi szlaban. Kierowca przejeżdża. Sytuacja wyjeżdżającego samochodu jest taka sama. Kierowca odbija przepustkę – strażnik sprawdza zgodność i czynności kontrolne pojazdów następnie strażnik podnosi szlaban.
	2. Strażnik sprawdza deklarowany towar co wwozi i do kogo jedzie. System powinien posiadać funkcję możliwości wyznaczania trasy przejazdu do wybranego kontrahenta na terenie chronionym, oraz możliwość monitorowania trasy przejazdu pojazdu.
	3. 30% kierowców posiada przepustki stałe, 70% to dostawcy jednorazowi.
	4. W bazie ma być zdefiniowany rodzaj dostaw.
	5. System musi obsługiwać listy przewozowe, które strażnik pobiera od kierowcy i je archiwizuje.
	6. W bazie ma być Lista materiałów niebezpiecznych oraz lista osób uprawnionych do wystawiania przepustek materiałowych ( z wzorem podpisu) na wóz i wywóz materiałów niebezpiecznych. Niezbędna jest funkcja możliwości aktualizacji list osób przez osobę do tego uprawnioną w komórce NS.
	7. Ponadto w bazie powinna znaleźć się również lista osób upoważnionych do podpisywania pozostałych przepustek materiałowych na wywożone materiały ( z wzorem podpisu).
	8. Specyfikacja w wersji papierowej co wwozi jakie narzędzia – potem przy wyjeździe co wywozi- w referencji do przepustki wywozowej. Przy wyjeździe kierowca oddaje przepustkę strażnikowi.
	9. System ma obsłużyć samochody wywożące popiół lub gips, biomasę nie spełniającą wymaganych parametrów oraz inne materiały produkowane przez firmy mające swe siedziby na terenie Elektrowni, pośredniczące w obrocie itp.

W związku z dynamicznymi zmianami organizacyjnymi w EEP procedury mogą ulec zmianie i zostaną przedstawiane w ramach realizacji projektu.

1. Książka telefoniczna
	1. Moduł administracyjny
		1. Lokalna baza danych z użytkownikami (administratorami) na różnych poziomach uprawnień do ręcznej edycji danych, konfiguracji systemu
		2. Administratorzy z uprawnieniami do całości i odpowiednich zakładów –spółki z GK, spółki spoza GK
		3. Import z pliku csv z danymi ze spółek
	2. Moduł użytkowy – przeszukiwanie po wszystkich kolumnach po wyborze tak jak jest obecnie z kolumn Zakład, Dział, Stanowisko, oraz wpisaniu z palca dla pozostałych. Przy czym wybór z kolumny powoduje zawężenie przeszukiwania do ograniczenia, który ten wybór powoduje.
	3. Integracja z bazą oprogramowania do kontroli dostępu – informacja kto jest, kogo nie ma na terenie zakładu
	4. Integracja z SAP (lub AD) – informacja o pracowniku – imię nazwisko, nr tel., stacjonarnego… itd. – tak jak jest obecnie – zrzut w załączniku
	5. Integracja z oprogramowaniem z pkt 3, 4 offline lub przy pomocy bezpośredniego przesyłania (zaciągania) danych to tabel bazodanowych (jeśli to możliwe)
	6. Działanie – po standardowej przeglądarce – https
	7. Szata graficzna – zgodnie z wytycznymi biura promocji
2. Integracje
	1. System ma współpracować z system SAP HR,
	2. Książką telefoniczną oparta na www (PHP),
		1. Widok view\_user\_stat

Widok view\_user\_stat został stworzony w celu wystawienia go dla potrzeb zewnętrznych systemów, oprogramowania. Oparty jest on na zawartości tabeli users i zawarta jest w nim lista użytkowników wraz z ich aktualnym statusem przejścia.

* 1. Systemem awizacji dostaw biomasy.
		1. System KD musi zostać zintegrowany z systemem do awizacji Biomasy poprzez widoki z bazy systemu np.:

Widok view\_scan\_doc\_id



Rys. Diagram ERD widoku view\_scan\_doc\_id

Widok view\_scan\_doc\_id został stworzony w celu wystawienia go dla potrzeb zewnętrznych systemów, oprogramowania. Oparty jest on na zawartości tabeli temp i odzwierciedla dokumenty osobowe (dowody osobiste i paszporty) skanowane w zainstalowanych w systemie kontroli dostępu skanerach dokumentów. Widok ten jest interfejsem dla systemu firmy Wikpol.

* + 1. Widok view\_scan\_doc\_reg



Rys. Diagram ERD widoku view\_scan\_doc\_reg

Widok view\_scan\_doc\_reg został stworzony w celu wystawienia go dla potrzeb zewnętrznych systemów, oprogramowania. Oparty jest on na zawartości tabeli temp i odzwierciedla dokumenty pojazdów (dowody rejestracyjne) skanowane w zainstalowanych w systemie kontroli dostępu skanerach dokumentów. Widok ten jest interfejsem dla systemu firmy Wikpol.

* + 1. Widok view\_user\_stat2



Rys. 4.17 Diagram ERD widoku view\_user\_stat2

Widok view\_user\_stat2 został stworzony w celu wystawienia go dla potrzeb zewnętrznych systemów, oprogramowania. Oparty jest on na zawartości tabeli users i zawarta jest w nim lista użytkowników wraz z ich aktualnymi danymi. Widok ten jest interfejsem dla systemu firmy Wikpol. Skrypt tworzący widok view\_user\_stat2:

1. **System Monitoringu Wizyjnego CCTV**
2. Modernizacją systemu CCTV Technologicznego i Dozorowego na terenie Elektrowni Połaniec wraz z integracją w Systemie Zarządzania Bezpieczeństwem.

Zakres zadania obejmuje opracowanie projektu wykonawczego wraz z dostawą, montażem i uruchomieniem systemu CCTV wraz z platformą integrującą wyzwalającą alarmy.

* 1. Założenia dla systemu CCTV
		1. System CCTV technologiczny
* System CCTV technologiczny oparty jest na kamerach i rejestratorach analogowych różnych producentów.
	+ 1. System CCTV Dozorowy
* System CCTV dozorowy zbudowany jest na platformie VMS Mirasys Enterprise. Do zarządzania służy System Menager Enterprise w wersji 9.2.0.1 , natomiast do wyświetlania i eksportowania obrazu w czasie rzeczywistym oraz do odtwarzania zapisanego wideo służy program użytkownika Spotter.
	+ 1. System CCTV zbudowany jest na serwerze wirtualnym skonfigurowanym z macierzą dyskową Synology ( zlokalizowane w serwerowni ) oraz stacji roboczej z kartą grafiki Matrox na cztery monitory.
		2. Serwer, stacje robocze działają w przygotowanym do tego celu dedykowanym VLanie .
		3. Oprócz powyższego systemu CCTV są jeszcze 2 rejestratory 4 kanałowe na których są wpięte kamery 4 szt. kamer analogowych stacjonarnych, oraz drugi rejestrator 4 kanałowy na którym również wpięte są 4 szt. kamer analogowych stacjonarnych.
1. Podsumowanie

Razem – 196 kamer jak również tyle samo licencji SMA kanałów do wykupienia,

Do wymiany cały system zainstalowany na obiektach technologicznych z analogowego na IP

1. Opis Warunków zamówienia – System CCTV w Enea Elektrowni Połaniec
	1. Wykonawca ma obowiązek zaprojektować, dostarczyć oraz wdrożyć System Kontroli Dozoru telewizji CCTV wskazany przez Zamawiającego wraz z platformą ingerującą. Zgodny z poniżej określonymi wytycznymi. Wskazania Zamawiającego należy traktować, jako priorytetowe. System CCTV musi posiadać minimum 2 letnie wsparcie serwisowe i 5 letnie wsparcie po serwisowe,
	2. Instalacja winna zawierać dostawę, montaż oraz instalację: wykonanie niezbędnego okablowania wraz z punktami dystrybucyjnymi IT, modernizację serwera do nadzoru wizyjnego, dedykowanej macierzy dyskowej, a także dostawę oraz montaż kamer IP CCTV, obrotowe (minimum 2Mpix z doświetleniem lub stacjonarne 4Mpix z doświetleniem) w punktach (propozycje od wykonawcy). System Mirasys winien zawierać funkcję licencję VCA dla wskazanych kamer (liczba kamer do VCA 100). Dostarczony system musi posiadać integracje z systemem platformy integrującej potwierdzoną przez producenta tego systemu. W chwili zdarzenia powiadamiania operatora w momencie wykrycia ruchu w obrazie z kamery na dedykowanym komputerze z zainstalowaną aplikacją platformy integrującej
2. Specyfikacja Systemu CCTV
	1. System CCTV Mirasys
* Wykupienie dodatkowych licencji Mirasys - minimum 200 kanałów,
* Wykupienie licencji VCA – minimum 100 kanałów,
* Zakup dodatkowej dedykowanej macierzy, przechowywania materiału minimum 40 dni,
* Zakup dodatkowego zestawu komputerowego z obsługą platformy integrującej z aplikacją wyzwalającą alarmy,
* Platforma z aplikacja integrująca systemy z wyzwalaniem alarmowym.
	1. Dwa stanowiska dla stacji roboczej ( *workstation ),*
	+ Procesor minimum, Intel ® Xeon® CPU E-3-1245 V2@3,40 GHz,
	+ Pamięć RAM minimum, 8 GB,
	+ Płyta główna serwerowa lub do pracy ciągłej,
	+ Dysk SSD minimum, 10GB
	+ Karta graficzna z wyjściami na cztery i osiem monitorów,
	+ Osiem monitorów do pracy ciągłej minimum 55”,
	+ Cztery monitory do pracy ciągłej minimum 55”,
	+ Stelaż do montażu monitorów,
	+ Sterownik-klawiatura do kamer szybkoobrotowych PTZ IP, 2 sztuki,
	1. Wymiana kamer analogowych na IP
	+ Około 70 szt. kamer obrotowych analogowych na IP, minimum 2 Mpix z doświetleniem powyżej 100 metrów,
	+ Około 134 szt. kamer stałych analogowych na IP, minimum 4 Mpix z doświetleniem powyżej 30 metrów,
	+ Około 10 szt. kamer IP na IP, minimum 4 Mpix stacjonarne, z doświetleniem powyżej 30 metrów,
	1. Integracja
	+ System kontroli dostępu, system CCTV, system awizacji – zdarzenia alarmowe mają być wyświetlane na komputerze z obsługą platformy integrującej z aplikacją wyzwalającą alarmy,
1. **System Awizacji**

Awizacja Ruchu Towarowego 2 (ART2) będzie głównym narzędziem operacyjnym i platformą integrującą w zakresie procesów dostaw i wywozu transportem kołowym i kolejowym z Elektrowni Połaniec.

ART 2 zostanie zbudowany w oparciu o platformę techniczną zarządzania procesami biznesowymi klasy BPMS umożliwiając Zamawiającemu adaptację systemu do zmian w ślad za zmianami w procesach biznesowych.

System będzie realizował usługi integracyjne back office w zakresie zasilania i odczytu danych podstawowych, dotyczących dostaw i wywozów, systemów użytkowanych przez Elektrownię,

a w szczególności z systemy wagowe MicroWAG, GSW i SCALEX DSRS, systemem poboru prób LabSys, systemem zarządzania zasobami przedsiębiorstwa SAP, systemem Kontroli Dostępu oraz umożliwi w przyszłości integrację z innymi systemami.

System będzie umożliwiał tworzenie harmonogramu dostaw i wywozu wszystkich asortymentów dla Enea Elektrownia Połaniec.

System będzie umożliwiał awizowanie dostaw i wywozu przez kontrahentów zewnętrznych w definiowanych horyzontach czasowych.

Ponadto system ma spełniać:

1. Wymagane warunki wdrożenia
	1. Zamawiający wymaga wdrożenia rozwiązania w architekturze klient serwer, w które hostowane będzie na serwerach wskazanych przez Zamawiającego przy zachowaniu określonych przez Zamawiającego wymagań bezpieczeństwa.
	2. Zamawiający wymaga analizy obszaru dziedzinowego logistyki w Enea Elektrownia Połaniec w zakresie awizowania dostaw i wywozów środkami transportu kołowego i kolejowego
	3. Zamawiający wymaga wdrożenia równoległego do obecnie użytkowanego systemu Awizacji
	4. Zamawiający wymaga opracowania dokumentacji etapu analizy – modelu biznesowego opisującego przepływ danych, użytkowników zaangażowanych w przepływ, role i zakresy odpowiedzialności użytkowników i systemów w notacjach BPMN/BPEL/UML
	5. W przypadku opracowanie Systemu od podstaw Zamawiający wymaga prowadzenia prac w metodologii RAD metoda etapowa na podstawie analizy ID A04 i integracji Systemu z istniejącymi Systemami i aplikacjami Zamawiającego, w szczególności: SAP, GSW, microWAG, LabSys, SCALEX DSRS, Qdata, KD oraz wskazanie możliwości integracji przez dostarczenie wraz z dokumentacją opisującą (opis metod) - specjalistycznego API umożliwiającego integracje bez zmian programistycznych w dostarczonym oprogramowaniu w szczególności w zakresie zasilania danymi wprowadzanymi ręcznie. Integracja z systemem CEPiK.
	6. W przypadku dostarczenia istniejącego już Systemu wdrożonego w innych przedsiębiorstwach Zamawiający wymaga dostarczenia referencji z wdrożeń oraz skonfigurowania Systemu pod wymagania Zamawiającego zgodnie z wynikiem analizy ID A04 wraz z integracją z istniejącymi systemami, aplikacjami, w szczególności: SAP, GSW, microWAG, LabSys, SCALEX DSRS, Qdata, KD oraz wskazanie możliwości integracji przez dostarczenie wraz z dokumentacją opisującą (opis metod) - specjalistycznego API umożliwiającego integracje bez zmian programistycznych w dostarczonym oprogramowaniu w szczególności w zakresie zasilania danymi wprowadzanymi ręcznie. Integracja z systemem CEPiK.
	7. Zamawiający wymaga opracowania harmonogramu wdrożeniowego uwzględniającego scenariusze testowe wraz z ich realizacją dla kolejnych wersji przedmiotu zamówienia
	8. Zamawiający wymaga opracowania scenariuszy testowych dla wszystkich etapów harmonogramu w których powstaje System.
	9. Zamawiający wymaga przygotowania wersji testowej Systemu, a po testach akceptacyjnych wersji produkcyjnej Systemu, na środowisku wykorzystującym infrastrukturę Zamawiającego w terminach wskazanym przez Zamawiającego w czasie trwania umowy.
	10. Zamawiający wymaga oszacowania kosztów utrzymania systemu po upływie okresu gwarancji w ramach umowy serwisowej/licencyjnej oraz okresu na jaki może być ona zawarta.
	11. Zamawiający wymaga objęcia systemu usługą asysty technicznej i konserwacji (ATiK).
	12. Zamawiający wymaga licencjonowania systemu bez ograniczeń na liczbę instalacji systemu, użytkowników, komputerów, serwerów, transakcji, ilości danych itp.
	13. Zamawiający wymaga wdrożenia systemu w oparciu o platformę BPMS
	14. Okna dialogowe systemu powinny być dostępne w wariantach językowych: polski, angielski, rosyjski, niemiecki, ukraiński. Jeżeli aplikacja będzie wykonana w technologii WWW to pliki z literałami powinny mieć postać zbliżoną do resx by bez zmian programistycznych była możliwość zmian literałów.
2. Wymagania dotyczące dokumentacji
	1. Wykonawca w ramach przedmiotu zamówienia przygotuje i dostarczy koncepcję techniczną i biznesową rozwiązania oraz instrukcje eksploatacyjne administratora i użytkowników zarówno wewnętrznych jak i zewnętrznych (Kontrahenci)
	2. Dokumentacja będzie dostarczana Zamawiającemu przez Wykonawcę w trakcie realizacji Umowy, w terminach określonych Harmonogramem Wdrożenia, odpowiednio do postępu prac i będzie podlegała opiniowaniu i akceptacji.
	3. Zamawiający wymaga dokumentacji sporządzonej w języku polskim.
	4. Zamawiający wymaga dokumentacji w formie edytowalnej w formacie bpmn, bpmn.di , .docx , .xls, .vsdx itp.
3. Techniczne warunki wdrożenia
	1. Wszystkie strony wykorzystywane w ramach Systemu muszą zostać zabezpieczone certyfikatem bezpieczeństwa SSL.
	2. System musi zabezpieczać integralność przetwarzanych informacji.
	3. System musi wspierać integrację z AD/IdM w ramach SSO.
	4. System musi zapewnić możliwość zarządzania prawami dostępu do Systemu w oparciu o mechanizm ról (RBAC), obsługę ograniczeń dla kont użytkowników uprawnionych.
	5. System musi gromadzić i archiwizować logi operacji mających na celu zapewnienia rozliczalności Użytkowników Uprawnionych:
* Logi związane ze zmianą uprawnień (kto, kiedy, kogo dotyczy, jakie uprawnienia).
* Logi związane ze zmianą konfiguracji Systemu (kto, kiedy, co, opcjonalnie wartość).
* Logi związane z obsługą Systemu przez Użytkowników Uprawnionych (kto, kiedy, id procesu, rodzaj operacji, opcjonalnie wartości).
	1. Wykonawca wskaże miejsce i sposób przechowywania/gromadzenia logów, udostępni do wglądu Zamawiającego i opisze w dokumentacji sposób ich odczytu (weryfikacji).
	2. Dostęp do Systemu musi być możliwy we wszystkich wymienionych przeglądarkach internetowych: MS Edge, Firefox, Chrome, Opera ze wsparciem wstecznym dwóch wersji.
	3. Dostęp do System dla użytkowników zewnętrznych (Kontrahenci) musi umożliwiać uwierzytelnianie dwuskładnikowe
1. Infrastruktura Zamawiającego
	1. Na potrzeby wdrożenia w środowisku Zamawiającego, Zamawiający zapewni własną infrastrukturę informatyczną obejmującą cały obszar wdrożenia Systemu. Środowisko serwerowe i bazodanowe Zamawiającego jest zlokalizowane w Centrach Przetwarzania Danych i jest otwarte pod względem skalowalności zasobów (mocy obliczeniowej, pamięci operacyjnej, przestrzeni dyskowej). Instalacja i konfiguracja serwerów, systemów operacyjnych i instancji baz danych zostaną przeprowadzone przez Zamawiającego w uzgodnieniu z Wykonawcą oraz w oparciu o Koncepcję Techniczną dostarczoną przez Wykonawcę.
	2. Zamawiający udostępni platformę sprzętową z oprogramowaniem wirtualizacyjnym w środowisku VMware vSphere na serwerach z procesorami INTEL.
	3. Dopuszczalne systemy operacyjne serwerów dla tego środowiska :
	* system operacyjny Windows Serwer 2016 64-bit
	* system operacyjny Linux:
	* Red Hat 64-bit
	* SLES 64-bit
	* Oracle Entrprice Linux
	* Centos
	1. Zamawiający wymaga aby System działał na najnowszych wersjach systemów operacyjnych wymienionych powyżej. Zastosowanie innych wersji wymaga uzgodnienia z Zamawiającym.
	2. Wykonawca w ramach Koncepcji Technicznej dostarczy zestawienie serwerów, które będą wykorzystane przez System. Wykaz będzie zawierał informacje o wydajności (moc obliczeniowa, pamięć operacyjna, obszar dyskowy) i wymaganiach konfiguracji ze wskazanym systemem operacyjnym, na podstawie którego Zamawiający przygotuje i skonfiguruje serwery dla Systemu.
	3. Licencje niezbędne do uruchomienia i udostępnienia środowiska serwerowego (systemy operacyjne, wirtualizator, bazy danych) na potrzeby Systemu zostaną dostarczone przez Zamawiającego. Wykonawca dostarczy pozostałe licencje, które będą wymagane do prawidłowego działania Systemu.
	4. Zamawiający udostępni bazy danych:
* ORACLE w wersji 19c Enterprise Edition
* Microsoft MSSQL wersja 2014 Standard
* MySQL
	1. Zamawiający dysponuje systemem backupu obejmującym swoim działaniem posiadaną infrastrukturę serwerową i bazodanową, w tym zasoby które będą udostępnione dla Systemu.
	2. Zamawiający wymaga, by każdy istotny element oprogramowania wchodzącego w skład Systemu objętego umowami licencyjnymi innymi, niż Open Source lub freeware:
	+ pochodził od uznanych wytwórców, o światowym zasięgu,
	+ był realizowany w nowoczesnej i rozwojowej technologii,
	+ był wspierany przez możliwie licznych liczących się integratorów i innych usługodawców działających na terenie Polski i Unii Europejskiej,
	+ nie był objęty prawami wyłącznymi Wykonawcy ani żadnej spółki powiązanej kapitałowo z Wykonawcą (w tym z konsorcjantem).
	1. Zamawiający wymaga, by każdy istotny element oprogramowania wchodzącego w skład Systemu objętego umowami licencyjnymi Open Source lub freeware:
	+ był realizowany w nowoczesnej i rozwojowej technologii,
	+ nie był wskazany przez wytwórcę, jako produkt, którego dalszy rozwój lub wsparcie będą wstrzymane w terminie krótszym niż 5 lat od daty oferowanego zakończenia realizacji umowy.
	1. Na potrzebę dostępu Wykonawcy do prowadzenia prac zdalnie zostanie zestawiony tunel VPN site-to-site pomiędzy Wykonawcą, a Zamawiającym. W tym celu Wykonawca musi zapewnić w swojej lokalizacji i na swój koszt urządzenie pozwalające na konfigurowanie tunelu VPN w technologii IPSec według parametrów podanych przez Zamawiającego po podpisaniu Umowy.
1. Wymagania bezpieczeństwa
	1. System i wszystkie jego komponenty oraz mechanizmy zabezpieczeń zapewniają monitorowane parametrów związanych z bezpieczeństwem poprzez wysyłanie logów systemowych do systemu SIEM Zamawiającego.
	2. Kontrola i eliminacja błędów programistycznych
	* na etapie opracowywania kolejnych wersji oprogramowania dokonywana jest automatyczna kontrola kodu przez Wykonawcę,
	* Zamawiający jest uprawniony do dowolnego przeprowadzania testów bezpieczeństwa aplikacji/systemu oraz infrastruktury technicznej utrzymywanej na potrzeby systemu.. W przypadku zidentyfikowania błędów bezpieczeństwa, w oprogramowaniu i konfiguracji dostarczonej przez Wykonawcę, Wykonawca niezwłocznie je poprawi bez pobierania dodatkowych opłat.
	1. Komunikacja pomiędzy wszelkimi elementami Systemu powinna być zabezpieczona kryptograficznie.
	2. Wykonawca zapewnia uprawnienia na najniższym wymaganym do utrzymania i rozwoju systemu poziomie i tylko dla wykwalifikowanego personelu Wykonawcy. Pozostali pracownicy Wykonawcy nie mają dostępu do sieci i infrastruktury IT dedykowanej dla ENEA Elektrownia Połaniec S.A.. Praca serwisów zewnętrznych (dostawców sprzętu i rozwiązań IT) możliwa tylko pod stałą kontrolą uprawnionego personelu Wykonawcy. Wykonawca prowadzi rejestr takich prac i na wniosek Zamawiającego umożliwi wgląd w ten rejestr.
	3. Wszelkie komponenty sprzętowe i software’owe stosowane przez Wykonawcę na potrzeby świadczenia usługi posiadają Wsparcie producenta i mają na bieżąco instalowane poprawki bezpieczeństwa.
	4. System zapewnia granulację uprawnień (podział na Grupy), zgodnie z potrzebami biznesowymi Enea Elektrownia Połaniec S.A. przy zachowaniu zasady przydzielania minimalnych potrzebnych uprawnień.
	5. System będzie zintegrowany z systemem AD Grupy ENEA.
	6. Wykonawca musi zapewnić rozwój systemu zgodnie z powstającymi wymaganiami Zamawiającego uwarunkowanymi zmianami prawnymi.
	7. Wykonawca musi zapewnić rozwój systemu zgodnie z powstającymi wymaganiami Zamawiającego uwarunkowanymi powstawaniem nowych zagrożeń cybernetycznych oraz nowych wymagań bezpieczeństwa Zamawiającego.
2. Wymagania funkcjonalne
	1. awizacja dostaw i wywozów wszystkich asortymentów realizowanych w Enea Elektrownia Połaniec S.A. transportem samochodowym i kolejowym
	2. dodawanie i parametryzacja bram(przepustowość, kierunek ruchu, obsługiwane asortymenty)
	3. algorytm podziału doby na sloty czasowe(awizacje) spełniający wszystkie twarde ograniczenia
	4. dokumentacja algorytmu(opis działania) w systemie
	5. GUI(formatki) do ręcznego wprowadzania ograniczeń
	6. moduł do tworzenia raportów z możliwością eksportu do Excel
	7. wyświetlanie zbiorczej informacji o zbliżających się dostawach/wywozach (awizacje) oraz poruszających się po terenie elektrowni dostawach/wywozach (informacje z systemów zintegrowanych)
	8. filtrowanie wyświetlanych awizacji wedle parametrów określonych przez użytkownika
	9. import/export harmonogramów asortymentów z poza SAP
	10. panel podglądu wszystkich dostaw i wywozów w bieżącej dekadzie wraz z możliwością zwiększania zakresu dat
3. Funkcjonalności dla użytkowników wewnętrznych
	1. tworzenie i usuwanie zapotrzebowań na asortymenty
	2. wyświetlanie zapotrzebowań wraz z filtrowaniem
	3. tworzenie i usuwanie dyspozycji dobowych
	4. wyświetlanie dyspozycji dobowych wraz z filtrowaniem
	5. dodawanie i usuwanie awizacji
	6. powielanie awizacji
	7. wyświetlanie awizacji w formie tabelarycznej wraz z filtrowaniem
	8. wyświetlanie awizacji w formie kalendarza (dobowy/tygodniowy) z granulacją wynikającą z podziału doby na sloty wraz z filtrowaniem oraz wolnymi slotami
	9. tworzenie harmonogramów dostaw i wywozów z podziałem na asortymenty i kontrahentów
	10. awaryjne sloty awizacyjne widoczne tylko dla Biura Awizacji
	11. informacja o odbyciu szkolenia (do weryfikacji czy nie powinno to być w KD)
4. Funkcjonalności dla użytkowników zewnętrznych
	1. wprowadzanie, edycja i wyświetlanie danych podstawowych kierowców (poprzez wywołanie metody do systemu KD)
	2. wprowadzanie, edycja i wyświetlanie danych podstawowych pojazdów (poprzez wywołanie metody do systemu KD)
	3. dodawanie i usuwanie awizacji
	4. powielanie awizacji
	5. wyświetlanie awizacji w formie tabelarycznej wraz z filtrowaniem
	6. wyświetlanie awizacji w formie kalendarza (dobowy/tygodniowy) z granulacją wynikającą z podziału doby na sloty wraz z filtrowaniem oraz wolnymi slotami
	7. panel nawigacyjny wyświetlający informację o aktualnie zaawizowanym wolumenie z zamówienia, aktualnie dostarczonym, itp..: w celu ułatwienia planowania awizacji
	8. udostępnianie i workflow akceptacji harmonogramów
	9. informacja o czasie obsługi na bramie/ilości aut w kolejce/przybyłych transportach
5. Ograniczenia do algorytmu F03
	1. Przepustowość bram
	2. Przepustowość asortymentów
	3. Wolumen asortymentu z zamówień
	4. Pula awizacji dla kontrahenta wynikająca z wolumenu umowy
	5. Zapotrzebowanie na asortyment (10 dni)
	6. Dyspozycja dobowa na asortyment (1 doba)
	7. Równomierne obciążenie pór dnia
	8. Sloty czasowe dla dostawców równomiernie na dobę, np. dostawca 'x' w godzinnym przedziale czasowym może mieć tylko 1 slot
	9. Informacja zwrotna z systemów wagowych o rzeczywistym wolumenie zrealizowanej dostawy zmniejsza dostępny do awizowania wolumen z zamówienia
	10. Anulowanie awizacji w przypadku braku wolumenu na skutek nadmiarowych dostaw rzeczywistych w ramach poprzednich awizacji z zamówienia wraz z powiadamianiem email kontrahenta
	11. Strefy w ramach doby w ramach których kontrahent może mieć określoną liczbę awizacji
6. **Serwis**
7. Czas reakcji na awarię 2 godziny
8. Napraw w reżimie 24 godziny 7 dni w tygodniu
9. Przewidywana liczba czytników 140 +/- 10 szt
10. W koszty serwisu wchodzą także koszty aktualizacji systemu