Grupa LOTOS S.A.	**SPECYFIKACJA TECHNICZNA**	Spec. Nr. 3870
	Kontrola dostępu	

Spis treści

1 Przedmiot specyfikacji 2
2 Zakres obowiązywania 2
2.1 Odstępstwa 2
2.2 Wyłączenia 2
3 Hierarchia dokumentów 2
4 Definicje 2
4.1 Podstawowe pojęcia 2
4.2 Oznaczenia 3
4.3 Warunki otoczenia 3
4.4 Dane elektryczne 3
5 Opis 3
5.1 Zasada działania 4
5.2 Wymagania systemowe 4
5.3 Elementy składowe systemu 5
5.4 Urządzenia mechaniczne blokujące 8
5.5 Terminale rejestracji ruchu pojazdów 9
5.6 Elektroniczny system ewidencji kluczy 9
5.7 Okablowanie sygnałowe 10
5.8 Oprogramowanie 10
5.9 Zasilanie elektryczne 11
5.10 Znakowanie 11
5.11 Usługi 11
5.12 Kable, przewody, pozycje pomocnicze 12
5.13 Dokumentacja 12
6 Dokumenty związane 13
7 Normy i przepisy 13
7.1 Przepisy 13
7.2 Normy 13
8 Załączniki 14
9 Karta zmian 15

Opracowanie jest własnością Grupy LOTOS SA i nie może być reprodukowane ani udostępniane osobom trzecim w całości lub w części bez pisemnej zgody Grupy LOTOS SA

1 Przedmiot specyfikacji

Niniejsza specyfikacja zastosowana w połączeniu z innymi specyfikacjami technicznymi Grupy LOTOS S.A. (GLSA) ustala minimalne wymagania odnośnie projektowania i wykonania systemu kontroli dostępu.

2 Zakres obowiązywania

Specyfikacja ta ma zastosowanie przy sporządzaniu zapytań ofertowych i kontraktów dla nowo planowanych przedsięwzięć inwestycyjnych i modernizacyjnych Grupy LOTOS S.A..
Stanowi ona również podstawę do opracowania szczegółowych specyfikacji i zapytań ofertowych dla dostaw indywidualnych i pakietowych.

2.1 Odstępstwa

Wszelkie odstępstwa od niniejszej specyfikacji oraz specyfikacji, norm i dokumentów związanych łącznie z propozycjami, które wg oferenta urządzeń lub prac pokazują bardziej ekonomiczne i/lub lepsze technicznie rozwiązania muszą być przedstawione na piśmie do sprawdzenia i zatwierdzenia przez Grupę LOTOS S.A. Niedopuszczalne są żadne odstępstwa niezatwierdzone na piśmie przez Grupę LOTOS S.A.
Oferent winien zgłosić w formie pisemnej każdą niejasność w tej lub innej specyfikacji Grupy LOTOS S.A. lub niezgodność z przywołanymi dokumentami/normami i uzyskać pisemne wyjaśnienie Grupy Lotos S. A..

2.2 Wyłączenia

Niniejsza specyfikacja nie obejmuje:

- Wymagań dla systemu rozdziału zasilania niskiego napięcia,
- Wymagań dotyczących parametrów kabli,
- Wymagań odnośnie prowadzenia i układania kabli.

Wyżej wymienione wyłączenia stanowią przedmiot odrębnych specyfikacji wymienionych w pkt. 5.

3 Hierarchia dokumentów

W przypadku wystąpienia rozbieżności pomiędzy wymaganiami poszczególnych dokumentów należy zachować następującą hierarchię ważności:

- Aktualne polskie przepisy prawne
- Zapisy kontraktu i inne pisemnie uzgodnione wymagania GLSA
- Arkusze danych zatwierdzone przez Grupę LOTOS S.A.
- Niniejsza specyfikacja
- Inne specyfikacje
- Rysunki i inne dokumenty
- Normy

4 Definicje

4.1 Podstawowe pojęcia

Odbezpieczony w razie awarii (Fail-Safe) - blokada która przyjmuje domyślnie położenie „odblokowana” w przypadku braku zasilania. Wymaga zasilania aby przejść do położenia „zablokowana”.

Zabezpieczony w razie awarii (Fail-Secure) - blokada która przyjmuje domyślnie położenie „zablokowana" w przypadku braku zasilania. Wymaga zasilania aby przejść do położenia „odblokowana".

Blokada sprzężona - para lub grupa oddzielnych drzwi wyposażonych w system sterowania uniemożliwiający jednoczesne otwarcie więcej niż jednych drzwi jednocześnie.

Zbliżeniowy - w kategoriach kontroli dostępu, termin „zbliżeniowy" odnosi się do wprowadzenia karty dostępowej w obręb pola częstotliwości radiowej (RF) czytnika, bez konieczności faktycznego fizycznego jej zetknięcia z samym czujnikiem.

Wiegand - protokół komunikacyjny przyjęty jako standard przemysłowy w wytwarzaniu urządzeń kontroli dostępu.

Przełącznik przeciwsabotażowy - przełącznik stosowany w sterownikach, zamkach, elektro-zaczepach. Zabezpiecza przed otwieraniem obudowy urządzenia i/lub odrywaniem od podstawy.

4.2 Oznaczenia

GLSA – Grupa Lotos S. A.

KiA – Branża automatyki

SKD - system kontroli dostępu

RCP - system rejestracji czasu pracy

SEK - system ewidencji kluczy

4.3 Warunki otoczenia

Warunki otoczenia charakterystyczne dla rafinerii Grupy LOTOS S.A. (atmosfera morska, agresywna przemysłowa, chemiczna i pyłowa).

Temperatura zewnętrzna:

▪ Projektowa maksymalna	36ºC
▪ Projektowa minimalna	–25ºC
Wilgotność minimalna średniomiesięczna	70%
Wilgotność maksymalna średniomiesięczna	90%
Wysokość nad poziomem morza	1m
Prędkość wiatru	26m/s
Opady śniegu	290mm

4.4 Dane elektryczne

Źródło zasilania dostępne na miejscu budowy:

Częstotliwość	50 Hz
Niskie napięcie	230 VAC TN-S

5 Opis

5.1 Zasada działania

5.1.1 Podstawowe zasady

System kontroli dostępu należy zaprojektować w sposób zapewniający kontrolę obszaru zdefiniowanego w ogólnych warunkach kontraktowych za pomocą środków technicznych. Zaprojektowany system powinien spełniać wymogi klasy dostępu B zaś klasy rozpoznania 2 lub 3 (uzgodnić ze przedstawicielem Biura bezpieczeństwa i ochrony GLSA) zdefiniowane w załączonych normach.

5.1.2 Architektura

System kontroli dostępu powinien mieć samodzielną strukturę rozproszoną, składającą się z:

- Serwera kontroli dostępu,
- Stacji operatorskich systemu kontroli dostępu,
- Kontrolerów obszaru,
- Kontrolerów drzwiowych,
- Kart zbliżeniowych i czytników zbliżeniowych,
- Czytników biometrycznych (jeżeli są wymagane),
- Elektrozaczepów drzwiowych,
- Zwor elektromagnetycznych,
- Przycisków wyjścia.
- Przycisków ewakuacyjnych

W skład zakładowego SKD wchodzą lokalne stacje operatorskie będące stanowiskami wydawania przepustek, wyposażone w jednostkę PC, monitor i odpowiednią drukarkę do kart plastikowych (np. termosublimacyjną) lub inną. Takie stacje przewidziane są w recepcjach głównych budynków administracyjnych mających wejścia na zewnątrz zakładu oraz na posterunkach służby ochrony na bramach.

Serwer kontroli dostępu, kontrolery obszaru i kontrolery drzwiowe muszą być połączone poprzez magistralę komunikacyjną lub sieć komputerową. Funkcjonalność magistrali lub sieci komputerowej musi być sprawdzana automatycznie.

Serwer kontroli dostępu powinien spełniać wymagania dla komputerów w systemach automatyki zawarte w standardzie 3620.

Czytniki zbliżeniowe kart, elektrozaczepy drzwiowe, zwory elektromagnetyczne i przyciski drzwiowe muszą być połączone bezpośrednio z kontrolerami drzwiowymi. Cały system powinien opierać się na kontrolerach cyfrowych w pełni programowalnych.

Kontroler obszaru powinien umożliwiać podłączenie wymaganych interfejsów do współpracy z:

- Systemem telewizji przemysłowej,
- Systemem alarmu przeciwwłamaniowego,
- Systemem sygnalizacji pożaru,
- Systemem zarządzania budynkiem,

5.2 Wymagania systemowe

5.2.1 Zagadnienia ogólne

Proponowane wyposażenie musi być zaprojektowane w celu zminimalizowania skutków wynikających z awarii samego urządzenia lub urządzenia podłączonego do systemu. Dostawca powinien przedstawić wszystkie informacje niezbędne do oceny niezawodności systemu w proponowanej przezeń konfiguracji. Identyfikacja i lokalizacja usterek w systemie musi być w największym możliwym stopniu zautomatyzowana. Dodatkowo musi istnieć możliwość wysłania sygnału alarmowego do urządzenia zewnętrznego. Wszystkie metody sterowania, procedury obsługi i konserwacji muszą być zaprojektowane w sposób umożliwiający łatwą konserwację i obsługę.

Proponowany system należy zaprojektować tak, aby zminimalizować konieczny zapas utrzymywanych części zamiennych. Na tyle, na ile istnieje konfiguracja rezerwowa, musi być możliwa wymiana modułów systemu bez przerywania działania samego systemu.

5.2.2 Wymagania funkcjonalne

Aby zagwarantować maksymalną ochronę i bezpieczeństwo, system ten powinien zapisywać wszystkie wymienione poniżej zdarzenia:

- upoważnione wejście do strefy zabezpieczanej,
- upoważnione wyjście ze strefy zabezpieczanej,
- próba nieupoważnionego wejścia,
- wymuszenie wejścia,
- sabotaż urządzeń systemu,
- utrata komunikacji z systemem,
- brak dostępnego źródła zasilania.

System powinien kontrolować i rejestrować przemieszczanie się osób przez obszar poprzez przypisywanie indywidualnych zezwoleń dla każdego przejścia, z zastosowaniem stref czasowych w celu ochrony przejścia, oraz kontrolować czas przebywania wewnątrz tego obszaru.

Opuszczanie strefy (otwarcie drzwi od wewnątrz strefy) musi być realizowane za pomocą klamki drzwiowej lub przycisku. Kontrolowane przez system drzwi muszą być wyposażone w automatyczne urządzenia zamykające.

System powinien posiadać konfigurację modułową i działać na podstawie kart identyfikacyjnych. System powinien posiadać również możliwość wymiany danych dla potrzeb modułu rejestracji czasu pracy, wykorzystując czytniki jako czytniki RCP. Użytkownik otwierając przejście kontrolowane na podstawie zadanej metodyki (np. pierwszy i ostatni raz w ciągu doby) generuje sygnał, który powinien być wykorzystywany przy rejestracji czasu pracy.

Projektowany system kontroli dostępu powinien wykorzystywać do transmisji danych wydzieloną sieć LAN dedykowaną dla komunikacji pracujących już w GLSA urządzeń kontroli dostępu.

5.3 Elementy składowe systemu

5.3.1 Kontroler obszaru

Kontroler obszaru powinien łączyć serwer dostępu oraz sieć kontrolerów drzwiowych. Kontroler obszaru powinien wysyłać zapytania do kontrolerów drzwiowych i sprawdzać dane w miarę ich wprowadzania, wykorzystując przechowywane wewnętrznie tabele uprawnień w celu monitorowania i kontroli dostępu na całym obiekcie. Jeden kontroler obszaru powinien obsługiwać wszystkie kontrolery drzwiowe zlokalizowane na obiekcie. Kontroler obszaru powinien być wyposażony we wbudowany zasilacz bezprzerwowy (UPS), który powinien gwarantować 4-godzinne działanie na zasilaniu rezerwowym. Połączenie do serwera dostępu należy zrealizować z zastosowaniem protokołu RS232/485, Ethernet lub TokenRing.

Kontroler obszaru powinien być wyposażony w:

- Procesor o wysokiej wydajności,
- Pamięć z podtrzymaniem bateryjnym,
- Dwa oddzielne kanały komunikacji szeregowej do szybkiego zapytywania,
- Obsługę radiowego odbiornika czasu,
- Złącze monitora do diagnostyki systemu.

5.3.2 Kontroler drzwiowy

Kontroler drzwiowy powinien nadzorować bezpośrednio zbliżeniowe czytniki kart, elektrozaczepy drzwiowe, zamki i przyciski otwierania drzwi, przyjmując, analizując i przekazując komunikaty umożliwiające dostęp.

Każdy kontroler powinien cechować się co najmniej następującymi funkcjami:

- 2 wyjścia zamków drzwiowych,
- 4 wyjścia LED,
- 2 wyjścia alarmów,
- 2 wejścia czytników,
- 2 wejścia klawiatury wprowadzania identyfikatora PIN,
- 7 wejść cyfrowych,
- 2 wyjścia sygnalizacji akustycznej.

Zamki drzwiowe muszą być sterowane za pomocą przekaźnika. Muszą być podłączone w sposób ustalający stan „otwarty" lub „zamknięty" w razie awarii. Do zasilania zamków należy zastosować wewnętrzny zasilacz 12V prądu stałego, lub alternatywnie można zastosować przekaźnik jako przełącznik beznapięciowy z zewnętrznym zasilaczem zamków drzwiowych. Standardowy zasilacz 12VDC powinien pokryć zapotrzebowanie prądu dla dwóch typowych zamków 250 mA – 500 mA.

Kontroler powinien być zamknięty w obudowie. Zdjęcie przedniej pokrywy obudowy musi spowodować natychmiastowe uruchomienie przełącznika przeciwabotażowego.

5.3.3 Inteligentny kontroler drzwiowy

Urządzenie musi łączyć w sobie funkcje Kontrolera Obszaru i Kontrolera Drzwiowego. Dodatkowe zasoby muszą pozwolić na gromadzenie w nim tabel uprawnień i bufora transakcji. Urządzenie musi weryfikować uprawnienia, przyjmować rozkazy z systemu informatycznego i przesyłać do niego oczekiwane dane. Inteligentny Kontroler drzwiowy powinien dodatkowo nadzorować bezpośrednio zbliżeniowe czytniki kart, elektrozaczepy drzwiowe, zamki i przyciski otwierania drzwi na określonych zasadach i reagując w zaprogramowany sposób. Praca urządzenia musi być możliwa przy przerwanej komunikacji pomiędzy kontrolerem a serwerem systemu kontroli dostępu, umożliwiając pracę w sposób autonomiczny.

Każdy kontroler powinien cechować się co najmniej następującymi funkcjami:

- 2 wyjścia zamków drzwiowych,
- 4 wyjścia LED,
- 2 wyjścia alarmów,
- 2 wejścia czytników,
- 2 wejścia klawiatury wprowadzania identyfikatora PIN,

- 7 wejść cyfrowych,
- 2 wyjścia sygnalizacji akustycznej.

Zamki drzwiowe muszą być sterowane za pomocą przekaźnika. Muszą być podłączone w sposób ustalający stan „otwarty" lub „zamknięty" w razie awarii. Do zasilania zamków należy zastosować wewnętrzny zasilacz 12V prądu stałego, lub alternatywnie można zastosować przekaźnik jako przełącznik beznapięciowy z zewnętrznym zasilaczem zamków drzwiowych. Standardowy zasilacz 12VDC powinien pokryć zapotrzebowanie prądu dla dwóch typowych zamków 250 mA – 500 mA.

Kontroler powinien być zamknięty w obudowie. Zdjęcie przedniej pokrywy obudowy musi spowodować natychmiastowe uruchomienie przełącznika przeciwsabotażowego.

5.3.4 Zbliżeniowe czytniki kart

Zbliżeniowe czytniki kart muszą łączyć w sobie kilka opcji konfiguracyjnych i umożliwiać ich zastosowanie zarówno wewnątrz, jak i na zewnątrz pomieszczeń. Czytnik powinien umożliwiać:

- sygnalizację akustyczną i optyczną (wielokolorowy sygnalizator LED), które mogą być kontrolowane z serwera dostępu i/lub lokalnie,
- różne konfigurację sygnalizatora i diod LED, w zależności od indywidualnych wymagań obiektu,
- odczytywanie kart o formatach do 85 bitów,
- montowanie bezpośrednio na podłożu metalowym bez zmiany zasięgu odczytu,
- odczytywanie protokółu Wiegand.

Wewnętrzna procedura samotestu musi sprawdzać i weryfikować konfigurację ustawień, określać wewnętrzną lub zewnętrzną kontrolę wyświetlacza LED i sygnalizatora akustycznego, oraz inicjalizować działanie czytnika. Dodatkowy, zewnętrzny test pętli zwrotnej powinien umożliwiać weryfikację wyjść i wejść czytnika bez konieczności stosowania dodatkowego wyposażenia testowego.

Dla obsługi ruchu pojazdów należy stosować czytniki zbliżeniowe dalekiego zasięgu.

5.3.5 Czytniki biometryczne

Dla obiektów o wysokim stopniu zagrożenia albo zajmowanych przez szczególnie ważne komórki organizacyjne można zastosować po uzgodnieniu z GLSA czytniki biometryczne:

- czytniki linii papilarnych,
- czytniki siatkówki oka,
- czytniki kształtu twarzy.

Czytniki biometryczne muszą umożliwiać również zastosowanie kart zbliżeniowych dzięki wbudowanemu czytnikowi zbliżeniowemu pracującemu w standardzie Wiegand.

5.3.6 Elektrozaczepy drzwiowe

Elektrozaczep powinien być urządzeniem odbezpieczonym w razie awarii zasilania. Aktywowany elektrycznie powinien blokować zaczep. Zamek powinien być wyposażony w przełącznik informujący o stanie otwarcia drzwi. Zamek powinien być zasilany napięciem 12VDC.

5.3.7 Zamki elektromagnetyczne

Zamek elektromagnetyczny powinien być urządzeniem odbezpieczonym w razie awarii zasilania, które wymaga ciągłego zasilania do podtrzymania stanu zablokowania. Powinien składać się z elektromagnesu montowanego do ościeżnicy drzwi, oraz płyty zwierającej, która jest montowana do skrzydła drzwi. Płyta zwierająca musi być biernym elementem stalowym osadzonym na drzwiach,

który po wyosiowaniu z elektromagnesem w stanie zasilanym powinien zostać magnetycznie wciągnięty i zblokowany z nim. Siła przyciągania zamka musi wynosić co najmniej 250 kg. Zamek powinien być wyposażony w przełącznik położenia drzwi. Zasilanie zamka 12VDC.

5.3.8 Karta zbliżeniowa

Karta zbliżeniowa musi współpracować z czytnikami, które porozumiewają się z kontrolerami w oparciu o protokół Wieganda. Karta musi być wykonana tak aby mogła podlegać personalizacji bezpośrednio poprzez zadruk na drukarce termo transferowej bądź poprzez umieszczenie na niej naklejki PCV zadrukowanej w powyżej wymienionej technologii. Karty muszą być mocne i elastyczne, odporne na złamanie, oraz pozwalające na pracę w szerokim zakresie temperatur i wilgotności.

5.3.9 Urządzenia wyjściowe

Urządzenie wyjściowe musi być zaprojektowane w celu umożliwienia natychmiastowego wyjścia w dowolnej chwili bez konieczności użycia w tym celu klamki lub pokrętła. Musi być zlokalizowane w pobliżu drzwi i zawsze w oznaczonym ciągu drogi ewakuacyjnej.

5.3.10 Urządzenia pomocnicze

W systemie kontroli dostępu w zależności od potrzeb mogą być zastosowane dodatkowo następujące urządzenia:

- Klawiatury,
- czujniki otwarcia drzwi,
- moduły do otwierania drzwi przez telefon,
- urządzenia domofonowe.

5.4 Urządzenia mechaniczne blokujące

5.4.1 Bramki obrotowe

Podstawą uruchomienia mechanizmu odblokowującego musi być otrzymanie impulsu sterującego po pozytywnej weryfikacji danych użytkownika karty zbliżeniowej. Wewnętrzny rygiel powinien odblokować bramkę na określony czas. Stan otwarcia i zamknięcia bramki powinien być sygnalizowany na obudowie urządzenia. Po odblokowaniu mechanizmu i przejściu przez bramkę musi nastąpić samoczynne załączenie mechanizmu dopychającego, wspomagającego przejście i zablokowanie obrotu do czasu otrzymania następnego sygnału sterującego. Oprogramowanie procesora sterującego bramką musi umożliwiać działania w obu kierunkach oraz zapamiętywanie sygnału z urządzeń zewnętrznych z naprzemiennym odblokowywaniem rygla.

Urządzenie musi również umożliwiać odblokowania mechanizmu przy pomocy dodatkowego przycisku instalowanego przy stanowisku strażnika.

W przypadkach awaryjnych (brak zasilania lub ewakuacja osób) musi istnieć możliwość odblokowania mechanizmu poprzez:

- odbezpieczenia blokady ruchu ramion (ramiona obracają się swobodnie w obydwu kierunkach),
- wymontowania ramion bramki (przez odkręcenie śruby głównej w rotorze bramki).

5.4.2 Bramki uchylne

Układ procesorowy bramki w momencie otrzymania sygnału sterującego powinien odblokować ramię co umożliwia pchnięcie i przejście przez bramkę osoby upoważnionej. Po przejściu przez bramkę mechanizm sprężynowy powinien przywrócić ramię do punktu zamknięcia i spowodować

automatyczne zablokowanie bramki. Moment odblokowania ramienia powinien być potwierdzany sygnałem dźwiękowym w celu umożliwienia osobie przechodzącej zorientowanie się czy została uprawniona do wejścia lub wyjścia. Bramka musi być wyposażona w możliwość zdalnej blokady ramienia (np. za pomocą wyłącznika umieszczonego w pomieszczeniu strażnika).

W przypadku próby przejścia przez osobę nieupoważnioną urządzenie musi uruchamiać sygnał alarmowy.

5.5 Terminale rejestracji ruchu pojazdów

5.5.1 Wymagania ogólne

Przy każdej z bram wjazdowych na teren GLSA powinien zostać zainstalowany terminal rejestracji ruchu pojazdów. Każdy z terminali powinien być wyposażony w zintegrowany czytnik kart zbliżeniowych, klawiaturę alfanumeryczną i funkcyjną, wyświetlacz LCD. Terminal powinien komunikował się z serwerem systemu kontroli dostępu za pośrednictwem sieci LAN. Terminal będzie pełnił funkcję weryfikacji i rejestracji. Funkcja fizycznej kontroli wjazdu realizowana będzie przez szlabany wjazdowe lub bramy (w zależności od wymagań GLSA) sterowane ręcznie przez pracownika ochrony lub automatycznie. Terminale obsługiwane będą wyłącznie przez pracowników ochrony.

5.5.2 Terminal wjazdowy - wymagania

Urządzenie rejestracyjne musi być przystosowane do zastosowań zewnętrznych. Urządzenie wyposażone w kartę sieciową musi umożliwiać dołączanie do zarządzającego systemu informatycznego poprzez sieć LAN i zapewniać dwukierunkowe przesyłanie informacji.

Terminal powinien spełniać co najmniej następujące wymagania:

- Obudowa ze stali nierdzewnej,
- Klawiatura alfanumeryczna z opisem menu funkcyjnego,
- Wyświetlacz LCD 6 wierszy po 40 znaków
- Pamięć wewnętrzna 256 kB RAM,
- Dwa wyjścia sterujące,
- Złącze dla dodatkowego czytnika zewnętrznego,
- Osiem wejść cyfrowych,
- Możliwość podłączenia dodatkowych urządzeń peryferyjnych (skanery, wagi itd.),
- Zintegrowany UPS,
- Standardowe porty komunikacyjne RS 232, RS 485, TCP/IP,
- Stopień ochrony IP66.

5.6 Elektroniczny system ewidencji kluczy

5.6.1 Wymagania podstawowe

Projekt systemu kontroli dostępu w wybranych, ważnych obiektach wskazanych przez GLSA powinien uwzględniać zastosowanie elektronicznego systemu ewidencji kluczy. System powinien do tego celu wykorzystywać depozytory elektroniczno-mechaniczne. Depozytory muszą umożliwiać elektroniczny nadzór oraz mechaniczne zabezpieczenie kluczy oraz sterowanie dostępem uprawnionych osób do odpowiednich kluczy z jednoczesnym wykorzystaniem kart zbliżeniowych stosowanych w systemie kontroli dostępu.

5.6.2 Oprogramowanie

Oprogramowanie systemu musi umożliwiać nadawanie uprawnień oraz rejestrację podstawowych zdarzeń związanych z pobraniem klucza tj. czasu pobrania i zwrotu klucza oraz identyfikację osoby uprawnionej wg następującej procedury:

- uwierzytelnienia swoich uprawnień w system SEK kartą lub/i czytnikiem biometrycznym,
- otworzenie depozytora kluczy,
- fizyczne zwolnienie panelu zabezpieczenia mechanicznego,
- odnotowanie zdarzenia przez system SEK,
- pobór klucza przez osobę uprawnioną,
- zamknięcie depozytora.

Ustawienia uprawnień muszą być przechowywane nie ulotnej pamięci depozytora.

Oprogramowanie SEK musi być dostępne z poziomu serwera systemu kontroli dostępu i umożliwiać bieżące przeglądania zdarzeń i drukowania raportów ze stacji operatorskiej tego systemu.

Oprogramowanie depozytowa musi pozwalać także na grupowanie gniazd w strefach oraz tworzenia tzw. okien czasowych w celu ograniczenia czasu dostępu do depozytowa dla poszczególnych użytkowników.

5.6.3 Budowa depozytowa kluczy

Depozytor powinien być wyposażonych w zasilacz awaryjny umożliwiający działanie urządzenia przez 72 godz. w przypadku braku zasilania podstawowego. Depozytor powinien posiadać również możliwość mechanicznego otwarcia i odryglowania wszystkich kluczy zdeponowanych w urządzeniu. Wyświetlacz LCD oraz klawiatura numeryczna muszą umożliwiać ręczna konfigurację depozytora.

Kontroler depozytora powinien posiadać wyjścia przekaźnikowe w celu sygnalizacji alarmów o następujących zdarzeniach:

- próbie sabotażu depozytora,
- wyjęciu albo włożeniu klucza bez wybrania odpowiedniego kodu,
- zaistnieniu tzw. cichego alarmu,
- przekroczeniu maksymalnego czasu otwarcia szuflady albo po 3 błędnych wczytaniach karty,
- braku napięcia 220V lub napięcie akumulatora jest zbyt niskie,
- przepaleniu się jednego z bezpieczników rygli lub innej awarii rygla,
- wykryciu błędu w pamięci nie ulotnej i utracie ustawień depozytora.

5.7 Okablowanie sygnałowe

Okablowanie sygnałowe musi łączyć między sobą serwer dostępu i pozostałe urządzenia systemu kontroli dostępu. System powinien umożliwić kontrolę torów transmisyjnych w ramach systemu kontroli dostępu i rejestracji czasu pracy i wykrywać zmiany mogące mieć wpływ na poprawne działanie powyższego systemu.

5.8 Oprogramowanie

Specjalistyczne oprogramowanie zapewnia graficzny interfejs systemu kontroli dostępu pozwalający na pełną zdalną kontrolę podłączonych urządzeń. Oprogramowanie to zapamiętuje wszystkie dane niezbędne do kontrolowania systemu i umożliwia tworzenie i drukowanie raportów.

5.9 Zasilanie elektryczne

GLSA zapewni Dostawcy obwody zasilania wydzielone dla zasilania Systemu Kontroli Dostępu, zgodnie z wymaganą mocą określoną przez Dostawcę. Dostawca musi zapewnić wszystkie urządzenia niezbędne do generowania napięć zasilających o innych wartościach wymaganych wewnętrznie przez system kontroli dostępu. Jeżeli nie określono inaczej, zasilanie i system jego rozdziału nie muszą być dublowane. Należy przewidzieć sygnał wyjściowy, sygnalizujący awarię w zasilaniu elektrycznym oraz w systemie rozdziału mocy.

Kontrolery drzwiowe muszą być zasilane z rezerwowej baterii gazoszczelnej, zapewniającej 4 godziny podtrzymania zasilania w przypadku awarii zasilania głównego.

Dostawca zapewni zabezpieczenie przepięciowe urządzeń. Zabezpieczenie to musi gwarantować bezpieczeństwo kontrolerów jak również innych elementów składowych systemu w przypadku impulsowego wyładowania elektromagnetycznego.

5.10 Znakowanie

System kontroli dostępu powinien być oznakowany nazwą i logo producenta, w celu zapewnienia integralności kompletnego systemu. Każde urządzenie musi być wyposażone w etykietę uwidaczniającą dedykowany numer urządzenia zgodnie z dokumentacją i procedurą numerowania powiązanych urządzeń. Etykietę należy nanieść drogą wytłoczenia na tabliczce znamionowej. Tabliczki znamionowe muszą być sporządzone ze stali nierdzewnej, niekorodującego stopu, lub sztywnego plastiku i muszą być trwale przymocowane do niedemontowalnej części ramy urządzenia. Dostawca powinien przedłożyć propozycję etykiety celem zatwierdzenia jej przez GLSA przed rozpoczęciem wytwarzania.

5.11 Usługi

Usługi które powinien zapewnić Dostawca:

- projekt wykonawczy,
- programowanie systemu,
- fabryczna próba odbiorcza oraz inspekcja,
- pakowanie i wysyłka,
- montaż na miejscu budowy,
- próba eksploatacyjna systemu trwająca od 7 do 28 dni,
- szkolenie personelu (użytkowników, administratorów i serwisantów) wskazanego przez GL,
- opracowanie instrukcji obsługi, konserwacji oraz procedur reakcji na sygnały alarmowe,
- konserwacja w okresie gwarancyjnym.

Dostawca powinien posiadać koncesję MSWiA na świadczenie usług w zakresie technicznej ochrony mienia zgodnie z art. 15 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia. Projektant powinien posiadać licencję pracownika zabezpieczenia technicznego. Do zawarcia umowy z podwykonawcą potrzebna jest zgoda GL SA**.**

5.12 Kable, przewody, pozycje pomocnicze

Wszystkie kable, przewody, wtyczki, osprzęt i mechaniczne urządzenia zabezpieczające muszą być ujęte w zakresie dostawy Dostawcy. Okablowanie systemu kontroli dostępu musi obejmować wszystkie wymagane łącza do urządzeń zapewnianych przez Dostawcę. Wszystkie kable i listwy zaciskowe muszą być oznakowane z zastosowaniem systemu znakowania zgodnego z procedurą GLSA zawartą w standardzie 6120.

Wszystkie urządzenia przeznaczone do montażu na zewnątrz muszą być dostarczone z dławikami kablowymi. Dostawca powinien dokonać wyboru wpustów kablowych odpowiednio do średnic nominalnych kabli podanych przez ich producenta.

5.13 Dokumentacja

Zestawy dokumentacji, które muszą być dostarczone wraz z systemem przez Dostawcę celem dokonania odbioru i przyjęcia systemu:

1. Opis techniczny, obejmujący:
   - Przedmiot opracowania,
   - Podstawę opracowania zawierającą podstawę prawną strony wykonania projektu,
   - Charakterystykę obiektu chronionego, konstrukcyjną, architektoniczną,
   - Podział na strefy dozorowe,
   - Założenia i projekty związane (podstawy sporządzenia projektu tj. ustalenia z inwestorem potwierdzone notatką służbową, projekty aranżacji pomieszczeń , elektryczne itp.),
   - Analizę zagrożeń,
   - Przepisy i normy będące podstawą do opracowania koncepcji zabezpieczenia,
   - Opis organizacyjny systemu,
   - Opis techniczny systemu i charakterystykę zastosowanych urządzeń,
   - Opis instalacji przewodowej systemu, zawierający dane kabli i elementów instalacyjnych, sposób ich prowadzenia i wskazówki montażowe,
   - Informacje o miejscu i sposobie zasilania central i urządzeń liniowych,
   - Obliczenia bilansu mocy systemu wraz z zasilaniem awaryjnym, z podaniem uzgodnień i norm przyjętych dla określenia czasu pracy awaryjnego,
   - Wykaz zastosowanych urządzeń,
   - Informacje dla użytkownika dotyczące zasady obsługi, konserwacji i serwisu,
   - Uwagi montażowe,
   - Instrukcje obsługi, instalowania i konserwacji,
   - Wykaz norm związanych i innych dokumentów.
2. Zestawienie materiałów
3. Wykaz kabli
4. Rysunki
   - opis symboli graficznych,
   - schematy blokowe

- plan rozmieszczenia urządzeń w obszarach dozorowanych,
- plan rozmieszczenia urządzeń w pomieszczeniu ochrony,
- schematy połączeń (okablowania),
- jednoliniowe schematy zasilania,
- rysunki układu paneli,
- przykłady montażowe.

5. Dokumentacja powykonawcza obejmująca zrewidowane rysunki, odzwierciedlające zmiany dokonane względem urządzeń i systemu połączeń.
6. Lista kontrolna rozruchu
7. Raport odbiorowy

Przed przystąpieniem do szczegółowego projektowania, Dostawca powinien uzgodnić wymagania dla systemu (tj. funkcjonalność systemu, lokalizację urządzeń, prowadzenie kabli, interfejsy do istniejących instalacji) z przedstawicielami GLSA w tym z przedstawicielem Biura bezpieczeństwa i ochrony. Uzgodnienia te należy sporządzić na piśmie.

6 Dokumenty związane

Pozostałe Specyfikacje Techniczne, wymienione na przekazanym wykazie Specyfikacji Technicznych Grupy Lotos S.A.

7 Normy i przepisy

W każdym przypadku rozumie się, że przywołane normy, przepisy, dyrektywy i rozporządzenia są najnowszego wydania z obowiązującymi zmianami, załącznikami i suplementami.

7.1 Przepisy

Ustawa a dnia 22 sierpnia 1997 r. O ochronie osób i mienia. (Dz. U. Nr 114 dnia 26 września 1997 r. Poz. 740) z późniejszymi zmianami. Tekst jednolity (Dz. U. Nr 145 dnia 4 września 2005 r. Poz. 1221).

Ustawa z dnia 30 sierpnia 2002 r. o systemie oceny zgodności. (Dz.U. 2002 nr 166 poz. 1360) z późniejszymi zmianami. Tekst jednolity (Dz. U. 2010 nr 138 poz. 935).

Rozporządzenie Ministra Gospodarki z dnia 21 sierpnia 2007 r. w sprawie zasadniczych wymagań dla sprzętu elektrycznego (Dz.U. 2007 nr 155 poz. 1089)..

Ustawa z dnia 29 sierpnia 2003 r. o zmianie ustawy o systemie oceny zgodności oraz o zmianie niektórych ustaw (Dz.U. 2003 nr 170 poz. 1652) z późniejszymi zmianami.

Ustawa z dnia 30 sierpnia 2002 r. o systemie oceny zgodności (Dz.U. 2002 nr 166 poz. 1360). Tekst jednolity Dz. U. 2010 nr 138 poz. 935.

7.2 Normy

PN-EN 50133-1 - Systemy alarmowe – Systemy kontroli dostępu w zastosowaniach dotyczących zabezpieczenia – Część 1: Wymagania systemowe.

PN-EN 50133-2-1 Systemy włamaniowe – Systemy kontroli dostępu – Część 2-1:wymagania dla podzespołów

PN-EN 50133-7 Systemy alarmowe. Systemy kontroli dostępu stosowane w zabezpieczeniach. Część 7: Zasady stosowania

8 Załączniki

- Zał. 1. Kontrola dostępu – schemat blokowy.

9 Karta zmian

Lp.	Data	Opis	Wprowadzona przez
bb	5.12.2005	Zmiana wymagań dla sieci LAN w pkt. 4.2.2 oraz w załączniku 1. Zastąpienie standardu 3770 przez standard 6120.	Krzysztof Drabek
1	30-11-2013 (rev. 1)	Przegląd, aktualizacja, ujednolicenie i zmiany standardu w ramach zlecenia OK/990/2012	Redakcja zbiorowa. Koordynacja T. Wróbel
-	31-08-2015	Korekta nagłówka strony, bez mian w treści dokumentu	T. Wróbel