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 Pojęcia podstawowe 3
4.2 Warunki otoczenia 3
4.3 Dane elektryczne 4
5 Opis 4
5.1 Zasada działania 4
5.2 Wymagania systemowe 5
5.3 Centrala alarmowa 6
5.4 Elementy składowe systemu 7
5.5 Okablowanie sygnałowe 10
5.6 Zasilanie elektryczne 10
5.7 Malowanie 11
5.8 Znakowanie 11
5.9 Usługi 11
5.10 Kable, przewody, pozycje pomocnicze 11
5.11 Dokumentacja 12
6 Dokumenty związane 13
8 Normy i przepisy 13
8.1 Przepisy 13
8.2 Normy 13
9 Załączniki 14
10 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 ze innymi specyfikacjami technicznymi Grupy LOTOS S.A. (GLSA) ustala minimalne wymagania odnośnie projektowania i wykonania systemu sygnalizacji włamania.

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 niskonapięciowego systemu zasilania,
- Wymagań dotyczących parametrów kabli,
- Wymagań dotyczących prowadzenia i układania kabli.

Powyżej wymienione wyłączenia stanowią przedmiot oddzielnych specyfikacji.

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

GLSA – Grupa Lotos S. A.

KiA – Branża automatyki

4.1 Pojęcia podstawowe

Pamięć typu Flash - pamięć, w której zapisany jest podstawowy program centrali alarmowej. Jest ona kasowana elektrycznie, a jej zawartość może być zmieniana przy pomocy komputera.

Obiekt - grupa stref stanowiąca niezależny system alarmowy.

Strefa - grupa wejść nadzorujących wydzieloną część obiektu. Zbrojenie i rozbrajanie jest wykonywane jednocześnie dla całej grupy.

Wejście - para styków na płycie głównej centrali alarmowej lub płycie ekspandera (podłączonego do centrali alarmowej za pośrednictwem magistrali), do której podłączone są czujniki. Centrala nadzoruje za pośrednictwem wejść stany czujników.

Naruszenie wejścia - zmiana stanu wejścia, przy której następuje uaktywnienie czujnika (na przykład: otwarcie lub zwarcie styku wejścia, zmiana parametrycznej rezystancji czujnika).

Wyjście - para styków na płycie głównej panelu sterowania lub płytach ekspanderów, na których napięcie jest kontrolowane przez centrale alarmową.

Wyjście przekaźnikowe - przełącznik elektromagnetyczny znajdujący się na płycie ekspandera, kontrolowany (przełączany) przez centralę alarmową.

Magistrala - grupa przewodów, do których podłączone są ekspandery współpracujące z płytą główną centrali alarmowej. Jedna magistrala jest wykorzystywana do podłączania manipulatorów LCD, a inne magistrale – do podłączania ekspanderów.

Ekspander - urządzenie elektroniczne (moduł) rozszerzające funkcje centrali alarmowej. Występują ekspandery zwiększające ilość wejść centrali alarmowej lub (i) wyjść.

Zabezpieczenie sabotażowe - funkcja stosowana w centralach, ekspanderach, urządzeniach alarmowych i czujnikach. Zabezpiecza ona przed otwieraniem i/lub odrywaniem od podstawy.

Zabezpieczenie przed maskowaniem (antymasking) - funkcja stosowana w czujnikach ruchu. Sygnalizuje ona obiekty przemieszczające się blisko z przodu detektora, zapobiegając dzięki temu próbom zakrycia go.

4.2 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

4.3 Dane elektryczne

Dostępne źródło zasilania na miejscu:

Częstotliwość	50 Hz
Niskie napięcie	230 VAC TN-S

5 Opis

5.1 Zasada działania

5.1.1 Podstawowe zasady

System sygnalizacji włamania należy zaprojektować w sposób zapewniający bezpieczeństwo obszaru zdefiniowanego w ogólnych warunkach kontraktowych, przy użyciu środków technicznych. System ten należy zaprojektować zgodnie z wymaganiami dla klasy SA3 zdefiniowanej w normie PN-93/E-08390. W uzasadnionych sytuacjach należy przeprowadzić analizę ryzyka w celu właściwego doboru klasy systemu alarmowego.

5.1.2 Architektura

System sygnalizacji włamania musi cechować samodzielna, rozproszona struktura, na którą składają się:

- centrala alarmowa,
- ekspandery wejść,
- ekspandery wyjść (w razie potrzeby),
- manipulatory LCD,
- klawiatury strefowe,
- czujniki,
- przyrządy alarmowania wizualnego i akustycznego.

Centrala alarmowa, ekspandery i klawiatury muszą być podłączone za pomocą magistral komunikacyjnych. Funkcjonalność magistral musi być sprawdzana automatycznie. Czujniki ruchu, zestyki magnetyczne, czujniki wybicia szyby muszą być podłączone bezpośrednio z centralą alarmową lub ekspanderami wejść. Dla pojedynczego obiektu należy przewidzieć co najmniej 2 urządzenia alarmowe. Cały system powinien być oparty na cyfrowych, w pełni programowalnych centralach alarmowych. W uzasadnionych sytuacjach, po analizie funkcjonalnej tworzonego systemu, zaleca się stosowanie systemów adresowalnych.

Centrala alarmowa musi umożliwiać podłączenie wymaganych interfejsów do współpracy z:

- systemem telewizji przemysłowej,
- systemem kontroli dostępu.

Centrala alarmowa musi być połączona z centrum nadzoru w budynku wartowni za pomocą łącza komunikacyjnego lub linii telefonicznej. Interfejs ten powinien zapewniać dostęp do wszystkich informacji pochodzących z elementów składowych systemu.

Obiekty muszą być podzielone na strefy. Wielkość strefy należy uzgodnić ze służbami ochrony Grupy LOTOS S.A. Każda strefa musi mieć własną klawiaturę strefową, która może również w razie potrzeby być wykorzystywana do kontrolowania innych stref. Strefy mogą być kontrolowane przez

użytkowników, regulatory czasowe, sygnały sterujące, lub też ich stan może zależeć od stanu innych stref.

5.2 Wymagania systemowe

5.2.1 Zagadnienia ogólne

Oferowany system powinien być zaprojektowany tak, aby zminimalizować skutki awarii samego systemu lub urządzeń z tym systemem współpracujących. Dostawca powinien przedstawić wszystkie informacje niezbędne do oceny niezawodności systemu w proponowanej przezeń konfiguracji. Identyfikacja i lokalizacja usterek w systemie musi być w jak największym stopniu zautomatyzowana. Ponadto musi być możliwe wysyłanie alarmów do urządzenia zewnętrznego. Wszystkie metody sterowania, procedury obsługi i konserwacji należy zaprojektować w sposób umożliwiający ich łatwe wykonywanie.

Oferowany system powinien być zaprojektowany tak, aby zminimalizować zapas utrzymywanych części zamiennych. Na tyle, na ile istnieje konfiguracja rezerwowa, musi być możliwe dokonywanie wymiany modułów systemu bez przerywania jego działania.

System powinien umożliwiać kontrolowanie centrali alarmowej poprzez manipulator LCD i komputer PC (poprzez port RS-232, linię telefoniczną lub sieć komputerową). System ten powinien umożliwiać edycję nazw użytkowników, stref, wejść, wyjść i modułów w celu ułatwienia kontroli i nadzorowania systemu.

System ten powinien zapewniać stałe zapisywanie wszystkich prób włamań do kontrolowanej strefy. Dziennik zdarzeń powinien realizować następujące funkcje:

- pojemność zapisu do 1000 zdarzeń,
- zapisywane zdarzenia: uzbrajanie, rozbrajanie, alarmy, kasowanie alarmów, pomijanie, usuwanie pomijania stref, awarie, zastosowanie funkcji użytkownika, uruchamianie trybu serwisowego, itp.,
- rejestrowanie zdarzeń związanych z kontrolą dostępu,
- data i czas wystąpienia zdarzenia,
- funkcja wydruku zdarzenia z opcjonalnym wyborem zdarzenia, nazwami stref, modułów i użytkowników tak, jak są one zdefiniowane w systemie.

Jeżeli system ten jest uzupełniany przez telewizję przemysłową i nastąpi wtargnięcie do strefy, powinien zostać wyzwolony alarm, a odpowiednia kamera skierowana na naruszoną strefę. W tym samym czasie musi rozpocząć się nagrywanie obrazu z kamery.

5.2.2 Wymagania dla transmisji sygnałów.

Klasy systemów transmisji (opóźnienia transmisji, opóźnienia informacji monitorowanej, dostępność) muszą być odpowiednie dla klasy SA3 zgodnie z normami PN-93/E-08390/51, 52, 54, 55 i 56 dla transmisji sygnałów alarmu. Transmisja sygnałów przez tory specjalizowane musi być zgodna z klasą 2, transmisja sygnałów przez cyfrowy system łączności musi być zgodna z klasą 1, transmisja sygnałów przez system łączności akustycznej musi być zgodna z klasą 1.

5.2.3 Wymagania odnośnie ochrony budynków

System powinien opierać się na cyfrowych dualnych czujnikach ruchu i czujnikach rozbicia szkła. Zestyki magnetyczne muszą być zamontowane we wszystkich oknach i drzwiach, przez które może nastąpić wejście do chronionego obszaru. Musi być możliwe wzajemne zsynchronizowanie czujników i regulacja ich czułości, aby zapobiegać fałszywym alarmom.

Na ile to możliwe, wszystkie elementy instalacji i kable związane z systemem sygnalizacji włamania muszą być zlokalizowane wewnątrz strefy. Magistrale komunikacyjne, prowadzone na zewnątrz obszaru chronionego, muszą być ukryte i zabezpieczone przed uszkodzeniem. Prace montażowe należy wykonać zgodnie z instrukcjami producenta.

5.2.4 Wymagania dotyczące ochrony obwodowej

System ten powinien opierać się na:

- aktywnych barierach podczerwonych,
- dualnych czujkach ruchu,
- przewodach sensorowych.

przystosowanych do pracy na zewnątrz i odpornych na działanie czynników atmosferycznych.

Bariery muszą być ustawione wzdłuż wewnętrznej strony ogrodzenia, tak by tworzyły szczelny pierścień ochrony. Bariery należy ustawić tak, aby pokrywane przez nie obszary nie nakładały się. Bariery muszą być zainstalowane w odpowiedniej odległości od ogrodzenia, takiej aby intruz nie był w stanie zeskoczyć ze szczytu ogrodzenia poza obszar objęty ich działaniem. Zalecany odstęp pomiędzy wiązkami barier a ogrodzeniem wynosi 2 – 2,5 metra.

Przewody sensorowe muszą być zastosowane w miejscach gdzie bariery nie mogą być użyte z uwagi na przeszkody przecinające linię skutecznego widzenia pomiędzy nadajnikiem a odbiornikiem.

Wiązka bariery lub przewody sensorowe, zabezpieczające obszar chroniony, muszą być zblokowane z systemem kontroli dostępu, który kontroluje bramy, aby automatycznie dezaktywować ochronę właściwego sektora, gdy na teren wkracza upoważniony pojazd lub osoba. Szczegóły należy dostosować zgodnie z procedurami bezpieczeństwa obszaru chronionego i dyspozycjami Grupy LOTOS S.A..

Wszystkie czujniki i zestyki muszą być podłączone do panelu sterowania jako oddzielne linie, dzięki czemu ewentualne dalsze zmiany i rekonfiguracje będzie można wykonać w łatwy sposób. Taki sposób podłączenia pozwoli również na kontrolowanie stanu każdej strefy z wysoką dokładnością.

Monitorowanie stanu wszystkich stref musi być możliwe za pomocą oprogramowania współpracującego z centrala alarmową.

Wszystkie czujniki muszą być łączone w trybie połączenia parametrycznego, dzięki czemu oprócz stanu samego czujnika, można będzie również kontrolować stan kabli. Każda ustawiona wiązka bariery musi być podłączona jako oddzielna linia, dzięki czemu będzie można precyzyjnie określić pozycję intruza.

5.3 Centrala alarmowa

Urządzenie to musi umożliwiać monitorowanie obecności i sprawności działania czujnika wykorzystując różne możliwe do wybrania opcje konfiguracyjne i typy reakcji. Pojemność centrali alarmowej dotycząca ilości ekspanderów i klawiatur musi być dostosowana do wymagań systemu.

Program centrali powinien być zapisany w nie ulotnej pamięci, zapewniającej utrzymanie ustawień centrali nawet przy braku zasilania.

Aktualizacja oprogramowania firmowego musi być możliwa do wykonania bez konieczności demontowania centrali.

Programowanie ustawień centrali alarmowej musi być możliwe:

- lokalnie za pomocą manipultora LCD,

- lokalnie za pomocą komputera podłączonego do portu RS-232,
- zdalnie, za pomocą komputera podłączonego do centrali poprzez modem.

Centrala musi umożliwiać ustawienie do 240 kodów użytkownika, do 8 kodów głównych (1 kod na każdy obiekt) i 1 kodu serwisowego. Dodatkowo kodowanie musi umożliwiać stosowanie:

- kilka typów kodów użytkownika z opcją definiowania dodatkowych poziomów uprawnień dostępu do systemu,
- funkcji menu klawiatury w zależności od uprawnień użytkownika i typu kodu,
- definiowanego dostępu do klawiatur, zamków szyfrowych i zbliżeniowych czytników kart,
- okresowej zmiany kodów dostępu za pomocą przedrostków.

W celu lepszego zabezpieczenia przed nieuprawnionym dostępem do obiektu musi być zagwarantowane definiowanie stref zabezpieczonych dwoma hasłami.

Centrala alarmowa musi generować dziennik zdarzeń o następujących parametrach:

- pojemność zapisu do 1000 zdarzeń,
- zapisywane zdarzenia: uzbrajanie/rozbrajanie, alarmy, kasowanie alarmów, pomijanie/usuwanie pomijania stref, awarie, zastosowanie funkcji użytkownika, uruchamianie trybu serwisowego, itp.,
- rejestrowanie zdarzeń związanych z kontrolą dostępu,
- data i czas wystąpienia zdarzenia.

Dodatkowo centrala alarmowa musi być wyposażony w:

- magistrale komunikacyjne do rozbudowy systemu,
- automatyczną diagnostykę elementów składowych systemu,
- zegar czasu rzeczywistego z kalendarzem i podtrzymaniem bateryjnym,
- wizualną sygnalizację stanu wyjść,
- obwód ładowania baterii,
- wybieranie numerów telefonicznych,
- zabezpieczenie elektroniczne wszystkich wejść, wyjść i magistral komunikacyjnych.

5.4 Elementy składowe systemu

5.4.1 Ekspandery wejść

Ekspander powinien być stosowany jako urządzenie przeznaczone do pracy łącznie z centralą alarmową. Powinien pozwalać na rozszerzenie systemu alarmowego o co najmniej osiem wejść, posiadających identyczne funkcje jak wejścia płyty głównej centrali alarmowej. Do ekspandera mogą być podłączone czujniki typu NO (normalnie otwarte) i NC (normalnie zwarte). Wejścia te mogą być skonfigurowane do pracy z pojedynczym parametrem (EOL) i z podwójnym parametrem (2EOL). Każde z wejść musi być indywidualnie programowalne i mieć przypisany jeden z kilku typów odpowiedzi na naruszenie.

5.4.2 Aktywna bariera podczerwona

Każda bariera musi składać się z jednego nadajnika i odbiornika. Nadajnik powinien emitować niewidzialne światło podczerwone w kierunku odbiornika. W przypadku przerwania przez osobę

biegu wiązki w dowolnym miejscu pomiędzy nadajnikiem a odbiornikiem, powinien zostać uruchomiony alarm.

Pojedyncza bariera musi być zespolona i składać się z dwóch podwójnych zwierciadeł parabolicznych, tworzących 4-kanałową automatycznie synchronizowaną barierę podczerwieni.

Odległość pomiędzy pojedynczymi wiązkami musi być mniejsza niż 20 cm. Bariery mogą być zwielokrotniane by utworzyć kurtynę podczerwieni.

Tryb oceny alarmu i czułość odpowiedzi alarmu muszą być regulowane. Czułość odpowiedzi alarmu musi być indywidualnie nastawiana dla każdej z barier.

W przypadku gdy warunki widoczności pomiędzy nadajnikiem a odbiornikiem zmieniają się w wyniku silnego zamglenia, opadów śniegu, lub gdy układ optyczny ulega zabrudzeniu a wzajemna komunikacja może zostać przerwana, wówczas powinien być włączony alarm. Powinien on uaktywniać się, gdy poziom sygnału utrzymuje się poniżej nastawionej wartości w przeciągu określonego czasu (5 – 30 s).

Dla każdego urządzenia należy zamontować oddzielny podgrzewacz. Podgrzewacz powinien być zasilany prądem stałym.

Dla każdego nadajnika i odbiornika należy przewidzieć również przełącznik zabezpieczający przed manipulacjami, dzięki któremu każde usiłowanie uszkodzenia kabla lub osłony bariery musi skutkować uruchomieniem alarmu. Alarmy techniczne muszą być wzbudzane w przypadku wystąpienia błędu w urządzeniu przetwarzania danych, lub jego awarii wskutek zakłóceń zewnętrznych. Bariery muszą być zamknięte w obudowach o klasie ochrony co najmniej IP54.

5.4.3 Przewód sensorowy

Przewód sensorowy powinien wykorzystywać sygnały generowane przy nieznacznym ugięciu przez mikrofonowy przewód czujnikowy. Przewód powinien wykrywać wykonywanie przez intruza prób przecięcia, wspinania się na ogrodzenie lub podnoszenia siatki ogrodzenia. Izolacja kabla musi być odporna na promieniowanie UV oraz na trudne warunki klimatyczne. System powinien eliminować alarmy powodowane przez zdarzenia naturalne i środowiskowe.

Specjalne cechy charakterystyczne dla wtargnięcia muszą być analizowane przez cyfrowy procesor sygnału. Terminator na końcu kabla powinien pozwalać na nadzorowanie integralności każdej strefy przez procesor sygnału. W przypadku wykrycia intruza lub przerwania ciągłości kabla powinien zostać uruchomiony alarm. Procesor powinien komunikować się z centrala alarmową poprzez zestyk przekaźnikowy lub łącze danych. Procesor ten powinien być zamknięty w obudowie o klasie ochrony IP66 wewnątrz chronionej strefy.

5.4.4 Dualny czujnik ruchu

Cyfrowe dualne czujniki ruchu muszą łączyć w sobie fotoelektryczny czujnik podczerwieni (podwójny element piroelektryczny), oraz czujnik mikrofalowy, co musi zapewnić wysoką skuteczność i maksymalną odporność na zakłócenia. Czujnik ten powinien być dodatkowo wyposażony w filtr UV i filtr światła widzialnego.

Czujnik powinien opierać się na cyfrowym przetwarzaniu sygnału, posiadać cyfrową kompensację temperaturową, regulację czułości, zabezpieczenie przed maskowaniem i sabotażem. Wymagane jest nadzorowanie napięcia zasilającego, jak również należy uwzględnić niski pobór mocy. Cyfrowe przetwarzanie sygnału musi uaktywniać alarm tylko wtedy, gdy oba czujniki wykryją ruch.

Wymienne soczewki Fresnela muszą umożliwiać szeroki kąt widzenia oraz zastosowanie kurtyny wykrywania pionowego z możliwością regulowania na chroniony obszar. Wraz z detektorem należy dostarczyć regulowany uchwyt umożliwiający łatwe montowanie czujnika na ścianie lub suficie.

5.4.5 Czujnik rozbicia szyby.

Metoda wykrywania rozbicia szyby musi być przystosowana do różnych rodzajów szkła (również szkła laminowanego i zbrojonego, jeżeli jest to wymagane).

Musi być możliwe nastawianie poziomu czułości. Wymagane jest nadzorowanie napięcia zasilania, jak również należy zadbać o niski pobór mocy. Czujnik powinien być wyposażony w zabezpieczenie sabotażowe.

O ile wystąpi potrzeba Dostawca może zastosować czujki innego typu niż wymienione powyżej.

5.4.6 Zestyk magnetyczny

Zestyki magnetyczne należy stosować wszędzie tam gdzie wymagane jest kontrolowanie stanu drzwi, bram, okien i/lub innych ruchomych elementów używanych do zabezpieczania lub nadzorowania dostępu do określonej strefy.

Rodzaje zestyków magnetycznych mogą różnić się konfiguracją montażową i obudową w zależności od materiału zastosowanego do wytworzenia okien i drzwi. Preferuje się stosowanie zestyków magnetycznych do montażu wpuszczanego. Jeżeli zestyki magnetyczne zostały zaprojektowane do montażu powierzchniowego, to muszą być wówczas wyposażone w zabezpieczenie przed sabotażem. Każdy z elementów styków magnetycznych powinien być umieszczony w obudowie wodoszczelnej.

5.4.7 Urządzenie alarmowe

Samo-uruchamiająca się syrena zewnętrzna z sygnalizacją błyskową musi być uruchamiana z centrali alarmowej. Syrena ta musi mieć następujące cechy:

- sygnał akustyczny – sygnał dźwiękowy magnetodynamiczny,
- sygnał optyczny – ksenonowe światło strobujące,
- dostępne 4 różne dźwięki,
- 2 wejścia sterujące,
- wysokowytrzymała obudowa poliwęglanowa,
- zabezpieczenie przed sabotażem polegającym na otwieraniu i demontowaniu,
- pokrywa wewnętrzna ze stali ocynkowanej,
- impregnowane obwody elektroniczne,
- opcjonalny hermetyczny zestyk magnetyczny,
- indywidualne zasilanie z akumulatora –12V 1,3 Ah,
- obudowa o stopniu ochrony min. IP34.

Akustyczna syrena wewnętrzna musi mieć następujące cechy:

- sygnał akustyczny – buczek piezoelektryczny,
- dostępne min. 3 różne dźwięki,
- trwała obudowa z ABS,
- zabezpieczenie przed nieupoważnionym otwieraniem i demontowaniu,
- impregnowane obwody elektroniczne,
- obudowa o stopniu ochrony min. IP32.

5.4.8 Manipulator LCD

Manipulator LCD powinien umożliwiać programowanie centrali alarmowej. Manipulator powinien cechować się następującymi właściwościami:

- duży, czytelny wyświetlacz o minimum 2 x 16 znakach, ze stałym lub chwilowym podświetlaniem aktywowanym przyciśnięciem klawisza lub przez dowolne wejście centrali alarmowej,
- 16-klawiszową klawiaturę z podświetlaniem kontrolowanym w taki sam sposób jak podświetlenie wyświetlacza,
- 2 wejścia o właściwościach identycznych, jak wejścia centrali alarmowej,
- mikroprzełącznik wykrywający próby manipulowania przy klawiaturze,
- port RS-232 pozwalający na obsługiwanie systemu alarmowego za pomocą komputera nadzorującego i programu użytkownika.

5.4.9 Klawiatura strefowa

Klawiatura strefowa musi być przyrządem zaprojektowanym do pracy z centrala alarmową. Musi być wykorzystywana do uzbrajania i rozbrajania pojedynczej strefy i wyposażona w funkcję kontroli dostępu, oraz elementy kontrolujące działanie elektromagnetycznych zamków drzwi i monitorujące czy drzwi są otwarte, czy zamknięte. Klawiatura strefowa musi pozwalać na zmianę kodu użytkownika i wywoływanie funkcji sterujących urządzeniami zewnętrznymi.

Klawiatura strefowa musi być wyposażona w 12 klawiszy z chwilowym podświetlaniem (działającym automatycznie), oraz diody LED opisane jak poniżej:

- ALARM (czerwona) - ciągłe świecenie będzie wskazywać uruchomienie alarmu w strefie obsługiwanej przez tę klawiaturę, a miganie diody LED będzie wskazywać, że alarm w tej strefie wystąpił wcześniej,
- DOZÓR/CZUWANIE (zielona) - ciągłe świecenie będzie informować, że strefa przypisana do tej klawiatury jest uzbrojona. Dioda LED będzie migać w trakcie odliczania czasu opóźnienia,
- AWARIA (żółta) - ta dioda LED będzie migać, gdy zostanie wykryty problem techniczny w systemie.

Na klawiszach muszą być nadrukowane litery wraz z cyframi w celu identyfikacji numerów kodowych z hasłami. Jeżeli trzykrotnie zostanie wprowadzony błędny kod (nierozpoznany przez panel sterowania), musi nastąpić uruchomienie alarmu.

5.5 Okablowanie sygnałowe

Okablowanie sygnałowe musi łączyć centrale alarmową z innymi urządzeniami elektronicznego systemu bezpieczeństwa. W uzupełnieniu do sygnałów użytkownika przekazywanych po standardowym okablowaniu sygnałowym, należy przesłać sygnał monitorujący po linii antysabotażowej w celu wykrywania wszelkich odłączeń tych urządzeń. Przerwanie dowolnego przewodu musi być wykryte i zarejestrowane w dzienniku. Wymaganie to dotyczy wszystkich elementów elektronicznego systemu bezpieczeństwa.

5.6 Zasilanie elektryczne

GLSA zapewni wydzielone obwody zasilania dla systemu sygnalizacji włamania, dostosowane do wielkości mocy określonej przez Dostawcę.

Dostawca musi zapewnić wszelkie wyposażenie niezbędne do generowania napięć zasilających o innych wartościach, potrzebnych wewnętrznie w systemie sygnalizacji włamania.

Jeżeli nie określono inaczej, zasilanie i system jego rozdziału dla systemu nie musi być refundowany. Należy przewidzieć sygnał wyjściowy, sygnalizujący awarię w zasilaniu elektrycznym oraz w

systemie rozdziału mocy. System powinien być uzupełniony o zasilanie rezerwowe z gazoszczelnej baterii zapewniającej 24-godzinne zasilanie awaryjne w przypadku awarii zasilania głównego.

Dostawca zapewni odpowiednie zabezpieczenie przepięciowe systemu sygnalizacji włamania. Zabezpieczenie to musi gwarantować bezpieczeństwo centrali alarmowej jak również urządzeń przyłączonych do centrali w przypadku impulsowego wyładowania elektromagnetycznego.

5.7 Malowanie

Malowanie urządzeń montowanych na zewnątrz należy wykonać zgodnie z wymaganiami obowiązującymi dla atmosfery przemysłowej, chemicznej i morskiej. Należy dopilnować, aby wszystkie elementy konstrukcyjne były właściwie pomalowane. Kolor urządzeń może być zgodny z normami producenta.

5.8 Znakowanie

Wszystkie urządzenia systemu sygnalizacji włamania muszą być oznakowane nazwą producenta i znakiem firmowym Dostawcy, aby zagwarantować integralność kompletnego systemu. Każde urządzenie musi być wyposażone dodatkowo w etykietę wskazującą (specyficzny) numer urządzenia zgodnie z dokumentacją, oraz procedurą numerowania urządzeń.

Opisy urządzeń zewnętrznych muszą być naniesione poprzez odciśnięcie na tabliczkach znamionowych. Tabliczki znamionowe muszą być wykonane ze stali nierdzewnej, stopu niekorodującego lub sztywnego plastiku, oraz trwale przymocowane do niedemontowalnej części urządzenia. Dostawca powinien przedłożyć Grupie LOTOS SA propozycję etykiety do zatwierdzenia przed rozpoczęciem produkcji.

5.9 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 z późniejszymi zmianami. Projektant powinien posiadać licencję pracownika zabezpieczenia technicznego. Do zawarcia umowy z podwykonawcą potrzebna jest zgoda GL SA**.**

5.10 Kable, przewody, pozycje pomocnicze

Wszystkie kable, przewody, wtyczki, osprzęt i mechaniczne urządzenia zabezpieczające muszą być ujęte w zakresie dostawy Dostawcy. Okablowanie systemu musi obejmować wszystkie wymagane

łącza do urządzeń dostarczanych przez Dostawcę. Wszystkie kable i listwy zaciskowe muszą być oznakowane na każdym końcu, z zastosowaniem systemu znakowania zgodnego z procedurą GLSA.

Wszystkie urządzenia przeznaczone do pracy na zewnątrz muszą być wyposażone w dławiki kablowe. Dostawca powinien dokonać wyboru dławików kablowych ściśle według nominalnych średnic kabli podanych przez ich producenta.

5.11 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 Uzgodnienia te należy sporządzić na piśmie.

6 Dokumenty związane

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

7

8 Normy i przepisy

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

8.1 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).

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).

Ustawa z dnia 13 kwietnia 2007 r. o kompatybilności elektromagnetycznej (Dz.U. 2007 nr 82 poz. 556).
Rozporządzenie Ministra Gospodarki z dnia 22 grudnia 2005 r. w sprawie zasadniczych wymagań dla urządzeń i systemów ochronnych przeznaczonych do użytku w przestrzeniach zagrożonych wybuchem (Dz.U. 2005 nr 263 poz. 2203)

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

8.2 Normy

PN-E-08390-1 Systemy alarmowe. Terminologia.

PN-E-08390-5 Systemy alarmowe. Włamaniowe systemy alarmowe. Wymagania i badania sygnalizatorów.

PN-EN 50130-4 Systemy alarmowe. Część 4: Kompatybilność elektromagnetyczna. Norma dla grupy wyrobów: Wymagania dotyczące odporności urządzeń systemów sygnalizacji pożarowej, sygnalizacji włamania, sygnalizacji napadu, CCTV, kontroli dostępu i osobistych.

PN-EN 50130-5 Systemy alarmowe – Część 5: Próby środowiskowe.

PN-EN 50131-1 Systemy alarmowe. Systemy sygnalizacji włamania i napadu. Część 1: Wymagania systemowe.

PN-E-08390-22 Systemy alarmowe. Włamaniowe systemy alarmowe. Ogólne wymagania i badania czujek.

PN-E-08390-23 Systemy alarmowe. Włamaniowe systemy alarmowe. Wymagania i badania aktywnych czujek podczerwieni.

PN-E-08390-24 Systemy alarmowe. Włamaniowe systemy alarmowe. Wymagania i badania ultradźwiękowych czujek Dopplera.

PN-EN 50131-2-4 - Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Część 2-4: Wymagania dotyczące dualnych czujek pasywnych podczerwieni i mikrofalowych.

PN-EN 50131-2-2 - Systemy alarmowe -- Systemy sygnalizacji włamania i napadu -- Część 2-2: Czujki sygnalizacji włamania -- Pasywne czujki podczerwieni.

PN-EN 50136-1 Systemy alarmowe – Systemy i urządzenia transmisji alarmu – Część 1: Wymagania ogólne dotyczące systemów transmisji alarmu (oryg.).

PN-EN 50136-2-1 Systemy alarmowe – Systemy i urządzenia transmisji alarmu – Część 2-1: Wymagania ogólne dotyczące urządzeń transmisji alarmu.

9 Załączniki

- Załącznik Nr 1. Schemat blokowy. Sygnalizacja włamania.

10 Karta zmian

Lp.	Data	Opis zmian	Zmianę wprowadził
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