Spis zawartości

1 Przedmiot specyfikacji 2
2 Zakres obowiązywania 2
2.1 Odstępstwa 2
3 Hierarchia dokumentów 2
4 Definicje i oznaczenia 2
5 Opis 3
5.1 Ogólne wymogi dla komputerów pracujących w systemach automatyki 3
5.2 Podział funkcjonalny komputerów pracujących w systemach automatyki 4
5.3 Szczegółowe wymogi dla komputerów pracujących w systemach automatyki 6
5.4 Ochrona oprogramowania oraz danych komputerowych 7
5.4.1 Zabezpieczenie sprzętowe w miejscu powstawania awarii 7
5.4.2 Redundancja urządzeń komputerowych 7
5.4.3 Ochrona oprogramowania i danych poprzez narzędzia administracyjne 7
5.4.4 Wykonywanie kopii bezpieczeństwa dla oprogramowania i danych na zewnętrzne nośniki 7
5.4.5 Przechowywanie kopii zapasowych i bezpieczeństwa 8
5.5 Prawidłowa zabudowa systemów komputerowych 9
5.6 Zasilanie komputerów 9
6 Dokumenty związane 9
7 Normy i przepisy 9
7.1 Dyrektywy Wspólnoty Europejskiej 10
7.2 PN 10
7.3 Inne normy 11
8 Karta zmian 12

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 standardowymi specyfikacjami technicznymi Grupy LOTOS S.A. ustala minimum wymagań stanowiących przewodnik jakościowy dla wykonania projektu technicznego Kontroli i Automatyki, w zakresie doboru komputerów pracujących w systemach automatyki. Pewne zagadnienia znajdujące się poza tą specyfikacją będą przedmiotem szczegółowych standardów bądź będą wymagały szczególnych niezależnych rozważań.

Niniejsza specyfikacja określa wytyczne techniczne, według których muszą być konfigurowane komputery pracujące w układach automatyki służące do akwizycji, wizualizacji, sterowania, przetwarzania i składowania danych procesowych. Specyfikacja określa również podstawowe wymogi zabudowy, zasilania, serwisowania oraz zabezpieczenia oprogramowania i danych.

2 Zakres obowiązywania

Specyfikacja ta ma zastosowanie przy sporządzaniu zapytań ofertowych i kontraktów dla nowo planowanych przedsięwzięć inwestycyjnych, modernizacyjnych lub remontowych Grupy LOTOS S.A..

Stanowi ona również podstawę do opracowania szczegółowych specyfikacji i zapytań ofertowych dla dostaw indywidualnych i pakietowych.

Specyfikacja ta odnosi się, więc jedynie do komputerów pracujących w systemach automatyki, a nie odnosi się do tych systemów całościowo ani także do ich innych elementów takich jak np. układy we/wy, kontrolery DCS, PLC. Specyfikacja nie odnosi się także do komputerów i serwerów pracujących w sieci zakładowej GLSA.

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..

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 GLSA
- Niniejsza specyfikacja
- Inne specyfikacje
- Rysunki i inne dokumenty
- Normy

4 Definicje i oznaczenia

GLSA - Grupa LOTOS S.A.

KiA – branża automatyki

CR (Control Room) - Centralna sterownia.

DCS (Distributed Control System) - Rozproszony Komputerowy System Sterowania.

DDS (Digital Data Storage), DLT (Digital Linear Tape) - typy napędów streamer'a i taśmy.

ER (Engineering Room) - pokój stacji inżynierskich.

ESD (Emergency Shut Down System) - System Blokad użyty do implementacji funkcji bez zdefiniowanego poziomu SIL.

SIS (Safety Instrumented System) - System Automatyki użyty do implementacji funkcji bezpieczeństwa ze zdefiniowanym poziomem SIL.
SIL (Safety Integrity Level) - Poziom nienaruszalności bezpieczeństwa.

HMI (Human Machine Interface) - Interfejs człowiek / maszyna.

IP (Ingress Protection) - stopień ochrony przed pyłem i wodą.

I/O (Input/Output) - wejście/wyjście.

LCD (Liquid Crystal Display) - Monitor ciekłokrystaliczny.

MTBF (Mean Time Between Failures) - Średni Czas Między Awariami.

PLC (Programmable Logic Controller) - Sterownik Programowalny.

RAID (Redundant Array of Independent Disks) - Redundantna Macierz Niezależnych Dysków.

USB (Universal Serial Bus) - port USB.

TFT (Thin Film Transistor) - rodzaj kolorowego wyświetlacza ciekłokrystalicznego z aktywną matrycą.

UPS (Uninterrupted Power Supplier) - system bezprzerwowego zasilania.

5 Opis

5.1 Ogólne wymogi dla komputerów pracujących w systemach automatyki

Komputery pracujące w systemach automatyki są elementami niezawodnego i efektywnego systemu monitorowania i sterowania, a także składowania i zarządzania danymi procesowymi w celu wszechstronnej analizy danych z produkcji w GLSA. Przemysłowa baza danych jest udostępniana przez rozbudowaną sieć kliencką w sieci zakładowej.

Istotnym elementem charakterystyki komputerów pracujących w systemach automatyki jest ich niezawodność mająca swe odzwierciedlenie także w bezpieczeństwie danych, a także wysoki komfort pracy pracowników. W związku z tym założeniem, dostawca systemów automatyki powinien wziąć pod uwagę konstrukcję komputerów pod względem odporności na warunki przemysłowe istniejące w miejscu instalacji komputera, specyficzne wymagania dotyczące wydajności, funkcji interakcji operatora z procesem, a także dobór elementów komputerowych i ich ewentualną redundancję. Elementy komputerów muszą być elementami o wysokiej niezawodności i muszą być wyprodukowane przez renomowanych producentów.

Komputery pracujące w systemach automatyki muszą mieć możliwość łatwej naprawy, wprowadzania zmian, rozbudowy (skalowalność) i aktualizacji systemu operacyjnego oraz oprogramowania (patches, upgrades) przez GLSA w trakcie produkcji, także po okresie

gwarancyjnym. W związku z tym konfiguracja sprzętowa oraz programowa musi być zgodna ze standardami przyjętymi w GLSA - preferowane jest wykorzystanie standardowych technologii komputerowych obecnych np.: w instalacjach biurowych i każdorazowo szczegółowo uzgodnionych. W przypadku konieczności zastosowania rozwiązań dedykowanych wymagane jest zapewnienie na etapie kontraktu pełnych szkoleń inżynierskich dla pracowników GLSA.

Innym ważnym elementem dla użytkowania komputerów jest wymagany szybki czas reakcji i naprawy w przypadku awarii. Naprawa musi nastąpić w miejscu instalacji komputera.

Oprogramowanie musi posiadać możliwość wprowadzania zmian przez GLSA bez utraty gwarancji na komputer, a także na całość systemu automatyki. Działania GLSA, które spowodują utratę gwarancji muszą być zminimalizowane oraz szczegółowo określone na etapie kontraktowym.

Dostarczane komputery muszą być modelami aktualnie oferowanymi przez producenta. Nie mogą to być komputery pochodzące z zapasów magazynowych, po zakończeniu produkcji, czy modele aktualnie wycofywane. Dlatego specyfikację sprzętu należy w miarę możliwości ustalać w końcowym etapie przygotowania projektu.

5.2 Podział funkcjonalny komputerów pracujących w systemach automatyki

Komputery pracujące w systemach automatyki dzielimy funkcjonalnie jak w tabeli poniżej:

l.p.	Funkcja komputera	Opis funkcjonalny i podstawowe wymogi techniczne komputera
1	**Stacja operatorska**	**Funkcjonalność:** komputer przeznaczony do komunikacji systemu monitorowania i sterowania procesem z człowiekiem (operatorem) (HMI) w celu prezentacji danych procesowych i wprowadzania komend i parametrów sterowania przez operatora. **Podstawowe wymogi techniczne:** - Możliwość podpięcia dwóch monitorów (o niezależnym obrazie). - Monitor minimum 19" LCD (aktywna matryca TFT) o rozdzielczości 1600x1200, kąt widzenia ponad 160° w pionie i poziomie, kontrast przynajmniej 500:1, luminancja przynajmniej 250 $cd/m^{2.}$ - Klawiatura i trackball (preferowany) lub myszka optyczna. - Podwójna karta sieciowa preferowany FastEthernet (100Base-TX) (lub o większej szybkości) dla redundowanej komunikacji w systemie automatyki. - Możliwość generowania sygnałów akustycznych.
2	**Stacja inżynierska**	**Funkcjonalność:** ta sama funkcjonalność jak dla stacji operatorskiej, dodatkowo narzędzia do konfiguracji systemu, zmian w oprogramowaniu, a także do parametryzacji i diagnostyki urządzeń obiektowych. **Podstawowe wymogi techniczne:** - Wymogi techniczne jak dla stacji operatorskiej. - Wewnętrzna lub zewnętrzna nagrywarka CD/DVD do podłączenia poprzez USB lub FireWire

l.p.	Funkcja komputera	Opis funkcjonalny i podstawowe wymogi techniczne komputera
3	**Stacja procesowa**	**Funkcjonalność:** komputer lub komputer zintegrowany ze sterownikiem w jednej obudowie; przeznaczony do pobierania danych z urządzeń automatyki przemysłowej, przetwarzania i przesyłania informacji do innych stacji, systemów sterowania i serwerów. Stacja przechowuje tylko informacje bieżące; Jako stacja procesowa może być użyty komputer przemysłowy*) lub kompaktowy**). **Podstawowe wymogi techniczne:** - Komputer kompaktowy: brak elementów rotujących - konstrukcja z chłodzeniem biernym (bez wentylatora), preferowane rozwiązanie bez mechanicznego dysku, wyposażony w wymagane interfejsy komunikacyjne. - Komputer przemysłowy: wolne gniazda PCI do rozbudowy, możliwość zamontowania pełnowymiarowej karty, preferowany kontroler RAID1, (tzw. mirroring sprzętowy) lub wyższy, wyposażony w wymagane interfejsy komunikacyjne.
4	**Serwer systemu automatyki**	**Funkcjonalność:** komputer typu serwer przeznaczony do zbierania, archiwizacji i udostępniania danych pochodzących z urządzeń automatyki lub stacji procesowych lub operatorskich. W małych***) systemach funkcje stacji i serwera może realizować jeden fizyczny komputer spełniający wymogi wszystkich klas. **Podstawowe wymogi techniczne:** - Podwójny zasilacz z możliwością wymiany podczas pracy (Hot Swap). - Redundantne wentylatory z możliwością wymiany podczas pracy (Hot Swap). - Sprzętowy kontroler RAID 5 z możliwością wymiany dysków podczas pracy (Hot Swap) + dysk w gorącej rezerwie – preferowane dyski SCSI. - Pamięć taśmowa. - Monitor LCD 19”.
5	**Serwer historii**	**Funkcjonalność:** komputer typu serwer przeznaczony do zbierania, archiwizacji i udostępniania danych z innych serwerów i stacji w długim okresie czasu (minimum 1 rok). **Podstawowe wymogi techniczne:** - Wymogi techniczne jak dla serwera systemu automatyki.

Komputer przemysłowy*) - przeznaczony do działania w warunkach przemysłowych (na instalacji). Charakteryzuje się większą odpornością na warunki zewnętrzne i zwiększonym poziomem niezawodności działania.

Komputer kompaktowy**) - komputer o zintegrowanych elementach, małej obudowie do montażu na szynie w szafie

Mały system***) - system automatyki, w którym liczba zmiennych procesowych jest mniejsza od 1000.

5.3 Szczegółowe wymogi dla komputerów pracujących w systemach automatyki

Komputery i jego elementy dla systemów automatyki muszą spełniać wymagania oprogramowania, które będzie zainstalowane i używane na danym komputerze. Dobór elementów komputera należy dokonać na podstawie wymogów producenta oprogramowania. Szybkość procesora, wielkość pamięci RAM, pojemność dysków twardych (HDD), moc karty graficznej muszą znacznie przekraczać wymogi oprogramowania dla długiego okresu użytkowania. W przypadku typowych wymagań komputer powinien spełniać je przynajmniej z 20% zapasem, natomiast, gdy podane są tylko minimalne wymagania to należy zastosować sprzęt przynajmniej dwa razy mocniejszy.

Ponadto każdy z komputerów musi być wyposażony w:

- Interfejsy: Ethernet (100Mbps lub więcej) oraz USB (2.0 lub wyższy) lub FireWire (IEEE 1394[1]) wraz z możliwością startu systemu za pośrednictwem jednego z nich,
- Redundantne zasilacze i wentylatory z możliwością wymiany podczas pracy dla ważnych stacji komputerowych i serwerów, gdzie awaria jednego z nich nie ma wpływu na pracę urządzenia,
- Obudowy przemysłowe nadające się do montażu w standardowych szafach 19”; odstępstwo jest możliwe tylko w przypadku komputerów kompaktowych w specjalnych zastosowaniach.

Komputery (także monitory i urządzenia peryferyjne) muszą posiadać znak CE, oznaczający deklarację producenta o spełnieniu wymogów odpowiednich Europejskich Dyrektyw dotyczących bezpieczeństwa użytkowania i ochrony środowiska. Zalecane jest także posiadanie innych oznaczeń bezpieczeństwa (np. TCO, UL, CSA, TUV-GS, SEMKO, GOST, FCC-B, TICK, VCCI-2, MRP).

Dla komputerów a w szczególności dla jego elementów takich jak: zasilacze, twarde dyski, wentylatory dostawca powinien podać wartość MTBF (wymagana wartość powyżej 100 000 godz.).

Komputery muszą posiadać przynajmniej roczną gwarancję od momentu uruchomienia instalacji realizowaną na miejscu (bez konieczności wysyłania sprzętu do dostawcy) i przynajmniej trzyletnią u dostawcy. Dodatkowo w przypadku serwerów dostawca musi posiadać możliwość serwisu 24-godzinnego u klienta. Czas reakcji wraz definicją postępowania, a także maksymalny czas naprawy będą zdefiniowane przez dostawcę i uzgodnione z GLSA. Należy dążyć do zakupów sprzętu u lokalnego dostawcy z szybkim czasem reakcji i lokalnym serwisem.

Komputery pełniące funkcje stacji operatorskiej, inżynierskiej, a także serwery będą zlokalizowane w centralnej sterowni (CR), pokoju inżynierskim (ER) lub ewentualnie innym pomieszczeniu klimatyzowanym.

Dla stacji procesowych (komputery kompaktowe lub przemysłowe-specjalne) zlokalizowanych w pomieszczeniach przemysłowych (bez klimatyzacji), takich jak hale produkcyjne muszą charakteryzować się wykonaniem dla typowo przemysłowych zastosowań, gdzie kluczową rolę odgrywają:

- Niezawodność, niewielkie rozmiary i mały pobór mocy,
- Odpornością na ciepło, wibrację i rozpuszczalniki unoszące się w powietrzu (np. użycie złoconych styków odpornych na korozyjną atmosferę),
- Stopień ochrony przynajmniej IP65 dla szafki, w której zainstalowany jest komputer,

[1]IEEE 1394 A High-Performance Serial Bus - IEEE Computer Society

- Standard ochrony dla użytku w strefie zagrożenia wybuchem (Ex), jeśli pracuje w tej strefie,
- Chłodzenie o dużej wydajności i bezawaryjności (redundancja wentylatorów), jeśli chłodzenie jest wymagane,
- Stosowanie monitorów przeznaczonych do zastosowań w warunkach zakłóceń elektromagnetycznych oraz w trudnych warunkach środowiskowych (pył i wilgoć).

Dla komputerów zlokalizowanych w pomieszczeniach przemysłowych zalecane jest zastosowanie:

- Komputerów bez urządzeń rotujących np. twardych dysków,
- Membranowych klawiatur i dotykowych monitorów LCD przystosowanych do pracy w rękawicach,
- Zasilania prądem 24VDC.

5.4 Ochrona oprogramowania oraz danych komputerowych

Ochrona dla oprogramowania i danych komputerowych dotyczy systemu operacyjnego oraz sterowników dla urządzeń, oprogramowania systemowego, oprogramowania aplikacyjnego, oprogramowania narzędziowego i diagnostycznego, danych procesowych sterowanej instalacji.

W celu zabezpieczenia oprogramowania i danych komputerowych przed awariami sprzętowymi, przypadkowym usunięciem, zainfekowaniem wirusem określa się działania związane z czterema zakresami: zakresy 4.4.1. i 4.4.2 należy dostosować do wymaganego stopnia zabezpieczeń, podczas gdy zakresy 4.4.3. i 4.4.4 należy stosować w każdym przypadku dla wszystkich systemów.

5.4.1 Zabezpieczenie sprzętowe w miejscu powstawania awarii

Zabezpieczenie danych komputerowych poprzez stosowanie redundantnych dysków skonfigurowanych zgodnie z odpowiednim poziomem zabezpieczeń (RAID1, RAID5), redundancję zasilania czy też łączy komunikacyjnych. Zabezpieczenie stosowane dla serwerów oraz ważnych stacji komputerowych, w szczególności, gdy są to stacje pojedyncze.

5.4.2 Redundancja urządzeń komputerowych

Dla stacji komputerowych i serwerów, gdzie wymagany jest wysoki poziom niezawodności stosuje się redundancję, czyli zwielokrotnianie (zwykle podwajanie) identycznych funkcjonalnie jednostek, gdzie awaria jednej jednostki komputerowej nie ma wpływu na drugą. Np. układ dwóch (lub więcej) niezależnych, identycznych funkcjonalnie stacji operatorskich, serwerów, podpiętych do tego samego segmentu sieci komputerowej systemu automatyki.

5.4.3 Ochrona oprogramowania i danych poprzez narzędzia administracyjne

Zawsze wymagana jest ochrona dostępu do systemu komputerowego na różnych poziomach dla użytkowników i dla administratora. Struktura dostępu musi być przedstawiona przez dostawcę i uzgodniona z GLSA.

5.4.4 Wykonywanie kopii bezpieczeństwa dla oprogramowania i danych na zewnętrzne nośniki

Rozróżnia się następujące czynności związane z wykonaniem kopii danych:

- Archiwizacja – po zakończeniu danego etapu pracy dokonuje się archiwizacji danych zakończonej na danym etapie – dotyczy to projektów, analiz, raportów i służy do łatwego odnalezienia zabezpieczonych informacji, lecz nie koniecznie dla odzyskania tych danych w przypadku awarii komputera. Archiwizowanie wykonywane jest rzadko i dane przechowywane są na długi okres czasu (np. kilka lat).

- Back-up (kopia bezpieczeństwa) – dzienna kopia bezpieczeństwa, która służy do przywrócenia komputera do pełnej funkcjonalności po jego awarii – nie służy bezpośrednio do zabezpieczenia informacji, przy czym możemy rozróżnić:
  - Kopię normalną – zawiera wszystkie pliki podlegające kopiowaniu; charakteryzuje się długim czasem kopiowania, dużą zajętością nośnika, wysoką pewnością odzyskania danych z nośnika
  - Kopię różnicową (differential) – w celu odzyskania pełnych danych należy odzyskać dane z ostatniej kopii normalnej, a potem ostatniej kopii różnicowej
  - Kopię przyrostową (incremental) – w celu odzyskania pełnych danych należy odzyskać dane z ostatniej kopii normalnej, a potem w porządku chronologicznym ze wszystkich kopii przyrostowych

Zalecanym sposobem back-up'u ze względu na zajętość nośnika i względnie łatwe odzyskanie danych jest wykonywanie jeden raz w tygodniu kopii normalnej oraz w pozostałych dniach tygodnia kopii różnicowych.

Wykonawca systemu automatyki, w którym wykorzystuje się komputery musi przedstawić procedurę wykonania kopii zapasowej aktualnego stanu komputera, kopii danych oraz procedurę odtworzenia. Istotnym warunkiem pewności wykonywania prawidłowego back-up'u jest okresowe (np. raz na pół roku) odzyskiwanie danych (restore) na zapasowym komputerze i ich pobieżne sprawdzenie.

Oprócz kopii danych komputerowych należy posiadać kopie całości dysku komputera (image), a także nośniki dla systemu operacyjnego i wszystkich zainstalowanych na komputerze programów w wersji instalacyjnej.

Wykonawca systemu automatyki musi dostarczyć procedurę instalacji i konfiguracji oprogramowania na komputerach systemu automatyki. Zainstalowane oprogramowanie musi odpowiadać w ilości jak i w sposobie instalacji, użytkowania związanej z danym oprogramowaniem licencji. Warunki licencji muszą umożliwiać wykonanie przynajmniej jednej kopii zapasowej oprogramowania.

Dla przyśpieszenia działań serwisowych w przypadku awarii, należy posiadać historię napraw komputerów oraz aktualne specyfikacje sprzętowe oraz programów zainstalowanych na każdym komputerze.

5.4.5 Przechowywanie kopii zapasowych i bezpieczeństwa

Zaleca się, aby nośniki oprogramowania instalacyjnego, kopie zapasowe i bezpieczeństwa były składowane w bezpiecznym miejscu, w miarę możliwości w innym pomieszczeniu niż komputery, z których te kopie wykonano.

Zaleca się również dla ważnych danych, aby dzienne kopie bezpieczeństwa były wykonywane na osobnych nośnikach, co ma przeciwdziałać zniszczeniu (np. poprzez uszkodzenie mechaniczne, temperaturowe) kopii z kilku dni. Codzienna wymiana nośnika musi być powiązana z kontrolą komunikatów z wykonania kopii bezpieczeństwa z dnia poprzedniego.

Wymagane jest, aby kopia bezpieczeństwa wykonywana była automatycznie każdego dnia/nocy, przy czym dla danych o mniejszej ważności nośniki muszą być wymieniane przynajmniej jeden raz w tygodniu.

Zaleca się używanie pamięci taśmowych typu DDS (Digital Data Storage) – szerokość 4 mm, a dla większych pojemności (powyżej 10GB) pamięci taśmowych typu DLT (Digital Linear Tape). Pojemność taśmy musi być większa niż objętość kopiowanych danych (z kompresją/bez kompresji danych) podczas jednej sesji back-up'u (dzienna kopia).

System przechowywania kopii bezpieczeństwa powinien umożliwiać odzyskanie danych przynajmniej z każdego z ostatnich 7 dni. Z jednego dnia każdego tygodnia, ostatniego miesiąca oraz

z jednego dnia każdego miesiąca (tzw. procedura: Dziadek-Ojciec-Syn). Odzyskane taśmy będą użyte jako nośniki danych dla kopii bezpieczeństwa w następnych dniach.

Również certyfikat licencji lub inny dokument na podstawie, którego zainstalowano i użytkowane jest oprogramowanie powinien być przechowywany w oddzielnym względem pracujących komputerów automatyki zabezpieczonym miejscu. Hasła administratora muszą być zabezpieczone (np. w zamykanej szafie i zaplombowanej kopercie), lecz w każdym momencie dostępne.

5.5 Prawidłowa zabudowa systemów komputerowych

Stacja operatorska musi być wyposażona w ergonomiczny interfejs (HMI) do wygodnej i bezpiecznej obsługi procesu technologicznego, tzn. monitor ustawiany pod różnymi kątami z regulacją położenia panelu: obrót w prawo, w lewo, pochylenie w pionie, regulację wysokości, a także ergonomiczną klawiaturę i manipulator (preferowany jest trackball).

Miejsce pracy z zabudowaną stacją operatorską musi zostać wykonane zgodnie z zasadami ergonomii dla stanowisk komputerowych (ergonomiczny stół, fotel). Dodatkowo należy odpowiednio zabezpieczyć wszystkie kable prowadzące od szaf z komputerami do stanowisk operatora. Kable należy prowadzić w korytkach i niedopuszczalne jest, aby kable były narażone na łatwe uszkodzenie lub rozłączenie.

Obudowy jednostek centralnych muszą być zamontowane w szafach standardu 19” przeznaczonych do pracy w warunkach przemysłowych (odporne na zapylenie). Wyjątkiem są komputery kompaktowe, które mogą być zamontowane bezpośrednio w szafach systemów automatyki.

Szafy i sposób montażu musi zapewniać prawidłowe odprowadzanie ciepła (wymuszone wentylatorami lub dzięki naturalnej konwekcji). Dostęp do komputerów powinien być chroniony przez drzwiczki zamykane na klucz. Dodatkowo szafa musi posiadać łatwo dostępny i zdejmowany tył lub bok dla celów serwisowych.

Prowadzenie kabli wewnątrz szafy nie może utrudniać montażu czy demontażu komputerów i innych elementów wymagających serwisu. Należy w miarę możliwości odseparować kable zasilające od sygnałowych (prowadzić osobnymi trasami). Wszystkie kable muszą posiadać jednoznacznie identyfikujące je opisy lub oznaczenia.

Wymogi dotyczące lokalizacji i instalacji komputerów muszą być przekazane do GLSA. Instalacja komputerów musi być bezpieczna ze względu na pracę ludzi, systemu automatyki i danych przechowywanych na nich.

5.6 Zasilanie komputerów

Komputery w systemach automatyki zasilane są z bezprzerwowego systemu zasileń UPS.

W przypadku wymagania o wysokiej niezawodności jednostki komputerowej, zasilanie musi być redundowane z dwóch UPS lub, gdy dostępny jest tylko jeden UPS za pomocą dwóch kabli zasilających prowadzonych osobnymi trasami, zabezpieczonych dwoma niezależnymi zabezpieczeniami w szafie zasilania systemu automatyki (za UPS). Wymagane jest, aby redundowane zasilacze miały niezależne gniazda zasilające do zasilania z dwóch niezależnych źródeł.

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.

Wymienia się tutaj głównie normy specyficznie związane z komputerami. Pozostałe normy dotyczące KiA podane są w specyfikacji GLSA 3010 – Ogólne wymagania branży KiA.

7.1 Dyrektywy Wspólnoty Europejskiej

2006/95/WE	Sprzęt elektryczny przewidziany do stosowania w niektórych granicach napięcia (LVD).
2004/108/WE	Kompatybilność elektromagnetyczna (EMC).
93/68/EWG	Oznakowanie CE (Conformance European) – Europejski standard zdrowotny dla ludzi pracujących przy urządzeniach, bezpieczeństwie urządzeń oraz wpływie na otoczenie zapewniające zdrowie pracujących przy urządzeniu ludzi.
94/9/EWG	Urządzenia i systemy ochrony przeznaczone do użytku w przestrzeniach zagrożonych wybuchem (ATEX).

7.2 PN

PN-EN 60950	Bezpieczeństwo urządzeń techniki informatycznej.
PN-EN 55022	Kompatybilność elektromagnetyczna (EMC).Urządzenia informatyczne. Charakterystyki zaburzeń radioelektrycznych. Poziomy dopuszczalne i metody pomiaru.
PN-EN 55024	Kompatybilność elektromagnetyczna (EMC) - Urządzenia informatyczne - Charakterystyki odporności - Poziomy dopuszczalne i metody pomiaru (oryg.).
PN-EN 61000	Kompatybilność elektromagnetyczna (EMC).
PN-EN ISO 9241-302	Ergonomia interakcji człowieka i systemu – Część 302: Terminologia dotycząca monitorów ekranowych elektronicznych (oryg.).
PN-EN ISO 9241-303	Ergonomia interakcji człowieka i systemu. Część 303: Wymagania dotyczące elektronicznych monitorów ekranowych (oryg.).
PN-EN ISO 9241-304 -	Ergonomia interakcji człowieka i systemu – Część 304: Metody badań z zastosowaniem wykonania zadań przez użytkownika (oryg.).
PN-EN ISO 9241-305	Ergonomia interakcji człowieka i systemu – Część 305: Metody laboratoryjnych badań optycznych monitorów ekranowych elektronicznych (oryg.).
PN-EN ISO 9241-307	Ergonomia interakcji człowieka i systemu – Część 307: Analiza i metody badania spełnienia wymagań dotyczących monitorów ekranowych elektronicznych (oryg.).

7.3 Inne normy

TCO, UL, CSA, TUV-GS, SEMKO, GOST, FCC-B, TICK, VCCI-2, MRP – inne narodowe standardy bezpieczeństwa dla urządzeń komputerowych i elektrycznych a w szczególności:

- ISA99: Security for Industrial Automation and Control Systems.
- ISO 27002: Security techniques — Code of practice for information security management.

EPA Energy Star –urządzenia z niskim poziomem zużycia energii.

8 Karta zmian

Lp.	Data	Opis zmian	Zmianę wprowadził
1		Niniejsza specyfikacja zastępuje w całości poprzedni standard Grupy LOTOS S.A. nr PR 07 374 o tym samym tytule	M. Domaniewski
2	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