Spis zawartości

1 Przedmiot specyfikacji 3
2 Zakres obowiązywania 3
2.1 Odstępstwa 3
2.2 Wyłączenia 3
3 Hierarchia dokumentów 3
4 Definicje i oznaczenia 4
5 Opis 8
5.1 Sprawy ogólne 8
5.2 Wymagania odnośnie zgodności projektowania z wymaganiami normy 9
5.2.1 Analiza i koncepcja – projekt bazowy 11
5.2.2 Wykonanie projektu technicznego 14
5.2.3 Montaż i uruchomienie 16
5.3 Techniki wykorzystywane w automatycznych systemach zabezpieczeń 17
5.4 Konfiguracje elementów pomiarowych używanych w funkcjach SIF 18
5.5 Konfiguracje elementów wykonawczych 19
5.6 Wymagania odnośnie urządzeń pomiarowych i wykonawczych 19
5.6.1 Dokumentacja dla urządzeń pomiarowych i wykonawczych będących częściami SIS. 21
5.7 Wymagania odnośnie sterownika programowalnego SIS-PLC 23
5.7.1 Dokumentacja 25
5.7.2 Moduły I/O 25
5.7.3 Jednostka centralna – CPU 26
5.7.4 Oprogramowanie 26
5.7.5 Forsowanie wejść/wyjść, sygnały MOS 27
5.7.6 Połączenia z DCS i innymi systemami 27
5.7.7 Stacja sekwencji zdarzeń (SOER) 28

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

5.7.8 Szafy 28
5.8 Bezpieczeństwo maszyn 28
5.8.1 Wymagania certyfikatu zgodności 28
5.8.2 Bezpieczeństwo urządzeń 29
5.8.2.1 Piece, kotły 29
5.8.2.2 Inne maszyny 29
5.8.2.3 Kryterium porównawcze oceny ryzyka 30
6 Dokumenty związane 30
7 Normy i przepisy 30
7.1 Dyrektywy i Decyzje Wspólnoty Europejskiej 30
7.2 Polskie akty prawne 31
7.3 PN-EN 31
7.4 PN-EN ISO 33
7.5 PN-IEC 33
8 Karta zmian 34

1 Przedmiot specyfikacji

Niniejsza specyfikacja zastosowana w połączeniu z innymi specyfikacjami technicznymi Grupy LOTOS S.A. ustala minimalne wymagania odnośnie projektowania i wykonania automatycznego systemu zabezpieczeń na instalacjach technologicznych, w oparciu o wymagania norm PN-EN 61508 (wszystkie części), PN-EN 61511 (wszystkie części) oraz dyrektywy Rady Europejskiej 96/82/WE (Seveso II) z późniejszymi zmianami M1 do M4.

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.

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

Następujące urządzenia bądź prace związane z przedmiotem niniejszej specyfikacji wchodzą w zakres prac projektowych i dostaw innych branż:

- Identyfikacja zagrożeń i analiza ryzyka - opracowanie technologiczne (na etapie projektu bazowego).
- Specyfikacja wymagań bezpieczeństwa, definicja automatycznych funkcji SIF wraz z określeniem poziomu nienaruszalności bezpieczeństwa SIL - opracowanie technologiczne (na etapie projektu bazowego).

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

TERMINY ZACZERPNIĘTE WPROST Z PN-EN 61508-4. W NAWIASACH [..] DODANO POZANORMATYWNE UWAGI.

Bezpieczeństwo - (Safety) niewystępowanie ryzyka nieakceptowanego.

Bezpieczeństwo funkcjonalne - (Functional Safety) część bezpieczeństwa całkowitego odnosząca się do EUC i systemu sterowania EUC, która zależy od prawidłowego działania systemów E/E/PE związanych z bezpieczeństwem [SIS], systemów związanych z bezpieczeństwem wykonanych w innych technikach i zewnętrznych środków do zmniejszania ryzyka.

Funkcja bezpieczeństwa - (Safety Function) funkcja, do zaimplementowania przez system E/E/PE związany z bezpieczeństwem [SIS], system związany z bezpieczeństwem wykonany w innej technice lub zewnętrzne urządzenie do zmniejszenia ryzyka, której przeznaczeniem jest osiągnięcie lub utrzymanie stanu bezpiecznego EUC, w odniesieniu do konkretnego zdarzenia zagrażającego.

Nienaruszalność bezpieczeństwa - (Safety Integrity) prawdopodobieństwo, że system związany z bezpieczeństwem wykona w sposób zadowalający wymagane funkcje bezpieczeństwa, we wszystkich określonych warunkach i w określonym przedziale czasu.

Ryzyko - (Risk) kombinacja prawdopodobieństwa wystąpienia szkody i ciężkości tej szkody.

Ryzyko tolerowalne - (Tolerable Risk) ryzyko, które jest akceptowalne w określonym kontekście opartym na aktualnych wartościach społecznych.

Rodzaj pracy - (Mode of operation) przewidziany sposób pracy systemu związanego z bezpieczeństwem, odniesiony do częstości przywołań [żądań zadziałania], który może być:

- **Rodzajem pracy na rzadkie przywołanie** (low demand mode)**:** gdy system związany z bezpieczeństwem jest przywoływany nie częściej niż raz na rok i nie częściej niż wynosi dwukrotność testów okresowych.
- **Rodzaj pracy na częste przywołanie lub ciągłe przywołanie** (high demand or continous mode)**:** gdy system związany z bezpieczeństwem jest przywoływany częściej niż raz na rok i częściej niż wynosi dwukrotność testów okresowych.

Weryfikacja - (Verification) potwierdzenie wykonaniem badań i przedstawieniem obiektywnego dowodu, że zostały spełnione wymagania [Daje odpowiedź na pytanie „Czy buduję poprawnie system?”].

Walidacja - (Validation) potwierdzenie badaniem i przedstawieniem obiektywnego dowodu, że zostały spełnione wymagania dotyczące konkretnego zamierzonego użycia [Daje odpowiedź na pytanie: „Czy zbudowano poprawny system?”].

Uszkodzenie - (Failure) utrata zdolności jednostki funkcjonalnej do wypełniania wymaganej funkcji.

Uszkodzenie sprzętu przypadkowe - (Random Hardware Failure) uszkodzenie występujące w przypadkowej chwili i wynikające z co najmniej jednego możliwego mechanizmu powodującego degradację sprzętu Intensywność uszkodzeń sprzętowych da się oszacować z pewną dokładnością. [Dotyczy uszkodzeń, których, źródłem jest defekt sprzętu].

Uszkodzenie systematyczne - (Systematic Failure) uszkodzenie związane w sposób deterministyczny z pewnymi przyczynami, które mogą zostać usunięte tylko przez modyfikację projektu lub procesu wytwarzania, procedur eksploatacyjnych, dokumentacji lub innych odpowiednich czynników. Intensywność występowania tych uszkodzeń nie może być oszacowana. [Dotyczy uszkodzeń, których źródłem jest błędna analiza problemu lub niewłaściwe wykonanie zadania i związane jest bezpośrednio z czynnikiem ludzkim].

Pokrycie diagnostyczne - (Diagnostic Coverage) względne zmniejszenie prawdopodobieństwa niebezpiecznych uszkodzeń sprzętu, wynikające z działania automatycznych testów diagnostycznych [Nie wszystkie uszkodzenia mogą być wykryte przez diagnostykę. Większość uszkodzeń może być jednak wykryta przy okresowych testach sprawdzających].

Osoba niezależna - (Independent Person) osoba oddzielona i odrębna od czynności wykonywanych podczas fazy cyklu życia: całkowitego, E/E/PES lub oprogramowania, będącej przedmiotem oceny lub walidacji bezpieczeństwa funkcjonalnego, i która nie jest odpowiedzialna bezpośrednio za te czynności.

Niezależna organizacja - (Independent Organisation) organizacja oddzielona i odrębna, przez zarządzanie i inne zasoby, od organizacji odpowiedzialnych za czynności wykonywane podczas fazy cyklu życia: całkowitego, E/E/PES lub oprogramowania, będącej przedmiotem oceny lub walidacji bezpieczeństwa funkcjonalnego.

TERMINY INNE

Niezależność - niezależność systemu lub urządzenia oznacza brak możliwości ingerencji w jego działanie poprzez inne systemy lub urządzenia. Nie musi to znaczyć, że brak jest jakichkolwiek powiązań między systemem czy urządzeniem niezależnym a innymi systemami (w szczególności DCS); niezależność w tym wypadku cechuje się brakiem możliwości zmiany funkcji jednostki niezależnej przez czynniki zewnętrzne.

Ochrona dostępu - polega na stosowaniu mechanizmów ograniczenia dostępu, dzięki którym dostęp do systemów (urządzeń) mają tylko osoby o odpowiednich uprawnieniach i jednocześnie przewidziane do pracy z nimi. Rozróżnia się w zależności od aplikacji, różne poziomy dostępu dla różnych osób.

Redundancja - technika zwielokrotniania elementów (lub ich podzespołów) w projektowanej instalacji, stosowana w celu zminimalizowania prawdopodobieństwa postoju instalacji lub nawet jej części wskutek uszkodzenia pojedynczego elementu (dotyczy np. urządzeń pomiarowych oraz wykonawczych automatycznego systemu zabezpieczeń, CPU sterownika, modułów I/O, zasilania, lub innych). Najczęściej spotykanym rozwiązaniem w przypadku urządzeń KiA, jest podwojenie elementów, tak, że w przypadku uszkodzenia urządzenia podstawowego, automatycznie wszelkie zadania przejmuje urządzenie rezerwowe. Co istotne, przełączenie następuje niezauważalnie dla procesu, bez wpływu na funkcjonalność spełnianą przez te elementy. Redundancja w swych sposobach realizacji nie ogranicza się jednak do podwojenia elementów. Znane są rozwiązania z potrojonymi elementami, szczególnie w aplikacjach krytycznych, związanych z bezpieczeństwem. Dodatkowo stosuje się wówczas głosowanie między rezerwującymi się elementami, polegające na odrzuceniu urządzenia, którego działanie pozostaje w sprzeczności z dwoma pozostałymi – zostaje ono przegłosowane.

STOSOWANE AKRONIMY:

GLSA	-	Grupa LOTOS S.A..
KiA		Branża automatyki
CPU	-	moduł jednostki centralnej (Central Processing Unit).
DCS	-	rozproszony komputerowy system sterowania (Distributed Control System).
PLC	-	sterownik programowalny (Programmable Logic Controller).
ESD	-	system blokad użyty do implementacji funkcji bez zdefiniowanego poziomu SIL (Emergency Shut Down system).
I/O	-	wejście/wyjście (Input/Output).
DC	-	napięcie stałe (Direct Current).
AC	-	napięcie przemienne (Alternating Current).
UPS	-	system bezprzerwowego zasilania (Uninterruptible Power Supply).
CR	-	pomieszczenie operatorskie / centralna sterownia (Control Room)
TIR	-	pomieszczenie techniczne automatyki (Technical Instrument Room).
ER	-	pokój stacji inżynierskich (Engineering Room).
SOER	-	stacja sekwencji zdarzeń (Sequence of Events Recorder).

EUC - wyposażenie sterowane (Equipment Under Control) – wyposażenie, maszyny, aparaty lub instalacje stosowane w wytwarzaniu, **procesach**, transporcie, medycynie i w innych dziedzinach działalności.

E/E/PE - Elektryczny / Elektroniczny / Programowalny Elektroniczny (Electrical / Electronic / Programmable Electronic) - oparty na technice elektrycznej (E) i/lub elektronicznej (E) i/lub programowalnej elektronicznej (PE).
Automatyczne systemy zabezpieczeń w normie PN-EN 61508 określane są mianem "E/E/PE safetey related systems".

SIS - system automatyki użyty do implementacji funkcji SIF (Safety Instrumented System).
Mianem SIS określa się w normie PN-EN 61511 automatyczne systemy zabezpieczeń.

SIS-PLC - sterownik PLC, w którym zaimplementowane są funkcje SIF

ESD-PLC - sterownik PLC, w którym zaimplementowane są funkcje bez zdefiniowanego poziomu SIL

SRS - Specyfikacja wymagań bezpieczeństwa (Safety Requirements Specification) – specyfikacja zawierająca wszystkie wymagania dotyczące funkcji bezpieczeństwa, które powinny wypełniać systemy związane z bezpieczeństwem

SIF - Funkcja bezpieczeństwa ze zdefiniowanym poziomem SIL (Safety Instrumented Function).

SIL - Poziom nienaruszalności bezpieczeństwa (Safety Integrity Level) – poziom dyskretny (jeden z czterech możliwych) do wyszczególnienia wymagań nienaruszalności bezpieczeństwa funkcji bezpieczeństwa, które powinny być przypisane w systemach E/E/PE związanych z bezpieczeństwem [SIS], przy czym poziom nienaruszalności bezpieczeństwa 4 jest poziomem najwyższym, a poziom nienaruszalności bezpieczeństwa 1 jest poziomem najniższym.

PFD_{avg} - średnie w określonym czasie prawdopodobieństwo niezdolności do wykonania powierzonej funkcji na żądanie (average Probability of Failure on Demand)

RRF - Współczynnik redukcji ryzyka (Risk Reduction Factor).

SFF - ta część wszystkich przypadkowych uszkodzeń sprzętu tyczących się urządzenia, która skutkuje uszkodzeniami bezpiecznymi lub wykrywanymi uszkodzeniami niebezpiecznymi (Safe Failure Fraction).

CCF - Uszkodzenie spowodowane wspólną przyczyną (Common Cause Failure) - uszkodzenie, które jest wynikiem jednego zdarzenia lub kilku zdarzeń, powodujące jednoczesne uszkodzenie dwóch lub kilku oddzielnych kanałów w systemie wielokanałowym, prowadzące do uszkodzenia systemu. Oznaczany jako β. Stosowany jest przy obliczaniu niezawodności układów redundantnych.

PTI - czas między testami sprawdzającymi (Proof Test Interval).

PTC - Stopień wykrywalności uszkodzeń podczas okresowych testów sprawdzających (Proof Test Coverage).

MTTR - średni czas potrzebny na naprawę urządzenia (Mean Time to Restoration).

MTTFS - Akceptowany czas między nieuzasadnionymi wyłączeniami (Mean Time To Failure Spurious).

MOS - sygnały wyzwalane ręcznie, nadpisujące sygnały blokadowe. Stosowane w celach serwisowych (Maintenance Override Switch).

POS - sygnały wyzwalane ręcznie, nadpisujące sygnały blokadowe. Stosowane w celach technologicznych, np. podczas rozruchu (Process Override Switch).

FAT - zespół testów przeprowadzonych przez kupującego dane urządzenie u producenta urządzenia. Odbywa się po wytworzeniu urządzenia, ale przed jego dostarczeniem na miejsce przeznaczenia.(Factory Acceptance Test).

FSA - Ocena bezpieczeństwa funkcjonalnego (Functional Safety Assessment) - Badanie oparte na dowodach, podjęte w celu oceny bezpieczeństwa funkcjonalnego osiągniętego przez jeden system E/E/PE (lub kilka systemów E/E/PE), związany(-ych) z bezpieczeństwem, systemy związane z bezpieczeństwem wykonane w innych technikach i zewnętrzne środki zmniejszania ryzyka. Ocena ta przeprowadzona jest przez osobę lub organizację niezależną (patrz też PN-EN 61508-1 paragraf 8).

5 Opis

Jednym z priorytetów oraz nakazów, którego przestrzeganie przy projektowaniu, wykonawstwie oraz eksploatacji instalacji jest bezwzględnie wymagane, jest bezpieczeństwo. Niniejsza specyfikacja wskazuje na aspekty bezpieczeństwa oraz związane z nimi stosowne wymagania, do których odwołują się postanowienia międzynarodowego standardu PN-EN 61508 (wszystkie części) oraz jego odmiany dla sektora procesowego PN-EN 61511 (wszystkie części).

Konsekwencją stosowania standardu PN-EN 61508 jest, aby w każdej fazie projektowania, budowy, i uruchamiania jak również pracy i utrzymania instalacji bądź kompleksu instalacji, przestrzegany był zaplanowany system zarządzania bezpieczeństwem. W tym względzie należy zwrócić szczególną uwagę na następujące aspekty:

- **kompetencje** wykonujących przydzielone zadania,
- **dokumentowanie** poszczególnych etapów we wszystkich fazach inwestycyjnych,
- **weryfikację** wykonania postawionych zadań,
- **ocenę** realizacji bezpieczeństwa funkcjonalnego.

Bardziej szczegółowe wytyczne w zakresie technik realizacji powyższych wymagań, zadań stawianych przez zapisy standardu oraz to, w jakim stopniu efekt tych działań wpływa na wymagania stawiane poszczególnym urządzeniom KiA związanych z automatycznym systemem zabezpieczeń, opisano w poniższych paragrafach.

5.1 Sprawy ogólne

Bezpieczeństwo w ujęciu standardu PN-EN 61508, traktowane jest w powiązaniu z możliwymi *zagrożeniami* i odpowiadającymi im *ryzykami* związanymi z pracą instalacji (nie znaczy to jednak, że podczas postoju czy remontu zagrożenia nie występują!). Stąd wymagania, jakie stawia ten standard w zakresie zarządzania bezpieczeństwem mają swoje odniesienie w poziomie ryzyka, a zadania stawiane automatycznemu systemowi zabezpieczeń dotyczą zmniejszenia tego ryzyka do poziomu akceptowalnego. I choć ryzyko poniesienia szkód zgodnie ze standardem dotyczą głównie ludzi, to postępowanie zapewniające bezpieczeństwo wymagane jest również w odniesieniu do mienia oraz środowiska.

W zakresie uregulowań prawnych w odniesieniu do bezpieczeństwa należy przywołać w tym miejscu dyrektywę 96/82/WE „w sprawie kontroli niebezpieczeństwa poważnych awarii związanych z substancjami niebezpiecznymi" (SEVESO II), która stawia sobie za cel „zapobieganie poważnym awariom (...) oraz ograniczenie ich skutków dla ludności i środowiska naturalnego". Intencją wymogu stosowania zasad ujętych w standardzie PN-EN 61508 jest również dostarczenie odpowiedniego materiału do tworzenia wymaganego wspomnianą dyrektywą „sprawozdania o bezpieczeństwie". Sprawozdania, którego poszczególne wymogi wykazują analogie ze standardem PN-EN 61508. W tym względzie należy zatem, odnosząc się do zasadniczych postulatów polityki GLSA w sprawie przeciwdziałania poważnym awariom, traktować standard PN-EN 61508 jako techniczny wyznacznik, dobrą praktykę inżynierską przy przygotowaniu odpowiedniego wkładu do sprawozdania o bezpieczeństwie, ze szczególnym uwzględnieniem automatycznego systemu zabezpieczeń. Działania te powinny być zawsze skoordynowane z branżą technologiczną, uwzględniając przy tym specyfikację GLSA 1170 w przedmiotowym zakresie.

Pracując w oparciu o standard PN-EN 61508, identyfikację potencjalnych zagrożeń winno się traktować jako szeroko pojętą analizę, miejscami wykraczającą poza zakres dyrektywy SEVESO II. Bezpieczeństwo, należy odnieść nie tylko do ludzi i środowiska, ale również do mienia. Źródeł zagrożeń należy szukać i identyfikować we właściwie zdefiniowanym i uwarunkowanym obiekcie (uwzględniając np. otoczenie), nie ograniczając niebezpieczeństw jedynie do tych z udziałem substancji uznanych za niebezpieczne.

Wymaga się, aby przy podejściu do bezpieczeństwa stosować zasadę zmniejszenia ryzyka poprzez zapobieganie (niedopuszczanie) powstaniu groźnych zdarzeń a nie jedynie poprzez stosowanie środków minimalizujących skutki awarii (te, nie są przedmiotem niniejszej specyfikacji).

5.2 Wymagania odnośnie zgodności projektowania z wymaganiami normy

PN-EN 61508 (wszystkie części) i PN-EN 61511 (wszystkie części)

W ujęciu normy PN-EN 61508 i PN-EN 61511 bezpieczeństwo funkcjonalne instalacji osiąga się poprzez ukierunkowane działania na wszystkich etapach „życia" instalacji tzn. od koncepcji przez projekt bazowy, projekt techniczny, wykonanie i eksploatację do ostatecznego demontażu- likwidacji instalacji.

Można wydzielić trzy fazy cyklu życia instalacji.

- Analiza i koncepcja –projekt bazowy,
- Wykonanie projektu technicznego,
- Montaż i uruchomienie instalacji.

Każda faza życia instalacji może być dalej podzielona na etapy, w których wykonuje się określone prace związane z wprowadzaniem bądź utrzymaniem bezpieczeństwa.

Na schematach 1, 2 i 3 przedstawiono charakterystyczne etapy działań dla każdej fazy.

Uwaga:

Poniżej po opisie każdego z etapów prac pojawia się paragraf Dokumentacja. Zawiera on informacje nt. wymaganej przez Grupę Lotos S.A. dokumentacji (zestawu dokumentów), która musi być dostarczona przez odpowiedzialną za dany etap organizację.

Oprócz tego równolegle z tymi fazami wykonawcy - organizacje odpowiedzialne za dany etap prac lub jego część(podwykonawcy) muszą przeprowadzić działania dodatkowe takie jak:

- Zarządzać bezpieczeństwem zgodnie z wytycznymi podanymi w PN-EN 61508-1 paragraf 6 lub PN-EN 61511-1 paragraf 5.
  Dokumentacja:
  Odpowiedni dla danego etapu prac raport potwierdzający wypełnienie wymagań podanych w PN-EN 61508-1 paragraf 6 lub w PN-EN 61511-1 paragraf 5 wykonany przez odpowiedzialną za dany etap organizację.
- Zapewnić techniki i środki do unikania i kontroli uszkodzeń systematycznych adekwatne do wymaganego poziomu SIL zgodnie z wytycznymi podanymi w PN-EN 61508-2 Aneks A i B.
  Dokumentacja:
  Odpowiedni dla danego etapu prac raport potwierdzający wypełnienie wymagań podanych w PN-EN 61508-2 Aneks A i B wykonany przez odpowiedzialną za dany etap organizację.
- Stworzyć „Plan działań bezpieczeństwa" (Safety Plan) określający niezbędne działania do wykonania wraz z przypisaniem do nich osób-grup odpowiedzialnych za dane zadanie. Plan powinien być dokumentem na bieżąco aktualizowanym przechowywanym przez cały okres życia instalacji. Szczegółowe wytyczne można znaleźć w PN-EN 61511-1 paragraf 6 lub PN-EN 61508-1 paragraf 7.
  Dokumentacja:
  "Plan działań bezpieczeństwa" wg wytycznych zawartych w PN-EN 61511-1 paragraf 6 lub PN-EN 61508-1: paragraf 7.
- Organizować regularne wewnątrzorganizacyjne audyty bezpieczeństwa, przeglądy podejmowanych działań i wprowadzanych rewizji/modyfikacji, podczas całego cyklu życia instalacji, poczynając od projektu bazowego Do tego celu powinien być powołany dedykowany zespół ludzi posiadający odpowiednie kwalifikacje i doświadczenie właściwe dla danego typu instalacji.
- Wykonać ocenę bezpieczeństwa funkcjonalnego (FSA) prowadzoną przez zewnętrzną organizację lub osobę niezależną (Functional Safety Assessment) po następujących etapach:
  - Ocena ryzyka, alokacja funkcji bezpieczeństwa stworzenie specyfikacji bezpieczeństwa SRS,
  - Po etapie projektu technicznego,
  - Instalacja urządzeń SIS i sprawdzenie poprawności ich konfiguracji i działania (pre-commissioning),
  - Po modyfikacjach i przed demontażem SIS,

  Dokładne wytyczne na temat „Functional Safety Assessment" można znaleźć w PN-EN 61508-1: paragraf 8.

  Dokumentacja:

  1. Potwierdzenie wykonania oceny bezpieczeństwa funkcjonalnego (FSA) (jeśli wymagane dla danego etapu prac).
  2. Na żądanie GLSA potwierdzenie przeprowadzonych audytów wewnętrznych.
  3. Na żądanie GLSA potwierdzenie kompetencji osób związanych z bezpieczeństwem funkcjonalnym.

5.2.1 Analiza i koncepcja – projekt bazowy

Grupa Lotos S.A weryfikuje założenia, wymagania i obostrzenia wynikające z projektu bazowego lub opracowania wykonanego przez rzeczoznawcę w stosunku do nowoprojektowanej instalacji takie jak:

- Definicja szkody - tzn. określenie czy wytyczne normy PN-EN61508 mają służyć ochronie życia ludzkiego czy ochronie majątku trwałego czy może ochronie środowiska. Możliwe jest także połączenie kilku aspektów równocześnie.
- Przy kryterium ochrony życia: Ilość osób w miejscu zagrożenia, czas przebywania, środki ochrony przed urazami.
- Przy kryterium ochrony majątku: Wielkość strat produkcji, wielkość strat wyposażenia.
- Przy kryterium ochrony środowiska: Rodzaj zagrożenia i jego skutki.
- Akceptowane metody oceny ryzyka.
- Ryzyko tolerowalne.
- Zakładany czas życia instalacji.
- Czas przywrócenia instalacji do ruchu po jej zatrzymaniu.
- Akceptowany czas między nieuzasadnionymi wyłączeniami (MTTFS).
- Dla czujników, systemu kontroli (SIS-PLC) i elementów wykonawczych -czas między testami sprawdzającymi (PTI), Stopień wykrywalności testów (PTC) i czas naprawy (MTTR). Należy przyjąć, że okresowe testy sprawdzające wykonywane będą podczas postoju instalacji. W związku z tym, czas pomiędzy testami okresowymi dla urządzeń pomiarowych, wykonawczych oraz SIS-PLC będzie nie krótszy niż projektowany okres międzypostojowy instalacji powiększony o 50%. W przypadku SIF oraz związanych z nimi urządzeń pomiarowych i wykonawczych, dla których wykonalne są okresowe testy sprawdzające on-line (bez zakłócania normalnej pracy instalacji), czas pomiędzy tymi testami może zostać skrócony, po uzgodnieniu z GLSA.

Wszystkie założenia przyjęte do obliczeń muszą być zawsze przedstawione do akceptacji GLSA.

Przy tworzeniu systemów bezpieczeństwa należy kierować się poniższymi wskazaniami:

- Należy wzorować się na istniejących poprawnych rozwiązaniach analogicznych procesów i poprzednich rozwiązaniach,
- Norma PN-EN 61508/PN-EN 61511 nie zwalnia od działań „dobrej praktyki inżynierskiej”,
- Należy pamiętać, że bezpieczeństwo nie jest tylko osiągane przez ustanowienie automatycznych systemów bezpieczeństwa, lecz także poprzez właściwy system organizacji pracy i kontroli uszkodzeń.

Na etapie projektu bazowego należy przeprowadzić identyfikację zagrożeń i analizę istniejącego ryzyka, której celem jest:

- rozpoznanie zagrożeń i ich skutków,
- oszacowanie prawdopodobieństwa zagrożeń,
- oszacowanie wymaganej redukcji ryzyka,

- ocena czy zastosowane zabezpieczenia technologiczne, mechaniczne i inne oprócz funkcji bezpieczeństwa realizowanych przez elementy automatyki są wystarczające a jeśli nie to:
  - stworzenie funkcji zabezpieczających realizowanych przez systemy E/E/PE redukujących ryzyko do poziomu ryzyka akceptowanego i wydzielenie z nich funkcji SIF,
  - zdefiniowanie dla funkcji SIF wymagań w SRS pozwalających na osiągnięcie ryzyka tolerowalnego.

Należy starać się, aby instalacja była bezpieczna sama w sobie tzn. aby nie wymagała dodatkowych warstw ochrony. Jeśli nie jest to możliwe należy stosować mechaniczne zabezpieczenia np. zawory bezpieczeństwa (PSV) a jeśli i to jest niewystarczające należy stosować funkcje realizowane przez systemy E/E/PE.

Rozpoznanie zagrożeń wynikających z normalnie działającej instalacji jest niewystarczające, dlatego konieczne jest zatrudnienie do tej analizy fachowców specjalizujących się w bezpieczeństwie instalacji danego typu.

Szczegółowe wymagania odnośnie analizy zagrożeń przedstawione są w PN-EN61511-1 paragraf 8.

Specyfikacja wymagań SRS musi zawierać dla każdej funkcji:

- Dokładny opis każdej funkcji(definicja wejścia i wyjścia),
- Definicja zakresu wartości pomiarowych i wartości, przy których następuje wyzwolenie logiki,
- Wymagania dla elementów wykonawczych takie jak Tight Shut-Off,
- Definicja logiki zastosowanej w sterowniku i wymagań co do oprogramowania,
- Definicja stanu bezpiecznego,
- Tryb pracy (Low Demand/ High Demand),
- Definicja wymaganego poziomu bezpieczeństwa SIL i współczynnik redukcji ryzyka RRF(lub PFD_{avg}),
- Okresy testów sprawdzających dla czujników, sterownika i elementów wykonawczych,
- Wymagany czas odpowiedzi-wykonania funkcji bezpieczeństwa,
- Czas wymiany uszkodzonych elementów(zgodnie z założeniami Grupy Lotos S.A.),
- Wymagania środowiskowe, które mogą wpłynąć na działanie funkcji,
- Metoda wyzwolenia funkcji Energized /De-energized to trip,
- Metody kasowania–reset jeśli występuje,
- Wymagany minimalny czas między nieuzasadnionymi wyłączeniami(zgodnie z założeniami Grupy Lotos S.A.),
- Opis zastosowanej diagnostyki jeśli występuje,
- Czy jest możliwe ręczne wyzwolenie funkcji?,
- Użycie MOS, POS dla funkcji,
- Zachowanie funkcji przy braku energii,
- Wymagania dla operatora,
- Powiązania z innymi systemami,

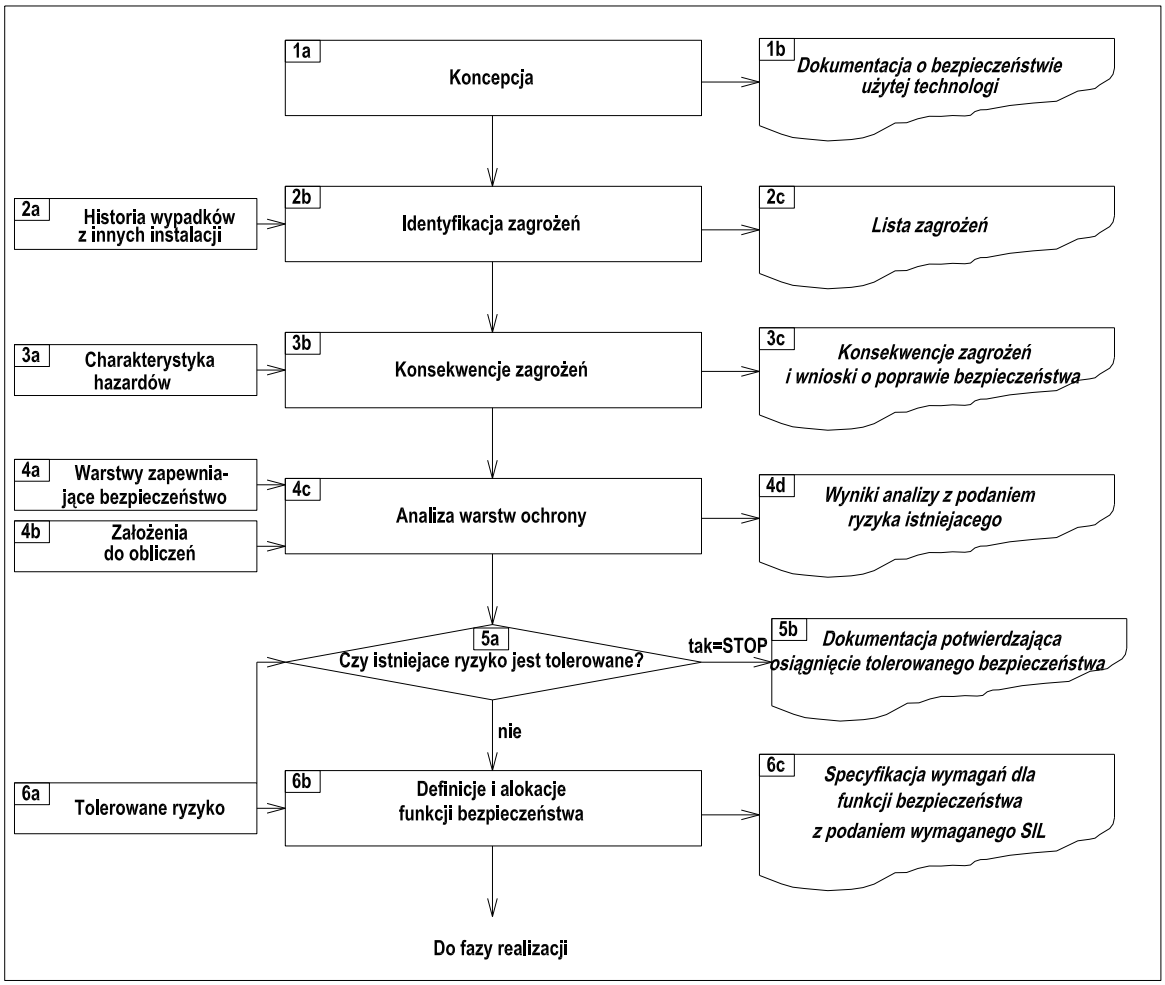
- Sposób działania operatora w przypadku zauważenia błędów w działaniu funkcji,
- Inne, które wpływają na działanie funkcji SIF.

Detaliczne wskazania na temat specyfikacji wymagań SRS znajdują się w PN-EN 61511-1 paragraf 10.3

Dokumentacja:

- Opis zastosowanej w projekcie bazowym technologii działania instalacji ze szczególnym uwzględnieniem aspektów bezpieczeństwa.
- Pełny raport oraz wyniki analizy zagrożeń i ryzyka wraz z przypisanymi funkcjami zabezpieczającymi SIF i wymaganym od nich RRF lub PFD_{avg}.
- Specyfikacja wymagań SRS.

Schemat działań właściwych dla fazy analizy bezpieczeństwa i koncepcji działania został przedstawiony na schemacie 1.



Schemat 1 Faza- Analiza i koncepcja –projekt bazowy

5.2.2 Wykonanie projektu technicznego

Każda z funkcji bezpieczeństwa musi mieć obliczony - wymagany od niej współczynnik redukcji ryzyka RRF lub PFD_{avg}.

Te funkcje bezpieczeństwa, których RRF jest większy lub równy 10 „stają się" funkcjami SIF ze zdefiniowanym poziomem SIL i tylko one są przedmiotem wymagań normy PN-EN 61508 i 61511. Funkcje te należy implementować w systemie SIS-PLC.

Funkcje, dla których obliczony RRF jest mniejszy niż 10 są funkcjami, które nie podlegają wymaganiom normy PN-EN 61508 i 61511. Funkcje te należy implementować w systemie ESD-PLC lub zostawić w systemie przeznaczonym dla funkcji SIF licząc się jednak z tym, że będą je obowiązywać takie same obostrzenia i wymagania, jakie nakładają normy PN-EN 61508 i 61511dla funkcji SIF.

Urządzenia wchodzące w skład funkcji bezpieczeństwa SIF muszą mieć zbadaną przez producenta niezawodność działania i potwierdzoną odpowiednimi dokumentami (patrz punkt 5.6 i 5.7). Proces weryfikacji funkcji SIF z wymaganiami postawionymi w SRS i założeniami Grupy Lotos S.A. daje wytyczne co do wymaganego rodzaju, niezawodności i architektury elementów funkcji SIF. Pierwotnie ustalona konfiguracja urządzeń funkcji SIF może zostać zmieniona tak, aby spełnić wymagania SRS (np. zmiana jednego przetwornika na dwa w konfiguracji 1oo2). Pokazane to jest na schemacie 2 blok 8a.

Proces weryfikacji musi być udokumentowany.

Wyniki procesu weryfikacji mogą powodować zmiany w szeregu dokumentów związanych, np Cause and Effect Diagram, specyfikacje techniczne, schematy technologiczne, instrukcje obsługi instalacji i inne. Należy zadbać o to, aby wszystkie zmiany i wymagania co do własności urządzeń i ich późniejszej eksploatacji znalazły odbicie w stosownych dokumentach i nie zostały przeoczone.

Podczas fazy projektu technicznego musi być też wykonany proces weryfikacji projektu HAZOP gdyż projektowanie według wytycznych PN-EN 61508/ PN-EN 61511 nie zwalnia od stosowania technik eksperckich.

Dokumentacja finalna musi zawierać wszystkie dane o niezawodności urządzeń, certyfikaty i inne założenia wykorzystane przy obliczeniach.

Jeśli jest to konieczne muszą zostać utworzone dodatkowe dokumenty zawierające informacje związane z osiągnięciem i utrzymaniem wymaganego poziomu bezpieczeństwa. Mogą znaleźć się tam wymagania co do montażu i eksploatacji oraz demontażu urządzeń SIS.

Po zakończeniu fazy projektowania należy przeprowadzić walidację prac projektowych oraz zlecić ocenę bezpieczeństwa funkcjonalnego wykonaną przez osobę lub organizację niezależną. Dokładne wytyczne na temat „Functional Safety Assessment" można znaleźć w PN-EN 61508-1 paragraf 8.

Po zakończeniu etapu projektowania instalacji główny wykonawca projektu powinien stworzyć dokument - przewodnik, który porządkuje wszystkie dokumenty (również te utworzone przez podwykonawców) w jeden pakiet dokumentacji o bezpieczeństwie funkcjonalnym instalacji.

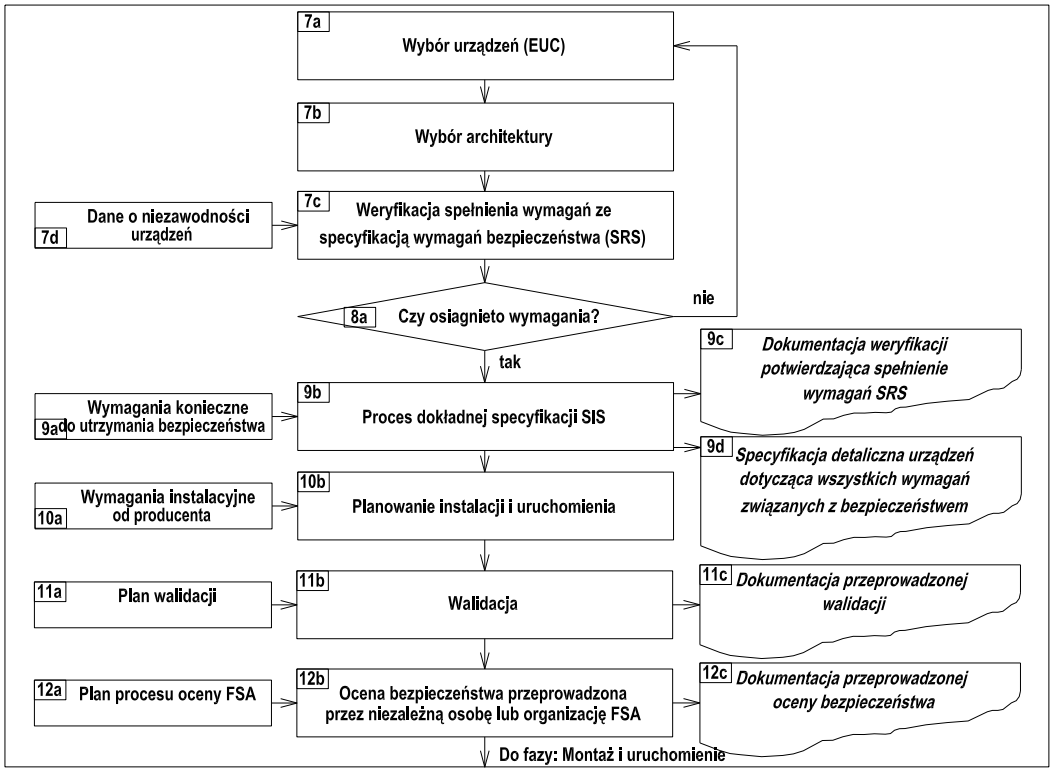
Wyżej wspomniany dokument przewodni powinien służyć jako klucz do wszystkich dokumentów związanych z bezpieczeństwem. Znaczy to, że wymagania do zapewnienia bezpieczeństwa funkcjonalnego znajdują się tylko w nim i dokumentach przez niego powołanych i nigdzie więcej.

Wyżej wspomniany dokument przewodni i dokumenty w nim powołane tworzą pakiet dokumentujący Grupie Lotos S.A. zgodność projektu z wymaganiami normy PN-EN 61508 i PN-EN 61511.

Dokumentacja:

- Dokumentacja przeprowadzonej weryfikacji.
- Umieszczenie informacji związanych z bezpieczeństwem we wszystkich stosownych dokumentach.
- Dokumentacja założeń do obliczeń (certyfikaty, warunki ważności certyfikatów).
- Dokumentacja wymagań związanych z osiągnięciem i utrzymaniem bezpieczeństwa.
- Utworzenie dokumentu przewodniego do wszystkich dokumentów związanych z bezpieczeństwem.
- Potwierdzenie przeprowadzonej walidacji.
- Potwierdzenie przeprowadzonej oceny przez organizację niezależną.

Faza związana z wykonaniem projektu została zobrazowana na schemacie 2



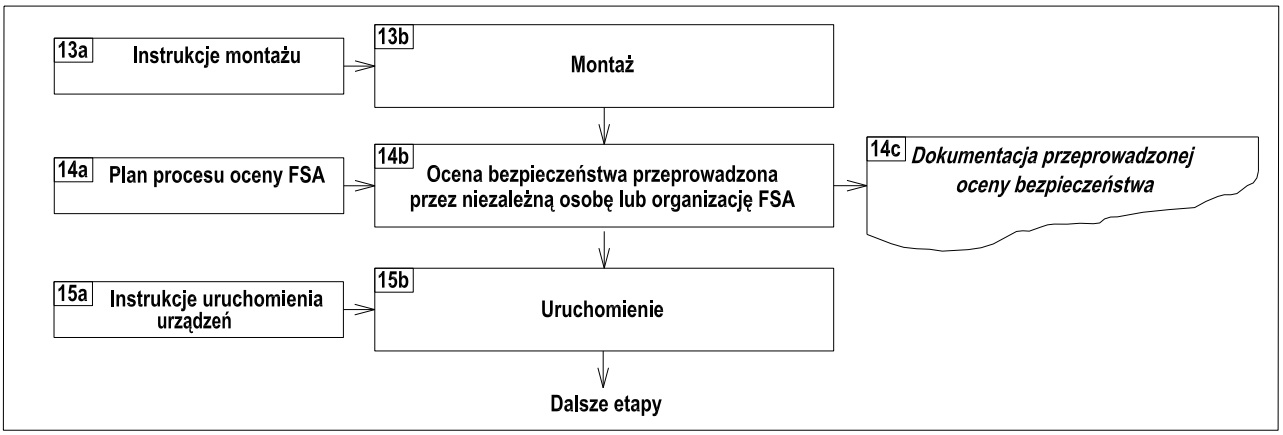
Schemat 2- Faza- wykonanie projektu technicznego

5.2.3 Montaż i uruchomienie

Projekt techniczny powinien być zakończony testami FAT. Wymagania odnośnie testów zostały przedstawione w PN-EN 61511-1 paragraf 13.

Po montażu urządzeń na instalacji a przed jej uruchomieniem osoba lub organizacja niezależna (patrz PN-EN 61508-1 paragraf 8. a także PN-EN 61511-1 paragraf 15) musi przeprowadzić ocenę systemu SIS. Działanie to polega na sprawdzeniu m.in. prawidłowości montażu urządzeń, ich połączeń, sposobu oznaczeń, wartości progów wyzwalających działanie funkcji SIF, wymaganych czasów działania poszczególnych funkcji SIF, poprawności ich działania i innych wymagań zawartych w pakiecie dokumentacji bezpieczeństwa. Powinien zostać wydany odpowiedni dokument potwierdzający wykonanie sprawdzenia i ocenę.

Dopiero po pozytywnej ocenie FSA i usunięciu ewentualnych niezgodności można przejść do etapu uruchomienia instalacji.



Schemat 3 – Faza - montaż i uruchomienie

Pozostałe etapy takie jak eksploatacja, utrzymanie w ruchu instalacji, modyfikacje funkcji SIF i ich demontaż nie są przedmiotem tej specyfikacji.

5.3 Techniki wykorzystywane w automatycznych systemach zabezpieczeń

Dla poszczególnych elementów systemu należy stosować ogólnie znane i akceptowane techniki (sposoby realizacji, własności urządzeń), które pomagają a niekiedy stanowią wymóg zasadniczy przy realizacji automatycznych systemów zabezpieczeń. Poniżej wymieniono kilka z nich, którymi należy się kierować przy projekcie, specyfikacji oraz konstrukcji:

FAIL SAFE – termin należy odnosić do wszelkich urządzeń KiA związanych z automatycznymi systemami zabezpieczającymi tak w zakresie oprogramowania jak i sprzętu i polega na przejściu elementu-urządzenia do właściwego dla danego przypadku stanu bezpiecznego w razie awarii. Pojęcie awarii zależy od konkretnego przypadku np. dla zaworu oznacza to, że w razie braku powietrza zasilającego lub zerwania połączeń elektrycznych zawór przechodzi pod wpływem sprężyny do zdefiniowanej pozycji bezpiecznej. Przykłady patrz punkt 5.6 i 5.7

FAULT TOLERANCE – zgodnie z normą PN-EN 61508, zdolność układu funkcjonalnego do kontynuacji wykonywania wymaganej funkcji (spełniania powierzonych zadań), przy obecności defektów (faults) lub błędów (errors).Z pojęciem FAULT TOLERANCE wiąże się znana i szeroko stosowana REDUNDANCJA (nadmiarowość) oraz VOTING (głosowanie). Jako przykład można tu podać układ funkcjonalny służący do pomiaru parametru technologicznego z głosowaniem ‘2oo3’. Zastosowano tu trzy REDUNDANTNE elementy z VOTINGIEM (funkcja jest realizowana, gdy co najmniej dwa czujniki wskazują taką konieczność), natomiast FAULT TOLERANCE układu wynosi jeden (funkcja będzie realizowana prawidłowo w przypadku uszkodzenia nie więcej jak jednego czujnika).

DIAGNOSTYKA – jako cecha lub mechanizm sprawdzający prawidłowość działania urządzenia bądź oprogramowania, jest zalecaną techniką w odniesieniu do poszczególnych urządzeń jak również systemu, który tworzą. Diagnostyka urządzeń oraz implementacja mechanizmów wykrywających defekty układu funkcjonalnego pozwala skuteczniej i bardziej efektywnie realizować automatyczne systemy zabezpieczające. Sygnały diagnostyczne należy najpierw uzyskać (odczytać, zinterpretować) a potem właściwe wykorzystać w zamierzonym celu. Istotnym parametrem w odniesieniu do diagnostyki urządzenia, jest tzw. DIAGNOSTIC COVERAGE, informujący o tym jaki procent uszkodzeń jest wykrywany. Jest kilka rodzajów diagnostyk np. diagnostyka wykonywana przez urządzenie wewnętrznie czyli samokontrola, diagnostyka wykonywana przez urządzenie na żądanie (np. test zaworu- Partial Stroke Test) lub diagnostyka na warsztacie po wcześniejszym demontażu urządzenia.

DYWERSYFIKACJA – jest metodą stosowaną przy urządzeniach redundowanych polegającą na różnicowaniu rodzajów środków dla osiągnięcia tego samego celu. Przykładem może być stosowanie dwóch różnych (w dużym stopniu wzajemnie NIEZALEŻNYCH) rodzajów przetworników służących do pomiaru parametru technologicznego pracujących w układzie głosowania 1oo2. Może to być też stosowanie przetworników różnych producentów lub opartych na różnych metodach pomiaru mierzących to samo i użytych w jednej funkcji bezpieczeństwa. Innym, praktycznym sposobem różnicowania w doborze środków, jest realizacja dwutorowego odłączenia (np. od przycisku): poprzez ESD-PLC oraz niezależną drogą np. poprzez przekaźniki ze stykami pomocniczymi włączonymi odpowiednio w obwody sterowania czy zasilania wszelkich związanych urządzeń wykonawczych. Stosowanie urządzeń różnych typów może poprawić kilkakrotnie niezawodność całego układu.

5.4 Konfiguracje elementów pomiarowych używanych w funkcjach SIF

Poniżej przedstawiono rozumienie wg PN-EN 61508 najczęściej stosowanych konfiguracji elementów pomiarowych w funkcjach SIF:

Głosowanie 1oo1
Architektura zawiera pojedynczy kanał gdzie każde uszkodzenie niebezpieczne kanału (λ_D) powoduje niewykonanie funkcji SIF, na zgłoszone żądanie – funkcja traci w takim przypadku zdolność do wykonania powierzonego zadania.

Głosowanie 1oo1D
Architektura zawiera pojedynczy kanał gdzie część uszkodzeń niebezpiecznych(λ_{DD}) jest wykrywana przez diagnostykę. Ma tą zaletę nad 1oo1, że w przypadku wykrycia uszkodzenia niebezpiecznego przez diagnostykę układ przechodzi do stanu bezpiecznego przez co niezawodność układu jest większa niż w konfiguracji 1oo1. Urządzenia te mają przeważnie osobne wyjście do sygnalizacji wyników diagnostyki.

Głosowanie 1oo2
Architektura zawiera dwa kanały połączone tak, że każdy z nich może wykonywać funkcję SIF. Stąd wynika, że równocześnie dwa kanały muszą być uszkodzone aby funkcja nie została wykonana. Jeśli jest jakakolwiek diagnostyka to wyniki jej są tyko raportowane bez wpływu na stan wyjścia czy głosowania.

Głosowanie 1oo2D
Architektura zawiera dwa kanały połączone tak, że podczas normalnej pracy oba kanały muszą żądać wykonania funkcji SIF aby została wykonana. Dodatkowo jeżeli diagnostyka w jakimkolwiek kanale wykryje uszkodzenie tego kanału wtedy głosowanie jest modyfikowane w ten sposób, że wyjście układu zależy tylko od stanu drugiego pracującego poprawnie kanału. Jeśli diagnostyka wskaże uszkodzenie w obu kanałach lub rozbieżność między nimi, której nie można przypisać do konkretnego kanału wtedy wyjście układu jest ustawiane w stan bezpieczny. Rozbieżność między kanałami musi być wykrywana środkami niezależnymi od działania tych kanałów.

Głosowanie 2oo2
Architektura zawiera dwa kanały połączone tak, że oba kanały muszą żądać wykonania funkcji zanim zostanie ona wykonana. Jeśli jest jakakolwiek diagnostyka to wyniki jej są tyko raportowane bez wpływu na stan wyjścia czy głosowania.

Głosowanie 2oo3
Architektura zawiera trzy kanały połączone równolegle w większościowym głosowaniem pomiędzy wejściami tak, że sygnał wyjściowy nie zmienia się jeżeli tylko jeden kanał daje sygnał żądający wykonanie funkcji SIF co jest w sprzeczności z dwoma pozostałymi które żądania nie zgłaszają. Aby zainicjalizować wykonanie funkcji przynajmniej dwa kanały muszą żądać jej wykonania. Jeśli jest jakakolwiek diagnostyka to wyniki jej są tyko raportowane bez wpływu na stan wyjścia czy głosowania.

Głosowanie NooM
Architektura zawiera M kanałów połączonych tak, że N kanałów musi żądać wykonania funkcji zanim zostanie ona wykonana. Jeśli jest jakakolwiek diagnostyka to wyniki jej są tyko raportowane bez wpływu na stan wyjścia czy głosowania.

5.5 Konfiguracje elementów wykonawczych

Poniżej przedstawiono rozumienie wg PN-EN 61508 najczęściej stosowanych konfiguracji elementów wykonawczych

Głosowanie 1oo1

Architektura zawiera pojedynczy element wykonawczy gdzie każde uszkodzenie niebezpieczne (λ_D) powoduje niewykonanie funkcji SIF.

Głosowanie 1oo2

Architektura zawiera dwa elementy wykonawcze połączone tak, że każdy z nich może wykonywać funkcję SIF. Wynika stąd, że aby funkcja SIF nie została wykonana, równocześnie dwa elementy wykonawcze muszą nie zadziałać.

Głosowanie 2oo2

Architektura zawiera dwa elementy wykonawcze połączone tak, że oba muszą zadziałać prawidłowo, aby funkcja SIF została wykonana. Wynika stąd, że wystarczy uszkodzenie jednego elementu wykonawczego aby funkcja nie została wykonana.

Głosowanie NooM

Architektura zawiera M elementów wykonawczych połączone tak, że N elementów musi zadziałać prawidłowo aby funkcja SIF została wykonana.

5.6 Wymagania odnośnie urządzeń pomiarowych i wykonawczych

Zakres aparatury KiA dla potrzeb automatycznego systemu zabezpieczeń, wynika bezpośrednio z projektu detalicznego SIS, pozostającego w zgodności z postawionymi wymaganiami bezpieczeństwa w SRS. Oznacza to, że na tym etapie znane są poszczególne elementy systemu SIS (jak np. przetworniki ciśnienia, zawory blokadowe), ich ilość, konfiguracja oraz detaliczne wymagania co do ich wymaganej niezawodności.

Elementy funkcji SIF muszą być szczególnie odporne na zakłócenia takie jak: elektromagnetyczne, wibracji i eksploatacji właściwe dla miejsca montażu. Należy zwrócić uwagę aby elementy funkcji SIF nie pracowały przy swoich granicznych parametrach takich jak prąd, napięcie i warunki środowiskowe (należy zachować odpowiedni margines bezpieczeństwa).

W przypadku nadmiernego nasłonecznienia w miejscu montażu urządzenia należy stosować daszki ochronne a klasa obudowy IP musi być dobierana z marginesem bezpieczeństwa.

Konstrukcje elementów pomiarowych i wykonawczych muszą być wytrzymałe pod względem mechanicznym (przypadkowe zawadzenie o te urządzenia nie może powodować ich uszkodzenia).

Przetworniki nie mogą pracować ani blisko początku ani blisko końca zakresu pomiarowego.

Urządzenia będące częściami funkcji SIF nie mogą być wykorzystywane do pełnienia innych funkcji niż SIF. Zabronione jest użycie elementu w systemie SIS oraz dla potrzeb jakichkolwiek funkcji w innym systemie. Wymaganie to dotyczy również poboru impulsu pomiarowego jak i trasę od miesca poboru do przetwornika.

Każdy element pomiarowy, wykonawczy lub pośredniczący (np. bariera) powinien być dostosowany do wymaganego poziomu bezpieczeństwa SIL. Dopasowanie to polega na:

1. Zastosowaniu elementu o wymaganej gwarantowanej niezawodności (dokumentacja patrz pkt. 5.6.1),
2. Zastosowanie odpowiedniego do SIL stopnia redundancji urządzeń wg PN-EN 61508-2 7.4.3 Tabela 2 lub Tabela 3 lub PN-EN 61511-1 11.4 tabela 6
   Odnośnie redundancji urządzeń, należy uwzględnić zalecenia paragrafu 5.7.5
3. Stosowanie odpowiedniej dla wymaganego poziomu SIL kontroli uszkodzeń systematycznych (patrz punkt 5.2)

Preferowanym rozwiązaniem jest stosowanie urządzeń pomiarowych oraz wykonawczych, posiadających certyfikat zgodności z PN-EN 61508.

Urządzenia nie-elektryczne takie jak np. zawór pneumatyczny, pomimo iż nie podlegają wprost restrykcjom standardu PN-EN 61508 muszą również być produktem certyfikowanym (gdyż niezawodność działania zdefiniowanej funkcji SIF, do której zawory te przynależą opiera się w dużej mierze o niezawodność działania tego zaworu).

W funkcjach SIF preferuje się stosowanie przetworników ze względu na większą niezawodność i większe możliwości detekcji błędów przetworników w odróżnieniu od sygnalizatorów. Dodatkowo przemawia za tym fakt, że większość (na czas pisania niniejszej specyfikacji) urządzeń pomiarowych certyfikowanych to przetworniki.

Wszystkie urządzenia muszą pracować jako FAIL SAFE.

Dla elementów pomiarowych w przypadku braku energii elektrycznej sygnał wyjściowy z przetwornika (lub sygnalizatora) powinien być niski podobnie jak ma to miejsce przy zerwaniu ciągłości okablowania.

W przypadku sygnalizatorów, zaleca się stosowanie sygnalizatorów zbliżeniowych, zgodnych ze standardem PN-EN 60947-5-6 (NAMUR).

Jeżeli stosowane są sygnalizatory ze stykiem beznapięciowym, należy dobierać urządzenia posiadające certyfikat zgodności z PN-EN 61508.

Dla urządzeń wykonawczych w przypadku niskiego stanu sygnału sterującego lub przerwania ciągłości połączeń element wykonawczy powinien samoczynnie i bez energii z zewnątrz przejść do stanu bezpiecznego dla instalacji „de-energize to trip". Dotyczy to zarówno braku zasilania energią elektryczną jak i zasilania pneumatycznego czy hydraulicznego.

Interfejsy urządzeń pomiarowych i wykonawczych używanych w funkcjach SIF muszą być zabezpieczone przed zmianą parametrów przez osoby niepowołane. Zmiana jakichkolwiek parametrów dla tych urządzeń musi odbywać się zgodnie z obowiązującą w tym względzie procedurą GLSA oraz wiąże się z koniecznością przestrzegania zasad modyfikacji SIS opisanych w normach PN-EN 61508/61511.

Zmiana parametrów kluczowych dla bezpieczeństwa urządzeń może być przeprowadzona tylko przez osoby odpowiedzialne za bezpieczeństwo funkcjonalne w Grupie Lotos S.A określone w dokumencie „Plan działań bezpieczeństwa" (Safety Plan).

Elementy manipulacyjne bloku zaworowego przetwornika (sygnalizatora) muszą być ściągane lub wyposażone w blokadę. To samo dotyczy innych zaworów na drodze połączeń procesowych przetwornika (sygnalizatora). Celem zabezpieczenia jest ochrona przed zakłóceniem pracy elementów pomiarowych. Zabezpieczenie to będzie mogło zostać usunięte, odblokowane tylko przez osoby odpowiedzialne za bezpieczeństwo funkcjonalne w Grupie Lotos S.A..

Elementy układów redundantnych muszą być obsługiwane przez osobne moduły I/O.

Szczególnie zaleca się stosowanie urządzeń różnych typów (o różnej zasadzie działania lub różnych producentów, patrz Dywersyfikacja pkt. 4.3) w konfiguracjach redundantnych oraz w układach różnych warstw ochrony lecz związanych z jednym określonym zagrożeniem (np. jeden przetwornik w układzie regulacji DCS a drugi, innego typu w systemie bezpieczeństwa SIS).

Dla wyzwolenia działania elementów wykonawczych systemu SIS należy przewidzieć przyciski (manual means) niezależne od SIS-PLC, chyba, że specyfikacje wymagań bezpieczeństwa nakazują inaczej.

Preferowane są urządzenia z certyfikatem zgodności z normą PN-EN 61508 w odróżnieniu od dokumentacji Proven in Use czy Prior Use.

W przypadku, gdy w danej lokalizacji występuje wiele urządzeń pomiarowych i/lub wykonawczych systemu SIS, należy je łączyć do dedykowanych skrzynek złącznych, do których podłączone będą wyłącznie urządzenia pracujące w systemie SIS. Dodatkowo, zaleca się podłączanie urządzeń tworzących układ redundantny do różnych (oddzielnych) skrzynek złącznych.

W przypadkach, gdzie w jednej skrzynce występują obwody funkcji SIF i inne odnośnie podłączeń w skrzynkach złącznych (segregacja sygnałów) obowiązują zapisy paragrafu ‘Skrzynki złączne’ w specyfikacji GLSA 3110.

Elementy pomiarowe i wykonawcze będące częściami funkcji SIF muszą być oznaczone w sposób pozwalający na łatwą identyfikację spośród elementów nie będących częściami funkcji SIF. Szczegóły wykonania oznaczeń zawarte są w standardzie 3030 paragraf 5.3.2.1.

5.6.1 Dokumentacja dla urządzeń pomiarowych i wykonawczych będących częściami SIS.

Poniżej przedstawiono wymaganą przez Grupę Lotos S.A dokumentację dla urządzeń pomiarowych i wykonawczych będących częściami funkcji SIF.

Jeśli urządzenie posiada certyfikat zgodności z PN-EN 61508 to wymagana jest następująca dokumentacja:

a) W przypadku, gdy sposób działania urządzenia jest złożony lub może nie być oczywisty np. zawór z rozbudowanym systemem sterowania należy przedstawić opis działania urządzenia z dokładnym przedstawieniem zagadnień mających wpływ na niezawodność działania.

b) Współczynniki niezawodności urządzenia określające uszkodzenia wykryte przez diagnostykę wewnętrzną urządzenia - λ_{DD}, λ_{SD}.

c) Współczynniki niezawodności urządzenia określające uszkodzenia nie wykryte przez diagnostykę wewnętrzną urządzenia - λ_{DU}, λ_{SU}.

d) Wymagania środowiskowe (mogą być zawarte w certyfikacie).

e) Czas życia urządzenia.

f) Sugerowana częstotliwość testów sprawdzających-okresowych i możliwy stopień pokrycia tych testów (PTC).

g) Częstotliwość wewnętrznych (przeprowadzanych przez urządzenie samo w sobie) testów diagnostycznych.

h) Stopień pokrycia diagnostycznego wewnętrznych testów diagnostycznych.

i) Wskazania co do czasu naprawy MTTR-wymiany urządzenia.

j) Maksymalny poziom SIL (dla określonej konfiguracji), przy którym urządzenie może pracować.

k) Certyfikat zgodności z PN-EN 61508.

l) Dokumentacja warunków(środowiskowe, obsługi, i inne) jakie muszą być spełnione aby certyfikat zachowywał swoją ważność.

Uwagi:

1) Punkty g) i h) są wymagane jeśli testy wewnętrzne urządzenia są uwzględniane w obliczeniach niezawodności.

2) Punkty od b) do i) potrzebne są do obliczenia PFD dla urządzenia

3) Punkty b), c), g), h) są wymagane gdy urządzenie pomiarowe lub wykonawcze może być użyte w redundowanej architekturze. Jeśli nie zachodzi taka sytuacja możliwe jest podanie PFD_{avg} z tym, że należy wtedy podać wytyczne punktu f).

Jeśli urządzenie nie posiada certyfikatu zgodności z PN-EN 61508 to wymagana jest następująca dokumentacja:

a) W przypadku gdy sposób działania urządzenia jest złożony np. zawór z rozbudowanym systemem sterowania należy przedstawić opis działania urządzenia z dokładnym przedstawieniem zagadnień mających wpływ na niezawodność działania.

b) Współczynniki niezawodności urządzenia określające uszkodzenia wykryte przez diagnostykę wewnętrzną urządzenia - λ_{DD}, $\lambda_{SD.}$

c) Współczynniki niezawodności urządzenia określające uszkodzenia nie wykryte przez diagnostykę wewnętrzną urządzenia - λ_{DU}, $\lambda_{SU.}$

d) Wymagania środowiskowe.

e) Czas życia urządzenia.

f) Sugerowana częstotliwość testów sprawdzających-okresowych i możliwy stopień pokrycia tych testów (PTC).

g) Częstotliwość wewnętrznych (przeprowadzanych przez urządzenie samo w sobie) testów diagnostycznych.

h) Stopień pokrycia diagnostycznego wewnętrznych testów diagnostycznych.

i) Wskazania co do czasu naprawy MTTR -wymiany urządzenia.

j) Współczynnik SFF lub dane do jego obliczenia.

k) Parametr FAULT TOLERANCE dla urządzenia.

l) Dokumentacja Proven in Use według PN-EN 61508-2 7.4.7 lub Prior Use według PN-EN 61511-1 11.5.3.

Uwagi:

1) Punkty g) i h) są wymagane jeśli testy wewnętrzne urządzenia są uwzględniane w obliczeniach niezawodności.

2) Punkty od b) do i) potrzebne są do obliczenia PFD dla urządzenia.

3) Punkty b), c), g), h) są wymagane gdy urządzenie pomiarowe lub wykonawcze może być użyte w redundowanej architekturze. Jeśli nie zachodzi taka sytuacja możliwe jest podanie PFD_{avg} z tym, że należy wtedy podać wytyczne punktu f).

5.7 Wymagania odnośnie sterownika programowalnego SIS-PLC

Sterownik SIS-PLC, w którym zaimplementowane są funkcje SIF powinien być szczególnie odporny na zakłócenia takie jak: elektromagnetyczne, temperatury, wilgotności, wibracji i eksploatacji właściwe dla miejsca montażu.

Należy zwrócić uwagę, aby moduły elementów funkcji SIF nie pracowały przy swoich granicznych parametrach takich jak prąd, napięcie, częstotliwość (należy zachować odpowiedni margines bezpieczeństwa).

Wszelkie detaliczne wymagania, wynikają ze specyfikacji wymagań bezpieczeństwa będących wynikiem przekrojowego studium nad zdefiniowanymi uprzednio funkcjami SIF oraz postawionymi im wymaganiami niezawodności działania.

Specyficzne wymagania postawione w poniższych paragrafach odnośnie SIS-PLC, stanowią dopełnienie wymagań zasadniczych dla sterowników PLC opisanych w GLSA 3640. Dotyczy to zarówno funkcjonalności jak też zabudowy. Wszędzie tam, gdzie zachodziłaby rozbieżność, priorytetem są wytyczne niniejszej specyfikacji.

Sterownik programowalny SIS-PLC może obsługiwać urządzenia pomiarowe i wykonawcze będące częściami funkcji SIF oraz w wyjątkowych sytuacjach urządzenia, które są funkcjami bezpieczeństwa bez zdefiniowanego poziomu SIL.

Funkcje, dla których obliczony RRF jest mniejszy niż 10, nie podlegają wymaganiom normy PN-EN 61508 ani PN-EN 61511. Funkcje te należy implementować w systemie ESD-PLC lub za zgodą GL w systemie SIS-PLC przeznaczonym dla funkcji SIF licząc się jednak z tym, że będą je obowiązywać takie same obostrzenia i wymagania jakie nakładają normy PN-EN 61508 i 61511dla funkcji SIF.

Zaleca się, aby sterownik ESD-PLC wykonywał tylko funkcje bez zdefiniowanego poziomu SIL a dla funkcji SIF przewidziany był osobny sterownik (SIS-PLC).

Jeśli dla systemu SIS przewidziany jest osobny sterownik to musi on być niezależny od innych systemów. Podobnie sterownik ESD-PLC powinien być systemem niezależnym od innych systemów.

Działanie funkcji SIF musi być niezależne od działania innych funkcji bezpieczeństwa.

Wobec sterownika SIS-PLC oraz ESD-PLC należy stosować wymóg FAULT TOLERANT i FAIL SAFE.

Sterownik, w którym zaimplementowane są funkcje SIF musi spełniać wymagania SIL o poziomie równym co najmniej maksymalnemu poziomowi spośród SIL funkcji obsługiwanej przez sterownik.

Sterownik SIS-PLC <u>musi posiadać stosowny certyfikat zgodności z normą PN-EN 61508</u>, w odróżnieniu od dokumentacji Proven in Use czy Prior Use (wymagania patrz pkt 5.7.1). Sterownik (oraz jego certyfikat) powinien przewidywać możliwość wprowadzania zmian w oprogramowaniu on-line, tzn. bez przerywania pracy ani sterownika ani obiektu. Kompletny SIS-PLC, uwzględniając konieczne w tym celu moduły jak CPU, I/O oraz wewnętrzne łącza komunikacyjne i inne wymagane musi spełniać wymagania postawione w SRS.

Zgodność wykonania sterownika systemu SIS z normami PN-EN 61508 musi być potwierdzona właściwą dokumentacją – patrz punkt 5.7.1

Stopień redundancji sterownika SIS-PLC zależy od wymaganego poziomu SIL i powinien odpowiadać wymaganiom PN-EN 61508-2 7.4.3 Tabela 3 lub PN-EN 61511-1 11.4 tabela 5 lecz nie może być mniejszy niż jeden.

Odpowiednia diagnostyka zaimplementowana w systemie SIS musi wykrywać przerwanie ciągłości okablowania urządzeń pomiarowych i w zależności od ich konfiguracji dokonywać redukcji układu lub inicjalizować wykonanie funkcji SIF (patrz punkt 5.4).

Jeżeli diagnostyka elementów pomiarowych i wykonawczych zaimplementowana w systemie SIS–PLC wykryje uszkodzenie elementu to sygnalizacja tego uszkodzenia musi odbywać się niezależnie od działania systemu DCS lub jeśli odbywa się za pomocą DCS to podlega ona testom sprawdzającym-okresowym podobnie jak element z którym jest związana.

Następujące informacje kluczowe dla utrzymania odpowiedniego poziomu SIL dla danej SIF muszą być dostępne dla operatora:

- W jakim stanie pracy znajduje się aktualnie funkcja,
- Sygnalizacja zadziałania funkcji,
- Sygnalizacja zablokowania działania funkcji,
- Wyniki diagnostyki i wskazanie stopnia degradacji układów redundantnych (patrz np. głosowanie 1oo2D pkt. 5.4),
- Stan elementów pomiarowych i wykonawczych,
- Uszkodzenia urządzeń mających wpływ na prawidłowe wykonanie SIF np. awaria układów regulacji warunków środowiskowych (grzanie, chłodzenie, wentylacja).

Interfejs stacji SIS-PLC powinien umożliwiać wykonanie poniższych funkcji z zapewnieniem dla każdej z nich stosownego zabezpieczenia przed nieautoryzowanym dostępem (m.in. osobnego hasła dostępu):

- Tryb pracy SIS, program, dane, środki do wyłączenia alarmów, testy, forsowanie stanu I/O, konserwacja,
- Diagnostyka SIS, głosowanie i obsługa błędów,
- Dodawanie funkcji, usuwanie, modyfikacja oprogramowania,
- Moduł analizy programu i szukania błędów.

Dostęp do zapisu w pamięci systemu SIS powinien być tylko z poziomu systemu SIS i przez osoby o odpowiednich uprawnienia przewidzianych przez Grupę Lotos S.A..

System SIS powinien być tak zaprojektowany, aby pomimo awarii lub zakłócenia na łączach komunikacyjnych tego systemu z innymi systemami możliwa była praca SIS-PLC do czasu usunięcia usterki komunikacji oraz w razie konieczności doprowadzenie przez SIS-PLC funkcji SIF do stanu bezpiecznego.

System SIS-PLC powinien umożliwiać testowanie funkcji SIF od elementu pomiarowego aż do elementu wykonawczego.

Wymagany systemowy czas skanowania Ts (całkowity czas potrzebny do: odczytu wejść, wykonania logiki i wypracowania stanu wyjść, zapisania wyjść), należy określić uwzględniając specyfikację wymagań bezpieczeństwa dla wszystkich zdefiniowanych SIF oraz rozkład czasu reakcji funkcji SIF na poszczególne jej elementy (urządzenia do pomiaru, SIS-PLC, urządzenia wykonawcze). Czas skanowania Ts musi spełniać nierówność Ts <= (wymagany czas wykonania całej funkcji SIF) – (czas potrzebny dla elementów pomiarowych i wykonawczych).

Sterownik implementujący funkcje SIF powinien spełniać wymagania odnośnie kontroli uszkodzeń systematycznych postawione w PN-EN 61508-2 tabela A.16

5.7.1 Dokumentacja

Poniżej przedstawiono wymaganą przez Grupę Lotos S.A dokumentację dla sterowników obsługujących funkcje SIF.

Ponieważ sterownik SIS-PLC będzie posiadał certyfikat zgodności z PN-EN 61508 to wymagana jest dla niego następująca dokumentacja:

a) Opis działania sterownika z dokładnym przedstawieniem zagadnień mających wpływ na niezawodność działania.

b) Współczynniki niezawodności urządzenia określające uszkodzenia wykryte przez diagnostykę wewnętrzną urządzenia - λ_{DD}, λ_{SD} dla wszystkich modułów mających wpływ na wykonywanie funkcji SIF.

c) Współczynniki niezawodności urządzenia określające uszkodzenia nie wykryte przez diagnostykę wewnętrzną urządzenia - λ_{DU}, λ_{SU} dla wszystkich modułów mających wpływ na wykonywanie funkcji SIF.

d) Wymagania środowiskowe (mogą być zawarte w certyfikacie)

e) Czas życia urządzenia.

f) Sugerowana częstotliwość testów sprawdzających-okresowych i możliwy stopień pokrycia tych testów (PTC).

g) Wskazania co do czasu naprawy MTTR-wymiany urządzenia.

h) Maksymalny poziom SIL (dla określonej konfiguracji), przy którym urządzenie może pracować.

i) Certyfikat zgodności z PN-EN 61508.

j) Dokumentacja warunków dla certyfikatu (środowiskowe, obsługi, i inne) jakie muszą być spełnione aby certyfikat zachowywał swoją ważność.

5.7.2 Moduły I/O

Preferowanym rozwiązaniem dla sygnałów I/O w zakresie ochrony przeciw atmosferze wybuchowej jest stosowanie obwodów iskrobezpiecznych. Separatory Exi, oprócz certyfikatów zgodności z wymaganiami iskrobezpieczeństwa, muszą posiadać certyfikat zgodności ze standardem PN-EN 61508 (dokumentacja wg punktu 5.7.1). Celem podłączeń do SIS-PLC sygnałów zewnętrznych przewiduje się stosowanie następujących typów I/O:

- WEJŚCIA
  - 4-20mA.
  - binarne typu NAMUR, dla wejść od czujników zbliżeniowych zgodnych z PN-EN 60947-5-6,
- WYJŚCIA (dwustanowe)
  - styk beznapięciowy,
  - 0/24V DC.

Dodatkowo, wejścia binarne typu NAMUR muszą być przystosowane do obsługi sygnałów typu styk beznapięciowy (np. dla potrzeb sygnałów typu RESET, MOS, certyfikowanych urządzeń stykowych).

Maksymalna ilość obsadzonych punktów I/O na pojedynczym module I/O nie może przekraczać:

- 8 kanałów dla wejść 4-20mA oraz NAMUR,
- 8 kanałów dla wyjść dwustanowych.

Pod względem zabezpieczenia, w ramach jednej grupy sygnałów obowiązuje ograniczenie do max. 8 sygnałów na jeden bezpiecznik.

Przy układach redundantnych zaleca się podłączać redundantne elementy pomiarowe i wykonawcze do różnych modułów I/O. Również sygnały dotyczące redundowanych urządzeń procesowych (np. pompy rezerwowe) muszą być podłączane do różnych modułów I/O.

5.7.3 Jednostka centralna – CPU

Jako minimalne wymaganie w zakresie rezerwowania się CPU, przyjmuje się stosowanie redundantnych modułów jako oddzielnych urządzeń. Zastosowanie znajduje tu wspomniany wcześniej wymóg FAIL SAFE oraz FAULT TOLERANT.

5.7.4 Oprogramowanie

W zakresie języków programowania SIS-PLC oraz ESD-PLC obowiązują wymagania standardu PN-EN 61131-3. Dopuszczalne reprezentacje to:

- schemat bloków funkcjonalnych (FBD - functional block diagrams).
- schemat drabinkowy (LAD - ladder diagram).
- schemat bloków sekwencyjnych (SFC – sequential function chart).

W przypadku zastosowania wspólnego sterownika SIS-PLC do implementacji funkcji bezpieczeństwa SIF oraz funkcji bez określonego poziomu SIL, należy właściwe im programy, logikę umieszczać w osobnych modułach programów.

Kod źródłowy winien być prosty, czytelny i zrozumiały oraz umożliwiać testowanie i późniejsze modyfikacje. Bezwzględnie wymagane są opisy stanów „0” i „1” jak i zmiennych wewnętrznych. Tak dalece jak to możliwe projekt powinien minimalizować tę część programu, która związana jest z bezpieczeństwem.

W programie należy zaimplementować logikę FIRST OUT, pozwalającą na szybką identyfikację zdarzenia inicjującego w sytuacjach gdy dochodzi do odłączenia częściowego bądź całej instalacji.

Dostęp do oprogramowania systemu SIS winien być zabezpieczony przed dostępem osób niepowołanych. Zmiany w oprogramowaniu mogą być przeprowadzone tylko przez osoby odpowiedzialne za bezpieczeństwo funkcjonalne w Grupie Lotos S.A. określone w dokumencie „Plan działań bezpieczeństwa” (Safety Plan).

Dodatkowo, odnośnie programowania i zmian „on-line”, należy ściśle przestrzegać postanowień certyfikatu oraz „instrukcji bezpieczeństwa” (czyli „safety manual”) sterownika SIS-PLC w tym względzie. Zasadnicze modyfikacje lub modernizacje należy przeprowadzać podczas postoju instalacji. Każdorazowo należy przestrzegać zaleceń wszelkich powołanych procedur norm PN-EN 61508/61511 odnośnie modyfikacji systemów.

Ewentualna wymiana firmware, pociąga za sobą konieczność pełnej procedury ponownego uruchomienia automatycznego systemu bezpieczeństwa (SIS).

5.7.5 Forsowanie wejść/wyjść, sygnały MOS

Forsowanie stanu wejść lub wyjść w sterowniku SIS-PLC nie może być użyte jako część składowa:

- programu aplikacyjnego,
- procedur eksploatacji (prowadzenia instalacji),
- utrzymania ruchu, z wyjątkiem jak opisano poniżej.

Niedozwolone jest forsowanie stanu wejść lub wyjść SIS-PLC bez uprzedniego zatrzymania (wyłączenia) SIS, chyba, że odbywa się to przy zastosowaniu odpowiednich procedur oraz ochrony dostępu przewidzianych przez Grupę Lotos S.A. Użycie forsowania musi być w odpowiedni sposób zgłoszone (zapowiedziane) lub musi zostać włączony alarm.

Forsowanie oraz użycie MOS-a musi być odpowiednio zabezpieczone przed nieautoryzowanym dostępem.

Jeżeli dla funkcji SIF zastała założona de-blokada (MOS, forsowany stan I/O) to alarmy i ręczne środki doprowadzenia SIF do stanu bezpiecznego nie mogą być zablokowane.

Sygnały MOS dla konfiguracji nieredundantnej elementów pomiarowych lub wykonawczych i funkcji SIF pracującej w trybie „low demand" mogą być zastosowane tylko przy:

- Uprzednim doprowadzeniu funkcji do stanu bezpiecznego,
- Zastosowaniu na czas trwania sygnału MOS innego środka zapewniającego bezpieczeństwo w stopniu co najmniej równym poziomowi zapewnianemu przez „by-pasowaną" funkcję SIF. Czas ten nie może przekraczać założonego do obliczeń czasu MTTR. Po upływie tego czasu działanie funkcji SIF musi zostać przywrócone w pełnej konfiguracji a sygnał MOS musi zostać automatycznie usunięty (zdezaktywowany) przez system SIS-PLC lub funkcja SIF musi osiągnąć stan bezpieczny.

Dla funkcji bezpieczeństwa, istotnych z punktu widzenia prowadzenia instalacji (np. tam gdzie sprowadzenie SIF do stanu bezpiecznego wiąże się z przerwami w produkcji), zaleca się stosowanie konfiguracji redundantnych (nawet jeśli to nie jest wymagane względami bezpieczeństwa) celem umożliwienia stosowania MOS dla poszczególnych urządzeń KiA.

Sygnały MOS dla konfiguracji redundantnej elementów pomiarowych lub wykonawczych i funkcji SIF pracującej w trybie „low demand" mogą być zastosowane tylko przy:

- Uprzednim doprowadzeniu funkcji do stanu bezpiecznego,
- By-pasie (obejściu) jednego elementu na czas MTTR. W tym czasie funkcje układu są podtrzymywane przez elementy nie by-pasowane (aktywne). Po upływie tego czasu działanie funkcji SIF musi zostać przywrócone w pełnej konfiguracji a sygnał MOS musi zostać automatycznie usunięty (zdezaktywowany) przez system SIS-PLC lub funkcja SIF musi osiągnąć stan bezpieczny.

Dla każdego MOS-a należy przewidzieć stosowny interfejs operatorski, informujący o jego statusie, pozostałym do wykorzystania czasie MTTR oraz zaimplementować alarm informujący o tym, że czas MTTR dobiega końca.

5.7.6 Połączenia z DCS i innymi systemami

W zakresie łączy komunikacyjnych, połączenia systemu SIS-PLC z DCS będą odpowiadały wymaganiom postawionym komunikacji pomiędzy PLC a DCS w specyfikacjach GLSA 3710 oraz GLSA 3640. Ponadto, wymaga się aby łącza komunikacyjne były redundantne.

Sygnały istotne z punktu widzenia strategii sterowania lub technologii instalacji, będą wymieniane z DCS (lub innymi systemami) na drodze połączeń przez karty I/O (hardware'owych), z wyłączeniem połączeń komunikacji cyfrowej.

5.7.7 Stacja sekwencji zdarzeń (SOER)

SIS-PLC oraz ESD-PLC należy wyposażyć w stację rejestracji sekwencji zdarzeń (SOER) wraz z drukarką. Wszelkie zdarzenia muszą być przechowywane ze znacznikiem czasowym, który nadawany jest w CPU.

5.7.8 Szafy

Wszelki wymagania mechaniczne, wyposażenia i zabudowy w szafie jak również kwestię sieci zasilającej oraz wymagania odnośnie dystrybucji zasilania opisano w GLSA 3640 oraz GLSA 3130.

5.8 Bezpieczeństwo maszyn

Niniejszy paragraf poświęcony jest zagadnieniu bezpieczeństwa maszyn, pod kątem wytycznych dla stosowania automatycznych systemów zabezpieczających.

5.8.1 Wymagania certyfikatu zgodności

Wszelkie urządzenia techniczne, o których mowa w niniejszym paragrafie, przed dopuszczeniem ich do pracy podlegają systemowi oceny zgodności. Zakres oceny zgodności, czyli zestaw przepisów, który go tworzy, zależy od konkretnego urządzenia. Znajdują tu głównie zastosowanie dyrektywy nowego podejścia:

- ⇒ 2006/42/WE, Maszyny (MAD)
- ⇒ 97/23/WE, Urządzenia ciśnieniowe (PED)
- ⇒ 2009/142/WE, Urządzenia spalające paliwa gazowe (GAD)
- ⇒ 2009/104/WE, Sprzęt Roboczy

oraz właściwe normy zharmonizowane z powyższymi.

System oceny zgodności tworzą wymagania stawiane badanym urządzeniom, w szczególnym przypadku wszelkie wymagania odnośnie bezpieczeństwa, stosowne do typu rządzenia.

Warunkiem dopuszczenia urządzenia do pracy jest pozytywny wynik procesu oceny zgodności, potwierdzony *certyfikatem zgodności*, wydanym przez notyfikowaną jednostkę certyfikującą. Należy pamiętać, że certyfikacji podlegają zarówno urządzenie (maszyna) jak i proces jego wytwarzania – również, a może przede wszystkim z uwzględnieniem stosownych aspektów bezpieczeństwa.

Na dzień pisania niniejszej specyfikacji, jedyną polską notyfikowaną jednostką certyfikującą jest Urząd Dozoru Technicznego (UDT-CERT). W związku z tym, wszelkie wnioski o przeprowadzenie badań należy kierować właśnie do UDT-CERT i stosować się do zaleceń dyktowanych przez ten Urząd.

Spełnienie wymagań określonych przez system oceny oraz dopełnienie wszelkich formalności związanych z uzyskaniem certyfikatu zgodności, jest powinnością dostawcy urządzenia (producenta) lub w przypadku modernizacji urządzenia wykonawcy tej modyfikacji. W szczególnych przypadkach w imieniu producenta, wnioskodawcą może być również jego upoważniony przedstawiciel. W przypadku modernizacji maszyn należy pamiętać o spełnieniu wymagań dyrektywy 2009/104/EC w zakresie dostosowania urządzeń niespełniających aktualnych wymagań właściwych dyrektyw i norm.

5.8.2 Bezpieczeństwo urządzeń

Poza zasadniczymi wymaganiami zawartymi w dyrektywach, należy w przypadku konkretnych urządzeń (tj. pieców, kotłów, innych maszyn), spełnić wymagania stawiane przez odpowiednio wyselekcjonowane normy, odnoszące się do zagadnień bezpieczeństwa.

Niejednoznaczność, wynika tu z faktu różnorodności urządzeń z jednej strony oraz, że w odniesieniu do pewnych urządzeń mogą mieć zastosowanie różne dyrektywy, które traktują bezpieczeństwo w swoisty sposób, odwołując się do różnego zestawu norm zharmonizowanych. Za określenie dyrektyw/norm odnoszących się do przedmiotowego urządzenia (które zarazem wchodzą w skład systemu oceny zgodności) odpowiedzialny jest producent urządzenia.

Ważnym aspektem, który należy tu uwypuklić jest to czego (lub kogo) bezpieczeństwo ma dotyczyć. Poniższe paragrafy definiują to jednoznacznie.

5.8.2.1 Piece, kotły

1. W sytuacji gdy kotły projektowane i wykonywane są zgodnie z normą EN 12952 lub EN 12953, w zakresie zabezpieczeń na bazie urządzeń elektrycznych podlegają rygorowi zgodności z normą **EN 50156-1**. Wymagania stawiane systemom zabezpieczającym opisane w tej normie, w swoim podejściu do zagadnień bezpieczeństwa wskazują na analogie z normą PN-EN 61508 (również dotyczącej elektrycznych urządzeń zabezpieczających), do której norma PN-EN 50156-1 częstokroć się odwołuje. Pomimo iż PN-EN 61508 odnosi się zasadniczo do bezpieczeństwa ludzi, to norma EN 50156-1 określa wymagania w celu zapewnienia bezpieczeństwa ludzi, mienia oraz środowiska.
2. Innym przypadkiem jest sytuacja gdy wymagania bezpieczeństwa pieca oparte są o zapisy z normy PN-EN 746. Wówczas przy projektowaniu systemów sterowania związanych z bezpieczeństwem, analizie zagrożeń, ocenie ryzyka oraz przy wyborze środków zmniejszających ryzyko należy kierować się wytycznymi następujących norm:

   - **PN-EN ISO 13849-1**,
   - **PN-EN ISO 12100.**

   Powyższe normy również odwołują się do postanowień zawartych w PN-EN 61508. Zgodnie z zapisem w PN-EN ISO 12100 nt. szacowania ciężkości szkody, chronione (zabezpieczane) mają być ludzie, mienie i środowisko.

Pamiętać należy, że normy, którym podporządkowuje się proces projektowania, w tym zagadnienia bezpieczeństwa danego urządzenia traktowane były całościowo i konsekwentnie. Nieprawidłowym postępowaniem jest spełnianie wymagań poszczególnych norm jedynie wybiórczo, tj. odnoszenie się do jednej normy (np. PN-EN 12952) w kwestii pewnych aspektów przy jednoczesnym stosowaniu innej, odrębnej normy (np. PN-EN 746) w odniesieniu do reszty zagadnień. W kwestiach nie zdefiniowanych w przedmiotowej normie a zidentyfikowanych przez producenta, np. szczególny rodzaj zagrożeń i związane z tym ryzyko, należy sprawę rozwiązać stosując właściwe zabezpieczenia, odpowiednio to dokumentując.

5.8.2.2 Inne maszyny

Wyznacznikiem w podejściu do zagadnień bezpieczeństwa maszyn w ogóle, jest dyrektywa maszynowa i wykaz odpowiednich norm zharmonizowanych. Podobnie jak w §5.8.2.1/2, w odniesieniu do zagadnień automatycznych systemów bezpieczeństwa obowiązują normy PN-EN ISO 13849-1, PN-EN ISO 14100.

5.8.2.3 Kryterium porównawcze oceny ryzyka

Należy pamiętać o koniecznych uzgodnieniach z GLSA w zakresie parametrów określonych w §5.2.1, w szczególności w odniesieniu do ryzyka tolerowalnego.

6 Dokumenty związane

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

7 Normy i przepisy

Projektowanie, wykonanie i montaż musi być zgodne z najnowszymi edycjami wyszczególnionych poniżej norm i przepisów.

Wymienia się tutaj głównie normy specyficznie związane z instalacjami elektrycznymi. Pozostałe normy dotyczące KiA podane są w specyfikacji nr 3010 - Wymagania ogólne.

7.1 Dyrektywy i Decyzje Wspólnoty Europejskiej

2006/95/WE	Sprzęt elektryczny przewidziany do stosowania w niektórych granicach napięcia (LVD).
2004/108/WE	Kompatybilność elektromagnetyczna (EMC)
2008/765/EC	ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (WE) NR 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93.
2008/768/WE	DECYZJA PARLAMENTU EUROPEJSKIEGO I RADY NR 768/2008/WE dnia 9 lipca 2008 r. w sprawie wspólnych ram dotyczących wprowadzania produktów do obrotu, uchylająca decyzję Rady 93/465/EWG.
2009/104/WE	Dyrektywa Parlamentu Europejskiego i Rady 2009/104/WE z dnia 16 września 2009 r. dotycząca minimalnych wymagań w dziedzinie bezpieczeństwa i higieny użytkowania sprzętu roboczego przez pracowników podczas pracy.
94/9/WE	Urządzenia i systemy ochronne przeznaczone do użytku w przestrzeniachzagrożonych wybuchem (ATEX 100A)
99/92/WE	Minimalne wymagania mające na celu poprawę stanu bezpieczeństwa i ochrony zdrowia pracowników potencjalnie narażonych na ryzyko spowodowane atmosferami wybuchowymi (ATEX 137)
2006/42/WE	Maszyny (MAD).
97/23/WE	Urządzenia ciśnieniowe (PED).
2009/142/WE	Urządzenia spalające paliwa gazowe (GAD).
96/82/WE	Dyrektywa Rady w sprawie kontroli niebezpieczeństwa poważnych awarii związanych z substancjami niebezpiecznymi (COMAH, SEVESO II) z późniejszymi zmianami M1 do M4.

7.2 Polskie akty prawne

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

Dz. U. z 2001r. Nr 62, poz. 627 Ustawa z dn. 27 kwietnia 2001r. Prawo ochrony środowiska (z późniejszymi zmianami). Tekst jednolity Dz. U. 2008 Nr 25 Poz. 150

7.3 PN-EN

PN-EN 746-1	Urządzenia przemysłowe do procesów cieplnych. Ogólne wymagania bezpieczeństwa dotyczące urządzeń przemysłowych do procesów cieplnych.
PN-EN 746-2	Urządzenia przemysłowe do procesów cieplnych. Wymagania dotyczące bezpieczeństwa systemów spalania i układów paliwowych (oryg.).
PN-EN 746-3	Urządzenia przemysłowe do procesów cieplnych. Wymagania dotyczące bezpieczeństwa wytwarzania i stosowania atmosfer gazowych.
PN-EN 50156-1	Wyposażenie elektryczne pieców oraz ich urządzeń pomocniczych. Część 1: Wymagania dotyczące projektowania i instalacji (oryg.).
PN-EN 12952-1	Kotły wodnorurowe i urządzenia pomocnicze. Część 1: Postanowienia ogólne
PN-EN 12952-2	Kotły wodnorurowe i urządzenia pomocnicze. Część 2: Materiały na części ciśnieniowe kotłów i wyposażenie (oryg.)
PN-EN 12952-3	Kotły wodnorurowe i urządzenia pomocnicze. Część 3: Konstrukcja i obliczenia części ciśnieniowych (oryg.)
PN-EN 12952-4	Kotły wodnorurowe i urządzenia pomocnicze. Część 4: Obliczenia oczekiwanej trwałości kotłów podczas eksploatacji (oryg.)
PN-EN 12952-5	Kotły wodnorurowe i urządzenia pomocnicze. Część 5: Wytwarzanie i budowa części ciśnieniowych kotłów (oryg.)
PN-EN 12952-6	Kotły wodnorurowe i urządzenia pomocnicze. Część 6: Badania podczas wytwarzania. Sporządzanie dokumentacji i znakowanie części ciśnieniowych kotłów (oryg.)
PN-EN 12952-7	Kotły wodnorurowe i urządzenia pomocnicze. Część 7: Wymagania dotyczące wyposażenia do kotłów (oryg.)
PN-EN 12952-8	Kotły wodnorurowe i urządzenia pomocnicze. Część 8: Wymagania dotyczące instalacji paleniskowych na paliwa ciekłe i gazowe do kotłów
PN-EN 12952-9	Kotły wodnorurowe i urządzenia pomocnicze. Część 9: Wymagania dotyczące pyłowych instalacji paleniskowych do kotłów
PN-EN 12952-10	Kotły wodnorurowe i urządzenia pomocnicze. Część 10: Wymagania dotyczące zabezpieczeń przed wzrostem ciśnienia
PN-EN 12952-11	Kotły wodnorurowe i urządzenia pomocnicze. Część 11: Wymagania dla ograniczników kotła i osprzętu
PN-EN 12952-12	Kotły wodnorurowe i urządzenia pomocnicze. Część 12: Wymagania dotyczące jakości wody zasilającej i wody kotłowej
PN-EN 12952-13	Kotły wodnorurowe i urządzenia pomocnicze. Część 13: Wymagania dotyczące instalacji oczyszczania spalin
PN-EN 12952-14	Kotły wodnorurowe i urządzenia pomocnicze. Część 14: Wymagania dotyczące instalacji oczyszczania spalin DENOX stosujących ciekły amoniak pod ciśnieniem i roztwór wodny amoniaku
PN-EN 12952-15	Kotły wodnorurowe i urządzenia pomocnicze. Część 15: Badania odbiorcze

PN-EN 12952-16	Kotły wodnorurowe i urządzenia pomocnicze. Część 16: Wymagania dotyczące rusztowych i fluidalnych instalacji paleniskowym na paliwa stałe do kotłów
PN-CR 12952-17	Kotły wodnorurowe i urządzenia pomocnicze. Część 16: Wskazówki dotyczące wyboru organizacji badawczo-certyfikujących
PN-EN 12952-18	Kotły wodnorurowe i urządzenia pomocnicze. Część 18: Instrukcje obsługi (oryg.)
PN-EN 12953-1	Kotły płomienicowo-płomieniówkowe. Część 1: Postanowienia ogólne (oryg.)
PN-EN 12953-2	Kotły płomienicowo-płomieniówkowe. Część 2: Materiały na części ciśnieniowe kotłów i osprzęt (oryg.)
PN-EN 12953-3	Kotły płomienicowo-płomieniówkowe. Część 3: Konstrukcja i obliczenia części ciśnieniowych
PN-EN 12953-4	Kotły płomienicowo-płomieniówkowe. Część 4: Wytwarzanie i budowa części ciśnieniowych kotłów
PN-EN 12953-5	Kotły płomienicowo-płomieniówkowe. Część 5: Badania podczas wytwarzania, sporządzanie dokumentacji i znakowanie części ciśnieniowych kotłów
PN-EN 12953-6	Kotły płomienicowo-płomieniówkowe. Część 6: Wymagania dotyczące wyposażenia do kotłów (oryg.)
PN-EN 12953-7	Kotły płomienicowo-płomieniówkowe. Część 7: Wymagania dotyczące instalacji paleniskowych na paliwa ciekłe i gazowe do kotłów
PN-EN 12953-8	Kotły płomienicowo-płomieniówkowe. Część 8: Wymagania dotyczące zabezpieczeń przed wzrostem ciśnienia
PN-EN 12953-9	Kotły płomienicowo-płomieniówkowe. Część 9: Wymagania dla ograniczników kotła i osprzętu
PN-EN 12953-10	Kotły płomienicowo-płomieniówkowe. Część 10: Wymagania dotyczące jakości wody zasilającej i wody kotłowej
PN-EN 12953-11	Kotły płomienicowo-płomieniówkowe. Część 11: Badania odbiorcze
PN-EN 12953-12	Kotły płomienicowo-płomieniówkowe. Część 12: Wymagania dotyczące instalacji paleniskowych rusztowych na paliwa stałe do kotłów
PN-EN 12953-13	Kotły płomienicowo-płomieniówkowe. Część 13: Instrukcje eksploatacji (oryg.)
PN-EN 60204-1	Bezpieczeństwo maszyn - Wyposażenie elektryczne maszyn - Część 1: Wymagania ogólne.
PN-EN 61508-1	Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem. Część 1: Wymagania ogólne
PN-EN 61508-2	Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem. Część 2: Wymagania dotyczące elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem (oryg.)
PN-EN 61508-3	Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem. Część 3: Wymagania dotyczące oprogramowania (oryg.)
PN-EN 61508-4	Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem. Część 4: Definicje i skrótowce (oryg.)

PN-EN 61508-5	Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem. Część 5: Przykłady metod określania poziomów nienaruszalności bezpieczeństwa (oryg.)
PN-EN 61508-6	Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem. Część 6: Wytyczne do stosowania IEC 61508-2 i IEC 61508-3 (oryg.)
PN-EN 61508-7	Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem. Część 7: Przegląd technik i miar (oryg.)
PN-EN 61131-1	Sterowniki programowalne. Część 1: Postanowienia ogólne (oryg.)
PN-EN 61131-2	Sterowniki programowalne. Część 2: Wymagania i badania dotyczące sprzętu (oryg.)
PN-EN 61131-3	Sterowniki programowalne. Część 3: Języki programowania (oryg.)
PN-EN 61131-5	Sterowniki programowalne. Część 5: Komunikacja (oryg.)
PN-EN 61131-7	Sterowniki programowalne. Część 7: Programowanie rozmyte (oryg.)
PN-EN 61511-1	Bezpieczeństwo funkcjonalne. Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego. Część 1: Schemat, definicje, wymagania dotyczące systemu, sprzętu i oprogramowania
PN-EN 61511-2	Bezpieczeństwo funkcjonalne. Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego. Część 2: Wytyczne do stosowania IEC 61511-1
PN-EN 61511-3	Bezpieczeństwo funkcjonalne. Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego. Część 3: Wytyczne do określania poziomów wymaganych nienaruszalności bezpieczeństwa

7.4 PN-EN ISO

PN-EN ISO 13849-1:	Bezpieczeństwo maszyn. Elementy systemów sterowania związane z bezpieczeństwem. Część 1: Ogólne zasady projektowania (oryg.).
PN-EN ISO 12100 zmniejszanie ryzyka.	Bezpieczeństwo maszyn – Ogólne zasady projektowania – Ocena ryzyka i

7.5 PN-IEC

PN-IEC 60364	Instalacje elektryczne w obiektach budowlanych.

8 Karta zmian

Lp.	Data	Opis zmian	Zmianę wprowadził
1		Niniejsza specyfikacja zastępuje w całości poprzedni standard Grupy LOTOS S.A. nr PR 07 372 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