prof. dr inż. Tadeusz Missala
Przemysłowy Instytut Automatyki i Pomiarów, Warszawa

BEZPIECZEŃSTWO FUNKCJONALNE URZĄDZEŃ AUTOMATYKI I ROBOTYKI

Streszczenie:
Programowalne urządzenia zautomatyzowane i zrobotyzowane wymagają innego traktowania z punktu widzenia bezpieczeństwa człowieka, niż urządzenia tradycyjne. Pojawił się termin „bezpieczeństwo funkcjonalne". W referacie podano podstawowe określenia związane z tym pojęciem, jego atrybuty oraz wymagania formułowane w odpowiednich dokumentach normalizacyjnych.

Abstrakt:
Programmable equipment of automation and robotics represents such a new set of the properties, that the approach to its safety problems shall be other as in the case of the traditional equipment. The term „functional safety" was introduced. The paper deals with the fundamental definitions concerned this term, its attributes, as well as the technical requirements formulated in the relevant standardisation documents.

1. WSTĘP

Rozpowszechnianie się zautomatyzowanych urządzeń produkcyjnych i obsługowych, w tym robotów i systemów zrobotyzowanych, wprowadza nowy poziom komfortu ale i nowe zagrożenia w otoczenie człowieka. Szczególną rolę mają tu urządzenia programowalne, obecnie mikroprocesorowe, tym bardziej, że one właśnie lokują się w zastosowaniach krytycznych z punktu widzenia bezpieczeństwa. Z jednej strony wprowadzają niespotykane dotąd ułatwienia, z drugiej zaś nieznane dotychczas zagrożenia. Jest oczywiste, że współczesna technika powinna znaleźć odpowiednie środki zaradcze.

W powiązaniu z urządzeniami do nadzoru i sterowania przemysłowych procesów ciągłych i dyskretnych, technika mikroprocesorowa wkroczyła w obszary wymagające wysokiego poziomu nienaruszalności funkcjonowania. Konsekwencjami defektu w systemie mikroprocesorowym mogą być poważne szkody, włączając nadwerężenie zdrowia, a nawet śmierć ludzi.

Przykładowymi dziedzinami zastosowania programowalnych urządzeń automatyki i robotyki są:

- przemysł - pomiary i sterowanie maszyn i procesów oraz realizacja czynności, w tym w warunkach: zagrożenia wybuchem i zagrożenia chemicznego (toksyny);
- technika medyczna - sterowanie urządzeń medycznych oraz realizacja czynności, w tym: operacje: mózgu, serca, naczyń krwionośnych; sztuczne płuco-serce; sztuczna nerka; inkubatory dla niemowląt; aparatura monitorowania chorych; aparatura diagnostyczna;
- technika jądrowa - pomiary i sterowanie oraz realizacja czynności, w tym w: elektrowniach jądrowych; badawczych i doświadczalnych instalacjach nuklearnych; urządzeniach wojskowych; urządzeniach wykorzystujących izotopy (medycyna, agrotechnika itp.);
- transport naziemny - tu między innymi: automatyczne zabezpieczenie ruchu pociągów; automatyczne prowadzenie pociągów; systemy kontrolno-sterujące i nawigacyjne samochodów; systemy pilotowania i nadzoru ruchu ładunków niebezpiecznych;

- lotnictwo i astronautyka - tu między innymi: systemy kontrolno-sterujące i nawigacyjne samolotów i rakiet; systemy automatycznego startu rakiet; systemy naprowadzania na cel; systemy automatycznego lądowania samolotów; wszelkiego typu systemy lotniskowe i kosmodromowe zapewniające bezpieczny ruch;
- górnictwo podziemne i odkrywkowe - tu między innymi: pomiary stężenia metanu i sygnalizacja niebezpieczeństwa; sterowanie maszyn górniczych; automatyzacja urabiania i wydobywania;
- urządzenia ochronne zabezpieczające pracowników przed urazami.

Nic więc dziwnego, że zagadnienia bezpieczeństwa pracy urządzeń mikroprocesorowych od ponad 10 lat są przedmiotem badań i uzgodnień normatywnych. W 1985 roku Rada Ministerialna Organizacji Państw Nordyckich zleciła opracowanie stosownego raportu, który ukazał się w 1987 r.[9]. We wrześniu 1988 r. , na zebraniu w Sztokholmie, Podkomitet 65A IEC powołał dwie grupy robocze: WG9: „Safe software" i WG10 „Functional safety of programmable electronic systems: Generic aspects" . Rezultatem ich prac jest projekt siedmioarkuszowej normy IEC DIS 1508 [6].

2. JAKOŚĆ I BEZPIECZEŃSTWO

Jeżeli przywołać określenie jakości wg PN-ISO 8204: 1996 [8]: ogół właściwości obiektu, wiążących się z jego zdolnością do zaspokojenia stwierdzonych i przewidywanych potrzeb, przy czym obiektem jest: działanie lub proces, wyrób, organizacja, system albo osoba lub też dowolna kombinacja wyżej wymienionych, to widać, że bezpieczeństwo dowolnego obiektu jest atrybutem jego jakości.

Jak odczuwamy bezpieczeństwo ? Lapidarnie można to sformułować następująco: urządzenie nie zagraża człowiekowi ani środowisku gdy:
- Pracuje normalnie;
- Przypadkiem się z nim źle obejdziemy - może się popsuć, ale np. nie wybuchnie;
- Ulegnie samoczynnemu uszkodzeniu - może przestać działać, ale nie będzie zagrażać ani człowiekowi ani środowisku.

Stosuje się tu prawo robotyki Asimowa -
Robot nie ma prawa uczynić krzywdy człowiekowi.

Wszystkie urządzenia techniczne są więc badane pod względem tak zwanego bezpieczeństwa użytkowania. Odnoszą się do tego m.in. normy [1,2,3,4,5,7]. Atrybutami bezpieczeństwa użytkowania są np.:
- sprawdzenie bezpieczeństwa pracy urządzenia w stanie normalnym, np. stanu izolacji, prądu upływu, poziomu emisji promieniowania (tu komputery) itp.;
- sprawdzenie bezpieczeństwa działania w stanie pojedynczego uszkodzenia;
- sprawdzenie bezpieczeństwa działania w warunkach nienormalnego użytkowania, np. po zakleszczeniu się wirnika silnika elektrycznego
- sprawdzenie odporności na wpływy środowiska: klimatyczne, mechaniczne, elektromagnetyczne, oddziaływania specjalne, przykładowo promieniowanie jądrowe.

Ocena bazuje na wykonaniu prób i sprawdzeń. Jest ona **oceną deterministyczną.**

Jak wykazuje doświadczenie własne oraz literatura [9 - 13] takie podejście nie jest wystarczające w przypadku urządzeń programowalnych, szczególnie mikroprocesorowych. Nie można bowiem przeprowadzić prób obejmujących wszystkie możliwe stany systemu i tym bardziej jest to niewykonalne, im system jest bardziej złożony. Powstało nowe podejście do zagadnienia - **bezpieczeństwo funkcjonalne (functional safety).**

Atrybuty bezpieczeństwa funkcjonalnego (bf) można scharakteryzować następująco:

- pojęcie jest stosowane do systemów i funkcji związanych z zapewnieniem bezpieczeństwa działania urządzeń i systemów;
- bezpieczeństwo funkcjonalne uzyskuje się przez eliminowanie, metodami zapobiegawczymi, przyczyn mogących wywołać uszkodzenia systematyczne (tj. jakby „wrodzone wady konstrukcji");
- miarą bezpieczeństwa funkcjonalnego są wskaźniki probabilistyczne;
- drogą do uzyskania bezpieczeństwa funkcjonalnego jest stosowanie odpowiednich procedur postępowania przez odpowiednio biegły personel;
- drogą do upewnienia się o osiągnięciu wymaganego poziomy bezpieczeństwa funkcjonalnego jest systematyczne auditowanie i oceniane grup czynności;

Pojęcie bezpieczeństwa funkcjonalnego jest odnoszone , w szczególności, do programowalnych urządzeń elektronicznych.

3. BEZPIECZEŃSTWO FUNKCJONALNE

3.1. Określenia podstawowe

Bezpieczeństwo funkcjonalne - zdolność systemu związanego z bezpieczeństwem do wykonania działań niezbędnych do osiągnięcia stanu bezpiecznego przez urządzenie (system) ochraniane lub do utrzymania stanu bezpiecznego urządzenia (systemu) ochranianego [6]

System związany z bezpieczeństwem - system który:

- implementuje funkcje bezpieczeństwa wymagane do osiągnięcia stanu bezpiecznego urządzenia (systemu) sterowanego/ochranianego lub do utrzymania stanu bezpiecznego tego urządzenia (systemu) [6]
- jest przewidziany, sam lub w powiązaniu z innymi systemami związanymi z bezpieczeństwem, do osiągnięcia koniecznego poziomu nienaruszalności bezpieczeństwa w implementacji wymaganych funkcji bezpieczeństwa [6]

Zagrożenie (hazard) - możliwość doznania urazu lub nadwerężenia zdrowia [3].

Ryzyko (risk) - kombinacja prawdopodobieństwa wystąpienia i stopnia możliwego urazu lub nadwerężenia zdrowia w sytuacji zagrożenia [3].

Ocena bezpieczeństwa funkcjonalnego - badanie podjęte w celu dojścia do stwierdzenia, popartego dowodami, o osiągnięciu bezpieczeństwa funkcjonalnego przez jeden lub kilka systemów związanych z bezpieczeństwem i/lub przez zewnętrzne urządzenia ograniczające ryzyko [6].

Audit bezpieczeństwa funkcjonalnego - systematyczne i niezależne sprawdzanie w celu stwierdzenia, czy procedury wyraźnie adresowane do wymagań bezpieczeństwa funkcjonalne-

go są zgodne z zaplanowanymi działaniami, czy są efektywnie wdrożone oraz czy są odpowiednie do osiągnięcia zamierzonych celów [6].

Nienaruszalność bezpieczeństwa - prawdopodobieństwo, że system związany z bezpieczeństwem będzie zadowalająco realizował wymagane funkcje bezpieczeństwa w wymaganych warunkach i w wymaganym przedziale czasu [6]

Cykl trwałości bezpieczeństwa - niezbędne działania wchodzące w implementację systemów związanych z bezpieczeństwem, występujące w okresie czasu od rozpoczęcia opracowywania koncepcji projektu aż do chwili gdy żaden z systemów związanych z bezpieczeństwem nie nadaje się już do używania [6].
Funkcje związane z bezpieczeństwem - wybrane z [5]- to m.in.: stop; stop awaryjny; reset ręczny; start i restart; czas odpowiedzi; parametry związane z bezpieczną pracą: położenie, prędkość, temperatura, ciśnienie; lokalne funkcje sterowania np. panel przenośny/podwieszony; ręczne zawieszanie funkcji bezpieczeństwa.

3.2. Wymagania ogólne

Norma [6] precyzuje następujące warunki uzyskania bezpieczeństwa funkcjonalnego:

1. Posiadanie przez każdą z organizacji, związaną z projektowaniem, produkcją i użytkowaniem urządzeń, systemu zapewnienia jakości wg ISO 9000 lub podobnego.
2. Spełnienie wymienionych w normie wymagań i prowadzenie zapisów to wykazujących .
3. Wykazanie, że osoby odpowiedzialne za jakikolwiek element cyklu zapewnienia bezpieczeństwa mają wystarczające kompetencje do ponoszenia takiej odpowiedzialności.
4. Istnienie PLANU ZAPEWNIENIA BEZPIECZEŃSTWA jako części PLANU JAKOŚCI dotyczącego rozpatrywanego przedsięwzięcia.
5. Opracowanie cyklu trwałości (uzyskania i utrzymania) bezpieczeństwa, od fazy koncepcji do ostatecznego złomowania produktu.
6. Przeprowadzenie analizy zagrożeń i ryzyka.
7. Istnienie sformułowanych wymagań w zakresie bezpieczeństwa, w tym poziomu nienaruszalności (integrity) bezpieczeństwa.
8. Przypisanie (alokacja) poszczególnych wymagań do konkretnych elementów sprzętu i oprogramowania, w tym stosowania zewnętrznych środków zapewnienia bezpieczeństwa
9. Istnienie planu użytkowania i serwisu
10. Istnienie planu zatwierdzania, weryfikacji i oceny realizacji poszczególnych elementów projektu oraz urządzenia jako całości, pod względem bezpieczeństwa, w tym plan auditów.
11. Istnienie procedury instalowania i przekazywania do eksploatacji oraz zatwierdzania wykonania tych prac.
12. Istnienie procedury złomowania.

Przykładowe obszary zastosowania wymagań normy [6] to:

- przemysł przetwórczy - systemy bezpieczeństwa wyłączające (systemy wyłączania awaryjnego), systemy wykrywania gazu, systemy sterowania palnikami/paleniskami;
- przemysł wytwórczy - roboty przemysłowe i obrabiarki;
- transport - sygnalizacja kolejowa i zabezpieczenie ruchu pociągów, systemy hamulcowe, windy i dźwigi;
- medycyna - wszelka aparatura elektromedyczna, roboty operacyjne i inne inwazyjne, radiografia;
- inne - systemy wykrywania pożaru, urządzenia rekreacyjne wesołych miasteczek

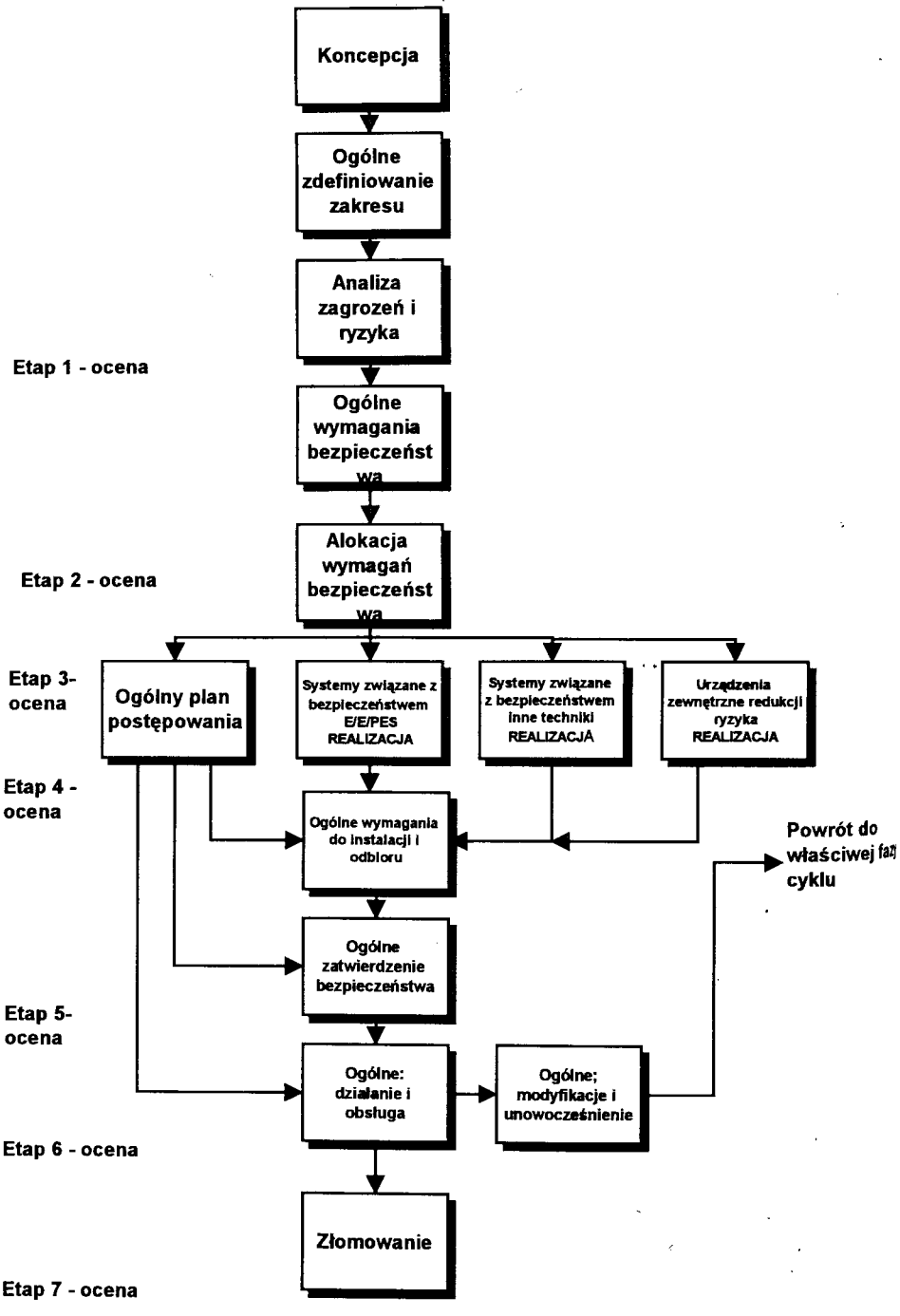
3.3. Cykl trwałości bezpieczeństwa

Podstawowym wymaganiem formułowanym przez normę [6] jest zrealizowanie cyklu trwałości bezpieczeństwa - rys. 1.

Komentarzem do przedstawionego rysunku jest tablica 1.

Tablica 1. Cele do osiągnięcia i ich składowe

CELE	SKŁADOWE CELÓW
Obiekty nienaruszalności bezpieczeństwa są dobrane prawidłowo w odniesieniu do ryzyka dopuszczalnego	* ryzyko dopuszczalne zostało zdefiniowane; * ryzyko zostało przeanalizowane; * ryzyko jest wymierzone właściwie odnośnie do zastosowanych systemów związanych z bezpieczeństwem.
Wymagania funkcjonalne zostały prawidłowo zdefiniowane	* wymagania wyspecyfikowano; * funkcje związane z bezpieczeństwem zostały zdefiniowane.
Bezpieczeństwo funkcjonalne zostało zrealizowane	* usunięto błędy; * opanowano źródła błędów.
Bezpieczeństwo funkcjonalne jest utrzymywane lub powiększane w eksploatacji	* jest projekt operatorski; * jest projekt serwisu; * są procedury operatorskie; * są procedury serwisu.
Bezpieczeństwo funkcjonalne jest zapewnione	* zostały zatwierdzone wymagania dotyczące bezpieczeństwa funkcjonalnego; * został oceniony poziom nienaruszalności bezpieczeństwa; * zamieszczono w dokumentach klauzulę o udowodnieniu osiągnięcia celów w zakresie bezpieczeństwa.



rys. 1. Ogólny cykl trwałości bezpieczeństwa

3.4. Wymagania dotyczące nienaruszalności bezpieczeństwa

Do sformułowania wymagań określających poziomy nienaruszalności bezpieczeństwa (SIL) stosuje się podział systemów podany w tablicy 2.

Tablica 2. Relacja systemów sterowania i ochronnych związanych z bezpieczeństwem i ich trybów pracy

TRYB PRACY	TYP SYSTEMU ZWIĄZANEGO Z BEZPIECZEŃSTWEM	
	Sterowanie	Ochrona
Na wezwanie	Wymaga się aby system sterowania pracował w krótkich przedziałach czasu np. ABS	Systemy ochronne których liczba zadziałań jest małą w porównaniu z liczbą testów sprawdzających (np. system odcięcia instalacji chemicznej)
Ciągły / na częste wezwanie	Wymaga się, aby system pracował mniej lub więcej ciągle w długich przedziałach czasu np. stymulator pracy serca	Systemy ochronne których liczba zadziałań jest dużą w porównaniu z liczbą testów sprawdzających (np. fotoelektryczny system ochronny maszyny)

Wartości prawdopodobieństwa poprawnej pracy, wymagane w odniesieniu do poziom nienaruszalności bezpieczeństwa i trybu pracy systemu wg tablicy 2, zestawiono w tablicy 3.

Tablica 3. Wartości prawdopodobieństwa poprawnej pracy wymagane dla określonych poziomów nienaruszalności bezpieczeństwa.

POZIOM NIENARUSZALNOŚCI BEZPIECZEŃSTWA (SIL)	TRYB PRACY NA WEZWANIE (prawdopodobieństwo upośledzenia zaprojektowanej funkcji systemu, realizowanej na żądanie)	TRYB PRACY CIĄGŁY LUB NA CZĘSTE WEZWANIE (prawdopodobieństwo niebezpiecznego uszkodzenia w ciągu roku pracy)
4	$\geq 10^{-5} \leq 10^{-4}$	$\geq 10^{-5} \leq 10^{-4}$
3	$\geq 10^{-4} \leq 10^{-3}$	$\geq 10^{-4} \leq 10^{-3}$
2	$\geq 10^{-3} \leq 10^{-2}$	$\geq 10^{-3} \leq 10^{-2}$
1	$\geq 10^{-2} \leq 10^{-1}$	$\geq 10^{-2} \leq 10^{-1}$

Wymagania związane z przeprowadzaniem oceny jakości wykonania poszczególnych etapów postępowania w cyklu trwałości bezpieczeństwa, zaznaczonych na rys. 1, podano w tablicach 4 i 5. Użyte symbole mają następujące znaczenie:

- HR - ten poziom niezależności oceniających (auditorów) jest wysoce zalecany; w przypadku przyjęcia niższego poziomu niezależności, należy to uzasadnić;
- NR - ten poziom niezależności oceniających (auditorów) jest stanowczo nie zalecany; w przypadku przyjęcia tego zbyt niskiego poziomu niezależności, należy to uzasadnić.

Tablica 4. Minimalny poziom niezależności auditorów oceniających bezpieczeństwo funkcjonalne (rys. 1, etapy 1, 2, 5, 6 i 7)

MINIMALNY POZIOM NIEZALEŻNOŚCI	KONSEKWENCJE			
	POMIJALNE	NIEWIELKIE	KRYTYCZNE	KATASTROFICZNE
Osoba niezależna	HR	HR	NR	NR
Dział niezależny	-	HR	HR	NR
Organizacja niezależna	-	-	HR	HR

Tablica 5. Minimalny poziom niezależności auditorów oceniających bezpieczeństwo funkcjonalne (rys. 1, etapy 3 i 4)

MINIMALNY POZIOM NIEZALEŻNOŚCI	POZIOM NIENARUSZALNOŚCI BEZPIECZEŃSTWA			
	1	2	3	4
Osoba niezależna	HR	HR	NR	NR
Dział niezależny	-	HR	HR	NR
Organizacja niezależna	-	-	HR	HR

3.5. Wymagania dotyczące wykrywania przypadkowych defektów sprzętu [ ]

Wymagania określające sposoby wykrywania defektów przypadkowych , jakie mogą wystąpić w sprzęcie oraz reakcje systemu zestawiono w tablicy 6. Przyjęto w niej poniżej podane kryteria podziału na elementy o małej i dużej sumie ogólnej defektów.

Elementy o małej sumie ogólnej defektów (low fault count components) to:

- elementy w pełni przetestowane;
- są wiarygodne dane o uszkodzeniach wynikające z doświadczeń zebranych na obiektach;
- za wiarygodne dane o uszkodzeniach uznaje się dane zestawione na podstawie 100 tys. godzin pracy w ciągu 2-ch lat, 10 systemów w różnych zastosowaniach.

Jeżeli dowolny z tych trzech warunków nie jest spełniony, to element zalicza się do grupy elementów o dużej sumie ogólnej defektów (high fault count components).

Tablica 6. Wymagania dotyczące przypadkowych defektów sprzętu

SIL	WYMAGANIA DOTYCZĄCE DEFEKTÓW (DEFEKTÓW PRZYPADKOWYCH) ELEMENTÓW O MAŁEJ SUMIE OGÓLNEJ DEFEKTÓW	WYMAGANIA DOTYCZĄCE DEFEKTÓW (DEFEKTÓW PRZYPADKOWYCH) ELEMENTÓW O DUŻEJ SUMIE OGÓLNEJ DEFEKTÓW
1	Nie wykryte defekty związane z bezpieczeństwem są wykrywane przez sprawdzenie kontrolne.	Nie wykryte defekty związane z bezpieczeństwem są wykrywane przez sprawdzenie kontrolne.
2	Nie wykryte defekty związane z bezpieczeństwem są wykrywane przez sprawdzenie kontrolne.	W przypadku elementów nie objętych diagnostyką on-line w średniej skali system powinien realizować funkcje bezpieczeństwa w stanie pojedynczego defektu. Nie wykryte defekty związane z bezpieczeństwem są wykrywane przez sprawdzenie kontrolne.
3	W przypadku elementów nie objętych diagnostyką on-line w średniej skali system powinien realizować funkcje bezpieczeństwa w stanie pojedynczego defektu. Nie wykryte defekty związane z bezpieczeństwem są wykrywane przez sprawdzenie kontrolne.	W przypadku elementów objętych diagnostyką on-line w wysokiej skali, system powinien realizować funkcje bezpieczeństwa w warunkach pojedynczego defektu. Nie wykryte defekty związane z bezpieczeństwem są wykrywane przez sprawdzenie kontrolne.
4	W przypadku elementów nie objętych diagnostyką on-line w wysokiej skali, system powinien realizować funkcje bezpieczeństwa w warunkach dwóch defektów. Nie wykryte defekty związane z bezpieczeństwem są wykrywane przez sprawdzenie kontrolne. Ilościowa analiza sprzętu powinna bazować na założeniu najgorszego przypadku.	Elementy powinny realizować funkcje bezpieczeństwa w warunkach dwóch defektów. Defekty powinny być wykrywane za pomocą diagnostyki on-line wysokiej skali. Nie wykryte defekty związane z bezpieczeństwem są wykrywane przez sprawdzenie kontrolne. Ilościowa analiza sprzętu powinna bazować na założeniu najgorszego przypadku.

Znaczenie pojęć dotyczących diagnostyki jest podane w tablicy 9.

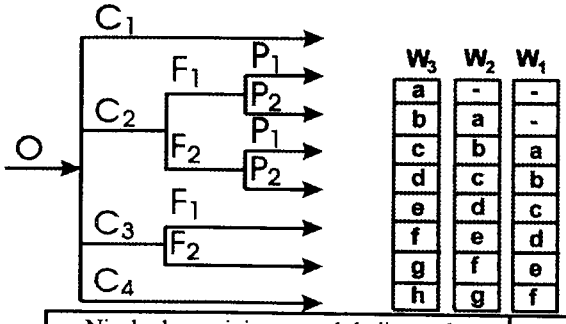
4. PRZYKŁADOWE TECHNIKI I STRATEGIE POSTĘPOWANIA

4.1. Ocena zagrożeń i ryzyka

Postępowaniem, które w świetle wymagań [5,6] musi zostać bezwzględnie przeprowadzone, jest ocena zagrożeń i ryzyka. Wymienione normy podają odpowiednią metodykę postępowania. Symbole stosowane w opisie postępowania zestawiono w tablicy 7, zaś graf ilustrujący postępowanie podano na rys. 2. [6].

Tablica 7. Ocena ryzyka - znaczenie symboli

PARAMETR RYZYKA	SYMBOL	KLASYFIKACJA
Konsekwencje (C)	C_1	Niewielkie urazy
	C_2	Poważne ciągłe urazy dotykające jednej lub kilku osób, śmierć jednej osoby
	C_3	Śmierć kilku osób
	C_4	Śmierć bardzo dużej liczby osób
Częstotliwość i czas narażania (F)	F_1	Rzadkie do częstszego narażanie w strefie zagrożenia
	F_2	Częste do ciągłego narażanie w strefie zagrożenia
Możliwość uniknięcia zdarzeń zagrażających (P)	P_1	Możliwe przy spełnieniu pewnych warunków
	P_2	Zupełnie niemożliwe
Prawdopodobieństwo zajścia zdarzeń niepożądanych (W)	W_1	Bardzo niewielkie prawdopodobieństwo, że zajdzie zdarzenie niepożądane i tylko nieliczne zdarzenia niepożądane są prawdopodobne
	W_2	Niewielkie prawdopodobieństwo, że zajdzie zdarzenie niepożądane i mało zdarzeń niepożądanych jest prawdopodobnych
	W_3	Relatywnie wysokie prawdopodobieństwo, że zajdzie zdarzenie niepożądane i liczne zdarzenia niepożądane są prawdopodobne



Niezbędne minimum redukcji ryzyka	Wymagany poziom nienaruszalności bezpieczeństwa
-	nie ma wymagań bezpieczeństwa
a	nie ma specjalnych wymagań bezpieczeństwa
b,c	1
d	2
e,f	3
g	4
h	ten rodzaj urządzenia jest niewystarczający

rys. 2. Ocena zagrożeń i ryzyka - graf.

Analizę rozpoczyna się w punkcie startowym O. Niech powodem zagrożenia jest otwarcie drzwi do strefy niebezpiecznej. Po pierwsze należy ocenić konsekwencje C - jeżeli są one znikome (C_1), to dalsza analiza jest niepotrzebna i niezależnie od prawdopodobieństwa zajścia tego niepożądanego zjawiska nie formułuje się wymagań dotyczących nienaruszalności bezpieczeństwa.
Gdy konsekwencje ocenia się jako katastroficzne (C_4), to zależnie od prawdopodobieństwa W ustala się wymagany poziom nienaruszalności bezpieczeństwa na 3, 4 lub ocenianą instalację dyskwalifikuje się.
Gdy konsekwencje ocenia się na poziomie C_2 lub C_3, należy prowadzić dalszą analizę, postępując według grafu i ustalając wymagane poziomy nienaruszalności bezpieczeństwa.

Norma [5] podaje nieco inną metodę oceny, prowadzącą do ustalenia kategorii bezpieczeństwa.

4.2. Wybrane strategie

Szczególnie ważną jest strategia wykrywania defektów przypadkowych i minimalizowania ich skutków oraz zapobiegania powstawaniu defektów systematycznych, do których należą:
◊ błędy ustalania wymagań;
◊ błędy wyposażenia;
◊ błędy oprogramowania;
◊ błędy wspólnej przyczyny w układach zredundowanych.
Strategia ta to trzy - punktowa strategia zapobiegania defektom, która obejmuje:
♦ zapewnienie wysokiej niezawodności;
♦ opracowanie i wprowadzenie konfiguracji odpornej na błędy;
♦ posiadanie systemu jakości przez wszystkie organizacje uczestniczące w procesu projektowania i realizacji.

4. 3. Projektowanie i prace rozwojowe

Jako przykłady technik stosowanych w pracach rozwojowych przedstawiono testowanie modułów oprogramowania - odpowiednie wymagania, wg [6], podano w tablicy 8

Tablica 8. Wymagania dotyczące testowania oprogramowania

TECHNIKI / METODY	SIL 1	SIL 2	SIL 3	SIL 4
1. Testowanie propabilistyczne	-	R	R	HR
2. Analiza i testowanie dynamiczne	R	HR	HR	HR
3. Rejestrowanie i analiza danych	HR	HR	HR	HR

Należy zauważyć, że testowanie modułów oprogramowania jest działaniem weryfikacyjnym, przy czym technika/metoda powinny zostać wybrane odpowiednio do wymaganego poziomu nienaruszalności bezpieczeństwa. Satysfakcjonujące jest zastosowanie jednej z pomiędzy równoważnych technik/metod.

4.4.Techniki / metody zapewnienia nienaruszalności bezpieczeństwa urządzeń elektronicznych

Jako przykłady technik stosowanych do zapewnienia nienaruszalności bezpieczeństwa urządzeń zestawiono w tablicy 9 metody diagnostyki wraz z oceną odpowiedniego zakresu zapewnianego przez każdą z metod [6].

Tablica 9. Techniki/metody diagnostyki urządzeń

TECHNIKA / METODA	ZAKRES DIAGNOSTYKI (DC)	UWAGI
wykrywanie uszkodzeń na podstawie obserwacji procesu (on-line)	niski do średniego	zależy od zakresu wykrywania uszkodzeń wewnątrz sprzętu
komparator	średni do wysokiego	wysoki, gdy bezpieczny
głosowanie większościowe	średni do wysokiego	zależy od jakości głosowania
próba z wykorzystaniem redundancji sprzętu	niski do średniego	zależy od zakresu wykrywania uszkodzeń wewnątrz sprzętu
zasady dynamiczne	niski do średniego	zależy od zakresu wykrywania uszkodzeń
portów dostępu do testów standardowych i architektury skanowania brzegów	niski do wysokiego	zależy od zakresu wykrywania uszkodzeń
sprzęt bezpieczny (doprowadzenie systemu do stanu bezpiecznego gdy nastąpi uszkodzenie)	wysoki	
redundancja monitorowana	średni do wysokiego	zależy od stopnia zredundowania i nadzoru
sprzęt sprawdzany automatycznie	niski do wysokiego	zależy od zakresu sprawdzeń

LITERATURA

[1] PN-M-42087:1994 (ISO 10218:1992) *Roboty przemysłowe. Bezpieczeństwo.*

[2] prPN-EN 60204-1:1992 - *Wyposażenie elektryczne maszyn. Arkusz 1: Wymagania ogólne.*

[3] pr PN-EN 292-2:1994 - *Bezpieczeństwo maszyn. Pojęcia podstawowe. Ogólne zasady projektowania.*
- *Arkusz 1:Określenia*
- *Arkusz 2: Zasady i wymagania techniczne.*

[4] PN-IEC 1010-1:1996 - *Wymagania bezpieczeństwa dotyczące elektrycznych przyrządów pomiarowych, automatyki i urządzeń laboratoryjnych. Arkusz 1: Wymagania ogólne. oraz uzupełnienia do niego: Uzupełnienie 1:1992 i Uzupełnienie 2: 1994.*

[5] EN 954-1:1993 - *Bezpieczeństwo maszyn - Części układu sterowania związane z bezpieczeństwem - Arkusz 1:Ogólne zasady projektowania.*

[6] IEC DIS 1508*: Bezpieczeństwo funkcjonalne: systemy związane z bezpieczeństwem.*
- *Arkusz 1: Wymagania ogólne.*
- *Arkusz 2: Wymagania dotyczące układów elektrycznych/elektronicznych/programowalnych elektronicznych.*
- *Arkusz 3: Wymagania dotyczące oprogramowania.*
- *Arkusz 4: Określenia.*
- *Arkusz 5: Wytyczne do stosowania arkusza 1.*
- *Arkusz 6: Wytyczne do stosowania arkuszy 2 i 3.*
- *Arkusz 7: Bibliografia stosowanych technik.*

[7] PN-ISO 11161: 1997 - *Systemy Automatyki przemysłowej. Bezpieczeństwo zintegrowanych systemów wytwarzania. Wymagania podstawowe.*

[8] PN-ISO 8402: 1996 - *Zarządzanie jakością i zapewnienie jakości. Terminologia.*

[9] *Personal safety in microprocessor control systems.* Nordisk Ministerrad. Kopenhaga 1987.

[10] Vautrin J-P.: *The concept of EN 954 cathegories for the design and the testing.* Raport National Research and Safety Institute. Department of Electronics and Safety Systems (F).

[11] Reinert D. i inni: *Validation of functional safety of programmable electronic systems according to IEC 1508.* Raport Berufsgenossenschaftliches Institut für Arbeitssicheerheit(BIA) i Institut für Qualität und Sicherheit in der Elektronik(IQSE) (G).

[12] Tiusanen R., Hietikko M., Kivipuro M.: *The safety assesment method for programmable electronics.* Raport Technical Research Centre of Finland. Tampere 1994.

[13] Bremer P., Haallden Á., Jacobson J.: *Mikroprocomputer-based protective functions in industrial production systems. Assesment method.* Swedish National Testing and Research Institute. Physics and Electronics. SP Report 1993:51.