

BEZPIECZENSTWO FUNKCJONALNE NA SŁUŻBIE OCHRONY ŚRODOWISKA

Przytoczono wybrane wymagania wynikające z prawodawstwa obowiązującego w zakresie ochrony środowiska i przedstawiono przykłady narzędzia jakich dostarcza technika bezpieczeństwa funkcjonalnego wg serii PN-EN 61508:2003(U) i serii EN 61511:2004 w zakresie projektowania procesów bezpiecznych dla środowiska

FUNCTIONAL SAFETY ON THE DUTY OF ENVIRONMENT PROTECTION

The chosen requirements resulting from the legislation concerning the environmental protection are referenced, as well as are presented the examples of tools, which are available for environment protection by the techniques of functional safety described in PN-EN 61508:2003(U) series and EN 61511:2004 series.

1. WPROWADZENIE

1.1. Wstęp

W referacie [1], prezentowanym na poprzedniej konferencji AUTOMATION przedstawiono wzajemne relacje między systemem zarządzania jakością spełniającym wymagania PN-EN ISO 9001: 2001[2] i zarządzaniem bezpieczeństwem funkcjonalnym opisanym w PN-EN 61508-1: 2003 [3]. Obecnie tematem jest wykorzystanie technik bezpieczeństwa funkcjonalnego opisanych w [3] i [4] w celu zapewnienia zminimalizowania zagrożeń dla środowiska, jakie niesie produkcja przemysłowa i transport jej wytworów. Odpowiednie przepisy prawne, których należy przestrzegać są zamieszczone w Ustawie „Prawo ochrony środowiska” [5] i one są punktem wyjścia dalszych rozważań.

1.2. Wybrane definicje [5]

- **emisja** – wprowadzane bezpośrednio lub pośrednio, w wyniku działalności człowieka, do powietrza, wody, gleby lub ziemi:
 - substancje,
 - energie, takie jak ciepło, hałas, wibracje lub pola elektromagnetyczne;
- **pole elektromagnetyczne** – pole elektryczne, magnetyczne oraz elektromagnetyczne o częstotliwościach od 0 Hz do 300 GHz;
- **poważna awaria** – zdarzenie, w szczególności emisja, pożar lub eksplozja, powstałe w trakcie procesu przemysłowego, magazynowania lub transportu, w którym występuje jedna lub więcej niebezpiecznych substancji, prowadzące do natychmiastowego powstania zagrożenia życia lub zdrowia ludzi lub środowiska lub powstania takiego zagrożenia z opóźnieniem;

- **poważna awaria przemysłowa** – poważna awaria w zakładzie;
- **prowadzący instalację lub zakład** – podmiot uprawniony na podstawie określonego tytułu prawnego do władania instalacją w celu jej eksploatacji zgodnie z wymaganiami ochrony środowiska, na zasadach wskazanych w ustawie;
- **środowisko** – ogół elementów przyrodniczych, w tym także przekształconych w wyniku działalności człowieka, a w szczególności powierzchnię ziemi, kopaliny, wody powietrze, zwierzęta i rośliny, krajobraz oraz klimat;
- **zanieczyszczenie** – emisja, która może być szkodliwa dla zdrowia ludzi lub stanu środowiska, może powodować szkodę w dobrach materialnych, może pogarszać walory estetyczne środowiska lub może kolidować z innymi, uzasadnionymi sposobami korzystania ze środowiska.

1.3. Wybrane wymagania restrykcyjne Ustawy [5]

- kto podejmuje działalność mogącą negatywnie oddziaływać na środowisko, jest obowiązany do zapobiegania temu oddziaływaniu;
- kto podejmuje działalność, której negatywne oddziaływanie na środowisko nie jest jeszcze w pełni rozpoznane, jest obowiązany, kierując się przezornością, podjąć wszelkie możliwe środki zapobiegawcze;
- kto powoduje zanieczyszczenie środowiska, ponosi koszty usunięcia skutków tego zanieczyszczenia;
- kto może spowodować zanieczyszczenie środowiska, ponosi koszty zapobiegania temu zanieczyszczeniu;
- wydanie decyzji w sprawie planowanego przedsięwzięcia mogącego znacząco oddziaływać na środowisko wymaga przeprowadzenia postępowania w sprawie oceny oddziaływania na środowisko;
- w postępowaniu w sprawie oceny oddziaływania na środowisko określa się, analizuje oraz ocenia – m.in. możliwości oraz sposoby zapobiegania i ograniczania negatywnego oddziaływania na środowisko;
- raport o oddziaływaniu przedsięwzięcia na środowisko powinien zawierać – m.in. – opis przewidywanych działań mających na celu zapobiegania, ograniczenie lub kompensację przyrodniczą negatywnych oddziaływań na środowisko oraz wskazanie trudności wynikających z niedostatków techniki lub luk we współczesnej wiedzy, jakie napotkano, opracowując raport;

1.4. Rola technik bezpieczeństwa funkcjonalnego

Techniki bezpieczeństwa funkcjonalnego umożliwiają, w odniesieniu do procesów przemysłowych:

- ustalenie poziomu ryzyka tolerowalnego z punktu widzenia ochrony środowiska;
- przeprowadzenie analizy zagrożeń środowiska naturalnego i powstającego ryzyka;
- dobranie środków technicznych do zmniejszenia ryzyka do poziomu tolerowalnego, lub wykazać konieczność przeprojektowania procesu.

2. ZASADY OCENY I REDUKCJI RYZYKA

2.1. Ryzyko tolerowalne

Ryzyko tolerowalne będzie zależeć od wielu czynników: zakresu zanieczyszczenia środowiska i innych szkód środowiskowych, liczby osób narażonych na niebezpieczeństwo, długotrwałości narażenia na niebezpieczeństwo. Ważnymi czynnikami będą tu spostrzegawczość i możliwość widzenia ze strony osób narażonych na zdarzenia zagrażające oraz możliwość przeciwdziałania pojawiającym się zdarzeniom zagrażającym. Przy dochodzeniu do konkluzji, jakie jest ryzyko tolerowalne w określonym zastosowaniu, rozważa się pewną liczbę danych wejściowych zawierających m.in.:

- wytyczne odpowiedniej jednostki określającej przepisy bezpieczeństwa;
- dyskusje i uzgodnienia z różnymi stronami zaangażowanymi w to konkretne zastosowanie;
- normy i przewodniki przemysłowe;
- międzynarodowe dyskusje i uzgodnienia; rola i ważkość norm krajowych i międzynarodowych stale wzrasta w procesie dochodzenia do kryteriów ryzyka tolerowalnego w odniesieniu do konkretnego zastosowania;
- najlepsze niezależne porady przemysłowe, eksperckie i naukowe ze strony instytucji doradczych;
- wymagania prawne, tak ogólne jak i dotyczące bezpośrednio konkretnego zastosowania.

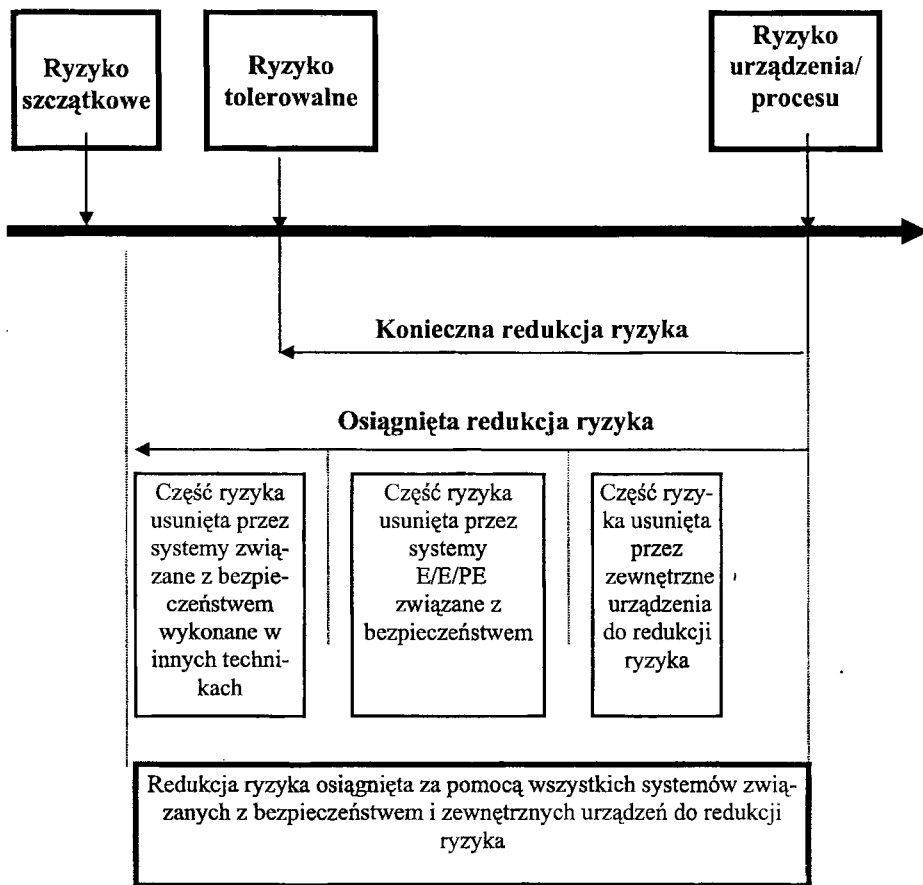
2.2. Schemat ogólny redukcji ryzyka

Schemat ogólny redukcji ryzyka przedstawiono na rysunku 1. Rodzaje ryzyka na nim wyszczególnione mają następujące znaczenie:

- *ryzyko urzędnika/procesu* - ryzyko, w odniesieniu do określonego zdarzenia zagrażającego, istniejące w urzędzeniu/procesie, systemie sterowania urządzeniem/procesem i powiązanymi z nim czynnikami ludzkimi, przy czym nie są brane pod uwagę żadne zabezpieczenia ochronne;
- *ryzyko tolerowalne* - ryzyko, które jest akceptowane w określonym kontekście na bazie bieżących wskaźników przyjętych w społeczeństwie (np. NDS);
- *ryzyko szczątkowe* - w rozumieniu IEC 61508-5 jest to ryzyko, w odniesieniu do określonego zdarzenia zagrażającego, pozostające w urzędzeniu/procesie, systemie sterowania urządzeniem/procesem i powiązanymi z nim czynnikami ludzkimi, lecz po wprowadzeniu

Zaznaczone redukcje ryzyka to:

- redukcja ryzyka osiągnięta za pomocą elektrycznych/elektronicznych programowalnych elektronicznych urządzeń związanych z bezpieczeństwem [4];
- redukcja ryzyka osiągnięta przez innego rodzaju urządzenia związane z bezpieczeństwem (elektromechaniczne, pneumatyczne, mechaniczne, hydrauliczne itp.);
- redukcja ryzyka osiągnięta przez dodatkowe urządzenia ochronne lub zabezpieczające, np. obwałowania, tamy.



Rysunek 1 - Ogólna koncepcja redukcji ryzyka

Redukcja ryzyka wynikająca z wprowadzenia systemów związanych z bezpieczeństwem jest osiągana przez zastosowanie urządzeń zabezpieczających/ochronnych o odpowiednim poziomie nienaruszalności bezpieczeństwa – SIL - [3], przy czym w przypadku instalacji procesowych to będą przyrządowe systemy związane z bezpieczeństwem [4].

Jest wiele metod oszacowania ryzyka i doboru SIL urządzeń zabezpieczających, z których zostaną naszkicowane dwie [4]:

- zasada ALARP (As Low As Reasonably Practicable), za której pomocą zostanie przedstawiona ogólna koncepcja postępowania;
- metoda grafów kalibrowanych dostosowana do zagadnienia ochrony środowiska.

3. ZASADA ALARP [4]

3.1. Wprowadzenie

Przy analizie zagrożeń i ryzyka mogą wystąpić trzy sytuacje:

1. ryzyko jest tak duże, że w ogóle się odrzuca możliwość eksploataowania obiektu;
2. ryzyko jest lub może być tak małe, że można je uważać za bez znaczenia;
3. ryzyko mieści się między stanami 1 i 2 i **może** być zredukowane do najniższego praktycznie poziomu, mając na względzie korzyści wynikające z jego zaakceptowania i biorąc pod uwagę koszty dalszej redukcji.

W odniesieniu do przypadku 3 zasada ALARP zaleca, aby dowolne ryzyko zostało zredukowane do poziomu tak niskiego, jak to jest rozsądnie wykonalne. Jeśli ryzyko mieści się między wymienionymi wyżej dwiema skrajnościami i zastosowano zasadę ALARP, to ryzyko wynikowe jest ryzykiem dopuszczalnym w danej konkretnej sytuacji. Te trzy strefy przedstawiono na rys. 2.

Ryzyko powyżej pewnego poziomu uznaje się za niedopuszczalne i nie może być ono usprawiedliwione żadnymi zwykłymi okolicznościami.

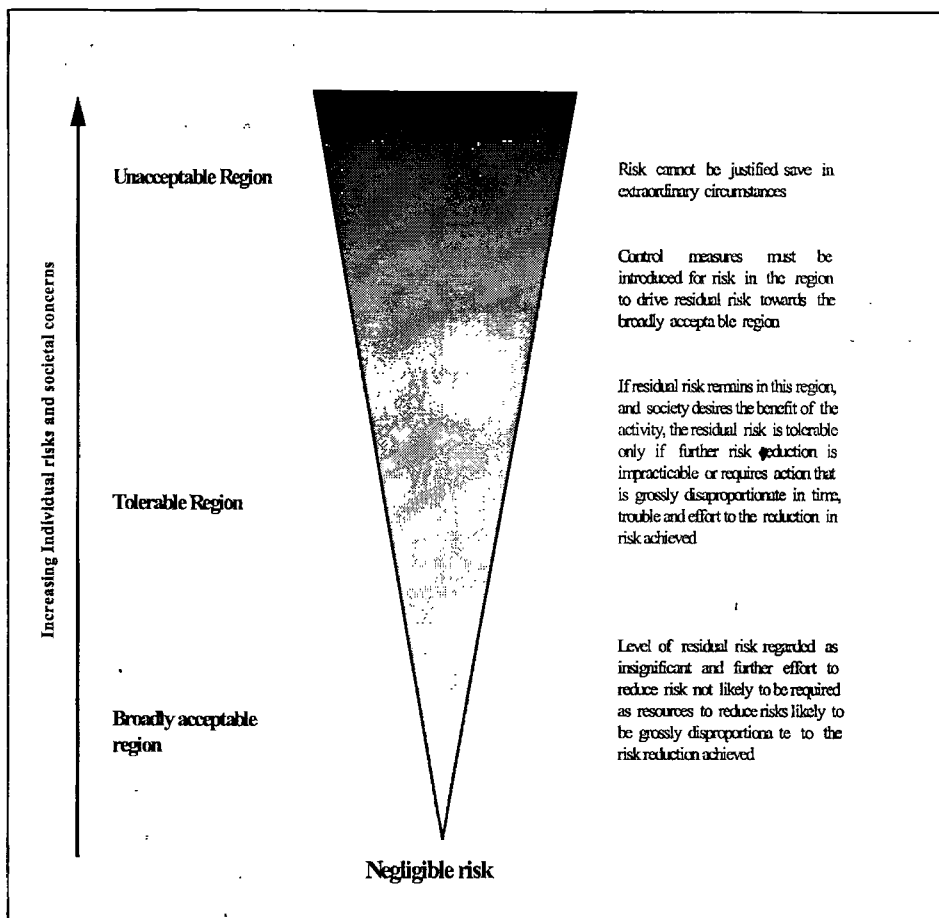
Poniżej tego poziomu jest obszar tolerowalności, w którym jest dopuszczalna działalność w założeniu, że związane z nią ryzyko zostało uczynione tak małe jak to jest rozsądnie wykonalne. Tolerowalne oznacza tu co innego niż dopuszczalne (akceptowalne) - wskazuje na chęć życia z ryzykiem tak by chronić pewne korzyści, jednocześnie spodziewając się, że będzie ono analizowane i redukowane jak tylko będzie to możliwe do wykonania.

3.2 Ryzyko tolerowalne jako cel do osiągnięcia

Jedną z dróg do osiągnięcia celu w postaci ryzyka tolerowalnego jest ustalenie zbioru konsekwencji i przypisanie im tolerowalnych częstości. Takie zestawienie konsekwencji i tolerowalnych częstości może następować na drodze dyskusji i uzgodnień między zainteresowanymi stronami (np. władzami wydającymi przepisy w zakresie bezpieczeństwa, producentami urządzeń potencjalnie niebezpiecznych i eksploatującymi je, a więc narażonymi na ryzyko).

Aby stosować zasadę ALARP, zestawienie konsekwencji z tolerowalnymi częstościami może być sporządzone w postaci klas ryzyka. W tablicy 1 podano przykład z czterema klasami ryzyka (I, II, III, IV) w odniesieniu do pewnej liczby konsekwencji i częstości. W tablicy 2 podano interpretację każdej z klas za pomocą zasady ALARP. Ryzyko ujęte w tak zdefiniowanych klasach ryzyka jest ryzykiem występującym już po wprowadzeniu środków redukcji ryzyka. W odniesieniu do rysunku 2 klasy ryzyka interpretuje się następująco:

- ryzyko odpowiadające klasie I leży w obszarze niedopuszczalnym;
- ryzyko odpowiadające klasom II i III jest w obszarze stosowania zasady ALARP, przy czym klasa II ryzyka jest dokładnie w obszarze stosowania zasady ALARP;
- ryzyko odpowiadające klasie IV znajduje się w powszechnie akceptowanym obszarze.



Rysunek 2 - Ryzyko tolerowalne i zasada ALARP

Tablica 1. - Klasyfikacja ryzyka związanego z wypadkami

Częstość	Konsekwencje			
	Katastrofalne	Krytyczne	Marginalne	Pomijalne
Częste	I	I	I	II
Prawdopodobne	I	I	II	III
Przypadkowe	I	II	III	III
Rzadkie	II	III	III	IV
Nieprawdopodobne	III	III	IV	IV
Niewiarygodne	IV	IV	IV	IV

UWAGA - Tablica jest jedynie przykładem jak należy taką tablicę wypełniać.

Tablica 2 - Interpretacja klas ryzyka

Klasa ryzyka	Interpretacja
Klasa I	Ryzyko niedopuszczalne
Klasa II	Ryzyko niepożądane i tolerowalne jedynie jeśli redukcja ryzyka jest niewykonalna lub jeśli koszty są nieproporcjonalnie wysokie do osiągniętych ulepszeń
Klasa III	Ryzyko tolerowalne, jeśli koszty redukcji ryzyka przekraczają osiągnięte ulepszenia
Klasa IV	Ryzyko pomijalne

4. METODA GRAFÓW KALIBROWANYCH [4]

4.1. Wprowadzenie

Metoda grafu ryzyka może być stosowana do określenia wymagań dotyczących poziomu nienaruszalności, gdy konsekwencje uszkodzenia obejmują dotkliwe straty w środowisku. Potrzebny poziom nienaruszalności zależy od właściwości substancji zrzucanej do środowiska i podatności środowiska. Poniżej zamieszczono ogólną tablicę, w której podano konsekwencje odniesione do środowiska..

Tablica 3 - Przykład kalibracji ogólnego grafu oceny ryzyka

PARAMETR RYZYKA	KLASYFIKACJA	UWAGI	
Konsekwencje (C) Średnia liczba nieszczęśliwych wypadków: Może to być obliczone przez określenie średniej liczby ludzi obecnych gdy obszar narażony na zagrożenie jest zajęty i pomnożonej przez stopień narażenia przez zidentyfikowane zagrożenie. Stopień zagrożenia wynika z natury zagrożenia przed którym jest ochrona. Można użyć następujące współczynniki: V = 0,01 Mały wyciek materiału palnego lub toksycznego V = 0,1 Duży wyciek materiału palnego lub toksycznego V = 0,5 Jak wyżej lecz także duże prawdopodobieństwo zapalenia lub materiał jest wysoko toksyczny V = 1 Rozpadnięcie się lub wybuch	C_A	Niewielkie urazy	1. System klasyfikacji posługuje się urazami i śmiercią ludzi. Inne systemy klasyfikacji należy opracować do szkód w środowisku lub materiałach. 2. Przy interpretacji C_A , C_B , C_C , C_D należy brać pod uwagę konsekwencje wypadków i normalnego leczenia.
	C_B	Zakres 0,01 do 0,1	
	C_C	Zakres > 0,1 do 1,0	
	C_D	Zakres > 1,0	

PARAMETR RYZYKA		KLASYFIKACJA	UWAGI
<p>Częstotliwość i czas narażenia (F) Ten parametr oblicza się określając czas, przez który obszar narażony na zagrożenie jest zajmowany w ciągu normalnej zmiany roboczej. UWAGA - Jeśli czas przebywania w obszarze zagrożonym jest różny i zależny od konkretnej zmiany roboczej, to należy wybrać czas maksymalny. UWAGA - Użycie F_A jest właściwe tylko wtedy, gdy można wykazać, że częstość wezwań jest przypadkowa i nie wiąże się z wyższą niż normalna, zajętością obszaru. To ostatnie dotyczy zwyczajowo wezwania pojawiającego się przy rozruchu wyposażenia.</p>	<p>F_A</p> <p>F_B</p>	<p>Rzadkie do częstszego narażenia w strefie zagrożenia</p> <p>Częste do ciągłego narażenia w strefie zagrożenia</p>	<p>3. Patrz uwaga 1 powyżej.</p>
<p>Prawdopodobieństwo uniknięcia zdarzeń zagrażających (P), w przypadku wypadnięcia z pracy systemu ochronnego</p>	<p>P_A</p> <p>P_B</p>	<p>Prawdopodobieństwo uniknięcia zdarzeń zagrażających (P), w przypadku wypadnięcia z pracy systemu ochronnego</p>	<p>4. P_A powinien być wybrany tylko, jeśli wszystkie poniższe warunki są prawdą:</p> <ul style="list-style-type: none"> • przewidziano urządzenia do zaalarmowania operatora, gdy SIS się uszkodzi; • przewidziano niezależne urządzenia do wyłączenia takie, że zagrożenie może zostać uniknięte lub które umożliwia wszystkim osobom ewakuację do obszaru bezpiecznego; • czas między zaalarmowaniem operatora i pojawieniem się zdarzenia zagrażającego przekracza 1 godzinę.

PARAMETR RYZYKA		KLASYFIKACJA	UWAGI
Prawdopodobieństwo zajścia zdarzeń niepożądanych (W)	W_1	Częstość wezwań mniejsza niż 0,03 na rok.	5. Celem współczynnika W jest oszacowanie częstości zdarzeń zagrażających występujących bez wprowadzenia SIS; 6. Jeśli częstość wezwań jest bardzo wysoka (np. 10 na rok), to SIL należy określić innymi metodami lub przekalibrować graf ryzyka. Teraz rodzaj pracy jest o dużej częstości wezwań lub ciągły (patrz tablica 4.4).
	W_2	Częstość wezwań między 0,3 i 0,03 na rok.	
	W_3	Częstość wezwań między 3 i 0,3 na rok. W przypadku częstości wezwań większej niż 3 na rok, należy wymagać większej nienaruszalności.	

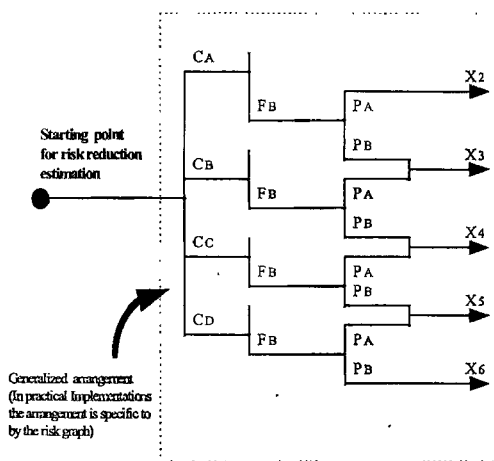
Każda indywidualna lokalizacja fabryki może mieć zdefiniowane wielkości związane ze specyficznymi substancjami, których przekroczenie wymaga zawiadomienia władz lokalnych. Projekt powinien określać co może być zaakceptowane w konkretnej lokalizacji

Konsekwencje zestawione w tablicy 3 mogą być użyte w powiązaniu ze specjalną wersją grafu ryzyka przedstawioną na rys. 3..

Tablica 4 - Ogólne konsekwencje dotyczące środowiska

PARAMETR RYZYKA		KLASYFIKACJA	UWAGI
Konsekwencje (C)	C_A	Zrzut powodujący małe szkody, gdyż nie jest bardzo groźny lecz jest na tyle rozległy, że ma być zgłoszony do zarządu obiektu lub do władz lokalnych.	Umiarkowany wyciek z kołnierza lub zaworu. Rozlanie się cieczy na niewielką skalę. Zanieczyszczenie gleby na niewielką skalę bez zanieczyszczenia wód gruntowych
	C_B	Zrzut wewnątrz ogrodzenia obiektu powodujący znaczące szkody.	Chmura nieprzyjemnych oparów przemieszczająca się ponad urządzeniami, będąca następstwem wydmuchania uszczelnienia kołnierza lub uszkodzenia zamknięcia wodnego sprężarki.

PARAMETR RYZYKA	KLASYFIKACJA	UWAGI
	C_C Zrzut na zewnątrz ogrodzenia obiektu, powodujący większe szkody, który może być wyczyszczony szybko, bez znaczących trwałych konsekwencji C_D Zrzut na zewnątrz ogrodzenia obiektu, powodujący większe szkody, który nie może być wyczyszczony szybko, lub ma znaczące trwałe konsekwencje	Zrzut oparów lub aerozoli z lub bez opadów cieczy, który powoduje chwilowe szkody dotyczące roślin lub zwierząt Rozlanie się cieczy do rzeki lub morza Zrzut oparów lub aerozolu z lub bez kropli cieczy, który powoduje trwałe szkody dotyczące roślin lub zwierząt. Opad cząstek stałych (pył, katalizator, sadza, popiół). Zrzut cieczy, który może zanieczyścić wody gruntowe.



C = Consequence parametr
F = not used
P = Possibility failing to avoid hazard parametr
W = Demand rate assuming no protection

	W₃	W₂	W₁
a		—	—
1		a	—
2		1	a
3		2	1
4		3	2
b		4	3

— = No safety requirements
a = No special safety requirements
b = A single E/E/PES is not sufficient
1,2,3,4 = Safety integrity level

Rysunek 3 - Graf ryzyka w przypadku strat środowiskowych

5. PODSUMOWANIE

Przedstawiono w zarysie niektóre narzędzia udostępniane przez techniki bezpieczeństwa funkcjonalnego, które mogą być przydatne przy sporządzaniu raportów o wpływie instalacji przemysłowych na zanieczyszczanie środowiska.

LITERATURA

1. Missala T.: Zarządzanie bezpieczeństwem funkcjonalnym a system zarządzania jakością - relacje Materiały Konferencji Naukowo-Technicznej Automatyzacja – Nowości i Perspektywy AUTOMATION 2004, ss. 199-204.
2. PN-EN ISO 9001: 2001, Systemy zarządzania jakością. Wymagania.
3. PN-EN 61508: 2003(U), Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem. Części 1 - 7.
4. EN 61511:2004, Functional safety – Safety instrumented systems for the process industry sector – Parts 1-3
5. Ustawa z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska (Dz. U. RP nr 62 poz. 627 ze zmianą Ustawa z dnia 3 października 2003 r. O zmianie ustawy – Prawo ochrony środowiska oraz niektórych innych ustaw (Dz. U. RP nr 190, poz. 1865)