mgr inż. Tomasz Strawiński
Centralny Instytut Ochrony Pracy

Dobór kategorii elementów systemów sterowania związanych z bezpieczeństwem

W maszynach, w których występują zagrożenia, można stosować, jako jeden ze środków bezpieczeństwa, elementy systemów sterowania związane z bezpieczeństwem (ESSZB). ESSZB powinny zapewniać odpowiedni poziom redukcji ryzyka wyznaczony na podstawie oceny ryzyka. Koniecznym warunkiem jest zastosowanie ESSZB o określonej kategorii (wg PN-EN 954-1:2001) określającej jego odporność na defekty. W pracy przedstawiono metodę doboru kategorii ESSZB na podstawie oceny ryzyka, z wykorzystaniem zbioru „wytypowanych" architektur.

The Selection of Category for Safety Related Control Systems

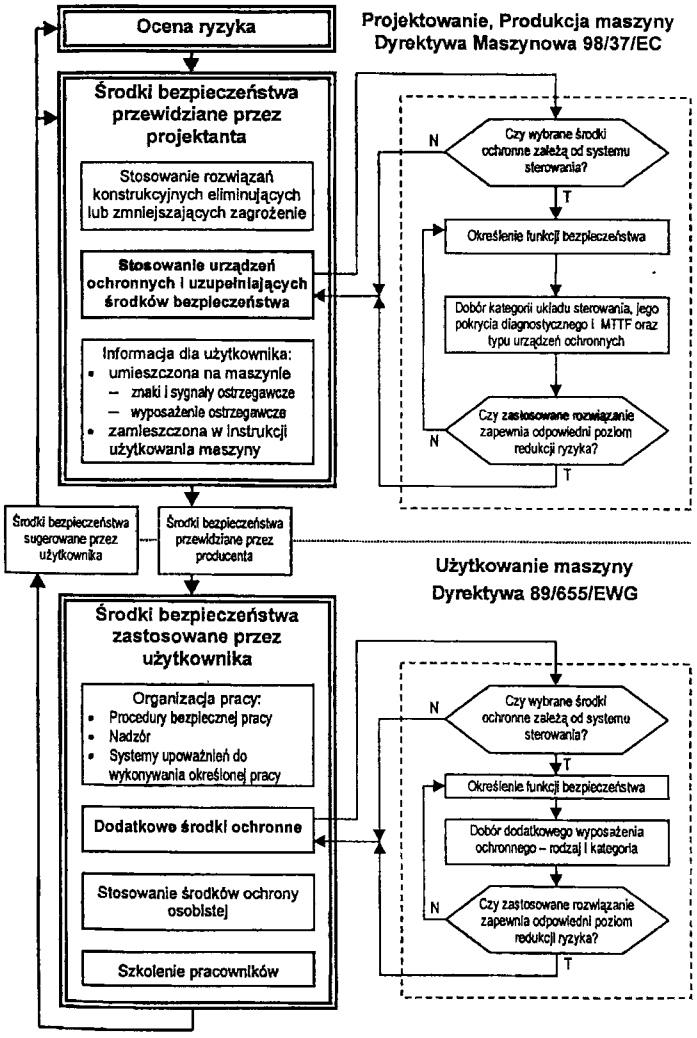
In the machines with hazards occurred, safety related parts of control systems could be applied as a one of safety measures. The suitable risk reduction level should be assured accordingly to risk assessment. The application of safety related parts of control system complying the proper category requirements (given in the standard PN-EN 954-1:2001), which states their fault-tolerant capabilities, is the obligatory term. The paper presents the method of category selection for safety related parts of control system using risk assessment and a set of designated architectures.

1. WPROWADZENIE

Bezpieczeństwo pracy jest w znacznym stopniu zależne od bezpieczeństwa związanego z maszynami wykorzystywanymi w procesach produkcyjnych i w usługach. Ogólne wymaganie zapewnienia bezpieczeństwa maszyn, wyrażone w Dyrektywie Maszynowej 98/37/EC (w odniesieniu do maszyn wprowadzanych po raz pierwszy do obrotu i użytkowania w krajach UE) i dyrektywie 89/655/EWG dotyczącej maszyn znajdujących się w użytkowaniu, prowadzi do zastosowania w maszynach różnego rodzaju środków ochronnych (rys. 1). Jednym z tych środków może być instalowanie wyposażenia ochronnego (np. maty czułej na nacisk, kurtyny świetlnej, skanera, itp.), którego działanie musi być powiązane z układem sterowania w sposób gwarantujący szczególną poprawność i skuteczność realizacji założonych funkcji bezpieczeństwa w całym okresie życia maszyny.

Wymagania dotyczące ESSZB zostaną zawarte w projektowanej normie prIEC 62061 *Safety of machinery – Functional safety – Electrical, electronic and programmable electronic control systems*. Do czasu jej ustanowienia można posługiwać się wieloczęściową normą IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*. Wprowadzono w nich pojęcie poziomu nienaruszalności bezpieczeństwa (tzw. SIL – ang. *Safety Integrity Level*), jako ilościowego parametru określającego bezpieczeństwo funkcjonalne, definiowanego poprzez prawdopodobieństwo sytuacji, w której ESSZB nie zrealizuje zaplanowanej funkcji bezpieczeństwa. Podano również przykładowe metody wyznaczania wymaganego SIL na podstawie oceny ryzyka. Znacznie trudniejsze jest

natomiast wykazanie, że konkretna realizacja ESSZB zapewnia wymagany SIL. Zadanie to jest praktycznie niewykonalne w małych i średnich przedsiębiorstwach, które chcą dostarczać maszyny na rynek krajów UE. Potrzebna jest zatem metoda lepiej dostosowana do typowych możliwości przeciętnych firm produkujących maszyny i jednocześnie zapewniająca spełnienie wymagań w zakresie bezpieczeństwa.



Rys. 1 Schemat działań związanych z zapewnieniem bezpieczeństwa maszyny

2. CHARAKTERYSTYKA ESSZB

ESSZB można opisać podając jego architekturę, kategorię odporności na defekty, pokrycie diagnostyczne, jakość użytych elementów oraz wynikający z tych parametrów poziom zapewnienia bezpieczeństwa. Pod pojęciem architektury ESSZB należy rozumieć kompletne rozwiązanie, tzn. urządzenie ochronne (czujnik), układ sterowania i elementy wykonawcze

wraz z podstawowymi kierunkami przepływu informacji. Architektura powinna być dostosowana do wymagań zakładanej kategorii odporności na defekty (wyróżniane są kategorie B, 1, 2, 3, 4 wg PN-EN 954-1:2001. *Maszyny. Bezpieczeństwo. Związane z bezpieczeństwem elementy systemów sterowania. Ogólne zasady projektowania).*

Pokrycie diagnostyczne (ang. diagnostic coverage - DC) – jest to stosunek prawdopodobieństwa wystąpienia uszkodzeń niebezpiecznych, które zostaną wykryte do prawdopodobieństwa wystąpienia wszystkich uszkodzeń niebezpiecznych;

Średni czas do wystąpienia uszkodzenia niebezpiecznego (ang mean time to dangerous failure - MTTF) – jest to oczekiwana, przeciętna wartość czasu działania ESSZB do chwili wystąpienia uszkodzenia niebezpiecznego. Jeśli zastosowano elementy o nieznanej wartości MTTF to stosuje się oceny szacunkowe na podstawie danych o podobnych elementach. Przy ocenach szacunkowych zazwyczaj stosuje się podział na trzy zakresy: niski (od 3 do 10 lat), średni (od 10 do 30 lat), wysoki (od 30 do 100 lat);

Poziom zapewnienia bezpieczeństwa (ang. safety performance level - SPL) – jest to zdolność ESSZB do realizacji funkcji bezpieczeństwa, w możliwych do przewidzenia warunkach w stopniu niezbędnym do osiągnięcia zakładanej redukcji ryzyka. W odróżnieniu od SIL, SPL jest miarą jakościową bezpieczeństwa z wyróżnionymi poziomami **a** (najniższy), **b**, **c**, **d**, **e** (najwyższy). Jest on zależny od następujących czynników:

- możliwości realizacji i „zachowania się" funkcji bezpieczeństwa w warunkach wystąpienia defektu;
- zdolności do realizacji funkcji bezpieczeństwa w oczekiwanych (przewidywanych) warunkach środowiskowych;
- możliwości (dostępności) realizacji funkcji bezpieczeństwa na żądanie (aktywizacja na żądanie przy uwzględnieniu częstotliwości aktywowania i MTTF);
- zdolności ESSZB do wykrywania defektów (pokrycie diagnostyczne);
- wpływu uszkodzeń spowodowanych wspólną przyczyną w systemach redundancyjnych;
- wpływu defektów systematycznych;
- wyboru środków ochronnych odpowiednich do zastosowania.

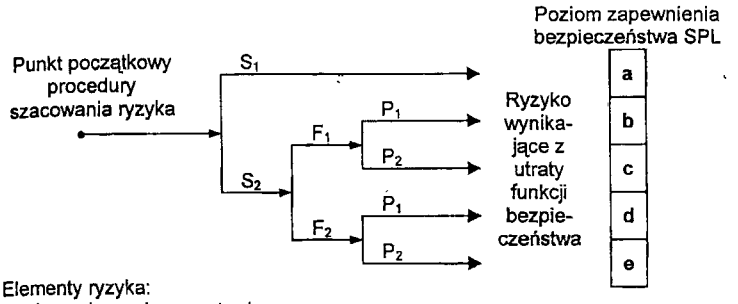
Wymagania dotyczące kategorii lepiej przystają do praktyki projektowania ESSZB niż wymaganie zapewnienia określonego poziomu SIL. Problem doboru kategorii ESSZB w celu redukcji ryzyka do założonego poziomu jest więc zasadniczy ze względu na potrzeby projektantów. Chcieliby oni mieć pewność, że zastosowany wariant realizacji ESSZB zapewnia i wystarcza do osiągnięcia bezpieczeństwa, oraz że stopień komplikacji i koszt układu odpowiada i wynika z wyznaczonego celu.

Niezbędne jest zatem pokazanie związku pomiędzy wynikiem oceny ryzyka a kategorią ESSZB realizującego funkcję bezpieczeństwa redukującą występujące ryzyko. Prace przeprowadzone w Berufsgenossenschaftlichen Institut für Arbeitssicherheit (BIA), oraz rezultaty programu STSARCES proponują metodologię traktującą kategorię ESSZB jako architekturę charakteryzującą się pewnym pokryciem diagnostycznym (DC) i jakością zastosowanych podzespołów (MTTF), co pozwala osiągnąć określony SPL.

3. WYZNACZENIE POZIOMU ZAPEWNIENIA BEZPIECZEŃSTWA

SPL powinien zostać wyznaczony na podstawie oceny ryzyka, której zasady sformułowano w normie PN-EN 1050:1999 *Maszyny. Bezpieczeństwo. Zasady oceny ryzyka.* Ocena ryzyka powinna być przeprowadzona dla każdego zagrożenia niezależnie. Jeżeli przewiduje się zastosowanie ESSZB realizującego funkcje bezpieczeństwa związane z kilkoma zagrożeniami, to przy projektowaniu ESSZB powinien zostać wzięty pod uwagę najwyższy wyznaczony poziom zapewnienia bezpieczeństwa.

Do oceny ryzyka prowadzącej do wyznaczenia SPL wykorzystano graf ryzyka o strukturze przedstawionej na rys. 2.



Elementy ryzyka:
S – konsekwencje zagrożenia
  S_1 – lekki uraz (normalnie odwracalny)
  S_2 – ciężki uraz (normalnie nieodwracalny łącznie ze śmiertelnym)
F – częstotliwość i czas narażenia
  F_1 – rzadko do niezbyt często i/lub krótki czas narażenia
  F_2 – często do ciągle i/lub długi czas narażenia
P – prawdopodobieństwo uniknięcia zdarzenia
  P_1 – możliwe w określonych warunkach
  P_2 – praktycznie niemożliwe
a, b, c, d, e – poziomy zapewnienia bezpieczeństwa SPL

Rys. 2. Wyznaczanie wymaganego poziomu zapewnienia bezpieczeństwa SPL dla ESSZB

Na podstawie wyników oceny ryzyka prowadzonych w celu wyznaczenia SIL i SPL można określić relację zachodzącą między tymi parametrami (tablica 1).

Tablica 1. Relacja pomiędzy SPL i SIL.

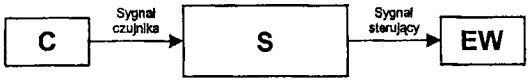
SPL	SIL	Średnie prawdopodobieństwo utraty funkcji bezpieczeństwa przy jej przywołaniu, w układzie sterowania przy niskiej częstotliwości aktywacji	Prawdopodobieństwo utraty funkcji bezpieczeństwa w czasie jednej godziny przy dużej częstotliwości lub ciągłej aktywacji
	4	$10^{-5} \le p < 10^{-4}$	$10^{-9} \le p < 10^{-8}$
e	3	$10^{-4} \le p < 10^{-3}$	$10^{-8} \le p < 10^{-7}$
d	2	$10^{-3} \le p < 10^{-2}$	$10^{-7} \le p < 10^{-6}$
b, c	1	$10^{-2} \le p < 10^{-1}$	$10^{-6} \le p < 10^{-5}$
a			

4. „WYTYPOWANE" ARCHITEKTURY ESSZB

W celu zaproponowania „wytypowanych" architektur ESSZB wyodrębniono klasę układów o niskiej złożoności. Należą do niej układy spełniające jeden z poniższych warunków:
- wymagany SPL wynosi **a** lub
- funkcja bezpieczeństwa realizowana jest sprzętowo i zachowanie układu w przypadku defektu jest wyraźnie zdeterminowane i wymierne lub
- udział elementów programowalnych w ESSZB, które realizują funkcję bezpieczeństwa jest niewielki oraz wymagany SPL jest mniejszy lub równy **d** lub
- funkcja bezpieczeństwa jest realizowana przez zróżnicowane pod względem sprzętu, oprogramowania i systemu operacyjnego programowalne systemy elektroniczne oraz wymagany SPL jest mniejszy lub równy **d** lub
- wykorzystane elementy były testowane i certyfikowane przez niezależne jednostki (akredytowane laboratoria) na zgodność z dyrektywą maszynową i odpowiednimi normami.

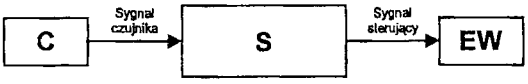
Dodatkowo, przewidziane do zastosowania części i podzespoły powinny być szeroko stosowane w różnych aplikacjach (elementy i podzespoły sprawdzone w praktyce) oraz być wyprodukowane przez kompetentnych producentów.

Przykładowe, „wytypowane" architektury ESSZB o różych kategoriach z wyznaczonym SPL, należące do klasy układów o niskiej złożoności, przedstawiono na rys. 3, 4, 5, 6 i 7.



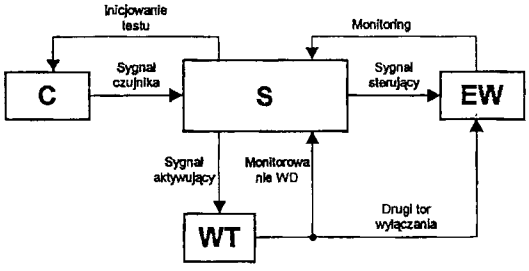
C – czujnik, **S** – sterownik, **EW** – element wykonawczy
Brak pokrycia diagnostycznego, MTTF - niski lub średni, SPL: **a**

Rys. 3 ESSZB kategorii **B**



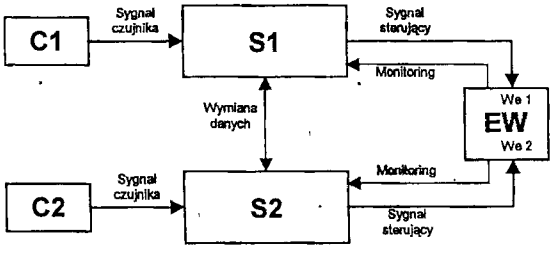
C – czujnik, **S** – sterownik, **EW** – element wykonawczy
Brak pokrycia diagnostycznego, MTTF - wysoki, SPL: **b**

Rys. 4 ESSZB kategorii **1**



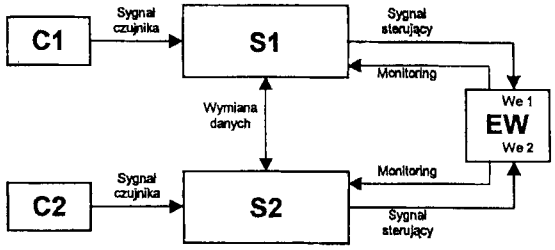
C – czujnik, **S** – sterownik, **EW** – element wykonawczy, **WT** –wyposażenie testujące
Pokrycie diagnostyczne niskie, MTTF - niski, SPL: **b**
Pokrycie diagnostyczne średnie, MTTF - wysoki, SPL: **d**

Rys. 5 ESSZB kategorii **2**



C1, **C2** – czujniki, **S1**, **S2** – sterowniki, **EW** – element wykonawczy
Pokrycie diagnostyczne niskie, MTTF - niski, SPL: **c**
Pokrycie diagnostyczne średnie, MTTF - wysoki, SPL: **d**

Rys. 6 ESSZB kategorii **3**

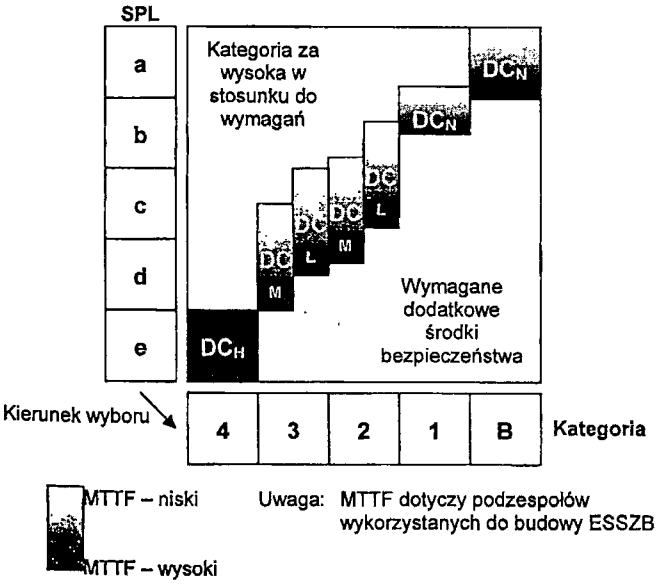


C1, C2 – czujniki, S1, S2 – sterowniki, EW – element wykonawczy
Pokrycie diagnostyczne wysokie, MTTF - wysoki, SPL: e

Rys. 7 ESSZB kategorii 4

5. DOBÓR KATEGORII ESSZB

Dla zbioru „wytypowanych" architektur ESSZB można sporządzić wykres obrazujący relację pomiędzy ich kategorią odporności na defekty i zapewnianym przez nie SPL. Na rysunku 8 przedstawiono wykres tej relacji dla architektur z rysunków od 3 do 7, które przedstawiono w formie prostokątów o wielkości i położeniu odwzorowującym odpowiadające im warunki.



DC_N – brak pokrycia diagnostycznego
DC_L – pokrycie diagnostyczne niskie
DC_M – pokrycie diagnostyczne średnie
DC_H – pokrycie diagnostyczne wysokie

Rys. 8 Racjonalne architektury – relacja pomiędzy kategorią i SPL

Przedstawiony wykres obrazuje sposób, w jaki SPL jest zależny od kategorii ESSZB, jakości wykorzystanych podzespołów (MTTF) i pokrycia diagnostycznego (DC). Z wykresu wynika również niejednoznaczność wyboru kategorii dla poziomów zapewnienia bezpieczeństwa a, b, c i d, co jest w tym przypadku związane z opracowanym zestawem „wytypowanych"

architektur ESSZB o pokrywających się możliwościach zapewnienia bezpieczeństwa.

W celu doboru kategorii ESSZB należy:
- wyznaczyć poziomy zapewnienia bezpieczeństwa dla każdej funkcji bezpieczeństwa posługując się grafem ryzyka z rys. 1;
- spośród dostępnych „wytypowanych" architektur ESSZB dokonać wyboru tej, która zapewni wymagany poziom bezpieczeństwa i określić jej kategorię odporności na defekty;
- określić wymagane MTTF i DC, które trzeba będzie zapewnić w projektowanym ESSZB.

Proponowana metoda doboru kategorii ESSZB jest stosunkowo prosta, bowiem nie wymaga wykonywania skomplikowanych obliczeń. Zakłada ona istnienie dostępnego zbioru „wytypowanych" architektur ESSZB o parametrach określonych przez kompetentne jednostki. Do zadań projektanta należeć będzie identyfikacja zagrożenia, przeprowadzenie oceny ryzyka, dobór środków ochronnych i określenie funkcji bezpieczeństwa dla ESSZB, wybór „wytypowanego" rozwiązania (architektura, kategoria, MTTF, DC), a następnie poprawna realizacja układowa. W etapie końcowym proces walidacji powinien potwierdzić zrealizowanie założeń funkcjonalnych i kategorii odporności na defekty oraz spełnienie wymagań środowiskowych, w zakresie kompatybilności elektromagnetycznej, bezpieczeństwa obsługi i innych. Należy sądzić, że metoda „wytypowanych" architektur pozwoli na ograniczenie ryzyka popełnienia błędów projektowych i ograniczenie nakładów związanych z walidacją układu.

Ograniczenie metody do klasy układów o niskiej złożoności nie jest praktycznie znaczące. W większości maszyn wymagania w stosunku do ESSZB, wynikające z realizowanych funkcji bezpieczeństwa, pozwalają na ich kwalifikację do tej klasy. ESSZB nie mieszczące się w klasie układów o niskiej złożoności powinny być projektowane zgodnie z wymaganiami normy prIEC 62061.

6. PRZYKŁAD WYZNACZANIA KATEGORII ESSZB

Ciężki pojazd transportowy kierowany automatycznie (bez kierowcy) może w pewnych sytuacjach powodować zagrożenie najechania na osoby znajdujące się na trasie jego przejazdu. Poprzez zainstalowanie urządzenia wykrywającego przeszkody w pewnej odległości od pojazdu (np. skanera laserowego) można zaimplementować funkcję bezpieczeństwa polegającą na wyhamowaniu i zatrzymaniu pojazdu w bezpiecznej odległości przed przeszkodą. Uderzenie pojazdu w człowieka może być przyczyną poważnych, nieodwracalnych uszkodzeń ciała (konsekwencje zagrożenia – S_2). Trasa przejazdu pojazdu, stanowiąca strefę zagrożenia, jest swobodnie dostępna dla wielu osób, co powoduje, że zagrożenie jest realne stosunkowo często (częstotliwość i czas narażenia – F_2). Pojazd porusza się z niewielką prędkością, porównywalną z prędkością pieszego, co zwykle umożliwia osobom znajdującym się na trasie przejazdu opuszczenie jej (prawdopodobieństwo uniknięcia zdarzenia – P_1).

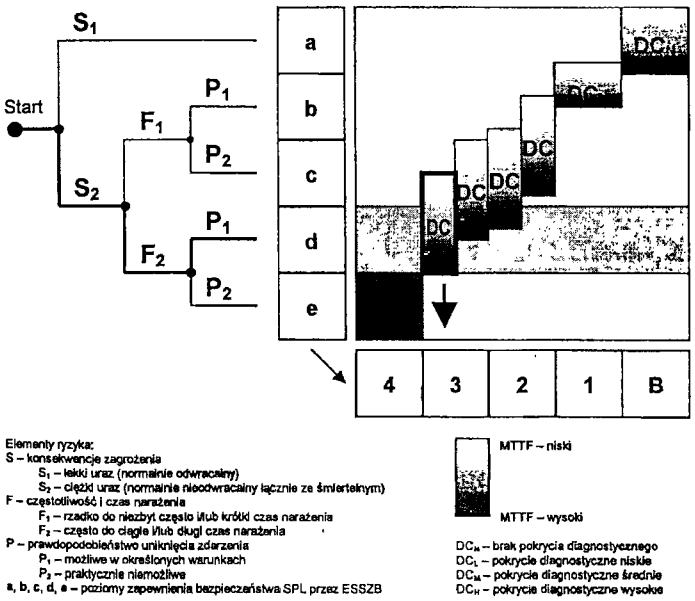
Zgodnie z rysunkiem 9 ocena ryzyka wskazuje na potrzebę zapewnienia bezpieczeństwa na poziomie **d**. W tym przypadku niezbędne jest wykonanie ESSZB realizującego założoną funkcję bezpieczeństwa jako układu kategorii **3**, według schematu blokowego przedstawionego na rysunku 6. Układ powinien charakteryzować się średnim pokryciem diagnostycznym. Do jego wykonania należy użyć elementów o wysokim MTTF.

7. PODSUMOWANIE

Przedstawiona metoda doboru kategorii ESSZB na podstawie oceny ryzyka z wykorzystaniem zbioru „wytypowanych" architektur pozwala uzyskać rozwiązania zapewniające wymaganą redukcję ryzyka. Należy zauważyć, że jest ona podobna do zalecanych w normie PN-EN 954-1:2001: korzystania ze sprawdzonych zasad

bezpieczeństwa i stosowania wypróbowanych części składowych. Obecnie w międzynarodowych zespołach trwają prace nad dopracowaniem szczegółów tej metody i wprowadzeniem jej do normy.

W Polsce, zgodnie ze strategią przystępowania do Unii Europejskiej, przewiduje się wprowadzenie przepisów Dyrektywy Maszynowej 98/37/EC (w dniu 3 lipca 2001 r. Rada Ministrów RP przyjęła projekt rozporządzenia w tej sprawie) i dyrektywy 89/655/EWG. W Polsce od szeregu lat trwają także prace nad ustanawianiem norm krajowych zgodnych z normami zharmonizowanymi. Należy się spodziewać, że w Polsce w niedługim czasie zapewnienie bezpieczeństwa maszyn w rozumieniu przepisów wspomnianych dyrektyw stanie się obligatoryjne, co nałoży określone rygory na stosowanie środków bezpieczeństwa w formie ESSZB. Przedstawiona metoda pozwoli spełnić część związanych z tym wymagań.



Rys. 9 Przykład doboru kategorii ESSZB

8. BIBLIOGRAFIA

1 Bell, R., Frederickson, A. (1994). Requirements for designated safety system architectures as defined by the IEC draft standard - Functional Safety: Safety Related Systems. *TÜV symposium*, Köln, 7-8 September.

2 Dźwiarek, M. (1997). Klasyfikacja systemów sterowania w zależności od zapewnianego poziomu bezpieczeństwa według EN 954-1. *Pomiary, Automatyka, Robotyka*. 8/1997, 4-9.

3 Dźwiarek, M. (1998). Problematyka EN 954-1 w projektowaniu systemów sterowania. *Pomiary, Automatyka, Robotyka*. 10/1998, 5-9.

4 Dźwiarek, M., (2000). Advanced Technology in Safety Related Control Systems of Machinery. *Ergonomics and Safety for Global Business Quality and Productivity*, (19-21 May, Warsaw) 475-478.

5 Missala, T. (1997). Bezpieczeństwo funkcjonalne urządzeń automatyki i robotyki. *Pomiary, Automatyka, Robotyka*, 3/1997.

6 (1997). Categories for Safety-related Control Systems in Accordance with EN 954-1. BIA Report 6/97.