Wojciech Danilczuk

Bezpieczeństwo maszyn – określanie poziomu nienaruszalności bezpieczeństwa SIL

JEL: L64. **DOI:** 10.24136/atest.2018.273.
Data zgłoszenia: 01.07.2018. **Data akceptacji:** 27.01.2018.

W artykule przedstawiono metodę oceny bezpieczeństwa maszyn polegającą na obliczaniu poziomu nienaruszalności bezpieczeństwa SIL (ang. Safety Integrity Level). Problematyka bezpieczeństwa maszyn została przedstawiona w kontekście obowiązujących przepisów prawnych i norm międzynarodowych. Na podstawie literatury oraz norm został za prezentowane metody określania poziomu nienaruszalności bezpieczeństwa, miary ilościowe i jakościowe używane w ramach normy PN-EN 62061 oraz podstawowe pojęcia związane z wymaganiami funkcjonalnymi. Dodatkowo przedstawiono zależność między poziomem nienaruszalności bezpieczeństwa SIL a poziomu zapewnienia bezpieczeństwa PL. Artykuł jest kontynuacją poprzedniej publikacji autora dotyczącej bezpieczeństwa maszyn [1].

Słowa kluczowe: zarządzanie ryzykiem, bezpieczeństwo maszyn, poziom nienaruszalności bezpieczeństwa.

Wstęp

Bezpieczeństwo maszyn jest jednym z podstawowych wymagań jakie musi spełniać urządzenie aby zostało ono dopuszczone do pracy. Obowiązek przeprowadzenia procedur związanych z oceną ryzyka wynika z przepisów prawa polskiego [9] oraz norm europejskich [2, 6]. Producent urządzeń (lub podmiot wprowadzający je do użytku na terenie Unii Europejskiej) jest zobligowani od określenia ryzyka i niebezpieczeństw jakie mogą zaistnieć z związku z użytkowaniem urządzenia (zarówno w trybie normalnej pracy jak i podczas konserwacji bądź awarii). Po zidentyfikowaniu ryzyka należy zminimalizować możliwość jego wystąpienia oraz potencjalne skutki jego wystąpienia.

Do ilościowej oceny potencjalnych niebezpieczeństw oraz ich skutków wykorzystuje się najczęściej jedną z dwóch norm. Pierwszą z nich jest norma PN-EN 13849 [7] która opiera się na określeniu poziomu zapewnienia bezpieczeństwa PL (ang. *Performance Level*). Szerzej o tej normie można przeczytać w publikacji autora [1]. Druga norma która jest stosowana w ilościowej ocenie ryzyka to PN-EN 62061 [8]. Wymaga ona od projektanta określenia poziom nienaruszalności bezpieczeństwa SIL (ang. *Safety Integrity Level*). Norma PN-EN 13849 ma zastosowanie do układów elektrycznych, pneumatycznych, hydraulicznych i mechanicznych, natomiast norma PN-EN 62061 skupia się przede wszystkim na układach elektrycznych.

W metodzie oceny ryzyka poprzez wyznaczenie poziomu SIL funkcje bezpieczeństwa są zazwyczaj realizowane przez połączenie trzech elementów: czujnika wykrywającego zagrożenie, jednostki logicznej przetwarzającej sygnał z czujnika oraz elementu wykonawczego realizującego funkcje bezpieczeństwa. Elementy te tworzą elektryczny system sterowania związany z bezpieczeństwem – SRECS (ang. *Safety-Related Electrical Control System*) [4].

Na specyfikację wymagań dla funkcji bezpieczeństwa składają się dwa elementy. Pierwszy z nich to wymagania funkcjonalne. Wymagania funkcjonalne są najczęściej określane w sposób naturalny np. zatrzymanie pracy motoreduktora gdy nastąpi wejście do strefy zagrożenia. System sterowania związany z bezpieczeństwem w tym przypadku mógłby składać się z optoelektronicznej kurtyny bezpieczeństwa (rola czujnika), sterownika bezpieczeństwa (element logiki) oraz stycznika serującego załączeniem motoreduktora (element wykonawczy). Drugim wymaganiem są wymagania nienaruszalności bezpieczeństwa który określa się poprzez wyznaczenie wymaganego poziomu SIL dla danej funkcji bezpieczeństwa.

W dalszej części artykułu przedstawiono wzory oraz tabele, które zostały opracowane na podstawie [5, 8, 4].

1. Algorytm wyznacznia wymaganego poziomy sil według normy ISO EN 62061

Pierwszym etapem oceny ryzyka zgodnie z normą PN-EN 62061 jest określenie docelowego Poziomu Nienaruszalności Bezpieczeństwa SIL. Poziom ten określa się osobno dla każdej funkcji bezpieczeństwa jaka występuje w układzie. Podobnie jak w metodzie oceny ryzyka opartej na normie ISO EN 13849 wymagany poziom bezpieczeństwa jest szacowany na podstawie czynników – ciężkość urazów, czas ekspozycji oraz możliwość uniknięcia zagrożenia. Dodatkowo w metodzie wyznaczania wymaganego poziomu SIL określa się prawdopodobieństwo wystąpienia awarii. Norma ISO EN 13849 wyznacza wymagany poziom PL (ang. Performance Level, poziom zapewnienia bezpieczeństwa) na podstawie grafu oceny ryzyka natomiast metoda oparta na wyznaczaniu wymaganego poziomu SIL wykorzystuje matryce oceny ryzyka (rysunek 1).

1.1. Ciężkość urazów S (ang. *Severity*)

Ciężkość urazu lub uszkodzenia zdrowia można oszacować, biorąc pod uwagę odwracalne obrażenia, nieodwracalne obrażenia i śmierć. Ciężkość urazów przedstawia tabela 1.

Skutek	Ciężkość	Klasa				
		C = F + P+ A				
		3–4	5–7	8–10	11–13	13–15
Nieodwracalne: śmierć, utrata oka lub ręki	4	SIL2	SIL 2	SIL2	SIL3	SIL3
Nieodwracalne: kalectwo, utrata palców	3		OM	SILI	SIL2	SIL3
Odwracalne: leczenie	2			OM	SILI	SIL2
Odwracalne: pierwsza pomoc	1				OM	SILI

Rys. 1. *Matryca oceny ryzyka [4]*

Tab. 1. Ciężkość urazów

Skutek	Ciężkość
Nieodwracalne: śmierć, utrata oka lub ręki	4
Nieodwracalne: kalectwo, utrata palców	3
Odwracalne: leczenie	2
Odwracalne: pierwsza pomoc	1

Tab. 2. Częstość narażania

Częstotliwość	Czas ekspozycji ≥10min	Czas ekspozycji <10min
≤ 1 h	5	5
> 1 h do ≤ 1 dzień	5	4
> 2 dni do ≤ 1 tydzień	4	3
> 2 tygodni do ≤ 1 rok	3	2
> 1 rok	2	1

Tab. 3. Prawdopodobieństwo wystąpienia

Prawdopodobieństwo wystąpienia sytuacji zagrożenia	
Częste	5
Prawdopodobne	4
Możliwe	3
Rzadkie	2
Nieistotne	1

Tab. 4. Prawdopodobieństwo o uniknięcia

Możliwość uniknięcia	
Niemożliwe	5
Możliwe	3
Prawdopodobne	1

1.2. Częstość narażania oraz czas ekspozycji zagrożenia F (ang. *Frequency*)

Parametr F określa jak często operator jest narażony na występowanie zagrożenia oraz jaki jest czas ekspozycji na zagrożenie. Analizując częstość narażenia należy wziąć pod uwagę różne trybów pracy urządzenia. Inne mogą być zagrożenia wynikające z pracy normalnej, konserwacja czy serwisowanie maszyny. Czas ekspozycji na zagrożenie może być błędnie mylony z częstością użytkowania urządzenia. Należy zwrócić uwagę, że sporadyczne wykonywanie danej czynności może wiązać się w ciągłym narażeniem na niebezpieczeństwo podczas wykonywania określonej czynności. Przykładowo szlifierka kątowa może być używana bardzo rzadko (na przykład raz w miesiącu przez godzinę) jednak czas ekspozycji na zagrożenie jest bardzo duży (przez godzinę użytkowania szlifierki jesteśmy narażeni na niebezpieczeństwo wynikające z wirującej tarczy) [1]. Tabela 2 zawiera wartości dla parametru częstości narażenia.

1.3. Prawdopodobieństwa wystąpienia sytuacji zagrożenia P (ang. *Probability*)

Współczynnik P określa możliwość wystąpienia sytuacji zagrożenia. Szacując prawdopodobieństwo należy uwzględnić zachowanie maszyny w różnych trybach użytkowania. Również ludzkie zachowanie, które może zwiększać ryzyko wystąpienie niebezpieczeństwa należy wziąć pod uwagę (np. stres ze względu na ograniczenia czasowe). Jeśli projektant urządzenia dysponuje danymi statystycznymi dobrą praktyką jest określenie prawdopodobieństwa wystąpienia sytuacji zagrożenia na podstawie danych historycznych lub poprzez modele probabilistyczne. W przypadku gdy projektowane urządzenie jest prototypem bądź konstruktorzy nie dysponują danymi historycznymi prawdopodobieństwo wystąpienia zagrożenia należy oszacować metodą ekspercką. Współczynniki wagowe dla parametru P zawiera tabela 3.

1.4. Prawdopodobieństwa uniknięcia lub ograniczenia szkody A (ang. *Avoiding*)

Określa możliwość uniknięcia wystąpienia zagrożenia bądź, w przypadku wystąpienia zagrożenia, szanse na minimalizację jego skutków. Analizując możliwość uniknięcia zagrożenia należy wziąć pod uwagę takie czynniki jak szybkość pojawienia się zagrożenia lub możliwość jego wykrycia przez operatora (np. detekcja wycieku gazów). Ważnymi czynnikami są też możliwości wydostania się ze strefy zagrożenia np. drogi ewakuacyjne, strefy stanowisk zrobotyzowanych poza zasięgiem robota. Tabela 4 przedstawia wartości liczbowe dla parametru A.

1.5. Klasa prawdopodobieństwa szkód C (ang. *Class of Probability of Harm*)

Klasa prawdopodobieństwa szkód jest sumą wartości liczbowych współczynników F (częstość narażenia), P (prawdopodobieństwo wystąpienia zagrożenia) oraz A (możliwości uniknięcia zagrożenia) (1):

$$C = F + P + A \tag{1}$$

Wymagany poziom bezpieczeństwa SIL jest określana na podstawie matrycy oceny ryzyka (rys. 1). Jest to pole w matrycy które leży na przecięciu klasy prawdopodobieństwa szkód C oraz ciężkości urazów S.

Należy pamiętać, że szacując wymagany poziom nienaruszalności bezpieczeństwa analizujemy pojedyncze funkcje bezpieczeństwa, a nie szacujemy ryzyko dla całej maszyny. Większość maszyn posiada więcej niż jedną funkcję bezpieczeństwa i dla każdej z nich procedura określania wymaganego poziomu SIL powinna być przeprowadzono osobno.

Po określeniu wymaganego poziomu nienaruszalności bezpieczeństwa należy określić jaki poziom SIL ma analizowana część układu bezpieczeństwa. Jeśli danej funkcja bezpieczeństwa został przypisany poziom SIL – inne metody OM (ang. *Other Methods*) wówczas jako metodę zmniejszenia ryzyka możne przyjąć środki organizacyjne (np. przeszkolenie operatorów, środki ochrony bezpośredniej).

2. Określanie poziomu nienaruszalności bezpieczeństwa osiąganego przez podsystemy

W celu obliczenia poziomu nienaruszalności bezpieczeństwa układu należy określić dwa wskaźniki:

- granica osiągnięcia poziomu nienaruszalności bezpieczeństwa SILCL (ang. *Safety integrity level claim limit*);
- średnią częstość uszkodzeń niebezpiecznych jakie mogą wystąpić w funkcjach bezpieczeństwa na godzinę PFHD (ang. *Probability of Dangerous Failure per Hour*).

Wskaźnik PFHD jest liczony jako możliwe do uzyskanie SIL całego układu powstającego z szeregowego połączenia podsystemów i prawdopodobieństwa błędu transmisji danych mającego wpływ na realizację funkcji bezpieczeństwa Pte (ang. *Probability of transmision error*) (2):

$$PHFD\ sys = PHFD\ 1 + PHFD\ 2 + \cdots + PHFD\ n + Pte \tag{2}$$

Wyznaczenie SILCL musi odbyć się dla każde z funkcji bezpieczeństwa z osobna. W celu obliczenia SILCL należy wyznaczyć następujące parametry:

- średni czas do uszkodzenia MTTF (ang. *Mean Time to Faliure*) i związany z nim intensywność uszkodzeń λ;
- poziom pokrycia diagnostycznego DC (ang. *Diagnostic Coverage*) oraz wskaźnik uszkodzeń bezpiecznych SFF (ang. *Safe Failure Fraction*);
- uszkodzenie spowodowane wspólną przyczyną CCF (ang. *Common Cause Failure*) oraz współczynnik wrażliwości na takie uszkodzenie β;
- architektura układu i oraz tolerancja sprzętu na uszkodzenia HFT (ang. *Hardware Fault Tolerance*).

2.1. Średni czas do uszkodzenia MTTF oraz intensywność uszkodzeń λ

Metodę SIL wykorzystuj się najczęściej dla urządzeń elektronicznych. W związku z tym w celu oszacowania poziomu MTTF dla całego kanału zlicza się wartości MTTF elementów wchodzących w skład kanału (tranzystorów, rezystorów etc.) (3):

$$\frac{1}{MTTF\ ch} = \frac{1}{MTTF\ 1} + \frac{1}{MTTF\ 2} + \cdots + \frac{1}{MTTF\ n} \tag{3}$$

Często producenci układów elektronicznych podają wartości MTTF jakie osiągają ich układy . W przypadku braku takich danych wskaźnik średniego czasu do uszkodzenia może być szacowany na podstawie metod dobrych praktyk inżynierskich (ang. *Good engineering practice method*). Pomocna jest również baza danych firmy Siemens SN 29500-2005-1 [10] oraz program MTBF Calculator firmy ALD [3].

Intensywność uszkodzeń λ dla podsystemu elektronicznego obliczana jest z zależności (4). W przypadku podzespołów elektromechanicznych korzysta się ze wzoru (5):

$$\lambda = \frac{1}{MTTF\ ch} \tag{4}$$

$$\lambda = 0{,}1\ \frac{C}{B10} = 0{,}1\ \frac{3600\ sek/godz}{B10\ T\ cycle} \tag{5}$$

gdzie:
B10 – liczba cykli łączeniowych, po których 10 proc. populacji ulegnie uszkodzeniu,
C – liczba cykli działania,
T cycle – czas pomiędzy rozpoczęciem dwóch kolejnych cykli, wyrażony w sekundach na cykl.

Dodatkowym warunkiem jaki musi zostać spełniony aby wyrażenia (4) i (5) były prawdziwe jest spełnienie kryterium (6) oraz praca systemu na ciągłe lub częste przywołanie:

$$\lambda\ T1\ \ll 1 \tag{6}$$

gdzie:
T1 – najmniejszy odstęp między okresowymi testami sprawdzającymi lub czasem życia.

Przykładowo przed rozpoczęciem pracy układu wykonywany jest kontrolny test zwarcia. Test ten pozwala wykryć defekty które są niewykrywalne przez automatyczne funkcje diagnostyczne układów logicznych.

2.2. Diagnostyka układu

Pokrycie diagnostyczne DC (ang. Diagnostic Coverage) oblicza się ze wzoru (7). Inną możliwością jest odszukanie wartości DC bezpośrednio z normy [7] lub [8]:

$$DC = \frac{\Sigma\lambda\ dd}{\Sigma\lambda\ dd + \Sigma\lambda\ du} \tag{7}$$

gdzie:
λdd – intensywność wykrywalnych niebezpiecznych uszkodzeń [1/h]
λdu – intensywność niewykrywalnych niebezpiecznych uszkodzeń [1/h]

Wskaźnik uszkodzeń bezpiecznych SFF oblicza się z zależności (8) do (12):

$$SFF = \frac{\sum\lambda\ s + \sum\lambda\ dd}{\sum\lambda\ s + \sum\lambda\ d} \tag{8}$$

$$\lambda = \lambda\ d + \lambda\ s = \frac{\lambda}{2} + \frac{\lambda}{2} \tag{9}$$

$$\lambda\ d = \lambda\ du + \lambda\ dd = \frac{\lambda}{2} \tag{10}$$

$$\lambda\ dd = \lambda\ d\ DC = \frac{\lambda}{2}\ DC \tag{11}$$

$$\lambda\ du = \lambda\ d\ (1 - DC) = \frac{\lambda}{2}\ (1 - DC) \tag{12}$$

gdzie:
λ dd – intensywność wykrywalnych niebezpiecznych uszkodzeń [1/h],
λ du – intensywność niewykrywalnych niebezpiecznych uszkodzeń [1/h],
λ d – intensywność uszkodzeń niebezpiecznych [1/h],
λ s – intensywność uszkodzeń bezpiecznych [1/h].

We wzorze (9) przyjęto że liczba uszkodzeń bezpiecznych i niebezpiecznych jest sobie równa i stanowi połowę wszystkich uszkodzeń. Zasadę tę stosuje się najczęściej w praktyce projektowej. W celu dokładniejszego podzielnie uszkodzeń na bezpieczne i niebezpieczne można posłużyć się modelami probabilistycznymi lub analizą FMEA.

2.3. Uszkodzenia spowodowane wspólną przyczyną

Jako uszkodzenie wspólną przyczyną rozumie się takie zdarzenie (lub splot zdarzeń) które powodują jednoczesne uszkodzenie dwóch lub więcej oddzielnych kanałów w układzie wielokanałowym i prowadzą do uszkodzenia funkcji sterowania. Przykładem takiego zdarzenia może być wzrost temperatury w szafie sterowniczej. Przekroczenie dopuszczalnych warunków pracy może spowodować awarie wielu układów znajdujących się wewnątrz szafy. Przyczyną wzrostu temperatury może być uszkodzenie wentylatora w szafie sterowniczej (jedna przyczyna dla wielu uszkodzeń). Należy zwrócić uwagę, że uszkodzenie nie muszą nastąpić w tym samym czasie.

Wskaźnik CCF określa się przypisując punkty za różne rozwiązania (rysunek 2). W zależności od czynnika przyznaje się pełną liczbę punktów (jeśli warunek jest spełniony) lub zero (jeśli warunek nie jest spełniony lub jest spełniony tylko częściowo). Po zsumowaniu liczby punktów określa się poziom współczynnika wrażliwości na wspólne uszkodzenie β na podstawie tabeli 5.

2.4. Architektura układu

Architekturę układu można podzielić na 4 kategorie [8] – A, B, C, D. Architektura układu zależy min. od ilości kanałów (redundancji układu), zastosowania funkcji kontrolnych, odporności na uszkodzenie czy pokrycia diagnostycznego. Determinuje też ona sposób obliczania współczynnika intensywności uszkodzeń λ. Rysunki 3–6 oraz równania (13)–(17) opisują poszczególne rodzaje architektury.

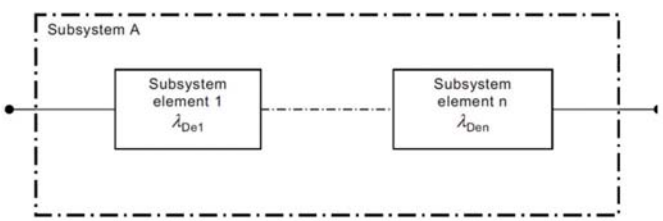
Rysunek 3 przedstawia architekturę typu A. Jest to najprostszy układ w którym elementy systemu są połączone szeregowo. Uszko-

Tab. 5. Współczynnik β

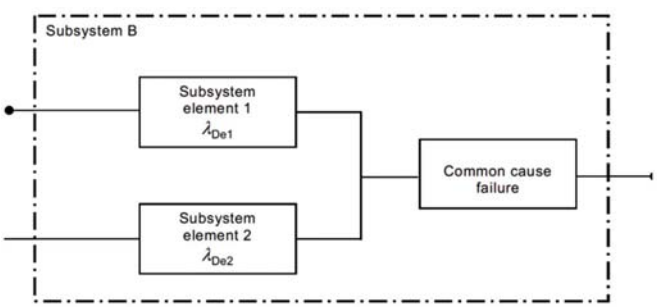
Suma CCF	Współczynnik β
< 35	10%
35-60	5%
60-85	2%
85-100	1%

ŚRODEK/WYMAGANIE	PUNKTY
SEPARACJA	
1a. Oddzielne prowadzenie kabli sygnałowych każdego z kanału albo ich ekranowanie lub…	5
1b. …lub zastosowanie właściwych środków do wykrywania błędów transmisji cyfrowej	10
Oddzielne prowadzenie kabli sygnałowych od zasilających albo ich ekranowanie – oddzielenie przewodów zasilających od przewodów z danymi nie jest konieczne, gdy dane przesyłane są optycznie lub gdy linie zasilające małej mocy służą do zasilania elementów bezpieczeństwa i jednocześnie do przesyłu danych	5
Rozmieszczenie elementów podsystemu wrażliwych na CCF w osobnych obudowach	5
RÓŻNORODNOŚĆ / REDUNDANCJA	
Różne technologie elektryczne, np. pierwszy kanał: programowalna elektronika, a drugi kanał: przekaźniki elektromechaniczne	8
Różne zasady fizyczne, np. czujniki elektromechaniczne i magnetyczne do monitorowania obecności osłony	10
Wykorzystanie elementów z chwilowymi różnicami w działaniu funkcjonalnym i/lub rodzajami uszkodzeń	10
Odstępy między testami diagnostycznymi ≤ 60 sekund	10
ZŁOŻONOŚĆ	
Zapobieganie przed połączeniami krzyżowymi między kanałami (z wyjątkiem stosowanych do diagnostyki)	2
ANALIZY	
Wyeliminowanie źródeł defektów spowodowanych wspólną przyczyną poprzez Analizę Rodzajów i Skutków Uszkodzeń FMEA	9
Uwzględnienie w projekcie wyników analizy uszkodzeń	9
SZKOLENIA	
Szkolenie projektantów w celu pojmowania skutków uszkodzeń spowodowanych wspólną przyczyną	4
ŚRODOWISKO	
Zbadanie elementów na wpływ temperatury, wilgotności, korozji, wibracji, kurzu itd.	9
Odporność podsystemu na działanie zaburzeń elektromagnetycznych w podwyższonych zakresach według IEC 61326-3-1	9

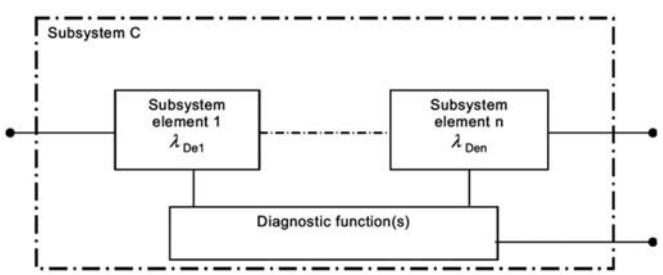
Rys. 2. *Wskaźnik CCF [4]*



Rys. 3. *Architektura typu A [11]*



Rys. 4. *Architektura typu B [11]*



Rys. 5. *Architektura typu C [11]*

dzenie któregokolwiek z elementów skutkuje utratą funkcji bezpieczeństwa stąd HFT=0. Intensywność uszkodzeń układu jest sumą intensywności wszystkich elementów (13). Średnia częstość uszkodzeń niebezpiecznych na godzinę wynosi (14). Wzór ten obowiązuje dla wszystkich rodzajów architektury.

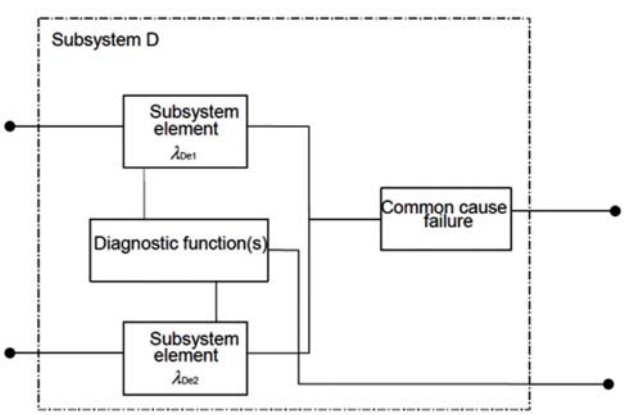
$$\lambda\, DssA = \lambda\, de1 + \lambda\, de2 + \cdots + \lambda\, den \qquad (13)$$

$$PFHD\ ssa = \lambda\, DssA\ 1h \qquad (14)$$

Architektura typu B (rysunek 4) to układ redundantny. Uszkodzenie jednego z elementów nie powoduje utraty funkcji bezpieczeństwa (HFT=1). Dla takiej architektury należy przeanalizować uszkodzenia o wspólnej przyczynie (15):

$$\lambda\, DssB = (1-\beta)^{\,2}\, \lambda\, de1\, \lambda\, de2\, T1 + \beta\, \frac{\lambda\, de1 + \lambda\, de2}{2} \qquad (15)$$

Architektura typu C (rysunek 5) jest podobna do architektury A. Szeregowo połączone elementy są poszerzone o funkcje diagno-



Rys. 6. *Architektura typu D [11]*

styczną (16). Pomimo zastosowania funkcji diagnostycznych tolerancja na uszkodzenie HFT=0.

$$\lambda\, DssC = \lambda\, de1(1 - DC1) + \lambda\, de2(1 - DC2) + \\ + \cdots + \lambda\, den(1 - DCn) \quad (16)$$

Układy o architekturze D (rysunek 6) mają równoległe połączenie elementów z dodatkową funkcją diagnostyczną (17). Dzięki redundancji kanałów HFT=1.

$$\lambda\, DssD = (1 - \beta)^2 \left(\frac{\lambda\, de1\, \lambda\, de2(DC1 + DC2)T2}{2} + \right. \\ \left. + \frac{\lambda\, de1\, \lambda\, de2(2 - DC1 - DC2)T1}{2} \right) \quad (17)$$

3. Wyznaczanie SILCL oraz PFHD całego systemu

Po wyznaczeniu poziomu SIL oraz PFHD dla wszystkich elementów i podsystemów należy obliczyć poziom tych parametrów dla całego układu. Częstość uszkodzeń niebezpiecznych funkcji bezpieczeństwa liczy się sumując PFHD dla wszystkich podsystemów zgodnie z (2). Jest ona wypadkową średniego czasu do uszkodzeń, intensywności uszkodzeń, pokrycia diagnostycznego, uszkodzeń spowodowanych wspólną przyczyną oraz architektury układu (18):

$$PFHD\ sys\ (MTTF, \lambda, DC, CGG, architektura) \quad (18)$$

Po obliczeniu PFHD dla całego systemu należy określić poziom SIL systemu zgodnie z tabela 6.

Kolejnym etapem jest obliczenie wskaźnika uszkodzeń bezpiecznych dla całego układu (8). Następnie określa się poziomu SIL układu zgodnie z tabelą 7 uwzględniając tolerancję sprzętu na uszkodzenia. Parametr SFF jest wypadkową intensywności uszkodzeń bezpiecznych, niebezpiecznych, wykrywalnych oraz niewykrywalnych i pokrycia diagnostycznego (19):

$$SFF(\lambda\, s, \lambda\, dd, \lambda\, d, DC) \quad (19)$$

Po określeniu poziomu nienaruszalności bezpieczeństwa na podstawie SFF i PFHD należy porównać otrzymane wartości. Jeśli wyniki są różne należy przyjąć gorszy przypadek. Następnie należy porównać otrzymany poziom SIL z wymaganym. Jeśli rozpatrywany układ ma wyższy lub równy poziom bezpieczeństwa od wymaganego wówczas rozwiązanie można uznać za bezpieczne. W przypadku gdy system otrzymał niższy stopień bezpieczeństwa niż jest wymagany musi zostać przeprojektowany a procedura obliczeniowa musi być powtórzona.

Tab. 6. Współczynnik β

SIL	PFHD	PL
-	≥ 10 -5 do <10 -4	a
1	≥ 3*10 -6 do <10 -5	b
1	≥ 10 -6 do < 3*10 -6	c
2	≥ 10 -7 do <10 -6	d
3	≥ 10 -8 do <10 -7	e

Tab. 7. Poziom SIL w zależności od SFF

SFF	HFT		
	0	1	2
< 60%	-	SIL 1	SIL 2
60%< 90%	SIL 1	SIL 2	SIL 3
90%< 99%	SIL 2	SIL 3	SIL 3
≥99%	SIL 3	SIL 3	SIL 3

Podsumowanie

Norma PN-EN 62061 jest jedną w dwóch najczęściej wykorzystywanych do oceny bezpieczeństwa maszyn. Dedykowana jest ona przede wszystkim do oceny bezpieczeństwa układów elektronicznych stąd też większą popularnością w branży maszynowej cieszy się norma PN-EN 13849. Nie mniej w wysoce zautomatyzowanych urządzeniach o zaawansowanych układach sterowania elektronicznego z powodzeniem można stosować algorytmu obliczeniowe poziomu SIL. Obie normy wykorzystują podobne lub takie same wskaźniki jednak algorytm postepowania oraz obliczenia są różne. Norma 62061 skupia się przede wszystkim na funkcjach sterowania związanych z bezpieczeństwem. Znając poziom częstości uszkodzeń niebezpiecznych istnieje możliwość porównania poziomów bezpieczeństwa liczonych obiema metodami (tabela 6).

Bibliografia:

1. Danilczuk W., *Komputerowe wspomagane metody ilościowe w bezpieczeństwie maszyn*, „Autobusy – Technika, Eksploatacja, Systemy Transportowe" 2018, nr 1-2.
2. Dyrektywa 2006/42/We Parlamentu Europejskiego i Rady z dnia 17 maja 2006 r. w sprawie maszyn, zmieniająca dyrektywę 95/16/WE.
3. Kalkulator MTF firmy ALD: https://aldservice.com/Free-MTBF-Calculator-User-Guide.html (dostęp 01.07.2018).
4. Kasprzyczak L., *Wyznaczanie poziomów bezpieczeństwa SIL i PL*, „Automatyka" 2015, nr 1–2.
5. Marszal E. M., Scharpf E. W., *Safety Integrity Level Selection: Systematic Methods Including Layer of Protection Analysis*, Instrumentation, Systems, and Automation Society, 2002.
6. Norma PN-EN ISO 12100: Bezpieczeństwo maszyn. Ogólne zasady projektowania. Ocena ryzyka i zmniejszanie ryzyka.
7. Norma PN-EN ISO 13849 1:2008: Bezpieczeństwo maszyn – Elementy systemów sterowania związane z bezpieczeństwem – Część 1: Ogólne zasady projektowania.
8. Norma PN-EN ISO 62061:2008 Bezpieczeństwo maszyn – Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem.
9. Rozporządzenie Ministra Gospodarki z dnia 21 października 2008 r. w sprawie zasadniczych wymagań dla maszyn: Dz. U 2008, nr 199, poz. 1228.
10. Siemens SN 29500 standard: https://www.isograph.com/software/reliability-workbench/reliability-prediction/siemens-sn-29500/ (dostęp 01.07.2018).
11. Sohal R., *Safety Categories*, Performance Levels and SILs for Machine Safety Control Systems, National Robot Safety Conference, 2016.

Machine safety – determination of Safety Integrity Level

The article presents a method for assessing the safety of machines based on the calculation of the safety integrity level (SIL). Problems of machine safety were presented in the context of applicable legal regulations and international standards. On the basis of literature and standards, methods for determining the level of safety integrity, quantitative and qualitative measures used within the PN-EN 62061 standard and basic concepts related to functional requirements were presented. Additionally, the relationship between the level of security integrity of SIL and the level of PL security is presented. The article is a continuation of the author's previous publication on machine safety [8].

Keywords: risk management, machine safety, safety integrity level.

Autor:

mgr inż. **Wojciech Danilczuk** – Politechnika Lubelska, Wydział Mechaniczny, Katedra Automatyzacji