SAFETY OF MACHINERY – DETERMINATION OF PERFORMANCE LEVEL

BEZPIECZEŃSTWO MASZYN – WYZNACZANIE POZIOMU ZAPEWNIENIA BEZPIECZEŃSTWA

Leszek Kasprzyczak

Instytut Technik Innowacyjnych EMAG

Abstract: *The article presents a method for determining the performance level (PL) on the basis of the PN-EN ISO 13849-1 standard, which is harmonized with the machinery directive 2006/42/EC. The risk assessment and risk reduction criteria, according to PN-EN ISO 12100, were briefly characterized. The focus was put on determining the required performance level PLr on the basis of a risk graph. The method was presented how to use a safety function composed of input-, logical- and execution subsystems. It was demonstrated how to determine the achieved PL for a safety function composed of hardware elements on the basis of a safety category, mean time to dangerous failures (MTTFd), diagnostic coverage (DC), and immunity to common cause failures (CCF).*

Keywords: *machinery directive 2006/42/EC, performance level PL, safety category, mean time to dangerous failures MTTFd, diagnostic coverage DC, common cause failures CCF.*

Streszczenie: *W artykule omówiono metodę wyznaczania Poziomu Zapewnienia Bezpieczeństwa PL na podstawie normy PN-EN ISO 13849-1, która jest zharmonizowana z dyrektywą maszynową 2006/42/WE. Krótko scharakteryzowano zasady oceny i zmniejszenia ryzyka wg normy PN-EN ISO 12100. Skoncentrowano się na określeniu wymaganego poziomu PLr na podstawie grafu ryzyka. Przedstawiono praktyczną realizację funkcji bezpieczeństwa złożonej z podsystemów wejściowych, logicznych i wykonawczych. Pokazano sposób wyznaczania osiągniętego PL dla funkcji bezpieczeństwa złożonej z elementów sprzętowych na podstawie struktury układu (kategorii), wartości średniego czasu pomiędzy niebezpiecznymi uszkodzeniami (MTTFd), pokrycia diagnostycznego (DC) i odporności na uszkodzenia spowodowane wspólną przyczyną (CCF).*

Słowa kluczowe: *dyrektywa maszynowa 2006/42/WE, poziom zapewnienia bezpieczeństwa PL, kategorie bezpieczeństwa, średni czas pomiędzy niebezpiecznymi uszkodzeniami MTTFd, pokrycie diagnostyczne DC, uszkodzenia spowodowane wspólną przyczyną CCF.*

1. Wstęp

Poziom Zapewnienia Bezpieczeństwa PL (ang. Performance Level) jest bardzo istotnym parametrem określającym stopień odporności na defekty danej funkcji bezpieczeństwa w układzie sterowania maszyny. Sposoby wyznaczania PL opisane są w angielskojęzycznej normie PN-EN ISO 13849-1 [1]. Norma ta jest zharmonizowana z dyrektywą maszynową (MD) 2006/42/WE, która wprowadzona została w Polsce rozporządzeniem Ministra Gospodarki. Do interpretacji przepisów dyrektywy opracowany został przewodnik Komisji Europejskiej. Celem wprowadzenia dyrektywy maszynowej było ułatwienie swobodnego przepływu towarów i zlikwidowanie technicznych przeszkód w handlu wewnątrz krajów Europejskiego Obszaru Gospodarczego.

Z dyrektywą MD zharmonizowana jest również angielskojęzyczna norma PN-EN ISO 12100 [2], w której zawarto dwa kluczowe aspekty dotyczące zasad oceny ryzyka i zmniejszania ryzyka. Praktyczną interpretację tych wytycznych przedstawiono w pracy [3]. Jeśli wymagane jest zmniejszenie ryzyka, to osiąga się to w trzech krokach zwanych triadą bezpieczeństwa:

- 1) rozwiązania konstrukcyjne bezpieczne same w sobie,
- 2) techniczne środki ochronne i uzupełniające środki ochronne,
- 3) informacje dotyczące bezpieczeństwa użytkowania.

Kroki te omówiono w pracy [3] i w normie [2].

Zrozumiałym jest, że im bardziej zmniejszenie ryzyka jest zależne od elementów systemów sterowania związanych z bezpieczeństwem, tym jest wymagana większa odporność tych elementów na defekty. Odporność ta może być wyrażona ilościowo wskaźnikami niezawodności oraz za pomocą struktury odpornej na defekty. Poziom zapewnienia bezpieczeństwa PL stosowany jest w drugim kroku triady bezpieczeństwa. Dalej przedstawiono praktyczne sposoby wyznaczania PL systemu zwłaszcza w sytuacji, gdy użyto podsystemów o nieokreślonych PL.

2. Specyfikacja funkcji bezpieczeństwa i poziomu bezpieczeństwa

W celu określenia wymaganego poziomu zapewnienia bezpieczeństwa PLr (ang. required) danej funkcji bezpieczeństwa stosuje się graf ryzyka składający się z ciężkości urazów, częstości narażenia i/lub czasu jego trwania oraz z możliwości uniknięcia zagrożenia lub ograniczenia szkód (rys. 1).

Graf ryzyka jest stosowany tylko do wyznaczenia PLr dla danych funkcji bezpieczeństwa i nie jest stosowany do szacowania ryzyka dla całej maszyny. Zazwyczaj funkcja bezpieczeństwa jest zrealizowana z trzech elementów (rys. 2): czujnika wykrywającego zagrożenie, jednostki logicznej analizującej sygnały z czujnika i podłączonego do jednostki sterującej elementu wykonawczego (np. stycznika wyłączającego niebezpieczny napęd). W tym przypadku

specyfikacja funkcji bezpieczeństwa mogłaby być zdefiniowana następująco „Zatrzymanie niebezpiecznego napędu przez otwarcie osłony bezpieczeństwa i uniemożliwienie jego uruchomienia do czasu zamknięcia osłony”.

Rys. 1. Graf ryzyka do wyznaczania wymaganego PLr danej funkcji bezpieczeństwa

Rys. 2. Podsystemy funkcji bezpieczeństwa zatrzymania niebezpiecznego napędu

3. Uzyskany poziom zapewnienia bezpieczeństwa

PL przyjmuje 5 dyskretnych poziomów: od „a” do „e”, przy czym poziom „e” charakteryzuje się największą niezawodnością i odpornością na defekty. Jeżeli funkcję bezpieczeństwa zrealizowano z elementów posiadających określone PL to możliwy do uzyskania PL całego systemu wynika z „najsłabszego” PL podsystemu składowego oraz z liczby podsystemów posiadających taki PL (tabela 1).

Tabela 1. Wyznaczenie PL systemu na podstawie znajomości PL podsystemów

Najniższy PL podsystemu	Liczba podsystemów posiadających taki PL	=>	Maks. możliwy do uzyskania PL systemu
a	> 3	=>	niedozwolony
	≤ 3	=>	a
b	> 2	=>	a
	≤ 2	=>	b
c	> 2	=>	b
	≤ 2	=>	c
d	> 3	=>	c
	≤ 3	=>	d
e	> 3	=>	d
	≤ 3	=>	e

W przypadku, gdy PL nie jest znany dla wszystkich podsystemów, należy najpierw samodzielnie określić poziom bezpieczeństwa takiego podsystemu. Określenie poziomu zapewnienia bezpieczeństwa dla podsystemu uzyskuje się na podstawie:

- struktury układu (kategorii),
- wartości średniego czasu pomiędzy niebezpiecznymi uszkodzeniami (MTTFd),
- pokrycia diagnostycznego (DC),
- odporności na uszkodzenia spowodowane wspólną przyczyną (CCF).

Struktura układu - kategorie

Istnieje 5 kategorii: B, 1, 2, 3, 4. Układy jednokanałowe mogą być kategorii B oraz 1. Kategoria 2 charakteryzuje układ jednokanałowy z monitorowaniem defektów w podsystemach. Kategorie 3 i 4 dotyczą układów wielokanałowych (redundantnych). W tabeli 2 przedstawiono porównanie poszczególnych kategorii.

Średni czas pomiędzy niebezpiecznymi uszkodzeniami MTTFd

W załączniku C normy PN-EN ISO13849-1 podano 4 metody obliczania/szacowania MTTFd dla pojedynczych części:

- 1) Metoda dobrych praktyk inżynierskich,
- 2) Metoda dla części hydraulicznych,
- 3) Dla części pneumatycznych, mechanicznych i elektromechanicznych,
- 4) Dla części elektrycznych.

W przypadku pierwszej metody w tabeli podano typowe wartości MTTFd w latach dla części mechanicznych i hydraulicznych. Dla części pneumatycznych i elektrycznych podano parametr B_{10d} , który określa ilość cykli, po których niebezpiecznemu uszkodzeniu ulegnie 10% badanej populacji.

Tabela 2. Skrócony opis kategorii bezpieczeństwa

Kat.	Skrócony opis			
B	Zastosowanie elementów zgodnych z normami i podstawowymi zasadami bezpieczeństwa, wytrzymujące przewidywane narażenia. Wystąpienie defektu może powodować utratę funkcji bezpieczeństwa.			
1	Jak w B oraz zastosowano wypróbowane elementy i sprawdzone zasady bezpieczeństwa. Wystąpienie defektu może powodować utratę funkcji bezpieczeństwa, ale prawdopodobieństwo tego jest niższe niż w kat. B.			
2	Jak w B oraz zastosowano sprawdzone zasady bezpieczeństwa. Funkcja bezpieczeństwa jest sprawdzana przez układ sterowania. Wystąpienie defektu może powodować utratę funkcji bezpieczeństwa między sprawdzeniami.			
3	Jak w B oraz zastosowano sprawdzone zasady bezpieczeństwa. Struktura odporna na pojedynczy defekt; częściowa detekcja usterek.			
4	Jak w B oraz zastosowano sprawdzone zasady bezpieczeństwa. Struktura odporna na kilka defektów. Wykryte w odpowiednim czasie defekty zapobiegają utracie bezpieczeństwa.			
		Sprawdzone zasady bezpieczeństwa		
		Detekcja usterek		
		Redundancja		

Dla części hydraulicznych, w metodzie drugiej podano sztywną wartość $MTTFd=150$ lat.

$MTTFd$ dla części pneumatycznych, mechanicznych i elektromechanicznych w metodzie trzeciej wyznaczany jest z parametru B_{10d} ze wzoru:

$$MTTFd = \frac{B_{10d}}{0,1 \cdot n_{op}} \quad (1)$$

gdzie:

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600 \frac{\text{sek.}}{\text{godz.}}}{t_{cycle}},$$

n_{op} – średnia ilość cykli na rok,

d_{op} – średni czas pracy w dniach na rok,

h_{op} – średni czas pracy w godzinach na dzień,

t_{cycle} – średni czas pomiędzy rozpoczęciem dwóch kolejnych cykli w sekundach na cykl.

Oszacowanie $MTTFd$ dla elementów elektronicznych w metodzie 4-tej polega na odczycie z tabel wartości $MTTFd$ dla elementów (tranzystorów, diod, kondensatorów itd.), z których zbudowany jest dany kanał. Czasy poszczególnych elementów w obrębie kanału należy następnie zsumować wg zależności:

$$\frac{1}{MTTFd_{CH1}} = \frac{1}{MTTFd_{el1}} + \dots + \frac{1}{MTTFd_{eln}} = \sum_{i=1}^n \frac{1}{MTTFd_{eli}} \quad (2)$$

Jeśli czasy $MTTFd$ poszczególnych kanałów w systemie redundantnym są różne to należy dokonać symetryzacji wg zależności:

$$MTTFd = \frac{2}{3} \left(MTTFd_{CH1} + MTTFd_{CH2} - \frac{1}{\frac{1}{MTTFd_{CH1}} + \frac{1}{MTTFd_{CH2}}} \right) \quad (3)$$

Do dalszej analizy bierze się czas uzyskany ze wzoru (3).

Średni czas pomiędzy niebezpiecznymi uszkodzeniami $MTTFd$ jest podzielony na trzy zakresy przedstawione w tabeli 3.

Tabela 3. Zakresy MTTFd dla kanału

Oznaczenie	Zakres dla kanału
Krótki	$3 \text{ lata} \leq \text{MTTFd} < 10 \text{ lat}$
Średni	$10 \text{ lat} \leq \text{MTTFd} < 30 \text{ lat}$
Długi	$30 \text{ lat} \leq \text{MTTFd} \leq 100 \text{ lat}$

Pokrycie diagnostyczne DC

Usterki można podzielić na bezpieczne i niebezpieczne. Stosunek wykrywanych uszkodzeń niebezpiecznych λ_{DD} do wszystkich uszkodzeń niebezpiecznych (wykrywanych λ_{DD} i niewykrywanych λ_{DU}) określa pokrycie diagnostyczne:

$$DC = \frac{\Sigma \lambda_{DD}}{\Sigma \lambda_{DD} + \Sigma \lambda_{DU}} \quad (4)$$

W załączniku E normy [1] stabelaryzowano rozmaite metody monitorowania defektów w podsystemach z podaniem typowych wartości DC w procentach. Np. jeśli monitoruje się główne styki stycznika przy pomocy sprzężonych mechanicznie styków pomocniczych, to przyjmuje się $DC=99\%$. Pokrycie diagnostyczne DC przyjmuje trzy zakresy przedstawione w tabeli 4.

Tabela 4. Zakresy pokrycia diagnostycznego DC

Oznaczenie	Zakres
Niskie	$60\% \leq DC < 90\%$
Średnie	$90\% \leq DC < 99\%$
Wysokie	$DC \geq 99\%$

Odporność na uszkodzenia spowodowane wspólną przyczyną CCF

Parametr CCF określa odporność na uszkodzenia różnych podsystemów spowodowane pojedynczym zdarzeniem, przy czym uszkodzenia te nie są wzajemnymi następstwami. W tabeli 5 zebrano środki/wymagania chroniące przed tego typu uszkodzeniami. Jeśli zastosowano w podsystemie dany środek zapobiegawczy to przyznaje się pełną liczbę punktów (nie przyznaje się punktów

częściowych!). Punkty następnie się sumuje. Maksymalna ilość punktów wynosi 100. Odporność na CCF jest zadawalająca, gdy suma punktów jest większa od 65 punktów łącznie. Sprawdzenie odporności na CCF wymagane jest tylko dla kategorii 2, 3 i 4.

Tabela 5. Odporność na CCF

ŚRODEK / WYMAGANIE		Punkty
Odseparowanie	Odseparowanie obwodów sygnałowych (przewodów elektrycznych, hydraulicznych, cięgien mechanicznych), dostateczne odstępy powierzchniowe i powietrzne	15
Zróźnicowanie	Różne technologie lub fizyczne zasady, np. pierwszy kanał programowalny a drugi kanał sprzętowy; pomiar cyfrowy i analogowy; elementy różnych producentów	20
Projekt zastosowanie doświadczenie	Ochrona przed przepięciem, przeciążeniem, zwiększonym ciśnieniem, np. w mechanice sprzęgła przeciążeniowe	15
	Zastosowanie wypróbowanych elementów	5
Ocena Analiza	Przeprowadzenie analizy rodzajów i skutków uszkodzeń (FMEA), aby uniknąć uszkodzeń spowodowanych wspólną przyczyną w projektowaniu	5
Kompetencje Szkolenia	Szkolenie projektantów w kierunku pojmowania przyczyn i skutków uszkodzeń spowodowanych wspólną przyczyną	5
Wpływy środowiska	EMC (dla elektryki), czystość medium (dla hydrauliki i pneumatyki), współczynnik bezpieczeństwa (dla mechaniki)	25
	Testy systemu pod kątem wpływu temperatury, wstrząsów, wibracji, wilgotności, substancji korozyjnych itp.	10

Określenie PL podsystemu

Mając wyznaczone wszystkie cztery parametry można przejść do określenia PL podsystemu korzystając z rys. 3. Np. jeżeli architektura układu jest wielokanałowa i $CCF \geq 65$ oraz pokrycie diagnostyczne jest na poziomie średnim, to przy czasie

MTTF_d=długi osiągnięte PL umiejscowione jest na pograniczu PL d/e. Jeśli jest to zasadne, w celu dokładnego odczytu, należy skorzystać z wartości stabelaryzowanych w tabeli K.1 [1] uwzględniających dodatkowy parametr PFH_D (prawdopodobieństwo niebezpiecznego uszkodzenia na godzinę). Lecz jeśli „słabsze” rozwiązanie jest satysfakcjonujące, to można poprzestać na jego przyjęciu.

Rys. 3. Wyznaczanie PL dla podsystemu

W celu określenia PL całego systemu korzysta się jak poprzednio z tabeli 1. Jeśli otrzymany PL z tabeli 1 jest większy lub równy od wymaganego dla funkcji bezpieczeństwa PL_r, to stwierdza się, że układ bezpieczeństwa spełnia właściwe wymagania i charakteryzuje się odpowiednią niezawodnością i odpornością na defekty.

4. Podsumowanie

Trudnością w implementacji dyrektywy maszynowej i wymienionych norm jest to, że wprowadzają one nowe, angielskojęzyczne pojęcia nieznane do tej pory szerokiemu gronu użytkowników. Obecnie w Komitecie Technicznym KT158 Polskiego Komitetu Normalizacyjnego trwają prace nad przetłumaczeniem tych norm na język polski.

5. Literatura

- [1] PN-EN ISO 13849-1:2008+AC:2009 Bezpieczeństwo maszyn – Elementy systemów sterowania związane z bezpieczeństwem – Część 1: Ogólne zasady projektowania
- [2] PN-EN ISO 12100:2011 Bezpieczeństwo maszyn – Ogólne zasady projektowania – Ocena ryzyka i zmniejszanie ryzyka
- [3] Kasprzyczak L.: Program certyfikacji wyrobów na zgodność z dyrektywą maszynową w Centrum Badań i Certyfikacji Instytutu EMAG. Mechanizacja i Automatyzacja Górnictwa, 6(496)/2012, ss.13-20

***dr inż. Leszek Kasprzyczak** – adiunkt w Instytucie Technik Innowacyjnych EMAG, specjalista w zakresie mechatroniki, systemów pomiarowych, bezpieczeństwa funkcjonalnego oraz budowy i eksploatacji maszyn.*