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

METODOLOGIA OCENY NIENARUSZALNOŚCI BEZPIECZENSTWA ELEMENTÓW O USTALONEJ TRWAŁOŚCI

Przytoczono definicję nienaruszalności bezpieczeństwa funkcji związanej z bezpieczeństwem i wymagania wynikające z odpowiednich norm, jak też wskazaną w normie metodę wyznaczenia poziomu nienaruszalności bezpieczeństwa elementów o ustalonej trwałości. Przeanalizowano zależność tego poziomu od poziomu trwałości i prawdopodobieństwa jego wyznaczenia. Przeanalizowano metodykę postępowania z punktu widzenia użytkownika i wytwórcy.

METHODOLOGY OF SAFETY INTEGRITY ASSESSMENT FOR THE ELEMENTS WITH DEFINED MISSION TIME

The definition of the safety integrity of the safety-related function and requirements resulting from the relevant standards are referenced, as well as the method of evaluation of the safety integrity level, recommended in the above mentioned standards for the elements with stated mission time. The dependency of the safety integrity level from the level of the mission time and from the probability of its evaluation are analyzed, as well as the method of evaluation from the points of view of the user and the manufacturer.

1. WPROWADZENIE

1.1. Wstęp

Wprowadzone dyrektywami Unii Europejskiej wymagania zasadnicze dotyczące maszyn wprowadzanych do obrotu [1], jak też wymagania minimalne dotyczące maszyn nabytych w Polsce przed 1 stycznia 2003 r. nakładają obowiązek przeanalizowania ryzyka powodowanego przez maszyny i inny sprzęt produkcyjny i gdy jest ono zbyt duże, wprowadzenia stosownych środków redukcji ryzyka.

Szczególne znaczenie ma odpowiednie podejście do układów sterowania maszyn, począwszy od najprostszych, np. automatycznego zamykania osłony bezpieczeństwa, do skomplikowanych urządzeń sterowania automatycznego grupami maszyn i urządzeń.

Jednym z elementów redukcji ryzyka są systemy związane z bezpieczeństwem realizujące funkcje bezpieczeństwa. Systemy te, z reguły zawierające składniki programowalne, powinny spełniać wymagania podane w [3], w więc mieć określony poziom nienaruszalności bezpieczeństwa.

W obwodach realizujących funkcje bezpieczeństwa występują czujniki, układy logiczne i elementy wykonawcze. Nienaruszalność bezpieczeństwa każdego z nich ma wpływ na nienaruszalność bezpieczeństwa wynikową całego obwodu [5]. Czujniki i elementy

wykonawcze są na ogół charakteryzowane przez ich trwałość wyrażaną w godzinach gwarantowanej pracy bezawaryjnej lub w cyklach gwarantowanej pracy bezawaryjnej.

Do przeprowadzenia oceny i uzyskania konkluzji potrzebna jest znajomość nienaruszalności bezpieczeństwa tych elementów.

W dotychczasowych pracach [9,10] autor podał wyniki uzyskane ze wstępnej oceny danych zamieszczonych w katalogach. Wydaje się celowe szersze przedstawienie zagadnienia.

1.2. Nienaruszalność bezpieczeństwa [4]

Definicja - Prawdopodobieństwo, że system związany z bezpieczeństwem wykona satysfakcjonująco wymagane funkcje bezpieczeństwa we wszystkich określonych warunkach i w określonym okresie czasu

Poziom nienaruszalności bezpieczeństwa SIL) jest to poziom dyskretny, jeden z czterech możliwych, do wyszczególniania wymagań nienaruszalności bezpieczeństwa funkcji bezpieczeństwa, przy czym poziom 4 jest najwyższym a poziom 1 – najniższym.

Wymagania – wg tablicy 1 [3]

Tablica 1 – Poziomy nienaruszalności bezpieczeństwa: docelowe miary uszkodzeń funkcji bezpieczeństwa działających w rodzaju pracy na częste żądanie lub ciągłym

Poziom nienaruszalności bezpieczeństwa	**Rodzaj pracy na częste żądanie lub ciągły** (Prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę)
4	od $\geq 10^{-9}$ do $< 10^{-8}$
3	od $\geq 10^{-8}$ do $< 10^{-7}$
2	od $\geq 10^{-7}$ do $< 10^{-6}$
1	od $\geq 10^{-6}$ do $< 10^{-5}$

Podany w tablicy 3 parametr dotyczący rodzaju pracy na częste żądanie lub ciągłego, prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę, jest niejednokrotnie nazywany częstością uszkodzeń niebezpiecznych lub intensywnością uszkodzeń niebezpiecznych i jest wyrażany w jednostkach uszkodzeń niebezpiecznych na godzinę.

1.3. Metoda obliczania, gdy urządzenia ma ustaloną trwałość [3]

Gdy system związany z bezpieczeństwem, działający w rodzaju pracy na częste żądanie lub ciągłym, od którego wymaga się pracy w określonym okresie trwałości, podczas którego nie mogą mieć miejsca naprawy, wymagany poziom nienaruszalności bezpieczeństwa funkcji bezpieczeństwa może zostać wyliczony następująco. Określa się wymagane prawdopodobieństwo uszkodzenia funkcji bezpieczeństwa w okresie trwałości i dzieli się je przez okres trwałości w celu otrzymania wymaganego prawdopodobieństwa uszkodzenia na godzinę, a następnie używa się tablicy 3 do wywnioskowania o poziomie nienaruszalności bezpieczeństwa.

Tę definicję przedstawia wzór:

$$P_{DF} = (1-P_T)/T_B \qquad (1)$$

gdzie:
P_{DF} – prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę;
P_T – prawdopodobieństwo wyznaczenia trwałości;
T_B – trwałość

2. CO DECYDUJE O WYNIKU

Rozważmy elementy, których trwałość wyraża się w godzinach pracy. Są to np. silniki elektryczne, prądnice tachometryczne i rezolwery.

Przy ustalonej wartości prawdopodobieństwa wyznaczenia trwałości, tj. przy $1\text{-}P_y$ = const. , prawdopodobieństwo niebezpiecznego uszkodzenia na godzinę jest odwrotnie proporcjonalne do trwałości. Przykładowo, gdy $1\text{-}P_y = 0.1472$ otrzymuje się (tablica 2):

Tablica 2 – Wartości P_{DF} przy stałej wartości $P_T = 0{,}8528$ i zmiennej wartości T_B

T_B [h]	3000	5000	8000	10000	16000	20000	25000	32000
$P_{DF} \times 10^{-5}$	4,9	2,9	1,84	1,47	0,92	0,736	0,589	0,46
SIL	X	X	X	X	1	1	1	1

X – nie określa się SIL z powodu zbyt małej nienaruszalności bezpieczeństwa. Przyjęta wartość 0,8528 dotyczą oszacowania przy nieznanej dystrybuancie uszkodzeń.

Przy określonej trwałości prawdopodobieństwo niebezpiecznego uszkodzenia na godzinę jest malejącą funkcją prawdopodobieństwa wystąpienia uszkodzenia. Przykładowo przy trwałości 20000 h (wartość typowa silników bezszczotkowych [9]) otrzymuje się dane jak w tablicy 3.

Tablica 3 – Wartości P_{DF} przy zmiennej wartości P_T i stałej wartości $T_B = 20000$ h

P_T	0,8	0,83	**0,8528**	0.90	0.95	0,98	0.99	**0,9958**
$1 - P_T$	0,2	0,17	**0,1472**	0,10	0,05	0,02	0.01	**0.0042**
$P_{DF} \times 10^{-5}$	1,0	0,85	**0,736**	0,5	0,25	0,1	0,05	**0,021**
SIL	X	1	!	1	1	1	2	**2**

X – nie określa się SIL z powodu zbyt małej nienaruszalności bezpieczeństwa
Wartości wyróżnione drukiem pogrubionym dotyczą oszacowania przy nieznanej dystrybuancie uszkodzeń.

Inna jest sytuacja, gdy rozpatrywać elementy pracujące w sposób impulsowy, których trwałość jest wyrażana w liczbie cyklów pracy. Do tej grupy należą m.in. przekaźniki, styczniki i kodery optyczne. Odpowiednią analizę zamieszczono w tablicach 4 i 5.

Tablica 4 – Wartości P_{DF} przy wartości $P_T = 0{,}8528$ i zmiennej liczbie cykli pracy T_B

$T_B \times 10^7$	0,001	0,003	0,005	0,01	0,03	0,05	0,10	1,0
$P_{DF} \times 10^{-5}$	1,472	0,49	0,294	0,147	0,049	0,029	0,0147	0,00147
SIL	X	1	1	1	2	2	2	3

X – nie określa się SIL z powodu zbyt małej nienaruszalności bezpieczeństwa.. Przyjęta wartość 0,8528 dotyczą oszacowania przy nieznanej dystrybuancie uszkodzeń.

Tablica 5 – Wartości P_{DF} przy zmiennej wartości P_T i stałej wartości $T_B = 10^7$ cykli

P_T	0,8	0,83	**0,8528**	0.90	0.95	0,98	0.99	**0,9958**
$1 - P_T$	0,2	0,17	**0,1472**	0,10	0,05	0,02	0.01	**0.0042**
$P_{DF} \times 10^{-7}$	0,2	0,17	**0,1472**	0,1	0,05	0,02	0,01	**0,0042**
SIL	3	3	**3**	3	4	4	4	**4**

Wartości wyróżnione drukiem pogrubionym dotyczą oszacowania przy nieznanej dystrybuancie uszkodzeń.

Jakie są konsekwencje tych zależności?

Istotnym parametrem wyznaczenia nienaruszalności bezpieczeństwa jest prawdopodobieństwo określenia deklarowanej trwałości. Jedynie przy elementach o trwałości odpowiadającej trwałości energetycznych elementów sterowniczych i zabezpieczających tj. 10^6 do 10^7 cykli pracy, prawdopodobieństwo powyżej 0,8 nie ma już istotnego znaczenia.

Podstawowym zagadnieniem metodyki jest więc:

- w sytuacji projektanta systemu związanego z bezpieczeństwem – oszacowanie nienaruszalności bezpieczeństwa elementów na podstawie danych katalogowych,
- w sytuacji wytwórcy elementów bezpieczeństwa - znalezienie drogi wyznaczenia deklarowanej trwałości z dużym prawdopodobieństwem, przy rozsądnych kosztach.

3. POSTĘPOWANIE W SYTUACJI PROJEKTANTA

Dysponując danymi katalogowymi projektant może na ogół znaleźć deklarowaną trwałość elementu, który ma zamiar zastosować, podaną w godzinach pracy bezawaryjnej lub liczbie cykli pracy. W dostępnych autorowi katalogach nie ma podanego prawdopodobieństwa wyznaczenia deklarowanej trwałości.

Projektant ma więc dwie drogi: zwrócenie się do wytwórcy o podanie prawdopodobieństwa wyznaczenia deklarowanej trwałości lub samodzielne oszacowanie tego prawdopodobieństwa.

Uzyskanie danych od wytwórcy rozwiązuje sprawę; wystarczy posłużyć się wzorem (1), aby zakończyć oszacowanie.

Jest inaczej, gdy takich danych nie można uzyskać. Projektant musi zrobić pewne założenia, umożliwiające oszacowanie prawdopodobieństwa wyznaczenia deklarowanej trwałości.

Pierwszym jest założenie, że dystrybuanta uszkodzeń jest nieznana; przy założeniu ciągłości i różniczkowalności dystrybuanty $F(t)$ trwałości T_B można zastosować nieparametryczną metodę wnioskowania o nieznanej dystrybuancie $F(t)$ i na tej podstawie o nieznanej funkcji niezawodności $R(t)$ rozpatrywanych elementów. Teoria takiego postępowania jest przedstawiona w pracy [6].

Sposób przeprowadzania testu przy takim założeniu oraz jego wyniki zostały przedstawione w pracy [7], skąd zaczerpnięto dane przytoczono w tablicy 6.

Tablica 6 – Granice przedziału ufności wskaźnika $R(t)$ na poziomie ufności $\beta = 0,9$

$M(t)$	Wskaźnik przy n	10	15	20	25	30	40	50	60
1	R_{jd}	0,6627	0,7642	0,8189	0,8528	0,8765	0,9060	0,9241	0,9365
	R_{jg}	0,9895	0,9930	0,9947	0,9958	0,9965	0,9973	0,9979	0,9982
2	R_{jd}	0,5502	0,6831	0,7547	0,8004	0,8322	0,8723	0,8971	0,9137
	R_{jg}	0,9483	0,9639	0,9731	0,9785	0,9821	0,9866	0,9893	0,9911

Oznaczenia: n – liczność próbki; $m(t)$ – liczba sztuk uszkodzonych w czasie próby;
R_{jd} – dolny przedział ufności wskaźnika $R(t)$; R_{jg} - górny przedział ufności wskaźnika $R(t)$.

Jeżeli jako oszacowanie zbliżone do rzeczywistości przyjąć wyniki z testu na próbce o liczności 25 szt. (próbka już statystycznie znacząca, a nie nadmiernie liczna), w którym jedna sztuka uległa uszkodzeniu, otrzyma się oszacowanie:

$$\mathbf{0,8528 \leq R(t) \leq 0,9958}$$

.To oszacowanie zostało wprowadzone do tablic 3 i 5 i wyróżnione drukiem pogrubionym, oraz przyjęte w tablicach 2 i 4. Z analizy tablicy 3 wynika, że przy pesymistycznym (ostrożnym) oszacowaniu $R(t)$ na poziomie dolnej granicy przedziału ufności, element o trwałości 20 000 h będzie miał nienaruszalność bezpieczeństwa na poziomie SIL1, zaś z tablicy 2 wynika, że elementy o trwałości mniejszej od 16000 h nie mogą być rozpatrywane jako elementy systemu związanego z bezpieczeństwem, gdyż ich nienaruszalność bezpieczeństwa będzie poniżej SIL1.

Elementy o gwarantowane liczbie cykli pracy 30 000 i większej mogą być uznane jako elementy do budowy systemów związanych z bezpieczeństwem.

4. POSTĘPOWANIE W SYTUACJI WYTWÓRCY

4.1. Wprowadzenie

W sytuacji wytwórcy wydaje się być korzystnym wykazanie możliwie wysokiego poziomu nienaruszalności bezpieczeństwa produkowanego elementu przy ponoszeniu rozsądnych nakładów na udowodnienie osiągniętego poziomu i jego ciągłe utrzymywanie. Zagadnieniem do rozstrzygnięcia jest wybór odpowiednich testów statystycznych.

4.2. Test przy nieznanej dystrybuancie uszkodzeń [6,7]

Plan testu i jego wyniki przedstawiono powyżej. Ten test, przy ograniczonej liczbowo próbce poddanej badaniom, nie umożliwia dokładniejszego oszacowania prawdopodobieństwa przepracowania deklarowanej liczby godzin, a więc i dokładniejszego oszacowania nienaruszalności bezpieczeństwa rozpatrywanego elementu. Chcąc uzyskać oszacowanie o niewielkim rozrzucie górnej i dolnej granicy ufności trzeba badać bardzo liczną próbkę 60 szt. i więcej, co jest drogie, zwłaszcza przy konieczności okresowego prowadzenia badań w celu wykazania stabilności produkcji.

Wydaje się, że korzystniejszym byłoby przejście na parametryczną metodę oceny niezawodności.

4.3. Identyfikacja dystrybuanty uszkodzeń

Podstawą posługiwania się parametryczną metodą oceny prawdopodobieństwa przepracowania deklarowanego czasu trwałości bez wystąpienia uszkodzenia jest zidentyfiko-

wanie dystrybuanty uszkodzeń. W statystycznej ocenie wyrobów stosuje się następujące modele teoretyczne rozkładu cech mierzalnych [6]::

- rozkład normalny (Gaussa),
- rozkład normalny ucięty,
- rozkład logarytmiczno-normalny,
- rozkład wykładniczy,
- rozkład Weibulla,
- rozkład gamma,
- rozkład potęgowy,
- rozkład uogólniony gamma

Ponadto stosowane są też modele :

- niecentralny.
- dwumianowy.

W praktyce oceny elementów napędowych autor zidentyfikował dystrybuantę uszkodzeń jednego rodzaj silników jako rozkład normalny ucięty [8], ponadto jeden z producentów przedstawił identyfikację dystrybuanty uszkodzeń jako rozkład Weibulla. Te dwa przypadki zostaną rozpatrzone poniżej, jako przykłady.

Warto wspomnieć, że próba pracy długotrwałej, konieczna przy wyznaczaniu deklarowanego czasu pracy bez uszkodzeń i identyfikacji dystrybuanty uszkodzeń, dostarcza konstruktorowi wielu innych informacji, między innymi pomocnych przy ulepszaniu konstrukcji i podwyższaniu nienaruszalności bezpieczeństwa [10].

4.4. Przykład analizy przy założeniu rozkładu normalnego uciętego

Zgodnie z zasadami podanymi w [6,7] obliczono prawdopodobieństwo przepracowania okresu 20 000 h na podstawie testu przeprowadzonego na próbce 25szt. (jak przy ocenie nieparametrycznej), w którym uszkodził się jeden egzemplarz po 16 000 h.

Otrzymano wynik:

$$R^*(t) = 0{,}9592$$

Ze wzoru (1) otrzymuje się teraz oszacowanie:

$$\lambda^* = 0{,}204 \times 10^{-5}$$

a więc SIL1

4.5. Przykład analizy przy założeniu rozkładu Weibulla

Zidentyfikowanie dystrybuanty uszkodzeń jako rozkładu Weibulla umożliwia wnioskowanie z badań mniej licznej próbki; zwykle przyjmuje się próbkę o liczności 10 szt. Niech trwałość gwarantowana elementu będzie, jak poprzednio, 20 000 h. Próbę prowadzono do uszkodzenia się 5-tego egzemplarza i otrzymano pary liczb zestawione w tablicy 7:

Tablica 7 – Zaobserwowane pary liczb

Numer próbki	K	1	2	3	4	5
Czas do uszkodzenia	h	16000	21000	24000	27000	30000

Po sporządzeniu wykresu na siatce funkcyjnej rozkładu Weibulla odczytano wartości:

- parametr kształtu – $\nu^* = 2,9$
- parametr skali – $b = 7,97 \times 10^4$

Obliczenia doprowadziły do oszacowań:

- wartość oczekiwana trwałości – $E(t) = 7,1 \times 10^4$ h,
- odchylenie standardowe - $\sigma^* = 2,63 \times 10^4$ h
- intensywność uszkodzeń odpowiadająca gwarantowanemu czasowi pracy 20 000 h:

$$\lambda^* = \mathbf{0,677 \times 10^{-5}}$$

co odpowiada SIL1.

Potwierdzenie poprzednich oszacowań otrzymano przy badaniu 10 szt. wyrobów, zamiast 25 szt., a więc przy znacznie niższych kosztach.

5. PODSUMOWANIE

Przedstawiono zagadnienia związane z oszacowaniem poziomu nienaruszalności bezpieczeństwa elementów scharakteryzowanych gwarantowanym czasem trwałości, które miałyby być zastosowane w systemach elektrycznych, elektronicznych, programowalnych elektronicznych związanych z bezpieczeństwem. Wykazano, że najniższe koszty przeprowadzenia odpowiednich testów można uzyskać, o ile dystrybuantę uszkodzeń elementu daje się przybliżyć rozkładem Weibulla.

LITERATURA

1. Dyrektywa Rady i Parlamentu 98/37/WE z dnia 22 czerwca 1998 r, w sprawie zbliżenia prawa państw członkowskich dotyczącego maszyn, zmieniona Dyrektywą Rady i Parlamentu 98/79/WE.
2. Dyrektywa Rady 89/655/EWG z dnia 30 listopada 1989 r. dotycząca minimalnych wymagań w dziedzinie bezpieczeństwa i higieny użytkowania sprzętu roboczego przez pracowników podczas pracy, zmieniona Dyrektywą Rady 95/63/WE i Dyrektywą Rady 2001/45/WE
3. PN-EN 61508-1: 2004, Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem. Część 1: Wymagania ogólne. (IEC 61508-1)
4. PN-EN 61508-4: 2004, Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem. Część 4: Definicje i skrótowce. (IEC 61508-4)
5. PN-EN 61508-6: 2003(U), Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem. Część 6: Wytyczne do stosowania IEC 61508-2 i IEC 61508-3 (IEC 61508-6)
6. Firkowicz S.: *Statystyczne badanie wyrobów*. Warszawa 1970. WNT
7. Missala T.: Ocena niezawodności silników elektrycznych do sprzętu powszechnego użytku. *Przegląd Elektrotechniczny*, t. LV, s. 253-256
8. Missala T.: Ocena nieznanej dystrybuanty teoretycznej uszkodzeń wybranych typów silników elektrycznych. *Krajowa Konferencja Automatyki 1980 r* .t. 1, s. 334-340 Szczecin.

9. Missala T.: Mechatronics elements in safety-related circuits. *5th International Conference MECHATRONICS 2004, Elektronika,* t. XVL, NR 8, S. 183-185.

10. Missala T.: Próba pracy długotrwałej jako narzędzie diagnostyki technicznej. *VII Krajowa Konferencja Naukowo-Techniczna Diagnostyka Procesów Przemysłowych 2005 r., Pomiary Automatyka Kontrola,* nr 9bis'2005, s. 321-323.