Dźwiarek Marek
Centralny Instytut Ochrony Pracy- Państwowy Instytut Badawczy, Warszawa, Polska

Hryniewicz Olgierd
Instytut Badań Systemowych PAN, Warszawa, Polska

Frequency of periodical inspections of safety-related control systems of machinery – practical recommendations for determining methods
Częstość okresowych kontroli dla związanych z bezpieczeństwem układów sterowania maszynami – praktyczne zalecenia sposobów wyznaczania

Keywords / Słowa kluczowe

safety of machinery, safety functions, functional safety, periodical inspections
bezpieczeństwo maszyn, funkcje bezpieczeństwa, bezpieczeństwo funkcjonalne, kontrole okresowe

Abstract

In preventing the accidents due to improper operation of the control systems the periodical inspection of their functioning is of crucial importance. Therefore, the control system designer should specify how often the system should undergo the periodical inspection. The paper presents some recommendations for the determination of periodical inspection frequency of safety related control systems in machinery. The recommendations are based on simple and easy to use mathematical models which have been developed by adaptation and simplification of models used for the determination of maintenance policies of complex systems. Practical implementation of the proposed recommendation is illustrated on some actual case studies.

1. Wprowadzenie

Analizy wypadków przy obsłudze maszyn przedstawione w [5] wykazały, że 36% z nich było spowodowanych przez niewłaściwe funkcjonowanie układu sterowania. Ponadto, w grupie wypadków spowodowanych przez niewłaściwe funkcjonowanie układu sterowania poważne wypadki zdarzały się znacznie częściej (41%) niż w wypadkach bez związku z układem sterowania (7%). Najczęstszą przyczyna takich wypadków był brak funkcji bezpieczeństwa (58%). Najczęściej brakowało takich funkcji jak monitorowanie położenia osłony czy obecności operatorów w strefie niebezpiecznej.
Inna grupa wypadków, to zdarzenia spowodowane niezadziałaniem związanego z bezpieczeństwem elementu układu sterowania w wyniku zbyt małej odporności na uszkodzenia (26% z wszystkich wypadków). Inne sygnalizowane przyczyny, tzn. błędy w definiowaniu funkcji bezpieczeństwa (4%), błędy w oprogramowaniu układu sterowania (6%), zbyt mała odporność na czynniki środowiskowe (czynniki klimatyczne, zaburzenia zasilania-6%), powodowały znacznie mniejszą liczbę zaistniałych wypadków. Wyniki te dowodzą, że układ sterowania maszyny jest bardzo ważny ze względu na bezpieczeństwo operatora maszyny.
Dlatego projektanci związanych z bezpieczeństwem układów sterowania maszynami powinni stosować rozwiązania, które poprawiają ich odporność na uszkodzenia, co w praktyce zwykle oznacza stosowanie niezawodnych układów oraz architektury redundantnej. Istotne znaczenie ma także okresowe sprawdzanie działania funkcji bezpieczeństwa. Dlatego projektant układu sterowania powinien określić jak często powinien on zostać poddany kontroli okresowej.

Niestety w obowiązujących normach nie ma zaleceń (wskazówek) odnośnie do sposobu wyznaczania częstotliwości okresowych kontroli układów sterowania. Problem ten był wielokrotnie dyskutowany na posiedzeniach grupy roboczej VG11 *Safety components* Europejskiej Koordynacji Jednostek Notyfikowanych w zakresie maszyn i elementów bezpieczeństwa (Dyrektywa Maszynowa 2006/42/WE), jednak dotychczas nie znaleziono satysfakcjonującego rozwiązania, dlatego jak dotychczas VG11 nie opracowało *Reccomendation for Use* dotyczącego prowadzenia kontroli okresowych elementów bezpieczeństwa w maszynach.

Problemy te skłoniły autorów do podjęcia prac mających na celu sformułowanie możliwie prostych zasad określania częstotliwości kontroli okresowych związanych z bezpieczeństwem elementów układów sterowania maszyn tak aby zapewnić odpowiednio wczesne wykrycie możliwych uszkodzeń.

W artykule zaprezentowane są wyniki tych prac. W Rozdziale 2 przedstawiono problem analizy funkcji bezpieczeństwa realizowanej przez układ sterowania maszyny. W szczególności podano wymagania niezawodności dla układów związanych z bezpieczeństwem zgodnie z normami międzynarodowymi. W Rozdziale 3 przedstawiono krótki przegląd wyników teoretycznych, które mogą być wykorzystane do poprawienia pewności działania układów sterowania przez zastosowanie kontroli okresowych. W drugiej części tego rozdziału zaprezentowano bardzo proste przybliżenia, które mogą być stosowane przez praktyków, którzy nie przeszli szkolenia w zakresie niezawodności, do planowania zasad kontroli. Ostatni rozdział artykułu poświęcono praktycznemu zastosowaniu zaproponowanych metod.

2. Funkcje bezpieczeństwa realizowane przez układy sterowania maszynami

Najczęściej układy sterowania maszyn realizują zarówno funkcje bezpieczeństwa, jak i te nie związane z bezpieczeństwem. Funkcja bezpieczeństwa to funkcja, której niewłaściwe zadziałanie może zwiększyć poziom ryzyka.

Ogólnie mówiąc, funkcja bezpieczeństwa może zostać zastosowana do redukcji poziomu ryzyka związanego z trzema następującymi grupami zagrożeń:

- zagrożenia spowodowane niewłaściwym działaniem maszyny,
- zagrożenia spowodowane zastosowaniem procesów technologicznych, których parametry fizyczne różnią się znacznie od standardowych warunków otoczenia,
- zagrożenia mechaniczne.

Najczęściej spotykane są następujące funkcje bezpieczeństwa to:

- związana z bezpieczeństwem funkcja zatrzymania uruchamiana przez urządzenie ochronne,
- ręczna funkcja resetowania,
- funkcja uruchomienia/powtórnego uruchomienia,
- funkcja lokalnego sterowania,
- zawieszenie wykonywania funkcji,
- monitorowanie wielkości związanych z bezpieczeństwem parametrów wejściowych,
- wymagany czas zadziałania; monitorowanie parametrów związanych z bezpieczeństwem, takich jak szybkość, temperatura czy ciśnienie,
- reakcja na zmiany, utratę i przywrócenie zasilania.

Ponieważ niezadziałanie tych funkcji może podnieść poziom ryzyka, projektanci związanych z bezpieczeństwem układów sterowania powinni stosować rozwiązania, które zwiększają ich odporność na uszkodzenia.

Z jednej strony odporność na uszkodzenia danego układu sterowania może być podniesiona poprzez obniżenie prawdopodobieństwa pojawienia się uszkodzenia, a z drugiej strony poprzez podjęcie środków mających na celu zapewnienie, że uszkodzenie, które może się pojawić nie będzie niebezpieczne. Taką poprawę możemy osiągnąć poprzez:

- zastosowanie niezawodnych "wypróbowanych" elementów oraz „wypróbowanych" zasad bezpieczeństwa,
- rozszerzenie struktury układu – na etapie projektowania bierze się pod uwagę dodatkowe podzespoły, które mają na celu wykrywanie uszkodzeń; najczęściej są to redundancje obwodów monitorujących pracę.

Podstawowe zasady poprawy odporności układu sterowania maszyny na uszkodzenia zostały podane w następujących normach scharakteryzowanych w pracach [6] i [7]:

- PN-EN 62061:2008 "Bezpieczeństwo maszyn. Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i programowalnych elektronicznych systemów sterowania związanych z bezpieczeństwem",
- PN-EN 138491-1:2008 "Bezpieczeństwo maszyn - Elementy systemów sterowania związane

z bezpieczeństwem - Część 1: Ogólne zasady projektowania".

W normie PN-EN 62061:2008 metodyka bezpieczeństwa funkcjonalnego sformułowana w PN-EN 61508 „Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych systemów związanych z bezpieczeństwem" z roku 2004 została zaadaptowana w sposób umożliwiający jej zastosowanie do układów sterowania maszynami.

Dla każdego związanego z bezpieczeństwem układu sterowania realizującego daną funkcję bezpieczeństwa w normie IEC 62061 podano probabilistyczne kryteria oceny ich odporności na uszkodzenia, nazwane Poziomem Nienaruszalności Bezpieczeństwa SIL (*Safety Integrity Level*). Te kryteria liczbowe przedstawiono w *Tabeli 1,* przy czym termin "uszkodzenie niebezpieczne" oznacza uszkodzenie tego elementu układu sterowania, który może spowodować zagrożenie lub stan niemożności realizacji funkcji.

Tabela 1. Poziomy Nienaruszalności Bezpieczeństwa oraz probabilistyczne kryteria dla funkcji bezpieczeństwa, która ma zostać wprowadzona do związanego z bezpieczeństwem układu sterowania

Poziom Nienaruszalności Bezpieczeństwa (SIL)	Prawdopodobieństwo wystąpienia uszkodzenia niebezpiecznego na godzinę
SIL 3	$[10^{-8}, 10^{-7})$
SIL 2	$[10^{-7}, 10^{-6})$
SIL 1	$[10^{-6}, 10^{-5})$

W normie ISO 13849-1 sformułowano uproszczoną metodę oceny układów sterowania maszyn. Następujące parametry charakteryzują każdy układ: struktura (kategoria), średni czas pracy do uszkodzenia (MTTF), pokrycie diagnostyczne (DC), współczynnik uszkodzeń o wspólnej przyczynie (CCF). Parametry te podzielono na następujące grupy jakościowe: *wysokie, średnie, niskie*.

Oczekiwany poziom zapewnienia bezpieczeństwa wyznacza się ze schematu, do którego wprowadzono szacunkowe parametry oraz strukturę układu (kanał pojedynczy, redundancja, monitorowanie, itd.). Pozwala to na ocenę projektowanego układu w stosunkowo prosty sposób. Poziom zapewnienia bezpieczeństwa (PL) odzwierciedla odporność układu na uszkodzenia. Zależność miedzy SIL a PL podana jest w *Tabeli 2*.

Według obu wyżej wymienionych norm projektant układu sterowania maszyny powinien, biorąc pod uwagę wyniki oceny ryzyka, określić wymagany SIL lub PL dla każdej funkcji bezpieczeństwa realizowanej przez ten układ sterowania. Wymagany

Tabela 2. Zależność między poziomem zapewnienia bezpieczeństwa PL a SIL

Poziom zapewnienia bezpieczeństwa (PL)	Prawdopodobieństwo uszkodzenia niebezpiecznego	Poziom nienaruszalności bezpieczeństwa (SIL)
a	$[10^{-5}, 10^{-4})$	Nie dotyczy
b	$[3x10^{-6}, 10^{-5})$	1
c	$[10^{-6}, 3x10^{-6})$	1
d	$[10^{-7}, 10^{-6})$	2
	$[10^{-8}, 10^{-7})$	3

SIL lub PL powinien zostać osiągnięty poprzez zastosowanie rozwiązań konstrukcyjnych odpowiednich dla projektowanego układu sterowania. Wymagany SIL lun PL powinien zostać utrzymany przez cały okres użytkowania maszyny.

Długotrwałe użytkowanie maszyny zwykle pociąga za sobą niszczenie jej podzespołów spowodowane pogorszeniem własności materiałowych i zużyciem mechanicznym. Zjawiska te mogą prowadzić do zmniejszenia uzyskanego SIL lub PL. Oznacza to, że wszystkie funkcje bezpieczeństwa powinny być okresowo sprawdzane w celu stwierdzenia jakichkolwiek zmian wartości parametrów, które mogą zmniejszyć zdolność układu sterowania do realizacji jego funkcji. Jednak, na obecnym etapie rozwoju normalizacji, nie ma zaleceń odnośnie częstotliwości z jaką te kontrole miałyby być przeprowadzane w odniesieniu do maszyn.

3. Kontrole okresowe układów

3.1. Optymalne przedziały kontroli

W wielu układach technicznych stan niezawodności (działanie lub uszkodzenie) nie może być zaobserwowany wprost, ale można go ocenić podczas monitorowania lub kontroli. Na przykład jeśli uszkodzenie układu nie ma charakteru destrukcyjnego, można je rozpoznać poprzez wykonanie kilku pomiarów lub obserwację jego działania.

Związane z bezpieczeństwem układy sterowania można uważać za kolejny przykład układów, których stanu nie można obserwować. Powinny one pracować prawidłowo „na żądanie" gdy układ główny ulegnie uszkodzeniu. Dlatego ich działania pomiędzy kolejnymi „żądaniami" zwykle nie są obserwowalne.

Innym przykładem układów, które wymagają monitorowania i kontrolowania są wielokanałowe układy redundantne. W pewnych przypadkach obserwujemy tylko wynik końcowy ich działania bez znajomości stanu poszczególnych kanałów. W układach związanych z bezpieczeństwem można

użyć specjalnych środków zapobiegających pogorszeniu ich działania jak np. automatyczne wykrywanie uszkodzeń. W przypadku większości układów związanych z bezpieczeństwem, także tych pracujących w małych i średnich przedsiębiorstwach, głównym mechanizmem poprawy ich niezawodności pozostają kontrole okresowe.

W późnych latach pięćdziesiątych i wczesnych sześćdziesiątych ubiegłego wieku problemem obliczania optymalnych przedziałów czasowych kontroli (monitorowania) zajmowało się wielu autorów. W przełomowej pracy Barlow et al. (1963) przedstawili pierwszy ogólny model wyznaczania optymalnych przedziałów czasowych kontroli. Od tego czasu wielu autorów zaproponowało nawet bardziej ogólne modele, gdzie optymalna kontrola stosowana była łącznie z naprawami okresowymi. Na przykład w ostatnich latach bardzo ważne wyniki zostały przedstawione w [2], [14], [15] oraz [17]. Książki [10] i [11] podają najważniejsze rezultaty osiągnięte w tej dziedzinie. Podsumowanie najnowszych wyników można znaleźć również w pracach [12] oraz [13].

Najbardziej ogólne modele matematyczne wyznaczania optymalnych zasad kontroli są, niestety, skomplikowane w stopniu znacznie ograniczającym możliwości ich zastosowania. Dlatego spotyka się je tylko w przypadkach rzeczywiście istotnych, takich jak np. układy bezpieczeństwa w elektrowniach atomowych czy szpitalach.

Pojawia się przeto potrzeba wykorzystania modeli uproszczonych, których mogą używać praktycy. Jeden z pierwszych takich modeli, oparty na prostej funkcji kosztów został zaproponowany przez Bakera (1990). Model ten został lekko zmodyfikowany i powtórnie zinterpretowany przez Vaurio (1994), który założył wykładniczy rozkład czasu do uszkodzenia charakteryzowany intensywnością uszkodzeń λ, oraz czasami napraw i kontroli oznaczonymi odpowiednio przez b i c. Optymalny przedział czasowy kontroli T0, który maksymalizuje gotowość (*availability*) można określić rozwiązując równanie:

$$(1+x_0)e^{-x_0} = 1-d\,, \tag{1}$$

gdzie: $x_0=\lambda T_0$, oraz

$$d = \frac{c}{\frac{1}{\lambda} - b}\,. \tag{2}$$

Najprostsze rozwiązanie przybliżone tego równania to

$$T_0 = \frac{1}{\lambda}\sqrt{2d}\,. \tag{3}$$

Bardziej dokładne rozwiązanie, prawdziwe dla warunku $d > 0{,}1$ zostało opracowane przez Vaurio (1994) w następującej postaci:

$$T_0 = \frac{1}{\lambda}\left\{-\frac{2}{3}\ln(1-d) + \sqrt{\frac{4}{9}\ln^2(1-d) - 2\ln(1-d)}\right\} \tag{4}$$

Kiedy używamy optymalnego przedziału czasowego kontroli, gotowość A można wyliczyć z formuły przybliżonej podanej w [15]:

$$A(T_0) = \frac{1-\lambda(b+c)}{1+\lambda T_0}\,. \tag{5}$$

W pracy [9] zaproponowano model przybliżony, prawdziwy dla uogólnionego rozkładu czasu użytkowania określonego przez jego wartość oczekiwaną τ. Autor tej pracy założył, że oczekiwany czas kontroli jest równy μ_0 i nie zależy od rzeczywistego stanu kontrolowanego układu. Ponadto założył możliwość fałszywych alarmów pojawiających się z prawdopodobieństwem α oraz znajomość oczekiwanej wartości μ_a czasu dodatkowego postoju, gdy zostanie wykryte rzeczywiste uszkodzenie, a także oczekiwanego czasu naprawy (wymiany) μ_r.

Dla tego modelu znaleziono oczekiwany czas pomiędzy kolejnymi wymianami T_r, rozumiany jako funkcja długości czasowego przedziału kontroli T, opisany zależnością

$$T_r = [A_1(T) + A_2]T + A_1(T)(\mu_0 + \alpha\mu_a) + A_2\mu_0 + \mu_r \tag{6}$$

gdzie $A_1(T)$ jest oczekiwaną liczbą kontroli przed uszkodzeniem, wyrażoną w postaci:

$$A_1(T) = \sum_{i=0}^{\infty} i\left[P(X < (i+1)T) - P(X < ih)\right] = \sum_{i=1}^{\infty} R(iT) \tag{7}$$

gdzie $R(ih)=1-F(ih)$, zaś A_2 jest oczekiwaną liczbą kontroli w czasie kiedy układ jest uszkodzony, zależną od prawdopodobieństwa nie znalezienia zaistniałego uszkodzenia, wyznaczaną ze wzoru

$$A_2 = \frac{1}{1-\beta}. \tag{8}$$

Optymalny przedział czasowy kontroli T_0 można znaleźć maksymalizując współczynnik gotowości dany zależnością

$$A(T) = \frac{\tau}{T_r(T)}. \tag{9}$$

Przybliżoną formułę reprezentującą podaną wyżej funkcję gotowości można znaleźć stosując następujące przybliżenie zaproponowane w [8]:

$$A_1(T) \approx \frac{\tau}{T} - 0.5, \tag{10}$$

prawdziwe gdy T jest znacząco mniejsze od τ. Gdy zastosujemy to przybliżenie do funkcji celu danej przez (9) otrzymamy

$$A(T) = \frac{\tau T}{W_1 T^2 + W_2 T + W_3}, \tag{11}$$

gdzie:

$$W_1 = A_2 - 0.5, \tag{12}$$

$$W_2 = \tau - 0.5\alpha\mu_a + \mu_r + (A_2 - 0.5)\mu_0, \tag{13}$$

$$W_3 = \tau(\alpha\mu_a + \mu_0). \tag{14}$$

Pochodna równania (11) względem T daje proste równanie na przybliżoną optymalną wartość T

$$-W_1 T^2 + W_3 = 0. \tag{15}$$

Dlatego, przybliżony optymalny przedział czasowy kontroli można zapisać w postaci prostego wyrażenia

$$T_0 = \sqrt{\tau \frac{\alpha\mu_a + \mu_0}{A_2 - 0.5}}. \tag{16}$$

W przypadku gdy kontrolowany układ związany z bezpieczeństwem składa się z dwóch podukładów (kanałów) połączonych równolegle możemy zastosować metody podane w [17]. Gdy oba podukłady opisane są tym samym wykładniczym rozkładem prawdopodobieństwa charakteryzowanym przez intensywność uszkodzeń λ, w pracy [17] zaproponowano znalezienie przedziału czasowego kontroli poprzez zapewnienie, że prawdopodobieństwo uszkodzenia układu nie jest większe od α. Wartość T można znaleźć rozwiązując następujące równanie:

$$R(T) = e^{-\lambda T}\left(2 - e^{-\lambda T}\right) = 1 - \alpha. \tag{17}$$

Funkcja gotowości jest w tym przypadku dana wzorem:

$$A(T) = \frac{2}{\lambda T}\left(1 - e^{-\lambda T}\right) - \frac{2}{2\lambda T}\left(1 - e^{-2\lambda T}\right). \tag{18}$$

Gdy $\lambda T << 1$ mamy w przybliżeniu:

$$A(T) \approx 1 - \frac{1}{2}\lambda^2 T^2, \tag{19}$$

a przedział czasowy kontroli można znaleźć stosując prostą formułę:

$$T_0 = \frac{1}{\lambda}\sqrt{2(1 - A_0)}, \tag{20}$$

gdzie A_0 jest wymaganą wartością gotowości układu.

3.2. Uproszczone algorytmy wyznaczania przedziałów czasowych kontroli

Pomimo ich prostoty, uproszczone metody zaprezentowane powyżej nie mogą być stosowane w praktyce przez większość użytkowników, którzy nie przeszli szkoleń z zakresu niezawodności. Jedynie czego oni potrzebują, to możliwie najprostszy sposób określenia zasad kontroli, które umożliwią związanym z bezpieczeństwem układom sterowania spełnienie wymagań międzynarodowych norm w zakresie bezpieczeństwa.

Jednak już od samego początku praktycy napotykają trudności, ponieważ normy te, takie jak np. PN-EN 13849-1, wyrażają wymagania niezawodności poprzez "prawdopodobieństwo uszkodzenia niebezpiecznego w ciągu godziny". Niestety pojęcie to nie zostało zdefiniowane w żadnej z tych norm. Są podstawy do przypuszczeń, że jest to wartość stałej intensywności uszkodzeń λ, która opisuje układ szeregowy, którego składowe reprezentowane są przez niezależne zmienne losowe o rozkładzie wykładniczym. Miara ta z pewnością jest niewłaściwa dla układów redundantnych, dla których intensywność uszkodzeń jest zawsze zmienna w czasie.

Ponadto, nie można jej użyć bezpośrednio do opisu układów związanych z bezpieczeństwem, które są kontrolowane okresowo aby zmniejszyć prawdopodobieństwo uszkodzenia kiedy układ ma

realizować funkcję bezpieczeństwa. Dlatego pojawiła się potrzeba zaproponowania prostej metody sprawdzenia, że zastosowane zasady kontroli pozwalają na spełnienie podanych w normach wymagań niezawodnościowych.

Rozważmy najprostszy przypadek, w którym kontrola pozwala na natychmiastowe sprawdzenie czy system jest gotowy do realizacji funkcji bezpieczeństwa czy nie. Założenie, że „prawdopodobieństwo wystąpienia uszkodzenia niebezpiecznego w ciągu godziny" pozostaje stałe przez cały okres użytkowania maszyny, przyjęte w normach ISO 13849-1 oraz IEC 62061 oznacza, że również gotowość układu nie powinna się zmieniać w każdym roku jej eksploatacji.

Gotowość układu, w przypadku gdy jego czas do pojawienia się uszkodzenia reprezentowany jest przez rozkład wykładniczy, można przedstawić przy pomocy prostego wzoru

$$A(T) = \frac{1}{\lambda T}\left(1 - e^{-\lambda T}\right). \qquad (21)$$

Jeśli $\lambda T << 1$, następujące przybliżenie jest prawdziwe

$$A(T) \approx 1 - \frac{1}{2}\lambda T + \frac{1}{6}(\lambda T)^2. \qquad (22)$$

Uwzględniając wartości PFHD podane w Tabeli 2 możemy określić wymaganą gotowość układu w ciągu roku A_r (patrz Tabela 3).

Tabela 3. Wymagana gotowość układu na rok dla poszczególnych SIL i PL

Poziom zapewnienia bezpieczeństwa(PL)	*Ar*	Poziom nienaruszalności bezpieczeństwa (SIL)
a	0,957	Nie dotyczy
b	0,987	1
c	0,997	1
d	0,99956	2
e	0,999956	3

Jeśli ustalimy wymaganą wartość gotowości A_r, to możemy znaleźć przedział czasowy kontroli T rozwiązując równanie $A(T) = A_r$. Stąd wartość tę można wyznaczyć z wyrażenia

$$A_r = 1 - \frac{1}{2}\lambda T + \frac{1}{6}(\lambda T)^2. \qquad (23)$$

A zatem wymagany przedział czasowy kontroli należy obliczyć z podanego niżej równania

$$T_0 = \frac{3 - 6\sqrt{0{,}25 - (2/3)(1 - A_r)}}{2\lambda} \approx \frac{2(1 - A_r)}{\lambda}. \qquad (24)$$

Gdy związany z bezpieczeństwem układ sterowania ma strukturę równoległą z dwoma kanałami opisanymi przez zmienne losowe o rozkładzie wykładniczym reprezentowane odpowiednio przez λ_1 i λ_2, możemy wtedy zastosować procedurę zaproponowaną w normie PN-EN 13849-1, Załącznik D. Procedura ta pozwala na przybliżone przedstawienie tego układu w postaci układu równoważnego, mającego dwa identyczne kanały reprezentowane przez intensywność uszkodzeń obliczoną z następującego równania

$$\frac{1}{\lambda} = \frac{2}{3}\left[\frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2}\right]. \qquad (25)$$

Następnie, możemy zastosować wyrażenie (20) do obliczenia przedziału czasowego kontroli. Wartość A_r można obliczyć używając tej samej metody co w poprzednim przypadku.

W przypadku gdy czasów trwania kontroli i napraw nie można pominąć, optymalna wartość przedziałów czasowych kontroli może być obliczona przy użyciu formuły (3) albo dokładnie używając wyrażenia (4) lub (16). Gotowości obliczone odpowiednio z wyrażeń (5) lub (11) są wartościami optymalnymi. Dlatego nie można ich poprawić poprzez zmianę przedziału czasowego kontroli.

W przypadku określonych wymagań niezawodności możemy tylko porównać je z wymaganą gotowością podaną w Tabeli 3. Oba modele optymalizacyjne mają jeden cel: maksymalizacja gotowości. Dlatego interesujące jest porównanie wyników dla tego samego zbioru parametrów.

Model zaproponowany w [9] jest bardziej ogólny więc, aby porównać go z modelem zaproponowanym w [15], musimy założyć, że kontrola jest idealna (α=β=0 i μ_a=0) Stąd optymalną wartość przedziału czasowego kontroli wylicza się z bardzo prostego wzoru przybliżonego:

$$T_0 = \sqrt{\frac{2\mu_0}{\lambda}}. \qquad (26)$$

W tym przypadku gotowość jest obliczana następująco:

$$A(T_0) = \frac{1}{\lambda}\frac{1}{T_0 + \tau_r}, \tag{27}$$

gdzie:

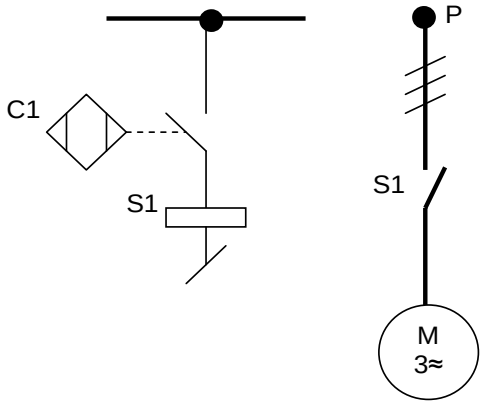
$$\tau_r = \frac{1}{\lambda} + \mu_R + \frac{\mu_0}{2}. \tag{28}$$

Porównamy teraz oba rozpatrywane modele na przykładzie liczbowym. Niech $\lambda = 0{,}001$ 1/h, $c=\mu_0$=1h, i $b=\mu_R$=50h. Optymalny przedział czasowy kontroli obliczony z wzoru (4) zgodnie z modelem Vaurio (1994) równy jest 45,9 h. Gotowość w tym przypadku, wyliczona z wzoru (5) wynosi 0,907. Jeśli teraz obliczymy optymalny przedział czasowy kontroli zgodnie z modelem podanym w pracy [9] otrzymamy jego wartość 44,5 h. Gotowość obliczona z wzoru (27) jest teraz równa 0,913. Zatem oba rozważne modele dają praktycznie te same wyniki.

4. Przykłady praktyczne

Zaprezentowana powyżej metoda wyznaczania częstotliwości kontroli związanych z bezpieczeństwem układów sterowania maszyn została zastosowana w praktyce do układów o różnym stopniu złożoności i różnych wymaganiach dotyczących ich odporności na uszkodzenia. Zwykle kontrole okresowe maszyn przeprowadzane są w czasie ich postoju i czas trwania takich kontroli jest pomijalny w porównaniu z czasem pracy maszyny. Zdarza się jednak że czas trwania kontroli nie może zostać pominięty, dlatego należy uwzględnić oba te przypadki.

4.1. Układ kategorii B



Rysunek 1. Przykładowy układ sterowania kategorii B.

Najprostsze układy kategorii B są stosowane w przypadku gdy poziom ryzyka spowodowanego zagrożeniem, które ma być obniżone jest bardzo niski. Typowym przypadkiem jest monitorowanie zamknięcia drzwi, za którymi wolno porusza się element niebezpieczny. W takim przypadku ocena ryzyka przeprowadzona zgodnie ze schematem A1 podanym w normie ISO 13849-1 daje wymagany poziom zapewnienia bezpieczeństwa PL_r równy b oraz $3x10^{-6} \le \lambda_r < 10^{-5}$.
Do monitorowania stanu zamknięcia zwykle używa się czujników zbliżeniowych. Przykładowy układ tego typu pokazano na *Rysunku 1*. Gdy osłona się otwiera, zasilanie silnika M jest odcinane przez stycznik S, sterowany przez czujnik zbliżeniowy C1. Czujnik ten jest klasycznym czujnikiem zbliżeniowym, dla którego MTTF wynosi 20 lat. W deklaracji producenta S1, zadeklarowano zdolność przełączania jako B_{10}S1= 10 000.
Ponieważ w rozpatrywanym przypadku drzwi dostępu do strefy niebezpiecznej mają być otwarte średnio raz na godzinę a maszyna pracuje 24 godziny na możemy wyznaczyć:

$$MTTF_d\ S1 = 11{,}41 \text{ lat} \tag{29}$$

Ostatecznie dla funkcji bezpieczeństwa mamy:

$$MTTF_d = 7{,}27 \text{ lat} \tag{30}$$

$$\lambda_d = \text{PFHD} = 1{,}57x10^{-5}$$

Jeśli układy kategorii B nie mają wbudowanych mechanizmów wykrywania uszkodzeń, a pojedyncze uszkodzenie powoduje utratę funkcji bezpieczeństwa konieczne jest przeprowadzanie ich okresowych kontroli. W takim przypadku kontrola polega na włączeniu funkcji bezpieczeństwa i sprawdzeniu czy zatrzymany został ruch niebezpieczny. Jak widać kontrola jest prosta i trwa krótko.
W tym przypadku stosujemy wzór (24). Zgodnie z równaniami (22) i (24) mamy:

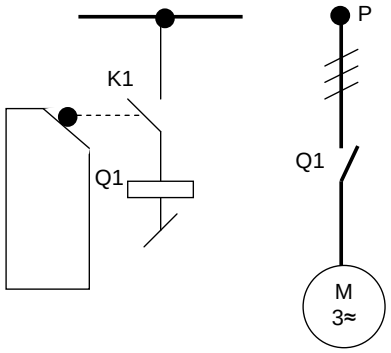
$$T_0 = \frac{2(1-0{,}987)}{1{,}57 \cdot 10^{-5}} = 1656h \approx 10 \text{ tygodni}. \tag{31}$$

4.2. Układ kategorii 1

Jeśli drzwi dostępu umieszczone są przy automatycznej linii produkcyjnej, otwiera się je bardzo rzadko, ale powstałe zagrożenia są znacznie większe. W tym przypadku poziom ochrony zapewniany przez układ kategorii B jest niewystarczający. Ocena ryzyka daje wymagany poziom zapewnienia bezpieczeństwa PL_r równe c oraz $10^{-6} \le \lambda_r < 3x10^{-6}$.
Można to osiągnąć przez zastosowanie urządzenia monitorującego zamknięcie drzwi, które spełnia wymagania kategorii 1. W takim przypadku należy

zastosować łącznik krańcowy wyprodukowany zgodnie z normą IEC 60947-5-1. Do zatrzymania silnika należy stosować stycznik spełniający wymagania podane w Tablicy 3 normy ISO 13849-2 dla elementów wypróbowanych.
W deklaracji producenta dla łącznika krańcowego określono B10 K1 = 10^6, natomiast dla stycznika zdeklarowano B10 Q1 = 1,3x10^6. Załóżmy, że linia produkcyjna pracuje dwadzieścia cztery godziny na dobę a dostęp do strefy niebezpiecznej powinien być możliwy raz w tygodniu. Dla takich warunków pracy zakładamy wartość minimalną λ_d określoną w normie ISO 13849-1dla układów kategorii 1:

$$\lambda_d = 1{,}14\text{x}10^{-6} \qquad (32)$$



Rysunek 2. Przykładowy układ sterowania kategorii 1.

Aby przeprowadzić kontrolę zautomatyzowanej linii produkcyjnej trzeba ją zatrzymać na całej długości. Zatrzymanie całej linii produkcyjnej a potem jej ponowne uruchamianie wymaga sporo czasu i pociąga za sobą konieczność zaangażowania specjalnego personelu nadzorującego co może zająć kilka godzin. Po zastosowaniu wzoru (26) mamy:

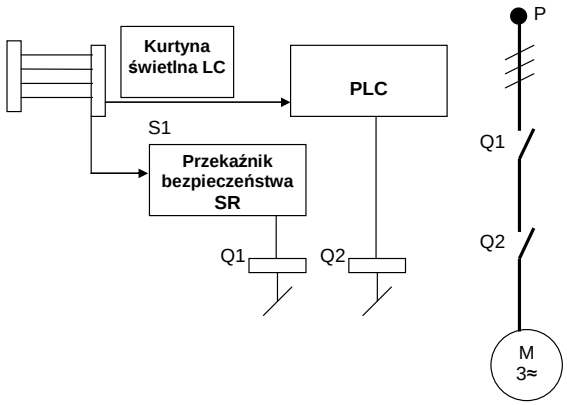
$$\mu_0 = 4\text{h}$$

$$T_0 = \sqrt{\frac{2\mu_0}{\lambda_d}} = 2649h \approx 3{,}7 \text{ miesiąca.} \qquad (33)$$

Co oznacza, że funkcja bezpieczeństwa powinna być sprawdzana przynajmniej raz na trzy miesiące.

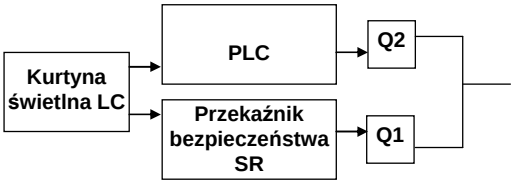
4.3 Układ kategorii 3

Innym przykładem jest układ, w którym do monitorowania dostępu do strefy niebezpiecznej automatu montażowego zastosowano kurtynę świetlną. W takim układzie pojawia się zagrożenie zranieniem odwracalnym, dostęp do strefy niebezpiecznej wymagany jest co minutę, a zagrożenia można łatwo uniknąć. Także w tym przypadku ocena ryzyka daje wymagany poziom zapewnienia bezpieczeństwa PL_r równy *c* oraz $10^6 \leq \lambda_r < 3\text{x } 10^{-6}$.
Z uwagi na wysoką częstotliwość przywołania funkcji bezpieczeństwa do jej realizacji przewidziano układ kategorii 3, pokazany na *Rysunku 3*. Kurtyna świetlna LC spełnia wymagania kategorii 4 PFHD LC = 5x10^{-7}. Sygnał z kurtyny przekazywany jest do klasycznego sterownika programowalnego (PLC), dlatego należy założyć MTTF PLC= 25 lat. PLC przełącza stycznik Q2, który odłącza silnik. Przekaźnik bezpieczeństwa SR stanowi kanał redundantny dla PLC i spełnia wymagania kategorii 4. W deklaracji producenta określono, że PFHD SR = 3x10^{-7}.



Rysunek 3. Przykładowy układ sterowania kategorii 3.

Sterownik przełącza stycznik Q1, który także odłącza silnik. W deklaracji producenta styczników Q1 i Q2 kreślono wartość parametru B10 Q1, Q2 = 10^6.



Rysunek 4. Schemat blokowy niezawodności dla funkcji bezpieczeństwa pokazanej na rysunku 3.

Schemat blokowy niezawodności funkcji bezpieczeństwa podano na *Rysunku 4.* Zakładając, że automat pracuje w systemie dwuzmianowym przez 220 dni w roku i uwzględniając częstość przywołań funkcji bezpieczeństwa otrzymujemy:

MTTF Q1, Q2 = 47,3 lat (34)

Możemy teraz określić wartości MTTF dla każdego kanału:

MTTF LC,PLC,Q2 = 15,89 lat, (35)
MTTF LC,SR, Q1 = 41,74 lat.

A po zastosowaniu symetryzacji (25) mamy:

$MTTF_m = 21,6$ lat, $\lambda_m = 1,32 \times 10^{-5}$ (36)

W podanym wyżej przypadku kontrola okresowa polega na uruchomieniu funkcji bezpieczeństwa i obserwacji sygnałów świetlnych generowanych przez kurtynę świetlną oraz sterowniki S1 i PLC. Częstotliwość kontroli okresowych można wyznaczyć stosując wzór (20)

$$T_0 = \frac{1}{1,32 \cdot 10^{-5}} \sqrt{2(1-0,997)} = 5868h \approx 1,5 \text{ roku} \quad (37)$$

5. Wnioski

Zarówno rozważania przedstawione powyżej jak i pokazane przykłady dowodzą, że problem oceny odporności na uszkodzenia jaką posiada układ sterowania można rozwiązać w stosunkowo prosty sposób. Obliczone okresy kontroli okresowych są zgodne z powszechnie stosowanymi zasadami ich przeprowadzania. Producenci maszyn i urządzeń ochronnych powinni wykonać takie obliczenia a wyniki zamieścić w Instrukcji Obsługi, zgodnie z wymaganiami Dyrektywy Maszynowej 2006/42/WE.

Informacja o pracy badawczej

Publikacja opracowana na podstawie wyników uzyskanych w ramach I etapu programu wieloletniego pn. „Poprawa bezpieczeństwa i warunków pracy" dofinansowanego w latach 2008-2010 w zakresie zadań służb państwowych przez Ministerstwo Pracy i Polityki Społecznej. Główny koordynator: Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy.

Literatura

[1] Badia, F.G., Berrade, M.D. & Campos, C.A. (2001). Optimization of inspection intervals based on costs. *Journal of Applied Probability*, 38, 872-881.

[2] Badia, F.G., Berrade, M.D. & Campos, C.A. (2002). Optimal inspection and preventive maintenance of units with revealed and unrevealed failures. *Reliability Engineering & System Safety*, 78, 157-163.

[3] Baker, M.J.C. (1990). How often should a machine be inspected?. *International Journal of Quality and Reliability Management*, 4 (4), 14-18.

[4] Barlow, R.E., Hunter, L.C & Proschan, F. (1963). Optimum checking procedures. *Journal of SIAM*, 11, 1078-1095.

[5] Dźwiarek, M. (2004). An analysis of Accident Caused by Improper Functioning of Machine Control Systems. *International Journal of Occupational Safety and Ergonomics*, Vol. 10 No. 2, 129-136.

[6] Dźwiarek, M. (2006). Assessment of software and hardware safety of programmable control systems of machinery. In: C. Guedes Soares & E. Zio (ed.) *Safety and Reliability for Managing Risk*, 2325-2330. Taylor & Francis Group, London, ISBN 978-0-415-42315-2.

[7] Dźwiarek, M. (2007). Functional safety of machinery control systems - general consideration. In: Kosmowski K. T. (ed.) *Functional Safety Management in Critical Systems*, 101-114. Fundacja Rozwoju Uniwersytetu Gdańskiego, ISBN 978-83-7531-006-1.

[8] Hryniewicz, O. (1992). Approximately optimal economic process control for a general class of control procedures. In: H.J. Lenz et al (Eds.) *Frontiers in Statistical Quality Control* IV: 201-215, Heidelberg, Physica Verlag.

[9] Hryniewicz, O.H. (2008). Optimal inspection intervals for maintainable equipment. In: Matorell S., Guedes Soares C., Barnett J. (Eds.): *Safety, Reliability and Risk Analysis. Theory, Methods and Applications* Vol.1, 581-586.

[10] Nakagawa, T. (2005). *Maintenance theory of reliability*. London, Springer.

[11] Nakagawa, T. (2008). *Advanced reliability models and maintenance policies*. London, Springer.

[12] Nakagawa, T. & Mizutani, S. (2009). A summary of maintenance policies for a finite interval. *Reliability Engineering and System Safety*, 94, 89-96.

[13] Nakagawa, T., Mizutani, S. & Chen, M. (2010). A summary of periodic and random inspection policies. *Reliability Engineering and System Safety*, 95, 906-911.

[14] Taghipour, S., Banjevic, D., Jardine & A.K.S. (2010). Periodic inspection optimization model for a complex repairable system|. *Reliability Engineering and System Safety*, 95, 944-952.

[15] Vaurio, J.K. (1994). A note on optimal inspection intervals. *International Journal of Quality and Reliability Management*, 11(6), 65-68.

[16] Vaurio, J.K. (1999). Availability and cost functions for periodically inspected preventively

maintained units. *Reliability Engineering & System Safety*, 63, 133 – 140.

[17] Zequeira, R.I. & Berenguer, Ch. (2005). On the inspection policy of a two-component parallel system with failure interaction. *Reliability Engineering and System Safety*, 88, 99-107.