# Wyznaczanie częstości kontroli okresowych urządzeń ochronnych

Marek Dźwiarek

## Wstęp

Analizy wypadków przy obsłudze maszyn przedstawione w [1] wykazały, że 36% z nich było spowodowanych przez niewłaściwe funkcjonowanie urządzeń ochronnych realizujących funkcje bezpieczeństwa. Ponadto w tej grupie wypadków poważne wypadki zdarzały się znacznie częściej (41%) niż w wypadkach bez związku z układem sterowania (7%). Najczęstszą przyczyną takich wypadków był brak lub obejście urządzenia ochronnego (58%) w wyniku działań operatora maszyny. Najczęściej brakowało takich funkcji, jak monitorowanie położenia osłony czy obecności operatorów w strefie niebezpiecznej. Inna grupa wypadków to zdarzenia spowodowane niezadziałaniem urządzenia ochronnego na skutek zbyt małej jego 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, jak istotne, ze względu na bezpieczeństwo operatora maszyny jest zapewnienie pewności realizacji funkcji bezpieczeństwa przez urządzenia ochronne. Dlatego projektanci urządzeń ochronnych 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 tych urządzeń. Dlatego projektant maszyny powinien określić, jak często zainstalowane na niej urządzenia ochronne powinny być poddawane kontroli okresowej. Niestety w obowiązujących normach nie ma zaleceń (wskazówek) odnośnie do sposobu wyznaczania częstotliwości okresowych kontroli urządzeń ochronnych. 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 jak dotychczas VG11 nie opracowała 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 urządzeń ochronnych tak, aby zapewnić odpowiednio wczesne wykrycie możliwych uszkodzeń. Wyniki tych prac zaprezentowane zostały w [4] i [5]. W artykule przedstawione są przykłady zastosowania tych zasad.

***Abstract:*** *The paper deals with the problem of choosing an appropriate inspection interval for monitoring of safety related control systems in machinery. Extremely simple approximate models have been proposed in order to provide practitioners without reliability training useful tools for the determination of inspection policies. These methods allow practitioners to design improved systems and procedures that will be able to fulfill requirements stated by international industry standards.*

## Funkcje bezpieczeństwa realizowane przez układy sterowania maszynami

Najczęściej układy sterowania realizują zarówno funkcje bezpieczeństwa, jak i te niezwiązane 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:

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

Najczęściej spotykane są następujące funkcje bezpieczeństwa:

- związana z bezpieczeństwem funkcja zatrzymania, uruchamiana przez urządzenie ochronne;
- ręczna funkcja resetowania;
- funkcja uruchomienia/powtórnego uruchomienia;
- funkcja lokalnego sterowania;
- zawieszenie wykonywania funkcji przez urządzenia ochronne;
- monitorowanie wielkości związanych z bezpieczeństwem parametrów wejściowych;
- 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, ich projektanci powinni stosować rozwiązania, które zwiększają odporność urządzeń ochronnych na uszkodzenia. Podstawowe zasady poprawy odporności urządzeń ochronnych na uszkodzenia zostały podane w następujących normach (patrz: [2] i [3]):

- PN-EN 62061:2008 „Bezpieczeństwo maszyn. Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych 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 61508:2004 „Bezpieczeństwo funkcjonalne elektrycznych (elektronicznych) programowalnych systemów związanych z bezpieczeństwem" została zaadaptowana w sposób umożliwiający jej zastosowanie do układów sterowania maszynami. Ocena odporności funkcji bezpieczeństwa na defekty dokonywana jest na podstawie kryteriów probabilistycznych, nazwanych Poziomami Nienaruszalności Bezpieczeństwa SIL.

W normie ISO 13849-1 sformułowano uproszczoną metodę oceny układów realizujących funkcje bezpieczeństwa. 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 poziomem zapewnienia bezpieczeństwa (PL) podana jest w tabeli 1.

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 urządzenia ochronne. Wymagany SIL lub PL powinien zostać osiągnięty poprzez zastosowanie rozwiązań konstrukcyjnych odpowiednich dla projektowanego układu sterowania. Wymagany SIL lub 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 wykrycia jakichkolwiek zmian wartości parametrów, które mogą zmniejszyć zdolność układu sterowania do realizacji jego funkcji.

## Uproszczone algorytmy wyznaczania przedziałów czasowych kontroli urządzeń ochronnych

Kwestie określania częstości kontroli okresowych systemów związanych z bezpieczeństwem analizowane były przede

wszystkim w aspekcie infrastruktury krytycznej w przemyśle procesowym. Wynikało to zarówno z wielkości występujących tam zagrożeń, jak i ze znacznych kosztów związanych z koniecznością zatrzymania procesu na czas kontroli, a także kosztów jej przeprowadzenia. W efekcie opracowano niezwykle złożone procedury określania częstości kontroli okresowych takich systemów. Procedury te są zbyt złożone i kosztowne, aby mogły być stosowane do kontroli okresowych urządzeń ochronnych stosowanych do maszyn. Wynika to przede wszystkim z ich złożoności matematycznej. Dlatego też znacznie bardziej przydatne są procedury uproszczone, opisane w [2] i [3].

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 dostępność układu nie powinna się zmieniać w każdym roku jej eksploatacji.

Dostępność układu w przypadku, gdy jego czas do pojawienia się uszkodzenia reprezentowany jest przez rozkład wykładniczy, można przedstawić przy pomocy prostej formuły:

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

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

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

Uwzględniając wartości PFHD podane w tabeli 1, możemy określić wymaganą dostępność układu na rok $A_r$ (patrz tabela 2).

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

$$A_r=1-\frac{1}{2}\lambda T+\frac{1}{6}(\lambda T)^2 \tag{3}$$

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

$$T_0=\frac{3-6\sqrt{0{,}25-(2/3)(1-A_r)}}{2\lambda}\approx\frac{2(1-A_r)}{\lambda} \tag{4}$$

Gdy związany z bezpieczeństwem układ sterowania ma strukturę równoległą z dwoma kanałami opisanymi przez zmienne losowe o rozkładzie wykładniczym reprezentowane odpowiednio przez $\lambda_1$ i $\lambda_2$, 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:

Tabela 1. Zależność między poziomem zapewnienia bezpieczeństwa PL a SIL

| Poziom zapewnienia bezpieczeństwa (PL) | Prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę | Poziom nienaruszalności bezpieczeństwa (SIL) |
|---|---|---|
| a | $[10^{-5}, 10^{-4})$ | Nie dotyczy |
| b | $[3\times10^{-6}, 10^{-5})$ | 1 |
| c | $[10^{-6}, 3\times10^{-6})$ | 1 |
| d | $[10^{-7}, 10^{-6})$ | 2 |
| | $[10^{-8}, 10^{-7})$ | 3 |

Tabela 2. Wymagana dostępność układu na rok dla poszczególnych SIL i PL

| Poziom zapewnienia bezpieczeństwa (PL) | $A_r$ | 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 |

$$\frac{1}{\lambda}=\frac{2}{3}\left[\frac{1}{\lambda_1}+\frac{1}{\lambda_2}-\frac{1}{\lambda_1+\lambda_2}\right] \tag{5}$$

Następnie możemy zastosować wyrażenie:

$$T_r=\frac{1}{\lambda}\sqrt{2(1-A_r)} \tag{6}$$

do obliczenia przedziału czasowego kontroli.

W przypadku, gdy czasów trwania kontroli i napraw nie można pominąć, optymalna wartość przedziałów czasowych kontroli może być obliczona przy użyciu formuły:

$$T_r=\sqrt{\frac{2\mu_0}{\lambda}} \tag{7}$$

gdzie $\mu_0$ oznacza czas przestoju maszyny w godzinach.

## Przykłady praktyczne

Zaprezentowana powyżej metoda wyznaczania częstotliwości kontroli urządzeń ochronnych stosowanych do 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.

## Urządzenie kategorii B

Najprostsze urządzenia 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 $PL_r$ równe *b* oraz $3 \times 10^{-6} \leq \lambda_r < 10^{-5}$.

Do monitorowania stanu zamknięcia zwykle używa się czujników zbliżeniowych. Przykład takiego urządzenia 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 jego 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 dobę możemy wyznaczyć:

$$MTTF_d S1 = 11{,}41 roku \tag{8}$$

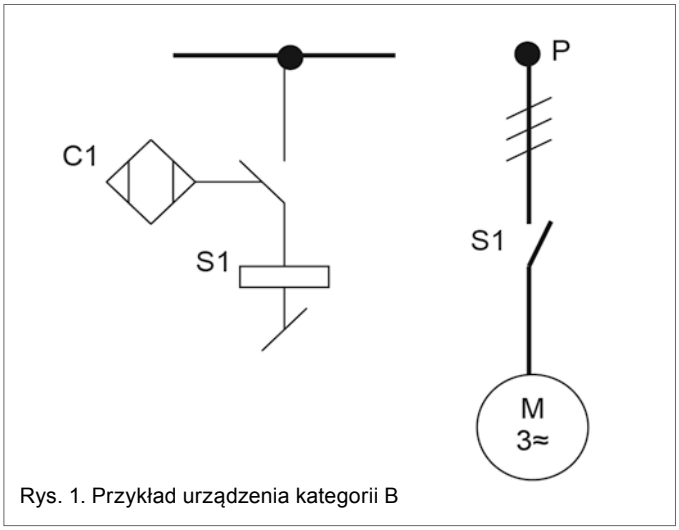
Ostatecznie dla funkcji bezpieczeństwa mamy:

$$\begin{aligned} MTTF_d &= 7{,}27 roku \\ \lambda_d &= PFHD = 1{,}57 \cdot 10^{-5} \end{aligned} \tag{9}$$

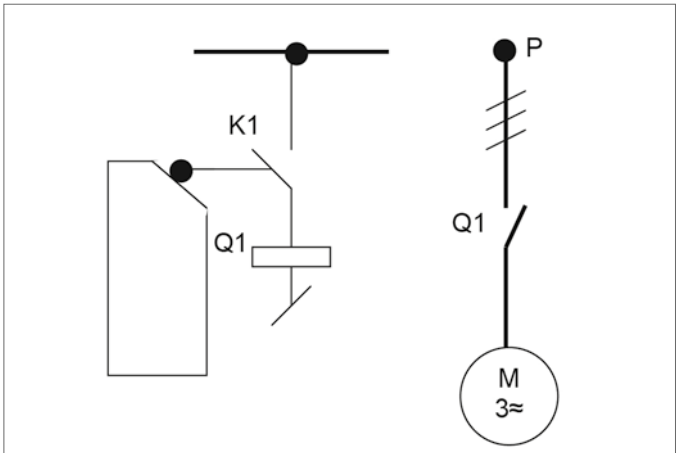
Ponieważ układy kategorii B nie mają wbudowanych mechanizmów wykrywania uszkodzeń, a pojedyncze uszkodzenie powoduje utratę funkcji bezpieczeństwa, konieczne jest przeprowadzanie ich okresowych kontroli. W takim przypadku kontrola polega na włączeniu funkcji bezpieczeństwa i sprawdzeniu, czy zatrzymany został ruch niebezpieczny. Jak widać, kontrola jest prosta i trwa krótko.

W tym przypadku stosujemy wzór (4):

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



Rys. 1. Przykład urządzenia kategorii B



Rys. 2. Przykład urządzenia kategorii 1

## Urządzenie 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 urządzenie kategorii B jest niewystarczający. Ocena ryzyka daje wymagany poziom zapewnienia bezpieczeństwa $PL_r$ równe *c* oraz $10^{-6} \leq \lambda_r < 3 \times 10^{-6}$.

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, Załącznik K. 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 $B_{10}$ K1 = $10^6$, natomiast dla stycznika zdeklarowano $B_{10}$ Q1 = $1{,}3 \times 10^6$.

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 $\lambda_d$, określoną w normie ISO 13849-1 dla układów kategorii 1:

$$\lambda_d = 1{,}14 \cdot 10^{-6} \tag{11}$$

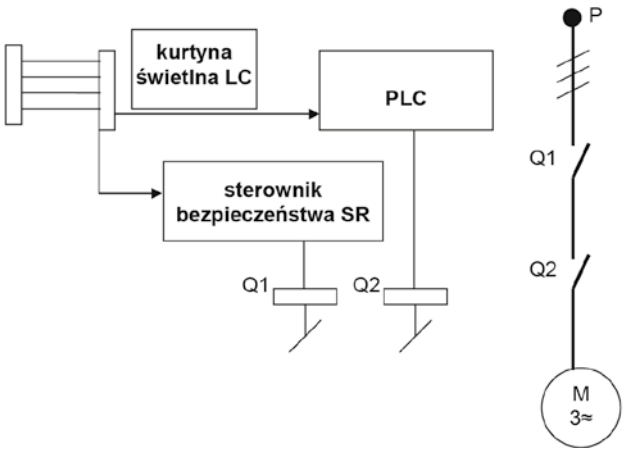
Aby przeprowadzić kontrolę zautomatyzowanej linii produkcyjnej, trzeba ją zatrzymać na całej długości. Zatrzymanie całej linii produkcyjnej, a potem jej ponowne uruchamianie, wymaga sporo czasu i pociąga za sobą konieczność zaangażowania specjalnego personelu nadzorującego, co może zająć kilka godzin.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

$$\begin{aligned} \mu_0 &= 4h \\ T_0 &= \sqrt{\frac{2\mu_0}{\lambda_d}} = 2649h \approx 3{,}7 \text{ miesiąca.} \end{aligned} \tag{12}$$

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

## Urządzenie kategorii 3

Innym przykładem jest urządzenie, w którym do monitorowania dostępu do strefy niebezpiecznej automatu montażowego zastosowano kurtynę świetlną. W takim urządzeniu poja-




Rys. 3. Przykład urządzenia kategorii 3

wia 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 $10^{-6} \leq \lambda_r < 3 \times 10^{-6}$.

Z uwagi na wysoką częstość przywołania funkcji bezpieczeństwa do jej realizacji przewidziano układ kategorii 3, pokazany na rys. 3. Kurtyna świetlna LC spełnia wymagania kategorii 4 i PFHD LC = $5 \times 10^{-7}$. Sygnał z kurtyny przekazywany jest do klasycznego sterownika programowalnego (PLC), dlatego na-


Rys. 4. Schemat blokowy niezawodności funkcji bezpieczeństwa pokazanej na rys. 3

leży założyć MTTF PLC = 25 lat. PLC przełącza stycznik Q2, który odłącza silnik. Sterownik bezpieczeństwa SR stanowi kanał redundantny dla PLC i spełnia wymagania kategorii 4. W deklaracji producenta określono, że PFHD SR = $3 \times 10^{-7}$.

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

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:

$$MTTF\ Q1,Q2 = 47{,}3lat \tag{13}$$

Możemy teraz określić wartości MTTF dla każdego kanału:

$$MTTF\ LC, PLC, Q2 = 15{,}89lat$$
$$MTTF\ LC, SR, Q1 = 41{,}74lat \quad (14)$$

A po zastosowaniu symetryzacji (5) mamy:

$$MTTF_m = 21{,}6lat, \lambda_m = 1{,}32 \cdot 10^{-5} \quad (15)$$

W podanym wyżej przypadku kontrola okresowa polega na uruchomieniu funkcji bezpieczeństwa i obserwacji sygnałów świetlnych generowanych przez kurtynę świetlną oraz sterowniki S1 i PLC. Częstość kontroli okresowych można wyznaczyć, stosując wzór (6):

$$T_0 = \frac{1}{1{,}32 \bullet 10^{-5}} \sqrt{2(1-0{,}997)} = 5868h \approx 1{,}5roku \quad (16)$$

## Wnioski

Zarówno rozważania przedstawione powyżej, jak i pokazane przykłady dowodzą, że problem oceny odporności na uszkodzenia urządzeń ochronnych 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.

Publikacja przygotowana na podstawie wyników badań prowadzonych w ramach II etapu programu wieloletniego pn. „Poprawa bezpieczeństwa i warunków pracy", dofinansowanego w latach 2011–2013 w zakresie projektów badawczych rozwojowych przez Ministerstwo Nauki i Szkolnictwa Wyższego. Główny koordynator: Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy.

## Literatura

[1] 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.

[2] 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.

[3] 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.

[4] Dźwiarek M., Hryniewicz O.: (2011). *Periodical inspection frequency of safety related control systems of machinery – practical recommendations for the determination*. In: *Advances in Safety, Reliability and Risk Management. Berenguer, Grall & Guedes Soares (eds.)* © Taylor & Francis Group, London, ISBN 978-0-415-68379-1, p. 495–502.

[5] Dźwiarek M., Hryniewicz O.: (2011). *Praktyczny przykład określania częstości kontroli okresowych urządzeń ochronnych stosowanych do maszyn*. W: *Innowacyjne techniki i technologie dla górnictwa. Bezpieczeństwo – Efektywność – Niezawodność.* Klich A., Kozieł A. (ed)., 161–177.

dr inż. Dźwiarek Marek – p.o. kierownika Zakładu Techniki Bezpieczeństwa w Centralnym Instytucie Ochrony Pracy – Państwowym Instytucie Badawczym, specjalizuje się w problematyce urządzeń ochronnych stosowanych do maszyn, bezpieczeństwa funkcjonalnego systemów sterowania maszynami, oceny ryzyka, interfejsów człowiek – maszyna. Jest przewodniczącym Komitetu Technicznego 281 „Bezpieczeństwo Maszyn. Aspekt Elektrotechniczny", członkiem grupy roboczej ISO/TC 199/JWG 8 „Safe control systems", Komitetu Technicznego IEC 44 „Safety of Machinery. Electrotechnical Aspects", Komitetu Horyzontalnego „Co-ordination of Notified Bodies – Machinery" i grup roboczych VG11 „Safety components"; tel. 22-623 46 35, e-mail: madzw@ciop.pl.