ELEMENTY NIEZAWODNOŚCI UKŁADÓW STEROWANIA BEZPIECZEŃSTWEM MASZYN

THE UNITS OF THE RELIABILITY OF THE ARRANGEMENTS OF CONTROL SYSTEMS THE SAFETY OF MACHINES

Marek Trajdos - Partner Serwis Sp. z o.o., „Klub Paragraf 34" SBT, Łódź

W pracy omówiono wybrane zagadnienia z zakresu obliczeń niezawodnościowych części układu sterowania związanego z bezpieczeństwem w oparciu o normy: PN-EN 60508, PN-EN 62061 i PN-EN ISO 13849-1. Podkreślono również znaczenie określania niezawodności systemów bezpieczeństwa w celu realizacji projektów właściwych w punktu widzenia zasadniczych i minimalnych wymagań bezpieczeństwa w odniesieniu do maszyn w Unii Europejskiej. W rozważaniach wykorzystano techniki zawarte w wymienionych wyżej normach zharmonizowanych i wykorzystanie zasady domniemania zgodności dla maszyn objętych obowiązkiem oznaczania CE.

Chosen questions talked over in the work from range of calculations reliability of piece of arrangement of control systems connected with the safety in the support about standards: EN 60508, EN 62061 and EN ISO 13849-1. The meaning of defining the reliability of the systems of the safety in the aim of the realization of proper projects in the point of the sight of the principal and minimum requirements of the safety in the reference to machine engines in European Union (EOG) was also underlined.

Wprowadzenie

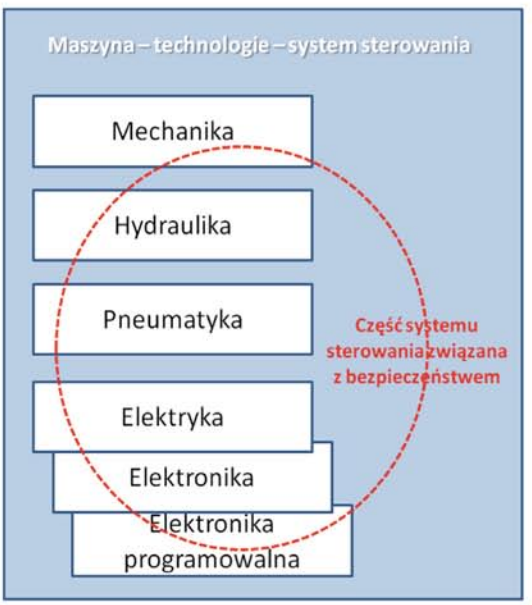
W ogólnym przypadku maszyna może być skonstruowana jako system składający się z podsystemów wykonanych w różnych technologiach. Tak jak to pokazano na rysunku 1. Należą do nich: mechanika (osłona, element uruchamiający pozycyjnego wyłącznika bezpieczeństwa), hydraulika (siłownik, zawór bezpieczeństwa), pneumatyka (siłownik, zawór trójdrożny), elektryka (stycznik, przycisk stopu awaryjnego), elektronika (kurtyna świetlna) i oprogramowanie (określane jako elektronika programowalna – np. programowalny przekaźnik bezpieczeństwa, skaner laserowy, przekształtnik z zaimplementowaną funkcją bezpieczeństwa). Zagadnienia niniejsze omówiono w publikacji [2].

Wszystkie układy maszyny we współczesnych konstrukcjach są z reguły sterowane i tę część systemu określa się zatem jako system sterowania (CS). Oczywiście system sterowania maszyny pełni przede wszystkim funkcje technologiczne, a jedynie jego wyspecjalizowana część realizuje określone funkcje bezpieczeństwa tworząc tym samym tak zwaną „część systemu sterowania związaną z bezpieczeństwem" (SRP/CS) przenikającą w ogólnym wypadku wszystkie systemy maszyny. Posiada on z reguły część elektryczną (SRECS), na której koncentruje się norma PN-EN 62061. Natomiast wszystkich technologii dotyczy norma PN-EN ISO 13849-1 (rys. 2). Wyżej wymienione normy pozwalają na projektowanie systemu sterowania bezpieczeństwem maszyny zgodnie z zasadniczymi wymaganiami bezpieczeństwa, a zatem w przypadku maszyn wprowadzanych do obrotu po raz pierwszy oraz „głębokiej" modernizacji maszyn użytkowanych.

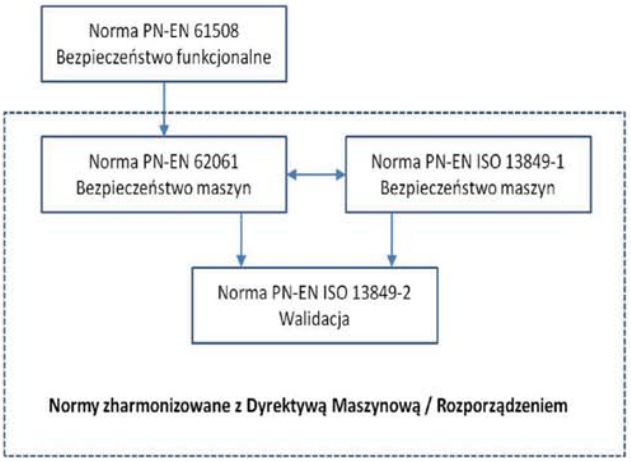
Jak wspomniano wyżej istnieje znacząca różnica, co do zakresu stosowalności wymienionych norm ze względu na technologię, w której projektowany jest system. Drugą, zasadniczą różnicą jest wskazanie na stosowanie normy PN-EN ISO 13849-1 do projektowania układów o niskim stopniu złożoności, a normy PN-EN 62061 do systemów o wysokim stopniu złożoności. Przy czym przez system o niskim stopniu złożoności rozumieć należy taki, którego wszystkie możliwe stany pracy mogą być przewidziane i opisane.

Podstawę konstrukcji normy PN-EN 62061 (zharmonizowanej z Dyrektywą Maszynową [6]) stanowi norma PN-EN 61508 opisująca ogólne zasady bezpieczeństwa funkcjonalnego, z których po dokonaniu pewnych praktycznych uproszczeń skonstruowano normę odnoszącą się do bezpieczeństwa maszyn.

Proces projektowania, który rozpoczyna się oceną ryzyka, powinien kończyć się sprawdzeniem praktycznego spełnienia



Rys. 1. Część systemu sterowania maszyny związana w bezpieczeństwem na tle technologii (branż) występujących w maszynach



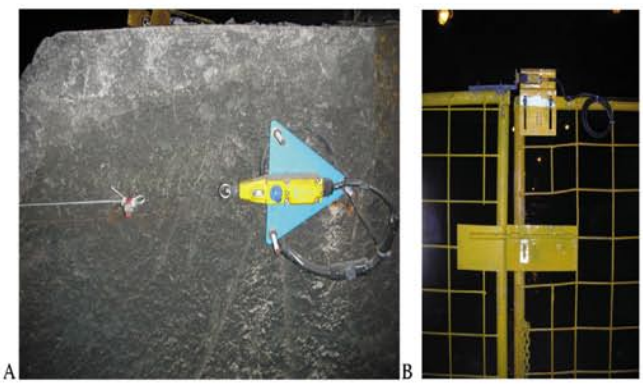
Rys. 2. Układ podstawowych norm wspierających projektowanie części układów sterowania związanych z bezpieczeństwem zgodnie z wymaganiami zasadniczymi bezpieczeństwa w odniesieniu do maszyn.

Rys. 3. Relacja pomiędzy poziomami zapewnienia bezpieczeństwa (PL), a poziomami nienaruszalności bezpieczeństwa (SIL) w odniesieniu do wartości PFHd (średniego prawdopodobieństwa niebezpiecznego uszkodzenia na godzinę).

wymagań zwanym walidacją. Zasady walidacji omawia druga część normy PN-EN ISO 13849-2, która może być stosowana we współpracy z obydwoma systemami normatywnymi. Są one zresztą spójne i w innym, bardzo ważnym punkcie: ponieważ w praktyce spotyka się mieszane technologie realizacji systemu bezpieczeństwa maszyny obie normy można wykorzystywać wspólnie. Niniejsze stwierdzenie wynika z faktu, że zgodnie z normą PN-EN 62061 system może być dzielony na podsystemy, dla których określa się poziom nienaruszalności bezpieczeństwa (SIL), a między poziomem SIL (którym posługuje się norma PN-EN 62061) i poziomem nienaruszalności bezpieczeństwa (PL) należącym do zasadniczych pojęć normy PN-EN ISO 13849-1 istnieje ścisły związek matematyczny (rys. 3). Relacja pomiędzy SIL i PL jest określona przedziałami wartości średniego prawdopodobieństwa niebezpiecznego uszkodzenia na godzinę (PFHd) podsystemu realizującego daną funkcję bezpieczeństwa. Zatem, możliwe jest zaprojektowanie podsystemu z danym PL, przeliczenie go na SIL, a następnie potraktowanie jako podsystemu składowego części systemu sterowania związanego z bezpieczeństwem.

Czujnik jako podsystem – elementy analizy

Jednymi z najczęściej spotykanych czujników aktywujących system realizujący daną funkcję bezpieczeństwa są elektromechaniczne wyłączniki pozycyjne linkowe (rys. 4A) lub współpracujące z osłonami (rys. 4B). W przypadku aplikacji pokazanych na rysunku 4, mamy do czynienia z bardzo typowym zastosowaniem zapewniającym ograniczenie dostępu pracowników do stref zagrożenia. Pokazane czujniki mają najczęściej podwójny (redundantny) układ elektryczny (styki przekaźnikowe z wymuszonym prowadzeniem) , lecz pojedynczy układ mechaniczny (element uruchamiający), tak jak to pokazano na rysunku 5A. Pełna redundancja zachodziłaby w przypadku, gdyby zastosowano dwa niezależne wyłączniki, każdy z pojedynczym stykiem w układzie uwidocznionym na rvsunku 5B.



Rys. 4. Przykłady zastosowania elementów inicjujących części systemu sterowania związanego z bezpieczeństwem w obszarze górnictwa podziemnego; A – wyłącznik linkowy (tu zastosowany do obsługi bariery poprzecznej w chodniku), B – wyłącznik pozycyjny stykowy współpracujący z osłoną ruchomą

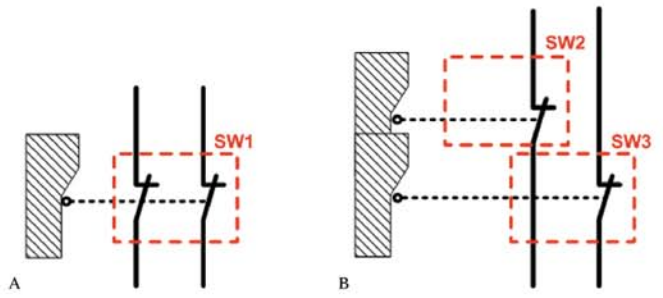
Powstaje pytanie: jakie znaczenie dla projektowanego układu bezpieczeństwa ma zastosowanie każdego w dwóch możliwych rozwiązań konstrukcyjnych: pojedynczego wyłącznika pozycyjnego z jednym mechanicznym elementem uruchamiającym i dwoma stykami elektrycznymi oraz dwóch niezależnych wyłączników z jednym stykiem elektrycznym każdy?

Należy rozważyć dwa niezależne aspekty: możliwość wprowadzenia przez pracownika kończyny górnej do strefy niebezpiecznej w wyniku uchylenia osłony oraz niezawodność zastosowanego rozwiązania.

W pierwszym przypadku, oczywiste jest, że zastosowanie pojedynczego wyłącznika i osłony o niewystarczającej sztywności będzie prowadzić do sytuacji, w której nie zostanie spełnione jedno z wymagań zasadniczych [6].

Odpowiedź na pytanie w drugim przypadku wymaga wykonania porównawczych obliczeń niezawodnościowych. Ponieważ układy przedstawione na rysunku 5 są elektromechaniczne, nie można się w tym przypadku posłużyć normą PN-EN 62061. Dlatego zostanie określony poziom zapewnienia bezpieczeństwa (PL) wg normy PN-EN ISO 13849-1 dla podsystemu, którym jest zarówno wyłącznik SW1 z redundantnymi stykami (rys. 5A), jak i układ wyłączników SW2 i SW3 z pojedynczymi stykami.

Aby dokonać obliczeń należy przekształcić schematy z rysunku 5 w odpowiadające im schematy blokowe, widoczne na rysunku 6. Do obliczeń potrzebne są również znane wzory zamieszczone zarówno w normie [7], jak i w pracach [1] i [3]. Poza wzorami, konieczna jest znajomość wartości niezawodnościowych poszczególnych elementów składowych oraz przewidywanej rocznej częstości użycia opisywanych elemen-



Rys. 5. Uproszczone schematy wyłączników pozycyjnych: A – z dwoma stykami typu NC, B – z jednym stykiem typu NC

tów elektromechanicznych. Przy czym częstość ta może być wynikiem pozyskania informacji od Klienta/Użytkownika lub uczynienia określonych założeń projektowych na bazie wcześniejszych doświadczeń. Pierwsza w metod z reguły sprawdza się w projektach jednostkowych, a druga w powtarzalnych (seryjnych).

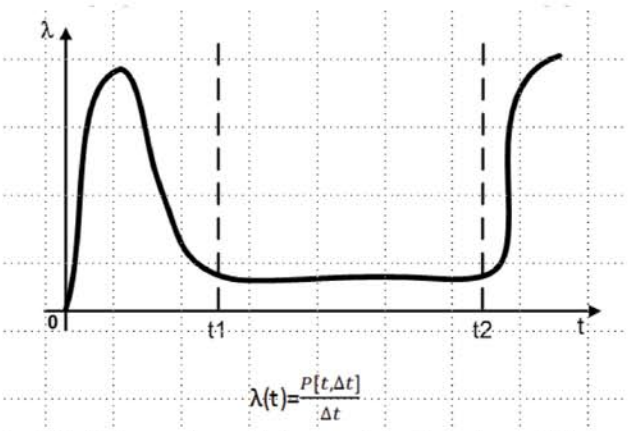
Na rysunku 6A widać wyraźnie, że awaria jednego (tu jedynego) elementu uruchamiającego może prowadzić (w wypadku zajścia tzw. uszkodzenia niebezpiecznego do utraty funkcji bezpieczeństwa całego podsystemu, natomiast w układzie pokazanym na rysunku 6B, utrata funkcji może wynikać jedynie z jednoczesnej awarii dwóch elementów uruchamiających. Zatem układ B ma wyraźną przewagę niezawodnościową, nad układem A. Tego typu rozważania jakościowe (poparte odpowiednimi obliczeniami ilościowymi – [1, 2]) stanowią podstawę projektowania systemów bezpieczeństwa dla maszyn.

Diagnostyka w układzie przekaźnika bezpieczeństwa – zagadnienia wybrane

Na rysunku 7 pokazano wykres i wzór opisujący intensywność uszkodzeń każdego elementu lub podsystemu. Przedział czasu od t_1 do t_2 jest nazywany – przedziałem właściwej eksploatacji i charakteryzuje go mniej więcej stała wartość funkcji intensywności uszkodzeń w czasie. Dla tego przedziału jest definiowana zasada projektowania układów bezpieczeństwa maszyn zarówno według normy PN-EN ISO 13849-1, jak i PN-EN 62061.

Zależność pomiędzy intensywnością uszkodzeń, a opisanym wcześniej (rys. 3) średnim prawdopodobieństwem niebezpiecznego uszkodzenia na godzinę, jest dana następującym wzorem:

$$PFH_d = \lambda_{DD} \times 1h$$



Rys. 7. Postać typowa krzywej intensywności uszkodzeń oraz definicja intensywności

Przekaźniki bezpieczeństwa są konstruowane w architekturze dwukanałowej typu „D" ([10], rys. 8). Przy czym w zależności od modelu lub producenta przekaźnika bezpieczeństwa widoczna na rysunku struktura dwukanałowa może być złożona z elementów (1 i 2) identycznych lub celowo zróżnicowanych. Różnicowanie elementów wpływa na odporność na uszkodzenia spowodowane wspólną przyczyną, lecz z reguły całkowicie tego wpływu nie eliminuje. Niezawodność takiego podsystemu w przypadku zastosowania elementów o takiej samej konstrukcji w obu kanałach opisuje wzór:

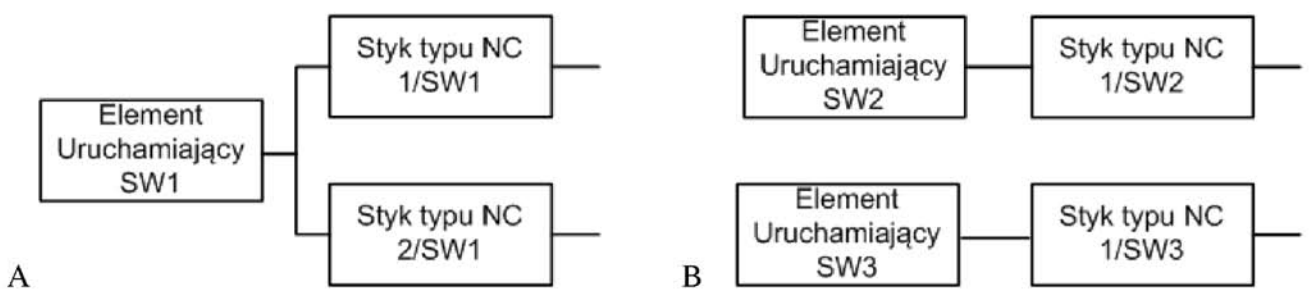
$$\lambda_{DD} = (1-\beta)^2\{[\lambda_D^2 \times 2 \times DC] \times T_2/2 + [\lambda_D^2 \times (1-DC)] \times T_1\} + \beta \times \lambda_D$$

Przy czym, jak wspomniano wyżej: $PFH_d = \lambda_{DD} \times 1h$.

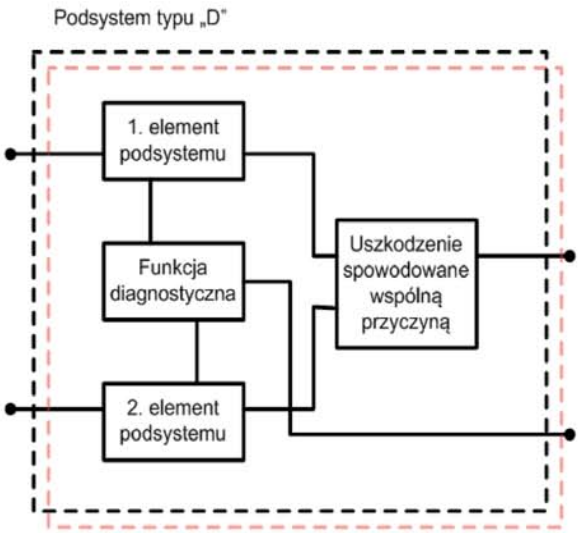
gdzie:
- λ_D jest częstością niebezpiecznych uszkodzeń kanału 1 lub 2 podsystemu
- T_1 jest odstępem miedzy testami okresowymi lub czasem życia w zależności, która z tych wartości jest mniejsza
- T_2 jest odstępem między testami okresowymi diagnostycznymi

Korzystając z powyższych wzorów, można obliczyć wartość współczynnika PFH_d [5], a co za tym idzie określić przynależność danego podsystemu do przedziału reprezentującego pewien poziom zapewnienia bezpieczeństwa.

Na szczególną uwagę zasługuje fakt, że w przypadku architektury „D" poza redundancją elementów, wprowadza się dodatkowo niezależną diagnostykę tych elementów, co podnosi (zgodnie z przytoczonym wyżej wzorem) niezawodność funkcji bezpieczeństwa.



Rys. 6. Schemat blokowy wyłączników pozycyjnych: A – jednego wyłącznika z dwoma stykami typu NC, B – układu dwóch wyłączników z jednym stykiem typu NC każdy



Rys. 8. Schemat ogólny podsystemu typu „D" wg [10]

Niestety uszkodzeń spowodowanych wspólna przyczyną nie da się całkowicie wyeliminować, co również wynika ze schematu na rysunku 7.

Podsumowanie

Powyższe rozważania pokazują główne idee projektowania części systemów sterowania związanych z bezpieczeństwem maszyn, wskazują na konieczność wykonania określonych czynności projektowych w celu spełnienia wymagań prawnych dla maszyn wprowadzanych do obrotu na wspólnym, europejskim obszarze gospodarczym zgodnie z wymaganiami prawa. Bez uwzględnienia powyższych idei nie ma mowy o wyeliminowaniu odpowiedzialności prawnej, w przypadku stwierdzenia przez uprawniony organ nadzoru rynku lub badania powypadkowe niezgodności z zasadniczymi wymaganiami [6].

Należy przy tym podkreślić, że zarówno model postępowania przedstawiony w normie PN-EN ISO 13849-1, jak i w normie PN-EN 62061 pozwala na spełnienie wymagań, przy czym można te modele wykorzystywać zamiennie w ramach projektowania jednego systemu, dzięki dekompozycji na podsystemy, z uwzględnieniem ograniczeń każdej w metod.

Literatura

[1] M. Trajdos „Wprowadzenie do projektowania bezpiecznych systemów sterowania maszyn" Materiały II Międzynarodowej Konferencji – Problemy bezpieczeństwa w budowie i eksploatacji maszyn i urządzeń górnictwa podziemnego, CBiDGP Ustroń 2010

[2] M. Trajdos, T. Guzewski, „Wybrane funkcje bezpieczeństwa systemów sterowania – funkcje bezpieczeństwa zintegrowane w urządzeniach przemysłowych" Materiały II Międzynarodowej Konferencji – Problemy bezpieczeństwa w budowie i eksploatacji maszyn i urządzeń górnictwa podziemnego, CBiDGP Ustroń 2010

[3] M. Trajdos „Wybrane zagadnienia bezpiecznego układu sterowania maszyn górnictwa odkrywkowego", Górnictwo Odkrywkowe, Rocznik LI, nr 5, 2010

[4] M. Trajdos „Zasady wykonywania przeglądów, remontów i modernizacji wg 2009/104/WE i 2006/42/WE." Materiały III Kongresu Maszynowego, FORUM, Warszawa 2011

[5] M. Trajdos „Niezawodność części systemu sterowania związanego z bezpieczeństwem – wybrane zagadnienia do zastosowania w projektowaniu układów w górnictwie." Materiały III Międzynarodowej Konferencji – Problemy bezpieczeństwa w budowie i eksploatacji maszyn i urządzeń górnictwa podziemnego, CBiDGP Ustroń 2011

[6] Rozporządzenie Ministra Gospodarki z dnia 21 października 2008 r. w sprawie zasadniczych wymagań dla maszyn (Dz. U. Nr 199, poz. 1228)

[7] Norma PN-EN ISO 13849-1:2008 „Bezpieczeństwo maszyn -- Elementy systemów sterowania związane z bezpieczeństwem -- Część 1: Ogólne zasady projektowania" PKN Warszawa 2008

[8] Norma PN-EN ISO 13849-2:2008 „Bezpieczeństwo maszyn -- Elementy systemów sterowania związane z bezpieczeństwem -- Część 2: Walidacja" PKN Warszawa 2008

[9] Norma PN-EN61508-6:2010„Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych /programowalnych elektronicznych systemów związanych z bezpieczeństwem -- Część 6: Wytyczne do stosowania IEC 61508-2 i IEC 61508-3" PKN Warszawa 2010

[10] Norma PN-EN 62061:2008 „Bezpieczeństwo maszyn - Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem" PKN Warszawa 2008

Artykuł recenzował mgr inż. Wiesław Monkiewicz
*Rękopis otrzymano 16.08.2011 r. *2210*