Inżynieria Maszyn, R. 17, z. 2, 2012

systemy i układy bezpieczeństwa,
niezawodność, ocena ryzyka, MTTF

Wojciech KRAMAREK[1]
Piotr SZULEWSKI[1]

SYSTEMY BEZPIECZEŃSTWA WSPÓŁCZESNYCH MASZYN I URZĄDZEŃ TECHNOLOGICZNYCH

W artykule zasygnalizowano problemy związane z określaniem niezawodności działania układów sterujących odpowiedzialnych za bezpieczeństwo maszyny lub procesu. Układ sterujący odpowiedzialny za bezpieczeństwo jest niezbędny w maszynach lub systemach stwarzających poważne zagrożenie. Układ ten musi reprezentować odpowiedni poziom niezawodności działania (wykonywania poleceń bezpieczeństwa), dopasowany do tworzonego przez maszynę lub instalację ryzyka. Wiarygodność systemu sterującego jako układu bezpieczeństwa może być określona przez podanie poziomu nienaruszalności bezpieczeństwa *(safety integrity level-_SIL)* lub podanie wartości poziomu zapewnienia bezpieczeństwa (*performance level-PL*). Poziom tych współczynników jest zależny od odporności układu na błąd wewnętrzny (uszkodzenie elementów) w czasie pracy systemu. Artykuł przedstawia także czynniki wpływające na niezawodność działania układu sterowania związanego z bezpieczeństwem.

1. WPROWADZENIE

Nie wszystkie systemy bezpieczeństwa maszyn i instalacji zapewniają taki sam poziom bezpieczeństwa. Pewne grupy układów zapewniają wykonywanie poleceń związanych z bezpieczeństwem tylko w przypadku prawidłowego działania wszystkich elementów składowych. Układy te są nieodporne na błędy elementów. Istnieją także grupy układów sterujących, które potrafią realizować funkcje bezpieczeństwa nawet w przypadku pojawienia się uszkodzeń elementów tworzących system. Systemy bezpieczeństwa maszyn są dzielone na kategorie (poziomy) związane z ich przeznaczeniem oraz zdolnością zapewnienia działania funkcji bezpieczeństwa. Według normy EN 954-1 (obowiązującej do końca roku 2011) występowało pięć kategorii związanych z bezpieczeństwem układów sterujących. Oznaczane one były odpowiednio symbolami: B, 1, 2, 3 oraz 4. Układy sterujące wykonane w kategorii B zapewniały najniższy poziom bezpieczeństwa, natomiast układy wykonane w kategorii 4 najwyższy poziom bezpieczeństwa [1].

Wprowadzona niedawno norma EN ISO 13849-1 2008 określa pojęcie poziomów działania (ang. *PL -performance level*). Występuje pięć poziomów działania różnicujących bezpieczeństwo. Najniższy z nich, zapewniający najniższe bezpieczeństwo układów to PLa,

[1] Zakład Automatyzacji, Obrabiarek i Obróbki Skrawaniem, Wydział Inżynierii Produkcji Politechniki Warszawskiej

najwyższy to Ple. Normy IEC 61508 oraz IEC 61511 (normy przeznaczone głównie dla przemysłu chemicznego i procesowego) definiują wymagany stopień ograniczenia ryzyka oraz zdolność systemu do ograniczania ryzyka przez podanie parametru SIL (ang. *Safety Integrity Level*) nazywanego poziomem nienaruszalności bezpieczeństwa. Występują cztery poziomy SIL. Poziom zapewniający najniższe bezpieczeństwo to poziom SIL 1, natomiast najwyższy stopień bezpieczeństwa gwarantują układy z poziomem SIL 4.

Obowiązujące i stosowane aktualnie poziomy PL oraz poziomy SIL są koncepcyjnie zbliżone i mogą być stosowane wymiennie. Niezawodność działania układu sterującego i stopień bezpieczeństwa gwarantowany przez ten układ mogą być ocenione zarówno z wykorzystaniem poziomów SIL jak i poziomów PL [2].

2. POJĘCIA ZWIĄZANE Z BEZPIECZEŃSTWEM

W rozdziale tym zostaną przedstawione i nieco bardziej szczegółowo omówione podstawowe pojęcia i sformułowania często występujące podczas analizy ryzyka wystąpienia stanu awaryjnego. Ich jednoznaczne rozumienie jest warunkiem koniecznym dla poprawnego i efektywnego stosowania norm i zaleceń wykorzystywanych współcześnie w tego typu zagadnieniach. I tak odpowiednio:

Funkcja bezpieczeństwa - jest to funkcja realizowana przez system sterowania o określonym poziomie nienaruszalności, która przeznaczona jest do utrzymania warunków bezpieczeństwa maszyny lub zapobiegania bezpośredniemu wzrostowi ryzyka. Niezgodne z założeniami zadziałanie układu realizującego funkcję bezpieczeństwa może spowodować bezpośredni wzrost ryzyka. Przykład jest zaprezentowany na rysunku 1.

Rys. 1. Przykład układu realizującego funkcję bezpieczeństwa (zabezpieczenie przed nadmiernym wzrostem ciśnienia)
Fig. 1. The example of the mechanical safety system (safety valve)

Uszkodzenie sprzętu przypadkowe – jest to uszkodzenie występujące w przypadkowym czasie, które powstaje w wyniku degradacji (zużycia lub uszkodzenia) sprzętu.

Uszkodzenie systematyczne – jest to uszkodzenie powtarzalne, występujące w określonych sytuacjach, wynikające z zastosowania nieprawidłowo dobranych elementów lub błędnego oprogramowania.

Zagrożenia te mogą być wyeliminowane tylko przez zmianę konstrukcji, procesu wytwarzania, zastosowanych elementów, procedur działania lub innych odpowiednich czynników.

SIS – (*ang. safety instrumented system)* - system bezpieczeństwa złożony z układów tworzących system sterowania odpowiedzialny za bezpieczeństwo.

SRCS – (*ang. safety related control system)* - system odpowiedzialny za bezpieczeństwo (odpowiednik SIS).

SIF - (*ang. safety instrumented functions)* – elementarne przyrządowe systemy bezpieczeństwa tworzące system bezpieczeństwa.

SIL – (*ang. safety integrity level)* - poziom nienaruszalności bezpieczeństwa określający wiarygodność systemu jako układu bezpieczeństwa.

PL – (ang. performance level - poziom zapewnienia bezpieczeństwa przez system.

HFT – (ang. hardware fault tolerance) - odporność systemu na wystąpienie błędu, zależna od struktury kanałowej poszczególnych systemów tworzących kompletny układ.

PFD – (ang. failure probability in the event of a request occurring) - prawdopodobieństwa niezadziałania układu w przypadku przywołania funkcji bezpieczeństwa.

SFF – (ang. proportion of safe faults or safe failures) - udział błędów bezpiecznych w układzie monitorującym prawidłowość działania.

T proo f- (ang. test interval for the entire safety system) - okresów testowania systemu bezpieczeństwa.

MTTF - (ang. mean time till failure) - średni czas pomiędzy niebezpiecznymi uszkodzeniami.

DC – (*ang. diagnostic coverage)* - pokrycie diagnostyczne.

CCF – (ang. common cause failure) - współczynnik defektów o wspólnej przyczynie.

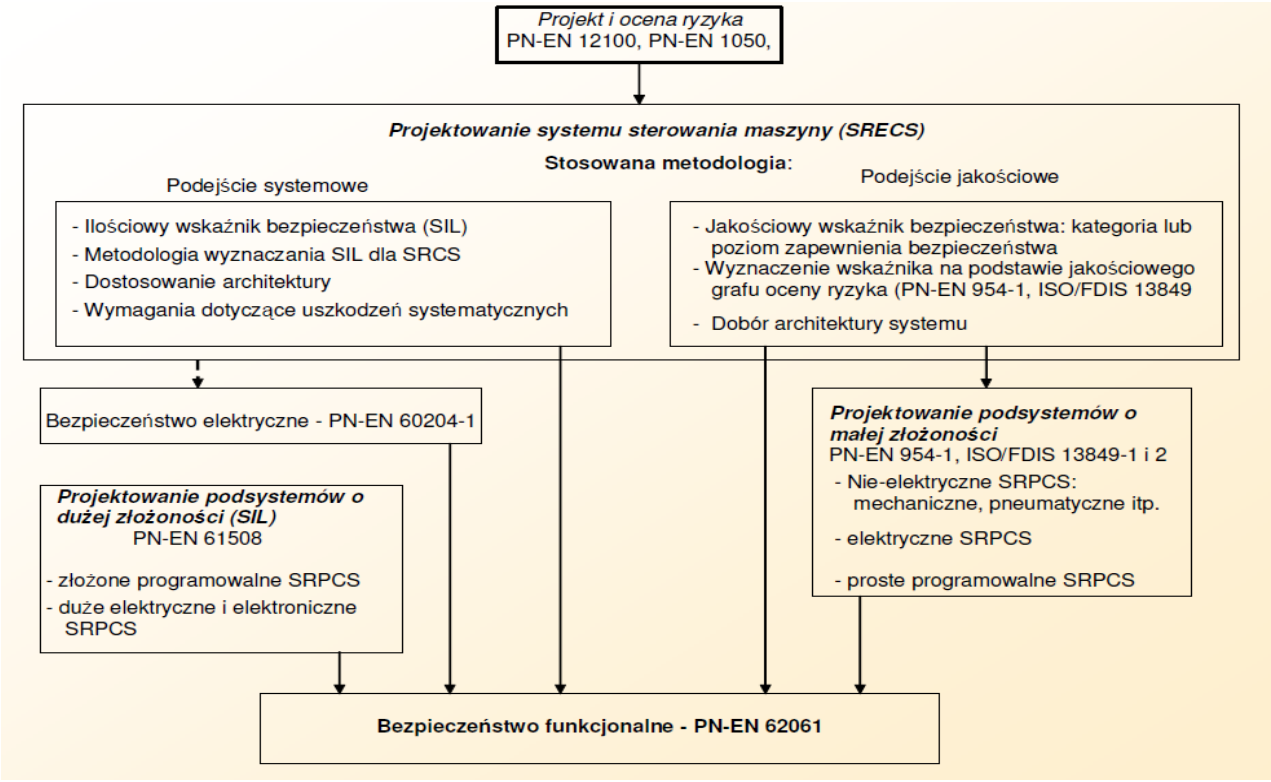
PFHd – (ang. probability of dangerous failure per hour) - prawdopodobieństwo błędnego zadziałania elementu bezpieczeństwa w określonej jednostce czasu.

3. SYSTEM BEZPIECZEŃSTWA

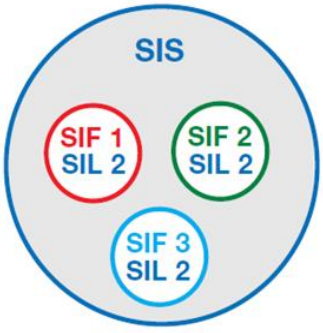
Przy projektowaniu układu sterującego odpowiedzialnego za bezpieczeństwo można wykorzystać jedną z dwóch możliwych dróg. Pierwsza możliwość to projekt oparty o podejście systemowe, bazujący na pojęciu SIL, natomiast druga droga jest oparta na podejściu jakościowym korzystającym z pojęcia PL. Obydwie drogi projektowania są przedstawione na rys. 2.

System bezpieczeństwa SIS stanowią układy tworzące system sterowania odpowiedzialny za bezpieczeństwo. Kompletny system bezpieczeństwa (SIS) składa się z pewnej ilości przyrządowych systemów bezpieczeństwa SIF, których zadaniem jest zmniejszenie, mogącego wystąpić w czasie produkcji, potencjalnego niebezpieczeństwa lub wyeliminowanie tego zagrożenia. Przykład koncepcji SIS jest zamieszczony na rysunku 3. System bezpieczeństwa w tym przypadku składa się z trzech elementarnych systemów bezpieczeństwa. Przykładem może być system bezpieczeństwa reaktora chemicznego,

zabezpieczający przed nadmiernym ciśnieniem, temperaturą oraz wzrostem poziomu czynnika powyżej poziomu dopuszczalnego.



Rys. 2. Schemat pokazujące dwie możliwe metody projektowe układów bezpieczeństwa funkcjonalnego [3]
Fig. 2. The different project methods of functional safety system [3]



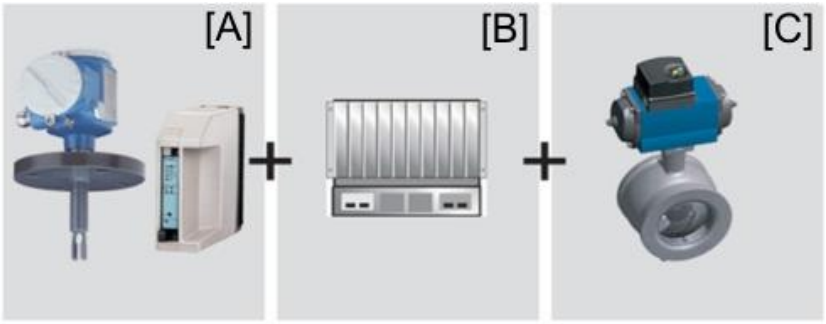
Rys. 3. Układ SIS z odpowiednim poziomem nienaruszalności bezpieczeństwa [4]
Fig. 3. The SIS system with adequate safety level [4]

W elementarnym systemie bezpieczeństwa (SIF) poprawność, niezawodność jego działanie zależy od trzech składników systemu, wymienionych poniżej:

- czujników przekazujących dane o stanie systemu, od stanu układu zasilającego czujników oraz interfejsów i układów przekształcających [5],

- układu logicznego wraz z jego zasilaniem i systemem przekazywania danych, wytwarzającego, po otrzymaniu sygnałów z sensorów, odpowiednie sygnały wyjściowe,
- elementów wykonawczych jak zawory, styczniki, falowniki, elementy elektroniczne, realizujących otrzymane z układu logicznego polecenia.

Przykład elementarnego systemu bezpieczeństwa jest przedstawiony na rys. 4, gdzie odpowiednimi symbolami literowymi zostały oznaczone: (A)-sensor, (B)-układ logiczny, (C)-element wykonawczy.



Rys. 4. Przykład realizacji funkcji bezpieczeństwa (SIF) [1]
Fig. 4. The safety function (SIF) realization - simple example [1]

Norma IEC 61511 definiuje SIF jako funkcję bezpieczeństwa z określonym poziomem niezawodności bezpieczeństwa (SIL), który jest niezbędny do osiągnięcia założonego bezpieczeństwa funkcjonalnego. SIF może być funkcją bezpieczeństwa realizowaną przyrządowo (zabezpieczenie przed nadmiernym ciśnieniem przez zawór ciśnieniowy) lub funkcją realizowaną układowo (czujniki, układ logiczny, układ wykonawczy). Przykładem sytuacji, w której postało zagrożenie i muszą zadziałać systemy realizujące funkcje bezpieczeństwa, jest nieprzewidziany wzrost ciśnienia w zbiorniku reaktora, który może skutkować rozerwaniem zbiornika. Funkcję bezpieczeństwa zapewnia układ z zaworem ciśnieniowym, który po osiągnięciu określonego ciśnienia otwiera się samoczynnie uniemożliwiając dalszy wzrost ciśnienia w zbiorniku (rys. 1).

4. NIEZAWODNOŚĆ SYSTEMU BEZPIECZEŃSTWA

Wiarygodność systemu jako układu bezpieczeństwa wyraża się poziomem nienaruszalności bezpieczeństwa SIL, który zależy od prawdopodobieństwa wystąpienia błędu wewnętrznego w czasie pracy systemu [6]. Poziom nienaruszalności bezpieczeństwa został określony przez normę EN 62061 (oraz powiązane z nią normy z serii EN 61508, EN 61511 i in.). Poziom nienaruszalności bezpieczeństwa jest zdefiniowany jako prawdopodobieństwo, że system związany z bezpieczeństwem wykona w sposób zadowalający wymagane funkcje bezpieczeństwa we wszystkich określonych warunkach i w określonym przedziale czasu.

Wiarygodność systemu jako układu bezpieczeństwa może być również określona zgodnie z normą EN 13849 przez podanie wartości poziomu zapewnienia bezpieczeństwa PL. Poziomem zapewnienia bezpieczeństwa jest określana zdolność układów związanych z bezpieczeństwem do wykonania funkcji bezpieczeństwa pod przewidywalnymi warunkami w celu wypełnienia oczekiwanej minimalizacji ryzyka. Wymienione powyżej wskaźniki określające bezpieczeństwo działania układów sterujących mogą być używane przez projektantów zgodnie z ich preferencjami wynikającymi z doświadczenia i umiejętności.

Podstawowe zadanie dla systemu bezpieczeństwa nie polega na wyeliminowaniu możliwości awarii układu, lecz na spowodowaniu, że w wypadku awarii odpowiednie urządzenia przełączone zostaną w stan bezpieczny. Stopień niezawodności zadziałania elementów przeznaczonych do stworzenia przyrządowych systemów bezpieczeństwa określa ich poziom nienaruszalności bezpieczeństwa SIL [6].

SIL określa tolerowane przez użytkownika, dopuszczalne w systemie bezpieczeństwa prawdopodobieństwo niezadziałania przywoływanej funkcji bezpieczeństwa. Poniżej przedstawiono tabelę określającą niezbędny do uzyskania przez system bezpieczeństwa poziom SIL w zależności od zagrożeń wytwarzanych przez proces lub maszynę.

Tabela 1. Poziom SIL i odpowiadający mu opis ochrony
Table 1. The short description of the SIL's safety level

Wymagany poziom SIL	Wytworzona ochrona przed potencjalnymi zagrożeniami
4	Ochrona przed katastroficznymi zagrożeniami dla społeczności lokalnej
3	Ochrona przed umiarkowanymi zagrożeniami dla pracowników i społeczności lokalnej
2	Zabezpieczenie sprzętu i produkcji. Umiarkowany poziom ochrony zdrowia pracowników
1	Zabezpieczenie w umiarkowanym stopniu urządzeń i procesów

Im wyższe ryzyko wypadku oraz jego konsekwencji tym musi być wyższy wytworzony poziom SIL systemu bezpieczeństwa. Osiągnięcie wymaganego, w wyniku analizy ryzyka, poziomu nienaruszalności bezpieczeństwa dla projektowanego układu związanego z bezpieczeństwem wymaga uwzględnienia następujących problemów:

- architektury, struktury kanałowej poszczególnych systemów tworzących kompletny układ,
- prawdopodobieństwa niezadziałania układu w przypadku przywołania funkcji bezpieczeństwa,
- udziału błędów bezpiecznych w układzie monitorującym prawidłowość działania,
- okresów testowania systemu bezpieczeństwa.

W przypadku stosowania w układach bezpieczeństwa funkcjonalnego elektronicznych podzespołów należy zgodnie z przepisami normy EN IEC 62061 wyznaczyć poziom SIL, określający wymagany poziom nienaruszalności bezpieczeństwa funkcji bezpieczeństwa. Norma EN IEC 62061 jest normą sektorową dla branży maszyn, wywodzącą się z IEC 61508. Norma EN IEC 62061 odnosi się wyłącznie do układów elektrycznych i elektronicznych o wysokiej złożoności.

Część normy dotyczy zagadnień występujących w złożonych systemach programowalnych. Norma przedstawia szereg procedur mogących pomóc w określeniu poziomu niezawodności działania elektrycznych, elektronicznych i programowalnych systemów sterowania maszyn związanych z bezpieczeństwem.

5. OKREŚLANIE PL

Podczas określania PL należy przyjąć, że jest ono funkcją określonych parametrów. Osiągnięcie wyznaczonego w procesie oceny ryzyka, prowadzonego zgodnie z zaleceniami normy EN ISO 13849, wymaganego poziomu PL zależy od uwzględnienia w czasie projektowania następujących parametrów:

- architektury układu sterowania, (koncepcja, która występowała wcześniej pod pojęciem kategorii),
- średniego czasu pomiędzy niebezpiecznymi uszkodzeniami MTTF czyli parametru określającego niezawodność działania stosownych elementów. Znajomość tego współczynnika jest wymagana dla poszczególnych części składowych systemu,
- pokrycia diagnostycznego DC (pojęcie to reprezentuje ilość zadań monitorowania defektów systemu),
- współczynnika defektów o wspólnej przyczynie *CCF* (zdarzenia w czasie którego uszkodzenie jednego z elementów wiąże się z uszkodzeniem kolejnych elementów),
- sposobu zabezpieczenia przed błędami systematycznymi oraz przypadkowymi.

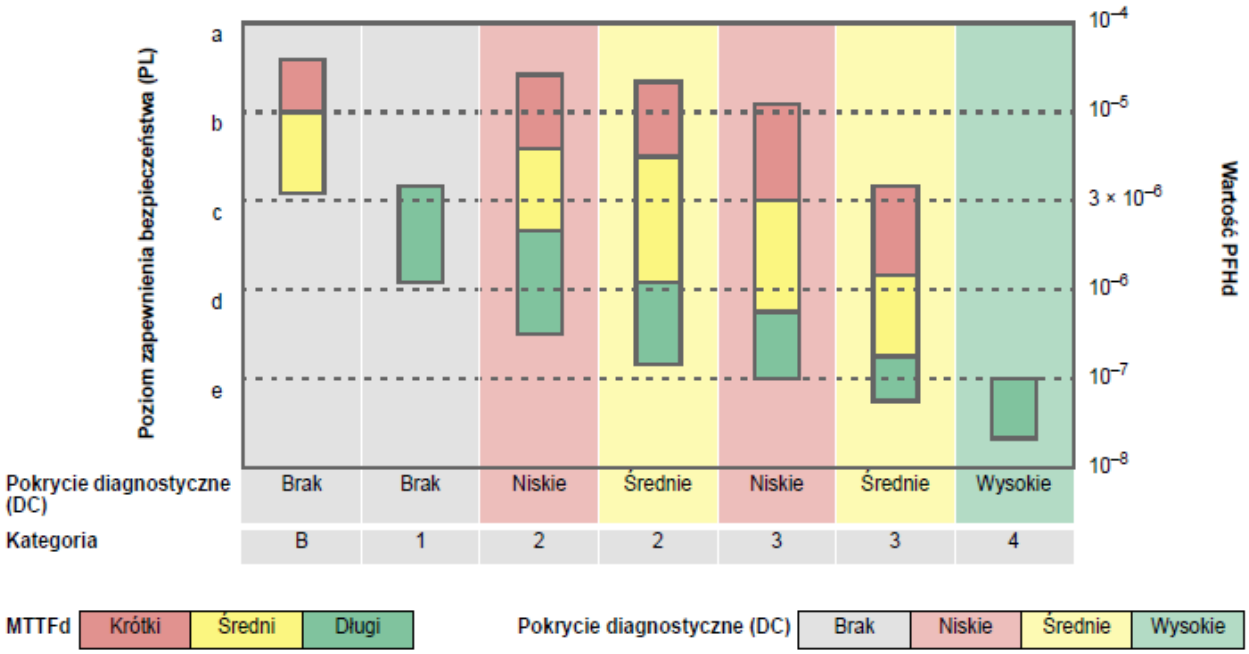
Czynniki wpływające na niezawodność działania układu sterowania związanego z bezpieczeństwem są rozmaitego pochodzenia. Nie zawsze można określić je wszystkie i do tego precyzyjnie. Jednak niezawodność działania układów sterowania można zwiększyć uwzględniając następujące zagadnienia [7]:

- defekty przypadkowe (w wyniku uszkodzeń lub zużycia elementów) można eliminować przez odpowiedni dobór struktury systemu (architekturę systemu) oraz stosowanie odpowiednio niezawodnych elementów i podzespołów,
- zwiększenie niezawodności działania można uzyskać stosując obwody wielokanałowe oraz stosując zasady różnorodności technicznej elementów,
- defekty systematyczne (błędy oprogramowania, powtarzalne błędy czujników) eliminowane są za pomocą działań prewencyjnych,
- warunkiem istnienia bezpieczeństwa funkcjonalnego jest przestrzeganie odpowiednich procedur przez odpowiednio wyszkolony personel,
- przez audyty (walidację) uzyskujemy pewność osiągnięcia wymaganego poziomu bezpieczeństwa funkcjonalnego,
- miernikiem osiągniętego poziomu bezpieczeństwa funkcjonalnego są wskaźniki probabilistyczne.

Zgodnie z obowiązującą przez wiele lat normą EN 954 dotyczącą bezpieczeństwa układów sterujących (straciła ważność 31 grudnia 2011) niezawodność działania układów bezpieczeństwa była tylko funkcją struktury układu (architektury). Obowiązująca obecnie

norma EN 13849 bierze pod uwagę architekturę, niezawodność działania elementów oraz sposób i częstość prowadzenia monitoringu. Rysunek 5 przedstawia wspomniane powyżej zależności. Z analizy rysunku 5 wynika, że tej samej architekturze układu mogą odpowiadać różne poziomy działania PL w zależności od zastosowanego pokrycia diagnostycznego DC oraz niezawodności działania zastosowanych elementów określonej współczynnikiem MTTFd.

Ponieważ norma EN IEC 61 508 dotycząca bezpieczeństwa układów sterujących oraz norma EN ISO 13849 dotycząca tych samych zagadnień zostały przyjęte w niewielkim odstępie czasu a zespoły redakcyjne korzystały z tych samych założeń i materiałów dlatego normy te są traktowane jako normy kompatybilne. Oznacza to, że poziom działania PL może być określany przez poziom nienaruszalności działania SIL oraz odwrotnie. Wspólnym parametrem określającym niezawodność działania tych układów lub elementów jest prawdopodobieństwo błędnego zadziałania w określonej jednostce czasu PFHd.



Rys. 5. Poziom zapewnienia bezpieczeństwa PL jako funkcja architektury układu, niezawodności działania elementów (MTTF) oraz pokrycia diagnostycznego DC
Fig. 5. The safety level (PL) as an function of system architecture, reliable components (MTTF) and DC diagnostic

Rys. 5 pokazuje przybliżony związek między PL i SIL dla typowych struktur obwodów uzyskiwanych przy użyciu mało skomplikowanych technologii.

Procedury określania SIL lub PL wspomniane powyżej mogą być stosowane do całego układu bezpieczeństwa, jego podsystemów lub poszczególnych elementów [8]. Założenie to ma tę zaletę, że elementy z podaną przez producentów wartością SIL mogą być zastosowane przy określaniu niezawodności układu prowadzonego według normy EN ISO 13 849-1:2008, natomiast elementy z podaną wartości PL mogą być użyte przy określaniu poziomu nienaruszalności działania SIL prowadzonego według rozważań normy EN IEC 62

061:2005. Przy zamianie (konwersji) parametru MTTFd na wartość PFHd lub odwrotnie można opierać się na tablicy zamieszczonej w Aneksie K normy EN ISO 13 849-1:2008.

Tabela 2. Przybliżony związek między PL i SIL dla typowych struktur nieskomplikowanych technologii [8]
Table 2. The simple/estimated relation between PL and SIL for typical easy technology structures [8]

PL (Poziom Działania)	PFH_D (prawdopodobieństwo wystąpienia uszkodzenia niebezpiecznego na godzinę)	SIL (Poziom Nienaruszalności Bezpieczeństwa)
A	10^{-5} do < 10^{-4}	brak
B	3×10^{-6} do < 10^{-5}	1
C	10^{-6} do < 3×10^{-6}	1
D	10^{-7} do < 10^{-6}	2
E	10^{-8} do < 10^{-7}	3

Od pewnego czasu pracują wspólne zespoły grup normalizacyjnych IEC oraz ISO mające na celu opracowanie jednolitej normy dotyczącej bezpieczeństwa maszyn jak i systemów procesowych. Pierwszym wynikiem pracy tych zespołów jest dokument opublikowany przez IEC jako IEC 62061-1, oraz przez ISO jako ISO 23849-1. Dokument ten występuje pod angielską nazwą: "*Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery*". (Przewodnik dotyczący stosowania ISO 13849-1 oraz IEC 62061 przy projektowaniu systemów bezpieczeństwa dla maszyn). Celem dalszych prac ma być utworzenie metodyki określania wspólnego wskaźnika niezawodności działania układów bezpieczeństwa. Wskaźnik ten będzie stosowany zarówno w procedurach związanych z maszynami jak i w inżynierii procesowej.

6. PODSUMOWANIE

System sterowania, w tym architektura systemu, metody testowania oraz niezawodność zastosowanych elementów, decyduje o osiągnięciu wymaganego poziomu bezpieczeństwa sterowanej maszyny. Należy jednak być świadomym, że określane i podawane poziomy bezpieczeństwa są wynikiem przeprowadzania szacunków i mają zdecydowanie charakter przybliżony. Nie zwalnia to obsługi ani projektanta od stosowania zasad dobrej praktyki inżynierskiej i zdrowego rozsądku podczas tworzenia koncepcji modernizowanej lub projektowanej maszyny czy urządzenia technologicznego.

LITERATURA

[1] ENDRESS+HAUSER, 2011, *People for process automation*, http://www.pl.endress.com.
[2] WIKI, 2012, http://wikipedia.org/wiki/Industrial_safety_systems.

[3] SICK,2012, http://www.sick.com/pl.
[4] SICK, 2010, *Przewodnik bezpieczne maszyny*, Opracowanie firmy Sick.
[5] OBORSKI P., SZULEWSKI P., 2003, *Integration of information flow in a Basic Manufacturing Unit, BMU*, Proceedings of the International Conference: Computer Integrated Manufacturing, CIM'03, Wisła, 230-238.
[6] NORMA PN, 2011, *Poziomy zapewnienia bezpieczeństwa. Przejście z EN 954-1 na EN ISO 13849-1*.
[7] ROCKWEL, 2011, http://www.rockwel automation.com.
[8] SCHMERSAL, 2011, *Specific Background Information on EN ISO 13 849-1:2006*, Opracowanie własne firmy.

THE SAFETY SYSTEMS OF MODERN MACHINES AND TECHNOLOGICAL EQUIPMENT

The paper presents problems connected with designation of control systems responsible for machine or industrial system safety. An industrial safety system is a countermeasure crucial in any hazardous plants or machines. This system should be matched to risk connected to designed machine or process. Immunity of control system for failure is defined by Safety Integrity Level (SIL) in accordance with EN 62061. In simple terms, SIL is a measurement of performance of safety. Designers of machines can also use a performance level (PL) as an assessment of risk reduction. In terms of system and machine safety, the performance level is determined in accordance with EN ISO 13849-1. Level of SIL or PL indicates the probability of failure for each safety function. In the paper there is also discussed the problem of factors, which can influence the performance of safety control systems.