SUR 03 _2014

Autorzy: Mgr inż. Krzysztof Ujczak
Kierownik Działu Bezpieczeństwa Procesowego

"Bezpieczeństwo w układach sterowania: SIL i PL - dwa wskaźniki operujące tym samym parametrem niezawodnościowym".

W związku z obowiązywaniem dwóch różnych norm dotyczących bezpieczeństwa układów sterowania dla maszyn, użytkownicy i producenci stają często przed dylematem, jaką metodologię do oceny obwodów automatyki wybrać. W artykule opisane zostaną najważniejsze podobieństwa i różnice pomiędzy normami PN-EN ISO 13849 oraz PN-EN 62061. Przedstawione zostaną praktyczne przykłady zastosowań obydwu nich.

Postęp technologiczny i automatyzacja, a także zwiększanie wydajności przy jednoczesnej redukcji kosztów jednostkowych powoduje, że maszyny produkcyjne stwarzają coraz to nowsze zagrożenia. Od wielu lat układy sterowania maszyn, oprócz elementów elektrycznych i elektromechanicznych – sprawdzonych i niezawodnych, zawierają również zaawansowane rozwiązania elektroniki programowalnej. Elementy takie, często o nieznanych parametrach niezawodnościowych stwarzają wiele problemów projektantom układów sterowania maszyn. W szczególności funkcje związane z bezpieczeństwem, od których wymaga się najwyższego poziomu skuteczności działania, powinny być zrealizowane za pomocą elementów o największej pewności.

Od niedawna normę PN-EN 954-1 dotyczącą układów sterowania związanych z bezpieczeństwem, zastąpiła norma PN-EN ISO 13849-1. Jednocześnie, równolegle obowiązuje norma międzynarodowej komisji elektrotechnicznej PN-EN IEC 62061. Standardy te są skierowane do projektantów oraz użytkowników maszyn, w których funkcje bezpieczeństwa realizowane przez układ sterowania są jednym ze środków użytych do redukcji ryzyka występującego na maszynie.

Obydwie, równolegle obowiązujące normy wyrażają niezawodność układów sterowania za pomocą parametru PFH_d. Określa on prawdopodobieństwo niebezpiecznego uszkodzenia na godzinę. Odpowiednim wartościom PFH_d odpowiadają określone Safety Integrity Level - SIL (opisane w PN-EN 62061) i Performance Level - PL (opisane w PN-EN ISO 13849-1). Zależności pomiędzy nimi przedstawione zostały w tabeli 1.

PL	PFH_d	SIL
a	od 10^{-5} do 10^{-4}	-
b	od 3×10^{-6} do 10^{-5}	1
c	od 10^{-6} do 3×10^{-6}	1
d	od 10^{-7} do 10^{-6}	2
e	od 10^{-8} do 10^{-7}	3

Tabela 1 Zależności pomiędzy SIL i PL

Norma PN-EN ISO 13849-1 zawiera w sobie jakościowe podejście znane z PN-EN 954-1 i dodaje aspekty ilościowe zaczerpnięte m.in. z rodziny norm PN-EN 61508. Cechy jakościowe obwodów są przedstawione za pomocą tzw. kategorii (B, 1,2,3 lub 4). Odpowiadają one określonym modelowym architekturom układów. Te natomiast, różnią się sprzętową tolerancją na uszkodzenia, testami diagnostycznymi oraz rodzajem użytych elementów. W skrócie, kategorie: B, 1 i 2 są modelami jednokanałowymi. Oznacza to, że wystąpienie jednego błędu w układzie spowoduje utratę funkcji bezpieczeństwa i bezpośrednio wpłynie na podwyższenie poziomu ryzyka obecnego na maszynie. Modele dla kategorii: 3 i 4 mają strukturę dwukanałową. Oznacza to, że jedno uszkodzenie nie spowoduje utraty funkcji bezpieczeństwa (układ posiada sprzętową tolerancję na uszkodzenia równą 1). Należy tutaj zaznaczyć, że prawdopodobieństwo wystąpienia dwóch błędów w każdym z kanałów układów uznaje się za bardzo małe i nie uwzględnia się go przy analizie niezawodnościowej układów sterowania maszyn.

Oprócz samej architektury, przy projektowaniu i walidacji układów sterowania związanych z bezpieczeństwem zgodnie z PN-EN ISO 13849-1 i PN-EN ISO 13849-2, należy również wziąć pod uwagę szereg aspektów ilościowych. Wprowadzony został parametr $MTTF_d$ jako średni czas pomiędzy uszkodzeniami niebezpiecznymi. Jego wartość powinna być podana przez producenta, lub wylicza się go na podstawie strumienia uszkodzeń spowodowanych przypadkowymi uszkodzeniami sprzętu (dla złożonej elektroniki i elementów o znanym strumieniu uszkodzeń) lub na podstawie parametru B_{10d}, który stosuje się m. in. dla urządzeń elektromechanicznych i innych, w których cechy niezawodnościowe są silnie uzależnione od zużycia (parametr B_{10d} określa ilość cykli, po których 10% populacji ulega uszkodzeniu niebezpiecznemu).

Kolejnym parametrem służącym określeniu niezawodności układu sterowania realizującego daną funkcję bezpieczeństwa, jest DC czyli pokrycie diagnostyczne. Opisuje ono efektywność funkcji diagnostycznych układu, jako stosunek strumienia uszkodzeń niebezpiecznych wykrytych do strumienia uszkodzeń niebezpiecznych niewykrytych. Diagnostyka elementów układu sterowania funkcjami bezpieczeństwa jest niezwykle istotna. Wyobraźmy sobie model równoległy z redundancją, w którym pokrycie diagnostyczne elementów jest małe lub nie ma go wcale. Jeżeli jeden z kanałów ulegnie uszkodzeniu, układ dalej będzie spełniał swoje funkcje bezpieczeństwa (Sprzętowa tolerancja jednego uszkodzenia). Uszkodzenie to nie zostanie jednak w żaden sposób wykryte, a użytkownik nie

zostanie powiadomiony o konieczności wymiany wadliwego elementu. Nietrudno sobie wyobrazić, że wystąpienie błędu w drugim kanale i co za tym idzie utrata możliwości wypełniania funkcji bezpieczeństwa jest tylko kwestią czasu. Takie sytuacje są bardzo niebezpieczne dla operatorów maszyn, którzy nie są świadomi istnienia ryzyka związanego z wadliwym zadziałaniem układu sterowania. Brak reakcji maszyny związanej z wyzwoleniem funkcji bezpieczeństwa przez urządzenie ochronne, czy też nieprzewidziane wysterowanie ruchu maszyny może okazać się tragiczne w skutkach. Diagnostyka elementów układu sterowania ma za zadanie m.in. powstrzymać przed wystąpieniem takiej kumulacji błędów.

Ostatnim parametrem jakościowym jaki należy wyznaczyć do określenia niezawodności układu sterowania związanego z bezpieczeństwem jest CCF - odporność układu na błędy o wspólnej przyczynie. Zgodnie z normą PN-EN ISO 13849-1 ocena takiej odporności jest dwustanowa. Analizowany obwód realizujący daną funkcję bezpieczeństwa może spełniać lub nie wymagania opisane w standardzie. W pierwszym przypadku - w ogóle nie uwzględniamy w dalszych kalkulacjach możliwości wystąpienia błędów o wspólnej przyczynie, w drugim natomiast - układ będzie niezgodny.

Norma PN-EN 62061 do oceny niezawodności układów sterowania używa podobnych, aczkolwiek różniących się pod pewnymi aspektami , parametrów. Przede wszystkim szacowanie prawdopodobieństwa niebezpiecznych przypadkowych uszkodzeń sprzętu opiera się na określeniu typu architektury podsystemów. W skrócie istnieją dwa typy bez tolerancji defektów (bez i z funkcji diagnostycznych), oraz dwa typy posiadające tolerancję pojedynczych defektów (analogicznie bez oraz posiadające funkcje diagnostyczne). Możemy tutaj doszukiwać się pewnych analogii pomiędzy typami i kategoriami. Zwróćmy jednak uwagę na różnice – typy architektur zgodnie z PN-EN 62061 pozostawiają więcej swobody projektantom systemów sterowania. Możemy stworzyć układ wielokanałowy posiadający dowolne wartości współczynników ilościowych. Architektury układów sterowania wyznaczone przez kategorie natomiast są modelami bardziej „zamkniętymi". Oznacza to, że użytkownik ma mniejszą swobodę w doborze modelu, jako że jest on uzależniony od większej liczby parametrów. Z drugiej strony mniejsza swoboda oznacza łatwiejszą implementację, brak skomplikowanych obliczeń i zmniejszenie prawdopodobieństwa popełnienia błędów projektowych i systematycznych.

Kolejnym parametrem, który należy określić postępując wg metodologii opisanej w normie PN-EN 62061 jest strumień uszkodzeń λ każdego z elementów. Jego wartość powinna być dana przez producenta elementów układu sterowania. Ostatecznie można go wyznaczyć stosując jedną z metod analitycznych takich jak analiza drzewa niezdatności, czy modele Markowa. Ogólnie rzecz ujmując parametr MTTF czy λ, są to wskaźniki mówiące o jakości użytych elementów i wskazują na, w przypadku pierwszym, czas pomiędzy, w przypadku drugim, prawdopodobieństwo wystąpienia uszkodzenia. Obydwa parametry są ze sobą powiązane za pomocą równości: λ=1/MTTF.

Funkcje testowania elementów układu są w obydwu normach przedstawione w ten sam sposób, za pomocą tego samego wskaźnika - pokrycia diagnostycznego DC, który został omówiony powyżej. Tym, czym w istocie obydwie metodologie się różnią jest podejście do błędów o wspólnej przyczynie. Metodyka zgodna z normą PN-EN ISO 13849-1 – jest bardzo okrojona. Traktowanie binarne (jest, bądź jej nie ma) odporności układu na błędy o wspólnej przyczynie wydaje się być bardzo

ogólnikowym. Norma PN-EN 62061 kwestię tę traktuje w sposób bardziej złożony i zbliżony do założeń wynikających z teorii niezawodności. Modele układów zgodne z tą normą zawsze posiadają pewną wartość współczynnika β, który wyraża ilość błędów o wspólnej przyczynie występujących w danym obwodzie. Wartość tego współczynnika waha się od ułamka do kilku, kilkunastu procent, jednak nigdy nie będzie on równy zero. Załącznik F normy PN-EN 62061 podaje proste podejście jakościowe do oszacowania odporności układu na błędy wspólnej przyczyny. Parametr β może przyjmować wartości 1, 2, 5 lub 10% - w zależności od zastosowanych metod unikania błędów o wspólnej przyczynie.

Podsumowując, stojąc przed wyborem odpowiedniej normy do implementacji układów sterowania realizujących funkcje bezpieczeństwa powinniśmy zwrócić uwagę na kilka aspektów. Obwody o niskiej złożoności, w których możemy zaimplementować proste modele architekturalne powinny zostać wykonane zgodnie z normą PN-EN ISO 13849-1. Pozwoli nam to zaoszczędzić czas poświęcony na obliczenia i analizy, pozwoli skorzystać z gotowych wzorców i wyznaczonych wartości parametrów niezawodnościowych zebranych w formie tabel na końcu normy. Dodatkowym, ale bardzo istotnym atutem tej normy jest fakt, że możemy ją zastosować do układów wykonanych we wszystkich technikach sterowania tj. elektrycznej, mechanicznej, pneumatycznej oraz hydraulicznej.

Z drugiej strony, dla układów o dużej złożoności (np. skomplikowanych układów elektroniki programowalnej) czy też o niestandardowych architekturach należałoby posłużyć się metodyką opisaną w normie PN-EN 62061. Dzięki niej będziemy mogli poprawnie i zgodnie z dobra praktyką inżynierską obliczyć i udokumentować niezawodność danego układu sterowania związanego z bezpieczeństwem.

ELOKON Polska Sp. z o.o.
Tytoniowa 22
04-228 Warszawa

Tel (+48 22) 812 71 38
Fax (+48 22) 613 36 32

elokon@elokon.pl
www.elokon.pl

Bank Zachodni WBK S.A.
23 Oddział Warszawa
50 1090 1030 0000 0001 2244 0365

NIP 5270202006
REGON 010088180
KRS 0000145346
Sąd Rejonowy dla m.st. W-wy w Warszawie
XX Wydział Gospodarczy
Kapitał Zakładowy 100.000 PLN