Napędy i sterowanie, luty 2014

Autorzy: Mgr inż. Krzysztof Ujczak
Kierownik Działu Bezpieczeństwa Procesowego

Walidacja układów sterowania związanych z bezpieczeństwem z wykorzystaniem normy PN-EN ISO 13849-2. Problemy z praktycznym wyznaczaniem Performance Level różnych funkcji bezpieczeństwa maszyn.

Streszczenie. Poniższy artykuł przedstawia najczęściej spotykane problemy i trudności przy praktycznym przeprowadzeniem walidacji zgodnie z normą PN-EN ISO 13849-2 zharmonizowaną z Dyrektywą Maszynową 2006/42/WE. Dotyczą one zarówno producentów urządzeń związanych z bezpieczeństwem jaki i użytkowników maszyn. Podane zostały wybrane przykłady i propozycje rozwiązań.

Abstract. This article shows problems and difficulties with practical process of validation according to EN ISO 13849-2 harmonized with Machine Directive 2006/42/EC. They affects both producers of machine safety related protective devices and end-users of the machines. Chosen examples and proposition of solutions are given. (Validation of safety related part of control system using of the EN ISO 13849-2 standard. Practical problems with qualifying of the Performance Level for various machine safety functions.).

Słowa kluczowe: PN-EN ISO 13849-2; Performance Level, walidacja, układ sterowania związany z bezpieczeństwem
Keywords: EN ISO 13849-2, Performance Level, validation, safety-related part of control system

Performance Level

Obecnie obowiązującą, podstawową wykładnią rozwiązań technicznych dotyczących konstrukcji i walidacji układów sterowania funkcjami bezpieczeństwa maszyn są normy PN-EN ISO 13849-1 i PN-EN ISO 13849-2.

Pierwsza z nich określa wymagania dla architektury połączenia i właściwości niezawodnościowych komponentów wykorzystywanych do realizacji funkcji bezpieczeństwa. Konstruktorzy mogą znaleźć tam narzędzia i wskazówki dotyczące skutecznej budowy systemów w oparciu o rozwiązania w różnych technologiach – mechanicznej, elektrycznej, pneumatycznej czy hydraulicznej.

Proces walidacji opisany w drugiej części normy polega na sprawdzeniu czy dany układ sterowania i związane z nim funkcje bezpieczeństwa spełniają założony poziom niezawodności - Performance Level Required (PLr), ustalony jako niezbędny do redukcji ryzyka przy wykorzystaniu różnych urządzeń ochronnych).

Performance Level jest parametrem określającym zdolność fragmentu układu sterowania do realizacji funkcji bezpieczeństwa. W celu jego ustalenia należy oszacować cztery parametry ilościowe oraz określić szereg aspektów jakościowych projektowanego bądź istniejącego systemu. Parametry wchodzące w skład PL to: Kategoria – związana przede wszystkim ze strukturą układu. Jest to parametr, który został przeniesiony z normy PN-EN 954-1. Ma on bardzo duże znaczenie dla niezawodności układu sterowania; MTTFd - Mean Time To Dangerous Failure (średni czas do

uszkodzenia niebezpiecznego) informujący o ilości czasu (w latach), jaki średnio upływa pomiędzy kolejnymi niebezpiecznymi uszkodzeniami komponentów. Jest on bezpośrednio związany z jakością użytych elementów. Parametr ten powinien być określony przez producenta. Dla sprawdzonych i powszechnie używanych komponentów bezpieczeństwa jest on stabelaryzowany w normie PN-EN 13849-1, jednakże aby móc zastosować te wartości, należy pamiętać aby zarówno producent jak i integrator spełniał wymagania określone jako podstawowe i sprawdzone zasady bezpieczeństwa; DC - Diagnostic Coverage (pokrycie diagnostyczne) - parametr informujący o tym ile uszkodzeń niebezpiecznych (w procentach) zostaje wykrytych spośród wszystkich możliwych. Wartości tego parametru dla wybranych metod są również stabelaryzowane w normie PN-EN 13849-1; CCF - Common Cause Failure (uszkodzenia o wspólnej przyczynie) - parametr informujący o odporności układu na uszkodzenia o wspólnej przyczynie. Takimi błędami może być np. utrata zasilania czy zakłócenia związane z brakiem kompatybilności elektromagnetycznej; W celu osiągnięcia odporności należy spełnić przynajmniej część z wymagań zawartych w liście kontrolnej wg PN-EN ISO 13849-1.

Przebieg walidacji wg PN-EN ISO 13849-2

Celem procesu walidacji jest potwierdzenie zgodności specyfikacji oraz projektu elementów systemu sterowania związanych z bezpieczeństwem z pełną specyfikacją wymagań dotyczących bezpieczeństwa maszyny [2].

Przebieg walidacji został dokładnie określony w normie PN-EN ISO 13849-2. Rozpoczyna się ona od planu z określeniem zasad, następnie przeprowadzany jest proces analizy bądź badania, w wyniku czego otrzymujemy protokół walidacyjny. Zawierać on powinien m. in. opis sposobu przeprowadzania walidacji, kryteria wykluczenia błędów, o ile miały miejsce, a także raporty z przeprowadzonych badań i o ile takie miały miejsce. Protokół jest dokumentem stwierdzającym poprawne i odpowiednio niezawodne realizowanie funkcji bezpieczeństwa przez układu sterowania

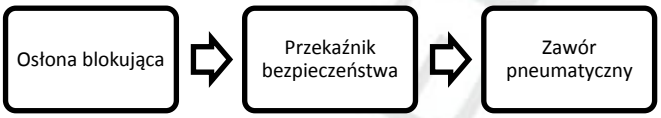
Pierwsza z technik przeprowadzania walidacji jest nazywana „walidacją przez analizę”. Aby móc ją stosować należy przygotować następujące dane wejściowe: zagrożenia stwarzane przez maszynę zidentyfikowane w trakcie analizy; nieuszkadzalność; strukturę systemu; niepodlegające określeniu ilościowemu czynniki jakościowe, które mają wpływ na zachowanie systemu czy też argumenty deterministyczne. Posiadając te czynniki należy wybrać jeden z dwóch rodzajów analizy: od skutku do przyczyny (np. analiza FTA, ETA) lub od przyczyny do skutku (np. analiza FMEA).

Badanie walidacyjne jest uzupełnieniem analizy. Należy je przeprowadzić jeżeli analiza nie jest wystarczająca. Założeniem walidacji przez badanie jest potraktowanie układu jak „czarnej skrzynki”. Stosując kombinacje sygnałów wejściowych należy porównywać otrzymywane sygnały wyjściowe z rezultatami założonymi podczas planu walidacji. W niektórych przypadkach należy zasymulować możliwe do przewidzenia uszkodzenia, a także uwzględnić możliwe do zaistnienia działania niewłaściwe.

Problemy przy praktycznym wyznaczeniu Performance Level

Stosowaną do roku 2011 norma dotycząca bezpieczeństwa układów sterowania PN-EN 954-1 w bardzo małym stopniu brała pod uwagę trwałość czy jakość elementów używanych do budowy obwodów sterowania. Mając to na uwadze, twórcy norm PN-EN ISO 13849, zdecydowali o uwzględnieniu również tego aspektu poprzez dodanie omówionych wcześniej wskaźników. Mimo racjonalności takiej zmiany, należy zaznaczyć, że wprowadziła ona wiele trudności przy praktycznej konstrukcji czy ocenie funkcji bezpieczeństwa maszyn.

Jednym z problemów, na jakie może natknąć się projektant, jest próba zrealizowania układu w architekturze odpowiadającej tzw. kategorii 2. Podstawowym wymogiem w tej kategorii jest zastosowanie systemu testującego wszystkie elementy wchodzące w skład obwodu. Test ten powinien być zrealizowany sto razy częściej, niż wywoływanie funkcji bezpieczeństwa. W praktyce oznacza to konieczność bardzo częstego testowania, niemożliwego do przeprowadzenia w większości aplikacji i maszyn z krótkim czasem cyklu, przykładowo – tam gdzie operatorzy są nadzorowani przez osłony blokujące. Przy łańcuchu bezpieczeństwa składającym się z osłony blokującej, przekaźnika bezpieczeństwa oraz elementu wyjściowego jakim jest zawór pneumatyczny odcinający zasilanie napędu stwarzającego zagrożenie w danej strefie (Rys 1.), należałoby taką osłonę otwierać sto razy częściej niż jest ona używana w podstawowym cyklu produkcyjnym. Takie wymagania są oczywiście nie do zaakceptowania i dlatego też kategoria 2 znajduje swoje zastosowanie głownie przy optoelektronicznych urządzeniach ochronnych (np. kurtynach świetlnych). Związane jest to z możliwością autotestowania urządzenia optoelektronicznego, nie do zrealizowania przy innych technicznych środkach bezpieczeństwa. Projektant często będzie wolał zrealizować układ w kategorii 3, która co prawda wymaga redundancji kanałów sterowania jednak okazuje się to łatwiejsze i przede wszystkim tańsze w realizacji od opracowania skomplikowanych technik i metod zapewniających odpowiedni poziom testowania przez układ sterowania.



Rys. 1. Przykładowy łańcuch bezpieczeństwa

Następnym problemem na jaki możemy natrafić podczas przeprowadzania walidacji zgodnie z PN-EN ISO 13849-2, jest wyznaczenie parametru MTTFd każdego z elementów wchodzących w skład układu bezpieczeństwa. Parametr ten, zgodnie z zaleceniami twórców norm, powinien być przede wszystkim podawany przez producentów komponentów układów sterowania. W praktyce okazuje się jednak, że wymaganie to jest respektowane przez bardzo niewielu z nich. Niejednokrotnie jesteśmy zmuszeni do wyznaczania go na podstawie stabelaryzowanych danych w normie. Wadą takiego rozwiązania jest wzięcie wartości uśrednionej dla danej grupy komponentów, podczas gdy faktyczna wielkość może się znacząco różnić. Dodatkowo musimy założyć, że producent danego elementu spełnił podstawowe i sprawdzone zasady bezpieczeństwa, opisane w normie PN-EN ISO 13849-2, stąd taka metoda może budzić uzasadnione wątpliwości. W przypadku braku możliwości zastosowania powyższego podejścia, ostateczną – mało inżynierską metodą, jest zastosowanie

wartości domyślnej (tj. 10 lat), która jako bardzo niska – może powodować obniżenie PL walidowanego układu do poziomu nieakceptowalnego.

Problemy z wyznaczeniem MTTFd uwidaczniają się przede wszystkim wtedy, gdy w skład łańcucha bezpieczeństwa wchodzą urządzenia elektroniczne. Przykładami rozwiązań, które będą stwarzać ogromne trudności przy próbie walidacji są: układy sterujące i zasilające silnikami asynchronicznymi oparte na falownikach, serwonapędy, roboty przemysłowe czy sterowniki dedykowane do danych aplikacji. Z naszych kontaktów z wieloma producentami, możemy przypuszczać, że nie przeprowadzają oni badań swoich produktów, zapewne ze względu na długi czas badań i oczekiwania na wyniki, czy też ich niszczący charakter. Nie prowadzą także analiz np. metodą „zliczania części" (parts count method) – która z kolei jest bardzo pracochłonna i wymaga wszystkich danych niezawodnościowych dotyczących każdego z elementów wchodzących w skład gotowego produktu. Z tego powodu, w praktyce, wartości parametrów MTTFd czy DC tych elementów nie są dokładnie kalkulowane, a jedynie szacowane na akceptowalnym poziomie ufności.

Projektowane obecnie układy bezpieczeństwa maszyn przemysłowych składają się bardzo często z programowalnych układów elektronicznych (tzw. sterowników bezpieczeństwa). Przy takich rozwiązaniach, walidacji powinien zostać poddany również program wgrany do sterownika. Zastosowanie metody walidacji przez badanie („czarnej skrzynki"), polega tutaj na podaniu na wejścia sterownika wszystkich kombinacji sygnałów związanych z urządzeniami ochronnymi. O ile testowanie układu składającego się z niewielkiej liczby komponentów nie będzie kłopotliwe, to przy aplikacjach bardziej rozbudowanych może się okazać już niemal niewykonalna ze względu na czasochłonność. Wraz ze wzrostem skomplikowania układu, liczba kombinacji rośnie wykładniczo. Przy dziesięciu urządzeniach ochronnych, liczba kombinacji będzie wynosić 210 czyli ponad tysiąc możliwości. Zgodnie z PN-EN ISO 13849-2 powinniśmy przeanalizować dodatkowo typowe sekwencje sterowania (np. zamknij bramkę, zresetuj, uruchom napęd), a także możliwe do przewidzenia działania niewłaściwe i uszkodzenia urządzeń ochronnych. Sumując wszystkie powyższe wymagania możemy otrzymać liczbę kombinacji, dla których sprawdzenie okaże się nieakceptowalne pod względem czasu i pracochłonności.

Reasumując, normy PN-EN ISO 13849-1 i 13849-2 wprowadzają bardzo istotne zmiany powiązane z różnymi aspektami projektowanych układów sterowania związanych z bezpieczeństwem. Przy próbie ich stosowania w praktyce natrafimy na wiele problemów i trudności. Aby ich uniknąć możemy zastosować pewne rozwiązania bazujące na wiedzy i doświadczeniu całej firmy. Przede wszystkim powinniśmy tworzyć i uaktualniać bazę parametrów dla najczęściej wykorzystywanych komponentów. Implementujmy rozwiązania dla układów sterowania, które zostały przez nas sprawdzone i zwalidowane. W końcu, stosujmy metody obliczeniowe, które w praktyce pozwolą nam zaoszczędzić czas i pieniądze na przeprowadzanie skomplikowanych badań i testów.

LITERATURA

[1] PN-EN ISO 13849-1
[2] PN-EN ISO 13849-2