Normy wspierające projektowanie związanych z bezpieczeństwem w

ADRIAN GIERJATOWICZ
zastępca kierownika Regionu Północ
inżynier bezpieczeństwa zawodowego – automatyk
ELOKON Polska Sp. z o.o.

Obecnie istnieją dwie normy zharmonizowane z dyrektywą maszynową 2006/42/WE, których właściwe zastosowanie pozwala na domniemanie zgodności części układu sterowania związanej z bezpieczeństwem z wymaganiami punktu 1.2.1 załącznika I tej dyrektywy. Niniejszy punkt definiuje następujące wymaganie ogólne: „Układy sterowania muszą być zaprojektowane i wykonane w sposób, który zapobiegnie powstawaniu sytuacji zagrożenia" oraz podaje kilka dodatkowych wymagań szczegółowych. Najnowszymi normami wspierającymi spełnienie tego wymagania zasadniczego są PN-EN ISO 13849 (dwie części: PN-EN ISO 13849-1:2016-02 i PN-EN ISO 13849-2:2013-04) oraz PN-EN 62061:2008 wraz ze zmianami.

Pierwsza z norm powstała na bazie wycofanej normy PN-EN 954-1, w której stosowano wyłącznie jakościowe podejście do opisywania niezawodności części układów sterowania związanych z bezpieczeństwem za pomocą kategorii (ang. *category*). W celu przyporządkowania układowi lub jego części określonej kategorii należało wziąć pod uwagę jego strukturę oraz właściwości (np. zachowanie w warunkach wystąpienia defektu). PN-EN ISO 13849-1 rozwija to podejście poprzez wprowadzenie kilku parametrów ilościowych, które w połączeniu z kategoriami pozwalają na określenie niezawodności części układu sterowania związanego z bezpieczeństwem poprzez przypisanie jednego z pięciu poziomów niezawodności (ang. *performance level* – PL). PN-EN ISO 13849-2 dostarcza wytycznych do przeprowadzenia walidacji (sprawdzenia) zaprojektowanej/ocenianej części układu sterowania związanej z bezpieczeństwem. Zawiera ona również obszerny przykład procesu walidacji.

Druga z norm powstała na bazie serii norm PN-EN 61508, które posłużyły również do utworzenia słynnych norm

i ocenę układów sterowania sektorze maszynowym

serii PN-EN 61511, dedykowanych dla sektora procesowego. W PN-EN 62061 niezawodność części układu sterowania związanych z bezpieczeństwem określana jest za pomocą jednego z trzech poziomów nienaruszalności bezpieczeństwa (ang. *safety integrity level* – SIL).

Obydwie normy (PN-EN ISO 13849-1 i PN-EN 62061) wykorzystują probabilistyczne podejście do analizy funkcji bezpieczeństwa. Zarówno poziomy niezawodności według PN-EN ISO 13849-1 (od a do e, gdzie e oznacza największą niezawodność), jak i poziomy nienaruszalności bezpieczeństwa według PN-EN 62061 (od SIL1 do SIL3, gdzie SIL 3 oznacza największą niezawodność) odpowiadają określonym przedziałom wartości średniego prawdopodobieństwa wystąpienia uszkodzenia niebezpiecznego na godzinę (ang. *average probability of dangerous failure per hour* – PFH_D). Dodatkowo w załącznikach informacyjnych obydwu norm podano ten sam zakres wymagań zasadniczych dyrektywy maszynowej, których spełnienie jest możliwe dzięki zastosowaniu tych norm. Wobec tego, którą normę wybrać do analizy lub wsparcia projektowania części układu sterowania związanej z bezpieczeństwem? W celu uzyskania odpowiedzi na to pytanie należy wziąć pod uwagę ograniczenia techniczne każdej z norm, łatwość wykorzystania do analizy, preferencje związane z warunkami projektu oraz dostępność narzędzi do wspomagania analizy.

Wskazówki do stosowania norm

W starszych wydaniach PN-EN ISO 13849-1 zawarta była tabela, która przedstawiała zalecane zakresy stosowania obydwu norm, ale zrezygnowano z niej, gdyż przedstawione tam ograniczenia stały się nieaktualne. Między innymi złagodzono niektóre obostrzenia dotyczące możliwości wykorzystania normy PN-EN ISO 13849-1 do złożonych systemów elektronicznych. Obecnie wskazówek do stosowania norm można szukać w raporcie technicznym ISO/TR 23849, do którego docelowo ma być zamieszczone odwołanie w obydwu normach. W raporcie tym można również znaleźć wzmiankę o tym, że planowane jest połączenie obydwu norm. Zapowiadane prace już nawet zostały rozpoczęte i przyszłej normie łączącej obydwa standardy przydzielono numer IEC/ISO 17305, ale oficjalnie prace zostały przerwane. Na razie nie ma informacji, czy do połączenia kiedykolwiek dojdzie.

Zakres norm

Przede wszystkim przy wyborze normy do przeprowadzenia analizy lub projektowania układu sterowania należy zwrócić uwagę na zakresy obydwu norm. W przypadku PN-EN 62061 podano, że nie określa ona wymagań dotyczących działania nieelektrycznych elementów sterowania maszyny (tj. hydraulicznych, pneumatycznych itd.). Chociaż, zgodnie z uwagami zawartymi w normie, określone zasady i metodologię można zastosować do części systemów sterowania wykorzystujących technologie inne niż elektryczna. Natomiast PN-EN ISO 13849-1, zgodnie z jej zakresem, można stosować do każdej części układu sterowania związanej z bezpieczeństwem, niezależnie od wykorzystywanej technologii i energii (elektrycznej, hydraulicznej, pneumatycznej, mechanicznej) bez dodatkowych obostrzeń. W związku z tym niniejsza norma zawiera informacje ułatwiające analizę układów sterowania zawierających takie elementy – przykładowo w postaci szacowanych, podanych wprost wartości parametrów niezawodnościowych dla zaworów hydraulicznych i pneumatycznych. Drugim udogodnieniem związanym z zastosowaniem normy PN-EN ISO 13849 jest to, że w jej części drugiej podano narzędzia walidacji elementów i systemów zawierających elementy wykonane w technologii innej niż elektryczna.

Przystępność normy do wykorzystania

Kolejnym aspektem decydującym o wyborze normy do analizy układu sterowania może być łatwość użytkowania. Biorąc pod uwagę subiektywne odczucia wielu użytkowników obydwu norm, można uznać normę PN-EN ISO 13849-1 za przystępniejszą do wykorzystania. Może to być spowodowane kilkoma czynnikami. Pierwszym z nich może być fakt, że norma ta bazuje na normie PN-EN 954-1, z której przeniesiono koncepcję kategorii, a także m.in. wymagania dotyczące charakterystycznych funkcji bezpieczeństwa. Została ona opublikowana w połowie lat 90., czyli znacznie wcześniej niż pierwsza wersja PN-EN 62061, co przyczyniło się do zakorzeniania tych koncepcji w sektorze maszynowym i skutkowało łatwiejszym przejściem na normę PN-EN ISO 13849-1. Drugim aspektem decydującym o odbiorze tej normy jako łatwiejszej w wykorzystaniu mogą być liczne uproszczenia ułatwiające analizę. Przykładowo w normie PN-EN ISO 13849-1 zamieszczono tabelę pozwalającą w łatwy sposób określić tzw. pokrycie diagnostyczne (ang. *diagnostic coverage*

Podczas wyboru normy do analizy układów sterowania związanych z bezpieczeństwem warto zwrócić uwagę na wymaganą redukcję poziomu ryzyka, wyrażaną poprzez konieczny poziom niezawodności lub wskazany poziom nienaruszalności bezpieczeństwa, jaki mają zapewnić analizowane funkcje.

– DC) w zależności od rodzaju rozważanego podsystemu (wejściowy, logiczny, wyjściowy) i zastosowanej technologii (np. dla podsystemu wyjściowego zawór/stycznik). Natomiast wykorzystanie normy PN-EN 62061 wiąże się z koniecznością szacowania wartości tego parametru z definicji, według której jest to stosunek liczby wykrywanych uszkodzeń niebezpiecznych do liczby wszystkich uszkodzeń. Drugie podejście wymaga większych nakładów pracy polegającej głównie na analizie uszkodzeń. Kolejne ułatwienia wynikające z wykorzystania normy PN-EN ISO 13849-1 to m.in. kilka uproszczonych metod szacowania poziomu niezawodności funkcji bezpieczeństwa oraz możliwość przeprowadzenia analizy w przypadku braku niektórych danych niezawodnościowych komponentu.

Wymagana redukcja poziomu ryzyka

Podczas wyboru normy do analizy układów sterowania związanych z bezpieczeństwem warto również zwrócić uwagę na wymaganą redukcję poziomu ryzyka, wyrażaną poprzez wymagany poziom niezawodności lub wymagany poziom nienaruszalności bezpieczeństwa, jaki mają zapewnić analizowane funkcje. Jako że obydwie omawiane normy określają niezawodność układu sterowania poprzez wartość współczynnika PFH_D, istnieje możliwość transponowania niezawodności wyrażonej za pomocą PL do SIL i odwrotnie (z pewnymi ograniczeniami; patrz ISO/TR 23849). Niezależnie od przyjętej metody wyznaczania wymaganej niezawodności funkcji bezpieczeństwa, wiąże się to jednak z tym, że korzystając z PN-EN 62061, nie możemy w żadnym przypadku uzyskać tak niskiej akceptowalnej niezawodności układu sterowania jak w przypadku PN-EN ISO 13849-1. Dotyczy to sytuacji, kiedy oczekiwana redukcja poziomu ryzyka przez funkcję bezpieczeństwa jest niewielka – wymagane PL a. Przedział wartości parametru PFH_D dla PL a jest taki, że nie odpowiada żadnemu z poziomów nienaruszalności bezpieczeństwa według PN-EN 62061. W związku z tym może się okazać, że w przypadku mniej niezawodnych systemów korzystniej jest stosować normę PN-EN ISO 13849-1, ponieważ spełnienie wymagań sformułowanych w postaci SIL może okazać się niemożliwe, podczas gdy wymagania sformułowane w postaci PL mogą być możliwe do spełnienia.

Wybór normy może być również podyktowany czynnikami zewnętrznymi zależnymi od klienta (wewnętrznego lub zewnętrznego).

Stopień skomplikowania projektowanego lub analizowanego układu sterowania a dobór normy

Następnym kryterium jest stopień skomplikowania projektowanego lub analizowanego układu sterowania. Jeżeli części układu sterowania związanego z bezpieczeństwem nie mogą zostać przyporządkowane do żadnej ze struktur (kategorii) przewidzianych przez normę PN-EN ISO 13849-1 (przykładowo z powodu istnienia dodatkowych kanałów realizacji funkcji bezpieczeństwa), to istnieją co najmniej dwie możliwości rozwiązania tego problemu. Pierwsza z nich to przekształcenie rozważanego podsystemu do postaci dopasowanej do kategorii według PN-EN ISO 13849-1 (przykładowo poprzez pominięcie dodatkowych kanałów, co skutkuje błędem szacowania niezawodności „w bezpieczną stronę"). Inna możliwość to zastosowanie normy PN-EN 62061 i jednej z metod przez nią przewidzianych (np. analizę drzewa niezdatności, modele Markowa itd.). W tym przypadku otrzymuje się dokładniejsze wyniki szacowania niezawodności układu sterowania, co może być istotne, gdy konieczna jest znaczna redukcja ryzyka poprzez techniczne środki ochronne wykorzystujące ten układ.

Wybór normy może być również podyktowany czynnikami zewnętrznymi zależnymi od klienta (wewnętrznego lub zewnętrznego). Przykładowo zakładając, że projektowana część układu sterowania związana z bezpieczeństwem będzie częścią maszyny, która zostanie włączona do instalacji procesowej, gdzie niezawodność układów sterowania związanych z bezpieczeństwem procesu

określana jest poprzez SIL (według serii norm PN-EN 61511), to zasadniejsze, ze względu na jedną nomenklaturę, wydaje się stosowanie normy PN-EN 62061. Innym powodem zastosowania danej normy może być preferencja klienta wynikająca z wcześniejszej znajomości któregoś z omawianych standardów.

Dostępność oprogramowania wspierającego analizę z wykorzystaniem norm

Kolejnym potencjalnym czynnikiem mający wpływ na wybór pomiędzy normą PN-EN ISO 13849-1 a PN-EN 62061 może być dostępność oprogramowania wspierającego analizę z ich wykorzystaniem. W przypadku pierwszego ze standardów dostępne jest m.in. oprogra-

Prawidłowe zastosowanie przedmiotowych norm jest podstawą do domniemania zgodności z zasadniczymi wymaganiami dyrektywy maszynowej 2006/42/WE.

mowanie przygotowane przez Niemiecki Instytut Bezpieczeństwa i Higieny Pracy (IFA) o nazwie SISTEMA. Narzędzie przygotowano specjalnie z myślą o analizie według PN-EN ISO 13849-1. Zawarto w nim szereg udogodnień, z których ważniejsze to: tabele i normy wspomagające wprowadzanie danych do analizy, mechanizmy sprawdzające poprawność wprowadzonych danych i spełnienie wymagań jakościowych podsystemu, moduły generowania raportów, możliwość korzystania z baz danych różnych producentów komponentów. Te czynniki, w połączeniu z faktem, że oprogramowanie jest darmowe, zadecydowały o tym, że stało się ono najpopularniejszym narzędziem do przeprowadzania analiz zgodnie z PN-EN ISO 13849-1. Istnieją również inne programy umożliwiające analizę według tej normy. Przykładowo te przygotowane przez producentów komponentów. Występują one w formie aplikacji do zainstalowania na komputerze lub w formie aplikacji webowych. Umożliwiają one również analizę układów składających się z komponentów innych producentów (często poprzez import tych samych bibliotek, które wykorzystuje SISTEMA) oraz zawierają dane wspomagające analizę bez konieczności zaglądania do tabel w normie, ale jest ich mniej niż w przypadku oprogramowania SISTE-

Stosowanie niewłaściwej normy do wyznaczania wymaganej niezawodności funkcji bezpieczeństwa oraz do analizy tych funkcji jest częstym błędem.

MA. Z kolei w przypadku PN-EN 62061 brak dedykowanego oprogramowania do wsparcia analizy według tej normy. Istnieją oprogramowania darmowe, które umożliwiają analizę z wykorzystaniem uproszczonej metody przedstawionej w tym standardzie. Niestety, w przypadku chęci skorzystania z bardziej skomplikowanych metod, takich jak np. modele Markowa czy analiza drzewa niezdatności, konieczne jest skorzystanie z innego oprogramowania, które częstokroć jest płatne i składa się z różnych osobno licencjonowanych produktów.

Doświadczenia z wyboru i zastosowania norm

Obydwie normy określają wymagania dla projektowania i implementacji części układów sterowania związanych z bezpieczeństwem maszyn. Prawidłowe zastosowanie którejkolwiek z nich jest podstawą do domniemania zgodności z zasadniczymi wymaganiami dyrektywy maszynowej 2006/42/WE. Obydwie klasyfikują części układu sterowania związane z bezpieczeństwem realizujące funkcje bezpieczeństwa według poziomów, które są określone poprzez średnie prawdopodobieństwo wystąpienia uszkodzenia niebezpiecznego na godzinę. Dodatkowo, jak pokazuje doświadczenie z wielu analiz oraz przykład zawarty w raporcie technicznym ISO/TR 23849, wyniki uzyskane przy wykorzystaniu metodologii z obydwu norm są porównywalne. Różnice wynikają m.in. z uproszczeń zawartych w metodach oraz odmiennego podejścia obydwu norm do szacowania wartości niektórych parametrów. Przykładowo uwzględnienie wpływu błędów o wspólnej przyczynie (ang. *common cause failures* – CCF) na prawdopodobieństwo utraty funkcji bezpieczeństwa w normie PN-EN 62061 odbywa się w sposób stopniowany poprzez uwzględnienie w obliczeniach wartości współczynnika wrażliwości na uszkodzenia spowodowane wspólną przyczyną (β). Współczynnik ten przyjmuje różne wartości w zależności od zastosowanych metod zapobiegania. Natomiast w PN-EN ISO 13849-1 przyjęto domyślnie stałą wartość tego współczynnika, gdy według wymagań normy, układ posiada wystarczającą odporność na uszkodzenia o wspólnej przyczynie. Jeśli warunek nie jest spełniony w wystarczającym stopniu, to dalsza analiza układu w tej formie nie jest możliwa.

Niejednokrotnie podczas analizy zdarza się, że konieczne lub wygodne byłoby zastosowanie do jednych części układu sterowania związanych z bezpieczeństwem normy PN-EN ISO 13849-1, a do innych normy PN-EN 62061 (i normy serii norm pokrewnych PN-EN 61508). Przykładowo sytuacja taka może mieć miejsce, kiedy całościowo na łańcuch funkcji bezpieczeństwa składają się elementy o niskim stopniu skomplikowania, gdzie wygodniej byłoby zastosować normę PN-EN ISO 13849-1 i elementy złożone, gdzie konieczne jest zastosowane normy PN-EN 62061 ze względu na wysoki stopień skomplikowania. Inny ciekawy przypadek, gdzie może to mieć zastosowanie, to sytuacja, gdy w łańcuchu funkcji bezpieczeństwa redukującej ryzyko związane z zagrożeniami maszynowymi (mechanicznymi) znajdują się elementy, które biorą udział w funkcjach związanych z bezpieczeństwem procesowym (np. w przemyśle papierniczym). Najczęściej dotyczy to procesowych sterowników PLC, dla których producenci nie zawsze udostępniają dane niezawodnościowe według PN-EN ISO 13849-1 (PL), a jedynie określają niezawodność według poziomów nienaruszalności bezpieczeństwa (SIL). W takich przypadkach, biorąc pod uwagę wcześniejsze rozważania na temat zastosowania poszczególnych norm oraz wytyczne ISO/TR 23849, możliwe jest przeprowadzenie analizy z wykorzystaniem obydwu norm. Przytoczony raport stwierdza, że możliwa jest integracja nieskomplikowanych części układów sterowania związanych

z bezpieczeństwem (jako podsystemów), zaprojektowanych na odpowiedni PL według PN-EN ISO 13849-1 do elektrycznego systemu sterowania związanego z bezpieczeństwem zaprojektowanego według PN-EN 62061. Odwrotne działanie również jest dopuszczalne. Z kolei w przypadku złożonych podsystemów zaprojektowanych na odpowiedni SIL według PN-EN 61508, możliwa jest ich integracja jako podsystemów do układów analizowanych lub projektowanych zarówno według normy PN-EN ISO 13849-1, jak i PN-EN 62061.

Na zakończenie należy wspomnieć, że w przypadku niektórych maszyn może wystąpić konieczność wykonania analizy funkcji bezpieczeństwa zgodnie z normą PN-EN 954-1. Jest to związane z datą wprowadzenia maszyny do obrotu i okresami obowiązywania poszczególnych norm. Przeprowadzenie analizy układu sterowania maszyny według PN-EN ISO 13849-1 może okazać się niemożliwe dla maszyn, które zostały wprowadzone do obrotu przed wprowadzeniem tej normy, ponieważ dane komponentów wykorzystanych do jej konstrukcji niezbędne do przeprowadzenia takiej analizy nie będą dostępne (np. MTTFD). Producenci elementów układów sterowania (np. przekaźników bezpieczeństwa) nie mieli obowiązku ich podawania.

Stosowanie niewłaściwej normy do wyznaczania wymaganej niezawodności funkcji bezpieczeństwa oraz do analizy tych funkcji jest częstym błędem. Dobór właściwej normy należy oprzeć na okresach, w których jej stosowanie zapewniało domniemanie zgodności. Dla maszyn wprowadzonych do obrotu przed dniem 1 lipca 2007 r. zastosowanie mają wymagania zawarte w normie PN-EN 954-1. Dla maszyn, które wprowadzono do obrotu w okresie od 1 lipca 2007 r. do 31 grudnia 2011 r., akceptowalne jest spełnienie wymagań jednej z powyższych norm (tzw. okres przejściowy). Natomiast dla maszyn, które wprowadzono do obrotu od dnia 1 stycznia 2012 r. aktualne są wymagania zawarte w PN-EN ISO 13849-1.

Literatura

1. PN-EN ISO 13849-1:2016-02, Bezpieczeństwo maszyn – Elementy systemów sterowania związane z bezpieczeństwem – Część 1: Ogólne zasady projektowania.
2. PN-EN ISO 13849-2:2013-04, Bezpieczeństwo maszyn – Elementy systemów sterowania związane z bezpieczeństwem – Część 2: Walidacja.
3. PN-EN 954-1:2001, Maszyny – Bezpieczeństwo – Elementy systemów sterowania związane z bezpieczeństwem – Część 1: Ogólne zasady projektowania.
4. PN-EN 62061:2008, Bezpieczeństwo maszyn – Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem.
5. PN-EN 61508 (wszystkie części), Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem.
6. ISO/TR 23849:2010, Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery.
7. BGIA Report 2/2008e, Functional safety of machine controls – Application of EN ISO 13849.