Bezpieczeństwo funkcjonalne – awers i rewers

Tadeusz Missala

Na tle cyklu życia bezpieczeństwa i zmniejszania ryzyka urządzeń i procesów technicznych przedstawiono idee bezpieczeństwa funkcjonalnego. Omówiono wymagania dotyczące nienaruszalności bezpieczeństwa urządzeń związanych z bezpieczeństwem i wskazano podstawowe sposoby osiągania wymaganych parametrów bezpieczeństwa, których stosowania wymagają odnośne normy. Na zakończenie zarysowano zagadnienie walidacji bezpieczeństwa funkcjonalnego.

Programowalne urządzenia elektroniczne, stosowane w technice sterowania, technice ochrony człowieka i środowiska naturalnego oraz do zabezpieczenia obiektów przed awariami, stworzyły nowe wyzwania dotyczące niezawodności – tak w sferze realizacji urządzeń i oprogramowania, jak i w sferze oceny osiągniętych wyników. Bardzo wielka, a praktycznie nieskończona, liczba stanów w jakich urządzenia te mogą się znaleźć, w sposób istotny ogranicza wiarygodność sprawdzenia gotowego wyrobu, ograniczając ją do badań, które się stają wyrywkowymi w relacji do liczby stanów możliwych. Ocena bezpieczeństwa a posteriori została zastąpiona oceną a priori [1]. Bezpieczeństwo funkcjonalne jest dziś podstawowym podejściem do tego zagadnienia i zostało sformalizowane w postaci licznych norm międzynarodowych [2, 3, 4, 5].

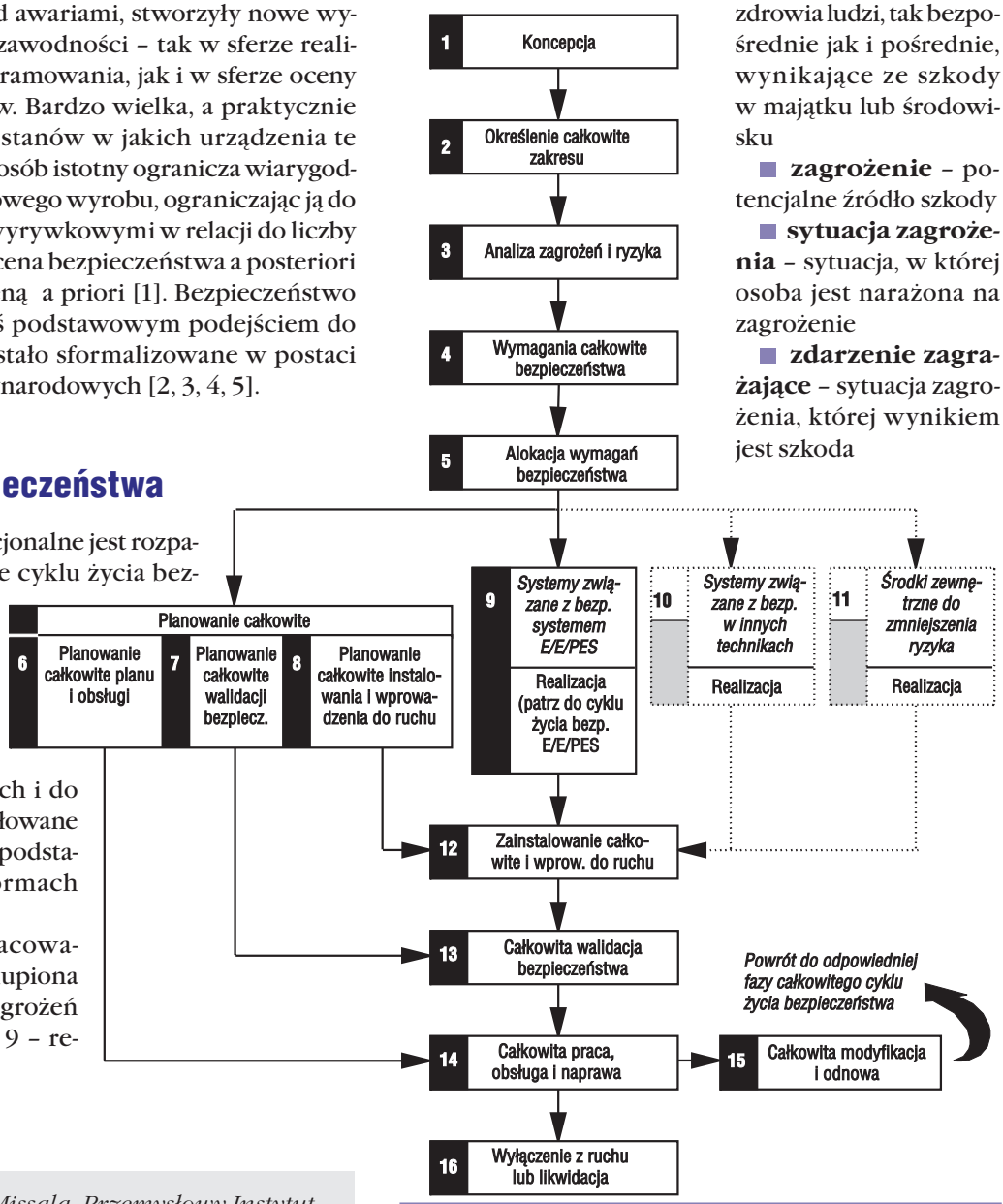
Cykl życia bezpieczeństwa

Bezpieczeństwo funkcjonalne jest rozpatrywane na podstawie cyklu życia bezpieczeństwa przedstawionego na rys. 1. Poszczególne fazy cyklu życia bezpieczeństwa są przedstawione za pomocą bloków funkcjonalnych i do każdej z nich są sformułowane wymagania w normie podstawowej [2] oraz w normach sektorowych [3, 4, 5].

W niniejszym opracowaniu uwaga zostanie skupiona na fazie 3 – analiza zagrożeń i ryzyka oraz na fazie 9 – realizacja.

W celu uniknięcia niejednoznaczności przytacza się kilka podstawowych definicji [1d].

- **szkoda** – fizyczny uraz lub pogorszenie stanu zdrowia ludzi, tak bezpośrednie jak i pośrednie, wynikające ze szkody w majątku lub środowisku
- **zagrożenie** – potencjalne źródło szkody
- **sytuacja zagrożenia** – sytuacja, w której osoba jest narażona na zagrożenie
- **zdarzenie zagrażające** – sytuacja zagrożenia, której wynikiem jest szkoda



Rys. 1. Cykl życia bezpieczeństwa urządzeń związanych z bezpieczeństwem

prof. dr inż. Tadeusz Missala, Przemysłowy Instytut Automatyki i Pomiarów, Warszawa

Tab. 1. Poziomy nienaruszalności bezpieczeństwa: docelowe miary uszkodzeń funkcji bezpieczeństwa

Poziom nienaruszalności bezpieczeństwa	Rodzaj pracy na rzadkie przywołanie (średnie prawdopodobieństwo uszkodzenia wykonania jego zaprojektowanej funkcji na żądanie)	Rodzaj pracy na częste przywołanie lub ciągły (prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę)
4	od $\geq 10^{-5}$ do $<10^{-4}$	od $\geq 10^{-9}$ do $<10^{-8}$
3	od $\geq 10^{-4}$ do $<10^{-3}$	od $\geq 10^{-8}$ do $<10^{-7}$
2	od $\geq 10^{-3}$ do $<10^{-2}$	od $\geq 10^{-7}$ do $<10^{-6}$
1	od $\geq 10^{-5}$ do $<10^{-1}$	od $\geq 10^{-6}$ do $<10^{-5}$

Tab. 2. Relacje rodzajów pracy systemów związanych z bezpieczeństwem

Rodzaj pracy	Typ systemu związanego z bezpieczeństwem	
	Sterowanie	Ochrona
Na rzadkie przywołanie	Wymaga się, aby system sterowania pracował w krótkich odstępach czasu, np. ABS.	Systemy ochronne, których liczba zadziałań jest mała w porównaniu z liczbą testów sprawdzających (np. system odcięcia instalacji chemicznej)
Ciągły/na częste przywołanie	Wymaga się, aby system pracował mniej lub więcej ciągle w długich przedziałach czasu, np. stymulator pracy serca.	Systemy ochronne, których liczba zadziałań jest duża w porównaniu z liczbą testów sprawdzających (np. fotoelektryczny system ochrony maszyny)

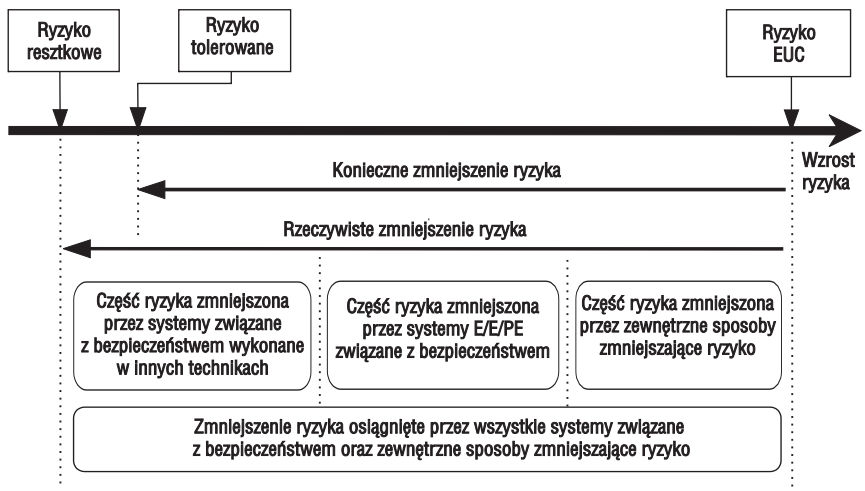
- **ryzyko** – kombinacja prawdopodobieństwa wystąpienia szkody i ciężkości tej szkody
- **ryzyko tolerowane** – ryzyko, które jest akceptowane w określonym kontekście opartym na aktualnych wartościach społecznych
- **ryzyko obiektu** – ryzyko pochodzące od obiektu sterowanego lub jego współdziałania z układem sterowania
- **bezpieczeństwo funkcjonalne** – część bezpieczeństwa całkowitego odnosząca się do obiektu sterowanego i systemu sterowania obiektem, która zależy od prawidłowego działania systemów elektrycznych/elektronicznych/programowalnych elektronicznych związanych z bezpieczeństwem, systemów związanych z bezpieczeństwem wykonanych w innych technikach i zewnętrznych środków zmniejszania ryzyka
- **nienaruszalność bezpieczeństwa** – prawdopodobieństwo, że system związany z bezpieczeństwem wykona w sposób zadowalający wymagane funkcje bezpieczeństwa we wszystkich określonych warunkach i w określonym przedziale czasu
- **poziom nienaruszalności bezpieczeństwa** – poziom dyskretny (jeden z czterech możliwych) do wyszczególniania wymagań nienaruszalności bezpieczeństwa funkcji bezpieczeństwa, przy czym poziom nienaruszalności bezpieczeństwa 4 jest poziomem najwyższym, a poziom nienaruszalności bezpieczeństwa 1 jest poziomem najniższym.

Poziomy nienaruszalności bezpieczeństwa są zdefiniowane, w zależności od rodzaju pracy urządzeń związanych z bezpieczeństwem, przez parametry zamieszczone w tab. 1 [2]. Rodzaj pracy na rzadkie przywołanie jest charakterystyczny w przypadku urządzeń i systemów zabezpieczeń, na przykład w przemysłach procesowych [3], rodzaj pracy na częste przywołanie lub ciągły występuje w przemyśle maszynowym [4] i zabezpieczeniach trakcyjnych [5]. Relacje między nimi przedstawiono w tab. 2. Źródła uszkodzeń to: błędy ludzkie, uszkodzenia przypadkowe i uszkodzenia systematyczne sprzętu i oprogramowania.

Bezpieczeństwo funkcjonalne a zmniejszanie ryzyka

Podstawowy schemat procesu zmniejszania ryzyka został przedstawiony na rys. 2 [2e, 6]. Przy analizie zagrożeń i ryzyka należy wziąć pod uwagę wszystkie rodzaje zagrożeń, jakie mogą wystąpić z powodu:

- oddziaływania środowiska – wpływy czynników mechanicznych, elektromagnetycznych, chemicznych, termicznych i ewentualne innych, jakie niesie środowisko



Rys. 2. Ogólny schemat zmniejszania ryzyka

– odchyleń w przebiegu procesu produkcyjnego – np. niespodziewana zwyżka prędkości obrotowej silnika napędowego, nieoczekiwana zwyżka ciśnienia w instalacji, powstanie nieszczelności w instalacji.

System związany z bezpieczeństwem powinien zapewnić poziom ryzyka tolerowanego przy działaniu wszystkich zidentyfikowanych zagrożeń.

Projekt systemu – co jest wymagane, na co zwrócić uwagę

Eliminowanie błędów ludzkich

Podstawowymi źródłami błędów popełnianych przez człowieka są: brak dostatecznych umiejętności oraz czynniki psychofizyczne m.in. zmęczenie, rozproszenie uwagi wskutek zdenerwowania lub trudności życiowych, prowadzące do postępowania nieuważnego. Drogami eliminowania błędów ludzkich są powierzanie pracy ludziom odpowiednio wykwalifikowanym oraz weryfikacja projektu, kontrola bieżąca produkcji, ocena i audity realizacji faz cyklu życia bezpieczeństwa. Ażeby powyższe czynności przynosiły pożądany skutek, ocena i audity powinny być przeprowadzane z zachowaniem odpowiedniego stopnia niezależności między osobami realizującymi i osobami sprawdzającymi. Wymagany poziom niezależności przedstawiono w tab. 3 [2a].

Tab. 3. Minimalne poziomy niezależności wykonujących ocenę bezpieczeństwa funkcjonalnego

Minimalny poziom niezależności	Poziom nienaruszalności bezpieczeństwa (SIL)			
	1	2	3	4
Osoba niezależna	HR	HR	NR	NR
Wydział niezależny	–	HR	HR	NR
Organizacja niezależna	–	–	HR	HR
HR – wysoce zalecane, NR – niezalecane				

Eliminowanie uszkodzeń – uwagi ogólne

Projekt systemu związanego z bezpieczeństwem, obejmujący sprzęt i oprogramowanie, powinien zapewniać:

(a) wystarczającą nienaruszalność bezpieczeństwa sprzętu obejmującą:
  – architekturę o akceptowanych ograniczeniach nienaruszalności bezpieczeństwa sprzętu
  – akceptowane prawdopodobieństwo niebezpiecznych przypadkowych uszkodzeń sprzętu

(b) wystarczającą nienaruszalność bezpieczeństwa systematyczną obejmującą:
  – unikanie uszkodzeń
  – kontrolę uszkodzeń
  – dowody, że urządzenia są „sprawdzone w użytkowaniu"

(c) wymagane zachowanie się systemu po wykryciu defektu.

Należy zachować ponadto następujące warunki:
– gdy implementuje się zarówno funkcje bezpieczeństwa jak i funkcje nie związane z bezpieczeństwem, to cały system należy traktować jako związany z bezpieczeństwem, chyba że można wykazać niezbicie, że uszkodzenia funkcji niezwiązanych z bezpieczeństwem nie mają wpływu na funkcje bezpieczeństwa
– gdy implementuje się funkcje bezpieczeństwa o różnym SIL, to cały system należy traktować jako mający najwyższy SIL, chyba że można wykazać niezbicie, przez podanie i uzasadnienie metody osiągnięcia niezależności funkcji, że uszkodzenia funkcji o niższym SIL nie zakłócają działania funkcji o najwyższym SIL.

Ograniczenia nienaruszalności bezpieczeństwa związane z architekturą

Są tu dwa źródła ograniczeń: skończona tolerancja sprzętu na defekty oraz udział uszkodzeń bezpiecznych, tj. nie powodujących zagrożenia. Ze względu na ocenę ograniczeń wynikających z architektury, podsystemy składowe dzieli się na typy A oraz B.

Podsystem może być traktowany jako podsystem typu A, jeśli spełnia wszystkie następujące warunki:
– rodzaje uszkodzeń wszystkich jego elementów są dobrze zdefiniowane
– zachowanie się systemu w warunkach defektu może być całkowicie określone
– są wystarczająco pewne dane zebrane z eksploatacji, dotyczące uszkodzeń, które pozwalają ocenić intensywności uszkodzeń niebezpiecznych wykrytych i niewykrytych.

Tab. 4. Nienaruszalność bezpieczeństwa sprzętu: ograniczenia architektoniczne podsystemów związanych z bezpieczeństwem typu A

Udział uszkodzeń bezpiecznych	Tolerancja defektów sprzętu (patrz uwaga)		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % – < 90 %	SIL2	SIL3	SIL4
90 % – < 99 %	SIL3	SIL4	SIL4
≥ 99 %	SIL3	SIL4	SIL4
UWAGA: Tolerancja N defektów sprzętu oznacza, że N + 1 defektów mogłoby spowodować utratę funkcji bezpieczeństwa			

Tab. 5. Nienaruszalność bezpieczeństwa sprzętu: ograniczenia architektoniczne podsystemów związanych z bezpieczeństwem typu B

Udział uszkodzeń bezpiecznych	Tolerancja defektów sprzętu (patrz uwaga w tablicy 4)		
	0	1	2
< 60 %	Niedozwolone	SIL1	SIL2
60 % – < 90 %	SIL1	SIL2	SIL3
90 % – < 99 %	SIL2	SIL3	SIL4
≥ 99 %	SIL3	SIL4	SIL4

System niespełniający dowolnego jednego z tych warunków zalicza się do typu B. W tab. 4 i tab. 5 [2b] przedstawiono ograniczenia wynikające z architektury.

Ocena prawdopodobieństwa niebezpiecznych przypadkowych uszkodzeń sprzętu

Ocenę tę wykonuje się biorąc pod uwagę:
- architekturę systemu
- oszacowaną intensywność uszkodzeń każdego podsystemu, w każdym rodzaju pracy
- podatność systemu na uszkodzenia spowodowane wspólną przyczyną
- pokrycie diagnostyczne testów diagnostycznych
- odstępy wykonywania testów sprawdzających w celu wykrycia defektów niebezpiecznych, nie wykrytych testami diagnostycznymi
- czasy napraw uszkodzeń wykrytych
- prawdopodobieństwo nie wykrytego uszkodzenia każdego procesu komunikacji
- możliwość wprowadzenia redundancji.

Jako przykład może posłużyć pracujący w sposób ciągły sterownik programowalny scharakteryzowany następująco [2f]:
- intensywność uszkodzeń na godzinę: λ = 1,0E10-07
- udział uszkodzeń niewykrytych mających wspólną przyczynę: β = 10 %
- udział uszkodzeń wykrytych mających wspólną przyczynę: β_D = 5 %
- odstęp między testami okresowymi: 3 miesiące.

W zależności od pokrycia diagnostycznego (DC) i typu redundancji otrzymuje się prawdopodobieństwo uszkodzenia na godzinę podane w tab. 6.

Tab. 6. Przykład – prawdopodobieństwo uszkodzenia na godzinę

Rodzaj redundancji	Pokrycie diagnostyczne (%)			
	0	60	90	99
1oo1	5,0E10-08	2,0E10-08	5,0E10-9	5,0E10-10
1oo2	5,0E10-09	3,5E10-09	2,8E10-09	2,5E10-09
2oo2	1,0E10-07	4,0E10-08	1,0E10-08	1,0E10-09
2oo3	5,0E10-09	3,5E10-09	2.8E10-09	2,5E10-09

Unikanie uszkodzeń

W przypadku podsystemów, których nie można uważać za wypróbowane (sprawdzone w praktyce), należy przy projektowaniu i realizacji systemu zastosować metody przeznaczone do zapobiegania wprowadzaniu, na tych etapach, defektów sprzętu. Te metody powinny zapewnić m.in:
- uzyskanie transparentności, modularności i innych cech ułatwiających kontrolę złożoności systemu
- jasne i dokładne przedstawienie wykonywanych funkcji, interfejsów do podsystemów, sekwencjonowania zdarzeń, informacji o przebiegach w czasie, współbieżności i synchronizacji
- jasną i dokładną dokumentację i wymianę informacji
- weryfikację i walidację projektu i wykonanego systemu
- opracowanie wytycznych dotyczących obsługi zapewniającej utrzymanie bezpieczeństwa funkcjonalnego
- zaplanowanie testów integracyjnych.

Kontrola defektów systematycznych

W przypadku podsystemów, których nie można uważać za wypróbowane, należy zapewnić kontrolę defektów systematycznych. W tym celu projekt systemu powinien mieć cechy, które uczynią system odporny na:
- wszystkie niedostrzeżone błędy projektowe pozostałe w sprzęcie
- narażenia środowiskowe, łącznie z zaburzeniami elektromagnetycznymi
- pomyłki popełniane przez operatora
- wszystkie defekty projektowe pozostałe w oprogramowaniu
- dowolne inne błędy i efekty pojawiające się w procesach wymiany danych.

Zachowanie się systemu w odniesieniu do wykrywania defektu

Wykrycie defektu niebezpiecznego w dowolnym podsystemie, który ma tolerancję defektów większą niż zerowa, powinno dawać jako wynik:
–określone, przewidziane z góry działanie w celu osiągnięcia lub utrzymania stanu bezpiecznego, lub
–izolowanie wadliwej części podsystemu, aby umożliwić bezpieczną pracę aż do usunięcia defektu.

Wykonywanie oprogramowania – na co zwrócić uwagę

Wybrana metoda projektowania powinna mieć właściwości ułatwiające m.in. [2c]:
- zarządzanie złożonym projektem, np. przez podział oprogramowania na moduły
- wyrażanie: funkcjonalności, przepływu informacji między składnikami, struktury danych, sekwencjonowania, konfliktów przy dostępie, ograniczeń
- weryfikacje i walidację
- testowanie i modyfikowanie, w tym funkcje oprogramowania przewidziane do testów sprawdzających.

Projekt powinien minimalizować do absolutnie niezbędnej wielkości tę część oprogramowania, która jest związana z bezpieczeństwem. Poziom nienaruszalności bezpieczeństwa oprogramowania powinien być co najmniej równy poziomowi nienaruszalności bezpieczeństwa funkcji bezpieczeństwa, do której przynależy. W tym celu należy wybierać stosowny język programowania, techniki projektowania i wytwarzania oraz weryfikacji i walidacji. Dobór technik odpowiednich do oczekiwanych poziomów nienaruszalności bezpieczeństwa podaje norma [2c].

Gdy w oprogramowaniu mają być zaimplementowane funkcje bezpieczeństwa i funkcje nie będące funkcjami bezpieczeństwa, to całe oprogramowanie należy traktować jako związane z bezpieczeństwem, chyba że można wykazać niezbicie odpowiednią niezależność między nimi. Podobnie, jeśli w oprogramowaniu implementuje się funkcje bezpieczeństwa o różnych SIL, to całe oprogramowanie należy traktować jako przynależne do najwyższego poziomu nienaruszalności bezpieczeństwa, chyba że można udowodnić niezbicie odpowiednią niezależność.

Dowody niezależności w obu przypadkach powinny być dobrze udokumentowane.

Kod źródłowy oprogramowania powinien być czytelny, zrozumiały i testowalny oraz spełniać wszystkie wymagania wynikające z przyjętego poziomu nienaruszalności bezpieczeństwa.

Kompatybilność elektromagnetyczna

Istotnym zagadnieniem przy projektowaniu i wykonywaniu systemów elektrycznych, elektronicznych i programowalnych elektronicznych jest zapewnienie właściwej kompatybilności elektromagnetycznej, to jest nie emitowania zaburzeń o niedopuszczalnych poziomach i właściwej pracy w środowisku do którego system jest przeznaczony. Odpowiednie działania powinny być realizowane w każdej fazie cyklu życia bezpieczeństwa systemu związanego z bezpieczeństwem. Zagadnienie zapewnienia kompatybilności elektromagnetycznej jest zagadnieniem zbyt obszernym do przedstawienia tutaj. Czytelnika należy odesłać do literatury [7, 8, 9].

Weryfikacja i walidacja

Wykonane: projekt, oprogramowanie oraz dokumentacja eksploatacyjna podlegają weryfikacji i walidacji. Weryfikacja mająca za zadanie usunięcie możliwie wszystkich pomyłek i niedociągnięć, które mogą powstawać w trakcie projektowania, realizacji, integracji i testowania systemu elektrycznego, elektronicznego lub programowalnego elektronicznego związanego z bezpieczeństwem, powinna być wykonywana po zrealizowaniu każdej fazy cyklu życia bezpieczeństwa systemu. Weryfikacja powinna być wykonywana według planu weryfikacji, opracowanego wcześniej i udokumentowana.

Walidacja ma za zadanie sprawdzenie, o ile to jest możliwe, że system jest odpowiedni do przewidzianego zastosowania, to znaczy będzie niezawodnie pracować w warunkach środowiskowych jego przewidzianego zastosowania.

Walidacja powinna przebiegać według planu opracowanego w fazie planowania (patrz rys. 1) i zawierać analizę dokumentacji oraz próby laboratoryjne i/lub obiektowe. Próby powinny obejmować:
- próby funkcjonalne
- próby współpracy z innymi urządzeniami i systemami, z którymi walidowany system ma współpracować
- próby odpornościowe: klimatyczne, mechaniczne, termiczne i kompatybilności elektromagnetycznej.

Poziomy narażeń przy próbach odpornościowych należy dobierać odpowiednio do przewidywanych warunków pracy i na podstawie norm [10]. Walidacja kompatybilności elektromagnetycznej powinna przebiegać zgodnie z ostatnio opracowanymi normami [11].

Zakończenie

Przedstawiono w zarysie zagadnienie bezpieczeństwa funkcjonalnego elektrycznych, elektronicznych i programowalnych elektronicznych systemów związanych z bezpieczeństwem, wskazując na parametry użytkowe (awers – to co widzi użytkownik) i wybrane aspekty projektowania i wykonania (rewers – to co widzi wykonawca).

Bibliografia

1. Missala T.: Ocena a priori i a posteriori bezpieczeństwa robota. Prace Naukowe Instytutu Cybernetyki Stosowanej Politechniki Wrocławskiej, Nr 99. Prace VI Krajowej Konferencji Robotyki, t.2. s.133-148, Wrocław wrzesień 1998 r.
2. PN-EN 61508 (IEC 61508): Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem:
   (a) PN-EN 61508-1:2004 – Część 1: Wymagania ogólne
   (b) PN-EN 61508-2:2005 – Część 2: Wymagania dotyczące elektrycznych/elektronicznych/ programo-

walnych elektronicznych systemów związanych z bezpieczeństwem
   (c) PN-EN 61508-3:2004 – Część 3: Wymagania dotyczące oprogramowania
   (d) PN-EN 61508-4:2004 – Część 4: Definicje i skrótowce
   (e) PN-EN 61508-5:2005 – Część 5: Przykłady metod określania poziomów nienaruszalności bezpieczeństwa
   (f) PN-EN 61508-6:2007 – Część 6: Wytyczne do stosowania IEC 61508-2 i IEC 61508-3
   (g) PN-EN 61508-7:2003(U) – Część 7: Przegląd technik i miar
3. PN-EN 61511 (IEC 61511): Bezpieczeństwo funkcjonalne. Przyrządowe systemy bezpieczeństwa do sektora przemysłów procesowych:
   (a) PN-EN 61511-1:2007 – Część 1: Schemat, definicje, wymagania dotyczące systemu, sprzętu i oprogramowania
   (b) PN-EN 61511-2:2005(U) – Część 2: Wytyczne do stosowania IEC 61511-1
   (c) PN-EN 61511-3:2005(U) – Część 3: Wytyczne do określania poziomów nienaruszalności bezpieczeństwa
4. PN-EN 62061:2005(U) Bezpieczeństwo maszyn – Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i programowalnych elektronicznych systemów sterowania związanych z bezpieczeństwem
5. PN-EN 50129:2007 Zastosowania kolejowe – Systemy łączności, przetwarzania danych i sterowania ruchem – Elektroniczne systemy sterowania ruchem związane z bezpieczeństwem
6. PN-EN 1050:1999 Maszyny – Bezpieczeństwo – Zasady oceny ryzyka
7. IEC 61000-1-2 Ed.2 (77/344/CD) Electromagnetic compatibility – General – methodology for the achievement of the functional safety of electrical and electronic equipment with regard to electromagnetic phenomena.
8. Missala T.: Aspekty kompatybilności elektromagnetycznej w bezpieczeństwie funkcjonalnym. Przegląd Elektrotechniczny, R. 83 nr 9/2007, s. 4-9.
9. Missala T.: Electromagnetic Compatibility versus Functional Safety – interactions problems. Monografia wyd. Komitetu Bezpieczeństwa Funkcjonalnego, Gdańsk , s. 115–132.
10. PN-EN 60654 Urządzenia do pomiarów i sterowania procesami przemysłowymi – Warunki pracy:
   (a) PN-EN 60654-1:1996 Warunki klimatyczne
   (b) PN-EN 60654-1:1999 Zasilanie
   (c) PN-EN 60654-3:2000 Czynniki mechaniczne
   (d) PN-EN 60654-4:2000 Czynniki korozyjne i erozyjne
11. IEC 61326 Electrical equipment for measurement, control and laboratory use – EMC requirements:
   (a) Part 3-1:2008 Immunity requirement for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – General industrial applications;
   (b) Part 3-2:2008 Immunity requirement for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – Industrial applications with specified electromagnetic environment.