Nowe unormowania w zakresie bezpieczeństwa funkcjonalnego – wynik postępu technicznego

Tadeusz Missala

Przemysłowy Instytut Automatyki i Pomiarów PIAP

Streszczenie: Scharakteryzowano zmiany wprowadzone w ciągu ostatnich 5 lat w normach bezpieczeństwa funkcjonalnego: serii podstawowej IEC 61508, sterowników programowalnych, sieci komunikacyjnych i wymagań kompatybilności elektromagnetycznej.

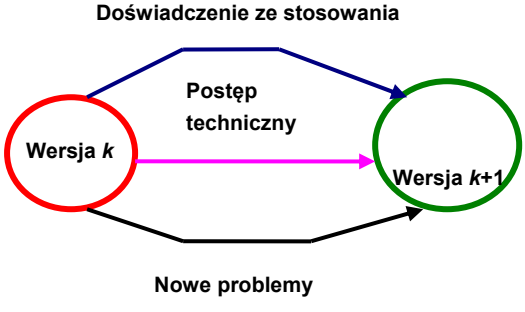
Słowa kluczowe: automatyka przemysłowa, bezpieczeństwo, bezpieczeństwo funkcjonalne, normalizacja, postęp techniczny

1. Wprowadzenie

Globalizacja gospodarki światowej, kolejne znoszenie barier w międzynarodowej wymianie towarów i usług powodują, że normalizacja międzynarodowa ma coraz większe znaczenie. Dążeniem międzynarodowych organizacji normalizacyjnych (IEC, ISO, UIT, CENELEC, CEN, ETSI) jest, aby normy odzwierciedlały możliwie wiernie aktualny stan techniki. Przyjęto więc procedurę okresowego, pięcioletniego przeglądu aktualności norm i trzyletniego raportów technicznych. W czasie przeglądu, na podstawie głosowania przez Komitety Krajowe, podejmuje się decyzje w zakresie:

- utrzymania normy bez wprowadzania zmian,
- wykreślenia ze zbioru norm aktualnych,
- zastąpienia przez nowe wydanie,
- wprowadzenie zmian.

Podstawą do podejmowania decyzji są ścieżki postępowania zilustrowane na rys. 1.



Rys.1. Ścieżki postępowania do nowelizacji norm

Fig.1. Acting paths for standards amendment

Przegląd okresowy norm z dziedziny bezpieczeństwa funkcjonalnego został przeprowadzony w latach 2008–2010 i zakończył się nowymi wydaniami całego pakietu norm podstawowych i dotyczących kompatybilności elektromagnetycznej oraz projektem normy grupy wyrobów. Ponadto znowelizowano lub wprowadzono normy wspomagające.

Treścią niniejszego artykułu jest zaprezentowanie zakresu wprowadzonych zmian.

2. Zmiany w normach IEC 61508 [5]

2.1. Uwagi ogólne

Seria norm dotyczy Elektrycznych, Elektronicznych lub Programowalnych Elektronicznych (E/E/PE) systemów związanych z bezpieczeństwem. Pierwsze wydanie norm serii 61508 było opracowywane w latach 1985–2000 i było połączone z trudnymi dyskusjami wynikającymi z przenoszenia doświadczeń przemysłu rafineryjnego i nuklearnego na szerokie forum przemysłowe. To przeniesienie było konieczne w związku ze zwiększającym się asortymentem urządzeń, od których zależało bezpieczeństwo ludzi i środowiska naturalnego. Po kilkuletnim doświadczeniu w stosowaniu tych norm i wobec ogromnego postępu technicznego w elektronice naturalnym stało się opracowanie i wydanie nowego, istotnie uzupełnionego, wydania tych norm, co nastąpiło w 2010 r.

2.2. Zmiany w PN-EN 51508-1 [5a]

Ta norma ma charakter ogólny i porządkujący, wprowadza pojęcie cyklu życia bezpieczeństwa i formułuje wymagania dotyczące zarządzania bezpieczeństwem funkcjonalnym. Ogólne ramy, które wprowadziła, w tym wartości wymaganych parametrów niezawodnościowych, pozostały bez zmiany. Zaistniałe zmiany wynikają głównie z doświadczenia zdobytego przy stosowaniu serii norm i pytań jakie były zgłaszane na forum dyskusyjnym IEC, dotyczącym bezpieczeństwa funkcjonalnego.

Zmiany o charakterze ogólnym obejmują:

- dodanie stwierdzenia, że norma obejmuje systemy zabezpieczające/ochronne oraz systemy sterowania,
- wyraźne stwierdzenie, że norma nie obejmuje zagrożeń wynikających z samego systemu E/E/PE związanego z bezpieczeństwem, np. porażenia elektrycznego lub podatności na wpływy środowiskowe,
- stwierdzenie, że norma nie obejmuje zabezpieczenia przed działaniami nieuprawnionymi i złej woli, oraz że w tej sprawie należy odnieść się do norm serii IEC 62443 [7, 8, 9] (powyższe jest potwierdzeniem stanowiska autora niniejszego artykułu zaprezentowanego w publikacjach [12, 13]),
- wyłączenie urządzeń medycznych, które podlegają odrębnym przepisom.

Zmiany o charakterze bardziej szczegółowym, których wynikiem jest usunięcie niejasności, obejmują:

- wprowadzenie kroku „specyfikacja wymagań bezpieczeństwa systemu E/E/PE związanego z bezpieczeństwem", który poprzednio był ukryty w kroku „realizacja",
- zrezygnowanie z podziału na „systemy wykonane w innych technikach" i „inne środki zapewnienia bezpieczeństwa" i zastąpienie krokiem wspólnym „inne sposoby zmniejszenia ryzyka",
- w rozdziale „Zarządzanie bezpieczeństwem funkcjonalnym" szczegółowe sprecyzowanie wymagań dotyczących wyznaczania odpowiedzialności oraz kryteriów dotyczących kompetencji personelu,
- uproszczenie załącznika A, omawiającego sposoby aranżacji dokumentacji (dotychczasowy był niezmiernie skomplikowany) oraz pominięcie załącznika B „Kryteria doboru personelu" (patrz wyżej).

Istotną zmianą o charakterze technicznym są zapisy dotyczące przypadku, gdy z analizy ryzyka wynika zastosowanie systemu E/E/PE związanego z bezpieczeństwem implementującego funkcję bezpieczeństwa o poziomie nienaruszalności SIL 4. W tym przypadku norma nakazuje podjęcie następujących działań:

- Powtórnie przeanalizować aplikację w celu określenia, czy któryś z parametrów ryzyka może zostać zmodyfikowany na tyle, aby uniknąć wymagania poziomu SIL 4, przy czym należy rozważyć, czy można:
  - wprowadzić dodatkowe systemy związane z bezpieczeństwem lub inne środki zmniejszenia ryzyka, nieoparte na systemach E/E/PE związanych z bezpieczeństwem,
  - ograniczyć ostrość konsekwencji,
  - zmniejszyć prawdopodobieństwo wyszczególnionych konsekwencji.
- Jeśli powtórna analiza wykaże konieczność wprowadzenia funkcji bezpieczeństwa o poziomie SIL 4, to należy przeprowadzić ocenę ryzyka metodami jakościowymi, uwzględniającą potencjalne uszkodzenia o wspólnej przyczynie między rozpatrywanym systemem E/E/PE związanym z bezpieczeństwem i:
  - jakimkolwiek innym systemem, którego uszkodzenia mogłoby spowodować wezwanie,
  - jakimkolwiek innym systemem związanym z bezpieczeństwem.

Powyższe wymagania wynikają z faktu, że poziom nienaruszalności SIL 4 funkcji bezpieczeństwa jest niezmiernie trudny do utrzymania podczas eksploatacji.

2.3. Zmiany w PN-EN 61508-2 [5b]

Podstawową zmianą o charakterze technicznym, wynikającą z postępu technicznego w elektronice, jest objęcie normą podsystemów:

- układy scalone z redundancją na chipie (ang. *on-chips redundancy ICs*),
- układy ASIC,
- komunikacja.

Wymagania dotyczące układów scalonych zebrano w załączniku E – normatywnym „Wymagania specjalne na ICs z redundancją na chipie", na który powołano się w odpowiednich punktach wymagań zamieszczonych w normie. W nim przywołano również wymagania kompatybilności elektromagnetycznej wg PN-EN 61326-3-1[3]. Wymagania na ASIC zamieszczono w postaci rys. 3 przedstawiającego cykl życia bezpieczeństwa ASIC, załącznika F – informacyjnego „Techniki sposoby na unikania uszkodzeń systematycznych w ASIC" oraz odpowiednich powołań w tekście.

Wymagania odnoszące się do komunikacji rozszerzono przez m.in. powołanie na normę PN-EN 61784-3 [6] prezentującą bezpieczne funkcjonalnie profile Fieldbus.

Ponadto wprowadzono zmiany porządkowe:

- uzgodniono z nową wersją części 1,
- wymagania uporządkowano w sposób bardziej zrozumiały i czytelniejszy dla stosującego, w tym wyszczególniono i opisano szczegółowo ścieżki postępowania do uzyskania zgodności z wymaganiami w zakresie systemu i sprzętu,
- zwrócono uwagę na konieczność uwzględniania błędów ludzkich,
- wymagania EMC odniesiono do IEC/TS 61000-1-2 [14],
- dodano załącznik D porządkujący zawartość dokumentacji dla użytkownika.

2.4. Zmiany w PN-EN 61508-3 [5c]

W zakresie merytorycznym nastąpiły następujące zmiany:

- dodano nowe załączniki:
  - załącznik C – informacyjny, zawierający zestawienie wymagań na odporność na uszkodzenia systematyczne,
  - załącznik D – normatywny, zawierający wymagania uzupełniające zawartość podręcznika użytkownika w zakresie oprogramowania,
  - załącznik E – informacyjny, przedstawiający korelacje wymagań części 2 i części 3 IEC 61508,
  - załącznik F – informacyjny, zawierający zestawienie technik do osiągnięcia niezakłócania się wzajemnego przez elementy oprogramowania pojedynczego komputera,
  - załącznik G – przewodnik do dostosowania cyklu życia bezpieczeństwa do systemów sterowanych danymi,
- wprowadzono wymagania w zakresie:
  - przeprowadzenia analizy możliwości powstawania uszkodzeń o wspólnej przyczynie i obowiązku podjęcia kroków zaradczych,
  - zapewnienia zabezpieczenia (ang. security),
  - ścieżek osiągnięcia zgodności systemowej przez moduły oprogramowania poprzednio stosowanego,
  - walidacji i weryfikacji narzędzi wspomagających i języków programowania.

Ponadto:

- poprawiono redakcję wymagań, przez co stały się bardziej czytelne i zrozumiałe,
- dostosowano do zgodności z wymaganiami i redakcją nowego wydania cz. 1 i 2,

- uaktualniono załącznik A – normatywny, wytyczne do wyboru technik i sposobów.

2.5. Zmiany w PN-EN 61508-4 [5d]

Nowe wydanie normy zostało znacznie poszerzone w porównaniu ze starym. Zawiera ono definicje 105 pojęć, w porównaniu z 82 w poprzednim wydaniu oraz 35 akronimów w porównaniu z 7 w poprzednim wydaniu.

Obie listy uzupełniono definicjami pojęć nowo wprowadzonych do serii norm IEC61508, np. definicją ASIC, oraz definicjami pojęć i akronimów z części 5 i 6 poprzednio niezamieszczonych w części 4.

2.6. Zmiany w PN-EN 61508-5 [5e]

W tekście tej normy zaszły duże zmiany w kierunku jej uzupełnienia.

Pozostały dotychczas prezentowane metody analizy ryzyka i ustalania wymaganego poziomu nienaruszalności bezpieczeństwa (SIL):

- ALARP i koncepcja ryzyka tolerowalnego,
- określanie poziomów nienaruszalności bezpieczeństwa: metoda ilościowa,
- określanie poziomów nienaruszalności bezpieczeństwa – metoda jakościowa: graf ryzyka,
- określanie poziomów nienaruszalności bezpieczeństwa – metoda jakościowa: tablice krytyczności zdarzenia zagrażającego.

Wprowadzono nowy załącznik prezentujący metodę pół-ilościową stosującą Analizę Warstw Zabezpieczeń (LOPA) [11], dotychczas prezentowaną w PN-EN 61511-3 [15] dotyczącej bezpieczeństwa funkcjonalnego w przemyśle procesowym, dodano nowy załącznik – wybór metody, w którym zaprezentowano metody zawarte w normie. W szczególności na podkreślenie zasługuje rozszerzenie załącznika A – ryzyko i nienaruszalność bezpieczeństwa (koncepcje ogólne) – w którym zamieszczono koncepcje postępowania w przypadku systemów pracujących na rzadkie przywołanie, na częste przywołanie oraz w sposób ciągły oraz koncepcję postępowania przy uwzględnianiu uszkodzeń o wspólnej przyczynie i uszkodzeń zależnych; te dwie ostatnie koncepcje przedstawiono na rys. 2 i 3 (w wersji oryginalnej).

Niezależnie od tego uzgodniono redakcję z pozostałymi częściami omawianej serii norm.

2.7. Zmiany w PN-EN 61508-6 [5f]

W tej normie również wprowadzono istotne uzupełnienia. Dotychczasowy załącznik B – przykłady technik do oceny prawdopodobieństwa uszkodzeń sprzętu – który w zakresie metod wyznaczania nieuszkadzalności elementów i systemów zawierał tylko opis metody schematów blokowych niezawodności, uzupełniono o:

- metody boolowskie, w tym model drzewa uszkodzeń,
- metodę grafów Markowa,
- metodę sieci Petriego,
- symulację Monte Carlo.

oraz o wskazanie innych metod możliwych do stosowania, np. języka AllaRica Data Flow.

Załącznik D – Metodyka ilościowego określania skutków uszkodzeń... – został uzupełniony o metodę dwumianowej intensywności uszkodzeń – model szokowy (ang. *binomial failure rate – shock model*). Ponadto dokonano odpowiedniego dopasowania redakcyjnego załącznika A – Zastosowanie IEC 61508-2 i IEC 61508-3 do zmienionej treści tych norm.

2.8. Zmiany w PN-EN 61508-7 [5g]

Ta norma jest właściwie informatorem bibliograficznym do pozostałych części serii IEC 61508 i oczywiście została odpowiednio poszerzona. Zmian tych nie będzie się prezentować szczegółowo.

3. Normy związane i uzupełniające

3.1. Uwagi ogólne

W czasie końcowych etapów opracowania serii IEC 61508 i okresu początkowego ich stosowania pojawiła się potrzeba opracowania i wprowadzenia norm:

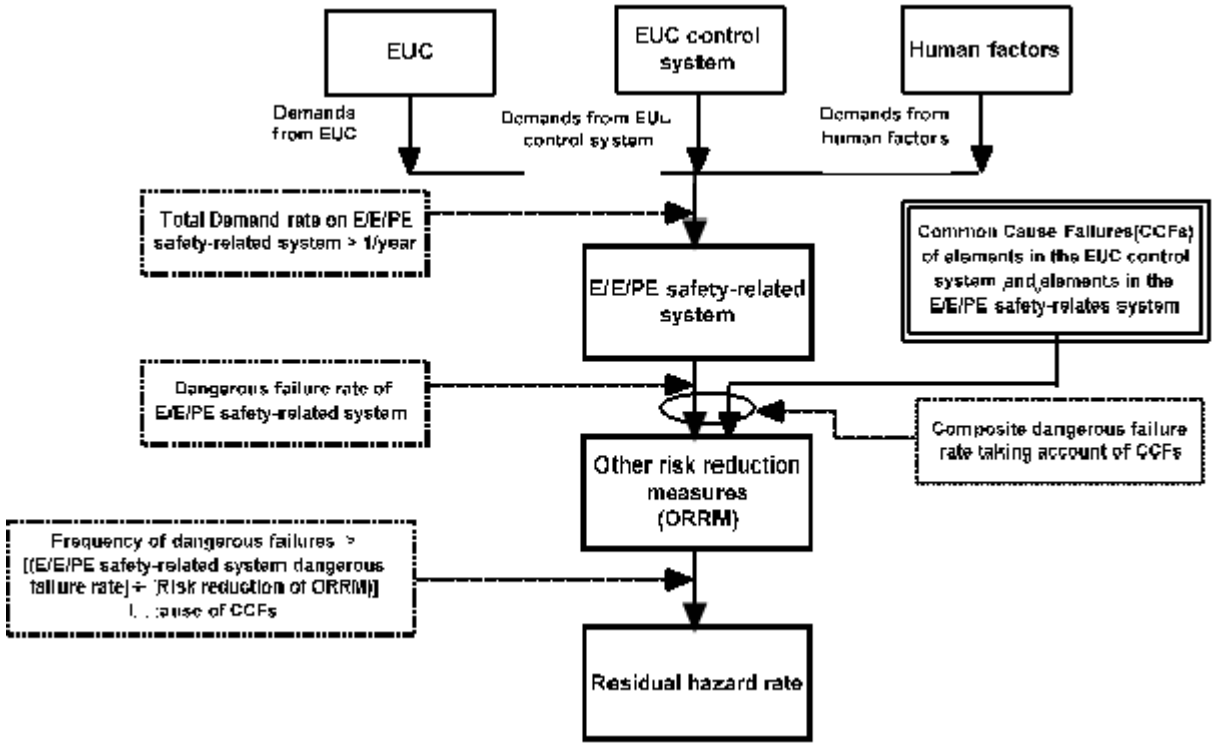
- dostosowujących wymagania norm ogólnych do potrzeb określonych obszarów gospodarczych, tzw. norm sektorowych,
- dostosowujących wymagania jw. do określonej dużej grupy urządzeń,
- określających wymagania, badania i kryteria zgodności, umożliwiające efektywną walidację systemów związanych z bezpieczeństwem.

Normy sektorowe (przemysły procesowe, maszyny, kolejnictwo, technika nuklearna itp.) stanowią obszerny obszar normalizacyjny i ich omówienie wykracza poza ramy niniejszego referatu. Wykaz tych norm jest podany np. w bibliografii do [11]. Tu zostaną pokrótce przedstawione pozostałe dwie grupy norm.

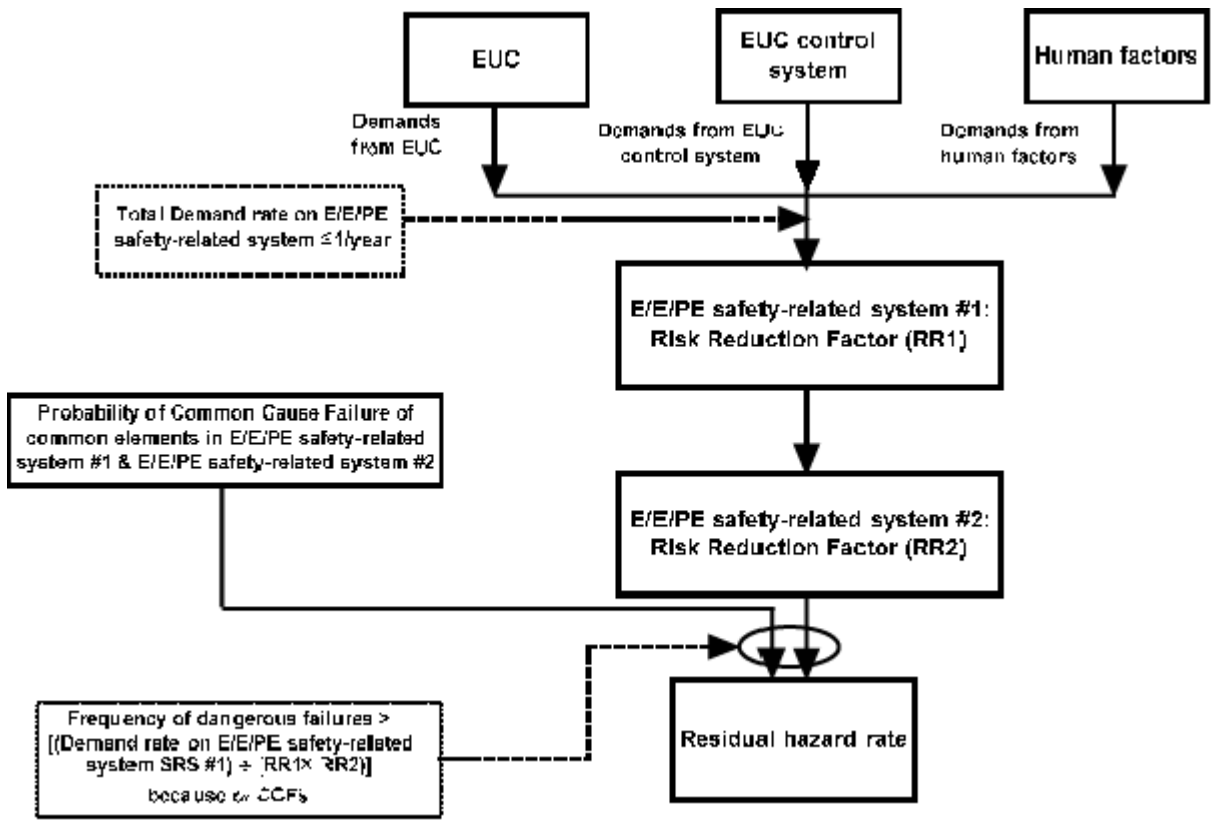
3.2. Norma grupy wyrobów – sterowniki programowalne [16]

Sterowniki programowalne są tak dużą grupą wyspecjalizowanych urządzeń automatyki, że odczuwało się potrzebę opracowania normy dostosowującej do nich wymagania norm ogólnych serii IEC 61508. Ze względu na konieczność uzyskania dostatecznego doświadczenia ze stosowania norm podstawowych i na trwającą ich nowelizację, finalizacja prac normalizacyjnych może następować dopiero obecnie. W październiku 2011 r. zakończyło się głosowanie nad dokumentem o statusie CDV (ang. *Committee Draft for Voting*). Omawiany projekt normy obejmuje:

- schemat cyklu życia bezpieczeństwa PLC integrujący wymagania wynikające z cz. 1, 2, 3 serii IEC 61508,
- badania do walidacji bezpieczeństwa PLC: nienaruszalność bezpieczeństwa, klimatyczne, mechaniczne, EMC,
- przykłady architektur z wyjściami 1oo1D, 1oo2, 1oo2D, 2oo2, 2002D, 2oo3D i ich ocena,
- wykaz dostępnych baz danych niezawodności.



Rys. 2. Postępowanie przy uwzględnianiu uszkodzeń o wspólnej przyczynie
Fig. 2. Acting for consideration of common cause failures



Rys. 3. Postępowanie przy uwzględnianiu uszkodzeń zależnych
Fig. 3. Acting for consideration of dependent failures

Całość jest zredagowana w sposób ułatwiający projektantowi zrealizowanie bezpieczeństwa funkcjonalnego, a oceniającemu – wykonanie oceny.

3.3. Norma grupy wyrobów – profile komunikacyjne bezpieczne

Norma wydana w 2008 r. została znowelizowana w roku 2010 równolegle z nowelizacją norm serii IEC 61508. Omawiana norma precyzuje zasady tworzenia komunikacji bezpiecznej funkcjonalnie przez wprowadzanie dodatkowej warstwy oprogramowania realizującej tę funkcję. Zaprezentowano w niej modele takich realizacji. Wprowadza ona wymagania dotyczące dopuszczalnych prawdopodobieństw uszkodzeń niebezpiecznych na godzinę i dopuszczalnych błędów resztkowych w sieci bezpiecznej funkcjonalnie, w zależności od deklarowanego poziomu nienaruszalności bezpieczeństwa SIL przy zasadzie, że parametry te mają zapewnić, iż transmisja nie wprowadzi dodatkowej podatności na uszkodzenia przekraczającej 1 % podatności podstawowej systemu związanego z bezpieczeństwem. Te parametry są identyczne jak w poprzednim wydaniu normy.

W omawianej normie ustalono i scharakteryzowano 8 profili realizacji komunikacji bezpiecznej funkcjonalnie. Są to profile sieci: Fieldbus Foundation, CIP, Profibus i Profinet, Interbus, CC-LINK, Ether-CAT, Ethernet Powerlink i EPA. Szczegółowe specyfikacje odpowiednich protokołów są przedmiotem norm podporządkowanych omawianej normie, również zaktualizowanych z datą 2010 r.

W celu ułatwienia i ujednolicenia oceny bezpieczeństwa funkcjonalnego sieci wydano stosowny raport techniczny [18].

Ponadto została wydana norma europejska [19], niepowiązana formalnie z normami IEC, tylko ISO, a dotycząca funkcjonalnie bezpiecznej wersji magistrali CAN. Powiązanie tej magistrali z normami ISO wynika stąd, że była ona opracowana na potrzeby techniki samochodowej, a nie automatyki przemysłowej, w której zastosowano ją później.

3.4. Normy wspomagające – kompatybilność elektromagnetyczna

Sprawa zdefiniowania wymagań stawianych systemom związanym z bezpieczeństwem w zakresie kompatybilności elektromagnetycznej pojawiła się zaraz na początku wdrażania norm serii IEC 61508. Pierwszym dokumentem w tej sprawie był Raport Techniczny IEC/TR [17], którego kolejna wersja ukazała się w 2008 r., a więc w czasie, gdy prace przy nowelizacji normy podstawowej były zaawansowane. 18 listopada 2011 r. rozpoczęto proces oceny aktualności tego raportu [20].

Wyżej wymieniony raport podaje jedynie ogólne ramy postępowania, konieczne było przełożenie go na konkretne wymagania. Tę funkcję spełniają normy kompatybilności elektromagnetycznej [2, 3, 4] odnoszące się do wyposażenia do pomiarów i sterowania. Norma PN-EN 61326-1 ustala wymagania odporności dotyczące wszelkiego sprzętu pracującego w warunkach przemysłowych lub innych (aktualnie w trakcie nowelizacji). W czerwcu 2011 r. zakończyło się pozytywnie głosowanie nad projektem o statusie CDV. Normy [3, 4] wyraźnie dotyczą sprzętu i systemów bezpiecznych funkcjonalnie. Zgodnie z ich postanowieniami sprzęt elektryczny i/lub elektroniczny związany z bezpieczeństwem powinien spełniać wymagania:

- wykazywać taką odporność na zaburzenia EMC, jaka wynika z wymagań PN-EN 61326-1, według tamże sformułowanych kryteriów,
- wykazywać odporność na zaburzenia EMC o podwyższonej ostrości przy zachowaniu wynikającym z „kryterium FS", wprowadzonego tymiż normami.

Istotą wymagań kryterium FS jest to, że w przypadku jakiegokolwiek zakłócenia w pracy urządzenia ma ono przejść w stan bezpieczny.

Należy jeszcze podkreślić, że norma [3] formułuje wymagania obowiązujące w dowolnej lokalizacji przemysłowej, zaś norma [4] podaje wymagania złagodzone, dotyczące urządzeń pracujących w „skonkretyzowanym środowisku elektromagnetycznym". To środowisko odznacza się wprowadzeniem pewnych środków ochronnych, w tym powiększeniem odstępów między obwodami sterowania i energetycznymi, charakterystycznych w instalacjach w przemyśle procesowym.

4. Podsumowanie

Scharakteryzowano zmiany jakie zaszły w czasie ostatnich 5 lat w normalizacji odnoszącej się do bezpieczeństwa funkcjonalnego. Należy przy tym zwrócić uwagę na fakt, że będą mieć miejsce kolejne zmiany spowodowane:

- nowelizacją norm sektorowych serii IEC 61511, kolejowych i innych,
- nieustannym postępem technicznym w zakresie elektroniki.

Wprowadzone zmiany czynią normy bardziej przyjazne dla wdrażających.

Bibliografia

1 Missala T.: *Kompatybilność elektromagnetyczna przemysłowych sieci komunikacyjnych związanych z bezpieczeństwem*, [w:] Prace VI Krajowego Sympozjum „Kompatybilność elektromagnetyczna w Elektrotechnice i Elektronice" EMC'09, Łódź 2009 r., 25.

2 PN-EN 61326-1:2009, Wyposażenie elektryczne do pomiarów, sterowania i użytku w laboratoriach Wymagania dotyczące kompatybilności elektromagnetycznej (EMC) – Część 1: Wymagania ogólne.

3 PN-EN 61326-3-1**:** 2008, Wyposażenie elektryczne do pomiarów, sterowania i użytku w laboratoriach Wymagania dotyczące kompatybilności elektromagnetycznej (EMC) – Część 3-1: Wymagania odporności dotyczące systemów związanych z bezpieczeństwem i wyposażenia przewidzianego do wypełniania funkcji związanych z bezpieczeństwem (bezpieczeństwo funkcjonalne) – Ogólne zastosowania przemysłowe (oryg.).

4 PN-EN 61326-3-2: 2008, Wyposażenie elektryczne do pomiarów, sterowania i użytku w laboratoriach – Wy-

magania dotyczące kompatybilności elektromagnetycznej (EMC) – Część 3-2: Wymagania odporności dotyczące systemów związanych z bezpieczeństwem i wyposażenia przewidzianego do wypełniania funkcji związanych z bezpieczeństwem (bezpieczeństwo funkcjonalne) – Zastosowania przemysłowe w skonkretyzowanym środowisku elektromagnetycznym (oryg.).

5 PN-EN 61508 (IEC 61508): Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem:
   a. PN-EN 61508-1:2010 Część 1: Wymagania ogólne (oryg.),
   b. PN-EN 61508-2:2010 Część 2: Wymagania dotyczące elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem (oryg.),
   c. PN-EN 61508-3:2010 Część 3: Wymagania dotyczące oprogramowania (oryg.),
   d. PN-EN 61508-4:2010 Część 4: Definicje i skrótowce (oryg.),
   e. PN-EN 61508-5:2010 Część 5: Przykłady metod określania poziomów nienaruszalności bezpieczeństwa (oryg.),
   f. PN-EN 61508-6:2010 Część 6: Wytyczne do stosowania IEC 61508-2 i IEC 61508-3 (oryg.),
   g. PN-EN 61508-7:2010 Część 7: Przegląd technik i miar (oryg.).

6 PN-EN 61784-3:2010, Przemysłowe sieci komunikacyjne – Profile – Część 3: Magistrale miejscowe bezpieczne funkcjonalnie – Ogólne zasady i definicje profili.

7 PN-EN 62061: PN-EN 62061: 2008 Bezpieczeństwo maszyn – Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i programowalnych elektronicznych systemów sterowania związanych z bezpieczeństwem.

8 IEC 62443-1-1: 2009: Industrial communication networks – network and system security – Part 1-1: Terminology, concepts and models.

9 IEC 62443-2-1(65/438/CDV: Industrial communication networks – network and system security – Part 2-1: Establishing an industrial automation and control system security program.

10 IEC/TR 662443-3-1:2009: Industrial communication networks – network and system security – Part 5: Security technologies for industrial automation and control systems.

11 Missala T.: *Analiza wymagań i metod postępowania przy ocenie ryzyka i określaniu wymaganego poziomu nienaruszalności bezpieczeństwa*, Przemysłowy Instytut Automatyki i Pomiarów PIAP, Warszawa 2009.

12 Missala T.: *Model „krok po kroku" oceny bezpieczeństwa funkcjonalnego systemów zabezpieczeniowych w przemyśle procesowym*, http://www.piap.pl/certyfikacja.

13 Missala T.: *Księga procedur do oceny zgodności bezpieczeństwa funkcjonalnego systemów zabezpieczeniowych w przemyśle procesowym*, http://www.piap.pl/certyfikacja

14 Missala T.: *Zabezpieczenie sieci przemysłowych przed intruzami – temat dnia*, „Pomiary Automatyka Robotyka", 2/2010, 180–189.

15 PN-EN 61511-3:2005, Bezpieczeństwo funkcjonalne – Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego: Część 3: Wytyczne do określania poziomów nienaruszalności bezpieczeństwa.

16 IEC 61131-6 ed.1.0, Programmable controllers – Part 6: Functional safety (IEC/65B_797/CDV).

17 IEC 61000-1-2: 2008, Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for achievement of the functional safety of electrical and electronic equipment with regard to electromagnetic phenomena.

18 IEC/TR 62685: 2010, Industrial communication networks – Profiles – Assessment guideline for safety devices using IEC 61784-3 functional safe communication profiles (FSCPs).

19 EN 50325-5: 2010, Industrial communication subsystem based on ISO 11898 (CAN) for controller-device interfaces – Part 5: Functional safety communication based on EN 50325-4.

20 IEC 77/311/Q; 2011, Review of status of publication IEC TS 61000-1-2 Ed. 2. ■

New functional safety standardization works – result of the technological progress

Abstract: There are characterized amendments introduced during last 5 years to standards concerning functional safety: basic series IEC 61508, programmable controllers, communication networks and electromagnetic compatibility requirements.

Keywords: industrial automation, safety, functional safety, technological progress

prof. dr inż. Tadeusz Missala

Absolwent Wydziału Elektrycznego PŁ, doktoryzował się w 1963 r. na Wydziale Elektrycznym PW. Po 10-letniej pracy w przemyśle i 7-letniej na WAT, od 1967 r. jest pracownikiem PIAP. W latach 1967–1988 kierował Ośrodkiem Automatyki Elektrycznej, obecnie Pełnomocnik Dyrektora ds. certyfikacji. Specjalności: automatyka i robotyka przemysłowa, bezpieczeństwo przemysłowe, elektromechaniczne elementy automatyki. Autor i współautor 5 książek i ponad 150 publikacji naukowych. Przewodniczący Komitetu Technicznego PKN ds. Automatyki i Robotyki Przemysłowej.
e-mail: tmissala@piap.pl