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

ZARZĄDZANIE BEZPIECZEŃSTWEM FUNKCJONALNYM A SYSTEM ZARZĄDZANIA JAKOŚCIĄ - RELACJE

Przedstawiono relacje zachodzące między systemem zarządzania bezpieczeństwem funkcjonalnym wg PN-EN 61508-1i systemem zarządzania jakością wg PN-EN 9001:2001. W organizacji produkującej urządzenia elektryczne realizujące funkcje bezpieczeństwa lub systemy ochronne korzystające z takich urządzeń, znajomość relacji między oboma systemami zarządzania będzie użyteczna do spełnienia wymagań obu norm jednocześnie.

MANAGEMENT OF FUNCTIONAL SAFETY AND QUALITY MANAGEMENT SYSTEM – THE RELATIONS

The relations between the functional safety management system according PN-EN 61508 and quality management system according PN-EN 9001:2001 are presented in the paper. For the organization which manufacture electrical equipment for safety functions realization or protective systems using such an equipment, the knowledge of these relation will be useful to comply the both standard simultaneously.

1. WPROWADZENIE

W referacie [1], prezentowanym na poprzedniej konferencji AUTOMATION i w artykule [2] przedstawiono wzajemne powiązania między pojęciami jakości i bezpieczeństwa. Aktualny referat jest poświęcony wykazaniu relacji między systemem zarządzania jakością spełniającym wymagania PN-EN ISO 9001: 2001 [5] i zarządzaniem bezpieczeństwem funkcjonalnym opisanym w PN-EN 61508-1: 2003 [4].

Bezpieczeństwo funkcjonalne w odniesieniu do urządzeń automatyki i robotyki było omówione podczas konferencji AUTOMATION w 1997 r. [3]. Należy przypomnieć, że pojęcie bezpieczeństwa funkcjonalnego odnosi się do urządzeń realizujących funkcje bezpieczeństwa, to jest funkcje ochrony człowieka i zabezpieczenia obiektów przed powstaniem sytuacji zagrażających, czyli prowadzących do możliwości powstania urazu, do śmierci włącznie, lub szkody materialnej o rozmiarach sięgających nawet katastrofy ekologicznej. Bezpieczeństwo funkcjonalne urządzeń jest jedną z dróg, bardzo istotną, w procesie zmniejszania ryzyka wnoszonego przez urządzenia techniczne. Charakteryzuje się ono ustaleniem wymaganych funkcji bezpieczeństwa i przypisaniem im bardzo wysokich probabilistycznych wskaźników pracy bezawaryjnej – nienaruszalności bezpieczeństwa; wymagania [4] precyzują następujące maksymalne poziomy miar docelowych nienaruszalności bezpieczeństwa:

- w trybie pracy na rzadkie przywołanie średnie prawdopodobieństwo uszkodzenia wypełnienia zaprojektowanej funkcji na przywołanie wynosi 10^{-1};

- w trybie pracy na częste przywołanie lub ciągłym prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę wynosi 10^{-5}.

W przypadku organizacji zainteresowanej systemem zarządzania jakością zgodnym z PN-EN ISO 9001:2001 i wprowadzającej zasady bezpieczeństwa funkcjonalnego, może być pomocna niniejsza propozycja sposobu zadośćuczynienia wymaganiom obu norm.

2. RELACJE MIĘDZY WYMAGANIAMI NORM

2.1 Wstęp

Relacje, które są przedmiotem referatu, zostaną przedstawione przez przyporządkowanie wymagań podanych w PN-EN 61508-1 do wymagań PN-EN ISO 9001:2001, które zostaną potraktowane jako bazowe. Ideą takiego rozwiązania jest, aby w organizacji istniał jeden, spójny system zarządzania jakością i bezpieczeństwem funkcjonalnym; tylko taka sytuacja daje gwarancję wdrożenia i przestrzegania wymagań bezpieczeństwa funkcjonalnego.

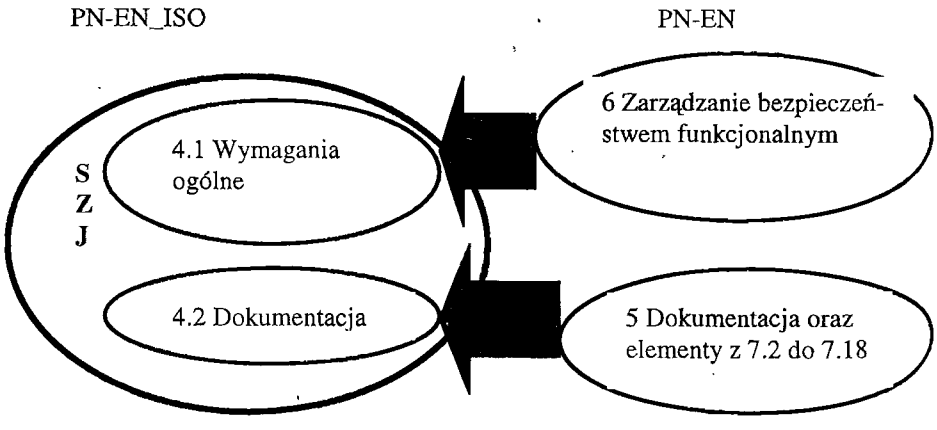
2.2 System zarządzania jakością

W rozdziale 4 PN-EN ISO 9001:2001 (dalej nazywanej PN-EN ISO) „System zapewnienia jakości" podane są wymagania dotyczące m.in.:

- całości systemu i identyfikacji procesów realizowanych w organizacji
- nadzoru nad dokumentami i nadzoru nad zapisami.

Te wymagania są adekwatne do zarządzania bezpieczeństwem funkcjonalnym, lecz są niewystarczające i jest konieczne ich uzupełnienie wg wymagań PN-EN 61508-1 (zwanej dalej PN-EN).

Z powyższej uwagi wynika, że do wymagań ogólnych (p.4.1 PN-EN_ISO) należy dodać wymagania rozdziału 6 PN-EN, zaś do wymagań dotyczących dokumentacji (p. 4.2 PN-EN_ISO) wymagania rozdziału 5 PN-EN (dokumentacja) oraz punktów szczegółowych zawartych w rozdziałach od.7.2 do 7.18; wymagania, które precyzują to, co ma być i kiedy udokumentowane. Te relacje zobrazowano na rysunku 1.



Rysunek 1 – Relacje na poziomie SZJ (Systemu Zarządzania Jakością

2.2 Zarządzanie zasobami

Wśród zestawu wymagań PN-EN_ISO dotyczących zarządzania zasobami zamieszczonych w rozdziale 6, znajduje się wymaganie podające ogólne wymagania dla personelu, To wymaganie należy rozszerzyć o bardziej szczegółowe wymagania zamieszczone w załączniku B do PN-EN, które zwracają szczególną uwagę na:

- odpowiedniość wyszkolenia, wiedzy technicznej, doświadczenia i innych kwalifikacji do konkretnych obowiązków, które dana osoba ma wypełniać;
- zależność oceny kompetencji od: konsekwencji uszkodzeń urządzeń, wymaganego poziomu nienaruszalności bezpieczeństwa i nowości projektu – im większe konsekwencje, wyższy wymagany poziom nienaruszalności bezpieczeństwa i bardziej nowy projekt, tym bardziej rygorystyczna ma być ocena kompetencji osób zaangażowanych w realizację zadań;
- udokumentowanie wyszkolenia, doświadczenia i kwalifikacji osób zaangażowanych w czynności związane z bezpieczeństwem funkcjonalnym.

2.3 Realizacja wyrobu

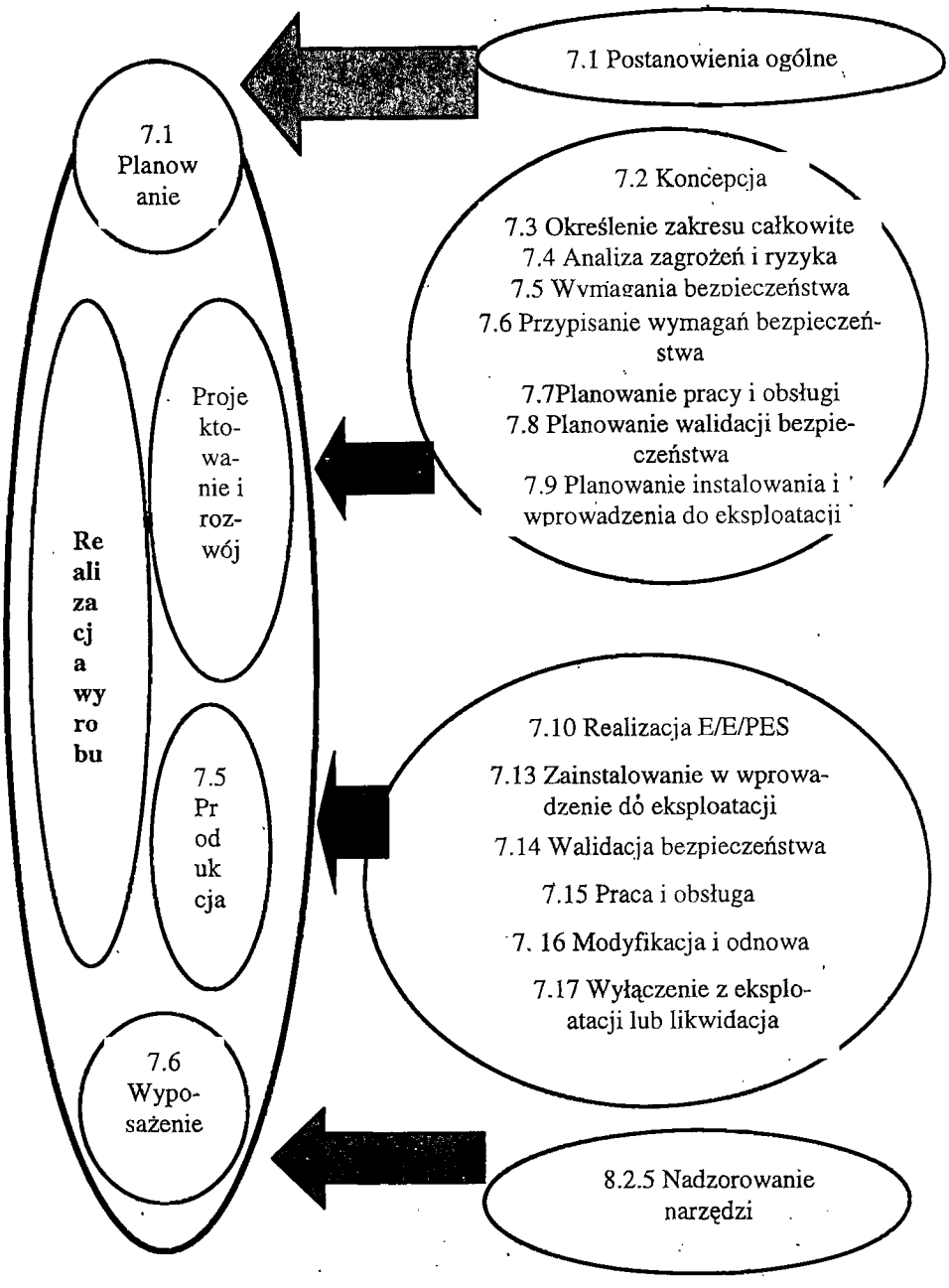
Na poziomie realizacji wyrobu występują liczne powiązania między wymaganiami obu rozpatrywanymi normami. Są one związane z postanowieniami zamieszczonymi w następujących podrozdziałach PN-EN_ISO:

- 7.1 Planowanie realizacji wyrobu;
- 7.3 Projektowanie i rozwój;
- 7.5 Produkcja i dostarczanie usługi.

Wymagania uzupełniające te wymagania z punktu widzenia bezpieczeństwa funkcjonalnego są sprecyzowane w PN-EN w oparciu o koncepcję „cyklu życia bezpieczeństwa" urządzenia związanego z bezpieczeństwem. Tak więc poszczególne :podrozdziały PN-EN mają poniżej podane relacje do podrozdziałów PN-EN_ISO:

- 7.1 Postanowienia ogólne - wprowadza podejście opierające się na cyklu życia bezpieczeństwa i jest rozszerzeniem podrozdziału 7.1 – Planowanie realizacji wyrobu w PN-EN_ISO;
- 7.2 Koncepcja, 7.3 Określenie zakresu całkowite, 7.4 Analiza zagrożeń i ryzyka, 7.5 Wymagania bezpieczeństwa całkowite, 7.6 Przypisanie wymagań bezpieczeństwa, 7.7 Planowanie całkowite pracy i obsługi, 7.8 Planowanie całkowite walidacji bezpieczeństwa oraz 7.9 Planowanie całkowite instalowania i wprowadzania do eksploatacji – są dopełnieniami podrozdziału 7.3 – Projektowanie i rozwój w PN-EN_ISO;
- 7.10 Realizacja E/E/PES, 7.13 Zainstalowanie całkowite i wprowadzenie do eksploatacji, 7.14 Walidacja całkowita bezpieczeństwa, 7.15 Całkowita praca, obsługa i naprawa, 7.16 Całkowita modyfikacja i odnowa oraz 7.17 Wyłączenie z eksploatacji lub likwidacja – są ukierunkowaniem wymagań zamieszczonych w podrozdziale 7.5 – Produkcja i dostarczanie usługi w PN-EN_ISO.

Relacje powyższe zobrazowano na rysunku 2.



Rysunek 3 – Relacje na poziomie realizacji wyrobu

2.4 Monitorowanie i pomiary

Do spełnienia wymagań PN-EN_ISO w tym zakresie (p. 8.2) PN-EN wprowadza dwa narzędzia:

- Weryfikację opisaną w p. 7.18;
- Ocenę bezpieczeństwa funkcjonalnego, opisaną w rozdziale 8.

Oba te procesy są traktowane jako rozłożone, realizowane przy każdej fazie cyklu życia bezpieczeństwa. Ocenę bezpieczeństwa funkcjonalnego mają wykonywać osoby/wydziały/organizacje niezależne od realizatorów urządzeń/systemów podlegających ocenie. Wymagany poziom niezależności wykonujących ocenę bezpieczeństwa funkcjonalnego zależy od konsekwencji uszkodzenia ustalonych przy analizie zagrożeń i ryzyka oraz wymaganego poziomu nienaruszalności bezpieczeństwa; PN-EN podaje wymagania minimalne. Wymagane poziomy niezależności przedstawiono w tablicach 1 i 2, zaś relacje zobrazowano na rysunku 3.

Tablica 1 – Minimalne poziomy niezależności wykonujących ocenę bezpieczeństwa funkcjonalnego (fazy od 1 do 8 i od 12 do 16 włącznie) całkowitego cyklu życia bezpieczeństwa

Minimalny poziom niezależności	Konsekwencje (patrz uwaga 2)			
	A	B	C	D
Osoba niezależna	HR	HR[1]	NR	NR
Wydział niezależny	-	HR[2]	HR[1]	NR
Organizacja niezależna	-	-	HR[2]	HR
UWAGA 1 – W sprawie szczegółów interpretacji tej tablicy patrz poniżej UWAGA 2 – Typowymi konsekwencjami mogłyby być: konsekwencja A – mały uraz (na przykład chwilowa utrata funkcji); konsekwencja B – poważny trwały uraz jednej lub kilku osób; śmierć jednej osoby; konsekwencja C – śmierć kilku osób; konsekwencja D – bardzo wiele osób zabitych.				

Tablica 2 – Minimalne poziomy niezależności wykonujących ocenę bezpieczeństwa funkcjonalnego (faza 9 całkowitego cyklu życia bezpieczeństwa)

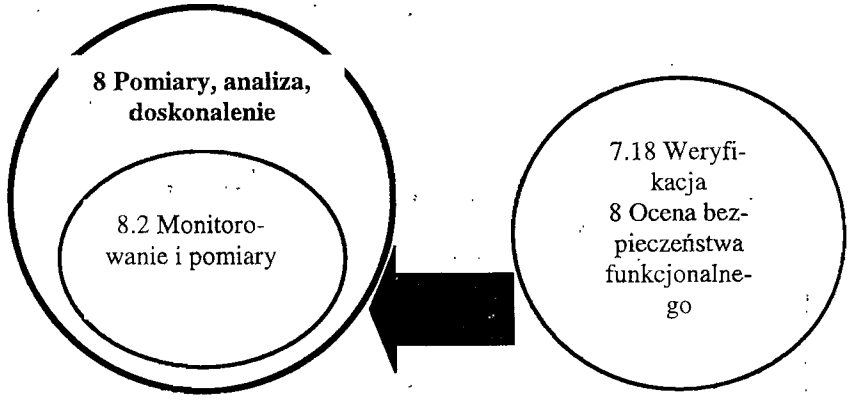
Minimalny poziom Niezależności	Poziom nienaruszalności bezpieczeństwa			
	1	2	3	4
Osoba niezależna	HR	HR[1]	NR	NR
Wydział niezależny	-	HR[2]	HR[1]	NR
Organizacja niezależna	-	-	HR[2]	HR
UWAGA - W sprawie szczegółów interpretacji tej tablicy patrz poniżej				

W tablicach zamieszczono następujące zalecenia:

- HR: niniejszy poziom niezależności jest wysoce zalecany jako minimalny w przypadku określonych konsekwencji (tablica 4) lub poziomu nienaruszalności bezpie-

czeństwa (tablica 5). Jeśli przyjęto niższy poziom niezależności, to zaleca się szczegółowe uzasadnienie nie przyjęcia poziomu HR.

- NR: niniejszy poziom niezależności jest uznany za niewystarczający i jest stanowczo niezalecany w przypadku określonych konsekwencji (tablica 4) lub poziomu nienaruszalności bezpieczeństwa (tablica 5). Jeśli przyjęto ten poziom niezależności, to zaleca się szczegółowe uzasadnienie przyjęcia go.
- -: nie ma zaleceń ani za ani przeciw przyjęciu tego poziomu niezależności.
-



Rysunek 3 – Relacje na poziomie pomiarów, analizy i doskonalenia

3 PODSUMOWANIE

Przedstawione relacje między wymaganiami PN-EN ISO 9001:2001 [5] i PN-EN 61508 [4] oraz propozycja skomponowania wymagań powinna pozwolić na potraktowanie postępowania w zarządzaniu bezpieczeństwem funkcjonalnym jako procedur Systemu Zarządzania Jakością zainteresowanej organizacji. W rezultacie otrzyma się spójny system zarządzania jakością i bezpieczeństwem funkcjonalnym

LITERATURA

1. Missala T.: Jakość a bezpieczeństwo – relacje wzajemne. Materiały Konferencji Naukowo-Technicznej Automatyzacja – Nowości i Perspektywy AUTOMATION 2003, ss. 113-122.

2. Missala T.: Janusowe oblicza jakości. Pomiary, Automatyka, Robotyka, 2003 r. nr 4 ss. 8-11.

3. Missala T.: Bezpieczeństwo funkcjonalne urządzeń automatyki i robotyki. Materiały Konferencji Naukowo-Technicznej Automatyzacja – Nowości i Perspektywy AUTOMATION 1997, ss. 113-125.

4. PN-EN 61508-1: 2003(U), Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem. Część 1: Wymagania ogólne.

5. PN-EN ISO 9001: 2001, Systemy zarządzania jakością. Wymagania.