SPIS TREŚCI

Przedmowa do Normy Europejskiej 5

Wprowadzenie 6

1 Zakres normy 7

2 Powołania normatywne 8

3 Terminy i definicje 8

4 Formy skrócone terminów 8

5 Proces bezpieczeństwa 9
5.1 Ocena ryzyka i kontrolowanie zagrożeń 9
5.2 A. Ocena ryzyka 11
5.2.1 Postanowienia ogólne 11
5.2.2 Prowadzenie oceny ryzyka 11
5.3 B. Wynik oceny ryzyka 11
5.4 C. Kontrolowanie zagrożeń 12
5.5 D. Rewizja oceny ryzyka 13
5.6 Obowiązki 13

6 Wykazywanie bezpieczeństwa i akceptacja 13
6.1 Wprowadzenie 13
6.2 Wykazywanie bezpieczeństwa i proces akceptacji bezpieczeństwa 14
6.3 Odpowiedzialność za zarządzanie dowodem bezpieczeństwa 17
6.4 Modyfikacje po akceptacji bezpieczeństwa 17
6.5 Zależności pomiędzy dowodami bezpieczeństwa 17
6.6 Relacja pomiędzy dowodami bezpieczeństwa i architekturą systemu 18

7 Organizacja i niezależność ról 19
7.1 Postanowienia ogólne 19
7.2 Początkowe fazy cyklu życia (fazy 1 do 4) 19
7.3 Dalsze fazy cyklu życia (począwszy od fazy 5) 20
7.4 Kompetencje personelu 22

8 Ocena ryzyka 23
8.1 Wprowadzenie 23
8.2 Analiza ryzyka 23
8.2.1 Postanowienia ogólne 23
8.2.2 Model ryzyka 23
8.2.3 Techniki analizy skutków 25
8.2.4 Profesjonalny osąd 26
8.3 Zasady akceptacji ryzyka i wycena ryzyka 27
8.3.1 Stosowanie kodeksów postępowania 27
8.3.2 Wykorzystywanie systemów odniesienia 27
8.3.3 Wykorzystywanie szacowania jawnego ryzyka 28
8.4 Stosowanie szacowania jawnego ryzyka 29
8.4.1 Podejście ilościowe 29
8.4.2 Zmienność przy stosowaniu ilościowego oszacowania ryzyka 32
8.4.3 Podejścia jakościowe i semiilościowe 33

9 Specyfikowanie wymagań bezpieczeństwa dla systemu 34
9.1 Postanowienia ogólne 34
9.2 Wymagania bezpieczeństwa 34
9.3 Kategoryzowanie wymagań bezpieczeństwa 34
9.3.1 Postanowienia ogólne 34

9.3.2 Wymagania bezpieczeństwa funkcjonalnego ... 35
9.3.3 Wymagania bezpieczeństwa technicznego ... 36
9.3.4 Wymagania kontekstowe związane z bezpieczeństwem ... 36

10 Rozdzielanie wymagań dotyczących nienaruszalności bezpieczeństwa funkcjonalnego ... 37
10.1 Wywodzenie i rozdzielanie wymagań bezpieczeństwa dla systemu ... 37
10.2 Nienaruszalność bezpieczeństwa funkcjonalnego dla systemów elektronicznych ... 37
10.2.1 Wywodzenie wymagań bezpieczeństwa funkcjonalnego dla systemów elektronicznych ... 37
10.2.2 Rozdzielanie wymagań bezpieczeństwa ... 37
10.2.3 Czynniki wpływające na nienaruszalność bezpieczeństwa ... 40
10.2.4 Nienaruszalność bezpieczeństwa funkcjonalnego a uszkodzenia losowe ... 40
10.2.5 Aspekt systematyczny nienaruszalności bezpieczeństwa funkcjonalnego ... 40
10.2.6 Zrównoważone wymagania dotyczące kontrolowania uszkodzeń losowych i systematycznych ... 41
10.2.7 Tablica poziomów SIL ... 42
10.2.8 Przypisanie poziomu SIL ... 42
10.2.9 Rozdzielanie TFFR po przypisaniu poziomu SIL ... 42
10.2.10 Wykazywanie celów ilościowych ... 43
10.2.11 Wymagania dla nienaruszalności podstawowej ... 43
10.2.12 Zapobieganie nieprawidłowemu używaniu poziomów SIL ... 44
10.3 Nienaruszalność bezpieczeństwa dla systemów nieelektronicznych – stosowanie CoP ... 44

11 Projektowanie i wdrażanie ... 45
11.1 Wprowadzenie ... 45
11.2 Analiza przyczyn ... 46
11.3 Identyfikacja zagrożeń (udoskonalona) ... 46
11.4 Analiza uszkodzeń o wspólnej przyczynie ... 47

Załącznik A (informacyjny) ALARP, GAME, MEM ... 48

A.1 ALARP, GAME, MEM jako metody definiowania kryteriów akceptacji ryzyka ... 48

A.2 ALARP (ryzyko tak niskie jak to tylko rozsądnie możliwe) ... 49
A.2.1 Postanowienia ogólne ... 49
A.2.2 Tolerowalność ryzyka a ALARP ... 50

A.3 Zasada „całościowo co najmniej tak bezpieczny jak zaakceptowany ekwiwalentny" (GAME) ... 50
A.3.1 Zasada ... 50
A.3.2 Stosowanie GAME ... 51
A.3.2.1 Postanowienia ogólne ... 51
A.3.2.2 Zasady podstawowe ... 51
A.3.2.3 Stosowanie GAME do formułowania jakościowych uzasadnień bezpieczeństwa ... 51
A.3.2.4 GAME przy stosowaniu ilościowych celów ryzyka ... 52

A.4 Minimalna śmiertelność endogenna MEM ... 52

Załącznik B (informacyjny) Wykorzystywanie statystyk uszkodzeń i wypadków do wywodzenia wartości THR ... 54

Załącznik C (informacyjny) Wytyczne przypisywania poziomu SIL ... 55

Załącznik D (informacyjny) Metody rozdzielania celów bezpieczeństwa ... 56

D.1 Analiza systemu i metod ... 56

D.2 Przykład metody rozdzielania jakościowego ... 56
D.2.1 Postanowienia ogólne ... 56
D.2.2 Przykład metody jakościowej dla efektywności bariery ... 57

D.3 Przykład metody rozdzielania ilościowego 59
D.3.1 Wprowadzenie 59
D.3.2 Funkcje z niezależnymi mechanizmami wykrywania i blokowania uszkodzeń 60
D.3.3 Funkcja i niezależna bariera działająca jako mechanizm wykrywania i blokowania uszkodzeń 62
D.3.4 Rozdzielanie celu bezpieczeństwa wartością prawdopodobieństwa 63
D.3.5 Rozdzielanie celu bezpieczeństwa wartością „na godzinę" 63

Załącznik E (informacyjny) Najczęstsze błędy podejścia ilościowego 65

E.1 Najczęstsze nieprawidłowe użycia 65

E.2 Mieszanie intensywności uszkodzeń z prawdopodobieństwami 65

E.3 Wykorzystywanie wzorów poza zakresem ich zastosowania 66

Załącznik F (informacyjny) Techniki / metody analizy bezpieczeństwa 67

Załącznik G (informacyjny) Kluczowe role i obowiązki w odniesieniu do bezpieczeństwa systemu 69

Załącznik ZZ (informacyjny) Powiązanie niniejszej Normy Europejskiej z zasadniczymi wymaganiami dyrektywy 2008/57/WE 74

Bibliografia 78