

Temat:**Określanie wymagań na poziom nienaruszalności bezpieczeństwa SIL (ang. safety integrity level) dla funkcji bezpieczeństwa****Wprowadzenie**

W analizie bezpieczeństwa funkcjonalnego systemów sterowania i zabezpieczeń należy określić poziom nienaruszalności bezpieczeństwa SIL (ang. *safety integrity level*). Zdefiniowane są cztery poziomy SIL (tablica nr 1), którym zgodnie z normą PN-EN 61508 odpowiadają ilościowe kryteria probabilistyczne, stanowiące przedziały prawdopodobieństwa niewykonania zadania na żądanie systemu E/E/PE związanego z bezpieczeństwem. Dla pracy częstego przywołania lub ciągłej poziomom SIL odpowiada intensywność uszkodzeń na godzinę. Jeśli zagrożenie stwarza ryzyko na poziomie nieakceptowanym, ryzyko to musi zostać zredukowane do poziomu akceptowanego. Warunkiem koniecznym jest zredukowanie tego ryzyka do poziomu tolerowanego. Określenie wymagań dotyczących niezbędnej redukcji ryzyka (na podstawie analizy ryzyka) z jednej strony i wymagań dotyczących funkcji zabezpieczających (redukujących ryzyko) z drugiej, umożliwia dobranie właściwego systemu E/E/PE (odpowiednia architektura i zasady eksploatacji) dla rozważanego zagrożenia.

Tabela 1. Poziomy nienaruszalności bezpieczeństwa SIL i przedziałowe kryteria probabilistyczne dla systemów E/E/PE [1]

SIL	PFD _{avg}	PFH
4	[10^{-5} , 10^{-4})	[10^{-9} , 10^{-8})
3	[10^{-4} , 10^{-3})	[10^{-8} , 10^{-7})
2	[10^{-3} , 10^{-2})	[10^{-7} , 10^{-6})
1	[10^{-2} , 10^{-1})	[10^{-6} , 10^{-5})

W celu utrzymania ryzyka dla systemu na poziomie akceptowalnym/tolerowanym, należy zdefiniować pewne wymagania spełnienia odpowiednich funkcji przez system związany z bezpieczeństwem, tzw. funkcji bezpieczeństwa. Istnieją dwa typy wymagań, które konieczne są do osiągnięcia bezpieczeństwa funkcjonalnego:

- wymagania na nienaruszalność bezpieczeństwa, czyli prawdopodobieństwo, że dana funkcja bezpieczeństwa wykona się zgodnie z założonym celem,
- wymagania bezpieczeństwa, czyli jakie zadanie ma spełniać dana funkcja bezpieczeństwa.

Ocena ryzyka - graf ryzyka jako metoda określania wymaganego poziomu SIL

Określanie wymaganego poziomu nienaruszalności bezpieczeństwa SIL wykonane może być jedną z kilku dostępnych metod, z tym że często wykorzystuje się do tego celu metodę grafu ryzyka, przedstawioną m.in. w dokumentach PN-EN 61508 lub PN-EN 61511. Jest to metoda jakościowa (w pierwszym przypadku) lub pół-ilościowa (w drugim), gdzie określony poziom SIL zależy od czterech parametrów C , F , P oraz W , które opisują charakter zagrożenia, gdy system związany bezpieczeństwem zawiedzie lub jest niedostępny.

Pół-ilościowe podejście można stosować wtedy, gdy wartość ryzyka tolerowanego może być określona w sposób ilościowy, tzn. jako konkretna określona wartość, np. ilość zgonów rocznie. Z kolei kalibracja grafu ryzyka ma na celu głównie:

- opisanie parametrów ryzyka w taki sposób, aby możliwe było przypisanie im pewnych przedziałów opisowych lub liczbowych,
- upewnienie się, że wybrany poziom SIL jest zgodny z założonymi kryteriami ryzyka i bierze pod uwagę także ryzyko pojawiające się z innych źródeł,
- umożliwienie przeprowadzenia weryfikacji wyboru wartości dla parametrów ryzyka.

Metoda grafu ryzyka opiera się na modelu ryzyka opisanego kombinacją częstości wystąpienia zagrożenia oraz jego konsekwencji. Model ten opisany jest wymienioną poniżej formułą:

$$R = f \times C \quad (1)$$

gdzie R oznacza ryzyko bez zastosowania systemów związanych z bezpieczeństwem, f jest częstością wystąpienia zagrożenia, a C konsekwencjami tego zdarzenia.

Częstość zdarzenia rozpatrywana jest jako składowa trzech czynników:

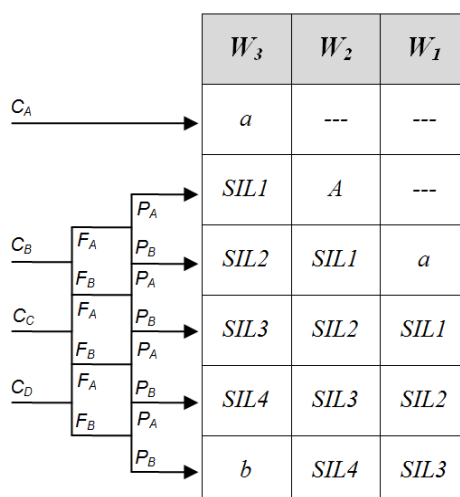
- częstości i czasu przebywania w strefie zagrożenia (F)
- możliwości uniknięcia zagrożenia (P)
- prawdopodobieństwa wystąpienia zagrożenia bez użycia systemu związanego z bezpieczeństwem (W)

Parametry te określone są za pomocą jakościowych przedziałów kryterialnych, które zostały zestawione w tabeli nr 2.

Tabela 2. Parametry ryzyka dla grafu ryzyka

Parametr ryzyka	Klasyfikacja	Opis
Konsekwencje C	C_A Drobne obrażenia C Zakres od 0,01 do 0,1 C_C Zakres > 0,1 do 1,0 C_D Zakres > 1,0	<p>Wartość parametru można obliczyć na podstawie oszacowania liczby osób przebywających na terenie objętym zagrożeniem w czasie wystąpienia zagrożenia i pomnożenia jej przez wartość podatności na to zagrożenie. Przykładowe wartości V dla sytuacji uwolnienia niebezpiecznej substancji do atmosfery:</p> <p>$V=0,01$ dla małego uwolnienia $V=0,1$ dla dużego uwolnienia $V=0,5$ dla dużego uwolnienia wraz zaistnieniem dużego prawdopodobieństwa zapłonu lub bardzo toksycznego materiału $V=1$ dla gwałtownego uwolnienia lub wybuchu</p>
Częstotliwość i czas ekspozycji w strefie zagrożenia F	F_A Rzadka do bardziej częstej (ekspozycja < 0,1) F_B Częsta do stałej	<p>Wartość parametru określa się na podstawie oszacowania czasu, podczas którego obszar zagrożony jest zajmowany podczas normalnej zmiany roboczej.</p> <p>Jeżeli czas ten jest zmienny dla każdej zmiany, pod uwagę należy wziąć czas maksymalny.</p> <p>Wartość parametru F_A powinna być brana pod uwagę tylko wtedy, gdy można wykazać, iż współczynnik przywołania jest losowy i niezwiązany z sytuacją, gdy obszar zagrożony jest zajmowany ponad normę, dot. np. sytuacji rozruchu instalacji lub testów.</p>
Możliwość uniknięcia zdarzenia zagrażającego P	P_A Możliwa po spełnieniu określonych warunków wg opisu P_B Niemożliwa	<p>Parametr ten rozważa się przy założeniu, że system zabezpieczający nie istnieje lub nie zadziałał.</p> <p>Wartość P_A może zostać wybrana tylko wówczas, gdy:</p> <ul style="list-style-type: none"> – istnieje system alarmowy, który zadziała w przypadku niezadziałania systemu związanego z bezpieczeństwem, – zapewniono odrębny system (niezależne urządzenia) do wyłączania/odstawienia instalacji, dzięki którym możliwa jest ewakuacja osób narażonych i uniknięcie skutków zagrożenia, – czas pomiędzy wystąpieniem alarmu u operatora a wystąpieniem konsekwencji zagrożenia jest większy niż 1 godzina
Prawdopodobieństwo zdarzenia niepożądanego W	W_1 Współczynnik przywołania < 0,1D / rok W_2 Współczynnik przywołania pomiędzy 0,1D a 1D / rok Współczynnik przywołania pomiędzy 1D a 10D / rok W_3 Dla wsp. przywołania > 10D / rok wymagany może być wyższy poziom nienaruszalności bezpieczeństwa	<p>Zadaniem tego parametru ryzyka jest estymacja częstości występowania zagrożenia w sytuacji braku systemu związanego z bezpieczeństwem. W sytuacji, gdy współczynnik przywołania jest bardzo wysoki, należy rozważyć wykorzystanie innej metody do określenia wymaganego SIL lub przekalibrować graf ryzyka.</p> <p>D jest współczynnikiem kalibracji</p>

Kombinacja wyżej wymienionych parametrów tworzy z kolei ogólną strukturę grafu ryzyka, który przedstawiony jest na rysunku 2.



Rysunek 2. Graf ryzyka wg normy PN-EN 61508

Użycie parametrów ryzyka C , F oraz P prowadzi do sześciu wyjść z grafu, które są przyporządkowane do jednej ze skal W_1 , W_2 i W_3 . Każdy punkt na tych skalach jest wskazaniem koniecznej nienaruszalności bezpieczeństwa, którą musi posiadać system E/E/PE związany z bezpieczeństwem. Mogą się pojawić sytuacje, w których dla określonych konsekwencji pojedynczy system E/E/PE związany z bezpieczeństwem będzie niewystarczający dla zapewnienia koniecznego zmniejszenia ryzyka (sytuacja z wartością b w grafie).

Zakładając, że w procesie oceny ryzyka związanego z wybraną funkcją bezpieczeństwa określono parametry jak w tabeli nr 3:

Tabela 3. Wybór parametrów ryzyka dla grafu

Parametr ryzyka		Klasyfikacja
Konsekwencje C	C_A	Drobne obrażenie
	C_B	Poważne lub trwałe uszkodzenie ciała jednej lub wielu osób; śmierć jednej osoby
	C_C	Śmierć wielu osób
	C_D	Bardzo wiele ofiar śmiertelnych
Częstotliwość i czas ekspozycji w strefie zagrożenia F	F_A	Rzadka do bardziej częstej
	F_B	Częsta do stałej
Możliwość uniknięcia zdarzenia zagrażającego P	P_A	Możliwa w określonych warunkach
	P_B	Prawie niemożliwa
Prawdopodobieństwo zdarzenia niepożądanego W	W_1	Bardzo nieznaczne prawdopodobieństwo, że zdarzenie niepożądane wystąpi
	W_2	Nieznaczne prawdopodobieństwo, że zdarzenie niepożądane wystąpi
	W_3	Względnie duże prawd., że zdarzenie niepożądane wystąpi

wymagany poziom nienaruszalności bezpieczeństwa dla wybranej funkcji bezpieczeństwa wynosi SIL1.

Zadanie

1. Dla przykładowego systemu technicznego, opisanego na laboratorium nr 1, zdefiniuj funkcje bezpieczeństwa, mające na celu redukcję ryzyka związanego z występowaniem zidentyfikowanych nieakceptowanych zagrożeń.
2. Zaproponuj jednolite schematy grafów ryzyka dla przeprowadzanych analiz ryzyka (dla kryteriów strat ludzkich, środowiskowych oraz ekonomicznych).
3. Skalibruj zaproponowane grafy ryzyka wg założonych kryteriów.
4. Na podstawie szczegółowego opisu warunków pracy przykładowego systemu (pamiętaj, że mają one bezpośredni wpływ na możliwość zajścia zidentyfikowanych zdarzeń awaryjnych) wykonaj ocenę ryzyka dla każdej zdefiniowanej funkcji bezpieczeństwa (za pomocą grafów ryzyka określ wymagany poziom nienaruszalności bezpieczeństwa SIL).
5. Wykonaj zestawienie wszystkich zaproponowanych funkcji bezpieczeństwa wraz z ich opisem funkcjonalnym (jakie jest ich zadanie) oraz przypisanymi poziomami wymaganego SIL (w rozbiciu na kryteria oraz wartość wynikową).