Barnert Tomasz
Politechnika Gdańska, Gdańsk, Polska

Determining required safety integrity level
Określanie wymaganego poziomu nienaruszalności bezpieczeństwa

Keywords / Słowa kluczowe

functional safety, hazards identification, risk assessment, safety requirements, safety integrity level
bezpieczeństwo funkcjonalne, identyfikacja zagrożeń, analiza i ocena ryzyka, nienaruszalność bezpieczeństwa

Streszczenie

One of the most important stage of technical system functional safety analysis is defining the safety-related functions as well as determining a safety integrity level (SIL) for each defined function. A properly carried out hazard identification process is the necessary condition for correct definition of the safety-related functions. Determining the safety integrity level (SIL) is based on risk assessment taking into account risk acceptance criteria. It guarantees accurate results which means that the risk associated with technical system is under good control and the risk level can be reduced to acceptable one. There are several safety integrity level determination methods and techniques described in normative documents and many papers. This article is aimed at presentation of some of them and in addition a new approache are outlined.

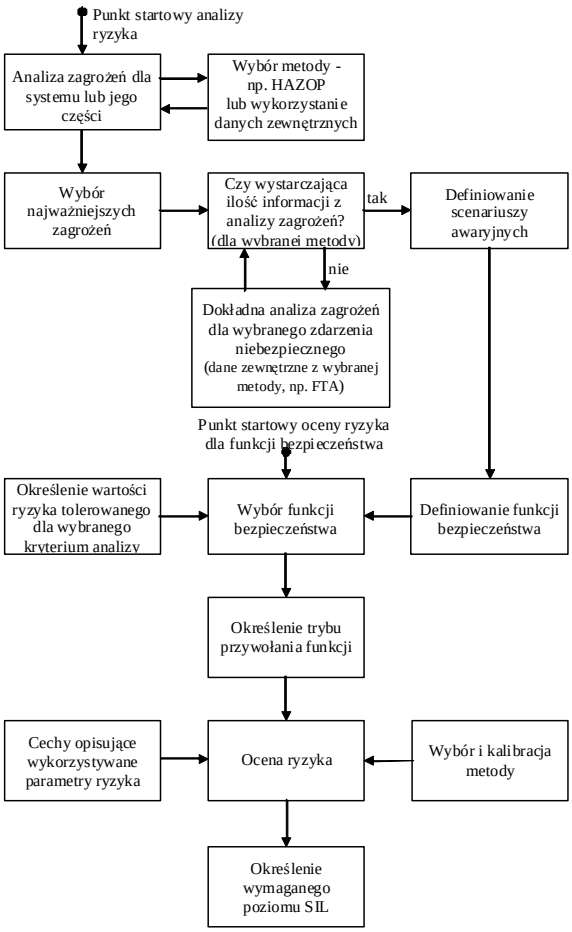
1. Wprowadzenie

Analizę bezpieczeństwa funkcjonalnego dzieli się na kilka odrębnych, choć powiązanych ze sobą etapów w cyklu życia systemu związanego z bezpieczeństwem. Ważną rolę pełni tutaj etap identyfikacji funkcji bezpieczeństwa, mogących pojawić się w systemie/procesie, a także późniejsze przypisanie im wymaganego poziomu nienaruszalności bezpieczeństwa (tzw. SIL – ang. *safety integrity level*). Poziom ten jest ściśle powiązany ze stopniem redukcji ryzyka, występującego w badanym systemie/procesie, przez wybraną funkcję bezpieczeństwa. W celu zidentyfikowania funkcji bezpieczeństwa i określenia dla niej całkowitej specyfikacji wymagań należy wykonać szereg analiz opisanych w niniejszym artykule. Ogólnie wszystkie wymienione działania można określić mianem analizy ryzyka dla rozważanego systemu technicznego.
Niezrozumienie idei stojącej za etapem analizy i oceny ryzyka, a także nieumiejętne posługiwanie się dostępnymi metodami służącymi tej analizie jest jedną z przyczyn występowania zdarzeń niebezpiecznych w systemach nowoprojektowanych lub też już istniejących. Analizując przypadki wystąpienia zdarzeń niebezpiecznych w przemyśle, wielu z nich można było uniknąć poprzez zastosowanie odpowiednich środków zmniejszających ryzyko.
Historia pokazuje przykłady wielu awarii przemysłowych, których wystąpienie kończyło się bardzo poważnymi konsekwencjami, zarówno z punktu widzenia kryteriów strat środowiskowych, życia i zdrowia ludzi, jak również materialnych [13], [10].

2. Analiza i ocena ryzyka w bezpieczeństwie funkcjonalnym

W analizie bezpieczeństwa funkcjonalnego kluczowe znaczenie mają aspekty związane ze znalezieniem potencjalnych źródeł zagrożeń, określeniem prawdopodobieństwa lub częstości ich wystąpienia oraz oszacowania ich skutków, określenie funkcji bezpieczeństwa, które zaimplementowane w odpowiedni sposób mają chronić przed konsekwencjami tych zagrożeń, określenie poziomu nienaruszalności bezpieczeństwa SIL dla obiektu (instalacji) podwyższonego ryzyka oraz następnie zaprojektowanie takiego systemu zabezpieczeniowego, który spełni te wymagania.

Procedura określenia poziomu SIL, wchodząca w skład szeroko pojętej analizy ryzyka, w procesie analizy bezpieczeństwa funkcjonalnego została przedstawiona na *Rysunek 1*.



Rysunek 1. Procedura analizy i oceny ryzyka

Podstawowa koncepcja procesu związanego z analizą bezpieczeństwa funkcjonalnego przedstawia się następująco:

- zdefiniowanie tolerowanego poziomu ryzyka dla analizowanego systemu,
- zidentyfikowanie potencjalnych zagrożeń,
- ustalenie aktualnego poziomu ryzyka na podstawie zidentyfikowanych zagrożeń,
- zidentyfikowanie funkcji związanych z bezpieczeństwem mających na celu redukcję poziomu ryzyka związanego z potencjalnymi zagrożeniami,
- ustalenie wymaganej wartości redukcji ryzyka dla każdej funkcji bezpieczeństwa, biorąc pod uwagę powyższe punkty,
- wyrażenie wymaganej wartości redukcji ryzyka za pomocą poziomów nienaruszalności bezpieczeństwa SIL.

3. Wymagania bezpieczeństwa

3.1. Model ryzyka

Mówiąc o wymaganiach bezpieczeństwa oraz o procesie określania wymaganego poziomu SIL należy jednoznacznie zdefiniować pojęcie ryzyka, na bazie którego taka analiza może zostać przeprowadzona. Pomimo, iż pojęcie ryzyka może się różnić w zależności od rozważanej dziedziny (nauki, techniki, itp.), przyjęło się jednak, iż w analizach systemów technicznych, ryzyko definiuje się najczęściej jako kombinację prawdopodobieństwa lub częstości wystąpienia pewnego zdarzenia niebezpiecznego oraz wielkości straty, które to zdarzenie może spowodować [19], [16].

I tak, zwykle wartość ryzyka wyznacza się na podstawie funkcji trzech zmiennych wektorowych, [7], [14] w skład których wchodzą:

- scenariusze zdarzenia niebezpiecznego,
- prawdopodobieństwo lub częstość ich wystąpienia,
- skutki ich wystąpienia.

Miarę ryzyka dla całego systemu technicznego wyznacza się zatem na podstawie opisanych powyżej parametrów [7], [14]:

$$\mathfrak{R} = H(\boldsymbol{S}, \boldsymbol{F}, \boldsymbol{N}) \tag{1}$$

gdzie $\boldsymbol{S}$ oznacza zbiór zdarzeń awaryjnych (scenariuszy), $\boldsymbol{F}$ oznacza zbiór częstości dla scenariuszy awaryjnych, a $\boldsymbol{N}$ zbiór skutków tych scenariuszy.

Warto przy tym zaznaczyć, że opis tej funkcji może być bardzo złożony, a same wartości opisujące te parametry mogą odnosić się do różnych miar ryzyka [8].

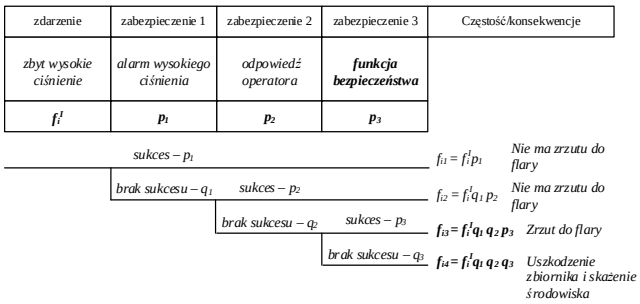
Dla każdego scenariusza awaryjnego oznaczonego S_k wyznaczyć można dwa parametry: f_k - częstość wystąpienia k-tego scenariusza oraz n_k - skutki, które mogą być przyczyną wystąpienia potencjalnych szkód. Koncepcję tą oddaje poniższy wzór:

$$\boldsymbol{R} = \{< S_k, f_k, n_k >\} \tag{2}$$

Jeżeli wprowadzimy do rozważanego scenariusza awaryjnego istnienie zabezpieczenia w postaci funkcji bezpieczeństwa, to częstość związana z wystąpieniem danego scenariusza zostanie zredukowana do wartości f_k^*. Przy założeniu stałych skutków n_k, ryzyko przedstawione może być w takiej sytuacji jako:

$$\boldsymbol{R}^* = \{< S_k, f_k^*, n_k >\} \quad (3)$$

Opis ten wynika bezpośrednio z rozpatrywanego scenariusza awaryjnego, który zobrazowany jest najczęściej poprzez drzewo zdarzeń [14]. Przedstawia ono w sposób poglądowy sekwencję zdarzeń, które prowadzą do wystąpienia poszczególnych skutków związanych z danym stanem awaryjnym. Jednocześnie w drzewie takim można uwzględnić istnienie różnego rodzaju zabezpieczeń istniejących w systemie technicznym, także tych związanych bezpośrednio z działaniem funkcji bezpieczeństwa (redukujących częstość f_k do f_k^*), oraz ich wpływ na prawdopodobieństwo wystąpienia zdarzenia awaryjnego. Przykładowe drzewo zdarzeń przedstawiono na *Rysunku 2*.



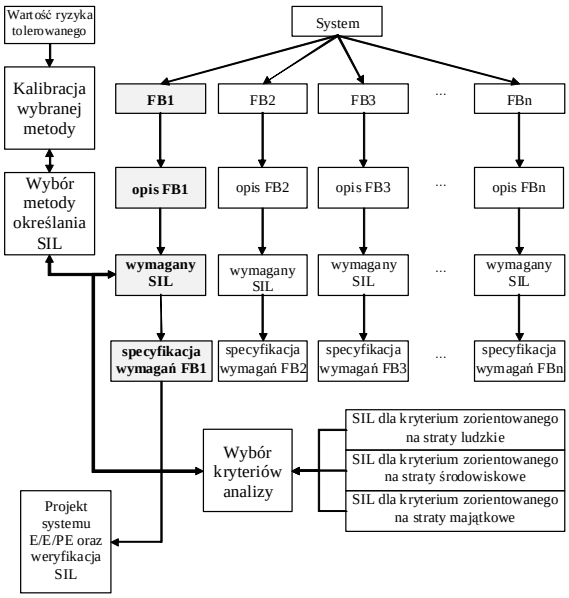
Rysunek 2. Przykładowe drzewo zdarzeń

3.2. Specyfikacja wymagań bezpieczeństwa

Istnieją dwa typy wymagań, które konieczne są do osiągnięcia odpowiedniego zdefiniowanego poziomu bezpieczeństwa funkcjonalnego:

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

Koncepcję tworzenia wymagań dla funkcji związanych z bezpieczeństwem (FB) zobrazowano na *Rysunek 3*.



Rysunek 3. Koncepcja wymagań bezpieczeństwa dla zidentyfikowanych funkcji bezpieczeństwa

3.3. Wymagania na nienaruszalność bezpieczeństwa

W analizie bezpieczeństwa funkcjonalnego systemów sterowania i zabezpieczeń należy określić poziom nienaruszalności bezpieczeństwa SIL (ang. *safety integrity level*). Zdefiniowane są cztery poziomy SIL, którym zgodnie z dokumentem [19] odpowiadają ilościowe kryteria probabilistyczne, stanowiące przedziały prawdopodobieństwa dla pracy na żądanie systemu E/E/PE (urządzenia elektryczne/ elektroniczne/ programowalne elektroniczne) związanego z bezpieczeństwem. Dla pracy częstego przywołania lub ciągłej poziomom SIL odpowiada intensywność uszkodzeń na godzinę. Jeśli zidentyfikowane zagrożenie stwarza ryzyko na poziomie nieakceptowanym, ryzyko to musi zostać zredukowane, za pomocą odpowiednich środków, najczęściej technicznych, do poziomu akceptowanego.

3.4. Wymagania funkcjonalne

Wymagania funkcjonalne opisują logikę, zasadę działania oraz zadania systemu, który będzie realizował zdefiniowaną funkcję bezpieczeństwa wraz ze wszystkimi wymaganiami związanymi z jej obsługą. W praktyce specyfikacja ta przybiera postać tabelarycznego bądź opisowego dokumentu lub też zbioru dokumentów, na podstawie których przebiega następnie etap projektowania struktury sprzętowej, która będzie realizować poszczególne funkcje bezpieczeństwa. Informacje na temat specyfikacji bezpieczeństwa wykorzystywane są także na etapie weryfikacji, czyli sprawdzenia czy

zaprojektowana struktura sprzętowa rzeczywiście spełnia wymagania na nienaruszalność bezpieczeństwa.
Specyfikacja funkcjonalna powinna zawierać szczegółowe opisy wszystkich funkcji bezpieczeństwa, które wymagane będą przy osiągnięciu określonego poziomu bezpieczeństwa funkcjonalnego dla analizowanego systemu. Ponadto należy uwzględnić szereg zagadnień technicznych oraz organizacyjnych wymienionych szczegółowo w dokumencie [20].

4. Określanie wymaganego poziomu SIL

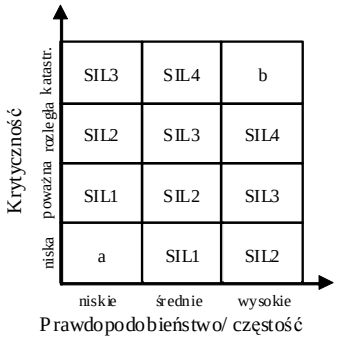
4.1. Określanie SIL w oparciu o zdefiniowany model ryzyka

W ramach analizy zagrożeń powinno się zidentyfikować wszystkie potencjalne sytuacje, mogące mieć wpływ na niepoprawne funkcjonowanie elementów systemu w różnych warunkach pracy. Jest to warunek konieczny do upewnienia się, czy wprowadzenie do systemu rozwiązań bezpieczeństwa funkcjonalnego będzie konieczne do zapewnienia odpowiedniego poziomu bezpieczeństwa systemu przy poszczególnych typach zagrożeń. Jeżeli okaże się, że zidentyfikowane funkcje bezpieczeństwa będą musiały zostać zaimplementowane w systemie, konieczna będzie ocena ich wymaganej sprawności, czyli jak niezawodny będzie musiał być system E/E/PE, który będzie je realizował. Wiąże się to z przeprowadzeniem oceny ryzyka dla poszczególnych zagrożeń i przypisanie każdej funkcji bezpieczeństwa z osobna wymaganego poziomu nienaruszalności bezpieczeństwa SIL.

4.2. Metody określania wymaganego SIL

4.2.1. Matryca ryzyka

Metodą pozwalającą uwzględnić przedstawione wcześniej parametry opisujące poziom ryzyka jest matryca ryzyka. Jest ona chętne wykorzystywana w analizach dla przemysłu procesowego, chemicznego oraz petrochemicznego [22]. Matryca taka budowana jest w oparciu o tzw. tablicę krytyczności zdarzenia zagrażającego, która precyzuje zakres wymaganej redukcji ryzyka dla każdej kombinacji parametrów częstości wystąpienia takiego zdarzenia oraz jego krytyczności. Przykładową tablicę przedstawiono na *Rysunku 4*.
Każde pole takiej tablicy odpowiada wymaganemu poziomowi SIL, który będzie musiał być spełniony przez system realizujący badaną funkcję bezpieczeństwa.

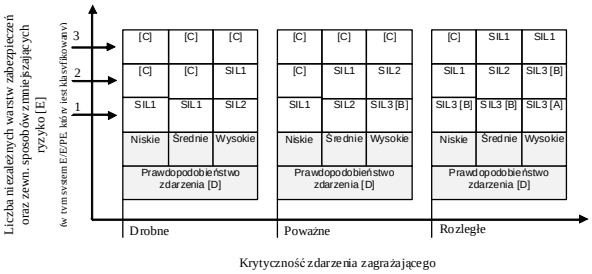


Rysunek 4. Przykładowa matryca ryzyka

Warto zwrócić w tym miejscu uwagę na to, iż metoda jakościowej matrycy ryzyka często stosowana jest w zmodyfikowanej wersji analizy zagrożeń HAZOP. Służy ona w takiej sytuacji do szybkiego i zgrubnego oszacowania ryzyka dla każdej zidentyfikowanej sytuacji awaryjnej w analizowanym systemie [9]. Dzięki wiedzy ekspertów, którzy przeprowadzają analizę HAZOP można na tym etapie wyróżnić już zagrożenia, które powodować mogą powstanie ryzyka na poziomie nieakceptowanym.
Często metodę matrycy ryzyka stosuje się wraz z analizą warstw zabezpieczeń występujących w analizowanym systemie, z tym że nie uwzględnia się ich oddziaływania na parametr prawdopodobieństwa wystąpienia zdarzenia awaryjnego. Uwzględnić należy jednak w takim przypadku pewne założenia [19]:
- każdy system związany z bezpieczeństwem (E/E/PE oraz wykonane w innych technikach) oraz każdy zewnętrzny sposób zmniejszania ryzyka są od siebie niezależne, jak również są traktowane jako osobne poziomy ochrony samodzielnie zmniejszające ryzyko (w przypadku przeprowadzania regularnych badań sprawdzających tak rozumiane poziomy ochrony),
- każdy kolejny poziom ochrony poprawia poziom nienaruszalności bezpieczeństwa o rząd wielkości (gdy systemy związane z bezpieczeństwem oraz zewnętrzne sposoby zmniejszania ryzyka uzyskają właściwy poziom niezależności),
- stosowany jest tylko jeden system związany z bezpieczeństwem wykonany w technice E/E/PE, dla którego tą metodą ustala się niezbędny poziom SIL (może być jednak stosowany w połączeniu z systemami bezpieczeństwa wykonanymi w innej technice i/lub zewnętrznymi sposobami zmniejszającymi ryzyko).

Gdy uwzględni się wszystkie powyższe założenia, otrzymać można 3-wymiarową tablicę krytyczności

zdarzenia zagrażającego. Przykładowa tablica przedstawiona jest na *Rysunku 5.*



Rysunek 5. Przykładowa 3-wymiarowa matryca ryzyka

Ogólne zasady opisanej metody uwzględniają pewne założenia, które szerzej opisane są w dokumencie [19]. Niewątpliwą zaletą przedstawionej powyżej metody jest jej prosta forma oraz bezpośrednie wykorzystanie modelu ryzyka. Jednak aby jej rezultaty były wiarygodne należy bardzo dobrze zrozumieć procesy rzutujące na poziom ryzyka badanego systemu. Ma to związek z jakościowym opisem parametrów ryzyka i ich odpowiednim skorelowaniu z wymaganymi poziomami redukcji ryzyka, a co za tym idzie z przypisaniem wymaganych poziomów SIL do funkcji bezpieczeństwa występujących w systemie. Jak każda metoda jakościowa, jej wyniki nie są precyzyjne i przy rezultatach dających wymagania na poziomie SIL3 i wyższych należy rozpatrzyć wykonanie analizy metodą ilościową.

4.2.2. Jakościowy graf ryzyka

Jedną z częściej stosowanych w praktyce metod określania wymaganego poziomu nienaruszalności bezpieczeństwa jest jakościowy graf ryzyka przedstawiony w dokumencie [19]. Oprócz parametru dotyczącego konsekwencji *C*, wykorzystuje się w nim dodatkowo trzy czynniki, będące częścią składową parametru częstości zdarzenia awaryjnego i są to:

- częstość lub czas przebywania w strefie zagrożenia (F),
- możliwość uniknięcia zagrożenia (P),
- prawdopodobieństwo wystąpienia zagrożenia bez użycia systemu związanego z bezpieczeństwem (W).

Parametry te określone są za pomocą jakościowych przedziałów kryterialnych, tzn. każdy przedział posiada swoją opisową definicję, jednoznacznie go identyfikującą. Takimi przedziałami mogą być przykładowo dla parametru *P*: „*możliwość uniknięcia zagrożenia*” (P_A) lub „*brak możliwości uniknięcia zagrożenia*” (P_B). Kombinacja wyżej wymienionych parametrów wraz z ich przedziałami tworzy ogólną strukturę grafu ryzyka dla kryterium strat personalnych, który przedstawiony jest na rysunku 6.

Wymagania określone są następująco [19]:

--- – brak wymagań bezpieczeństwa,

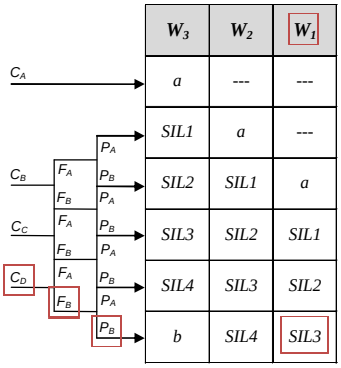
a – brak specjalnych wymagań bezpieczeństwa, SIL1÷SIL4 – poziom nienaruszalności bezpieczeństwa,

b – pojedynczy system E/E/PE jest niewystarczający do zapewnienia wymaganego poziomu bezpieczeństwa.

Użycie parametrów ryzyka *C*, *F* oraz *P* prowadzi do sześciu wyjść z grafu, które są przyporządkowane do jednej ze skal *W1*, *W2* i *W3*. Każdy punkt na tych skalach jest wskazaniem koniecznej nienaruszalności bezpieczeństwa, którą musi posiadać system E/E/PE realizujący wybraną funkcję bezpieczeństwa. Część tabelaryczna przedstawionego powyżej grafu jest więc wskazaniem koniecznego zmniejszenia ryzyka, które musi być zrealizowane przez system związany z bezpieczeństwem, i powiązane jest z wymaganymi poziomami nienaruszalności bezpieczeństwa SIL.

Parę słów wyjaśnienia należy się w tym miejscu parametrowi *W*, który określa prawdopodobieństwo wystąpienia zdarzenia awaryjnego. Oszacowując wartość tego parametru, przy wykonywaniu oceny ryzyka, należy jednak pamiętać o tym, iż nie uwzględnia się przy tym występowania systemów związanych z bezpieczeństwem wykonanych w różnych technikach, w tym w technice E/E/PE. Ale co ważne, wpływ zewnętrznych środków zmniejszających ryzyko powinien być tutaj jednak uwzględniony [19].

Rozważając metodę grafu ryzyka do określenia wymaganego poziomu nienaruszalności bezpieczeństwa SIL dla innych kryteriów niż ochrony życia i zdrowia człowieka, należy uwzględnić pewne zmiany w parametrach ryzyka, co skutkuje oczywiście także pewną zmianą struktury samego grafu [20].



Rysunek 6. Struktura grafu ryzyka wg PN-EN 61508

4.2.3. Kalibrowany pół-ilościowy graf ryzyka

Tabela 1. Przykładowa kalibracja grafu ryzyka [19]

Parametr ryzyka		Klasyfikacja jakościowa	Klasyfikacja ilościowa	
			Wartość dolna *d*	Wartość górna *g*
konsekwencji zdarzenia niebezpiecznego *C*	C_A	Drobne obrażenie		< 0,01
	C_B	Poważne lub trwałe uszkodzenie ciała jednej lub wielu osób; śmierć jednej osoby	0,01 0,1	0,1 1,0
	C_C	Śmierć wielu osób		
	C_D	Bardzo wiele ofiar śmiertelnych	> 1,0	
prawdopodobieństwa przebywania w strefie zagrożenia *F*	F_A	Rzadka do bardziej częstej	0,01	0,1
	F_B	Częsta do stałej	0,1	1,0
prawdopodobieństwa uniknięcia zagrożenia *P*	P_A	Możliwa w określonych warunkach	0,01	0,1
	P_B	Prawie niemożliwa	0,1	1,0
Częstość zdarzenia niepożądanego *W*	W_1	Bardzo nieznaczne prawdopodobieństwo, że zdarzenie niepożądane wystąpi	0,01	0,1
	W_2	Nieznaczne prawdopodobieństwo, że zdarzenie niepożądane wystąpi	0,1	1
	W_3	Względnie duże prawd., że zdarzenie niepożądane wystąpi	1,0	10

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.

Podobnie jak to miało miejsce w jakościowym grafie ryzyka, tak i w tym przypadku ryzyko rozpatrywane jest jako kombinacja częstości i konsekwencji (z podziałem na poszczególne parametry składowe) związanych z wystąpieniem zagrożenia.

Kalibracja grafu ryzyka ma na celu głównie:

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

Biorąc pod uwagę schemat grafu ryzyka przedstawiony na *Rysunku 6* oraz wykorzystane w nim parametry ryzyka wraz z jakościowym opisem ich przedziałów, można dokonać jego kalibracji. Będzie polegało to na przypisaniu wartości dolnej i górnej dla każdego przedziału parametru ryzyka. Wartości te będą miały główny wpływ na całościowy proces szacowania wymaganej redukcji ryzyka. Przykładowe dane do kalibracji grafu ryzyka przedstawione są w *Tabeli 1*.

Parametr W, który określa, podobnie jak to miało miejsce w przypadku grafu jakościowego, prawdopodobieństwo lub częstość wystąpienia zdarzenia awaryjnego, ma tutaj jednak nieco inne znaczenie. Określony jest bowiem przez wartość, która nie powinna uwzględniać występowania systemu związanego z bezpieczeństwem wykonanego w technice E/E/PE, lecz (i tutaj różnica w stosunku do grafu jakościowego) musi brać pod uwagę redukcję ryzyka związaną z innymi warstwami zabezpieczeń [20], [11].

Kalibrowany pół-ilościowy graf ryzyka może być z powodzeniem stosowany w przypadku istnienia dużej liczby funkcji bezpieczeństwa. Metoda ta umożliwia eliminację tych funkcji które nie mają zbyt dużej roli w eliminacji całkowitego ryzyka oraz uwydatnienie tych, które wpływają w dużym stopniu na jego redukcję. Z drugiej strony wymaga żmudnego procesu kalibracji i najlepiej nadaje się do analizy funkcji, w których wartość ryzyka szczątkowego jest relatywnie mała w porównaniu do wartości ryzyka tolerowanego.

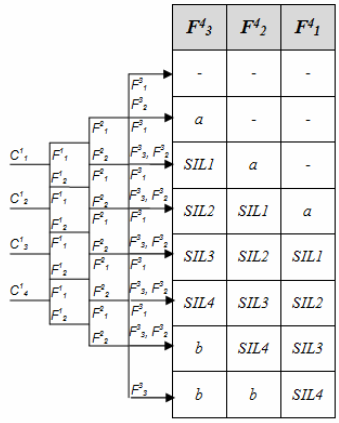
4.2.4. Modyfikacje metody grafu ryzyka

Pomimo popularności metody grafu ryzyka stwarza ona nieustannie pewne problemy interpretacyjne [13],[19]. W związku z tym prowadzone są prace nad udoskonaleniem tej metody. Z najbardziej znanych można wymienić tutaj próby Paula Baybutt'a, który zaproponował zmianę parametrów związanych z częstością, wykorzystywanych w grafie na inicjatory występowania zdarzeń awaryjnych *I*, parametr *E* związany z uwarunkowaniami wystąpienia zdarzenia oraz *S*, czyli parametr związany z prawdopodobieństwem niezadziałania zabezpieczeń. Każdemu z tych parametrów przypisanych zostało szereg przedziałów kryterialnych. Szczegółowe informacje na ten temat znaleźć można w publikacji [5].

Z kolei L. Blackmore w artykule [6] proponuje modyfikację grafu ryzyka na potrzeby przemysłu procesowego i wydobywczego i koreluje metodę grafu z ilościowym opisem parametrów ryzyka. Poprzez takie podejście powiązać można bezpośrednio uzyskaną wartość aktualnego poziomu ryzyka dla analizowanego systemu oraz wyrażoną w sposób ilościowy wymaganą redukcję tego ryzyka.

Istnieją próby rozszerzenia metody grafu ryzyka o aspekty logiki rozmytej. Dzięki temu podejściu można szacować stopień niepewności zarówno danych wykorzystywanych w procesie oceny ryzyka, jak również wyników w nim uzyskanych.

Przykładowe propozycje znaleźć można w publikacjach [17], [18] oraz [21].
Zaproponowano również metodę modyfikowania grafów ryzyka, pozwalającą na ich kształtowanie oraz wykorzystanie dowolnej liczby parametrów ryzyka oraz ich przedziałów kryterialnych. Metoda ta nosi nazwę modyfikowalnych grafów ryzyka i szerzej przedstawiona została w artykułach [1] i [2]. Przykładową strukturę modyfikowalnego grafu ryzyka przedstawiono na *Rysunku 7*. W grafie tym parametr C^1 określa kryteria związane z konsekwencjami wystąpienia analizowanego zdarzenia, natomiast parametry F^1-F^4 składają się na opis częstości wystąpienia ego zdarzenia.



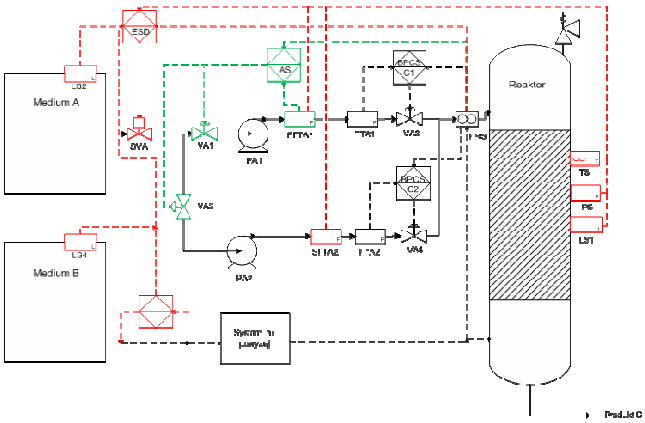
Rysunek 7. Struktura przykładowego modyfikowalnego grafu ryzyka [1]

Za pomocą modyfikowalnych grafów ryzyka można także badać wpływ poziomu ochrony (informacji i dostępu) systemów na wymagany poziom nienaruszalności bezpieczeństwa SIL. Można zatem w ten sposób powiązać zagadnienia bezpieczeństwa funkcjonalnego oraz ochrony informacji i dostępu (*security*) [3], [4].

4.2.5. Przykład wykorzystania grafu ryzyka

Na podstawie opisanej wcześniej metody grafu ryzyka zaprezentowany został poniżej prosty przykład jej wykorzystania.
Rozpatrywana jest przykładowa instalacja przedstawiona na *Rysunku. 8.* Kolorem czarnym oznaczono podstawowy system sterowania BPCS, kolorem czerwonym system związany z bezpieczeństwem SIS, a kolorem zielonym odrębną warstwę alarmową.

Na podstawie procesu identyfikacji zagrożeń (HAZOP) i ich wstępnej ocenie na podstawie jakościowego rankingu ryzyka, wyszczególniono zagrożenia prowadzące do poważniejszych awarii. Do przykładowej oceny ryzyka wybrano zdarzenie awaryjne - *zbyt duże ciśnienie w reaktorze*.



Rysunek 8. Przykładowa instalacja

Spowodować może ono bardzo poważne konsekwencje z punktu widzenia strat ludzkich. Na podstawie analizy takich czynników jak m.in. średnie zaludnienie terenu objętego zagrożeniem, czy też typ wybuchu, jego zakres, szkodliwość substancji (chmury gazu i dymu) oraz kierunki i siłę wiatrów, oszacowano, że może ono być przyczyną zgonu bardzo wielu osób. Nanosząc te informacje na przedziały kryterialne parametru konsekwencji C, otrzymuje się wartość C_D.
Prawdopodobieństwo przebywania osób narażonych na działanie zdarzenia awaryjnego oszacowano na częste do stałego ($F => F_B$).
Po przeanalizowaniu złożoności procesu i substancji w nim biorących udział, w tym szybkość rozprzestrzeniania się zagrożenia, oceniono możliwość uniknięcia konsekwencji wybuchu na minimalną ($P => P_B$).
Ustalono, że prawdopodobieństwo wystąpienia zdarzenia awaryjnego (bez stosowania jakichkolwiek systemów związanych z bezpieczeństwem (wykonanych w technice E/E/PE lub innych) lecz z udziałem wszystkich zewnętrznych sposobów zmniejszających ryzyko) jest bardzo małe. Wzięto pod uwagę m.in. niezawodność urządzeń BPCS, istnienie systemu alarmowego oraz działania operatorów. Stąd wybór przedziału $W => W_1$.
Wszystkie powyższe spostrzeżenia pozwalają na naniesienie ich bezpośrednio na parametry tworzące graf ryzyka, który został wcześniej odpowiednio skalibrowany na potrzeby analizowanej instalacji. Na tej podstawie uzyskać można wymagany stopień redukcji ryzyka, powiązany bezpośrednio z wymaganym poziomem nienaruszalności bezpieczeństwa (SIL3). Zobrazowano to na rys. 6. Struktura sprzętowa realizująca analizowaną funkcję bezpieczeństwa będzie musiała spełnić właśnie takie wymagania.

5. Podsumowanie

Dostępne i opisane w literaturze metody służące określaniu wymaganego poziomu SIL dla funkcji bezpieczeństwa, m.in. graf ryzyka przedstawiony w dokumentach [19], [20], często są tylko ogólne i nie pozwalają na bezpośrednie wykorzystanie ich w analizach konkretnych systemów. Źle zastosowane i skalibrowane na niewłaściwą wartość ryzyka tolerowanego metody te mogą prowadzić do zbyt rygorystycznych lub co gorsze do zbyt optymistycznych rezultatów. Jednocześnie pojawiają się coraz to nowe zagrożenia, których dotąd nie uwzględniało się w analizach, a w dzisiejszych czasach ich zajście okazuje się coraz bardziej możliwe (np. działania terrorystyczne, cyber-ataki, itp.). Stąd uzasadnienie dla ciągłych badań mających na celu opracowanie nowych lub rozszerzenie już istniejących metod i rozwiązań służących analizie bezpieczeństwa funkcjonalnego. Dzięki nim nowe formy zagrożeń mogą być uwzględniane w analizach, co przyczynić się może do znacznego wzrostu poziomu bezpieczeństwa współczesnych systemów technicznych.

Podziękowanie

Autor niniejszego artykułu dziękuje Ministerstwu Nauki i Szkolnictwa Wyższego za wsparcie badań oraz Centralnemu Laboratorium Ochrony Pracy – Państwowemu Instytutowi Badawczemu za współpracę w przygotowaniu projektu badawczego VI.B.10 do realizacji w latach 2011-13 dotyczącego zarządzania bezpieczeństwem funkcjonalnym w obiektach podwyższonego ryzyka z włączeniem zagadnień zabezpieczeń / ochrony i niezawodności człowieka.

Literatura

[1] Barnert, T., Kosmowski, K.T. & Śliwiński, M. (2008). Determining and verifying safety integrity level under uncertainty. ESREL, Valencia, Hiszpania.

[2] Barnert, T., Kosmowski, K.T. & Śliwiński, M. (2009). A knowledge-based approach for functional safety management. ESREL, Praga, Czechy.

[3] Barnert, T., Kosmowski, K.T. & Śliwiński, M. (2010*). Integrated functional safety and security analysis of process control and protection systems with regard to uncertainty issue.* PSAM, Seattle, USA.

[4] Barnert, T., Kosmowski, K.T. & Śliwiński, M. (2010). A method for including the security aspects in the functional safety analysis of distributed control and protection systems. ESREL, Rhodos, Grecja.

[5] Baybutt, P. (2007). An improved risk graph approach for determination of safety integrity level (SILs). *Process Safety Progress*, Vol. 26.

[6] Blackmore, L. (2000). *IEC 61508 – Practical experience in increasing the effectiveness of SIL assessments*. ISA.

[7] CCPS (1999). Guidelines for Consequence Analysis of Chemical Releases. Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York.

[8] CCPS (2000*). Guidelines for Chemical Process Quantitative Risk Analysis*. Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York.

[9] Cruz-Campa, H.J. & Cruz-Gomes, M.J. (2009). *Determine SIS and SIL using HAZOPs*. Wiley InterScience, AIChE.

[10] Gunn, A.M. (2008). *Encyclopedia of disasters. Environmental Catastrophes and Human Tragedies.* Greenwood Press, Westport.

[11] Gulland, W.G. (2004). Methods of determining safety integrity level (SIL). Requirements – Pros and Cons. Springer-Verlag, *Proc. of the Safety-Critical Systems Symposium.*

[12] Kirkwood, D. (2005). Developments in SIL determination. *IEE Computing & Control Engineering*, June/July 2005.

[13] Kletz, T. (1999). *What went wrong? Case Histories of Process Plant Disasters*. Gulf Professional Publishing, Huston.

[14] Kosmowski, K.T. (2003). *Metodyka analizy ryzyka w zarządzaniu niezawodnością i bezpieczeństwem elektrowni jądrowych*. Monografie 33, Politechnika Gdańska, Gdańsk.

[15] Kosmowski, K.T. (2006). *Functional safety in the context of risk appraisal criteria and cost-benefit analysis*. Functional Safety Management in Critical Systems, Gdańsk.

[16] Missala, T. (2009). *Analiza wymagań i metod postępowania przy ocenie ryzyka i określaniu wymaganego poziomu nienaruszalności bezpieczeństwa zawartych w normach bezpieczeństwa funkcjonalnego, normach związanych z nimi oraz literaturze*. PIAP, W-wa.

[17] Nait-Said, R., Zidani, F. & Ouzraoui, N. (2008). Fuzzy Risk Graph Model for Determining Safety Integrity Level. *International Journal of Quality, Statistics, and Reliability.*

[18] Ormos, L. & Ajtonyi, I. (2004*). Soft computing method for determining the safety of technological system by 1EC 6150. Proc. of the 1st Romanian-Hungarian Joint Sympsiom on*

Applied Computational Inelligence (SACI '04), Timisoara, Rumunia.

[19] PN-EN 61508 (2004). Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych elektronicznych systemów wiążących się z bezpieczeństwem. Części 1-7. PKN, Warszawa.

[20] PN-EN 61511 (2007). Bezpieczeństwo funkcjonalne. Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego. Części 1-3, PKN, Warszawa.

[21] Simon, C., Sallak, M. & Aubry, J. (2007). SIL allocation of SIS by aggregation of experts' opinions. *Proc. of the Safety and Reliability Conference ESREL '07*, Stavanger.

[22] Summers, A. (1998). Techniques for assessing a target safety integrity level. *ISA Transactions* 37. Elsevier