Kacprzak Przemysław
Politechnika Gdańska, Gdańsk, Polska

Layer of protection analysis in industrial hazadous installations
Analiza warstw zabezpieczeń w przemysłowych instalacjach podwyższonego ryzyka

Keywords / słowa kluczowe

functional safety, layer of protection analysis, human factros, alarm system
bezpieczeństwo funkcjonalne, analiza warstw zabezpieczeń, czynniki ludzkie, system alarmowy

Abstract

In this article the Layer of Protection Analysis (LOPA), as a technique for the risk evaluation relating to the hazardous industrial installations performance, is presented. The results of analyses are important in the terms of the safety management process in such installations. Based on obtained estimations the decisions might be undertaken which solutions to apply in order to mitigate the risk of hazardous installations performance to a tolerable level. The risk mitigation is provided by properly designed layers of protection, particularly the alarm system, treated as a part of protection layer. The alarm system should be designed and implemented with comprehensive consideration of the human factors. The role of the operator in hazardous installations is crucial mainly during abnormal and alarm situations in order to provide and/or recover system to normal or safety state. In the article some selected aspects of alarm systems designing process with special treating of human operator are outlined. Moreover, an example of the LOPA analysis for the accident sequence within a reaction container with consideration of human reliability analysis (HRA) is carried out.

1. Wprowadzenie

Eksploatacja każdego obiektu przemysłowego podwyższonego ryzyka związana jest z ryzykiem zajścia zdarzeń nieporządanych i/lub awaryjnych. Skutki takich zdarzeń mogą mieć negatywny wpływ na personel, infrastrukturę obiektu, środowisko. Ryzyka związanego z funkcjonowaniem takiego obiektu nie można wyeliminować. Możliwe jest natomiast szacowanie ryzyka, a następnie na podstawie wyników podejmowanie decyzji bazujących na ryzyku jakie opcje sterowania ryzykiem (OSR) zaimplementować na etapie projekotwania instalacji, aby utrzymywać jego wartość w granicach tolerowanych. Użytecznym narzędziem wspomagającym proces podejmowania decyzji odnośnie do implementacji OSR w każdej fazie cyklu życia instalacji jest metoda analizy warstw zabezpieczeń LOPA (*Layer of Protection Analysis*).

2. Analiza ryzyka w wykorzystaniem metody LOPA

Analiza warstw zabezpieczeń LOPA jest półilościową uproszczoną metodą analizy ryzyka [5]. Wyniki analizy dostarczają informacji dotyczących aktualnego poziomu ryzyka związanego z eksploatacją obiektu, które mogą być przydatne w procesie podejmowania decyzji opartych na ryzyku w kontekście potencjalnych działań związanych z zarządzaniem ryzykiem. Celem takich działań jest ograniczenie ryzyka związanego z eksploatacją instalacji przemysłowej przynajmniej do poziomu tolerowanego.
Opis podstawowych kroków analizy warstw zabezpieczeń zaprezentowano na rysunku 1. Punktem wyjścia do przeprowadzenia oceny ryzyka instalacji za pomocą metody LOPA są informacje uzyskane podczas analizy jakościowej (krok 2 na *Rysunku 1*). Taka analiza polega na identyfikacji zagrożeń jakie mogą wystąpić w analizowanej instalacji i jest wykonywana np. za pomocą metody

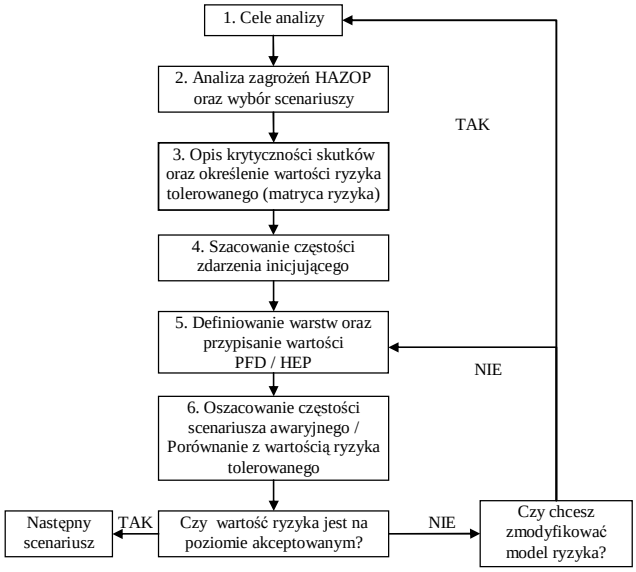
HAZOP (*Hazards and Operability*). Przykładowy scenariusz awaryjny zidentyfikowany podczas analizy HAZOP został zaprezentowany w *Tabeli 1.*
Kolejnym krokiem analizy LOPA jest oszacowanie poziomu ryzyka bez zastosowania środków zabezpieczeniowych w odniesieniu do wartości ryzyka tolerowanego zdefiniowanego przez zarząd przedsiębiorstwa za pomocą matrycy ryzyka (*Tabela 3*).

Tabela 1. Przykład dokumentowania analizy HAZOP

Nazwa:			Przykład HAZOP				*Arkusz:* 1 z 1		
Skład zespołu:			PK z zespołem				*Data:* 10.04.2011		
Rozważana część systemu:			Linia przesyłowa ze zbiornika A do zbiornika				*Data spotkania:* 10.04.2011		
Szczegóły:			*Materiał:* A materiału B		*Czynność:* *Źródło:*	Ciągły przepływ materiału A w dawce większej niż Zbiornik medium A	*Cel:*	zbiornik	
Nr	*Słowo kluczowe*	*Element/ Węzeł*	*Odchyłka*	*Przyczyna*	*Skutek*	*Zabezpieczenie*	*Poziom ryzyka*	*Wymagane akcje*	*Wykonał*
1	BRAK	Przepływ A (dawka większa od medium B)	Brak przepływu medium A	Pompa A zatrzymana, linia przesyłowa A zablokowana	Eksplozja / skutek najbardziej krytyczny	Brak	Nie akceptowalne, np. matrycy ryzyka (rysunek 9)	Opis w tekście	PK

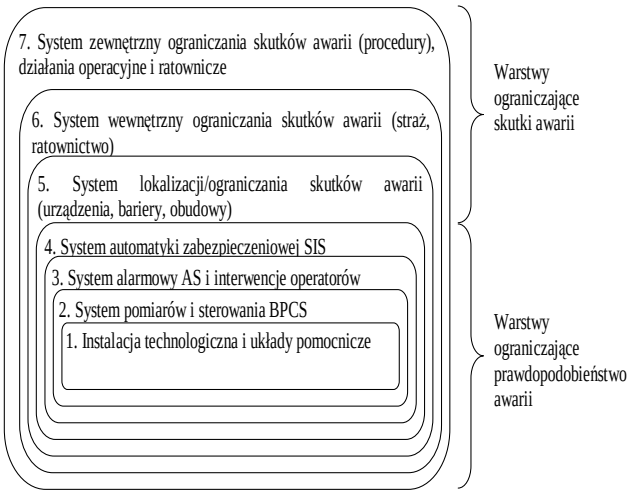
W przypadku gdy niezbędna jest redukcja ryzyka, aby spełnić wymagane kryteria bezpieczeństwa należy zaprojektować niezależne warstwy zabezpieczeniowe, dzięki którym będzie można zredukować wartość ryzyka przynajmniej do poziomu tolerowanego.
Każda z projektowanych warstw musi mieć określony oraz zweryfikowany poziom nienaruszalności bezpieczeństwa SIL (*Safety Integrity Level*). Przypisanie konkretnego poziomu SIL do danej warstwy (poziomy 1-4, gdzie poziom czwarty jest najbardziej restrykcyjny) zależy od architektury, konfiguracji oraz niezawodności elementów wchodzących w jej skład.
W literaturze dostępnych jest szereg metod wyznaczania wymaganego poziomu nienaruszalności bezpieczeństwa SIL dla każdej z projektowanych warstw zabezpieczeniowych. Ogólnie można je podzielić na metody ilościowe i jakościowe [14], [15].
Zależnie od analizowanego obiektu i dostępnej informacji każda z metod może okazać się przydatna. Metody ilościowe wymagają większego zakresu danych i dobrego przygotowania analityków, chociaż dostrzega się zalety metod jakościowych, szczególnie w przypadkach analizy systemów o dużej złożoności. Metody jakościowe wymagają skalowania w celu podejmowania racjonalnych decyzji z uwzględnieniem dostępnej informacji ilościowej.

Oznacza to, że każda z warstw projektowana jest w odpowiedni sposób zapewniający wymagany poziom nienaruszalności bezpieczeństwa SIL. Wraz ze wzrostem poziomu ryzyka dla danego scenariusza awaryjnego wymagany poziom SIL warstw odpowiednio wzrasta, aby możliwa była redukcja poziomu ryzyka do wartości akceptowanej.



Rysunek 1. Podstawowe kroki analizy warstw zabezpieczeń LOPA

W instalacjach przemysłowych podwyższonego ryzyka wyróżnia się kilka warstw związanych z bezpieczeństwem. Można je podzielić na warstwy ograniczające prawdopodobieństwo awarii oraz na ograniczające skutki (*Rysunek 2*).

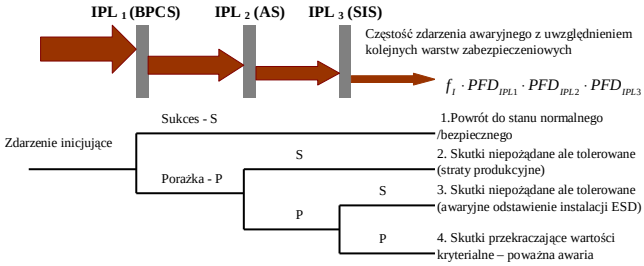


Rysunek 2. Warstwy zabezpieczeniowo – ochronne w obiektach podwyższonego ryzyka

Następnie za pomocą metody LOPA dokonywana jest ocena ryzyka scenariusza awaryjnego po zastosowaniu warstw zabezpieczeniowych i porównanie wyników z wartością tolerowaną.
Spełnienie kryteriów bezpieczeństwa może zostać osiągnięte za pomocą różnych technik. Metoda LOPA nie sugeruje jakie warstwy zabezpieczeniowe należy zaimplementować., ale jest pomocna podczas dokonywania wyboru pomiędzy alternatywnymi rozwiązaniami. W przypadku konieczności przeprowadzenia szczegółowej analizy ryzyka, lub gdy system jest złożony sugerowana jest analiza ilościowa CPQRA (*Chemical Process Quantitative Risk Analysis*).
Podstawowymi elementami niezbędnymi do przeprowadzenia analizy ryzyka wystąpienia scenariusza awaryjnego z wykorzystaniem metody LOPA są (kroki 4, 5 oraz 6 na *Rysunku 1*): częstość zdarzenia inicjującego, krytyczność skutków określona na podstawie zdefiniowanych kategorii oraz prawdopodobieństwo niewypełnienia funkcji związanych z bezpieczeństwem na przywołanie PFD (*Probability of Failure on Demand*) lub prawdopodobieństwa błędu człowieka HEP (*Human Error Probability*) przez poszczególne, niezależne bariery dla każdego zidentyfikowanego scenariusza awaryjnego.
Wartość ryzyka po zastosowaniu warstw dla każdego scenariusza (para przyczyna – skutek) obliczana jest na podstawie wzoru 1 [5]:

$$f_i^C = f_i^I \times \prod_{j=1}^{J} PFD_{ij} = f_i^I \times PFD_{i1} \times ... PFD_{iJ} \quad (1)$$

gdzie f_i^C jest częstością wystąpienia zdarzenia niebezpiecznego dla *i-tego* scenariusza awaryjnego (stałe konsekwencje C); f_i^I oznacza częstość wystąpienia *I-tego* zdarzenia inicjującego z rozpatrywaniem *i – tego* scenariusza awaryjnego; PFD_{iJ} jest prawdopodobieństwem nie wykonania funkcji prze *j-tą* warstwę.
Identyfikacja i budowa scenariuszy awaryjnych opiera się na metodzie drzew zdarzeń ET (*Event Tree*). Na *Rysunku 3* wyspecyfikowano trzy warstwy ograniczające prawdopodobieństwo wystąpienia awarii, które są kluczowe w trakcie analizy zajścia scenariusza za pomocą metody LOPA. Wyszczególniono także cztery skutki końcowe (1-4) oraz określono krytyczność ich konsekwencji, przy czym skutek czwarty jest najbardziej krytyczny, ale występujący najrzadziej. W trakcie projektowania warstw zabezpieczeniowych w celu zapobiegania wystąpieniu poważnej awarii skutek najbardziej krytyczny jest traktowany jako reprezentatywny w kontekście spełnienia kryteriów bezpieczeństwa.



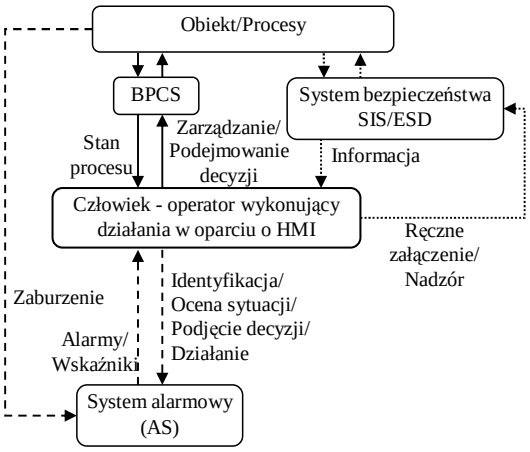
Rysunek 3. Drzewa zdarzeń w metodzie LOPA

Częstość zdarzenia po zastosowaniu warstw oraz przypisaniu do każdej z nich wartości PDF zostaje wyznaczona z wykorzystaniem wzoru (1) przy założeniu niezależności warstw.
Istotnym jest jednak zwrócenie uwagi na fakt, że biorąc pod uwagę wpływ czynników ludzkich i organizacyjnych w każdej z warstw, nie mogą one zawsze być traktowane jako strukturalnie i funkcjonalnie niezależne. Metodyka LOPA nie uwzględnia zależności pomiędzy poszczególnymi warstwami zabezpieczeniowymi, a także w sposób niedostateczny uwzględnia czynniki ludzkie co jest jej istotnym ograniczeniem.
Po przeprowadzonej analizie należy sprawdzić czy wartość ryzyka leży w obszarze tolerowanym. Jeśli nie należy dokonać koniecznych zmian w projektowanych warstwach, aby spełnić kryteria bezpieczeństwa.

3. Wybrane zagadnienia projektowania systemów alarmowych oraz rola człowieka–operatora

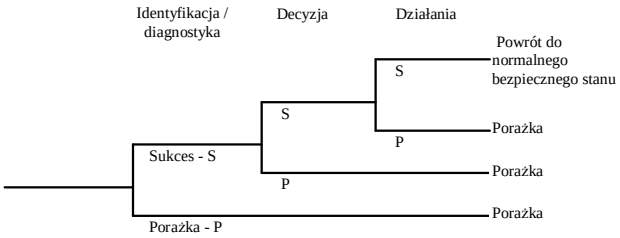
Działania człowieka – operatora w każdej z warstw zabezpieczeniowych mogą być różne, dlatego

wymagają szczególnego traktowania, a analiza tych działań jest niezbędna z punktu widzenia zapewnienia wymaganego poziomu niezawodności i bezpieczeństwa całego systemu technicznego [4], [6], [7]-[10]. Rolę i zadania operatora w różnych warstwach i stanach instalacji podwyższonego ryzyka przestawiono schematycznie na *Rysunku 4*.
W stanach awaryjnych obiektu rola operatora oraz właściwe wykonywanie zadań jest szczególnie ważne. Skuteczność działania operatora w takich sytuacjach zostaje oszacowana z wykorzystaniem odpowiedniej metody analizy niezawodności człowieka HRA (*Human Reliability Analysis*). Dekompozycja zadań wykonywanych przez operatora w stanach awaryjnych została zaprezentowana na *Rysunku 5*.



Rysunek 4. Rola oraz zadania operatora w różnych stanach obiektu

Wyniki analizy HRA zależą w znacznym stopniu od wydajności zaprojektowanego na obiekcie systemu alarmowego oraz mają istotny wpływ w oszacowaniu niezawodności całego systemu podczas analizy ryzyka w wykorzystaniem metody LOPA. Dlatego analiza HRA powinna być wykonywana podczas analizy ryzyka obiektu technicznego oraz włączana do modelu probabilistycznego rozważanego systemu technicznego.



Rysunek 5. Dekompozycja zadań operatora w sytuacji alarmowej

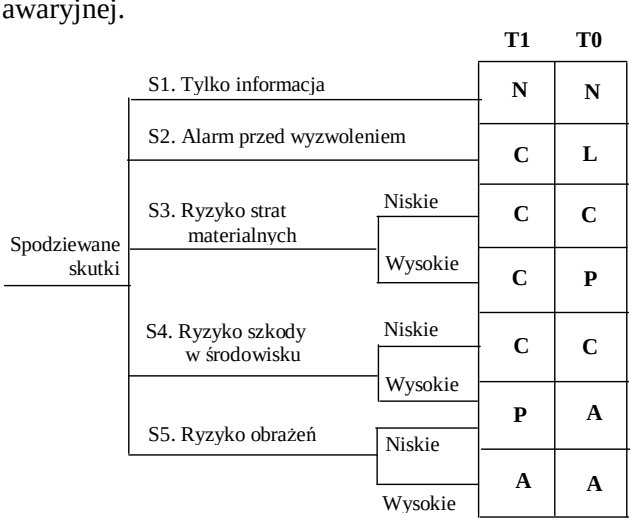
W obecnej praktyce inżynierskiej bazując na informacjach zawartych w normach związanych z bezpieczeństwem (norma ogólna PN-EN 61508 oraz norma PN-EN 61511 poświęcona sektorowi przemysłu procesowego) oraz literaturze we wstępnych oszacowaniach (analiza jakościowa) związanych ze skutecznością działania operatora dla różnych rozwiązań funkcjonalnych systemu alarmowego stosuje się wartości podane w *Tabeli 2* [1], [5].

Tabela 2. Wymagania probabilistyczne dla systemu alarmowego [1]

PFD systemu alarmowego	**Integralność systemu alarmowego / wymagania niezawodnościowe**	**Wymagania niezawodnościowe człowieka - operatora**
1 - 0.1 (alarm standardowy)	Alarm może zostać zaprojektowany jako część systemu DCS	Brak specjalnych wymagań dla osiągnięcia wymaganego poziomu PFD
0.1- 0.01 (alarm związany z bezpieczeństwem)	System alarmowy powinien zostać zaprojektowany jako IPL (*safety related)* na poziomie SIL1 zgodnie z normą IEC 61508	Operator powinien zostać przeszkolony w zarządzaniu systemem alarmowym oraz obiektem. System alarmowy powinien być bardzo przejrzysty i niezwykle prosty w obsłudze. Alarm powinien pozostawać na widoku przez cały czas gdy jest aktywny. Operator powinien posiadać jasną, pisemną procedurę działania dla danego alarmu
Poniżej 0.01	System alarmowy powinien zostać zaprojektowany jako związany z bezpieczeństwem i posiadać kategorię przynajmniej SIL2	Nie jest zalecane, aby w jakiejkolwiek sytuacji przypuszczać, że operatora może mieć wartość poniżej 0.01

W celu zapewnienia redukcji ryzyka na określonym poziomie przez system alarmowy (wartość PFD w *Tabeli 2*), obejmujący sprzęt, oprgramowanie i operatora, zostały opracowane wymagania odnośnie do integralności systemu w ramach konkretnych warstw zabezpieczeniowych oraz wymagania jakie musi spełniać w nich operator.
Ponadto decyzja odnośnie do implementacji systemu alarmowego w ramach warstwy BPCS lub jako niezależnej warstwy zabezpieczeniowej może zostać

podjęta na podstawie analizy następujących parametrów ryzyka za pomocą grafu jakościowego przedstawionego na *Rysunku 6* z uwzględnieniem spodziewanych skutków w przypadku wystąpienia sytuacji awaryjnej, poziomu ryzyka oraz czasu dostępnego na reakcję przez operatora [1].
Warto zwrócić uwagę, że przedział czasowy określony jako krótki wynosi 10 minut i wynika w trudności diagnozowania aktualnego stanu procesu przez operatora w przypadku wystąpienia sytuacji awaryjnej.

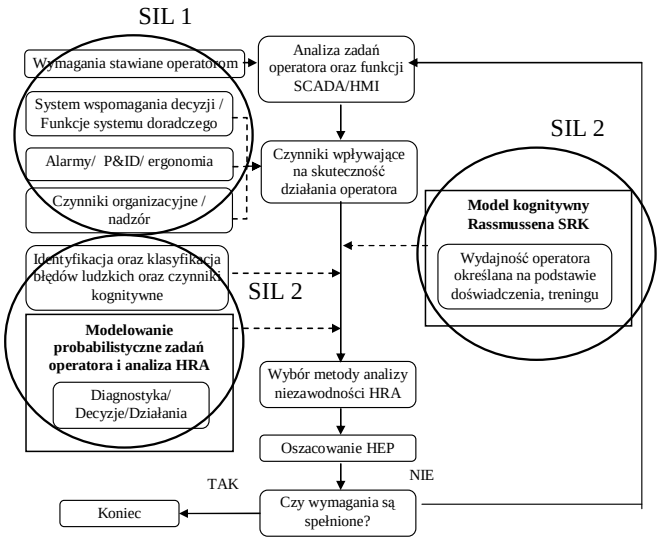


TO – wymagany bardzo krótki czas reakcji operatora, do 10 min.
T1 – dozwolony dłuższy czas reakcji operatora, powyżej 10 min.
N – informacja do przekazywania poza alarmem,
L – ograniczona korzyść stosowania alarmu,
C – rekomendowany alarm w ramach BPCS,
P – do zaakceptowania oddzielny system alarmowy lub w ramach BPCS,
A – rekomendowany oddzielny system alarmowy.

Rysunek 6. Wpływ parametrów ryzyka na założenia projektowe systemu alarmowego (na podstawie [1])

4. Analiza niezawodności człowieka i wyzwania

W przypadku konieczności oszacowania wartości prawdopodobieństwa błędu człowieka HEP (*Human Error Probability*), w celu weryfikacji proponowanych rozwiązań projektowych w ramach warstw zabezpieczeniowych, korzysta się z jednej z dostępnych metod, które można podzielić na: bazujące na wiedzy ekspertów np. SLIM (*Success Likelihood Index*), półilościowe np. SPAR-H (*Standarized Plant Analysis Risk – Human Reliability Analysis Method*) lub ilościowych np. THERP (*Technique of Human Error Rate Prediction*) [3], [6], [9], [10].
W niniejszym opracowaniu skorzystano w rozdziale 5 z metody SPAR-H z pewnymi uproszczeniami. Na *Rysunku 7* została przedstawiona wstępna propozycja procedury ułatwiającej wybór metody analizy niezawodności człowieka w zależności od wymaganego poziomu skuteczności działań operatora (wartość HEP lub odpowiednio SIL). Propozycja zakłada uwzględnienie grupy czynników podczas projektowania systemu alarmowego z celu zapewnienia wydajności działana systemu w tym także zadań realizowanych przez operatora na poziomie SIL1 lub SIL2.
Po wykonaniu projektu w celu weryfikacji proponowanych rozwiązań na poziomie SIL1 można skorzystać z metod bazujących na opinii ekspertów lub z metod półilościowych (np. metoda SPAR –H opisana w przykładzie poniżej).
Jeżeli zadania związane z interwencjami operatora są złożone, a wymagana skuteczność jest na poziomie SIL2 rozwiązania powinny zostać zweryfikowane za pomocą metod ilościowych np. THERP. Dodatkowo należy uzwględnić dodatkowe czynniki podczas projektowania takiego systemu [2], [7]-[13].
Nie należy przy tym zakładać, że jakiekolwiek działania związane z pracą systemu alarmowego, a także z zadaniami wykonywanymi przez operatora mogą być na poziomie wyższym niż SIL2.



Rysunek 7. Propozycja procedury ułatwiającej wybór metody analizy niezawodności człowieka

5. Przykład analizy LOPA z uwzględnieniem czynników ludzkich

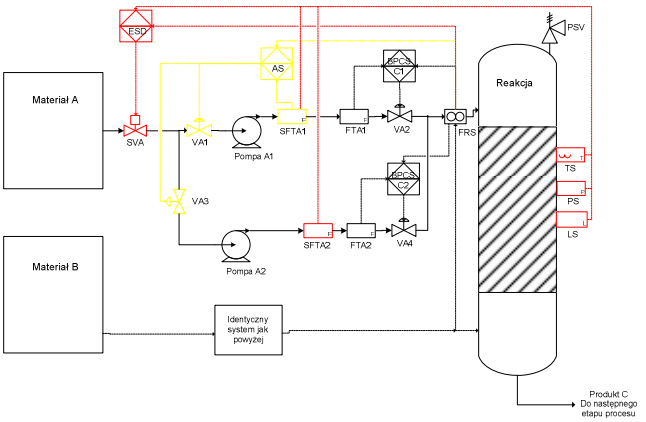
Na poniższym rysunku przedstawiono zbiornik w którym zachodzi reakcja chemiczna. Analizowany obiekt składa się z kilku elementów niezbędnych do jego poprawnego funkcjonowania: dwa zbiorniki w których przechowywane są substancje A oraz B, rurociągi transportujące materiały A i B do zbiornika reakcyjnego, w którym następuje mieszanie obu substancji i otrzymywany jest produkt C. Każdy rurociąg jest wyposażony w zestaw czujników

mierzących najważniejsze zmienne procesowe oraz elementów wykonawczych wykonujących odpowiednie do kontekstu sytuacji funkcje.
Podczas normalnego stanu procesu wykonywane są następujące pomiary: poziom przepływu substancji A i B (FTA1, FTA2), współczynnik proporcji przepływu (FRS) zaprojektowany jako system K z N czujników. Sterowanie przepływem mediów odbywa się za pomocą zaworów (VA2, VA4). Proces jest sterowany automatycznie za pomocą systemu BPCS (wizualizacja procesu jest dostępna za pomocą ekranów C1 oraz C2) i nie wymaga interwencji operatora, którego zadaniem jest nadzór nad jego poprawnym przebiegiem.
W celu wspierania operatora podczas awaryjnych stanów obiektu jako oddzielna strukturalnie i funkcjonalnie warstwa, został zaimplementowany system alarmowy składający się z następujących elementów: czujnik przepływu (SFTA1), system wizualizacji (AS) oraz zawory VA1 (otwarty podczas normalnego stanu procesu) i VA3 (zamknięty podczas normalnego stanu procesu).
W przypadku braku świadomości operatora na temat aktualnej sytuacji, błędnej diagnostyki lub braku reakcji na czas system SIS powinien zatrzymać proces technologiczny W analizowanym przypadku system SIS składa się z następujących komponentów: czujnik przepływu (SFTA1, SFTA2), czujniki ciśnienia (PS), temperatury (TS) i poziomu (LS) w zbiorniku reakcyjnym oraz zaworu odcinającego SVA. System sterowania i automatyki zabezpieczeniowej jest redundantny dla każdego z mediów (rurociągów) dostarczanych do zbiornika reakcyjnego.

Tabela 3. Przykładowa matryca ryzyka

Kategoria skutku → Częstość skutku, a^{-1}↓	Kategoria 1	Kategoria 2	Kategoria 3	Kategoria 4	Kategoria 5
$<10^{-1},10^{-2})$					
$<10^{-2},10^{-3})$					Start
$<10^{-3},10^{-4})$					
$<10^{-4},10^{-5})$					
$<10^{-5},10^{-6})$					

Aby proces mógł przebiegać w sposób bezpieczny łatwopalne medium A powinno być dostarczane bez przerwy do zbiornika reakcyjnego w ilości większej od łatwopalnego medium B, aby nie doprowadzić do wybuchu. Reakcja mieszania musi odbywać się w określonej temperaturze oraz ciśnieniu.



Rysunek 8. Przykład analizy warstw zabezpieczeń LOPA

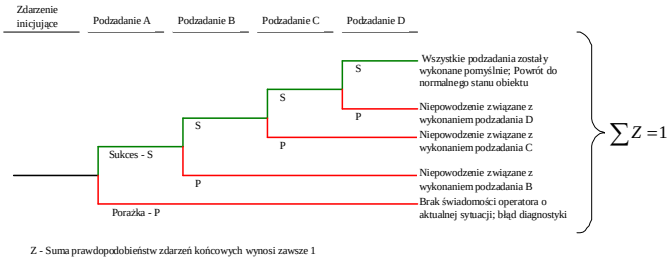
Przykładowy scenariusz awaryjny zakłada uszkodzenie pompy A1 za pośrednictwem której medium A jest dostarczane do zbiornika reakcyjnego oraz uszkodzenie systemu sterowania BPCS (C1). W wyniku utraty BPCS operator nie może odczytać na monitorze C1 uszkodzenia pompy A1 oraz nie może zostać załączony rurociąg standby oraz pompa A2. Skutkiem uszkodzenia pompy A1 jest zatrzymanie dopływu medium A do zbiornika reakcyjnego co może w ograniczonym horyzoncie czasowym doprowadzić do zaburzenia ustalonej proporcji mediów A i B w zbiorniku reakcyjnym. W najgorszym przypadku zdarzenie awaryjne może doprowadzić do eksplozji zbiornika.
W najbliższej okolicy nie pracuje personel więc negatywne skutki będą związane ze stratami sprzętu oraz infrastruktury (straty ekonomiczne). W celu wykonania analizy LOPA zostały zdefiniowane następujące założenia przedstawione poniżej, w raporcie HAZOP w tablicy nr 1 oraz w matrycy ryzyka w *Tabeli 3* (krok 2 analizy LOPA na *Rysunku 1*):

- Częstość zdarzenia inicjującego: (uszkodzenie pompy x uszkodzenie BPCS): 10^{-2},
- Ryzyko akceptowane: 10^{-5},
- Konieczna redukcja ryzyka: 10^{-3},
- Wymagania dla niezależnych warstw zabezpieczeniowych IPL (PFD/HEP) [a^{-1}]: BPCS: 10^{-1};AS: 10^{-1};SIS: 10^{-2}

W celu weryfikacji czy zaprojektowany system alarmowy spełnia stawiane mu wymagania zostanie przeprowadzona analiza HRA dla analizowanego scenariusza awaryjnego z wykorzystaniem metody SPAR – H [3].
Przywrócenie instalacji do stanu bezpiecznego będzie wymaga od operatora wykonania następujących czynności w odpowiedniej sekwencji:

A. Identyfikacja braku przepływu medium A do zbiornika reakcyjnego za pomocą funkcji HMI systemu alarmowego (AS) w czasie do 10 minut (identyfikacja aktualnej sytuacji),
B. Ręczne zamknięcie zaworu VA1 w celu izolacji rurociągu głównego,
C. Otwarcie zaworu VA3 w ceku inicjalizacji rurociągu standy,
D. Inicjalizacja pompy A2,

Analiza HRA za pomocą SPAR – H dla zdefiniowanej sekwencji składa się z następujących kroków:
Krok 1: Dekompozycja analizowanej sekwencji na podzadania oraz przypisanie im trybu diagnostyki lub działania. Drzewo zdarzeń analizy HRA przedstawia poniższy rysunek:



Rysunek 9. Przykład dekompozycji sekwencji awaryjnej na podzadania

W analizowanym scenariuszu awaryjnym tylko podzadanie A wymaga diagnostyki sytuacji. Pozostałe podzadania (B, C, D) zostały zdefiniowane jako działania.
Krok 2: Przypisanie wartości (opinia ekspercka) dla każdego z czynników kształtujących wydajność operatora PSF (*ang. Performance Shaping Factors*) dla przyjętej skali liczbowej. W metodzie SPAR – H wyróżnia się osiem czynników PSF (*Tabela 4* poniżej).

Tabela 4. Czynniki kształtujące wydajność operatora PSF

PSF		OPIS	ZAKRES	PODZADANIE			
				A	B	C	D
I	Dostępny czas	Czas nieadekwatny (10) dodatkowy czas (0,1)	<0,1;10>	5	2	2	2
II	Stres	Nominalny (1) ekstremalny (5)	<1;5>	2	2	1	1
III	Doświadczenie i trening	Niski (10) wysoki (0,5)	<0,5;10>	0,5	1	1	1
IV	Złożoność zadania	Złożone (5) oczywiste (0,1)	<0,1;5>	3	2	1	1
V	Ergonomia i HMI	Myląca (50) Dobra (0,5)	<0,5;50>	0,5	0,5	0,5	1
VI	Dostępność procedur	Niedostępne (50) diagnostyczne (0,5)	<0,5;50>	0,5	1	1	1
VII	Zdolność do pracy	Nominalna (1) słaba(5)	<1;5>	1	1	1	1
VIII	Czynniki organizacyjne	Dobre (0,5) słabe (5)	<0,5;5>	1	1	1	1

Krok 3: Oszacowanie wartości HEP dla każdego podzadania bez uwzględnienia zależności z wykorzystaniem wzoru 2:

$$P_k = HEP = \frac{NHEP \cdot PSF_{złożon}}{NHEP \cdot (PSF_{złożon} - 1) + 1} \qquad (2)$$

gdzie $NHEP_{diagnostyka} = 0.01$; $NHEP_{działał} = 0.001$; P_k oznacza prawdopodobieństwo błędu człowieka (HEP) bez uwzględnienia zależności.
Wartości PSF poniżej 1 mają pozytywny wpływ na działania operatora, natomiast powyżej 1 negatywny, wartość 1 jest uważana za nominalną/lub dany czynnik nie ma wpływu na efektywność wykonania podzadania.

Krok 4: Obliczenie prawdopodobieństwa sukcesu dla analizowanej sekwencji z wykorzystaniem wzoru 3:

$$S_{B/Z} = \prod_{k}^{n} S_k \qquad (3)$$

gdzie S_k to prawdopodobieństwo sukcesu dla *k*–tego podzadania w sekwencji bez uwzględnienia zależności.

Prawdopodobieństwo braku sukcesu dla analizowanej sekwencji obliczane jest według (4)

$$P_{B/Z} = 1 - S_{B/Z} \qquad (4)$$

gdzie $P_{B/Z}$ to prawdopodobieństwo porażki dla rozważanej sekwencji awaryjnej.
Uzykane wyniki zawarto w *Tabeli 5*.

Tabela 5. Wyniki analizy

	Podzadanie			
	A	B	C	D
P_k	0,04	0,004	0,001	0,002

S_k	0,96	0,996	0,999	0,998
$S_{B/Z} = \prod_k^n S_k \approx 0{,}95 \Rightarrow P_{B/Z} = \prod_k^n P_k \approx 0{,}05$				

Wyniki analizy pokazują, że zaproponowane rozwiązania projektowe systemu alarmowego zapewniają skuteczność działania operatora na poziomie SIL1. Analiza została wykonana w uproszczonej formie bez uwzględniania zależności pomiędzy zdarzeniami co powoduje, że otrzymane wyniki są optymistyczne. W celu bardziej dokładnego zweryfikowania skuteczności działania operatora w sytuacji złożonej należy skorzystać z metody ilościowej np. THERP.

6. Podsumowanie

Celowe jest rozwijanie metodyki uwzględniania analiz niezawodności człowieka w ramach analizy LOPA, co ma duże znaczenie praktyczne. Dostępne obecnie dokumenty normatywne wymienione w opracowaniu nie zawierają w wystarczającym stopniu wytycznych, ani wskazań metodycznych, uwzględniających poruszone w niniejszym artykule aspekty analizy warstw zabezpieczeń w obiektach podwyższonego ryzyka.

Podziękowania

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] Allars, K. (2007). *Alarm Systems. A Guide to Design, Management and Procurement*. The Engineering Equipment and Materials Users' Association - Publication No 191.Edition 2.

[2] Blackman, H.S. & Gertman, I.D. (1994). *Human Reliability and Safety Analysis Data Handbook*. Wiley-Interscience Publication. New York.

[3] Blackman, H.S. & Gertman, I.D. (2004). The SPAR-H Human Reliability Analysis Method. U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, DC 20555 – 0001, NUREG/CR-6883, INL/EXT-05-00509.

[4] Carey, M. (2001). Proposed Framework for Addressing Human Factors in IEC 61508. Prepared by Amey VECTRA Ltd. for Health and Safety Executive (HSE), U.K. Contract Research Report 373.

[5] Dowell, A. M. (2001). *Layer of Protection Analysis - Simplified Process Risk Assessment.* Center for Chemical Process Safety. American Institute of Chemical Engineers, New York 10016-5991.

[6] Guttmann, H.E. & Swain, A.D. (1983). Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Final Report. NUREG/CR-1278, Washington, DC (USA).

[7] Hollnagel, E. (2005). *Cognitive Reliability and Error Analysis Method CREAM*. Elsevier Science Ltd. 1988, new edition.

[8] Hollnagel, E. (2005). Human reliability assessment in context. *Nuclear Engineering and Technology*, Vol.37, 2, 159-166.

[9] Humphreys, P. (1988). Human Reliability Assessors Guide. Safety & Reliability Directorate. Wigshaw Lane, Culcheth, Warrington WA3 4NE.

[10] Mertens, J., Reer, B. & Strater, O. (1996). *Evaluation of Human Reliability Analysis Methods Addressing Cognitive Error Modelling and Quantification.* Julich: Berichte des Forschungszentrums 3222.

[11] Kacprzak, P. & Kosmowski, K.T. (2009). Human factors in the layer of protection analysis with emphasis on alarm system management. *Materiały konferencji ESREL*, Prague 2009, Reliability, Risk, and Safety - Theory and Applications (ed. by Radim Bris, Carlos Guedes Soares, Sebastián Martorell). ISBN: 978-0-415-55509-8, Published by CRC Press.

[12] Rasmussen, J. (1983*). Skills, rules, knowledge; signals, signs and symbols and other distinctions on human performance models. IEEE Transaction on Systems, Man and Cybernetics*, SMC-13/3.

[13] Reason, J. (1990). *Human Error*. Cambridge University Press.

[14] IEC 61508 (1998). Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-Related Systems. Parts 1-7. International Electrotechnical Commission, Geneva, Switzerland.

[15] IEC 61511 (2003). Functional Safety: Safety Instrumented Systems for the process industry sector. Parts 1-3. International Electrotechnical Commission, Geneva, Switzerland.