Kosmowski Kazimierz T.
Politechnika Gdańska, Gdańsk, Polska

Human factors and functional safety analysis
Czynniki ludzkie i analiza bezpieczeństwa funkcjonalnego

Keywords / Słowa kluczowe

human factors, human errors, functional safety, human reliability analysis, layers of protection
czynniki ludzkie, błędy człowieka, bezpieczeństwo funkcjonalne, analiza niezawodności człowieka, warstwy zabezpieczeń

Abstract

In this article some issues concerning the safety management in computerized complex hazardous plant are presented in the context of human factors. It has been shown that the risk of losses can be significantly reduced using appropriate technical solutions in the form of a layer protection system, which includes a basic process control system, human-operator and protection automatics. The significance of appropriate designing of interfaces including functions of the alarm system is emphasized. It will contribute to reducing the human-operator error probability. The functional safety management, which includes the risk control in a life cycle of complex plant, should be carried out in relation to requirements associated with possible avoiding of software systematic failures in programmable systems and reducing the frequency of hardware random failures.

1. Wprowadzenie

W niniejszym artykule przedstawia się wybrane zagadnienia dotyczące zarządzania bezpieczeństwem funkcjonalnym w złożonym obiekcie podwyższonego ryzyka. Zwraca się uwagę na problem możliwości niekorzystnego wpływu tzw. czynników ludzkich, jeśli zastosowane interfejsy i procedury realizacji zadań przez człowieka-operatora zostały zaprojektowane niewłaściwie.

Wymaga to przeprowadzenia analizy niezawodności człowieka-operatora w kontekście zarządzania bezpieczeństwem funkcjonalnym programowalnych systemów sterowania i zabezpieczeń [13]. Jest to zagadnienie ważne, ponieważ z różnych badań wynika, że niewłaściwie kształtowane czynniki ludzkie i uchybienia organizacyjne stanowią źródłową przyczynę aż od 70 do 90% zdarzeń awaryjnych, zależnie od kategorii obiektu technicznego [11], [12], [20].

Ocena możliwości powstania sytuacji zagrożenia i zdarzeń awaryjnych ma szczególne znaczenie w obiektach i systemach tzw. infrastruktury krytycznej, przy czym wspomniane działania intencyjne mogą być zainicjowane wewnątrz obiektu lub z zewnątrz. Działania takie dotyczą również stosowanych obecnie szeroko technologii i systemów programowanych, w tym systemów sterowania i zabezpieczeń, w postaci ataków hackerskich.

Zarządzanie bezpieczeństwem funkcjonalnym obejmuje zagadnienia sterowania ryzykiem w cyklu życia analizowanego obiektu złożonego w odniesieniu do wymagań zawartych w normie IEC 61508 [10]. Dotyczą one zmniejszenia ryzyka związanego z potencjalnym występowaniem zdarzeń nienormalnych lub awaryjnych, stosując m.in. programowalne systemy sterowania i zabezpieczeń.

Aby osiągnąć odpowiednią redukcję ryzyka przez te systemy, muszą być one właściwie zaprojektowane i odpowiednio eksploatowane w cyklu życia obiektu. Należy zastosować rozwiązania sprzyjające unikaniu błędów systematycznych, szczególnie oprogramowania (*software*) oraz uszkodzeń wyposażenia technicznego (*hardware*), zwłaszcza o charakterze losowym. Istotnym problemem w eksploatacji obiektów podwyższonego ryzyka są możliwe uszkodzenia CCF (*common cause failures*) w systemach zabezpieczeń z nadmiarowością strukturalną [14] oraz CCF w barierach – warstwach zabezpieczeniowo-ochronnych [17]. Dotyczy to

zwłaszcza warstw zabezpieczeniowych zawierających moduły i systemy programowalne [19] oraz człowieka operatora [15], [16]
Dużym problemem są w takich systemach potencjalne błędy człowieka [13], [16]. Zmniejszenie ich wpływu jest możliwe po rozpoznaniu mechanizmów popełniania błędów podczas wykonywania zadań przez człowieka-operatora - szeroko rozumianego, w tym w zespole ludzi współpracujących w sterowni lub w brygadzie dokonującej przeglądy profilaktyczne lub remonty.

2. Rozwiązania bezpieczeństwa funkcjonalnego a czynniki ludzkie

W normie IEC 61508 [10] napotyka się stosunkowo często wymagania dotyczące analizy czynników ludzkich. Wiadomo, szeroko rozumiane czynniki ludzkie i organizacyjne mają zwykle istotny wpływ na niezawodność i bezpieczeństwo systemów. W raporcie [3] zestawiono wiele odwołań do szeroko rozumianej problematyki czynników ludzkich, które pojawiają się w różnych częściach tej normy. Tak więc, norma IEC 61508 podkreśla znaczenie czynników ludzkich w analizie bezpieczeństwa funkcjonalnego, jednak nie zawiera jednoznacznych wymagań i odwołań metodycznych dotyczących analizy wpływu czynników ludzkich.
Czynniki ludzkie w nawiązaniu do normy IEC 61508 dotyczą między innymi:

- oceny potencjalnych błędów człowieka i działań korekcyjnych (restytucyjnych) w analizie zagrożeń i analizie ryzyka;
- planowania i wykonywania procedur operacyjnych i obsługi wyposażenia;
- projektowania interfejsu użytkownika (np. operator-system sterowania, operator-system automatyki zabezpieczeniowej, operator-system komputerowy wizualizacji procesu).

Odpowiednie analizy czynników ludzkich należy przeprowadzać we wszystkich fazach cyklu życia. Na przykład w fazie 3 - *Analiza zagrożeń i ryzyka* należy [10]:

- Włączyć wszystkie stosowne kwestie czynników ludzkich (Cześć 1/ 7.4.2.3; Część 4/ 3.2.4Przypis3; Część 5/ A.4; Część 6/ A.2i);
- Uwzględnić wyobrażalne niewłaściwe użytkowanie (Część 1/ 7.4.1.1; Część 4/ 3.1.11);
- Szczególną uwagę poświecić nienormalnym lub nieczęstym rodzajom pracy (Część 1/ 7.4.1.1)
- Wyszczególnić wiarygodne ograniczenia w działaniu lub interwencji człowieka (i odpowiednio udokumentować) (Część 1/ 7.4.2.10; Część 5/ A.4).

Natomiast w fazie 9 - *Realizacja systemów E/E/PE związanych z bezpieczeństwem*, wymaga się, aby:

- Wymagania bezpieczeństwa mają identyfikować obszary oddziaływania operatora i powinny być one uwzględnione podczas projektowania (Część 2/ 7.2.3.1, Część 2/ 7.4.4.5; Część 2/ 7.6.2.3; Część 3/ 7.2.2.4f; Część 6/ A.1);
- Projekt E/E/PE ma tolerować potencjalne błędy operatora sterowanego wyposażenia (Część 2/ 7.4.8.1c; Część 2/ tabl. A.18; Część 3/ 7.9.2.13c; Część 7/ B.4.6);
- Projekt systemów E/E/PE związanych z bezpieczeństwem ma uwzględniać możliwości i ograniczenia człowieka i być odpowiedni dla działań przypisanym operatorom i personelowi obsługi (Część 2/ 7.4.8.3; Część 7/ B.4.2, B.4.3);
- Projekt wszystkich interfejsów ma być zgodny z dobrą praktyką czynników ludzkich i uwzględniać przewidywany poziom wyszkolenia i świadomości operatorów (Część 2/ 7.4.8.3; Część 7/ B4.8);
- Wszystkie procedury użytkowania i obsługi systemów E/E/PE mają być sprawdzane poprzez testowanie i/lub analizę (Część 1/ tabl. 1, nr 7);
- Ocena uszkodzeń grupowych od wspólnej przyczyny (CCF) ma uwzględniać stosowne aspekty czynników ludzkich (Część 6/ tabl. D1).

W nawiązaniu do tych wymagań, przydatne w analizie czynników ludzkich mogą być następujące metody analizy lub inżynierie [3], [13]:

- Metoda analiza niezawodności człowieka *HRA* (*human reliability analysis*), umożliwiająca ocenę wpływu błędów człowieka na prawdopodobieństwo niewypełnienia funkcji przez wyposażenie sterowane *EUC* (*equipment under control*);
- Metoda analizy współdziałania człowiek – komputer *HCI* (*human - computer interaction*), a ostatnio inżynieria użyteczności UE (*usability engineering*), która umożliwia skupienie się na istotnych szczegółach interfejsu człowiek – komputer;
- Inżynieria czynników ludzkich *HFE* (*human factors engineering*), która umożliwia projektowanie wyposażenia, środowiska pracy i zadań użytkownika na poziomie systemu;
- Metoda integracji czynników ludzkich *HFI* (*human factors integration*), która systematyzuje struktury dokumentacyjne i organizacyjne związane z integrowaniem HFE w projekt procesów.

Aby spełnić wymagania normy IEC 61508 niezbędna jest stosowanie kombinacji tych wymagań zależnie od rozwiązywanego problemu. Najbardziej zbliżone są metody *HFE* i *UE*, przy czym metoda *HFE* była do tej pory stosowana głównie w aplikacjach

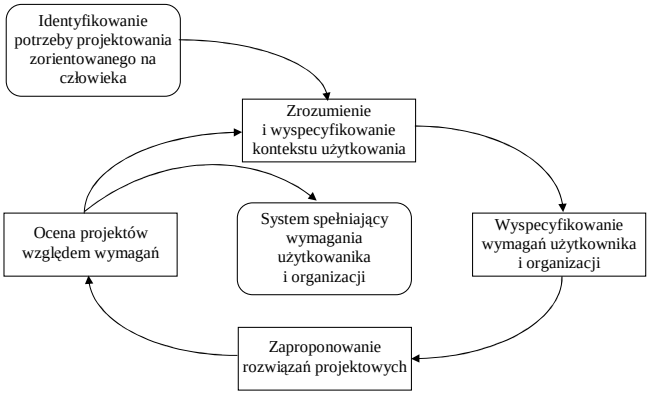
komputerowych i stanowiła podstawę opracowania UE.

Duże znaczenie w modelowaniu probabilistycznym systemu ma stosowanie odpowiedniej metody HRA [2], [6], [7], [11], [16], [22], [23]. Wzrasta ostatnio znaczenie opracowania nowej generacji metod HRA uwzględniających aspekty kognitywne diagnozowania sytuacji nienormalnych, działań i podejmowania przez człowieka-operatora. Niektóre z takich metod wydają się obiecujące [8], [9], chociaż ich niektóre aspekty teoretyczne, a szczególnie praktyczne stosowanie napotykają nadal na szereg trudności.

W procesie projektowania systemów interaktywnych duże znaczenia mają zasady podejścia UE zawarte w normie EN ISO 13407 [5]. Kluczowymi charakterystykami takiego procesu projektowania są:

- aktywny udział użytkownika, zrozumienie jego wymagań i zadań;
- odpowiednia alokacja funkcji między użytkownika i technologię;
- współdziałanie rozwiązań projektowych;
- projektowanie wielodyscyplinarne.

Zadania w procesie projektowania zorientowanego na człowieka przedstawiono na *Rysunku 1*.



Rysunek 1. Procesy w projektowaniu zorientowanym na człowieka (EN ISO 13407)

3. Klasyfikacja zachowań, działań i potencjalnych błędów człowieka

W opracowaniu technik analizy niezawodności człowieka korzysta się często z modelu koncepcyjnego zaproponowanego przez Rasmussena [20], [21]. W wyróżnionych w tym modelu trzech typach zachowań człowieka mogą dominować:

(1) *wprawa* - wykonywanie mniej lub bardziej podświadomie (odruchowo) wypraktykowanych lub wytrenowanych działań na podstawie zapamiętanych wzorów postępowania;

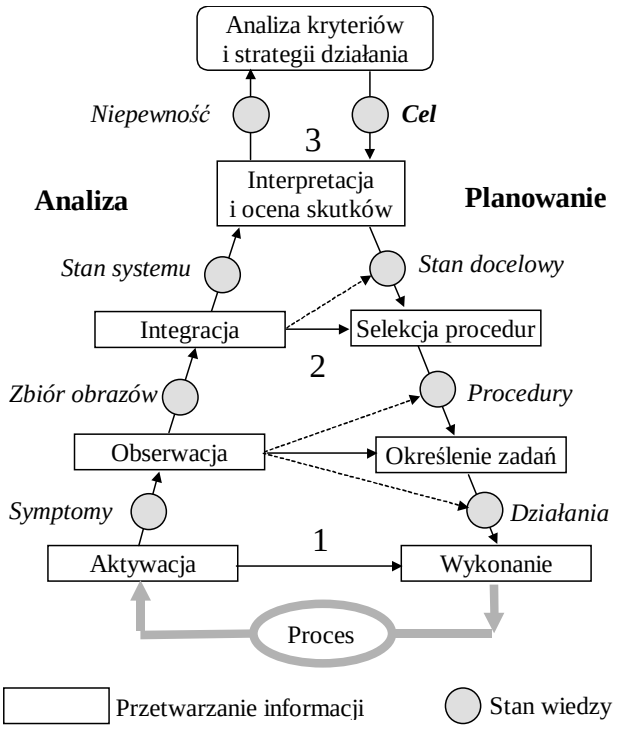
(2) *reguła* - wykonywanie mniej oczywistych działań, w których operator postępuje jednak według zapamiętanych, odczytanych lub przekazanych reguł, uprzednio opracowanych na wypadek wystąpienia symptomów przewidywanych sytuacji;

(3) *wiedza* - działanie w sytuacjach, w których wzorce zachowań lub reguły postępowania nie mogą być zastosowane bezpośrednio, a istotne staje się kognitywne przetwarzanie informacji związane z: rozpoznaniem nowej sytuacji i identyfikacją stanu obiektu, diagnozowaniem tego stanu oraz podejmowaniem racjonalnych decyzji.

Wyróżnione typy zachowań operatorskich oraz drzewo zawierające elementy analizy i planowania przedstawiono na *Rysunku 2*.

Zgodnie z modelem koncepcyjnym Rasmussena w przypadku wystąpienia w sterowni sygnałów prostych zdarzeń operator przystępuje odruchowo do wykonania sterowań (ścieżka 1 – poziom wprawy).

W bardziej złożonych przypadkach operator obserwuje symptomy sytuacji nienormalnej i dokonuje ich porównania z zapamiętanym zbiorem obrazów w myślowym procesie integrowania, co umożliwia selekcje odpowiednich reguł do wykonania (ścieżka 2 – poziom reguł). W przypadku wystąpienia nowej sytuacji operator diagnozuje stan systemu i określa na podstawie strategię działania (ścieżka 3 – poziom wiedzy). Obserwacja zachowań operatorów wykazała, że dokonują oni często działań na skróty, co zaznaczono na rysunku 2 liniami przerywanymi.



Rysunek 2. Schematyczne przedstawienie postępowania operatora na wyróżnionych poziomach: 1 – wprawy, 2 – reguł i 3 – wiedzy

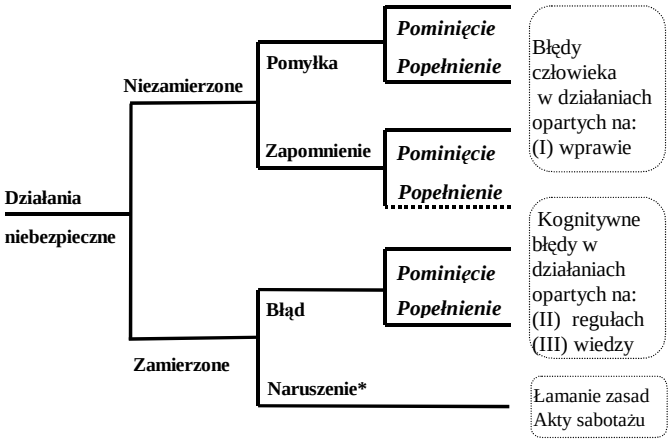
Opisane wyżej rodzaje zachowań związane są z różnymi mechanizmami błędów, które mogą wpływać istotnie na charakterystyki niezawodnościowe człowieka. Upraszczając klasyfikację niewłaściwych zachowań człowieka zaproponowaną przez Reasona [21], wyróżnić można ich trzy podstawowe rodzaje:

I. *Pomyłkę* - rozumianą jako (1) mylne zrealizowanie intencji, planu lub konkretnej decyzji (plan jest poprawny, natomiast jego wykonanie nie jest właściwe) spowodowane m.in. przez nieuwagę lub brak koncentracji, albo (2) niezamierzone działanie;

II. *Zapomnienie* - np. odstępstwo w realizacji kolejnego kroku w zadaniu kontrolno-sterowniczym; odstępstwa wynikają z chwilowych zaników pamięci, zapomnienia intencji lub zaplanowanych kroków działania;

III. *Błąd* - niewłaściwe zaplanowanie i realizacja ciągu działań, co wynika zwykle z niepoprawnego zdiagnozowania sytuacji lub przyjęcia nieprawidłowych decyzji dotyczących celów i strategii postępowania.

Klasyfikację niewłaściwych zachowań człowieka [21] w kontekście wyróżnionych w metodyce THERP [23] dwóch podstawowych rodzajów błędów: pominięcia czynności (*omission*) i popełnienia (*commission*) ze wskazaniem ich możliwych przesłanek (typów zachowań) [20 przedstawiono na *Rysunku 3*.



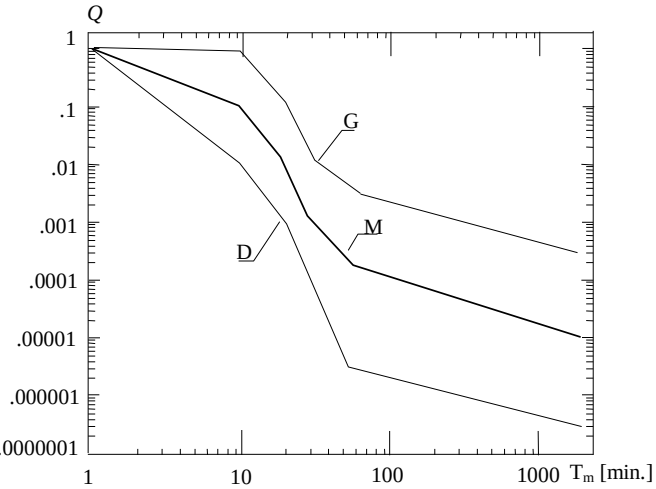
Rysunek 3. Klasyfikacja niewłaściwych zachowań człowieka, rodzajów błędów i ich przesłanek

Błędem kognitywnym nazywa się błąd wynikający z podjęcia niewłaściwej decyzji przez operatora, na przykład z powodu niepoprawnej diagnozy sytuacji, co prowadzi zwykle do określenia nieprawidłowego celu i strategii postępowania lub błędnego zaplanowania działań. Błąd taki występuje więc w kontekście poznawczym (kognitywnym). Błąd kognitywny może prowadzić do niepoprawnego działania lub niepodjęcia działania w wymaganym czasie, określonym przez dynamikę procesu.

W technice THERP [23] przyjęto, że niebezpieczne (niepoprawne) działania mogą przejawiać się jako: *błędy popełnienia* lub *błędy pominięcia*. Przez *błąd popełnienia* rozumie się niepotrzebne wykonanie w danej sytuacji działania lub niewłaściwe wykonanie działania wymaganego przez stan obiektu, co w konsekwencji może spowodować pogorszenie przebiegu procesu w sytuacji awaryjnej. Błąd pominięcia polega natomiast na zaniechaniu lub niezupełnym wykonaniu działań wymaganych w danej sytuacji.

Błędy pominięcia mogą być popełnione podczas przeglądów profilaktycznych i remontów, jak również po wystąpieniu sytuacji awaryjnej z powodu niezupełnego wykonania wymaganej sekwencji działań przez personel operatorski. Za błąd pominięcia uważa się również zupełny brak reakcji personelu operatorskiego w sytuacji nienormalnej [6], [23].

Ważne znaczenie w praktyce HRA ma oszacowanie prawdopodobieństwa błędu diagnozowania Q (*HEP – Human Error Probability*) przez człowieka – operatora stanu nienormalnego lub awaryjnego. *Rysunek 4* przedstawia wykres prawdopodobieństwa popełnienia błędu diagnozy sytuacji awaryjnej w funkcji czasu granicznego, dostępnego na wykonanie diagnozy.



(M - mediana i wartości graniczne: D - dolna i G - górna)

Rysunek 4. Wykresy prawdopodobieństwa błędu zdiagnozowania stanu awaryjnego obiektu złożonego w funkcji czasu granicznego [23]

THERP jest techniką HRA stosowaną nie tylko do szacowania prawdopodobieństw błędów człowieka. Jest ona również przydatna do przeprowadzania badań wpływu błędów człowieka na miary ryzyka związanego z eksploatacją rozważanego obiektu.

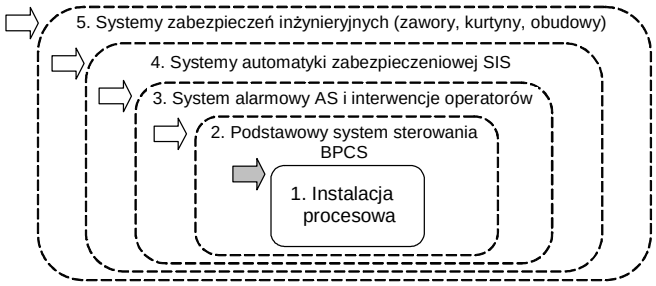
4. Redukcja ryzyka za pomocą warstw zabezpieczeniowo-ochronnych

W instalacji przemysłowej podwyższonego ryzyka poziom ryzyka zmniejsza się stosując na przykład warstwy zabezpieczeniowe uwzględnione na rysunku 5. Zalicza się do nich [17]:

(1) samą instalację procesową, jeśli posiada ona cechy inherentnego bezpieczeństwa,
(2) podstawowy system sterowania BPCS (*basic process control system*),
(3) system alarmowy AS (*alarm system*) z funkcjami diagnostycznymi i wspomagającymi interwencje operatorów,
(4) system automatyki zabezpieczeniowej SIS (*safety instrumented system*), który może pełnić funkcję wyłączania (odstawienia) awaryjnego instalacji ESD (*emergency shutdown system*) oraz
(5) systemy zabezpieczeń inżynieryjnych i lokalizacji skutków awarii (zawory bezpieczeństwa, kurtyny, bariery, obudowy i inne urządzenia).

W nawiązaniu definicji ryzyka społecznego rozważa się ocenę zmniejszenia ryzyka po wprowadzeniu zidentyfikowanej opcji sterowania ryzykiem (OSR), względem opcji bazowej (B) [14], [16].

Jedną z takich opcji może być zastosowanie systemu E/E/PE (elektrycznego/ elektronicznego/ programowalnego elektronicznego) [10] lub SIS [19], pełniących funkcje związane z bezpieczeństwem.



Rysunek 5. Warstwy zabezpieczeniowe instalacji podwyższonego ryzyka

Przy założeniu, że redukcję ryzyka do poziomu tolerowanego można osiągnąć dzięki zastosowaniu funkcji bezpieczeństwa realizowanej za pomocą systemu zabezpieczeniowego E/E/PE lub SIS, zakładając pesymistycznie ten sam poziom strat $N = const$, otrzymuje się wzór na względne obniżenie poziomu ryzyka w postaci [15]

$$r^R = R_t / R_{np} = F_t / F_{np} = r^F \tag{1}$$

gdzie R_{np} jest ryzykiem bez zastosowania rozważanych środków zabezpieczeniowych; F_{np} oznacza częstość zdarzenia zagrażającego przed wprowadzeniem systemu zabezpieczeniowego; R_t jest ryzykiem tolerowanym; F_t oznacza oczekiwaną częstością potencjalnego zdarzenia awaryjnego (wynikającą z poziomu ryzyka R_t) do osiągnięcia po wprowadzeniu środka zabezpieczeniowego; a r^F jest względną redukcją częstości rozważanego scenariusza awaryjnego.

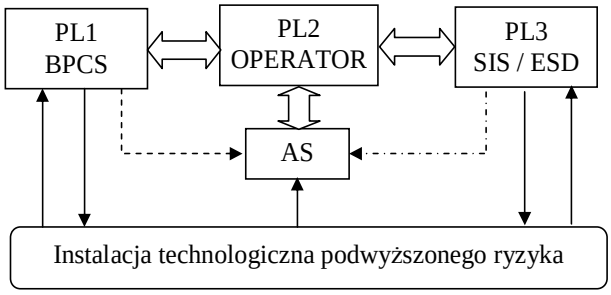
Rozważana funkcja bezpieczeństwa może być realizowana przez pojedynczy system E/E/PE i wówczas przeciętne prawdopodobieństwo niewypełnienia funkcji dla rodzaju rzadkiego przywołania do działania PFD_{avg} (*average probability of failure on demand*) [10] będzie równe $PFD_{avg} = r^F$.

W warstwowym systemie zabezpieczeniowym funkcja bezpieczeństwa jest realizowana przez poszczególne warstwy [11], na przykład warstwy 2, 3 i 4 na *Rysunku 3*. W analizie takiego systemu korzysta się często w praktyce z metody analizy LOPA (ang. *layer of protection analysis*) [9], przy czym dana funkcja bezpieczeństwa nie będzie w pełni wypełniona, jeśli zawiodą wszystkie elementy składowe rozważanej warstwy.

Na *Rysunku 6* przedstawiono trzy warstwy zabezpieczeniowe PL (*protection layer*), które mają zapobiec wstąpieniu zdarzenia awaryjnego o poważnych skutkach:

- PL1 – podstawowy system sterowania BPCS (*basic process control system*),
- PL2 – człowiek-OPERATOR, który nadzoruje proces i interweniuje w razie wystąpienia sytuacji nienormalnej lub awaryjnej sygnalizowanej przez BPCS i/lub system alarmowy AS,
- PL3 – system automatyki zabezpieczeniowej SIS, który pełni funkcję ESD (*emergency shutdown*).

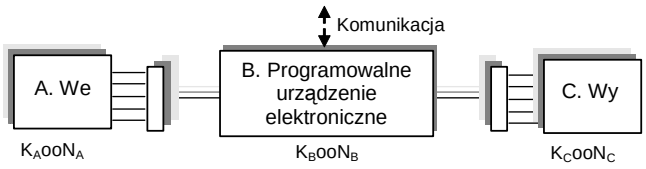
Projektowanie systemu alarmowego (AS) jest zadaniem trudnym. Zasady projektowania AS zawiera poradnik EEMUA (2007).



Rysunek 6. Człowiek OPERATOR w ramach warstw zabezpieczeniowych

Warstwy te powinny być funkcjonalnie i strukturalnie niezależne, chociaż nie zawsze udaje się to uzyskać w praktyce. W przypadku PL1 i PL3 osiąga się to na przykład stosując odrębne tory

sygnałowe, moduły przetwarzania informacji i elementy wykonawcze.
Na *Rysunku 7* przedstawiono uproszczony schemat systemu SIS, który zawiera następujące podsystemy: urządzenia wejściowe (A), programowalne urządzenie elektroniczne (B) i urządzenia wyjściowe (C) oraz urządzenia pomocnicze takie jak tory sygnałowe, zasilanie energią elektryczną i komunikacja w sieci komputerowej. W celu zwiększenia ich niezawodności działania, na przykład zmniejszenia prawdopobieństwa PFD_{avg}, każdy z tych podsystemów może wymagać zastosowania struktury nadmiarowej, na przykład 1oo2, 1oo3 lub 2oo3.



Rysunek 7. Struktura systemu SIS do realizacji funkcji związanej z bezpieczeństwem

Na podstawie modeli probabilistycznych tych podsystemów wyznacza się prawdopodobieństwo niezadziałania na przywołanie PFD_{avg} rozważanego systemu SIS. Przy założeniu bardzo małych wartości prawdopodobieństw niewypełnienia funkcji na przywołanie uzasadnione jest napisanie następującego przybliżonego wzoru dla całego rozważanego systemu S:

$$PFD_{\text{avg}}^{\text{S}} \cong PFD_{\text{avg}}^{\text{A}} + PFD_{\text{avg}}^{\text{B}} + PFD_{\text{avg}}^{\text{C}} \qquad (2)$$

gdzie $PFD_{\text{avg}}^{\text{A}}, PFD_{\text{avg}}^{\text{B}}, PFD_{\text{avg}}^{\text{C}}$ oznaczają prawdopodobieństwami niewypełnienia funkcji na przywołanie odpowiednio przez podsystemy A, B i C.
Odpowiedni poziom SIL (*safety integrity level*) systemu BPCS i SIS oraz wymaganą redukcję ryzyka za pomocą warstwowego systemu zabezpieczeń osiąga się przez odpowiednie rozwiązania architektoniczne podsystemów w nawiązaniu określonych kryteriów probabilistycznych [10], [19]. Występuje jednak problem z warstwą PL2 (OPERATOR), która jest zwykle zależna od warstwy PL1. Na jej zakres niezależności można jednak wpłynąć przez odpowiednie zaprojektowanie systemu alarmowego AS (*Rysunek 6*) i odpowiednie kształtowanie czynników wpływających na niezawodność działania człowieka-operatora, przy czym słowo operator jest rozumiane szeroko [4], [6], [14].

Tylko w przypadku założenia o niezależności rozważanych warstw można napisać następujący wzór na redukcję częstości rozważanego scenariusza awaryjnego [9]

$$F_i = F_i^I \cdot PFD_{i;PL1} \cdot PFD_{i;PL2} \cdot PFD_{i;PL3} = F_i^I \cdot PFD_i \qquad (3)$$

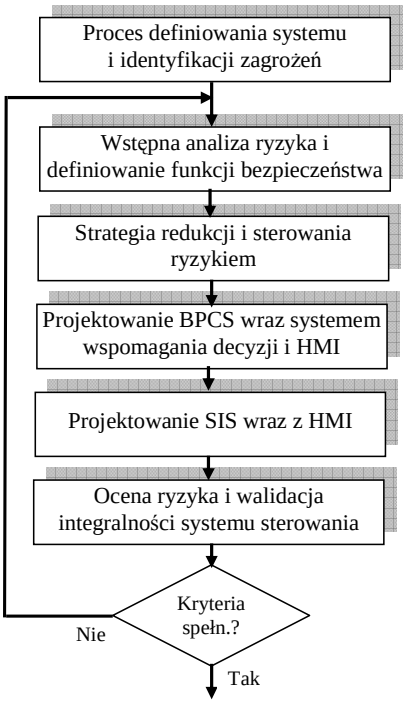
gdzie F_i^I jest częstością *i*-tego zdarzenia inicjującego (*I*), a^{-1}; $PFD_{i;PLj}$ oznacza prawdopodobieństwo niewypełnienia funkcji związanej z bezpieczeństwem przez *j*-tą warstwę na przywołanie dla *i*-tego zdarzenia inicjującego.
W przypadku drugiej warstwy zachodzi $PFD_{i;PL2} = HEP_{i;PL2}$, przy czym HEP (*human error probability*) jest prawdopodobieństwem błędu człowieka, które wyznacza się na podstawie odpowiedniej metody analizy niezawodności człowieka HRA [6], [11].
Ogólnie redukcję częstości przez warstwy zabezpieczeniowe dla danego scenariusza awaryjnego należy wyznaczać uwzględniając odpowiednie prawdopobieństwa warunkowe [6]

$$F_i^Z = F_i^I \cdot P(X_{i;PL1} \mid I) \cdot P(X_{i;PL2} \mid I \cdot X_{i;PL1}) \cdot P(X_{i;PL3} \mid I \cdot X_{i;PL1} X_{i;PL2}) = F_i^I \cdot PFD_i^Z \qquad (4)$$

gdzie $X_{i;PLj}$ oznaczają zdarzenia polegające na niewypełnieniu funkcji na przywołanie przez kolejne warstwy zabezpieczeniowe (j = 1, 2, 3), uwzględniane odpowiednio przy obliczaniu prawdopodobieństw warunkowych dla *i*-tego zdarzenia inicjującego.
Analizy wykazały, że uwzględnienie zależności warstw powoduje znaczne zwiększenie, co najmniej o rząd wielkości, prawdopodobieństwa niewypełnienia funkcji przez warstwy zabezpieczeniowe, czyli zachodzi $PFD_i^Z >> PFD_i$ w wyrażeniach według wzorów (3) i (4). Istotne znaczenie w ograniczaniu zależności wspomnianych warstw ma odpowiednie zaprojektowanie systemu alarmowego [4].

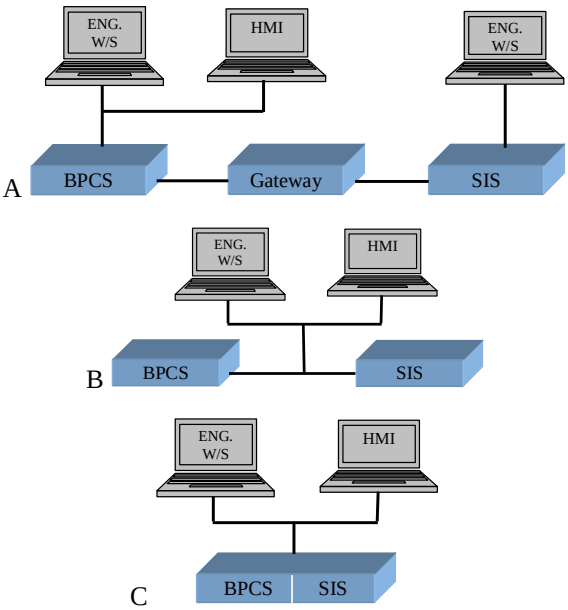
5. Proces projektowania warstw zabezpieczeń

Proces projektowania warstw zabezpieczeń przedstawiono schematycznie na *Rysunku 8*. Obejmuje on wstępną analizę ryzyka i projektowanie funkcji związanych z bezpieczeństwem oraz projektowanie systemów BPCS i SIS wraz z HMI.



Rysunek 8. Proces projektowania programowalnych systemów sterowania i zabezpieczeń

Pojawiają się nowe technologie oraz rozwiązania funkcjonalne, strukturalne i umożliwiające integrowanie systemów BPCS i SIS [1] (rysunek 9). Mają one określone wady i zalety. Należy jednak podkreślić, że rozwiązanie na poziomie integrowania C nie nadaje się do stosowania w przypadkach obiektów wysokiego ryzyka, w których mogą wystąpić poważne awarie z dużymi stratami (elektrownie jądrowe, zakłady chemiczne).



Rysunek 9. Poziomu integrowania SIS z BPCS [1]: A. Z interfejsem, B. Zintegrowany i C. Wspólny

Twierdzi się, że technologia zintegrowana jest bezpieczna i uzyskała certyfikat na poziomie nienaruszalności bezpieczeństwa SIL3 [1]. Należy jednak podkreślić, że występują różne oddziaływania funkcjonalne pomiędzy BPCS i SIS [18], co sprzyja możliwości wystąpienia uszkodzeń o wspólnej przyczynie CCF (*common cause failures*) [17], [19]. Problem ten wymaga dalszych pogłębionych badań w kontekście możliwości wystąpienia niesprawności funkcjonalnych spowodowanych błędami człowieka oraz błędami systematycznymi i uszkodzeń sprzętu o charakterze losowym w systemach zabezpieczeń i z nadmiarowością strukturalną, szczególnie jeśli występują one w warstwach zabezpieczeń.

6. Uwagi końcowe

W procesie eksploatacji obiektów przemysłowych podwyższonego ryzyka istotne dla bezpieczeństwa funkcje nadzorujące i decyzyjne pełni człowiek-operator. Dotyczy to zwłaszcza sytuacji nienormalnych i awaryjnych, kiedy to popełnione błędy mogą doprowadzić do poważnych awarii i dużych strat. Ryzyko tych strat można istotnie ograniczyć stosując odpowiednie rozwiązania techniczne w postaci warstwowego systemu zabezpieczeń, obejmującego podstawowy system sterowania, operatora i system automatyki zabezpieczeniowej.

W niniejszym artykule podkreślono znaczenie właściwego zaprojektowania systemów BPCS, SIS i systemu alarmowego, co przyczyni się do zmniejszenia prawdopobieństwa błędów człowieka-operatora. Umożliwi to odpowiednie ograniczenie ryzyka do poziomu wyznaczonego w procesie zarządzania bezpieczeństwem. Nie zaleca się integrowania systemów BPCS i SIS w przypadku obiektów/instalacji wysokiego ryzyka.

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] ARC (2005). Siemens' Process Safety Systems Deliver Modern Features on a Proven Platform. White paper. ARC Advisory Group. ARCweb.com.

[2] Berg, H.P. (2009). Human Factors in Safety and Reliability. *Proc. 3rd Summer Safety and Reliability Seminars*. Gdańsk-Sopot.
[3] Carey, M. (2001). Proposed framework for addressing human factors in IEC 61508. Amey VECTRA Limited for the Health and Safety Executive (HSE), Report 373/2001. HSE Books, Sudbury, Suffolk.
[4] EEMUA (2007). EEMUA Publication 191: Alarm Systems; A Guide to Design, Management and Procurement (Edition 2). The Engineering Equipment and Materials Users' Association.
[5] EN ISO 13407 (ISO 13407: 1999), Human-Centered Design Process for Interactive Systems.
[6] Gertman, I.D. & Blackman, H.S. (1994). *Human Reliability and Safety Analysis Data Handbook*. Wiley-Interscience Publication. New York.
[7] Hollnagel, E. (1992). The reliability of man-machine interaction. *Reliability Engineering and System Safety*, 38, 1-2, 81-89.
[8] Hollnagel, E. (1998). *Cognitive Reliability and Error Analysis Method – CREAM*. Elsevier Science Ltd., Oxford.
[9] Hollnagel, E. (2005). Human reliability assessment in context. *Nuclear Engineering and Technology*, Vol.37, 2, 159-166.
[10] IEC 61508 (2000, 2010). Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-Related Systems. Parts 1-7. International Electrotechnical Commission, Geneva.
[11] Kosmowski, K.T., Degen, G., Mertens, J. & Reer, B. (1994). *Development of Advanced Methods and Related Software for Human Reliability Evaluation within Probabilistic Safety Analyses*. Jülich: Berichte des Forschungszentrum 2928.
[12] Kosmowski, K.T. (2003). *Metodyka analizy ryzyka w zarządzaniu niezawodnością i bezpieczeństwem elektrowni jądrowych*. Wydawnictwo Politechniki Gdańskiej, Seria: Monografie 33, Gdańsk.
[13] Kosmowski, K.T., Śliwiński, M. & Piesik, J. (2004). Czynniki ludzkie w analizie bezpieczeństwa funkcjonalnego. *Materiały konferencji naukowo-technicznej Zarządzanie Bezpieczeństwem Funkcjonalnym*. Gdańsk, Jurata, 16-17 września 2004.
[14] Kosmowski, K.T. (2007) (ed.). *Functional Safety Management in Critical Systems*. Gdansk University of Technology. Wydawnictwo: Fundacja Rozwoju Uniwersytetu Gdańskiego. Gdańsk.
[15] Kosmowski, K.T. (2009). Safety management problems of a hazardous industrial plant (in Polish). In: *Diagnosis of Processes and Systems* (Ed.: Kowalczuk, Z.). PWNT Gdańsk, 181-190.
[16] Kosmowski, K.T. (2011). Functional Safety Analysis including Human Factors. *International Journal of Performability Engineering*, Vol. 7, No 1, 61-76.
[17] LOPA (2001). Layer of Protection Analysis, Simplified Process Risk Assessment. American Institute of Chemical Engineers, Center for Chemical Process Safety. New York.
[18] Marszal, E.M. & Weil, Ch.P. (2011). *Implementing Protective Functions in BPCS and Combined Systems*. Kenexis Consult. Corporation, Columbus, USA.
[19] PN-EN 61511 (2004). Bezpieczeństwo funkcjonalne. Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego. Części 1-3. Polski Komitet Normalizacyjny.
[20] Rasmussen, J. & Svedung, I. (2000): *Proactive Risk Management in a Dynamic Society*. Karlstad: Swedish Rescue Services Agency.
[21] Reason, J. (1990). *Human Error*. Cambridge University Press 1990.
[22] SPAR-H (2005). Human Reliability Analysis (HRA) Method, NUREG/CR-6883, INL/EXT-05-00509, USNRC.
[23] Swain, A.D. & Guttmann, H.E. (1983). Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application. NUREG/CR-1278.