Kosmowski Kazimierz T.
Politechnika Gdańska, Gdańsk, Polska

Risk analysis and functional safety management
Analiza ryzyka i zarządzanie bezpieczeństwem funkcjonalnym

Keywords / Słowa kluczowe

risk analysis, reliability and safety management, functional safety, cost-benefit analysis
analiza ryzyka, zarządzanie niezawodnością i bezpieczeństwem, bezpieczeństwo funkcjonalne, analiza kosztów i efektów

Abstract

This article addresses current issues concerning the risk analysis and functional safety management. Some cost-benefit analysis methods (CBA) are presented oriented on optimizing the safety-related solutions on example of functional safety technologies reducing risk based on programmable systems E/E/PE (PN-EN 61508) and SIS (PN-EN 61511). The importance of safety-related criteria, such as tolerability of risk (TOR) in the context of cost-benefit analysis (CBA), is emphasized to reach rational decisions as regards safety-related solutions to be sufficiently reliable, safe and preferably economically justified.

1. Wprowadzenie

Problematyka niezawodności i bezpieczeństwa złożonych obiektów podwyższonego ryzyka jest ostatnio w centrum uwagi nie tylko inwestorów, eksploatatorów i organów dozoru technicznego, ale również, po wystąpieniu szeregu katastrof transportowych i awarii przemysłowych oraz obiektów energetyki, również społeczeństwa i polityków. Powinna mieć ona więc istotne znaczenie przy opracowywaniu nowych technologii bezpieczeństwa, w tym w projektowaniu i wdrażaniu rozwiązań systemów sterowania i zabezpieczeń w takich obiektach. Systemy sterowania i automatyki zabezpieczeniowej postrzegane są m.in. jako środki do redukcji ryzyka związanego z potencjalnymi zdarzeniami awaryjnymi, a następnie utrzymywaniu tego ryzyka na określonym uzasadnionym ekonomicznie poziomie podczas eksploatacji [1]-[6], w nawiązaniu do określonych wymagań i kryteriów [7]-[9], [12], w tym tych zawartych w normach [10], [11].

W obiektach podwyższonego ryzyka mogą wystąpić zdarzenia nienormalne i awaryjne, a nawet stany krytyczne powodujące poważne straty ludzkie, środowiskowe i materialne. Zdarzenia takie mogą wystąpić z powodu dużych zakłóceń wewnątrz obiektu, jak i w obiektach współpracujących. Są one powodowane zawodnością wyposażenia, błędami człowieka, a więc mają związek ze stosowaną technologią i występującymi obiektywnie zagrożeniami [2].

Mówi się wówczas o bezpieczeństwie w sensie *safety* [8], w odróżnieniu od bezpieczeństwa w sensie *security*, kiedy to zagrożenia mają charakter intencyjny. Związane z tym zdarzenia zagrażające mogą powstać na przykład w wyniku sabotażu lub ataku terrorystycznego. Ocena możliwości powstania takich sytuacji 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, w postaci ataków hackerskich, dotyczą stosowanych szeroko technologii i systemów komputerowych, w tym programowanych systemów sterowania i zabezpieczeń [10], [11].

W niniejszym artykule przedstawia się wybrane zagadnienia dotyczące zarządzania bezpieczeństwem w sensie *safety* w zautomatyzowanym złożonym obiekcie podwyższonego ryzyka. Zwraca się uwagę na problem potencjalnego niekorzystnego wpływu różnych czynników, w tym czynników ludzkich, jeśli zastosowane interfejsy i procedury realizacji zadań przez człowieka-operatora zostały zaprojektowane

niewłaściwie. 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 [6], [7].

Zarządzanie bezpieczeństwem funkcjonalnym obejmuje zagadnienia sterowania ryzykiem w cyklu życia obiektu złożonego w odniesieniu do wymagań zawartych w normie o charakterze ogólnym PN-EN 61508 [10] lub w normie sektorowej PN-EN 61511 [11] (przemysł procesowy). Dotyczą one m.in. zmniejszenia ryzyka związanego z potencjalnym występowaniem zdarzeń nienormalnych lub awaryjnych, stosując programowalne systemy sterowania i zabezpieczeń: elektryczne/ elektroniczne, programowalne elektroniczne (E/E/PE) [10] lub przyrządowe systemy bezpieczeństwa SIS (*safety instrumented systems*) [11].

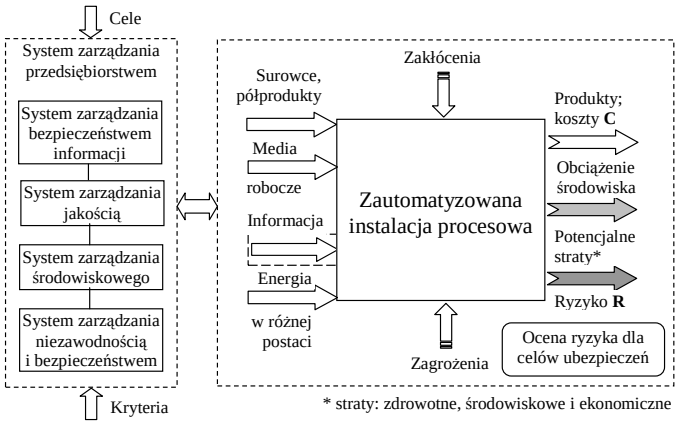
Aby osiągnąć odpowiednią redukcję ryzyka przez te systemy, muszą być one właściwie zaprojektowane i eksploatowane w cyklu życia. Należy zastosować rozwiązania sprzyjające unikaniu błędów systematycznych, szczególnie oprogramowania (*software*) oraz uszkodzeń wyposażenia technicznego (*hardware*), zwłaszcza o charakterze losowym. Normy te zawierają m.in. ilościowe kryteria probabilistyczne dotyczące wypełniania funkcji związanych z bezpieczeństwem, realizowanych za pomocą systemów (E/E/PE) lub SIS.

W artykule rozwija się również zagadnienia związane z podejmowaniem decyzji związanych z niezawodnością i bezpieczeństwem obiektów podwyższonego ryzyka w nawiązaniu do metodyki TOR (*tolerability of risk*) [4] oraz analizy kosztów i efektów CBA (*cost-benefit analysis*) [5], [6].

2. Instalacja procesowa i systemy zarządzania

Zautomatyzowaną instalację procesową złożonego obiektu przemysłowego podwyższonego ryzyka przedstawiono schematycznie na rysunku 1. Podstawowym celem jest uzyskanie w procesie technologicznym produktów o odpowiedniej jakości przetwarzając surowce i półprodukty w produkt spełniający określone wymagania.

Realizację tego procesu zapewniają: sama instalacja o określonej strukturze, media robocze (smary, chłodziwo, powietrze sprężone itd.), szeroko rozumiana informacja w postaci procedur i algorytmów w systemach starowania i zabezpieczeń oraz energia w różnej postaci (elektryczna, cieplna itd.). Niestety każdy proces technologiczny powoduje większe lub mniejsze obciążenia środowiska (uwolnione zanieczyszczenia, gazy, ciepło i odpady itd.), co wymaga odpowiedniej kontroli, aby unikać lub zmniejszać kary nakładane za szkodliwe emisje do środowiska.



Rysunek 1. Obiekt przemysłowy podwyższonego ryzyka i systemy zarządzania

Istotnym problemem w przemyśle są potencjalne straty o charakterze losowym powodowane zawodnością wyposażenia (przestoje lub zmniejszenie wydajności) oraz zakłóceniami wewnętrznymi i zewnętrznymi (np. niepotrzebne zadziałanie automatyki zabezpieczeniowej lub zanik zasilania elektrycznego). Mogą one doprowadzić do stanów awaryjnych instalacji procesowej i znacznych strat produkcyjnych.

Z badań firm ubezpieczeniowych wynika, że istotnymi przyczynami strat w przemyśle są pożary, zawodność wyposażenia, w tym automatyki zabezpieczeniowej oraz szeroko rozumiane błędy człowieka, spowodowane m.in. uchybieniami organizacyjnymi [8].

Zależnie od instalacji i realizowanego procesu technologicznego oraz jej powiązania z innymi instalacjami występują różnego rodzaju zagrożenia, które jeśli są nieodpowiednio kontrolowane, mogą doprowadzić do powstania strat, niekiedy poważnych, a nawet całkowitego zniszczenia instalacji (eksplozja uwolnionego gazu, pożar itd.). Zdarzenia zagrażające mogą spowodować również obrażenia u ludzi (pracownicy, ludzie przebywający w otoczeniu obiektu), a nawet zejścia śmiertelne. Przy emisjach substancji szkodliwych do otoczenia powstają straty zewnętrzne w otoczeniu obiektu.

Wyróżnia się trzy rodzaje strat do uwzględnienia w analizach ryzyka:

- straty zdrowotne (obrażenia i potencjalne zejścia śmiertelne),
- szkody środowiskowe (zanieczyszczenie powietrza, gleby i/lub wody),

- straty ekonomiczne (spowodowane zmniejszeniem lub zaprzestaniem produkcji, odszkodowaniami, remontami poawaryjnymi lub odbudową obiektu, utratą reputacji itd.) [8].

Jak wspomniano, zdarzenia powodujące straty mają charakter losowy. Nie można ich w pełni wyeliminować, natomiast możliwa jest analiza i ocena ryzyka występowania potencjalnych strat dla zidentyfikowanych w danym obiekcie zagrożeń. Odpowiednio przeprowadzone oceny zagrożeń i ryzyka pozwalają na ich racjonalne zmniejszenie lub utrzymywanie na odpowiednim poziomie stosując odpowiednie rozwiązania techniczne (technologie produkcji, systemy zabezpieczeń) i organizacyjne (nadzór, systematyczne szkolenie pracowników).

Utrzymywanie wysokiej niezawodności operacyjnej instalacji i jej wyposażenia wpływa korzystnie na poziom bezpieczeństwa całego obiektu złożonego. Osiąga się to m.in. poprzez odpowiednią eksploatację obiektu z zaplanowaniem i realizacją odpowiedniej strategii kontroli, przeglądów profilaktycznych i remontów wyposażenia technicznego, racjonalizowanych w cyklu życia.

Utrzymywanie wysokiej jakości produkcji, niezawodności i szeroko rozumianego bezpieczeństwa w zakładach przemysłowych podwyższonego ryzyka powinien zapewnić system zarządzania przedsiębiorstwem (SZP), który coraz częściej obejmuje (rysunek 1):

- system zarządzania bezpieczeństwem informacji (SZBI), projektowany np. w oparciu o normy: PN-ISO/IEC 27001:2007, ISO/IEC 17799:2005, ISO/IEC 15408:2005, ISO/IEC 13335:2004;
- system zarządzania jakością (SZJ), projektowany np. w oparciu o normy PN-EN ISO 9001:2001(2008);
- system zarządzania środowiskowego (SZŚ), projektowany np. w oparciu o normy PN-EN ISO 14001: 2005;
- system zarządzania niezawodnością i bezpieczeństwem, w tym bezpieczeństwem funkcjonalnym i bezpieczeństwem na stanowiskach pracy (SZNB), projektowany np. w oparciu o normy serii: PN-EN 61508:2002, PN-EN 62061:2005, PN-EN 61511:2005, PN-EN 60300-3-3:2005, PN-N 18001:2004 i inne.

Dąży się ostatnio do integrowania tych systemów zarządzania w jeden zintegrowany system zarządzania jakością, środowiskiem, niezawodnością i bezpieczeństwem w ramach systemu zarządzania przedsiębiorstwem i produkcją. Jest to szczególnym wyzwaniem w obiektach podwyższonego ryzyka, w których mogą wystąpić poważne awarie [6], [8].

3. Problem optymalizowania kosztów w obiektach podwyższonego ryzyka

Problem optymalizowania zadań produkcyjnych w obiektach i instalacjach podwyższonego ryzyka można przedstawić ogólnie następująco:

- *minimalizowanie wektora składowych kosztów produkcji* $\mathbf{C}_p$ (skumulowanych w ciągu roku lub jednostkowych) przy zachowaniu wektora wymagań jakościowych $\mathbf{Q}_p$ oraz spełnieniu wymagań / kryteriów (r) dotyczących:
- wektora obciążenia środowiskowego $\mathbf{E}_e$ z uwzględnieniem kar za emisję lub wydalanie substancji szkodliwych do otoczenia (np. dwutlenku węgla lub zanieczyszczonych ścieków),
- wektora miar związanych z niezawodnością $\mathbf{D}_i$ (*dependability*) instalacji w odpowiednich horyzontach czasowych (na przykład 1 roku), zależnego od realizacji przyjętej strategii obsługi profilaktycznej i planowanych remontów, oraz
- wektora ryzyka różnego rodzaju potencjalnych strat $\mathbf{R}_l$ o charakterze systematycznym, losowym i spowodowanych działaniami intencyjnymi; przy czym odpowiednio zdefiniowane miary ryzyka można redukować lub utrzymywać na określonym poziomie stosując odpowiednie środki zabezpieczające oraz strategię ich okresowej kontroli, testowania i obsługi profilaktycznej,

a więc

$$\min \mathbf{C}_p \; dla \; \mathbf{Q}_p \supseteq \mathbf{Q}_p^r, \mathbf{E}_e \subseteq \mathbf{E}_e^r, \quad \mathbf{D}_i \supseteq \mathbf{D}_i^r, \; \mathbf{R}_l \subseteq \mathbf{R}_l^r \tag{1}$$

Problem określony ogólnie kryterium i relacjami (1) jest przydatny w formułowaniu zagadnienia optymalizowania kosztów w cyklu życia LCC (*life cycle cost*), których wyznaczanie opisuje norma PN-EN 60300-3-3:2005. Przydatną metodą do rozwiązywania częściowych problemów optymalizacyjnych jest metoda CBA (*cost-benefit analysis*) [5]. Metody przydatne w tym celu na przykładzie bezpieczeństwa funkcjonalnego projektowanych systemów zabezpieczeń opisano w monografii [6] i pracach [9], [12].

Warto podkreślić, że zarządzanie niezawodnością i bezpieczeństwem złożonego obiektu, wpływające w oczywisty sposób na produktywność, a zatem efektywność ekonomiczną, przeprowadza się w całym cyklu życia, natomiast odpowiednie miary ryzyka dotyczące pojedynczych zdarzeń zagrażających lub zbioru zdarzeń zagrażających wyznacza się zwykle dla określonej misji lub rocznego okresu eksploatacji obiektu.

Ryzyko **R** związane z eksploatacją obiektu wymaga oceny w celu podjęcia decyzji i ewentualnej modyfikacji rozwiązań technicznych i/lub organizacyjnych sprzyjających jego redukcji lub utrzymywaniu podczas eksploatacji na określonym poziomie. W praktyce przemysłowej dokonuje się transferu części ryzyka do firmy ubezpieczeniowej wykupując odpowiednią polisę, której cena zależy od wyników oceny ryzyka.

Poniżej rozważane będą niektóre aspekty związane z zarządzaniem ryzykiem wystąpienia awarii przemysłowych, co ma szczególne znaczenie w obiektach podwyższonego ryzyka. Ze względu na zakres artykułu analiza ryzyka nie będzie się uwzględniać zagrożeń o charakterze intencyjnym i związanego z tym zarządzania bezpieczeństwem (w sensie *security*), a głównie zagrożeń rozumianych tradycyjnie i zarządzania bezpieczeństwem (w sensie *safety*).

4. Ryzyko związane z eksploatacją instalacji przemysłowej

Ryzyko (techniczne) definiuje się jako kombinację częstości lub prawdopodobieństwa wystąpienia niebezpiecznych zdarzeń awaryjnych i ich konsekwencji prowadzących do określonych szkód, w tym strat zdrowotnych, środowiskowych i/lub ekonomicznych [10]. W złożonym obiekcie może występować wiele takich zdarzeń, które grupuje się w kategorie i nazywa scenariuszami awaryjnymi [6].

Wyróżnia się *ryzyko indywidualne*, dotyczące jednostki ludzkiej znajdującej się w danym miejscu i czasie oraz *ryzyko grupowe* lub *ryzyko społeczne*, dotyczące określonej populacji przebywającej na danym terytorium w pobliżu instalacji niebezpiecznej [4].

Bezpieczeństwo ma natomiast związek z warunkami lub sytuacją niewystępowania ryzyka nieakceptowanego [10]. Żeby stwierdzić, czy ryzyko jest akceptowane, czy też nie, należy je oszacować i ocenić względem kryteriów, które wyznacza organ dozoru technicznego lub kierownictwo korporacji na podstawie badań porównawczych różnych ryzyk w odniesieniu do wartości akceptowanych przez daną społeczność. Uwzględnia się przy tym dostępne statystyki wypadków i miary ryzyka, np. FAR (*fatal accident rate*) [4], [8], wyznaczane w niektórych sektorach gospodarki, głównie w transporcie.

Zarządzanie ryzykiem polega na systematycznej realizacji polityki bezpieczeństwa w praktyce z realizacją procedur i działań mających na celu analizowanie, ocenę i sterowanie ryzykiem. *Sterowanie ryzykiem* jest natomiast procesem podejmowania decyzji mających na celu zarządzanie ryzykiem, w szczególności racjonalne zmniejszenie lub utrzymywanie ryzyka na określonym poziomie, korzystając z wyników oszacowania i oceny ryzyka. W sterowaniu ryzykiem wyróżnia się dwa zasadnicze podejścia: (a) aktywne polegające na oddziaływaniu na przyczyny i czynniki ryzyka oraz (b) pasywne, koncentrujące się na zabezpieczaniu przed ewentualnymi stratami. Najefektywniejsze są podejścia zintegrowane [4].

Miarę ryzyka długoterminowego dla danego systemu technicznego wyznacza się na podstawie zbioru trójek, które zawierają [6]: scenariusz zdarzenia awaryjnego, jego częstość lub prawdopodobieństwo występowania oraz niekorzystny skutek (szkodę) po jego wystąpieniu, a mianowicie

$$\Re = \{< S_k, F_k, N_k >\} \qquad (2)$$

gdzie S_k oznacza potencjalne zdarzenie awaryjne związane z *k*-tym scenariuszem, F_k jest częstością tego scenariusza (prawdopodobieństwo na jednostkę czasu, np. rok), a N_k oznacza niekorzystny skutek w wyniku wystąpienia *k*-tego scenariusza, czyli szkodę (stratę) w określonym zakresie, np. skutków zdrowotnych, szkód w środowisku i/lub strat majątkowych (ekonomicznych).

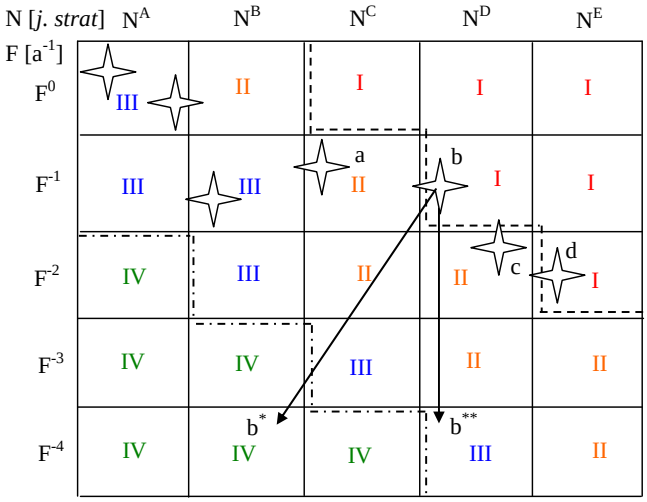
W ocenach ryzyka dla celów ubezpieczeniowych podstawowe znaczenie ma określenie start zagregowanych, wyrażonych w jednostkach pieniężnych.

Wyniki przykładowego ilościowego oszacowania ryzyka grupowego za pomocą *matrycy ryzyka* przedstawiono na *Rysunku 2*. Wyróżniono pięć kategorii strat od N^A do N^E (np. zdrowotnych lub środowiskowych) i pięć kategorii częstości F^{-4} do F^0, którym przyporządkowano odpowiednie przedziały liczbowe [8]. Wyniki oszacowania ryzyka w postaci zbioru par $\{(F_k, N_k)\}$ dla kolejnych scenariuszy awaryjnych reprezentują na tym rysunku gwiazdki.

Kategorie częstości i strat definiuje się niekiedy korzystając z informacji o charakterze jakościowym, stosując określenia słowne (np. *straty małe*, *umiarkowane*, *duże*, *wielkie*), co wymaga jednak kalibracji takiej jakościowej matrycy ryzyka, aby podejmować właściwe decyzje w zarządzaniu ryzykiem.

Na *Rysunku 2* wyróżniono również cztery klasy ryzyka związanego z potencjalnymi zdarzeniami awaryjnymi: I - ryzyko nieakceptowane, którego nie można tolerować ze względu na stosunkowo dużą częstość zdarzeń awaryjnych i ich poważne straty, II – ryzyko duże, które należy redukować zgodnie z zasadą ALARP [3], [10], III – ryzyko tolerowane

tylko wówczas, jeśli koszt jego redukcji jest nieproporcjonalne duży w stosunku do spodziewanych efektów (stosunkowo nieznaczne zmniejszenie ryzyka wymaga dużych nakładów finansowych) – w przeciwnym razie ryzyko należy zmniejszyć, oraz IV – ryzyko akceptowane, określone przez organy dozoru w nawiązaniu do ryzyka tolerowanego uwzględniającego oczekiwania społeczne [3].



Rysunek 2. Ilustracja wyników analizy ryzyka przykładowego obiektu złożonego na tle obszarów wyróżnionych klas ryzyka

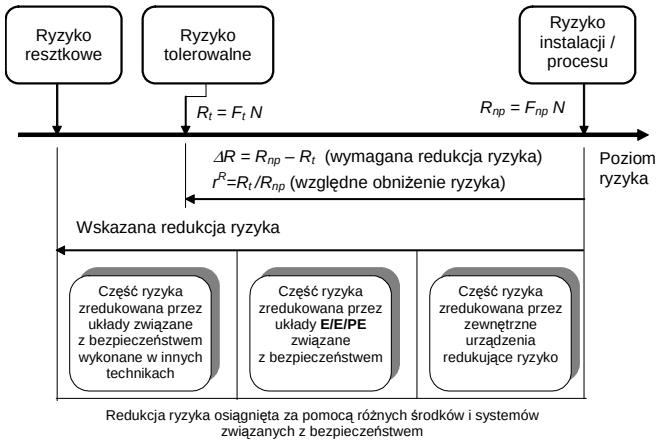
Jak widać na rysunku 2 w obszarach ryzyka niedozwolonego (klasa I) i niepożądanego (klasa II) znajdują się cztery punkty, oznaczone kolejnymi literami a, b, c, d - rosnąco według skutków. Zmniejszenie ryzyka rozpatrzone będzie na przykładzie punktu b. Zastosowanie środków zabezpieczeniowych, na przykład warstwowego systemu zabezpieczeń, spowoduje przesunięcie współrzędnej ryzyka w kierunku strzałki do punktu b^*, co dopowiada odpowiedniemu zmniejszeniu skutków i częstości rozważanego zdarzenia awaryjnego.
Jeśli założyć pesymistycznie, że wprowadzenie dodatkowych zabezpieczeń nie powoduje zmniejszenia strat, a jedynie częstości danego scenariusza awaryjnego, to redukcja ryzyka nastąpi do punktu b^{**}. Jak widać, przede wszystkim należy przeanalizować dogłębniej scenariusze b oraz d, ponieważ znajdują się one w obszarze ryzyka niedozwolonego. Celowa jest redukcja częstości tych zdarzeń, co najmniej o trzy dekady (zmniejszenie 1000 razy), wprowadzając na przykład dodatkową funkcję bezpieczeństwa realizowaną przez warstwowy system zabezpieczeniowo-ochronny, zawierający BPCS (Basic Proces Control System) i SIS [11].

5. Redukcja ryzyka za pomocą rozwiązań bezpieczeństwa funkcjonalnego

W instalacji podwyższonego ryzyka poziom ryzyka zmniejsza się stosując system E/E/PE, a w przemyśle procesowym za pomocą warstw zabezpieczeń, które obejmują podstawowy system sterowania BPCS (*basic process control system*), system alarmowy AS (*alarm system*) z odpowiednim interfejsem i działaniami operatorów, system automatyki zabezpieczeniowej SIS (*safety instrumented system*), który może pełnić funkcję wyłączania (odstawienia) awaryjnego instalacji ESD (*emergency shutdown system*), a także systemy zabezpieczeń inżynieryjnych i lokalizacji skutków awarii (zawory bezpieczeństwa, kurtyny, bariery, obudowy i inne urządzenia).
W nawiązaniu definicji ryzyka grupowego rozważa się poniżej ocenę zmniejszenia ryzyka po wprowadzeniu zidentyfikowanej opcji sterowania ryzykiem (OSR), względem opcji bazowej (B). Jedną z takich opcji może być zastosowanie systemu E/E/PE [10] lub SIS [11], pełniącego funkcje bezpieczeństwa. Miarę zmniejszenia ryzyka po wprowadzeniu danej OSR wyznacza się na podstawie wzoru [6]

$$\Delta R^{OSR} = \sum_k F_k^B N_k^B (1 - r_k^{F;OSR} r_k^{N;OSR}) \qquad (3)$$

gdzie F_k^B, N_k^B oznaczają częstość zdarzenia na rok [a^{-1}] i stratę [*jedn. straty*] w wyniku *k*-tego scenariusza awaryjnego według modelu ryzyka dla opcji B; $r_k^{F;OSR}$ jest względnym zmniejszeniem częstości tego scenariusza awaryjnego po wprowadzeniu OSR ($r_k^{F;OSR} = F_k^{OSR} / F_k^B$); $r_k^{N;OSR}$ oznacza względne zmniejszenia straty związanej z *k*-tym scenariuszem awaryjnym po wprowadzeniu OSR ($r_k^{N;OSR} = N_k^{OSR} / N_k^B$); ΔR^{OSR} ma wymiar [*jedn. straty/a*].
Sposoby zmniejszania ryzyka od poziomu ryzyka R_{np} (*no protection – np*), to jest bez zastosowania zabezpieczeń w obiekcie podwyższonego ryzyka, do poziomu tolerowanego R_t, np. po zastosowaniu systemu E/E/PE, przedstawiono na rysunku 3. Wyróżniono miary redukcji ryzyka: bezwzględnej ΔR i względnej r^R. Wyróżniono również na tym rysunku ryzyko resztkowe, jakie jeszcze istnieje mimo zastosowania środków zabezpieczeniowych. Ryzyka nie można w pełni wyeliminować.



Rysunek 3. Sposoby zmniejszania ryzyka w obiekcie 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 na podstawie (3) wzór na względne obniżenie poziomu ryzyka w postaci

$$r^R = R_t / R_{np} = F_t / F_{np} = r^F \tag{4}$$

gdzie R_{np} oznacza ryzyko bez zastosowania systemów zabezpieczeń (np. E/E/PE lub SIS); F_{np} jest częstością zdarzenia bez uwzględnienia systemu zabezpieczeniowego; R_t oznacza ryzyko tolerowane; F_t jest zredukowaną częstością zdarzenia awaryjnego (wynikającą z poziomu ryzyka tolerowanego R_t) do osiągnięcia po wprowadzeniu środka zabezpieczeniowego, r^F oznacza względną redukcję częstości rozważanego scenariusza awaryjnego.

Jak wspomniano, rozważana funkcja bezpieczeństwa może być realizowana przez system E/E/PE lub SIS i wówczas przeciętne prawdopodobieństwo niewypełnienia funkcji dla rodzaju rzadkiego przywołania do działania PFD_{avg} (*average probability of failure on demand*) [10] można wyznaczyć ze wzoru

$$PFD_{avg} = r^F = F_t / F_{np} \tag{5}$$

6. Analiza efektywności nakładów na poprawę bezpieczeństwa

Należy dążyć do zrównoważonej i uzasadnionej finansowo redukcji ryzyka związanego z potencjalnymi zdarzeniami awaryjnymi. Rozważane są opcje sterowania ryzykiem (OSR) w nawiązaniu do przyjętej strategii sterowania ryzykiem. Powinny one uwzględniać ważniejsze czynniki wpływające na poziom ryzyka [6]. OSR mogą mieć charakter:

- techniczny (funkcje i struktury wyposażenia, programowalne systemy monitorowania, sterowania i zabezpieczeń technologicznych, nowoczesne systemy wspomagania diagnostyki i systemy doradcze itp.);
- organizacyjny (programy cyklicznego szkolenia; procedury postępowania w sytuacjach: nienormalnych, awaryjnych i restytucyjnych; planowanie i nadzór administracyjny kontroli, przeglądów profilaktycznych i remontów wyposażenia; projekt i wdrożenie zintegrowanego systemu zarządzania niezawodnością i bezpieczeństwem);
- mieszany (systemy diagnostyczne i wspomagania decyzji, komputerowe systemy doradcze, systemy poprawiające bezpieczeństwo na stanowiskach pracy, zastosowanie nowych rozwiązań bezpieczeństwa funkcjonalnego systemów monitorowania, sterowania i zabezpieczeń itp.).

Przyrost kosztów rocznych ΔK^{OSR} związanych z zaimplementowaniem danej OSR wyznacza się ze wzoru [6]

$$\Delta K^{OSR} = r_d^L \Delta K_{In}^{OSR} + \Delta K_{Ek}^{OSR} - \Delta K_{Ko}^{OSR} \tag{6}$$

gdzie ΔK_{In}^{OSR} oznacza dodatkowe nakłady inwestycyjne na daną OSR [PLN]; ΔK_{Ek}^{OSR} jest przyrostem kosztów eksploatacyjnych, przyjmującym zwykle wartość dodatnią [PLN/a]; ΔK_{Ko}^{OSR} jest przyrostem korzyści eksploatacyjnych po zastosowaniu danej OSR, jeśli występują [PLN/a]; r_L^d oznacza współczynnik rocznych kosztów kapitałowych [1/a], wyznaczany dla czasu życia obiektu L [a] i stopy dyskonta d ; współczynnik ten wyznacza się z następującego wzoru [6]

$$r_d^L = \frac{d(1+d)^L}{(1+d)^L - 1} \tag{7}$$

Następnie wyznacza się wskaźnik efektywności rozumiany jako koszt na jednostkę zmniejszonego ryzyka (CURR: *cost per unit risk reduction*) zgodnie z wzorem

$$k^{OSR} = \frac{\Delta K^{OSR}}{\Delta R^{OSR}} \tag{8}$$

gdzie ΔK^{OSR} jest przyrostem rocznych kosztów po zastosowania OSR, wyznaczany według (6), *PLN/a*; ΔR^{OSR} oznacza redukcję ryzyka po wprowadzeniu OSR wyznaczona na podstawie modelu ryzyka według (3). Tak więc k^{OSR} ma wymiar [*PLN/j. straty*].
W procesie zarządzania ryzykiem identyfikuje się możliwe OSR (uzasadnione technicznie i organizacyjnie) i wyznacza się dla każdej z nich k^{OSR}. Najbardziej efektywna w sensie redukcji ryzyka jest OSR o najmniejszym wskaźniku k^{OSR}. Jak wspomniano, szkody można wyrażać jako straty ludzkie, środowiskowe lub materialne (ekonomiczne).

7. Metoda oceny uzasadnionych nakładów na rozwiązania bezpieczeństwa funkcjonalnego

Rozważania dotyczące uzasadnionego poziomu inwestowania w środki bezpieczeństwa można przeprowadzić również w nieco odmienny sposób. W pracy [9] wyprowadzono następujące wzory na uzasadniony poziom dodatkowych kosztów na poprawę bezpieczeństwa systemu E/E/PE lub SIS. W przypadku kryterium opartym na ryzyku indywidualnym ma on postać

$$\Delta K^{I}_{jus} = k_f \cdot VPF \cdot [F \cdot (PFD^{1}_{avg} - PFD^{2}_{avg})] \qquad (9)$$

a w przypadku kryterium opartym na ryzyku grupowym

$$\Delta K_{jus} = k_f \cdot VPF \cdot [F \cdot (PFD^{1}_{avg} - PFD^{2}_{avg})] \cdot N \cdot L^{ef} \qquad (10)$$

przy czym zachodzi relacja [3], [12]

$$CPF = k_f \cdot VPF \qquad (11)$$

gdzie we wzorach (9)-(11) *CPF* (*cost of preventing fatality*) jest kosztem zapobiegania zejścia śmiertelnego; *VPF* (*value of preventing fatality*) jest wartością zapobieżenia zejścia śmiertelnego; k_f jest współczynnikiem o wartościach, zależnie od rozważanego przypadku, z przedziału $k_f \in [1, 2)$; *F* jest częstością scenariusza bez środków zabezpieczeń; *N* jest liczbą zejść śmiertelnych po zaistnieniu rozważanego scenariusza awaryjnego, L^{ef} oznacza efektywny czas życia (eksploatacji) obiektu, który jest odwrotnością współczynnika r^{d}_{L} określonego wzorem (7), natomiast PFD^{1}_{avg} i PFD^{2}_{avg} są przeciętnymi prawdopodobieństwami niezadziałania na przywołanie systemu E/E/E lub SIS dla rozważanych rozwiązań: 1 (spełniającego podstawowe wymagania o niższym poziomie SIL) i 2 (o wyższym poziomie SIL, czyli mniejszym PFD).

8. Przykłady ilustrujące metody analizy kosztów i efektów stosowania systemów zabezpieczeń

Metod zostanie zilustrowana poniżej na trzech przykładach:

Przykład 1
Analizuje się ryzyko indywidualne w przypadku dominującego scenariusza awaryjnego o częstości $F = 10^{-2}$ [a^{-1}] (bez uwzględnienia środków zabezpieczeniowych) i bazowym rozwiązaniu systemu E/E/PE na poziomie SIL2 ($PFD_{avg} = 10^{-2}$); ocenia się, czy uzasadnione jest zwiększenie poziomu SIL tego systemu do SIL3 ($PFD_{avg} = 10^{-3}$); na podstawie [3] przyjęto wartość $VPF = 10^6$ EUR oraz $k_f = 1{,}5$. Po podstawieniu tych do wzoru (9) uzyskuje się

$$\Delta K^{I}_{jus} = 1{,}5 \text{ x } 2\ 10^6\ [10^{-2} - 10^{-3}] \cong 270 \text{ EUR/a}$$

Wartość ta wskazuje, że jest ograniczone uzasadnienie, aby podnieść poziom SIL, ponieważ uzasadnione koszty roczne o tej wartości są niższe niż dodatkowy koszt rozwiązania związany z zastosowaniem SLI3.

Przykład 2
Analizuje się ryzyko społeczne w przypadku dominującego scenariusza awaryjnego o częstości $F = 10^{-2}$ [a^{-1}]. Korzysta się w tym przypadku ze wzoru (10) przyjmując część danych jak poprzednio oraz $N = 10$ i $L^{ef} = 15$ – wartość tę uzyskano przy L = 30 [a] na podstawie odwrotności (7) dla d = 5%. Podstawiając te dane do (10) otrzymujemy

$$\Delta K^{I}_{jus} = 1{,}5 \text{ x } 2\ 10^6\ [10^{-2}\ (10^{-2}–10^{-3})]\ 10 \text{ x } 15 \cong 45000 \text{ EUR/a}$$

Uzyskana wartość wskazuje, że jest uzasadnione rozważenie zastosowania lepszego rozwiązania (o wyższym SIL), bo tyle w przybliżeniu wyniosą dodatkowe koszty lepszego rozwiązania. Należy przeprowadzić dodatkowe pogłębione analizy z oszacowaniem kosztów implementacji systemu zabezpieczeń na poziomie SIL3.

Przykład 3
Analizuje się sytuację, aby nie zwiększając ryzyka wydłużyć czas eksploatacji instalacji z 1 roku do 2 lat w celu przeprowadzania testowania wyposażenia, mającego na celu wykrycie uszkodzeń niebezpiecznych niewykrywalnych, co wymaga zwiększenia poziomu SIL systemu zabezpieczeniowego, na przykład z SIL2 na SIL3. Odstawienie instalacji na przeprowadzenie testów wynosi 24 godz., a powstałe z tego powodu straty ekonomiczne oszacowano na poziomie 50000 EUR. Przyjęto, że dzięki wydłużeniu czasu eksploatacji do testowania osiąga się korzyści ekonomiczne. Przyjęto połowę tej wartości do obliczeń z wykorzystaniem równania (6), to jest $\Delta K_{Ko}^{OSR} = 25000$ EUR. Przy założeniu, że ΔK^{OSR} i ΔK_{Ek}^{OSR} można przyrównać do zera uzyskamy na podstawie (6)

$$\Delta K_{In}^{OSR} = \Delta K_{Ko}^{OSR} / r_d^L = 25000/0{,}065 = 385\,000 \text{ EUR}$$

gdzie $r_L^d = 0{,}065$ uzyskano na podstawie (7) dla d = 5 % i L = 30 lat. Przy mniejszej wartości L uzyska się oczywiście mniej korzystny wynik.

8. Uwagi końcowe

Uzyskane wyniki świadczą o tym, że uzasadnione są niekiedy nawet dość wysokie dodatkowe nakłady inwestycyjne na systemy zabezpieczeń, co spowoduje, że bez niedozwolonego wzrostu ryzyka potencjalnych zdarzeń awaryjnych, możliwe będzie rzadsze odstawianie instalacji w celu przeprowadzenia testów systemów zabezpieczeń, co przyczyni się do wzrostu miary dyspozycyjności obiektu, a zatem efektywności jego eksploatacji.
Warto więc rozwijać i stosować w praktyce metody analizy kosztów i efektów w ocenie rozwiązań bezpieczeństwa funkcjonalnego w nawiązaniu do proponowanych kryteriów ryzyka indywidualnego i ryzyka grupowego.

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] Aven, T. (2008). *Risk Analysis, Assessing Uncertainties beyond Expected Values and Probabilities*. John Wiley & Sons, Ltd., Chichester.
[2] Cholewa, W., Kosmowski, K.T. & Radkowski, S. (2008). *Modele systemów oceny ryzyka i diagnostyki technicznej*. Praca zbiorowa, Politechnika Śląska, Zeszyt 138, Gliwice.
[3] Evans, A.W. (2005). *Safety Appraisal Criteria, The 2005 Lloyd's Register Lecture on Risk Management*, The Royal Academy of Engineering, Imperial College, London.
[4] HSE (2001). HSE's Decision Making Process Reducing Risk, Protecting People. Norwich.
[5] HSE (2006). HSE principles for Cost Benefit Analysis (CBA) in support of ALARP decisions. Health and Safety Executive, U.K.
[6] Kosmowski, K.T. (2003). *Metodyka analizy ryzyka w zarządzaniu niezawodnością i bezpieczeństwem elektrowni jądrowych*. Wydawnictwo Politechniki Gdańskiej, Seria: Monografie 33, Gdańsk.
[7] Kosmowski, K.T. (2006). Functional Safety Concept for Hazardous System and New Challenges. *Journal of Loss Prevention in the Process Industries* Vol. 19, ss. 298-305.
[8] Kosmowski, K.T. (2007) (red.). *Functional Safety Management in Critical Systems*. Gdansk University of Technology. Wydawnictwo: Fundacja Rozwoju Uniwersytetu Gdańskiego. Gdańsk.
[9] Kosmowski, K.T. (2007). Functional safety in the context of risk appraisal criteria and cost-benefit analysis. W monografii: *Functional Safety Management in Critical Systems*. Wydawnictwo: Fundacja Rozwoju Uniwersytetu Gdańskiego. Gdańsk.
[10] PN-EN 61508 (2004). Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem. Części 1-7. Polski Komitet Normalizacyjny.
[11] PN-EN 61511 (2004). Bezpieczeństwo funkcjonalne. Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego. Części 1-3. Polski Komitet Normalizacyjny.
[12] Timms, C.R. (2007). *Achieving ALARP with Safety Instrumented Systems*. Asset Integrity Management Limited, Riverview Business Centre, Aberdeen.