prof. dr inż. Tadeusz Missala
Przemysłowy Instytut Automatyki
i Pomiarów, Warszawa
e-mail: tmissala@sg.piap.waw.pl

OCENA RYZYKA W SYSTEMIE ZAUTOMATYZOWANYM – PROPOZYCJA POSTĘPOWANIA

Przedstawiono w skrócie postępowanie proponowane przy ocenie ryzyka w układzie zautomatyzowanym, w którym układ sterowania ma do spełnienia istotną rolę w ograniczeniu powstania wypadku. W postępowaniu tym położono nacisk na identyfikację potencjalnych zdarzeń zagrażających i określenie prawdopodobieństwa zaistnienia scenariuszy rozwoju zagrożeń oraz na zastosowanie przyrządowych systemów bezpieczeństwa o dostatecznie wysokim poziomie nienaruszalności bezpieczeństwa (SIL), zmniejszających to prawdopodobieństwo, jako najlepszej drogi do unikania wypadków.

RISK ASSESSMENT IN AUTOMATED SYSTEMS - PROPOSAL OF THE PROCEEDING

The proceeding proposed for the risk assessment in the automated systems, in which the control system has the important meaning in the accident prevention, is presented in a short way. The attention is turned on the problems of the identification of the potential hazardous events and the elaboration of the probability of the possible accident growing up scenarios, as well as on the application of the safety instrumented systems with the sufficient high Safety Integrity Level (SIS) to limit this probability, as the best way to avoid the accidents.

1. WSTĘP

Współczesne systemy automatyki sterują rozmaitymi instalacjami technologicznymi stwarzającymi niejednokrotnie, w przypadku powstania awarii, poważne zagrożenia dla personelu, jak też narażające środowisko naturalne i sam proces sterowany oraz finanse firmy. Skutkami awarii w instalacjach technologicznych, maszynach, gniazdach wytwórczych mogą być mniej lub bardziej rozległe obrażenia personelu, aż do utraty życia włącznie, zanieczyszczenie lub wręcz zdegradowanie środowiska naturalnego na terenie obiektu lub poza nim, a nawet katastrofa ekologiczna na dużym obszarze i co z tym jest związane, mniejsze lub nawet ogromne nakłady finansowe. Te względy powodują, że ocena ryzyka związanego z eksploatacją obiektu jest co raz częściej rozpatrywana. Między innymi metodyka projektowania oparta o pojęcie bezpieczeństwa funkcjonalnego [1] przewiduje badanie zagrożeń i ryzyka w fazie projektu systemu. Aby uściślić rozumowanie zostaną przytoczone podstawowe definicje [2,5]:

- **uszkodzenie** - utrata zdolności jednostki funkcjonalnej do wypełniania wymaganych funkcji;

- **defekt** - stan nienormalny jednostki funkcjonalnej, charakteryzujący się niezdolnością do wykonania wymaganej funkcji, z wyjątkiem niezdolności podczas przeglądów i konserwacji i innych zaplanowanych działań lub spowodowanej brakiem zewnętrznego zasilania;
- **błąd człowieka** - działanie lub zaniechanie przez człowieka, które wywołuje niezamierzone wyniki;
- **ograniczenie skutków** - działanie, które zmniejsza konsekwencje zdarzenia zagrażającego;
- **uraz** - fizyczna szkoda lub pogorszenie stanu zdrowia, majątku lub środowiska;
- **zagrożenie** - źródło możliwego doznania urazu lub sytuacji stwarzającej możliwość urazu;
- **ryzyko** - kombinacja prawdopodobieństwa wystąpienia lub pogorszenia stanu zdrowia i stopnia ich ciężkości w sytuacji zagrożenia (EN 292-1: 1991; EN 61204-1: 1997);
- **ryzyko** – kombinacja częstości lub prawdopodobieństwa wystąpienia i konsekwencji określonej sytuacji zagrażającej (IEC 61508-4: 1998, draft IEC 61882; 2000);
- **ryzyko urządzenia/procesu** - ryzyko wynikające z właściwości urządzenia/procesu lub jego interakcji z układem sterowania;
- **ryzyko tolerowalne** - ryzyko, które jest akceptowane w danym kontekście bazującym na bieżących danych społecznych;
- **ryzyko szczątkowe** - w rozumieniu IEC 61508-5 jest to ryzyko, w odniesieniu do określonego zdarzenia zagrażającego, pozostające w urządzeniu/procesie, systemie sterowania urządzeniem/ procesem i powiązanymi z nim czynnikami ludzkimi, lecz po wprowadzeniu zewnętrznych urządzeń do redukcji ryzyka, systemów E/E/PE wiążących się z bezpieczeństwem oraz systemów wiążących się z bezpieczeństwem, wykonanych w innych technikach.

- **warstwa ochrony** - dowolny mechanizm, który zmniejsza ryzyko przez sterowanie, zapobieganie lub ograniczanie skutków;

- **funkcja bezpieczeństwa** - funkcja zaimplementowana za pomocą SIS, systemu wiążącego się z bezpieczeństwem wykonanego w innej technologii lub zewnętrznych urządzeń przeznaczonych do zmniejszania ryzyka, który jest przewidziany do uzyskania lub utrzymania stanu bezpiecznego obiektu;

- **przyrządowa funkcja bezpieczeństwa** - funkcja E/E/PE o podanym takim poziomie nienaruszalności, jako jest konieczny do osiągnięcia bezpieczeństwa funkcjonalnego. Przyrządowa funkcja bezpieczeństwa może być albo przyrządową ochronną funkcją bezpieczeństwa, albo przyrządową sterowniczą funkcją bezpieczeństwa;
- **przyrządowy system bezpieczeństwa, SIS** - implementacja jednej lub kilku przyrządowych funkcji bezpieczeństwa; SIS jest złożony z czujnika(ów), przelicznika(ów) logicznego(ych) i urządzenia(ń) końcowego(ych).
- **nienaruszalność bezpieczeństwa** - prawdopodobieństwo, że przyrządowa funkcja bezpieczeństwa będzie realizowana w sposób zadawalający, we wszystkich określonych warunkach i w określonym okresie czasu

- **poziom nienaruszalności bezpieczeństwa, SIL** - dyskretny poziom (jeden z możliwych czterech), do podawania wymagań nienaruszalności bezpieczeństwa przyrządowej funkcji bezpieczeństwa, która ma być alokowana w przyrządowym systemie bezpieczeństwa; poziom 4 jest poziomem najwyższym, poziom 1 – najniższym (im wyższy poziom nienaruszalności bezpieczeństwa, tym mniejsze prawdopodobieństwo nie zrealizowania funkcji bezpieczeństwa).

2. ZASADA REDUKCJI RYZYKA

2.1. Wprowadzenie

Analizę zagrożeń i ryzyka w zakresie urządzeń automatyki przeprowadza się w powiązaniu z obiektem (maszyną, instalacją, procesem itd.), którym te urządzenia sterują. Same urządzenia spełniają określone funkcje sterownicze i powiązane z nimi funkcje bezpieczeństwa i aby zapewnić dostatecznie niskie ryzyko, powinny reprezentować poziom nienaruszalności bezpieczeństwa (SIL) [2], odpowiedni do wymagań związanych z konkretnym obiektem.

Systemy sterowania mają istotne znaczenie w procesie redukcji ryzyka; są stosowane m.in. do:

- zapobiegania powstawaniu zagrożeń, np. przez wprowadzanie blokad uniemożliwiających niebezpieczne sekwencje zdarzeń;
- ograniczania prawdopodobnej ostrości urazów, szkód zdrowia, szkód w środowisku, szkód w procesie związanych z sytuacją zagrażającą, np. ograniczanie prędkości, włączanie wentylacji awaryjnej, ograniczanie ciśnienia, włączanie alarmów ostrzegawczych lub nakazujących ewakuację;
- zapobieganie narażania na zagrożenie, np. przez blokowanie wejścia osób nieuprawnionych do stref niebezpiecznych;
- wprowadzanie dodatkowych środków ochronnych, np. zatrzymanie awaryjne połączone z procedurą zatrzymania bezpiecznego;
- redukowanie ryzyka w warunkach uszkodzeń, np. automatyczne monitorowanie, ochrona przeciążeniowa.

Systemy automatyki są więc często systemami wiążącymi się z bezpieczeństwem.

2.2 Ryzyko a nienaruszalność bezpieczeństwa [6]

2.2.1 Konieczna redukcja ryzyka

Konieczna redukcja ryzyka jest takim zmniejszeniem ryzyka, które należy osiągnąć, aby dojść do ryzyka tolerowalnego w danej konkretnej sytuacji. Ryzyko tolerowalne może być podane w postaci jakościowej lub ilościowej (np. jako stwierdzenie, że zdarzenie zagrażające wywołujące określone skutki może wystąpić raz na 10^8 h). Pojęcie koniecznej redukcji ryzyka ma podstawowe znaczenie przy opracowywaniu specyfikacji wymagań bezpieczeństwa dotyczącej systemów elektrycznych /elektronicznych /programowalnych elektronicznych (E/E/PE) wiążących się z bezpieczeństwem. Celem określenia ryzyka tolerowalnego w odniesieniu do określonego zdarzenia zagrażającego jest stwierdzenie, co uważa się za racjonalne w odniesieniu do obu parametrów: częstości (lub prawdopodobieństwa) wystąpienia zdarzenia zagrażającego i jemu właściwych konsekwencji. Systemy wiążące się z bezpieczeństwem są przeznaczone do redukowania częstości (lub prawdopodobieństwa) wystąpienia zdarzenia zagrażającego i/lub konsekwencji takiego zdarzenia.

Ryzyko tolerowalne, zwane też docelowym poziomem ryzyka, będzie zależeć od wielu czynników, na przykład: ciężkości obrażeń, liczby osób narażonych na niebezpieczeństwo, długotrwałości narażenia na niebezpieczeństwo, możliwych szkód w środowisku naturalnym. Ważnymi czynnikami będą tu spostrzegawczość i możliwość widzenia ze strony osób narażonych

na zagrożenie. Przy dochodzeniu do konkluzji, na jakim poziomie ustalić ryzyko tolerowalne w określonym zastosowaniu, rozważa się pewną liczbę danych wejściowych zawierających m.in.:

- wytyczne odpowiedniej jednostki określającej przepisy bezpieczeństwa;
- dyskusje i uzgodnienia z różnymi stronami zaangażowanymi w to konkretne zastosowanie
- normy i przewodniki przemysłowe;
- międzynarodowe dyskusje i uzgodnienia, w tym normy regionalne i międzynarodowe;
- najlepsze niezależne porady przemysłowe, eksperckie i naukowe ze strony instytucji doradczych;
- wymagania prawne, tak ogólne jak i dotyczące bezpośrednio konkretnego zastosowania.

2.2.2 Rola systemów E/E/PE wiążących się z bezpieczeństwem

Systemy E/E/PE (elektryczne/ elektroniczne/ programowalne elektroniczne) wiążące się z bezpieczeństwem uczestniczą w procesie koniecznej redukcji ryzyka, zmierzającej do osiągnięcia ryzyka tolerowalnego.,

System wiążący się z bezpieczeństwem realizuje dwa działania:

- implementuje wymagane funkcje bezpieczeństwa konieczne do osiągnięcia stanu bezpiecznego urządzeń kontrolowanych lub do utrzymania stanu bezpiecznego urządzeń kontrolowanych;
- jest przewidziany do osiągnięcia, samemu lub z innymi systemami z bezpieczeństwem i systemami zewnętrznymi redukującymi ryzyko, koniecznej nienaruszalności bezpieczeństwa w odniesieniu do wymaganej funkcji bezpieczeństwa [6].

Integralną częścią systemu wiążącego się z bezpieczeństwem może być człowiek - operator.

2.2.3 Nienaruszalność bezpieczeństwa

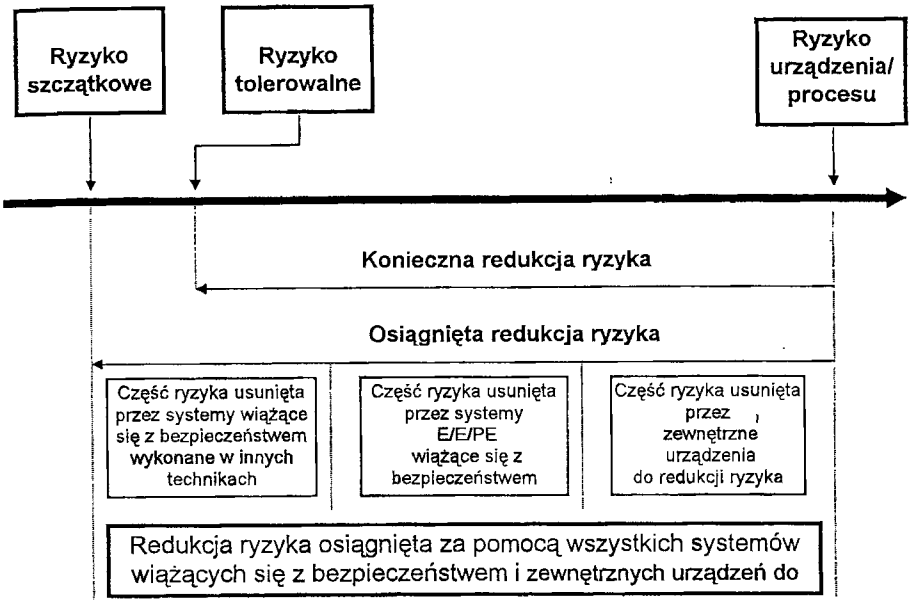
Nienaruszalność bezpieczeństwa jest zdefiniowana jako prawdopodobieństwo, że system wiążący się z bezpieczeństwem będzie wypełniał prawidłowo wymagane funkcje bezpieczeństwa, we wszystkich ustalonych warunkach i w ustalonym okresie czasu [5]. Nienaruszalność bezpieczeństwa odnosi się do wykonywania, przez systemy wiążące się z bezpieczeństwem, zadania realizacji funkcji bezpieczeństwa . Funkcjami tymi są przykładowo:

- uruchomienie procesu z zachowaniem należytych środków bezpieczeństwa;
- wyłączenie procesu z zachowaniem należytych środków bezpieczeństwa;
- wyłączenie awaryjne połączone z procedurą bezpiecznego zatrzymania;
- uniemożliwienie nieoczekiwanego uruchomienia.

Nienaruszalność bezpieczeństwa wymagana w odniesieniu do systemów wiążących się z bezpieczeństwem i zewnętrznych urządzeń do redukcji ryzyka musi mieć taki poziom, aby zapewnić że:

- częstość uszkodzeń systemów wiążących się z bezpieczeństwem jest wystarczająco niska, aby zapobiec przekroczeniu przez prawdopodobieństwo wystąpienia zdarzeń zagrażających wartości wymaganej do uzyskania ryzyka tolerowalnego. i/lub

• systemy wiążące się z bezpieczeństwem ograniczają konsekwencje uszkodzenia do rozmiarów wymaganych do uzyskania ryzyka tolerowalnego.



Rysunek 1 - Ogólna koncepcja redukcji ryzyka [6]

Na rysunku 1 przedstawiono ogólną koncepcję redukcji ryzyka. Model ogólny zakłada, że:

- występuje urządzenie sterowane i jego system sterowania;
- są wprowadzone powiązane czynniki ludzkie;
- na urządzenia ochronne składają się:

⇒ zewnętrzne urządzenia do redukcji ryzyka;

⇒ systemy E/E/PE wiążące się z bezpieczeństwem;

⇒ urządzenia wiążące się z bezpieczeństwem wykonane w innych technikach.

Schemat przedstawiony na rysunku 1 jest bardzo ogólny i w konkretnych przypadkach powinien być modyfikowany tak, aby odzwierciedlał rzeczywistą sytuację.

Różne rodzaje ryzyka wskazane na rysunku 1 mają znaczenia zdefiniowane w rozdziale 1.:

Ryzyko urządzenia/procesu jest funkcją ryzyka towarzyszącego samemu urządzeniu/ procesowi, lecz przy wzięciu pod uwagę redukcję ryzyka wprowadzaną przez system sterowania urządzeniem/procesem. Konieczna redukcja ryzyka zostaje osiągnięta za pomocą kombinacji wszystkich urządzeń ochronnych.

3. PROPONOWANA METODA POSTĘPOWANIA

3.1. Ustalenie ryzyka docelowego

Na podstawie kryteriów wymienionych w rozdziale 2.2.1 należy ustalić ryzyko docelowe i uzyskać zatwierdzenie go przez zamawiającego ocenę

3.2. Identyfikacja zdarzeń zagrażających

Metodą szczególnie dopasowana do identyfikacji zagrożeń w zautomatyzowanych obiektach przemysłowych, jest Metoda Badania Zagrożeń i Gotowości Operacyjnej (HAZOP) [7]. Jest ono uporządkowaną i systematyczną techniką do badania systemów, której celami są:

- zidentyfikowanie potencjalnych zagrożeń w systemie - zidentyfikowane zagrożenia mogą dotyczyć tylko bezpośredniego obszaru systemu, jak też mieć dużo szerszy zasięg oddziaływania np. mogą to być niektóre zagrożenia środowiska;
- zidentyfikowanie potencjalnych problemów w działaniu systemów i w szczególności zidentyfikowanie przyczyn tych zaburzeń w działaniu i odchyleń produkcyjnych, które mogą doprowadzić do produktu niezgodnego z wymaganiami.

Cechą charakterystyczna HAZOP jest „sesja badawcza", w czasie której wielodyscyplinarny zespół, kierowany przez lidera badania, systematycznie bada wszystkie istotne części projektu lub systemu. W odróżnieniu od wielu innych narzędzi i technik dostępnych do identyfikacji potencjalnych zagrożeń i problemów w działaniu, które mogą być stosowane we wczesnych fazach cyklu życia systemu, gdy jest dostępny mały zakres informacji, badanie HAZOP wymaga wielu szczegółów dotyczących rozpatrywanego systemu, za to dostarcza bardziej wyczerpującej informacji na temat zagrożeń i błędów w projekcie systemu.

Badanie HAZOP jest szczegółowym procesem identyfikacji zagrożeń i problemów w działaniu wykonywanym przez zespół. HAZOP zajmuje się identyfikacją potencjalnych odchyleń od zamierzenia projektowego, badaniem ich możliwych przyczyn i oceną ich konsekwencji.

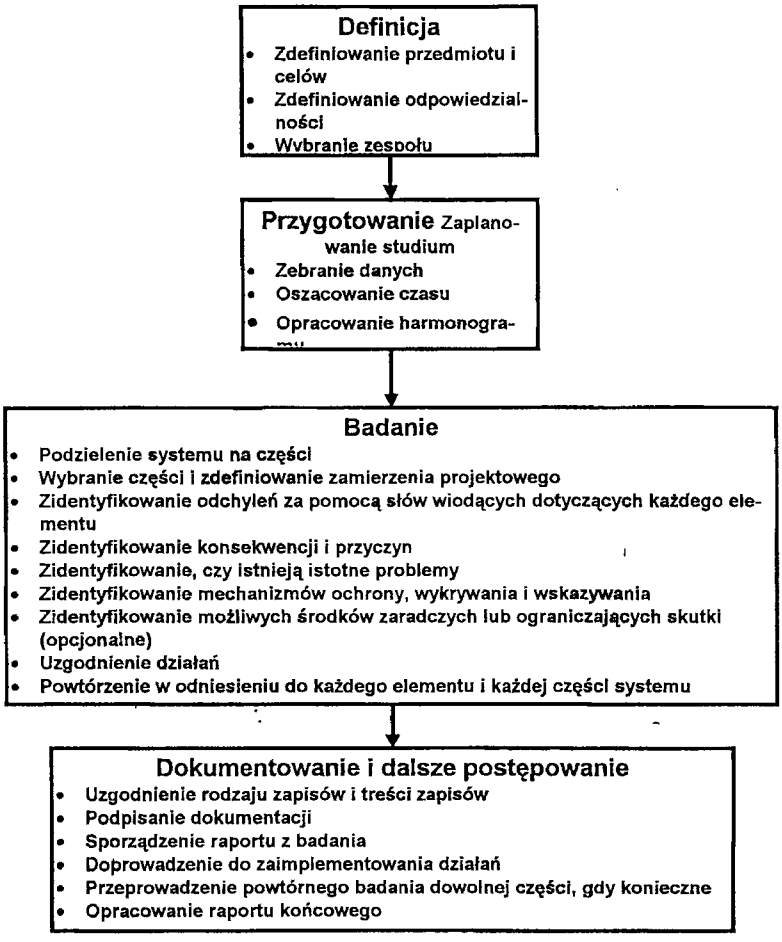
Badanie HAZOP składa się z czterech kolejnych kroków, jak to pokazano na rysunku 2.

Wyniki badania HAZOP powinny podawać, między innymi, co następuje:

- Szczegóły zidentyfikowanych zagrożeń i problemów operacyjnych, łącznie ze szczegółami postanowień dotyczących ich wykrywania i/lub ograniczenia;
- Działania wymagane do rozwiązania niepewności wykrytych podczas badania;
- Zalecenia dotyczące ograniczenia zidentyfikowanych problemów, bazujące na znajomości systemu przez zespół badający (gdy jest to w zakresie badania);
- Uwagi wskazujące na szczególne sprawy, które należy rozwiązać w procedurach operatorskich oraz obsługi i serwisu;

3.3. Ocena ryzyka

Wyniki badania HAZOP są wejściem do rozpoczęcia analizy ryzyka. Podstawowe znormalizowane metody są omówione w [xxxxxxxx, Sk i TM]. Proponuje się przyjęcie opisanej niżej metody postępowania.



Rysunek 2. - Procedura badania HAZOP

3.3.1. Identyfikacja warstw ochrony

Koncepcję zastosowania wielokrotnych warstw ochrony w przemysłach procesowych przedstawiono na rysunku 3.[3]. Polega ona na trzech podstawowych założeniach:

1. Warstwa ochrony (Protection Layer - PL.) składa się z zestawów wyposażenia i/lub posunięć administracyjnych, które współgrają z innymi warstwami w celu kontroli i/lub zmniejszania ryzyka związanego z procesem.
2. Niezależna warstwa ochrony (Independent Protection Layer - IPL) jest warstwą ochrony spełniającą następujące kryteria:

- Redukuje zidentyfikowane ryzyko co najmniej dziesięciokrotnie;
- Ma wysoki stopień dostępności (0,9 lub wyższy);

- Ma poniżej wymienione niezbędne właściwości:

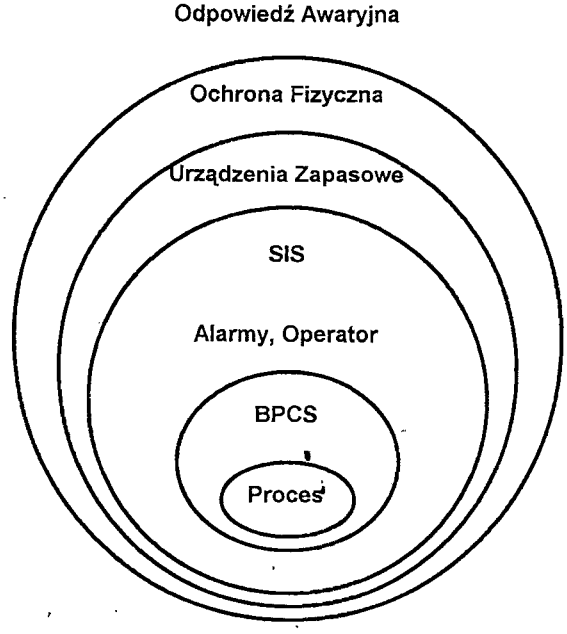
➢ szczególność - określona IPL jest przeznaczona do zapobieżenia lub zmniejszenia konsekwencji jednego zdarzenia potencjalnie zagrażającego; wielorakie przyczyny mogą powodować to samo zdarzenie zagrażające, tak więc wielorakie scenariusze powstania zdarzenia mogą inicjować działanie IPL;

➢ niezależność - IPL jest niezależne od innych warstw ochrony; inaczej mówiąc wystąpienie jednego zdarzenia ma wpływ tylko na tylko jedną IPL;

➢ pewność - można liczyć, że IPL wykona to do czego została zaprojektowana, również przy wystąpieniu tych błędów przypadkowych i systematycznych, które były rozważane przy jej projektowaniu;

➢ auditowalność - IPL jest zaprojektowana tak, aby ułatwić regularną walidację jej funkcji ochronnych.

3. Bezpiecznie blokująca warstwa ochrony (Safety Interlock Protection Layer - SIPL) jest IPL spełniającą definicję Przyrządowego Systemu Bezpieczeństwa.



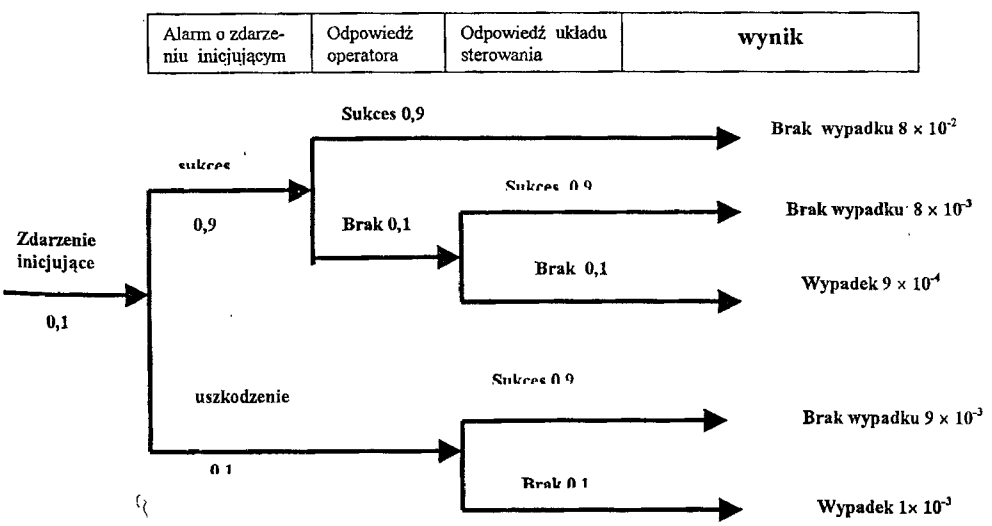
Rysunek 3. - Warstwy ochrony

3.3.2. Analiza zagrożeń

- Za pomocą badania HAZOP (patrz powyżej) należy wykonać, odnoszącą się do rozpatrywanego procesu, analizę zagrożeń w celu zidentyfikowania: potencjalnych zewnętrznych zdarzeń inicjujących zagrożenia, potencjalnych odchyleń w procesie i ich przyczyn, dostępnych systemów technicznych i potencjalnych zdarzeń zagrażających (wypadków), które mogą się pojawić.
- Każdemu zidentyfikowanemu zdarzeniu inicjującemu należy przypisać prawdopodobieństwo jego zaistnienia.

3.3.3. Identyfikacja warstw ochrony

- Należy zidentyfikować istniejące w rzeczywistości lub przewidziane w projekcie (zależnie w jakiej fazie życia systemu jest przeprowadzana ocena) niezależne warstwy ochrony - IPL;
- Każdej IPL należy przypisać prawdopodobieństwo niewykonania wymaganych od niej funkcji ochronnych; prawdopodobieństwo to może być wynikiem obliczenia jej nieuszkadzalności (np. współczynnika MTBF) lub oszacowania na podstawie praktyki;
- Każdemu zidentyfikowanemu zdarzeniu inicjującemu należy przypisać scenariusz rozwoju zdarzeń, aż do ewentualnego wystąpienia wypadku i konsekwencja tego wypadku;
- Każdą z dróg w scenariuszu należy opisać prawdopodobieństwem rozwoju zdarzenia po tej drodze i na tej podstawie wyliczyć prawdopodobieństwo zajścia zdarzeń końcowych;



Rys. 4 – Przykładowy graf scenariusza wypadku

- Jeżeli prawdopodobieństwo zajścia wypadków przekracza prawdopodobieństwo założone przy ustalaniu ryzyka docelowego, to należy wprowadzić dodatkowe warstwy ochrony o wyższym SIL i sprawdzić spełnienie wymagań.

- Uzyskanie zadowalającego prawdopodobieństwa zajścia wypadku stanowi zakończenie rozpatrywania danego zdarzenia inicjującego i umożliwia przejście do analizy następnego zdarzenia inicjującego;
- Rozpatrzenie wszystkich zidentyfikowanych zdarzeń inicjujących kończy ocenę ryzyka.

Przykład scenariusza zdarzeń przedstawiono na rysunku 4.

W przypadku, gdy docelowe ryzyko wymaga prawdopodobieństwa zajścia wypadku mniejszego niż 0,001 należy wprowadzić dodatkową warstwę ochrony o SIL 2 lub wyższym.

4. ZAKOŃCZENIE

Przedstawiona metoda postępowania umożliwia zidentyfikowanie potencjalnych zagrożeń, jakie mogą wystąpić w systemie w wyniku działania zewnętrznych i wewnętrznych czynników inicjujących oraz opracowanie scenariusza dalszego rozwoju sytuacji, skalibrowanego prawdopodobieństwami zaistnienia zdarzeń korzystnych i niekorzystnych. Scenariusz taki daje możliwość oszacowania prawdopodobieństwa zaistnienia wypadków i wskazuje gdzie należy wprowadzić przyrządowe funkcje bezpieczeństwa o podwyższonym SIL, tak aby osiągnąć ryzyko tolerowalne.

LITERATURA

1. Missala T.: *Bezpieczeństwo funkcjonalne urządzeń automatyki i robotyki.* Pomiary Automatyka Robotyka, 1997 r., z. 3.,ss 5-8 oraz Materiały Konferencji Automation'97, t. 1, ss 113-126, PIAP, 1997 r.
2. IEC 61511- 1 (65A/324/CDV: 2000) - *Functional safety: Safety Instrumented Systems for the process industry sector - Part 1: Framework, definitions, system, hardware and software requirements.*
3. IEC 61511- 3 (65A/325/CDV: 2000) - *Functional safety: Safety Instrumented Systems for the process industry sector - Part 3: Guidelines for the determination of safety integrity levels – informative.*
4. IEC 61508-1:1998. - *Functional safety: safety related systems - Part 1: General requirements (Bezpieczeństwo funkcjonalne - Systemy wiążące się z bezpieczeństwem - Wymagania ogólne);*
5. IEC 61508-4:1998. - *Functional safety: safety related systems - Part 4: Definitions and abbreviations of terms (Bezpieczeństwo funkcjonalne - Systemy wiążące się z bezpieczeństwem - Określenia);*
6. IEC 61508-5:1998. - *Functional safety: safety related systems - Part 5: Guidelines on the application of Part 1 (Bezpieczeństwo funkcjonalne - Systemy wiążące się z bezpieczeństwem - Wytyczne do stosowania arkusza 1);*
7. IEC 61882 (56/677/CDV): - *Guide for Hazard and Operability Studies (HAZOP).*