

LOPA

ANALIZA WARSTW ZABEZPIECZEŃ



**MGR INŻ.
JACEK ŻACZYŃSKI**

Kierownik Działu Technicznego
Oddział w Szczecinie
Urząd Dozoru Technicznego



**MGR INŻ.
DAMIAN FIEDOROWICZ**

Kierownik Działu Oceny Zgodności
Oddział w Szczecinie
Urząd Dozoru Technicznego

W całym cyklu artykułów przybliżamy Państwu tę bardzo szeroko stosowaną technikę analizy ryzyka LOPA (Layer of Protection Analysis). Szczegółowo prezentujemy procedurę prowadzenia analizy LOPA. Zaczęliśmy od procedury prowadzenia analizy LOPA, a następnie w szczegółach omawiamy kolejne jej kroki. W poprzednich częściach omówiliśmy zasady wyboru scenariuszy awaryjnych, identyfikacji zdarzeń inicjujących, niezależnych warstw zabezpieczeń oraz obliczenia częstotliwości zdarzenia awaryjnego i ryzyka. W kolejnych częściach opisujemy „podstawowe wymagania” (core attributes), które muszą spełnić zabezpieczenia, aby być IPL oraz odpowiadamy na pytanie „czy zakład jest gotowy na zastosowanie analizy LOPA?”. Analizujemy też wszystkie etapy metodyki LOPA na podstawie przykładu. Dotychczasowe opracowania były publikowane w magazynach INSPEKTOR 1/2024 oraz INSPEKTOR 2/2024.

ANALIZA WARSTW ZABEZPIECZEŃ (LOPA) TO PÓŁILOŚCIOWA METODA ANALIZY ORAZ OCENY RYZYKA OD 20 LAT POWSZECHNIE STOSOWANA GŁÓWNIEM W PRZEMYSLE CHEMICZNYM ORAZ PETROCHEMICZNYCH. W PORÓWNIANIU DO ILOŚCIOWYCH ANALIZ RYZYKA LOPA OSIĄGA PODOBNE REZULTATY PRZY RÓWNOCZESNYM OGRANICZENIU KOSZTÓW ORAZ WYKORZYSTANIA POTENCJAŁU LUDZKIEGO. JEDNOCZEŚNIE JEST METODĄ BARDZIEJ SZCZEGÓŁOWĄ NIŻ ANALIZY JAKOŚCIOWE. DAJE MOŻLIWOŚĆ ODKRYCIA SŁABYCH I MOCNYCH STRON STOSOWANYCH SYSTEMÓW BEZPIECZEŃSTWA (WARSTW ZABEZPIECZEŃ), ABY SKUTECZNIEJ CHRONIĆ PRACOWNIKÓW, ZAKŁAD I SPOŁECZEŃSTWO.

LOPA TO SPOŚÓB NA OCENĘ SCENARIUSZY AWARYJNYCH, KTÓRE POWODUJĄ NAJPOWAŻNIEJSZE SKUTKI W POWIĄZANIU Z WYSOKIM PRAWDOPODOBIEŃSTWEM ICH WYSTĄPIENIA.

Zgodnie z zapowiedzią tę część cyklu artykułów poświęcamy na omówienie podstawowych wymagań stawianych zabezpieczeniom IPL (**IPL – Independent Protection Layer**) tzw. **Niezależnym Warstwom Zabezpieczeń**.

W poprzednich częściach artykułu pisaliśmy już, że istotą LOPA jest identyfikacja istniejących zabezpieczeń oraz wybór spośród nich zabezpieczeń IPL. Ten krok jest kluczowym momentem podczas analizy, gdyż tylko zabezpieczenia zakwalifikowane jako IPL wpływają na redukcję poziomu ryzyka.

Prawidłowa identyfikacja niezależnych warstw zabezpieczeń IPL wpływa bezpośrednio na wyniki przeprowadzanych analiz. Błędy na tym etapie wprowadzają poczucie fałszywego bezpieczeństwa, a co za tym idzie, **akceptację niedoszacowanego ryzyka**, bezpośrednio obniżając całkowity poziom bezpieczeństwa. Pozorne osiągnięcie ryzyka na poziomie akceptowalnym lub tolerowanym może prowadzić do zaniechania stosowania zabezpieczeń rozumianych jako szeroko akceptowana dobra praktyka inżynierska. W związku z tym należy dołożyć należytej staranności, podejmując decyzję o uznaniu danego zabezpieczenia za IPL.

Aby zabezpieczenie mogło zostać zakwalifikowane jako IPL, musi spełnić poniższych siedem wymagań podstawowych core attributes:	ZAPAMIĘTAJ! Wszystkie IPL są zabezpieczeniami, ale nie wszystkie zabezpieczenia są IPL.
1. niezależność,	
2. funkcjonalność,	
3. nienaruszalność,	
4. niezawodność,	
5. audytowalność,	
6. bezpieczeństwo dostępu,	
7. zarządzanie zmianami.	

1. NIEZALEŻNOŚĆ

Pierwszym, fundamentalnym atrybutem jest **niezależność**, co oznacza, że każde zabezpieczenie IPL musi być niezależne od zdarzenia inicjującego (*initiating event*, IE) oraz innego zabezpieczenia IPL występującego już w analizowanym scenariuszu.

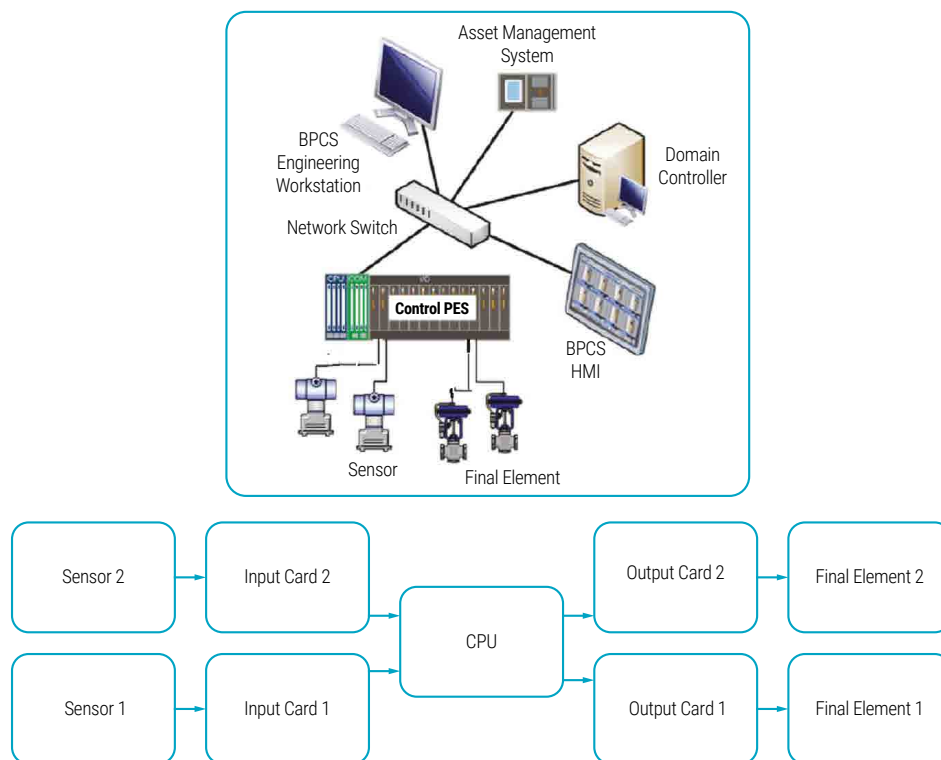
Niezależność uważa się za osiągniętą tylko wtedy, gdy działanie wybranego IPL lub jego komponentów nie jest zależne od awarii innego IPL lub IE. W przypadku gdy efektywna wydajność jednego elementu zależy od prawidłowego działania innego urządzenia, **warunek niezależności nie jest spełniony**.

Niezależność jest ważną koncepcją, chociaż absolutna niezależność jest zazwyczaj nieosiągalna. Zakłady mają wspólne media (np. powietrze PIA), zazwyczaj jeden personel konserwacyjny, wspólne urządzenia kalibracyjne i ustalonych dostawców, którzy dostarczają szereg podobnych komponentów do zastosowań w całym obiekcie. Jednak IPL powinny być wystarczająco niezależne, tak aby stopień współzależności nie był statystycznie istotny.

W metodyce LOPA do oceny niezależności IPL obejmujących układy podstawowego systemu sterowania procesem BPCS (ang. *Basic Process Control System*) stosuje się dwa podejścia – jak poniżej.

PODEJŚCIE A	PODEJŚCIE B
<p>Aby urządzenie lub działanie (np. operatora) zostało uznane za IPL, musi być niezależne zarówno od zdarzenia inicjującego, jak i od każdego zdarzenia umożliwiającego oraz od każdego innego urządzenia, systemu lub działania, które jest już uznawane za IPL dla tego samego scenariusza.</p> <p>Podejście A przyjmuje konserwatywne stanowisko, że każda awaria sprzętu BPCS wpływa na prawidłową pracę wszystkich innych układów zaimplementowanych w ramach BPCS.</p> <p>Jest ono stosowane w przypadku LOPA, ponieważ jego zasady są jasne i konserwatywne. Zapewnia wysoki poziom ochrony przed awariami o wspólnej przyczynie między IE i IPL lub między dwoma IPL.</p>	<p>Podejście B pozwala na użycie dwóch funkcji BPCS w jednym scenariuszu awaryjnym, jako dwóch zabezpieczeń IPL, lub jako zabezpieczenia IPL przy równoczesnym założeniu, że zdarzeniem inicjującym IE jest układ BPCS (z niezależnością wymaganą dla niektórych komponentów).</p> <p>To podejście opiera się na założeniu, że jeśli funkcja BPCS ulegnie awarii, prawdopodobne jest, że komponentem, który ją wywołał, jest przetwornik (czujnik) lub element końcowy (np. zawór), a nie sterownik logiczny BPCS (CPU). Doświadczenie przemysłowe wskazuje, że wskaźniki awaryjności czujników i końcowych elementów sterujących są zwykle znacznie wyższe niż wskaźniki awaryjności sterownika logicznego BPCS. To znaczy, że aby dwa układy BPCS były uważane za IPL, wszystko musi być niezależne z wyjątkiem płyty głównej – niezależne czujniki, niezależne karty wejściowe, niezależne karty procesora, niezależne karty wyjściowe i niezależne elementy końcowe (rys. 1) – z zastrzeżeniem Patrz: ramka „UWAGA”.</p>





Rys. 1. Podejście B. Dwie pętle BPCS ze współdzielonym procesorem CPU mogą być wykorzystywane w jednym scenariuszu po przeprowadzeniu dodatkowych analiz oraz potwierdzeniu, że całkowite PRD < 0,01/rok [3, 4]

UWAGA

Zastosowanie podejścia B wymaga, aby analityk ryzyka miał doświadczenie w projektowaniu BPCS, dysponował odpowiednimi danymi na temat rzeczywistej niezawodności BPCS i rozumiał, jak identyfikować i uwzględnić awarie o wspólnej przyczynie. Podejście B wymaga również zaangażowania się kierownictwa w egzekwowanie rygorystycznych praktyk niezbędnych do kontrolowania błędów systemowych, błędów zależnych oraz błędów o wspólnej przyczynie.

Przed użyciem podejścia B należy upewnić się, że istnieje wystarczająca ilość danych analitycznych i testowych, aby wykazać, że BPCS dla konkretnego procesu jest zaprojektowany i zarządzany w taki sposób, że dwa układy BPCS w połączeniu mogą osiągnąć ogólny wskaźnik awaryjności na poziomie < 0,01/rok.

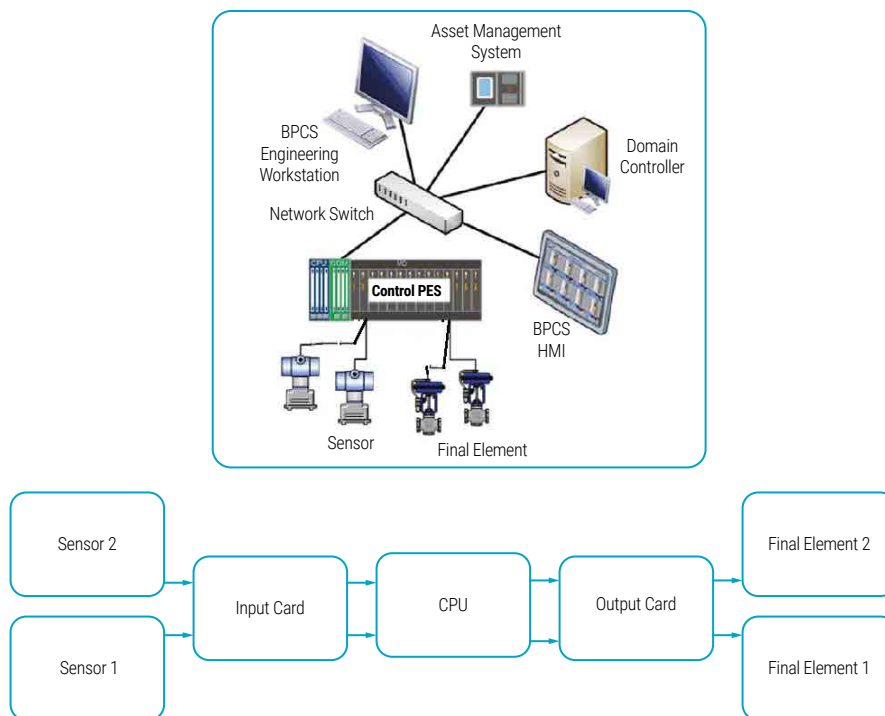
Analiza ta powinna obejmować co najmniej:

- ocenę potencjalnych wspólnych przyczyn, wspólnego trybu i systematycznych błędów między BPCS IE i IPL lub dwoma BPCS IPL, aby określić, że ich wpływ jest wystarczająco niski;
- pisemną specyfikację obejmującą pętle bezpieczeństwa w systemie, takie jak schematy przyrządów, schematy P&ID, schematy pętli i specyfikacje funkcjonalne;
- w przypadku ogólnego podejścia do walidacji danych ocenę poprzedniej historycznej wydajności procesora BPCS, kart wejścia/wyjścia, czujników, elementów końcowych, reakcji człowieka itp.;
- w przypadku podejścia do walidacji danych specyficznych dla danej instalacji ocenę danych z inspekcji, konserwacji i testów w znaczącym okresie w celu wykazania, że system osiąga deklarowaną wydajność;
- ocenę bezpieczeństwa dostępu do sprzętu i oprogramowania;
- zarządzanie zmianami i kontrolą wersji sprzętu i oprogramowania, w tym wartości nastaw, konfiguracji i nadpisów operatora.

Analiza tego typu wymaga większej wiedzy specjalistycznej i bardziej szczegółowego zrozumienia projektu sprzętu i oprogramowania BPCS niż zwykle jest wykorzystywana w zespołach LOPA.

W związku z tym wymagana jest dodatkowa weryfikacja i ocena funkcjonalna przeprowadzona przez osobę kompetentną w zakresie takiej analizy, aby upewnić się, że integralność i niezawodność BPCS są wystarczające.

Dopiero po wykonaniu powyższej analizy i dowiedzeniu, że współczynnik awaryjności dwóch wspólnych układów BPCS $< 0,01$ /rok, w prowadzonej analizie LOPA można zastosować podejście B.



Rys. 2. Podejście B. Dwie pętle BPCS ze współdzielonym procesorem i współdzielonymi kartami I/O. Ta architektura jest generalnie niedopuszczalna do zaliczania dwóch pętli BPCS w jednym scenariuszu. Jest to zgodne z CCPS LOPA (2001), który zalecał, aby nie zaliczać drugiej funkcji w BPCS, gdy karta wejściowa lub wyjściowa jest wspólna dla obu pętli [3, 4]

Jeżeli mówimy o niezależności, należy wspomnieć o sytuacjach, w których system bezpieczeństwa IPL może działać skutecznie tylko wtedy, gdy inny system jest przynajmniej częściowo skuteczny. Poniżej kilka typowych przykładów.

- Zawór bezpieczeństwa jest dobierany na scenariusz pożaru, a obliczenia jego doboru zakładają, że izolacja zbiornika jest na tyle sprawna, że ogranicza przepływ strumienia ciepła.
- Szeroko stosowane rozwiązania w przemyśle oil&gas związane ze stosowaniem zaworów bezpieczeństwa (*pressure safety valve*, PSV) uwzględniają zabudowanie na rurociągach dolotowych i wylotowych PSV-ów zaworów odcinających. W takich przypadkach skuteczność działania zaworów bezpieczeństwa jako IPL opiera się na założeniu, że wszystkie zawory odcinające w obrębie PSV ustawione są w odpowiednich pozycjach.

W powyższych przypadkach opisane zawory bezpieczeństwa same w sobie **nie stanowią niezależnych IPL**. Skuteczne zapobieganie skutkom awarii zależy od funkcjonowania **obu elementów**. Zamiast pojedynczego zaworu bezpieczeństwa w takich przypadkach **oba elementy* należy traktować jako jeden IPL**, a deklarowane PFD (Probability of Failure on Demand) nie może być mniejsze niż PFD najmniej niezawodnego elementu w systemie.

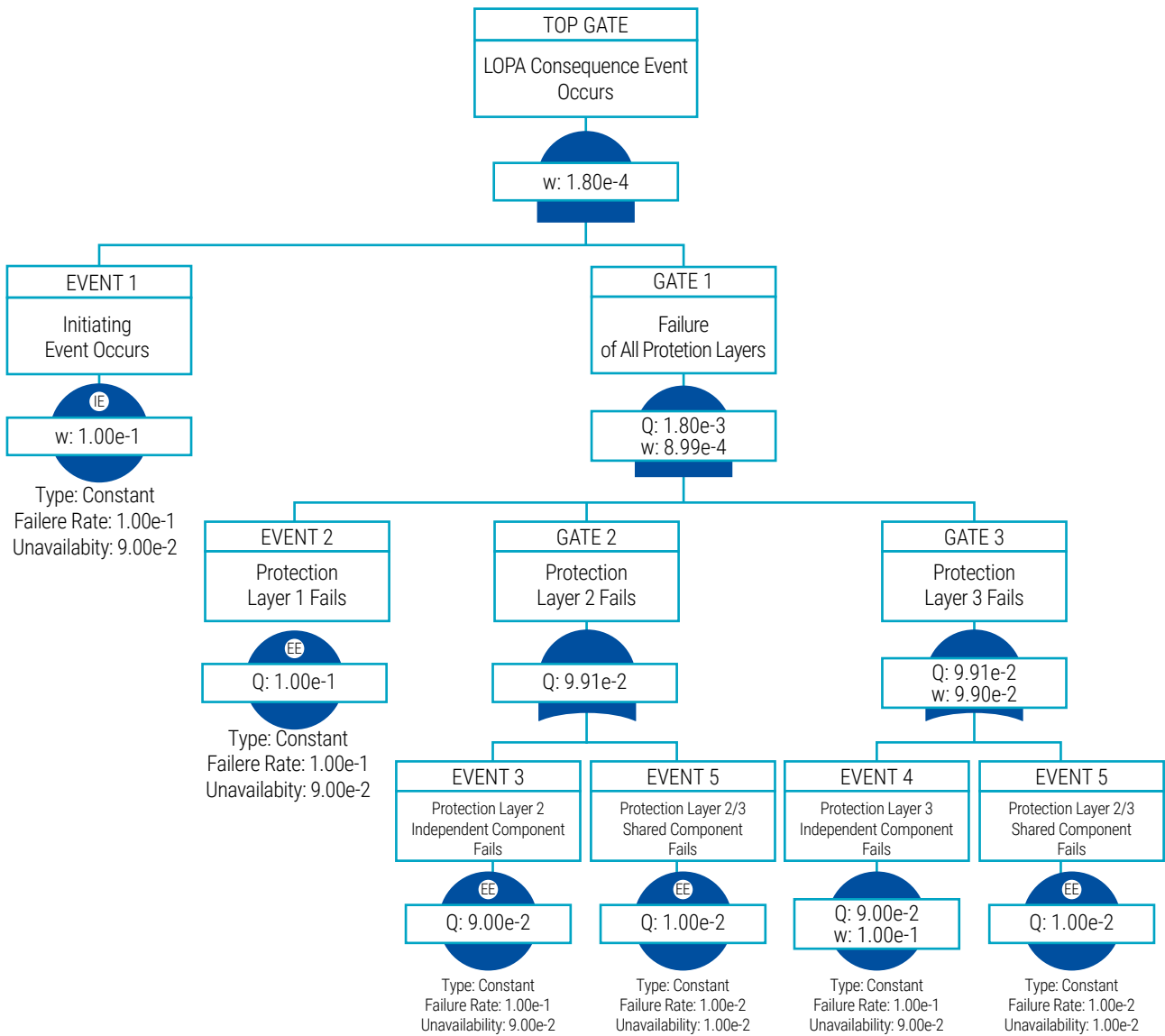
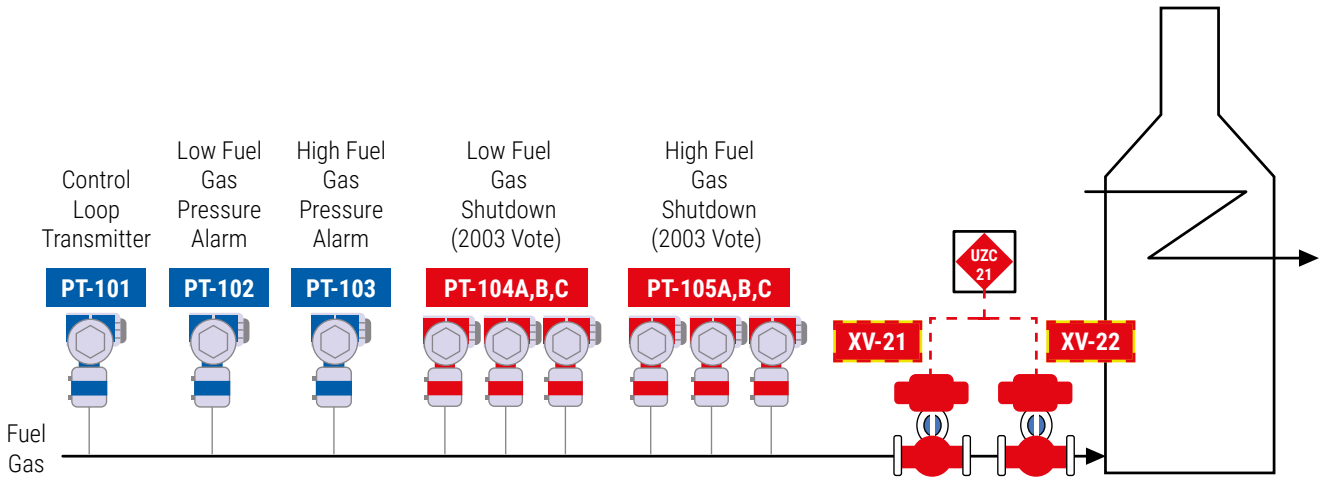
*np. zawór bezpieczeństwa + otwarcie zaworów ocinających „działanie operatora” lub zawór bezpieczeństwa + izolacja zbiornika

UWAGA

W przypadku instalacji, gdy funkcje bezpieczeństwa korzystają ze wspólnych elementów, np. elementów wykonawczych (BMS w kotłach parowych lub piecach technologicznych), gdzie zawory odcinające na „ścieżkach” gazu opałowego są wspólne dla wszystkich funkcji bezpieczeństwa, wykorzystywanie analizy LOPA w celu szacowania ryzyka lub analizy SIL jest niewłaściwe.

Konserwatywne zasady w LOPIE wykluczają możliwość kwalifikacji wszystkich funkcji bezpieczeństwa jako IPL (brak spełnienia wymogu niezależności).

W takich przypadkach analiza LOPA powinna być zastąpiona lub rozszerzona o analizę ilościową FTA (Fault Tree Analysis) w celu oszacowania PFD wszystkich funkcji bezpieczeństwa z uwzględnieniem błędów o wspólnej przyczynie.



Rys. 3. Ścieżka gazowa dla typowego pieca rafineryjnego, FTA – analiza drzewa błędu [7]

2. FUNKcjONALNOŚĆ

Zabezpieczenia, aby można je było uznać za IPL, muszą zostać zweryfikowane pod kątem funkcjonalności.

IPL musi wykonywać swoją zamierzoną funkcję w rzeczywistych warunkach roboczych procesu podczas niebezpiecznego zdarzenia, a szereg różnych czynników musi być wziętych pod uwagę, aby zapewnić skuteczne działanie IPL. Niektóre z tych czynników zostały wymienione poniżej.

- Podstawa projektowa IPL ma zastosowanie do konkretnego scenariusza, dla którego jest zaliczana. Stosowanie norm i standardów technicznych (takich jak EN, NFPA, ASME, API itp.) może pomóc w zapewnieniu, że zastosowane zabezpieczenia kwalifikują się jako IPL.
- IPL jest skuteczny dla analizowanego trybu działania (rozruch, zatrzymanie, normalna praca itp.).
- Gdy reakcja operatora jest częścią IPL, istnieje dobrze napisana procedura i skuteczny program szkoleniowy, aby zapewnić, że operatorzy rozumieją zagrożenie i są w stanie skutecznie reagować na alarm.
- IPL jest w stanie wykonać swoją funkcję w wystarczającym czasie, aby zapobiec skutkom scenariusza awaryjnego. W przypadku IPL związanego z działaniem człowieka należy potwierdzić, że operator ma wystarczająco dużo czasu na przywrócenie procesu do stanu bezpiecznego.

Funkcjonalność przypisuje unikalne i odpowiednie cechy zabezpieczeniom IPL. Na przykład zawór bezpieczeństwa jest zaprojektowany tak, aby otwierał się przy ciśnieniu wystarczająco niskim, a jego przepustowość wraz rurociągami są wystarczająco duże, aby zapobiec przekroczeniu ciśnienia projektowego w zbiorniku.

Krytycznym aspektem funkcjonalności jest działanie IPL w ściśle określonym czasie. Gdy wystąpi zdarzenie inicjujące, stan procesu może się szybko zmienić ze stanu normalnego, bezpiecznego, w stan niebezpieczny. Odchylenie procesu od stanu normalnego może ostatecznie doprowadzić do poważnej katastrofy przemysłowej.

Ocena IPL jest ważna, aby potwierdzić, że IPL może pomyślnie wykonać swoje działanie i że proces może powrócić do stanu bezpiecznego w zakresie czasu bezpieczeństwa procesu (Proces Safety Time, PST).

PST to okres między wystąpieniem awarii w procesie lub jego systemie sterowania a wystąpieniem skutków niebezpiecznego zdarzenia.

PRZYKŁAD

W momencie awarii układu regulacji ciśnienia zaczyna ono rosnąć powyżej normalnych wartości roboczych, czyli nastąpiło odchylenie od stanu normalnego. Następnie ciśnienie w dalszym ciągu rośnie, przekraczając ciśnienie obliczeniowe np. zbiornika. W tym momencie mamy do czynienia ze stanem awaryjnym, ale dopiero po wzroście ciśnienia do wartości dużo powyżej wartości obliczeniowych możemy spodziewać się rozerwania zbiornika, zatem czas pomiędzy awarią układu regulacji a rozerwaniem zbiornika jest naszym czasem PST.

Każde zabezpieczenie uznane za IPL w LOPA musi skutecznie wykonywać swoją funkcję, tzn. musi działać szybciej, niż pogarsza się stan procesu, zapobiegając w ten sposób ostatecznym konsekwencjom, np. rozerwaniu zbiornika, eksplozji uwolnionych węglowodorów lub wybuchowi pożaru itp.

PRZYKŁAD

Czas reakcji wymagany dla działania operatora jako IPL zależy od niżej wymienionych czynników.

1. Jeśli oparty jest na alarmie, jest to czas, w którym czujnik wykrywa limit krytyczny i ogłasza go pracownikowi (czas powiadomienia).
2. Czas, w którym człowiek wykrywa alarm lub inne wskazanie nieprawidłowej sytuacji (czas wykrywania).
3. Czas, w którym pracownik decyduje o sposobie działania (czas decyzji).
4. Czas na zdiagnozowanie problemu; kroki mogą obejmować ustalenie, czy alarm jest fałszywy (czas diagnozy).
5. Czas potrzebny pracownikowi na wykonanie wymaganej czynności, w tym przywrócenie procesu do stanu normalnego, sprowadzenie procesu do stanu bezpiecznego lub wyłączenie procesu (czas działania).
6. Czas wymagany na powrót procesu do stanu bezpiecznego po zakończeniu działania IPL (czas przywrócenia procesu).

Należy zwrócić uwagę, że jeżeli zdiagnozowanie problemu lub działanie operatora wymaga od niego, aby wszedł do obszaru(-ów) objętego scenariuszem zagrożenia, powinno się również rozważyć, czy czas bezpieczeństwa procesu jest wystarczający, aby pracownik mógł potwierdzić powodzenie (lub niepowodzenie) swojego działania i bezpiecznie opuścić obszar.



Jeśli czas bezpieczeństwa nie jest wystarczający, działania operatora nie można uznać za skuteczne, a co za tym idzie, za IPL.

Jeżeli natomiast całkowite wykrycie i odpowiedź, wliczając jakiegokolwiek opóźnienie (np. brak operatora na stanowisku w momencie aktywacji alarmu), mogą zostać osiągnięte w wymaganym czasie, odpowiedź operatora spełnia ograniczenia czasowe, jest tym samym skuteczna i można zakwalifikować ją do IPL.

Autorzy podręcznika *Layer of Protection Analysis: Simplified Process Risk Assessment [1]* zalecają łatwy do zapamiętania zestaw słów kluczowych do przesiewania kandydatów IPL w zakresie funkcjonalności.

3 Ds	4 Enoughs
Detect	Big enough
Decide	Fast enough
Deflect	Strong enough
	Smart enough

Wiele warstw zabezpieczających ma zdolność do:

1. wykrywania (**detect**), że wystąpiła przyczyna inicjująca i scenariusz zmierza w kierunku niepożądanych konsekwencji;
2. decydowania (**decide**) o podjęciu działań, które mogą zapobiec wystąpieniu niepożądanych konsekwencji;
3. zapobiegania (**deflect**) rozwijaniu się scenariusza awaryjnego lub wystąpieniu jego skutków.

PRZYKŁAD

Sprężyna w zaworze bezpieczeństwa wykrywa (detect) wzrost ciśnienia, sprężyna decyduje (decide) o otwarciu zaworu, a prawidłowo zaprojektowany zawór bezpieczeństwa jest wystarczająco duży (big enough), szybki (fast enough), aby zapobiec zagrożeniu (deflect) przekroczenia przez ciśnienie w zbiorniku poziomu ciśnienia projektowego.

3. NIENARUSZALNOŚĆ

Nienaruszalność oznacza, że IPL ma wystarczającą niezawodność, aby móc całkowicie zapobiec konsekwencjom scenariusza awaryjnego.

Nienaruszalność warstwy ochronnej jest związana z redukcją ryzyka, której można rozsądnie oczekiwać, biorąc pod uwagę projekt, instalację i zarządzanie warstwą ochronną. Zrozumienie wielkości redukcji ryzyka możliwej do osiągnięcia przez konkretny IPL jest niezbędne do ustalenia, czy istnieje wystarczająca ochrona przed konsekwencjami scenariusza awaryjnego.

Na nienaruszalność wpływają również procedury i praktyki stosowane przez organizację w celu zminimalizowania prawdopodobieństwa błędu ludzkiego, który mógłby doprowadzić do awarii IPL. Ostatecznie niezawodność zarówno sprzętu, jak i ludzkich IPL ograniczona jest przez skuteczność systemów zarządzania.

Aby IPL był niezawodny, musi być dostępny w razie potrzeby.

Możliwość wykrywania i korygowania awarii w odpowiednim czasie skraca czas, w którym proces działa w warunkach zakłóceń, w operacjach przejściowych (takich jak konserwacja lub wyłączenie) lub bez ochrony w pełni funkcjonalnego IPL.

PRZYKŁAD

Jeśli operator natychmiast zauważy awarię poprzez obserwację, wskazanie lub alarm, można podjąć działania naprawcze w stosunkowo krótkim czasie. Stopień, w jakim awaria zostanie ujawniona, wpływa na dostępność IPL i zwiększa niezawodność systemu.

Nienaruszalność IPL zależy od niezawodności jej komponentów i zmierzonej funkcji.

**PRZYKŁAD**

Jeśli odpowiedź operatora na alarm jest uważana za IPL, a wybrana wartość PFD wynosi 0,1, to całkowita nienaruszalność IPL zależy nie tylko od działania samego operatora, ale również od niezawodności czujnika i powiązanego systemu sterowania (BPCS), który generuje alarm, oraz od tego, kiedy i jak operator podejmie działanie.

Dlatego dla układów sterowania, aby zachować ich niezawodność, zaleca się przeprowadzanie częstych kontroli, takich jak testy funkcjonalne, testy kontrolne, weryfikacja i walidacja czujników i systemu sterowania. Podobnie odpowiedniość działań operatora należy zapewnić za pomocą pisemnych procedur, regularnych szkoleń i weryfikacji ich skuteczności.

W przypadku niektórych IPL, takich jak przyrządowe funkcje bezpieczeństwa (SAFETY INSTRUMENTED FUNCTION, SIF) zaleca się przeprowadzać testy funkcjonalne wraz z symulacjami stanów niebezpiecznych, aby zweryfikować ich skuteczność.

Odpowiedni wybór wartości PFD (Probability of Failure on Demand), jak widzimy, nie jest rzeczą prostą i nie wystarczy wybrać jej z tabel z podręcznika LOPA.

Aby zachować niezawodność IPL-ów na wymaganym poziomie, zaleca się wdrożyć i przestrzegać procedur zarządzania bezpieczeństwem procesowym i funkcjonalnym.

Autorzy metody zauważyli również ten problem, że wiele organizacji wybiera wartości PFD z podręczników i artykułów lub uzyskuje je z obliczeń opartych na dyskretnych wskaźnikach awaryjności komponentów z baz danych, a następnie zakłada, że te wartości mają zastosowanie w ich sytuacji.

Takie podejście nie jest dobrym założeniem.

Nadrzędnym czynnikiem niezawodności komponentu lub niezawodności działania człowieka jest często lokalne środowisko sprzętu i lokalna kontrola błędów ludzkich.

PRZYKŁAD

PSV w obsłudze czystego gazu ma zdecydowanie inną niezawodność niż PSV w obsłudze olefin lub kwasów.

Odpowiedzią na ten problem była publikacja w 2015 r. książki CCPS *Guidelines for Initiating Events and Independent Protection Layers* [3], która dobrze omawia tę kwestię.

Ponadto niektóre organizacje zakładają, że ich komponenty mają znacznie lepszą niezawodność (niższy PFD lub IEF), niż podano w podręczniku wskazanym powyżej, mimo tego, że nie posiadają wystarczającej historii operacyjnej, np. zakład istnieje od 5 lat. Dodatkowo organizacja nie do końca rozumie, jak oszacować wskaźnik awaryjności takich komponentów.

PRZYKŁAD

Częstym błędem w szacowaniu PFD IPL-ów np. dla PSV jest nieuwzględnianie:

- zaworów odcinających na rurociągach dolotowych i wylotowych zaworów bezpieczeństwa,
- rodzaju medium – czystego, obojętnego czy krystalizującego i korozyjnego,
- sposobu zabudowy podwójnych zaworów bezpieczeństwa,
- wartości nastaw zaworów bezpieczeństwa dla dwóch zaworów pracujących równolegle.

Używanie wartości IEF (ang. *Initiating Event Frequency*) lub PFD niższych niż podane w tablicach danych niezawodnościowych jak w podręczniku wspomnianym powyżej musi być uzasadnione i wykazane pisemnie (zarejestrowane).

Następnym, lecz nie mniej ważnym problemem jest utrzymywanie oraz kontrola IPL w taki sposób, aby podane wartości PFD dla IEF lub IPL zgodnie z tabelami z podręcznika CCPS można było zastosować w analizie LOPA. Jeżeli IPL nie był utrzymywany, tzn. konserwowany, testowany, zgodnie z instrukcjami lub procedurami, to nie można mu przypisać żadnej wartości PFD.

PRZYKŁAD

Przeanalizujmy zawór bezpieczeństwa. Jeżeli nie był on konserwowany oraz testowany zgodnie z przyjętymi w procedurach terminami oraz zakresem konserwacji, to nie możemy mu przypisać żadnej wartości redukcji ryzyka. Dodatkowo LOPA zakłada, że po konserwacji i testach zawór ten ma PFD jak nowy.

Zasady LOPA wymagają, aby organizacje utrzymywały swoje IPL w taki sposób, aby można było udowodnić wartość PFD taką, jakiej chce się użyć w obliczeniach LOPA.

4. NIEZAWODNOŚĆ

Niezawodność to cecha IPL związana z jej wyposażeniem, działającym zgodnie z przeznaczeniem, w określonych warunkach, przez określony czas.

Do określenia wymaganej niezawodności IPL niezbędne jest całościowe zrozumienie:

- projektu IPL,
- procesu technologicznego, który jest chroniony przez IPL,
- przypisanej funkcji w ramach tego procesu,
- środowiska, w którym IPL będzie działać.

IPL jest uważany za niezawodny, gdy w sytuacji, kiedy jest to wymagane, działa zgodnie z założeniami, nie ma częstych okresów przestoju i nie działa bez przyczyny (częściowo lub całkowicie). Niezawodność jest zatem związana z działaniem IPL zgodnie z przeznaczeniem w środowisku operacyjnym przez przewidywany czas.

Ta koncepcja obejmuje więcej niż teoretyczne prawdopodobieństwo, że poszczególne elementy systemu będą działać prawidłowo, gdy będzie to wymagane. W przypadku niektórych IPL, aby osiągnąć ich wystarczającą niezawodność, potrzebne są określone praktyki projektowe, operacyjne, inspekcyjne i konserwacyjne.

PRZYKŁAD

Zawór bezpieczeństwa może być zaprojektowany dla określonego środowiska procesowego, np. korozyjnego, i być poddawany rygorystycznym testom opartym na zdefiniowanych procedurach i specyfikacjach w celu zapewnienia niezawodności.

Szczególną uwagę na to wymaganie należy zwrócić podczas określania jako IPL działania operatora w odpowiedzi na ALARM.

Aby uznać je za niezawodne i skuteczne, należy potwierdzić, że:

- istnieją pisemne procedury definiujące działanie operatora oraz dokumenty potwierdzające, że operator je zna,
- operator jest zawsze obecny w miejscu, gdzie alarm jest aktywowany,
- operator jest w stanie zidentyfikować problem na podstawie alarmu,
- operator ma wystarczająco dużo czasu na podjęcie skutecznego działania,
- operator został przeszkolony i dokładnie wie, jakie działanie na wypadek konkretnego alarmu ma wykonać,
- operator przechodzi w tym zakresie regularne szkolenia.

Jak możemy zauważyć, przykład związany z odpowiedzią na alarm płynnie przechodzi przez atrybuty związane z funkcjonalnością, nienaruszalnością oraz niezawodnością, nie jest to bynajmniej przypadek czy błąd. W pierwszym podręczniku *LOPA – book* z 2001 r. wymagania podstawowe, *core attributes*, składały się z trzech cech:

1. niezależność,
2. skuteczność,
3. audytowalność.

Na podstawie powyższego możemy stwierdzić, że cecha skuteczności została podzielona na trzy: funkcjonalność, nienaruszalność oraz niezawodność.

5. AUDYTOWALNOŚĆ

Audytowalność to zdolność do potwierdzenia, że warstwa zabezpieczeń zakwalifikowana jako IPL spełnia podstawowe wymagania – *core attributes*.

Proces audytu musi potwierdzić, że IPL jest skuteczny w zapobieganiu konsekwencjom scenariusza awaryjnego, jeśli działa zgodnie z przeznaczeniem.

Audyt powinien również potwierdzić, że projekt IPL, montaż, testy funkcjonalne i systemy konserwacji są wykonywane prawidłowo, aby osiągnąć określony PFD.

- Testy funkcjonalne muszą potwierdzić, że wszystkie komponenty np. dla SIF (czujniki, układ logiczny, elementy końcowe itp.) są sprawne i spełniają wszystkie stawiane im wymagania.
- Systemy konserwacji są okresowo audytowane w celu sprawdzenia, czy istniejące procesy administracyjne zapewniają, że konserwacja jest wykonywana zgodnie z wymaganiami, a dokumentacja projektu, konserwacji i testów kontrolnych jest utrzymywana.

Proces audytu powinien dokumentować stan IPL, wszelkie modyfikacje wprowadzone od ostatniego audytu i śledzić do zakończenia wszelkie wymagane działania związane z naprawami.

Proces zarządzania zmianą MOC (Management of Change) jest audytowany w celu zapewnienia, że zmiany w materiałach, parametrach operacyjnych, sprzęcie, procedurach i organizacji są prawidłowo przeglądane i dokumentowane, a wszelkie punkty działań zalecone w przeglądzie zostały wykonane.

Jak widzimy, procedury audytowania IPL są nierozdzielnie połączone z pozostałymi *core attributes*, bo nie można w żaden inny sposób określić, czy np. wspomniany już wielokrotnie zawór bezpieczeństwa PSV da się zakwalifikować jako IPL.

W celu poprawnej kwalifikacji jako IPL dokumentacja PSV powinna umożliwiać potwierdzenie, że PSV spełnia wszystkie podstawowe wymagania core attributes.

W tym celu dokumentacja powinna zawierać:

- podstawę wymiarowania PSV (dobór),
- wszystkie scenariusze awaryjne wymagające zadziałania zaworu wraz z wymaganym przepływem,
- specyfikację projektową zaworu,
- wymagany przepływ w warunkach zrzutowych dla najgorszego scenariusza,
- szczegóły instalacji (np. układ rurociągów dopływowych i zrzutowych),
- procedury testowe i konserwacyjne, w tym protokoły potwierdzające ciśnienie nastawy.

Bez powyższych dokumentów analityk ryzyka odpowiedzialny za prawidłowe przeprowadzenie LOPA nie może zakwalifikować PSV jako IPL.

6. BEZPIECZEŃSTWO DOSTĘPU

Bezpieczeństwo dostępu obejmuje stosowanie kontroli fizycznych i/lub administracyjnych w celu zmniejszenia ryzyka nieautoryzowanych zmian w systemie, które mogą uszkodzić lub dezaktywować urządzenia zabezpieczające. Dotyczy to np. zmian nastaw progów działania alarmów lub przyrządowych funkcji bezpieczeństwa.

Przemysł procesowy stosuje szereg środków w celu zmniejszenia ryzyka nieautoryzowanych zmian w systemie.

PRZYKŁADOWE RODZAJE ZABEZPIECZEŃ PRZED NIEAUTORYZOWANYMI ZMIANAMI

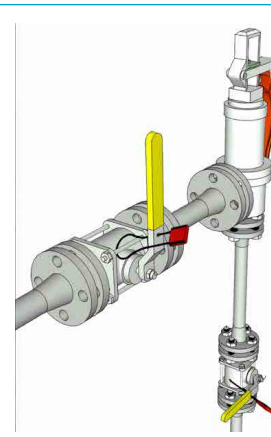
- Bezpieczeństwo dostępu do układów sterowania i automatyki zabezpieczającej stosuje się, aby zapobiec przypadkowym lub nieautoryzowanym modyfikacjom BPCS lub SIS (Safety Integrity System). Z jednej strony przypadkowa zmiana w układzie BPCS może prowadzić do rozwoju scenariusza awaryjnego, z drugiej zmiana nastaw progów działania alarmów lub by-pass przyrządowych funkcji bezpieczeństwa (SIF) może dezaktywować zabezpieczenia IPL.
- System zarządzania / procedura *Lock out, tag out* lub *lockout-tagout (LOTO)*, *Lock open / Lock closed*; *Car seal open / Car seal closed* to procedura bezpieczeństwa stosowana w celu zapewnienia, że ważne ze względów bezpieczeństwa zawory odcinające są ustawione w prawidłowych pozycjach i zabezpieczone przed przypadkową ich zmianą. Do tego celu używane są różne systemy wymuszające użycie dodatkowego narzędzia, np. klucza, aby móc zmienić ich pozycję. Dotyczy to najczęściej zaworów odcinających na dolocie i wylocie z zaworów bezpieczeństwa PSV lub ważnych ze względów bezpieczeństwa zaworów procesowych.

Typowy system zarządzania LOTO obejmuje następujące elementy:

1. listę zaworów i/lub urządzeń, w których system jest zastosowany,
2. udokumentowaną pozycję dla każdego zaworu NC/NO (normal closed / normal open),
3. okresowe kontrole pozycji bezpiecznych poszczególnych zaworów i urządzeń zabezpieczonych,
4. okresowe, niezależne audyty na instalacji w celu potwierdzenia, że poszczególne zawory są w prawidłowych pozycjach,
5. okresowe audyty dokumentacji inspekcyjnej w celu zapewnienia, że rutynowe inspekcje są wykonywane zgodnie z wymogami organizacyjnymi.



Rys. 4a. System LOTO na zaworze odcinającym [https://www.lockout-tagout.com/product/cable-lockout/ - dostęp: 11.2024]



Rys. 4b. System car seal na zaworach odcinających w obrębie PSV [https://totallockout.blogspot.com/2012/11/what-does-car-seal-open-car-seal-closed.html - dostęp: 11.2024]

7. ZARZĄDZANIE ZMIANAMI

Zarządzanie zmianą (MOC - Management of Change) to formalny proces wykorzystywany do przeglądania, zatwierdzania i dokumentowania zmian: procedur, materiałów, procesów, sprzętu lub obiektów.

Modyfikacje procesu lub trybu działania, takie jak zmiany surowców, warunków przetwarzania lub sprzętu, mogą tworzyć nowe scenariusze awaryjne lub zmniejszać skuteczność istniejących IPL.

Zmiany procesu mogą być dobrowolne, np. w celu zwiększenia produktywności. Zmiany mogą być również wymuszone, np. przestarzały sprzęt może ulec awarii i zostać zastąpiony innym, ponieważ oryginalny model może być już niedostępny.

Wszystkie zmiany procesu, działania lub prowadzenia konserwacji należy oceniać, aby upewnić się, że:

- wcześniej zidentyfikowane scenariusze LOPA są nadal ważne,
- można zidentyfikować nowe scenariusze utworzone przez zmianę,
- istniejące warstwy zabezpieczeń spełniają cały czas wymagania IPL.



W przypadku IPL zmiana może obejmować wyłączenie sprzętu z eksploatacji (*by-pass*) w celu przeprowadzenia testów lub tymczasową pracę z uszkodzonym IPL. Zarządzanie przeglądami zmian z odpowiednimi uzgodnieniami zapewni, że wdrożone zostaną środki kompensacyjne, które zapewnią redukcję ryzyka równą tej zapewnianej przez uszkodzony IPL. Bez odpowiednich środków ostrożności i środków kompensacyjnych proces będzie w stanie wyższego ryzyka, niż oszacowała LOPA.

Każda zmiana procedury, harmonogramu, metody, komponentu, oprogramowania, materiału lub procesu powinna być kontrolowana.

Proces kontroli powinien obejmować:

- identyfikację zmiany i jej podstawy technicznej,
- przeprowadzanie przeglądów ryzyka i alternatywnego planowania kontroli ryzyka,
- zatwierdzenie zmiany,
- określenie ograniczeń dotyczących tymczasowych zmian i objęść (np. demontaż PSV w celu konserwacji),
- dokumentowanie zmian i przeglądów ryzyka,
- walidację jakości wdrożenia procedury zarządzania zmianą,
- aktualizowanie powiązanych dokumentów, takich jak procedury, zapisy, harmonogramy i listy części,
- szkolenie i przekazywanie zmian pracownikom,
- zapewnienie dostępności odpowiedniego i kompetentnego personelu do utrzymania IPL.

Krytycznie ważne jest, aby zmiany, które mogą mieć wpływ na częstotliwość IE lub PFD IPL, były starannie zarządzane w celu zapewnienia ciągłego bezpieczeństwa operacji.

PODSUMOWANIE

LOPA to półościowa metoda analizy oraz oceny ryzyka od 20 lat powszechnie stosowana w przemyśle chemicznym i petrochemicznym. Służy do określenia, czy istniejące warstwy zabezpieczeń, zwane w metodologii LOPA niezależnymi warstwami zabezpieczeń IPL, są wystarczające dla danego scenariusza awaryjnego, tzn. czy ryzyko wystąpienia skutków awarii jest na poziomie tolerowanym.

Zgodnie z metodologią LOPA tylko zabezpieczenia zakwalifikowane jako IPL wpływają na redukcję ryzyka.

Dlatego w celu przeprowadzenia oceny, czy dane zabezpieczenia kwalifikują się jako IPL, należy przeprowadzić ocenę, czy spełniają one wymagania podstawowe *core attributes*, tzn.: niezależność, funkcjonalność, nienaruszalność, niezawodność, audytowalność, bezpieczeństwo dostępu i zarządzanie zmianami.

Wymienione powyżej *core attributes* muszą zostać zweryfikowane, aby zakwalifikować zabezpieczenia jako IPL.

- Należy pamiętać, że każdy IPL jest zabezpieczeniem, ale nie każde zabezpieczenie można zakwalifikować jako IPL.
- Istotne jest, aby zespół LOPA szczegółowo przeanalizował każde zabezpieczenie w odniesieniu do podstawowych wymagań opisanych w tej części artykułu oraz zdecydował, które zabezpieczenia zostaną uznane za IPL i jaką wartość PFD można im przypisać.
- Możemy postawić śmiałą tezę, że kwalifikacja warstw zabezpieczeń jako IPL jest najistotniejszym procesem w LOPA. Prawdopodobieństwo tej oceny bezpośrednio wpływa na wyniki analizy, a zarazem na bezpieczeństwo instalacji procesowej.
- „Kredytowanie”, czyli przypisywanie redukcji ryzyka zabezpieczeniom, w stosunku do których powyższe wymagania nie są spełnione, jest poważnym błędem i podważa jej wyniki.

W następnej, a zarazem ostatniej części artykułu wskażemy najczęściej popełniane błędy w stosowaniu LOPA, odpowiemy na pytanie, czy organizacja jest przygotowana na zastosowanie metodologii LOPA, oraz przeanalizujemy wszystkie kroki analizy LOPA na podstawie przykładu.

Literatura:

1. CCPS. 2001. *Layer of Protection Analysis: Simplified Process Risk Assessment*. New York: AIChE.
2. CCPS. 2007. *Guidelines for Safe and Reliable Instrumented Protective Systems*. New York: AIChE.
3. CCPS. 2015. *Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis*. New York: AIChE.
4. Summers, A. 2014. *Safety Controls, Alarms, and Interlocks as IPLs*. „Process Safety Progress”, Vol. 33, No. 2, June 2014, p. 186-194.
5. William G. Bridges, Arthur M. Dowell III. 2016. *Identify SIF and Specify Necessary SIL, and Other IPLs, as Part of PHA/HAZOP – or – Why It is Not Necessary to “Boldly Go beyond HAZOP and LOPA”*. „Process Safety Progress”, Vol. 35, No. 4, December 2016, p. 349-359.
6. Arthur M. Dowell III. 2011. *Is It Really an Independent Protection Layer?* „Process Safety Progress”, Vol. 30, No. 2, June 2011, p. 126-131.
7. Edward M. Marszał, John Applegate. „Supporting LOPA with Fault Tree Analysis” *Chemical Engineering Progress*. February 2024, p. 23-34