PRZEOCZONE ZAGROŻENIE

Scenariusze Double Jeopardy w instalacjach wysokiego ryzyka

MGR INŻ. JACEK ŻACZYŃSKI

Kierownik Działu Technicznego
Oddział w Szczecinie
Urząd Dozoru Technicznego

Analizy zagrożeń procesowych PHA (ang. Process Hazard Analysis), takie jak np. HAZOP (Hazard and Operability Study) czy LOPA (Layer of Protection Analysis), to zespołowe, usystematyzowane metodologie, które skupiają się na identyfikowaniu zagrożeń, ocenie ryzyka i zarządzaniu nim.

Podczas wykonywania analiz zespoły skupiają się na identyfikacji wiarygodnych przyczyn, które mogą prowadzić do odchyleń w przebiegu procesu, a w konsekwencji — do zdarzeń niebezpiecznych o poważnych skutkach. Przyczyny te określane są powszechnie jako „zdarzenia inicjujące" (initiating events). Typy i przykłady takich zdarzeń to:

Typ zdarzenia inicjującego	Przykład zdarzenia inicjującego
Błąd ludzki	Błąd operacyjny – zawór przypadkowo pozostawiony w pozycji zamkniętej
Awaria urządzenia	Awaria układu regulacji ciśnienia powodująca otwarcie bądź zamknięcie zaworu regulacyjnego
Zdarzenie zewnętrzne	Pożar na instalacji

Na ich podstawie określa się potencjalne skutki wystąpienia awarii oraz identyfikuje się warstwy zabezpieczeń. Gdy liczba lub skuteczność istniejących zabezpieczeń jest niewystarczająca, formułuje się odpowiednie zalecenia w celu redukcji ryzyka do odpowiednio niskiego poziomu zwanego ryzykiem tolerowanym lub akceptowalnym.

W trakcie analiz niezwykle istotne jest, aby w sposób metodyczny zidentyfikować wszystkie wiarygodne zdarzenia inicjujące, tak aby zapewnić, że powstałe scenariusze zagrożeń zostaną odpowiednio ocenione.

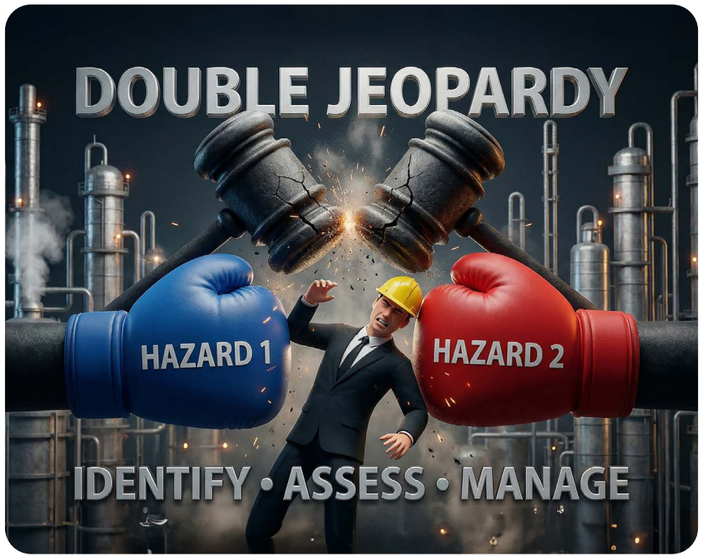
Trzeba jednak wyznaczyć granicę pomiędzy tym, co jest wiarygodnym zdarzeniem inicjującym, a tym, co nim nie jest.

W przypadku scenariuszy związanych z wielokrotnością awarii (gdy występują dwa lub więcej zdarzenia inicjujące jednocześnie, prowadząc do zdarzenia niebezpiecznego) można teoretycznie tworzyć wiele kombinacji awarii na podstawie zdarzeń zidentyfikowanych w PHA. W skrajnych przypadkach odpowiednie zabezpieczenie takich awarii mogłoby być niemożliwe do wykonania. W innych – zdarzenia o wysokim ryzyku mogłyby zostać pominięte.

Aby poradzić sobie ze złożonością takich analiz, stosuje się ogólnie przyjęte zasady, które ograniczają przegląd scenariuszy obejmujących jednoczesne awarie. Jedna z takich zasad nosi nazwę „double jeopardy".

- Czym jest „double jeopardy" i jak tę zasadę stosować podczas analiz postaramy się przedstawić poniżej.

Double jeopardy



„Nie musimy analizować tego scenariusza, bo to podwójna awaria."

„Nie ma możliwości, aby wszystkie te zdarzenia inicjujące wystąpiły jednocześnie."

„Czy to nie jest podwójne zagrożenie?"

**Ile razy słyszeliście takie stwierdzenia podczas analizy HAZOP?
Co zrobił wtedy zespół?
Czy zespół miał jasne rozumienie terminu „double jeopardy"?**

Termin „double jeopardy" ma swoje źródło w terminologii prawnej §

Pojawia się w Piątej Poprawce do Konstytucji Stanów Zjednoczonych [1]. W prawie odnosi się on do zakazu dwukrotnego sądzenia tej samej osoby za to samo przestępstwo — czyli „podwójnego narażenia na niebezpieczeństwo utraty życia lub zdrowia".

W bezpieczeństwie procesowym „double jeopardy" to powszechnie stosowany termin w analizach zagrożeń procesowych (PHA), który często bywa źle rozumiany i nadużywany. Zakwalifikowanie przyczyny w analizowanym scenariuszu awaryjnym jako „podwójnego zagrożenia" oznacza, że nie wymaga on dalszej analizy, ponieważ typowe metodyki PHA wyłączają takie przypadki z rozpatrywania.

„Podwójne zagrożenie" definiuje się jako równoczesne wystąpienie dwóch niezależnych zdarzeń inicjujących lub innych ujawnionych awarii.

Kluczowe jest zrozumienie, które wielokrotne awarie kwalifikują się jako „podwójne zagrożenie", a które nie — i dlatego powinny zostać uwzględnione w analizie PHA. Wielu uczestników analiz PHA zbyt pochopnie odrzuca zdarzenia inicjujące, które pozornie wpisują się w założenie „double jeopardy". Jeśli takie przyczyny zostaną błędnie pominięte, może to prowadzić do przeoczenia istotnych scenariuszy zagrożeń i pozostawienia ich bez odpowiednich zabezpieczeń.

Większość katastrof w instalacjach procesowych wynikała z wielu awarii — obejmowały one ukryte awarie lub wspólny mechanizm uszkodzenia. Dlatego tak ważne jest, aby przyczyny wielokrotnych awarii były dokładnie analizowane przed ich wykluczeniem, w celu zapewnienia, że wszystkie wiarygodne scenariusze zostaną zidentyfikowane.

Geneza

Na termin „double jeopardy" można się natknąć w artykułach związanych z bezpieczeństwem procesowym z lat 90., jeszcze przed oficjalnym pojawieniem się w przepisach i standardach. Dlatego nie można wskazać jednoznacznej „daty narodzin" terminu „double jeopardy" w kontekście bezpieczeństwa procesowego.

Czwarte wydanie wytycznych American Petroleum Institute (API) Recommended Practice (RP) 521: Guide for Pressure-Relieving and Depressuring Systems, opublikowane w 1997 roku, zawierało następujące sformułowanie w sekcji 2.2 [2]:

„Przyczyny nadciśnienia, w tym zewnętrzny pożar, uważa się za niezależne, jeśli między nimi nie występują powiązania procesowe, mechaniczne ani elektryczne, lub jeśli odstęp czasu między możliwymi kolejnymi wystąpieniami tych przyczyn jest wystarczający, aby uznać je za niepowiązane. Nie zakłada się jednoczesnego wystąpienia dwóch lub więcej warunków mogących spowodować nadciśnienie, jeśli przyczyny te są niezależne".

Nie padła tu jeszcze definicja „double Jeopardy" – ale zarysowała się pewna koncepcja, która później została rozszerzona i zaakceptowana do stosowania.

Rok 2003

W swojej książce skierowanej do prowadzących i uczestników PHA, **Guidelines for Process Hazards Analysis, Hazards Identification & Risk Analysis Nigel Hyatt** [3] użył po raz pierwszy stwierdzenia „Double jeopardy" w kontekście analiz zagrożeń i ryzyka:

„Prawdopodobieństwo, że dwa (lub więcej) niezależne zdarzenia lub incydenty wystąpią jednocześnie. (Ważne jest, aby zauważyć, że dwa lub więcej zdarzeń wynikających ze wspólnej przyczyny nie kwalifikuje się jako „double jeopardy").

Konkretne podwójne lub wielokrotne zagrożenia są często uważane za tak rzadkie, że ich rozważanie nie wymaga dalszej analizy. [Jednak należy zauważyć, że niespecyficzne wielokrotne zdarzenia zagrażające bezpieczeństwu wcale nie są rzadkie i często wiążą się z błędami ludzkimi w ramach wielu złożonych etapów. Ponieważ ich potencjalna liczba jest bardzo wysoka, mimo że prawdopodobieństwo wystąpienia konkretnego zdarzenia wielokrotnego zagrożenia jest niezwykle niskie, sprawia to, że zdarzenia niespecyficzne (bardzo trudne do przewidzenia) wielokrotnego zagrożenia są dość prawdopodobne]".

2014

Rok 2014 był przełomowy, gdyż dwie wpływowe organizacje – CCPS (Center of Chemical Process Safety) i API (American Petroleum Institute) – wprowadziły dodatkowe, jednoznaczne definicje pojęcia „Double Jeopardy".

Cytowany wcześniej fragment z 4 wydania API RP 521 występuje niemal dosłownie w sekcji 4.2.3 standardu API – API Standard 521: Pressure-relieving and Depressuring Systems (6. wydanie, 2014) [4]. Punkt 4.2.3 nosi tytuł „Double Jeopardy" i zawiera następujące sformułowanie:

„Przyczyny nadciśnienia uważa się za niezależne, jeśli między nimi nie występują powiązania procesowe, mechaniczne ani elektryczne lub jeśli odstęp czasu między możliwymi kolejnymi wystąpieniami tych przyczyn jest wystarczający, aby uznać je za niezależne. Jednoczesne wystąpienie dwóch lub więcej niezależnych przyczyn nadciśnienia (znane również jako podwójne lub wielokrotne zagrożenie) nie stanowi podstawy do projektowania… Standard ten opisuje scenariusze pojedynczego ryzyka, które powinny być brane pod uwagę przy projektowaniu urządzeń zrzutowych".

Dodatkowe wyjaśnienia znajdują się również w pkt. 4.2.4 tego samego standardu API:

„Awarię utajoną należy zwykle traktować jako istniejący warunek, a nie jako przyczynę powstania nadciśnienia podczas oceny, czy scenariusz stanowi pojedyncze czy podwójne zagrożenie."

Druga jednoznaczna definicja „double jeopardy" znajduje się w książce CCPS „Guidelines for Enabling Conditions and Conditional Modifiers in Layer of Protection Analysis" [1]:

„'Podwójne zagrożenie' można precyzyjniej zdefiniować jako jednoczesne wystąpienie dwóch niezależnych zdarzeń inicjujących lub innych ujawnionych awarii".

Zarówno projektowanie systemów ochrony przed nadciśnieniem, jak i analiza zagrożeń procesowych obejmują etap identyfikacji zagrożeń. W projektowaniu systemów ochrony przed nadciśnieniem konieczne jest zidentyfikowanie wiarygodnych scenariuszy nadciśnienia, natomiast w analizach PHA wymagane jest zdefiniowanie zdarzeń inicjujących (IE – Initiating events) przed przeprowadzeniem dalszej analizy. Obie te procedury powinny dojść do identycznego wniosku w kwestii tego, co jest wiarygodne, a co nie – w kontekście podwójnego zagrożenia.

Obecne różnice w podejściu prowadzą do niespójności w dokumentacji PHA i podstawach projektowych systemów ochrony przed nadciśnieniem. Może się zdarzyć, że zespół PHA zaleci wprowadzenie ochrony przed nadciśnieniem, podczas gdy podstawy projektowe systemu ochrony wg API 521 nie uwzględniają konkretnego scenariusza, ponieważ podwójne zagrożenie jest interpretowane w różny sposób.

Definicje przedstawione powyżej są podobne, ale nieidentyczne. Jasno widać, że „double jeopardy" ma swoje korzenie zarówno w doborze urządzeń zabezpieczających przed nadciśnieniem, jak i w analizie zagrożeń procesowych.

Często kierunek działania zespołu PHA jest zależny od doświadczenia członków zespołu. Jeśli inżynier procesowy posiada dużą wiedzę z zakresu analizy ochrony przed nadciśnieniem, „double jeopardy" jest rozpatrywane zgodnie z wytycznymi projektowymi wg API 521. Jeżeli posiada tylko wiedzę z zakresu zarządzania bezpieczeństwem procesowym to zapewnie jego wiedza w tym zakresie nie będzie odpowiednia.

Zasady „double jeopardy" nie są explicite omawiane w podstawowej książce CCPS „Guidelines for Hazard Evaluation Procedures", dotyczącej opisu dostępnych metod oceny zagrożeń, co stanowi obszar PSM, w którym nadal występują nieporozumienia i błędne stosowanie tego pojęcia. Staranna analiza elementów związanych z „double jeopardy" pozwoli czytelnikowi zrozumieć związane z nim komplikacje i stworzyć ramy do jego skutecznego stosowania. Skuteczne zastosowanie oznacza klarowność, spójność oraz zgodność z dobrą praktyką inżynierską.

W przemyśle procesowym istnieje wiele przypadków wielokrotnych awarii, które powinny mimo wszystko być rozważone i poddane dalszej analizie, aby zapewnić odpowiedni poziom kontroli ryzyka. Przed wykluczeniem z analizy przypadków „double jeopardy" należy uwzględnić kilka kluczowych czynników.

Niezależność zdarzeń inicjujących (IE)

Należy rozważyć, czy wszystkie zdarzenia inicjujące w potencjalnym scenariuszu awaryjnym są rzeczywiście niezależne, czy może mogą wystąpić w wyniku wspólnej przyczyny.

Przykładem może być awaria, która powoduje jednoczesne wyłączenie kilku układów, urządzeń lub systemów inżynieryjnych (np. utrata zasilania w media pomocnicze, np. powietrze sterujące czy awaria Podstawowego Systemu Sterowania Procesami, czyli BPCS ang. Basic Process Control System).

- Tryby powyższych przykładowych wspólnych awarii mogą być trudne do wykrycia, lecz należy traktować je jako wiarygodne scenariusze, ponieważ w przypadku jednoczesnego unieruchomienia wielu urządzeń nie można mówić o ich niezależności.
- Awarie niezależne oznaczają natomiast, że wystąpienie jednej awarii nie wpływa na prawdopodobieństwo wystąpienia drugiej – i odwrotnie.

Zgodnie z API 521, zdarzenia inicjujące są uznawane za niezależne, dopóki nie istnieją między nimi powiązania procesowe, mechaniczne ani elektryczne [2, 4]. Kryteria niezależności powinny również uwzględniać powiązania proceduralne.

Podczas analiz PHA powinny istnieć wytyczne dotyczące analizy niezależności zdarzeń inicjujących. Dokumentacja powinna obejmować zarówno proste przypadki niezależności, jak i bardziej złożone warunki, takie jak współlokalizacja, wspólne elementy konstrukcyjne, częściowa awaria zasilania, częściowa awaria sprężonego powietrza, awaria wspólnej karty I/O. Należy wybrać odpowiednią metodologię analizy, aby ocenić scenariusze zagrożeń związane ze złożonymi warunkami zależności pomiędzy wieloma zdarzeniami inicjującymi.

Dużym problemem jest też prawidłowa ocena niezależności między działaniami opartymi na procedurach.

- Na przykład błąd operatora przypadkowo zamykającego zawór ręczny oraz równoczesna awaria układu BPCS są zazwyczaj niezależnymi zdarzeniami inicjującymi.
- Z kolei błędy operatora, który nie otworzy kilku zaworów, mogą na pierwszy rzut oka wydawać się błędami niezależnymi, jednak zapoznanie się z odpowiednią procedurą może ujawnić, że wymaga ona otwarcia wszystkich zaworów w jednym kroku. W związku z tym pominięcie tego kroku przez niedoświadczonego operatora może skutkować nieprawidłową pozycją wielu zaworów, co nie spełnia warunku niezależności i stanowi jedno zdarzenie inicjujące (IE).

Widoczność zdarzenia inicjującego (utajone vs. ujawnione)

Po ustaleniu, czy wszystkie zdarzenia inicjujące są od siebie niezależne, kolejnym kryterium do oceny jest „widoczność".

W tym kontekście widoczność odnosi się do wykrywalności zdarzenia inicjującego. Zdarzenie inicjujące jest widoczne, jeśli zostało ogłoszone, wykryte lub ujawnione. To, czy pojedyncza awaria zostaje ujawniona lub wykryta wkrótce po jej wystąpieniu, czy też pozostaje nieujawniona przez pewien czas, ma kluczowe znaczenie przy określaniu, czy dany scenariusz wielokrotnej awarii można zakwalifikować jako przypadek „double jeopardy".

Jeżeli awaria pozostaje nieujawniona wystarczająco długo, by w tym czasie mogła wystąpić druga awaria, wówczas zasada „double jeopardy" nie ma zastosowania – a taki scenariusz należy uwzględnić w analizie PHA.

Nieujawnione awarie określa się zwykle mianem awarii utajonych (latent failures). Awarie te nie mają natychmiastowego wpływu na działanie systemu w chwili wystąpienia, w przeciwnym razie zostałyby zauważone.

PRZYKŁAD

Awaria zaworu regulacyjnego w pozycji otwartej, który ulega uszkodzeniu i blokuje się w pozycji otwartej to jeden z przykładów awarii nieujawnionej. Taka awaria nie zostanie wykryta, dopóki zawór nie będzie przywołany do zamknięcia na żądanie – co w zależności od warunków eksploatacji może nastąpić dopiero po kilku tygodniach, miesiącach lub latach. Tego rodzaju utajona awaria jako zdarzenie inicjujące, w połączeniu z innym niezależnym zdarzeniem inicjującym, może prowadzić do niebezpiecznego scenariusza awaryjnego.

- **Zespoły PHA powinny dążyć do zrozumienia widoczności każdego zdarzenia inicjującego.**

Analiza wielokrotnych awarii może być również uzasadniona w sytuacji, gdy **czas naprawy** ujawnionej awarii jest na tyle długi, że w tym czasie może dojść do drugiej awarii. Podczas określania czasu trwania awarii należy uwzględnić czas potrzebny na jej wykrycie, diagnozę i usunięcie. Długotrwałe działania naprawcze, w połączeniu z wystąpieniem innej niezależnej awarii, mogą doprowadzić do **wiarygodnego scenariusza wielokrotnej awarii**, który powinien być uwzględniony w analizie PHA.

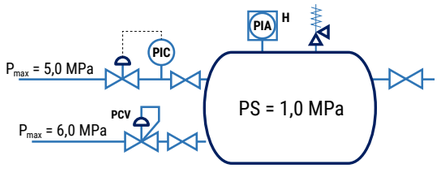
Oczywiście sam warunek **widoczności zdarzenia inicjującego** nie jest **wystarczający**, wymagane jest tutaj działanie, aby sprowadzić system do stanu bezpiecznego np. poprzez usunięcie awarii itp.

Dla pełnego zrozumienia, jak równoczesność awarii wraz z kryterium widoczności wpływają na prawdopodobieństwo, posłużymy się poniższym przykładem.

PRZYKŁAD

Zbiornik o ciśnieniu obliczeniowym PS = 1,0 MPa zasilany jest w sposób ciągły z dwóch źródeł zasilania o ciśnieniach, odpowiednio 6,0 MPa oraz 5,0 MPa. W trakcie normalnej pracy ciśnienia z obu źródeł są redukowane poprzez układ regulacji ciśnienia PIC – w przypadku pierwszego źródła oraz zawór redukcyjny PCV – dla drugiego źródła zasilania – do wartości roboczych około 0,8 MPa (rys. 1).

To, czy zastosowany zawór bezpieczeństwa PSV ma być dobrany na wielkość przepływu z uwzględnieniem jednego czy dwóch źródeł będzie zależało od wyniku analizy, czy jednoczesna awaria obu układów redukujących ciśnienie będzie kwalifikowała się jako „double jeopardy".

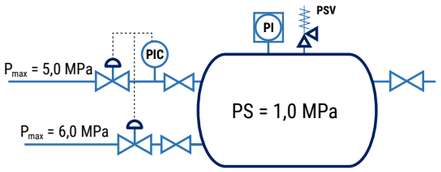


PSV - Ciśnieniowy zawór bezpieczeństwa (ang. Pressure Safety Valve)
PIC - Układ regulacji ciśnienia (ang. Pressure Indicator Controller)
PCV - Zawór regulacji ciśnienia / reduktor ciśnienia (ang. Pressure Control Valve)
PIA - Zdalne wskazanie wartości ciśnienia z alarmem od wysokiego poziomu (ang. Pressure Indicator and Alarm - High)
PS - Maksymalne dopuszczalne ciśnienie (ang. Maximum Allowable Pressure)

Rys. 1. Przykład zbiornika zasilanego w sposób ciągły z dwóch źródeł

Należy poddać ocenie niezależność obu układów. Już na pierwszy rzut oka widać, że awaria jednego układu nie będzie miała wpływu na poprawność działania drugiego.

Oznacza to, że ma tu zastosowanie kryterium **niezależności**. Co zatem z kryterium **widoczności zdarzenia inicjującego**?
W przypadku awarii jednego z układów redukcji ciśnienia (pełne otwarcie) należy spodziewać się wzrostu ciśnienia w zbiorniku (zbiornik wyposażony jest z zdalny pomiar ciśnienia z alarmem aktywowanym wzrostem wartości ciśnienia). W przypadku awarii układu redukującego ciśnienie i wzrostu ciśnienia w zbiorniku dojdzie do aktywacji alarmu, co pozwoli na podjęcie czynności przez operatora i np. odcięcie źródła zasilania w celu naprawy uszkodzonego układu.
W instalacji wystarczą czasami niewielkie zmiany, aby kryterium niezależności nie zostało spełnione. Jak na przykładzie poniżej.

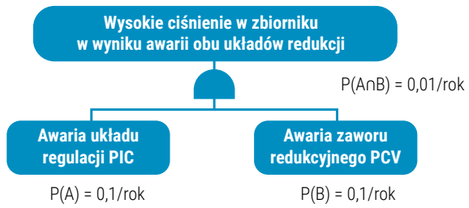


Rys. 2. Przykład zbiornika zasilanego w sposób ciągły z dwóch źródeł

Jak widzimy, mała zmiana sposobu sterowania procesem całkowicie zmienia scenariusz awaryjny. Teraz tylko pojedyncza awaria związana z uszkodzeniem układu regulacji ciśnienia PIC, powodująca pełne otwarcie zaworów regulacyjnych, spowoduje przepływ z obu źródeł zasilania. W takim przypadku zawór bezpieczeństwa na zbiorniku musi być dobrany z uwzględnieniem obu źródeł zasilania.

- Czy zatem spełnienie kryterium „niezależności" jest wystarczające?

Obliczmy prawdopodobieństwo wystąpienia obu awarii z uwzględnieniem kryterium „niezależności" jednej z awarii. Do obliczeń zastosujemy proste drzewo błędu FTA (ang. Fault Tree Analysis).

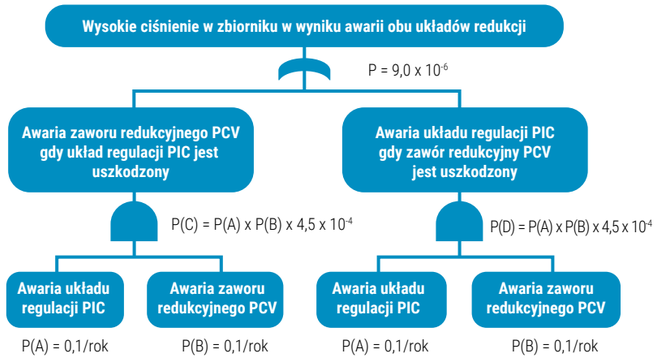


Przypadek A. Prawdopodobieństwo awarii układu PIC P(A) = 10^{-1}/rok
Przypadek B. Prawdopodobieństwo awarii zaworu PCV P(B) = 10^{-1}/rok
Prawdopodobieństwo wystąpienia obu awarii w tym samym czasie bez uwzględnienia kryterium „widoczności"
P(A∩B) = P(A) x P(B) = 10^{-1} x 10^{-1} = 10^{-2}/rok

Obliczone prawdopodobieństwo scenariusza awaryjnego, uwzględniające tylko kryterium „niezależności", nie jest wystarczająco niskie, aby go pominąć. Dlatego scenariusz obu awarii powinien być brany pod uwagę w analizach PHA, a zawór bezpieczeństwa na zbiorniku należy dobrać z uwzględnieniem obu źródeł zasilania.

Takie scenariusze awaryjne bez spełnienia obu kryteriów, tzn. „widoczności" i „niezależności" nie są zatem scenariuszami „double jeopardy" i nie powinny być odrzucane.

Poniżej prezentujemy obliczenia prawdopodobieństwa z uwzględnieniem obu kryteriów.



Przypadek A. Prawdopodobieństwo awarii układu PIC P(A) = 10-1/rok
Przypadek B. Prawdopodobieństwo awarii zaworu PCV P(B) = 10-1/rok
Czas potrzebny na przywrócenie układu regulacji PIC do stanu bezpiecznego = 4 godziny = 4/8760 = 4,5 x 10-4/rok
Czas potrzebny na przywrócenie zaworu redukcyjnego PCV do stanu bezpiecznego = 4 godziny = 4/8760 = 4,5 x 10-4/rok
Prawdopodobieństwo wystąpienia obu awarii w tym samym czasie z uwzględnieniem kryterium „widoczności":
P(CПD) = P(C) + P(B)
P(C) = P(AПBП4,5E-4) = 10-1 x 10-1 x 4,5 x 10-4 = 4,5 x 10-6/rok
P(D) = P(AПBП4,5E-4) = 10-1 x 10-1 x 4,5 x 10-4 = 4,5 x 10-6/rok
P(CПD) = P(C) + P(B) = 4,5 x 10-6 + 4,5 x 10-6 = 9,0 x 10-6/rok

Dopiero spełnienie obu warunków w obliczeniach prawdopodobieństwa wystąpienia obu awarii równocześnie daje argumenty – w postaci niskiej wartości – do odrzucenia takiego scenariusza.

Podstawą zakwalifikowania scenariusza jako „double jeopardy" jest zatem niskie prawdopodobieństwo wystąpienia scenariusza awaryjnego, co może mieć miejsce przy spełnieniu warunków „niezależności" oraz „widoczności".

Jest to również wystarczający argument do zaprojektowania zaworu bezpieczeństwa na pojedynczą awarię (do wymiarowania zaworu bezpieczeństwa należy wybrać przypadek o większym przepływie).

Zdarzenia współwystępujące

Po ustaleniu, czy wszystkie zdarzenia inicjujące są od siebie niezależne ORAZ, czy są to awarie utajone, kolejnym kryterium do oceny jest współwystępowanie. Terminy „równoczesne" (simultaneous) i „współwystępujące" (concurrent) nie oznaczają tego samego.

- „Równoczesne" często rozumiane jest jako rozpoczynające się i jednocześnie zachodzące w tym samym momencie i czasie. Stosując to dosłownie, bardzo niewiele zdarzeń inicjujących zachodzi równocześnie.
- Natomiast „współwystępujące" oznacza, że zdarzenia trwają w tym samym lub nachodzącym na siebie przedziale czasowym.

Choć podobne, te dwa pojęcia mają istotne różnice w kontekście definicji „double jeopardy". „Równoczesne" pozwala odrzucić zdarzenia inicjujące, które mogą współistnieć, co skutkuje odrzuceniem potencjalnie wiarygodnych scenariuszy zagrożeń. Uwzględniając zdarzenia współwystępujące, scenariusze zagrożeń mogą być wiarygodne, gdy jedno zdarzenie inicjujące wiąże się z warunkiem utajonym lub nienormalną pracą, a drugie zdarzenie powstaje w wyniku powrotu do normalnej pracy systemu.

Kryterium skumulowanego prawdopodobieństwa wystąpienia zdarzeń inicjujących

Aby ograniczyć liczbę scenariuszy ocenianych podczas analiz zagrożeń, zespoły powinny stosować kryteria pozwalające określić, które scenariusze są wiarygodne. W kontekście „double jeopardy" i ogólnej wiarygodności scenariuszy, wcześniej omówione kryteria tworzą niemal kompletny zestaw.

Ostatnim kryterium oceny i decyzji, czy nasze zdarzenie awaryjne należy rozpatrywać w trakcie analizy i czy może zostanie ono zakwalifikowane jako „double jeopardy", jest kryterium poziomu ryzyka analizowanego scenariusza.

Poziom ryzyka zależy od prawdopodobieństwa wystąpienia scenariusza awaryjnego i ciężkości skutków. W analizach zagrożeń i ryzyka zastosowanie warstw bezpieczeństwa w bardzo małym stopniu wpływa na ograniczenie ciężkości skutków. W przypadkach, kiedy ciężkość skutków jest możliwie najwyższa, poziom ryzyka zależy tylko od prawdopodobieństwa ich wystąpienia. Zasadnym zatem wydaje się zastosowanie skumulowanego prawdopodobieństwa zdarzeń inicjujących (SPZI) jako ostatniego kryterium.

Aby podczas analizy zagrożeń PHA scenariusz zasługiwał na analizę, poziom „SPZI" nie powinien być mniejszy od wstępnie ustalonej przez organizację dolnej wartości i powinien stanowić sumę wszystkich zdarzeń inicjujących. Podobnie jak w przypadku kryterium widoczności, grupę zależnych zdarzeń inicjujących należy traktować jako jedno zdarzenie przy obliczaniu skumulowanego prawdopodobieństwa.

W literaturze kryterium oparte o poziom ryzyka nie jest szeroko omawiane i rozpowszechnione. Można znaleźć szczątkowe informacje o konieczności analizy scenariuszy kwalifikujących się jako „double jeopardy" ze względu na wysoki poziom ryzyka analizowanego scenariusza.

Niemniej jednak ostateczna decyzja co do stosowania tego kryterium należy do właściciela instalacji, który powinien posiadać odpowiednie procedury związane z zarządzaniem bezpieczeństwem procesowym i świadomie podejmować decyzję w tym zakresie.

W przypadku scenariuszy o skrajnie wysokich konsekwencjach właściciel instalacji może zdecydować się na pełną ocenę scenariusza, pomimo bardzo niskiego SPZI.

Również w przypadku scenariuszy o skrajnie wysokich konsekwencjach, które SĄ uznawane za „double jeopardy", firma nadal może zdecydować się na pełną ocenę scenariusza.

Widzimy zatem, że należy zachować szczególną ostrożność przy określaniu, czy dwa lub więcej zdarzeń inicjujących można uznać za przypadek „double jeopardy". Pomimo wprowadzenia jednoznacznych definicji przez CCPS i API cały czas brak jest jasnego, spójnego podejścia w stosowaniu zasad „double jeopardy". Prowadzi to finalnie do niespójności w różnych analizach zagrożeń PHA oraz analizach na potrzeby doboru urządzeń zabezpieczających przed nadciśnieniem wg API 521. W drugiej części artykułu podamy przykłady które zdarzenia nie są uznawane, a które można zakwalifikować jako „double jeopardy".

Literatura:

1. CCPS. Guidelines for Enabling Conditions and Conditional Modifiers in Layer of Protection Analysis, New York, AICHE, 2014.
2. American Petroleum Institute, API RP 521: Guide for Pressure-Relieving and Depressuring Systems, 4th Edition, API Publishing Services, Washington, D.C., 1997.
3. Hyatt N., Guidelines for Process Hazards Analysis, Hazards Identification & Risk Analysis, 1st Edition, Dyadem Press, Ontario, Canada, 2003.
4. American Petroleum Institute, API Standard 521: Pressure-relieving and Depressuring Systems, 6th Edition, API Publishing Services, Washington, D.C., 2014.
5. Baybutt P., Treatment of Multiple Failures in Process Hazard Analysis, Process Safety Progress, 2013, 32(4): p. 361-364.