

PROWADZENIE ANALIZ I OCENA RYZYKA INSTALACJI PROCESOWYCH



MGR INŻ. JACEK ŻACZYŃSKI

Ekspert Urzędzeń Ciśnieniowych
Kierownik Działu Technicznego
Oddział w Szczecinie
Urząd Dozoru Technicznego



PROCES PROJEKTOWANIA ORAZ EKSPLOATACJI INSTALACJI PROCESOWYCH, ZWŁASZCZA DLA POTRZEB PRZEMYSŁU CHEMICZNEGO, NAFTOWO-GAZOWEGO CZY PETROCHEMICZNEGO, NIESIE ZA SOBĄ NIEODŁĄCZNE RYZYKO ZWIĄZANE Z PRZETWARZANIEM MATERIAŁÓW NIEBEZPIECZNYCH (PALNYCH, WYBUCHOWYCH, TOKSYCZNYCH). Z TEGO WZGLĘDU WSZYSCY INŻYNIEROWIE MAJĄ OBOWIĄZEK DOŁOŻYĆ WSZELKICH STARAŃ, ABY ZAPEWNIĆ, ŻE PROJEKT INSTALACJI PROCESOWEJ ORAZ JEJ OBSŁUGA SĄ POD ICH KONTROLĄ I SĄ TAK BEZPIECZNE, JAK TO TYLKO MOŻLIWE. JEST TO NIE TYLKO OBOWIĄZEK PRAWNY, ALE PRZEDĘ WSZYSTKIM MORALNY.

Obowiązki w zakresie zapewnienia bezpieczeństwa mają szeroki zasięg i można je podzielić na kilka obszarów.

1. Zapobieganie śmierci lub obrażeniom pracowników
2. Zapobieganie śmierci lub obrażeniom ogółu społeczeństwa
3. Zapobieganie uszkodzeniom instalacji oraz stratom finansowym
4. Zapobieganie szkodom w mieniu osób trzecich
5. Zapobieganie szkodom dla środowiska

Chociaż zapobieganie śmierci i obrażeniom ludzi jest najważniejsze, nie można traktować tej listy jako ogólnego wskazania kolejności priorytetów. Wielu ludzi dzisiaj przedkładałoby ochronę środowiska nad zyski finansowe. Termin *loss prevention* jest czasami używany do określenia powyższych pięciu obszarów, ale również szeroko pojętych strat ekonomicznych, takich jak utrata udziału w rynku oraz utrata reputacji, które mogą wynikać z wypadków i innych niepożądanych zdarzeń.

SZEROKIE KRĘGI BEZPIECZEŃSTWA

W większości branż najpoważniejszą troską pracodawców jest zapewnienie bezpieczeństwa pracowników. Najczęściej skupiają się oni na ochronie poprzez zastosowanie odpowiednich osłon maszyn, ostrzeżeń o ruchomym obciążeniu czy też niezbędnej ochronie przeciwporażeniowej. Wypadki, które zdarzają się pracownikom z powodu braku tego typu zabezpieczeń, bardzo rzadko mają wpływ na innych pracowników lub ogół społeczeństwa.

Jeśli dojdzie do wypadku w przemyśle przetwórczym, może to skutkować uwolnieniem toksycznych materia-

łów lub dużych ilości energii, co ma katastrofalne skutki dla wszystkich pracowników i osób trzecich. Szkodliwe emisje z zakładów chemicznych czy petrochemicznych mogą przedostać się daleko poza obszar zakładu i powodować skutki zarówno krótko-, jak i długoterminowe. Problemy spowodowane przez duże katastrofy przemysłowe, takie jak zdarzyły się w Flixborough, Seveso czy Bhopal, mają wymiar indywidualny, ale przede wszystkim społeczny. Należy jednak pamiętać, że nawet w branżach przetwórczych, w których przetwarzane są bardzo niebezpieczne materiały, większość wypadków nie ma związku z procesem.



Rys. 1. Widok katastrofy w zakładach chemicznych Nypro w Flixborough 1.06.1974 r. (źródło <https://www.lincolnshirelive.co.uk/>)

Wiele można zrobić, aby zapewnić bezpieczeństwo, kierując się przede wszystkim zdrowym rozsądkiem i podstawowymi umiejętnościami inżynierskimi. Jednak w miarę jak procesy stają się bardziej skomplikowane (i niebezpieczne), problem zapewnienia bezpiecznej eksploatacji jest coraz bardziej złożony. Wymaga to zastosowania specjalistycznych metod w celu zapewnienia odpowiedniego poziomu bezpieczeństwa instalacji procesowych, tzn. analiz zagrożeń i ryzyka.

ZARZĄDZANIE BEZPIECZEŃSTWEM PROCESOWYM

Na zdolność zapewnienia bezpieczeństwa procesowego w obiekcie wpływa wiele czynników. Można tu wymienić np. zastosowanie odpowiedniej technologii na etapie projektowania i budowy, przewidywanie skutków oddziaływania czynników zewnętrznych, zrozumienie ludzkich błędów i radzenie sobie z nimi oraz wprowadzenie skutecznych systemów zarządzania

BEZPIECZEŃSTWO PROCESOWE – GENEZA

Seria katastrof chemicznych, które miały miejsce w latach 70., 80. i na początku lat 90. XX w., m.in. katastrofa związana z największym wyciekiem dioksynu (2,3,7,8-tetrachlorodibenzodioxyny, czyli TCDD) do atmosfery w Seveso w północnych Włoszech w 1976 r. lub wyciek 40 ton gazowego izocyjanianu metylu w Bhopalu w Indiach w 1984 r., przyczyniła się do rozwoju dziedziny znanej dzisiaj jako bezpieczeństwo procesowe.

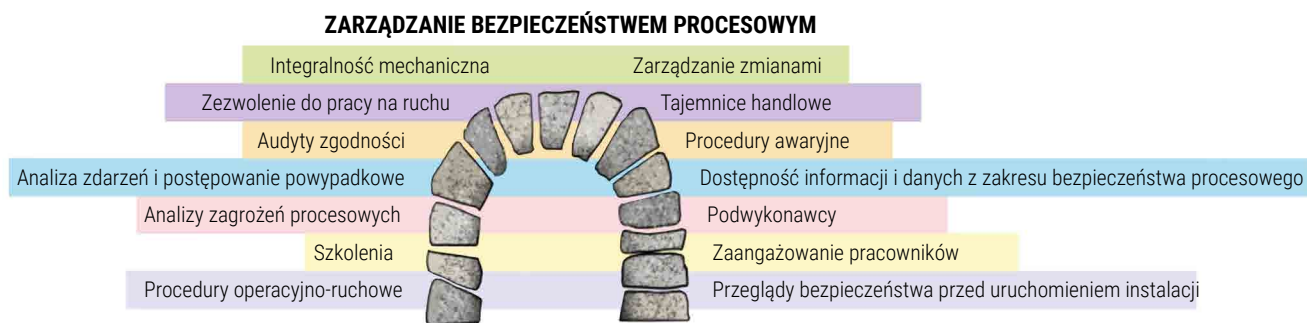
W wyniku awarii w Seveso ewakuowano 730 osób, około 700 mieszkańców zostało poszkodowanych w wyniku zatrucia, wiele zwierząt zginęło, tereny licznych w tym regionie przedsiębiorstw zostały skażone (ok. 40 zakładów), a wielkie obszary na wiele lat (ok. 10) z powodu skażenia wyłączono z gospodarki rolnej. Straty materialne oszacowano na kwotę 72 mln ECU.

Katastrofa w Bhopalu była jedną z najtragiczniejszych chemicznych katastrof przemysłowych. Jej skutki do dzisiaj nie są jednoznacznie ocenione, jedne źródła podają około 4000 ofiar śmiertelnych oraz 100 tys. osób z ciężkimi przypadkami utraty zdrowia, inne źródła mówią o 16 tys. ofiar oraz około 550 tys. osób z ciężkimi urazami.

Wspomniane katastrofy przyczyniły się do rozwoju dziedziny określanej obecnie jako bezpieczeństwo procesowe. Wydarzenia te spowodowały wprowadzenie przepisów regulujących zarządzanie bezpieczeństwem procesowym w zakładach, gdzie istnieje ryzyko poważnych awarii związanych z magazynowaniem i przetwarzaniem substancji niebezpiecznych.

W Europie wprowadzono dyrektywę SEVESO, a w USA rozporządzenie PSM (The Process Safety Management). Obecnie obowiązuje już trzecie wydanie dyrektywy SEVESO, która w Polsce została wprowadzona ustawą o ochronie środowiska. Oprócz regulacji wynikających z ustawy, w przemyśle procesowym szeroko stosowane są zagadnienia związane z PSM.

Podstawowym celem PSM jest zapobieganie lub minimalizowanie skutków uwolnień wysoce niebezpiecznych chemikaliów, które mogłyby narazić ludzi na poważne obrażenia ciała lub utratę życia. Aby osiągnąć ten cel, standard wymaga **SKUTECZNEGO WDROŻENIA PROGRAMU PSM**, który stanowi systematyczne podejście do proaktywnego przeglądu procesów chemicznych w celu identyfikacji i oceny potencjalnych zagrożeń oraz zapobiegania i łagodzenia skutków uwolnień substancji chemicznych. Program PSM obejmuje 14 elementów (rys. 2).



Rys. 2. Elementy programu PSM (źródło: www.creativesafetysupply.com/glossary/psm)

ZARZĄDZANIE BEZPIECZEŃSTWEM PROCESOWYM
1. Zaangażowanie pracowników (Employee Involvement)
2. Dostępność informacji i danych z zakresu bezpieczeństwa procesowego (Process Safety Information)
3. Analizy zagrożeń procesowych (Process Hazard Analysis)
4. Procedury operacyjno-ruchowe (Operating Procedures)
5. Szkolenia (Training)
6. Podwykonawcy (Contractors)
7. Przeglądy bezpieczeństwa przed uruchomieniem instalacji (Pre-Startup Safety Review)
8. Integralność mechaniczna (Mechanical Integrity)
9. Zezwolenie do pracy na ruchu (Hot Work Permit)
10. Zarządzanie zmianami (Management of Change)
11. Analiza zdarzeń i postępowanie powypadkowe (Incident Investigation)
12. Procedury awaryjne (Emergency Preparedness and Response)
13. Audyty zgodności (Compliance Audits)
14. Tajemnice handlowe (Trade Secrets)

Zgodność ze standardem PSM stanowi wyzwanie nawet dla najbardziej doświadczonych operatorów ze względu na szeroki zakres i wysoce techniczny charakter.

Jednym filarów skutecznego systemu zarządzania bezpieczeństwem procesowym jest odpowiedni program identyfikacji zagrożeń i analizy ryzyka. Zakłada on, że osiągnięcie bezpieczeństwa na odpowiednim akceptowalnym poziomie wymaga zastosowania wielu różnych analiz zależnych od:

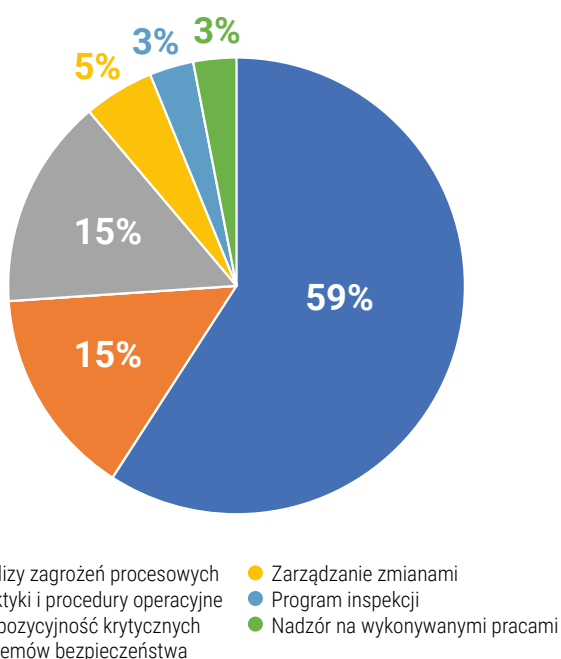
1. rodzaju koniecznych do uzyskania wyników,
2. rodzaju dostępnych informacji (dostępność oraz jakość dokumentacji),
3. zasobów przeznaczonych na ten cel.

ROLA ANALIZY ZAGROZEŃ I RYZYKA

W instalacjach procesowych (chemicznych, petrochemicznych itp.) zasadniczy wpływ na ogólny poziom bezpieczeństwa ma poprawność wykonania analiz zagrożeń oraz ryzyka. Przede wszystkim decyduje to o późniejszej bezpiecznej eksploatacji urządzeń technicznych. Optymalizuje również koszty inwestycyjne związane z koniecznością dokonywania zmian w końcowej fazie projektu, co jest z reguły trudne i bardzo kosztowne.

W dalszej części artykułu postaramy się wskazać, jak wybrane błędy wpływają na jakość analiz, a tym samym mogą powodować poczucie fałszywego bezpieczeństwa. Należy pamiętać, że akceptacja niedoszacowanego ryzyka w sposób bezpośredni obniża bezpieczeństwo eksploatacyjne. Bardzo często spotykamy się z sytuacjami, w których rezygnuje się ze stosowania zabezpieczeń rozumianych jako szeroko akceptowalna dobra praktyka inżynierska, uzasadniając to osiągnięciem kryteriów akceptacji ryzyka.

Jak bardzo wpływa na całkowite bezpieczeństwo obiektu prawidłowo dobrana i wykonana analiza zagrożeń i ryzyka, możemy przekonać się na podstawie analizy wykonanej na potrzeby rynku ubezpieczeniowego [8].



Rys. 3. Wtórne błędy w zarządzaniu bezpieczeństwem procesowym dla wypadków (uwolnień mediów) wynikających z niemechanicznej utraty integralności [8]

Na potrzeby tego badania [8] przeanalizowano 100 najpoważniejszych wypadków w przemyśle związanym z wydobywaniem i przetwórstwem ropy, gazu i produktów petrochemicznych w okresie 20 lat – od 1996 do 2015 r. Uwzględniono jedynie straty spowodowane przez ogień i eksplozję (wykluczono zdarzenia związane z katastrofami naturalnymi).

Analiza incydentów wykazała, że więcej niż jedno na pięć zdarzeń związanych z uwolnieniem wynikało z nieuwzględnienia przez organizację w pełni potencjalnych zagrożeń lub przyczyn awarii komponentu. Zdecydowana większość wypadków nastąpiła w wyniku nieodpowiedniego zaplanowania i wdrożenia przez organizację procedur kontroli ryzyka.

Co więcej, należy podkreślić, że wśród 57 największych awarii związanych z uwolnieniami, które zostały spowodowane przez niemechaniczne utraty integralności, w aż 33 przypadkach stwierdzono błędy w przeprowadzonych analizach zagrożeń i ryzyka.

Jest to zaskakujące, biorąc pod uwagę, że badania HAZOP i inne powiązane metody, jak LOPA, to ugruntowane i dobrze opisane metodologie, które zostały zaadaptowane i są powszechnie wykonywane na całym świecie.

BŁĘDY W PRZEPROWADZONYCH ANALIZACH ZAGROZEŃ I RYZYKA

Przedstawiamy wybrane błędy wpływające na końcową jakość analizy zagrożeń i ryzyka:

1. Błędny dobór metody
2. Błędne wykonanie analizy – łamanie podstawowych zasad
3. Błędne określenie skutków
4. Błędny dobór warstw zabezpieczeń

1. Błędny dobór metody

Każda technika PHA (Process Hazard Analysis), tj. Analiza Zagrożeń, ma swoje unikalne mocne i słabe strony. Zrozumienie tych atrybutów jest warunkiem wstępnym wyboru odpowiedniej techniki oceny zagrożenia. Poniżej wymieniono sześć kategorii czynników, które analitycy powinni wziąć pod uwagę przy wyborze techniki oceny zagrożenia dla konkretnego zastosowania. Znaczenie każdej z tych kategorii w procesie selekcji może się różnić w zależności od firmy i branży, jednak powinny się sprawdzić w niemal każdej sytuacji.

Czynniki wykorzystywane do wyboru techniki PHA:

- powody przeprowadzenia analizy
- wymagany rodzaj wyników
- dostępność informacji technicznych
- charakterystyka analizowanego problemu
- rodzaj postrzeganego ryzyka związanego z danym procesem
- dostępność zasobów oraz preferencje kierownictwa

PRZYKŁADY STOSOWANIA WW. KRYTERIÓW

Pierwsze kryterium wyboru metody powinno odnosić się weryfikacji etapu cyklu życia procesu.

Etap ten wyznacza praktyczny limit szczegółowych informacji dostępnych dla zespołu wykonującego analizę. Na przykład, jeśli w koncepcyjnej fazie projektu procesu ma zostać przeprowadzona ocena zagrożeń, jest bardzo mało prawdopodobne, że organizacja opracowała już szczegółowe schematy technologiczne (P&ID) dla proponowanego procesu. Tak więc jeśli analityk musi wybierać pomiędzy HAZOP a analizą typu What-If, czynnik fazy życia dyktowałby zastosowanie metody analizy typu What-If, ponieważ nie ma wystarczających informacji, aby przeprowadzić w sposób prawidłowy analizę HAZOP. Ostatecznie, jeśli analitycy uważają, że z powodu braku odpowiednich informacji oraz dokumentów cele badania nie mogą zostać osiągnięte przy użyciu odpowiedniej techniki oceny zagrożeń, powinni albo zaproponować zmianę metody analizy, albo odroczyć wykonanie analizy do czasu uzyskania wystarczających informacji.

Istotne informacje dotyczące bezpieczeństwa procesu:

- Opis procesu
- Schematy technologiczne P&ID
- Schematy przepływowe PFD
- Plany obiektu, rzuty rozmieszczenia poszczególnych jednostek
- Informacje dotyczące sterowania, alarmów oraz blokad procesowych
- Informacje dotyczące układów zrzutowych (zawory bezpieczeństwa, pochodnia itp.)
- Procedury ruchowe
- Wcześniejsze analizy PHA
- Informacje o zmianach w instalacji od poprzednich analiz PHA
- Raporty powypadkowe

Rys. 4. Zakres dokumentacji na potrzeby analizy HAZOP – podstawowe informacje na potrzeby analiz zagrożeń i ryzyka [7]

Niestety częstą praktyką jest wykonywanie analiz HAZOP na każdym etapie cyklu życia, nawet w fazie projektu koncepcyjnego. Tymczasem bez wymaganego kompletu dokumentacji PSI (Process Safety Information) czy też finalnych wersji P&ID wyniki takich analiz zazwyczaj zawierają wiele błędów. Kończy się to najczęściej koniecznością ponownego wykonania HAZOP po uzyskaniu niezbędnej dokumentacji.

Drugi warunek dotyczy jakości i aktualności istniejącej dokumentacji.

W celu oceny zagrożeń związanych z istniejącym procesem analitycy zagrożeń mogą stwierdzić, że P&ID nie są aktualne lub mają nieodpowiednią formę. Używanie jakiegokolwiek techniki oceny zagrożeń opartej na nieaktualnych informacjach o procesie jest nie tylko daremne, ale także powoduje stratę czasu i zasobów (jest także niebezpieczne, ponieważ wyniki mogą zostać fałszywie uznane za prawidłowe). Tak więc, jeśli wszystkie inne czynniki wskazują na zastosowanie techniki (np. techniki analizy HAZOP) do proponowanej oceny zagrożenia, która wymaga takich informacji, analitycy powinni poprosić kierownictwo o przekazanie m.in. niezbędnych aktualnych schematów P&ID i procedur operacyjnych.

Trzeci warunek to rodzaj (tryb) pracy instalacji.

To kryterium wyboru metody uwzględnia rodzaje pracy: praca ciągła (*continuous process*), praca okresowa związana z szarżą reaktorów (*batch process*), rozruch, zatrzymanie lub zatrzymanie awaryjne itp.

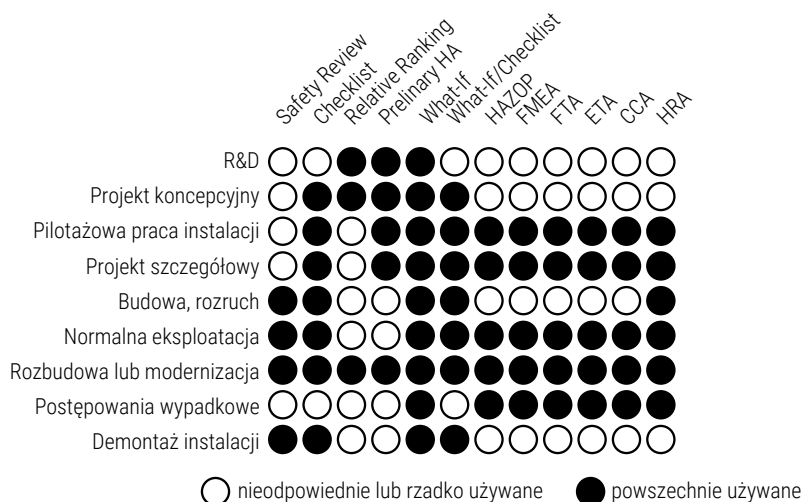
Do pierwszego trybu pracy odpowiednią metodą wydaje się tradycyjny HAZOP, a w przypadku pracy okresowej tzw. Batch-HAZOP. Podczas prac związanych z korzystaniem z odpowiednich procedur, np. podczas rozruchu, tradycyjny HAZOP nie sprawdzi się, należały w tym przypadku zastosować HAZOP proceduralny.

Czwarty warunek to rodzaj potrzebnych do uzyskania wyników.

Zdefiniowanie konkretnego rodzaju informacji potrzebnych do osiągnięcia celu oceny zagrożenia jest ważną częścią wyboru najodpowiedniejszej techniki oceny zagrożenia. Wybrana technika powinna więc być najskuteczniejszym sposobem dostarczenia informacji wymaganych do spełnienia przesłanek badania. Na przykład jeżeli chcemy określić, w jakiej lokalizacji powinny być umiejscowione budynki administracyjne, wykonując analizę HAZOP, nie otrzymamy spodziewanych wyników. W takiej sytuacji należałoby zastosować np. QRA.

PIĘĆ KATEGORII INFORMACJI, KTÓRE MOŻNA UZYSKAĆ NA PODSTAWIE OCENY ZAGROŻEŃ

- lista zagrożeń
- lista sytuacji awaryjnych
- lista alternatyw pozwalających zmniejszyć ryzyko lub obszary wymagające dalszych badań
- priorytetyzacja wyników
- dane wejściowe do ilościowej analizy ryzyka



Rys. 5. Typowe zastosowania metod oceny zagrożeń – metody analizy zagrożeń w cyklu życia instalacji procesowej [1]

2. Błędne wykonanie analizy – naruszenie bądź niespełnienie podstawowych zasad przyjętej metody analizy

Niektóre metodologie PHA są bardziej rygorystyczne niż inne. Do bardziej rygorystycznych zalicza się metodologie badania LOPA, HAZOP i FMEA. Mniej rygorystyczne metodologie PHA obejmują metodologie What-If, Check List i What-If/Check List. Stosując rygorystyczne metodologie PHA, rzadko ignoruje się potencjalne zdarzenia inicjujące i zakłócenia, które mogą prowadzić do poważnych skutków. Natomiast idąc na skróty i pomijając bardziej rygorystyczne elementy metody, dewaluuje się ich wartość.

Przykładem jest przeprowadzanie analizy LOPA bez spełniania zasadniczych wymagań **Core Attributes** stawianych zabezpieczeniom traktowanym jako **IPL** (Independent Protection Layer).

Niezależność

Ta najważniejsza zasada jest często łamana. Na przykład, aby w LOPA można było wykorzystywać w danym scenariuszu dwie pętle podstawowego systemu kontroli procesu (BPCS), jedną jako zdarzenie inicjujące, a drugą jako IPL, należy sprawdzić, czy obie pętle BPCS są od siebie niezależne. Oznacza to, że aby drugą pętlę BPCS można było uznać za IPL, musi być niezależna od pierwszej. Z wyjątkiem płyty głównej wszystkie następne elementy muszą być niezależne, tj. niezależne przetworniki, niezależne karty wejściowe, niezależne karty procesora, niezależne karty wyjściowe i niezależne elementy wykonawcze. Bez przeprowadzenia dowodu niezależności zabezpieczenie nie może być IPL.

Audytywalność

Jest to pięta achillesowa metody LOPA i najczęściej pojawiający się błąd w analizach. Proces audytu musi potwierdzić, że IPL skutecznie zapobiega konsekwencjom, jeśli działa zgodnie z przeznaczeniem oraz spełnia wszystkie wymagania **Core Attributes**. Audyt powinien także potwierdzić, że istnieją systemy projektowania IPL, instalacji, testów funkcjonalnych i konserwacji umożliwiające osiągnięcie określonego PFD dla IPL. Testy funkcjonalne muszą potwierdzić, że wszystkie komponenty IPL (czujniki, moduł logiczny, elementy wykonawcze itp.) działają i spełniają wymagania, aby mogły być **IPL**.

Podczas analizy zespół musi potwierdzić, że zabezpieczenie jest IPL – tylko pod takim warunkiem można obniżyć ryzyko. Jeżeli podczas analizy np. zawór bezpieczeństwa jest rozpatrywany jako **IPL**, dokumentacja musi zawierać:

- podstawę konstrukcyjną (wymiarową),
- scenariusze projektowe (wszystkie scenariusze wymagające otwarcia zaworu),
- specyfikację zaworu,
- wymagany przepływ w warunkach scenariusza awaryjnego,
- szczegóły instalacji (np. rozmieszczenie rur),
- procedury testowe i konserwacyjne, w tym potwierdzenie ciśnienia nastawy zaworu oraz prawidłowości działania.

3. Błędne określenie skutków – niedoszacowanie albo przeszacowanie potencjalnych skutków

Oszacowanie skutków dla każdego scenariusza awaryjnego przeprowadza się na wiele różnych sposobów, począwszy od jakościowej oceny zespołowej, po w pełni ilościową analizę konsekwencji przy użyciu numerycznych metod. Często przyjmuje się podejście pośrednie, przy czym zespół oceniający ryzyko dokonuje określenia skutków, jeśli to możliwe, wykorzystując zbiorową wiedzę i doświadczenie członków zespołu, ewentualnie uzupełnioną wynikami z wcześniejszych analiz, np. analiz HAZID. Jeżeli zespół nie jest w stanie dokonać oszacowania, może zalecić przeprowadzenie szczegółowej analizy konsekwencji dla zidentyfikowanego scenariusza. Zdarza się jednak, że zespół bez ugruntowanej wiedzy w tym zakresie sam dokonuje powyższej oceny.

Można wyróżnić dwa rodzaje błędnego oszacowania – zbyt pesymistyczne podejście oraz niedoszacowanie skutków.

Zbyt pesymistyczne podejście

W przypadku scenariuszy awaryjnych związanych z przekroczeniem ciśnienia obliczeniowego zespoły stwierdzają, że konsekwencją tego będzie katastrofalne rozerwanie, jeśli ciśnienie przekroczy wartość obliczeniową zbiornika bez względu na jego wielkość. Natomiast prawidłowe zadziałanie zaworu bezpieczeństwa dopuszcza wzrost ciśnienia w zbiorniku do 110% PS (ciśnienia obliczeniowego). Dla zaworów bezpieczeństwa na scenariusz pożaru bardzo często przyjmuje się wartość 121% PS jako dopuszczalny chwilowy wzrost ciśnienia w zbiorniku. Przy takich przekroczeniach definiowanie skutków jako katastrofalne rozerwanie zbiornika jest zbyt pesymistyczne.

TABELA 1. ORIENTACYJNE WARTOŚCI NADCIŚNIENIA ORAZ ICH POTENCJALNE KONSEKWENCJE DLA ZBIORNIKA CIŚNIENIOWEGO

Przyrost ciśnienia (% powyżej MAWP)	Znaczenie	Potencjalne skutki nadciśnienia	UWAGA Jeżeli zbiornik nie był odpowiednio kontrolowany, konserwowany, a jego stan techniczny jest nieznany, wówczas nie powinniśmy stosować wymienionych założeń (tabela).
10%	Dopuszczalny przyrost ciśnienia w zbiorniku w przypadku pojedynczego zaworu bezpieczeństwa	Nie przewiduje się żadnych poważnych skutków przy tej wartości nadciśnienia	
16%	Dopuszczalny przyrost ciśnienia w zbiorniku w sytuacji zastosowania kilku zaworów bezpieczeństwa	Nie przewiduje się żadnych poważnych skutków przy tej wartości nadciśnienia	
21%	Dopuszczalny przyrost ciśnienia w zbiorniku dla scenariusza „pożaru”	Nie przewiduje się żadnych poważnych skutków przy tej wartości nadciśnienia	
>21% do 30%	Typowa wartość nadciśnienia stosowana przy hydrostatycznej próbie ciśnieniowej	Wzrost prawdopodobieństwa nieszczelności na połączeniach kołnierzo-śrubowych	
>30%	Minimalna granica plastyczności, a tym samym ostateczna wytrzymałość zbiornika różnią się w zależności od rodzaju i gatunku materiału	Katastrofalna awaria staje się coraz bardziej prawdopodobna. Ponieważ ten poziom nadciśnienia wykracza poza dopuszczalne normy, konieczna będzie analiza uzupełniająca przeprowadzona przez organizację, aby ocenić powagę konsekwencji nadciśnienia.	

Tabela nie może stanowić podstawy do rezygnacji z odpowiednich zabezpieczeń na wypadek przekroczenia ciśnienia obliczeniowego.

Przykład dotyczy zbiorników wykonanych ze stali węglowej zgodnie z przepisami ASME (BPVC), Section VIII, Division 1 (2013); w przypadku innych przepisów projektowych oraz innych materiałów konsekwencje w stosunku do % akumulacji ciśnienia mogą być poważniejsze [3].

Niedoszacowanie skutków

Zdarzają się przypadki, w których skutki, a tym samym ryzyko zostało niedoszacowane ze względu na przewidywanie, że konsekwencje będą mniej poważne, niż byłyby. Przykładem ilustrującym taką sytuację jest incydent w Buncefield w Wielkiej Brytanii w 2005 r.

EKSPLOZJA ZBIORNIKÓW W SKŁADZIE PALIW BUNCEFIELD POD LONDYNEM

Przepełnienie jednego ze zbiorników benzyny spowodowało serię eksplozji, które wywołały ogromny pożar obejmujący 20 dużych zbiorników magazynowych (największy pożar w Wielkiej Brytanii od czasu II wojny światowej). Pożar trwał 5 dni. Nikt nie zginął, ale 43 osoby odniosły lekkie obrażenia. Do zdarzenia doszło wcześniej rano w niedzielę, ale gdyby doszło do niego w normalny dzień pracy, liczba ofiar śmiertelnych mogłaby być znaczna. Straty finansowe wyniosły około 1 mld funtów (1,5 mld dolarów).

Większość zespołów przeprowadzających analizę LOPA dla scenariusza przepełnienia zbiornika magazynowego benzyny założyłaby, że będzie ona spływać po ściankach zbiornika i gromadzić się w postaci cieczy w tacy zbiornika, co rzeczywiście miało miejsce.

JAKIE SKUTKI KOŃCOWE MOŻNA BYŁOBY ZAŁOŻYĆ, BIORĄC POD UWAGĘ, ŻE OBSZAR W OBRĘBIE TACY ZBIORNIKA JEST OBSZAREM OTWARTYM?

Byłby to najprawdopodobniej pożar powierzchniowy, skutki poważne, ale nie katastrofalne. Niewielu analityków przewidziałoby tak masowe eksplozje, ponieważ panowało powszechne przekonanie, że benzyna nie wybuchła łatwo. Konsekwencje, a tym samym ryzyko, zostałyby zatem niedoszacowane, a IPL, które obecnie uważamy za konieczne, uznano by za przesadę.

4. Błądny dobór warstw zabezpieczeń – jednym z ostatnich błędów, ale nie najmniej ważnych, często popełnianych podczas analiz, jest błądny dobór warstw zabezpieczeń.

Najczęściej popełnianie błędy na tym etapie dotyczą prawidłowej oceny istniejących zabezpieczeń, np. zaworów bezpieczeństwa czy też interwencji operatora w odpowiedzi na alarm bez sprawdzenia, czy te zabezpieczenia są adekwatne i skuteczne.

- **Zawory bezpieczeństwa** powinny zostać wymienione jako zabezpieczenia dopiero po potwierdzeniu, że rozmiar zaworu i ustawione ciśnienie są odpowiednie do analizowanego scenariusza. Można tego dokonać poprzez przegląd danych na schematach P&ID oraz dokumentacji zaworów bezpieczeństwa.
- Dużo większy problem wiąże się z **odpowiedzią operatora na alarm**. Wydaje się, że zbyt często uznawane jako IPL (skuteczna warstwa zabezpieczająca) są alarmy bez przeprowadzenia dowodu, czy:
 - istnieją pisemne procedury,
 - operator jest zawsze dostępny,
 - operator jest w stanie zidentyfikować problem,
 - operator ma wystarczająco dużo czasu,
 - operator jest przeszkolony i jest w stanie wykonać właściwe czynności,
 - przeprowadzane są regularne ćwiczenia,
 - wartości alarmowe są właściwie ustawione,
 - alarmy są testowane, a przetworniki sprawdzane.

Podjęcie decyzji o odpowiedzialności warstwy zabezpieczeń związanej z prawidłową interwencją operatora w odpowiedzi na alarm bez sprawdzenia powyższych warunków jest najczęściej popełnianym błędem w analizach zagrożeń i ryzyka.

Bez przeprowadzenia szczegółowej oceny, czy proponowane zabezpieczenia są odpowiednie i skuteczne, w konsekwencji następuje kolejny etap podczas którego fałszywie zaniża się poziom ryzyka.

PODSUMOWANIE

Jak wynika z przykładów przytoczonych powyżej, na osoby i zespoły wykonujące analizy zagrożeń i ryzyka czyha wiele pułapek. Czasami ze względu na małe doświadczenie prowadzącego, a czasami z powodu niewystarczających kompetencji lub ich braku wyniki analiz pozostawiają wiele do życzenia.

Tym opracowaniem chcielibyśmy zwrócić uwagę, że odpowiedni dobór metody analizy oraz jej prawidłowe wykonanie może zapobiec poważnym katastrofom w przemyśle. Błędne wykonanie analizy, dopuszczające zbyt wiele błędów w projekcie, bądź zastosowanie „fałszywych” warstw zabezpieczeń mogą skutkować poważnymi awariami, w wyniku których może nastąpić uwolnienie toksycznych łatwopalnych substancji do otoczenia, a następnie pożar, wybuch lub skażenie



środowiska.

W ŚWIEŁLE POWYŻSZEGO ANALIZY TE NABIERAJĄ ZUPEŁNIE INNEGO ZNACZENIA.

Poprawność wyboru i wykonania analiz pozwala już na etapie projektu wprowadzić jedno z ważniejszych narzędzi bezpieczeństwa procesowego, a mianowicie filozofię bezpieczeństwa inherentnego. Zgodnie z nią najlepszym sposobem radzenia sobie z zagrożeniem jest jego usunięcie. Dlatego to od poprawności wykonania analiz zależeć będzie w przyszłości bezpieczeństwo eksploatacji, a błędy na tym etapie mogą powodować dodatkowe koszty finansowe związane z koniecznością wprowadzenia dodatkowych zabezpieczeń oraz opóźnieniami w realizacji inwestycji.

UDT-CERT, jako techniczna jednostka ekspercka wspierająca przemysł, posiada ogromne 17-letnie doświadczenie w zakresie prowadzenia tego typu analiz. UDT-CERT wykonuje analizy zagrożeń i oceny ryzyka m.in. metodami: PHA – Wstępna Analiza Zagrożeń, HAZOP – Analiza Zagrożeń i Zdolności Operacyjnych, LOPA – Analiza Warstw Zabezpieczeń, FTA – Analiza Drzewa Błędów, ETA – Analiza Drzewa Zdarzeń itp.

Razem z projektantami, biurami projektowymi oraz przede wszystkim eksploatującymi instalacje przemysłowe wykonaliśmy około 600 analiz. Wspieraliśmy jako eksperci największe polskie inwestycje. Ten duży sukces osiągnęliśmy dzięki profesjonalnej wiedzy oraz ogromnemu zaangażowaniu, nasi eksperci uczestniczą w szkoleniach, seminariach czy też konferencjach krajowych i zagranicznych. Analizy typu HAZOP prowadziliśmy zarówno w kraju, jak i za granicą. W 2020 r., w trosce o bezpieczeństwo publiczne oraz wychodząc naprzeciw oczekiwaniom właścicieli instalacji przemysłowych, projektantów i biur projektowych uczestniczących w projektowaniu, wytwarzaniu oraz modernizacjach instalacji przemysłowych, Urząd Dozoru Technicznego opracował wytyczne „Prowadzenie analiz i ocena ryzyka” [10] w celu uporządkowania i wskazania wymagań im stawianych. Wytyczne te można pobrać ze strony www.udt.gov.pl.



Literatura:

1. Guidelines for hazard evaluation procedures, 3rd Edition. New York: Center for Chemical Process Safety, American Institute of Chemical Engineers: 2008.
2. Guidelines for consequence analysis of chemical releases, New York: Center for Chemical Process Safety, American Institute of Chemical Engineers: 1999.
3. Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis, New York, NY: Center for Chemical Process Safety, American Institute of Chemical Engineers: 2015.
4. Practical SIL Target Selection – Risk Analysis per the IEC 61511 Safety Lifecycle: exida.com LLC; First Edition: 2012.
5. https://en.wikipedia.org/wiki/Bhopal_disaster
6. https://en.wikipedia.org/wiki/Seveso_disaster
7. The HAZOP Leader's Handbook: How to Plan and Conduct Successful HAZOP Studies : PHIL EAMES: IChemE: 2022.
8. Ron Jarvis, Andy Goddard, 2017, An Analysis of Common Causes of Major Losses in the Onshore Oil, Gas & Petrochemical Industries: Symposium Series No 162, HAZARDS 27 IChemE <https://www.icheme.org/media/15486/paper-34.pdf>
9. Selection of Hazard Evaluation Techniques: William Bridges: 2008 : Process Improvement Institute, Inc. (PII).
10. Prowadzenie Analiz i Ocena Ryzyka – Wytyczne Urzędu Dozoru Technicznego, Wydanie 1: Urząd Dozoru Technicznego UDT-CERT, Warszawa 2020. Urząd Dozoru Technicznego – Analiza zagrożeń i oceny ryzyka <https://www.udt.gov.pl/ekspertyzy-techniczne/analiza-zagrozen-i-oceny-ryzyka>