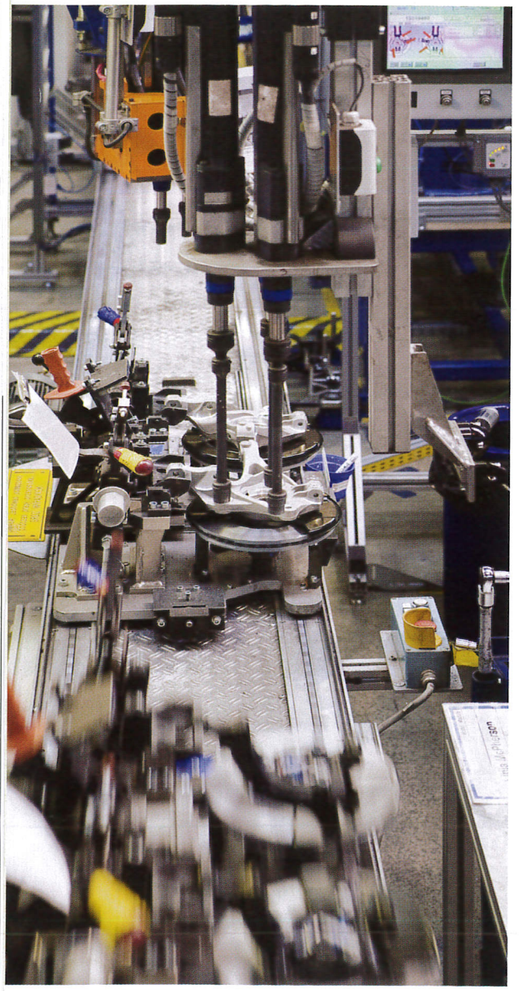
# Bezpieczeństwo procesów przemysłowych

## Wybrane metodologie i techniki oceny ryzyka instalacji przemysłowych

KRZYSZTOF UJCZAK
ELOKON Polska
www.elokon.pl



Bezpieczeństwo w procesach przemysłowych jest zagadnieniem obecnym w technice od lat. W ostatnim czasie jest ono jednak coraz częściej poruszaną tematyką. Potencjalne straty ludzkie, środowiskowe lub majątkowe, wynikające z przeoczeń w tej dziedzinie, mogą przyjmować bardzo dużą skalę. W artykule przedstawiono wybrane zagadnienia z dziedziny procesu oceny ryzyka i bezpieczeństwa procesów przemysłowych. Powinny one być w usystematyzowany sposób wdrażane przez osoby zaangażowane od etapu projektu, przez uruchomienie, aż do prowadzenia i utrzymania produkcji w celu zagwarantowania bezpiecznego funkcjonowania przedsiębiorstwa. Do takich kroków można zaliczyć m.in. rzetelnie przeprowadzoną analizę stanu bezpieczeństwa z wykorzystaniem metod typu HAZOP oraz LOPA, która umożliwia uzyskanie odpowiedzi na pytanie, czy prawdopodobieństwo wystąpienia groźnej w skutkach awarii przemysłowej jest na poziomie odpowiednio niskim/akceptowalnym. Wykorzystując komputerowe narzędzia modelujące skutki uwolnień substancji niebezpiecznych, możliwe jest zasymulowanie skali zagrożenia.





W analizach bezpieczeństwa procesowego posługujemy się ryzykiem zdefiniowanym jako kombinacja prawdopodobieństwa wystąpienia zdarzeń niepożądanych i wielkości ich skutków. Na oba te człony ma wpływ wiele aspektów związanych z charakterystyką danego procesu i rodzajem stosowanych substancji. Czynniki ograniczające ryzyko wystąpienia awarii to m.in. skuteczna identyfikacja zagrożeń, odpowiedni projekt i wykonanie instalacji, zastosowana odpowiednia aparatura kontrolna i pomiarowa, a także funkcje bezpieczeństwa realizowane przez przyrządowe systemy bezpieczeństwa (Safety Instrumented System – SIS). Stanowią one bardzo ważną warstwę zabezpieczeń instalacji procesowych. Określenie i poprawna realizacja SIS ma niewątpliwy wpływ na zmniejszenie prawdopodobieństwa wystąpienia zdarzenia niebezpiecznego. Zarówno proces określenia wymagań funkcji bezpieczeństwa, jak i metody ich realizacji są podane m.in. w normach dotyczących bezpieczeństwa funkcjonalnego – tj. grupy PN-EN 61508 oraz PN-EN 61511. Normy te w wyczerpujący sposób określają cykl życia bezpieczeństwa w przemyśle, których jednym z początkowych etapów jest ocena ryzyka.

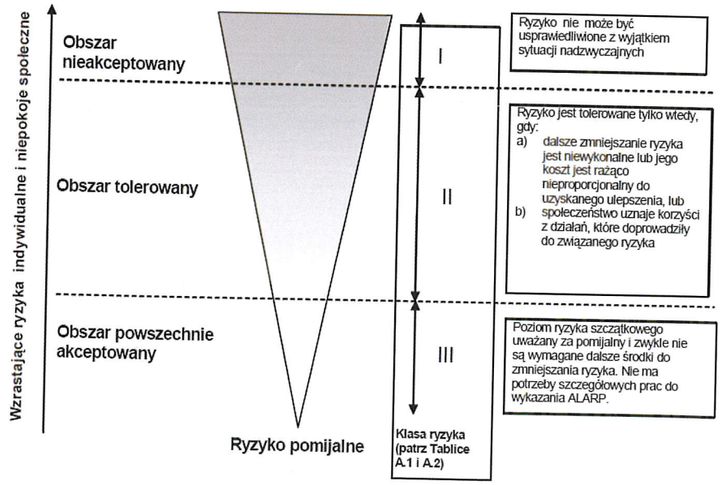
Każdą ocenę ryzyka należy rozpocząć od określenia koncepcji i wyznaczenia całkowitego zakresu rozpatrywanego projektu. Znając wartości graniczne i zakres wymaganej analizy ryzyka, można rozpocząć etap identyfikacji zagrożeń. Jest to punkt newralgiczny dla dalszego procesu szacowania i ewentualnej redukcji ryzyka. Dla porównania w przemyśle maszynowym identyfikacja zagrożeń jest etapem stosunkowo prostszym. Wynika to w dużej mierze z mechanicznego charakteru zagrożeń. Większość z nich jest związana z energiami towarzyszącymi napędom wykonującym określone i z góry zaplanowane zadania technologiczne. Dzięki temu możemy powiązać je z określonym stanem maszyny, konkretnymi czynnościami wykonywanymi w danych strefach i podejść do analizy ryzyka w sposób dyskretny – łącząc rodzaj zagrożenia, czynności wykonywane przez człowieka z prawdopodobieństwem wystąpienia z góry określonych skutków.

Przemysł procesowy natomiast charakteryzuje się ciągłością. Zagrożenia występujące w instalacjach przemysłowych nie są widoczne gołym okiem. Często samo określenie stanu badanego obiektu jest niemożliwe – występują różne, mniej lub bardziej zbadane, stany przejściowe. Dodatkowo sytuację komplikuje wyjątkowo złożone zadanie, jakim jest określenie wielkości zdarzeń awaryjnych i oszacowanie ich skutków. Warto pamiętać, że mówiąc „zdarzenie awaryjne", odnosimy się zarówno do występujących w danym systemie substancjach niebezpiecznych, jak i energiach, które mogą ulec uwolnieniu.

Istnieje wiele technik, które pomagają w identyfikacji zagrożeń. Jedną z najbardziej uniwersalnych i najczęściej stosowanych metod jest analiza HAZOP (Hazard and Operability Study), opisana w normie PN-IEC 61882. Była ona stosowana przez koncern ICI (Imperial Chemical Industries) od 1963 r., ale upubliczniona została przez ICI i Chemical Industries Associations Ltd. w 1977 r. Badanie HAZOP jest procesem twórczym i grupowym. Polega na wykorzystaniu doświadczenia, wiedzy i umiejętności członków zespołu, którzy powinni być specjalistami w swojej dziedzinie. Podstawą HAZOP jest badanie za pomocą słów kluczowych – zestawu określeń, które odpowiadają za możliwe odchylenia od założonych wartości projektowych. Wynikiem przeprowadzonego badania powinny być przemyślane i opracowane wspólnie wnioski. Zapisuje się je w postaci raportu z badania HAZOP. W raporcie przedstawia się dla każdego zagrożenia potencjalne przyczyny i możliwe skutki.

W następnym kroku szacuje się prawdopodobieństwo wystąpienia skutków i ich skalę. Na podstawie tych dwóch wskaźników określa się poziom ryzyka. W tym celu można wykorzystać metodę matrycy ryzyka, grafu ryzyka, metodę wskaźników ryzyka lub inne przyjęte w danym zakładzie metodologie. Znajomość oszacowanych poziomów ryzyka dla konkretnych zagrożeń jest pierwszym krokiem, aby znaleźć odpowiedź na pytanie, czy takie ryzyko jest dla użytkownika danej instalacji procesowej akceptowalne.

Tutaj pojawia się zyskująca na znaczeniu koncepcja ALARP (As Low As Reasonably Practicable) – (ryzyka) tak niskiego jak to praktycznie możliwe. Model ten określa trzy obszary akceptowalności ryzyka. Po pierwsze – ryzyko tak małe, że uznaje się je za bez znaczenia. Jest to poziom powszechnie akceptowany i nie wymaga się żadnych doraźnych działań poprawiających nadzorowanie zagrożenia. Konieczne może być stałe czuwanie i działania profilaktyczne, aby ryzyko nadal pozostało w tym obszarze. Drugim skrajnym obszarem jest ryzyko tak duże, że uznaje się je za nieakceptowalne. Nie może ono zostać usprawiedliwione żadnymi zwykłymi okolicznościami. Wtedy zaleca się, aby zostało ono zmniejszone do poziomu przynajmniej tolerowanego – w przeciwnym wypadku należy rozważyć usunięcie danego zagrożenia. Poziom ryzyka znajdujący się pomiędzy tymi dwoma skrajnymi obszarami jest to obszar ryzyka tolerowanego (rys. 1).




Rys. 1. Ryzyko tolerowane i ALARP. Źródło: PN-EN 61511-3:2009

Uznaje się dla niego, że ryzyko jest tolerowane, gdy dalsze jego zmniejszanie jest niewykonalne lub koszt redukcji jest nieproporcjonalny (zbyt wysoki) wobec oczekiwanej poprawy. Szukając odpowiedzi na pytanie, czy warto zaimplementować rozwiązania w celu poprawy bezpieczeństwa, trzeba zastanowić się nad następującymi kwestiami: jaki jest koszt stosowania wyższych standardów bezpieczeństwa, jakie są zyski z ich wdrożenia oraz jakie mogą być straty, jeżeli tego nie zrobimy. Znajdując odpowiedzi na te trzy pytania, określimy poziom ryzyka, który jest dla nas tolerowany (czyli jest ALARP).

Podstawową metodą ograniczania poziomu ryzyka związanego z danym procesem jest projektowanie z uwzględnieniem rozwiązań wewnętrznie bezpiecznych. Przykładem takich rozwiązań jest zmiana lub ograniczenie ilości substancji biorących udział w procesie na takie, która stwarza mniejsze zagrożenie w przypadku ewentualnego uwolnienia. W większości przypadków jednak z powodów technicznych, jakościowych lub wydajnościowych możliwość zastosowania przez projektantów rozwiązań wewnętrznie bezpiecznych jest mocno ograniczona. Wtedy też stosuje się warstwy zabezpieczeń. Przykłady warstw zabezpieczeń zebrane zostały w tabeli 1.

nienaruszalności bezpieczeństwa, czyli parametru SIL (Safety Integrity Level), zdefiniowanego w normach z cyklu PN-EN 61508 i PN-EN 61511. Powiązanie nienaruszalności bezpieczeństwa z ryzykiem jest kolejnym etapem poprawnie przeprowadzonej analizy ryzyka. W tym kroku należy najpierw przypisać funkcje bezpieczeństwa przyrządowym systemom bezpieczeństwa, a następnie określić ich wymaganą niezawodność (nienaruszalność). Podczas tej fazy, korzystając z wyników analiz jakościowych przeprowadzonych w celu identyfikacji zagrożeń, próbuje się narzucić wartości liczbowe – najczęściej wyrażone jako prawdopodobieństwo niezadziałania – poszczególnym komponentom danego układu. Jeżeli wymagana jest większa niezawodności systemu, powinien on spełniać wymagania wyższego poziomu SIL (w skali czterostopniowej).

W celu wyznaczenia wymaganych poziomów niezawodności powszechnie stosowanymi technikami są: analiza drzewa błędów (Fault Tree Analysis – FTA) oraz analiza warstw zabezpieczeń (Layer Of Protection Analysis – LOPA). Analiza drzewa błędów jest pełną metodą ilościową, a więc dającą najdokładniejsze wyniki. Jednocześnie jest również najbardziej czasochłonna i wymaga posiadania ogromnej ilości danych niezawodnościowych komponentów wchodzących

Tabela 1. Przykłady warstw zabezpieczeń występujących w przemyśle procesowym

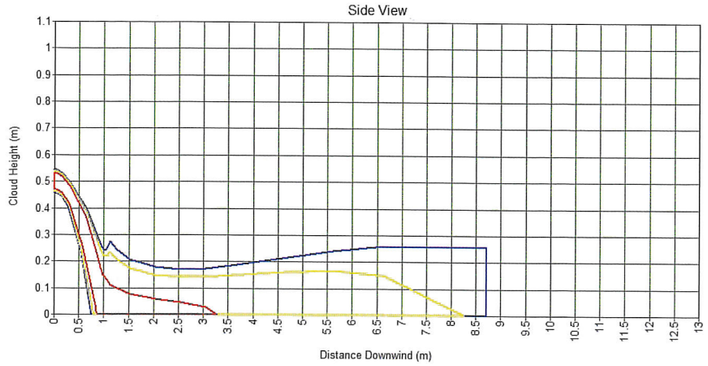
| Warstwa zabezpieczeń | Klasyfikacja zabezpieczeń | Wymagania funkcjonalne |
|---|---|---|
| Zapobieganie | projekt procesowy, standardy wykonania | Zapobieganie rozwojowi odchyleń od założeń procesowych. Zmniejszenie prawdopodobieństwa wystąpienia zdarzenia wypadkowego. |
| | podstawowa automatyka procesowa i alarmy i interwencje operatora (BPCS) | |
| Ochrona | alarmy krytyczne i interwencje operatora | Ograniczenie i spowolnienie narastania zdarzenia niebezpiecznego. Zmniejszenie prawdopodobieństwa wystąpienia i zmniejszenie skutków zdarzenia niebezpiecznego. |
| | układy automatyki zabezpieczeniowej | |
| | systemy upustowe | |
| | pasywne zabezpieczenia fizyczne | |
| Przeciwdziałanie | aktywny systemy reakcji awaryjnych służb wewnętrznych | Ograniczanie i łagodzenie skutków wewnętrznych i zewnętrznych uwolnień substancji niebezpiecznych |
| | działania i reakcja służb zewnętrznych | |

Z punktu widzenia automatyzacji jedną z najistotniejszych warstw są wspomniane na początku przyrządowe systemy bezpieczeństwa. Ich zadaniem jest zatrzymanie procesu, jeżeli pojawią się określone warunki krytyczne. W zależności od wymagań przyrządowy system bezpieczeństwa może mieć mniejszą lub większą niezawodność. Najczęściej jest ona określona za pomocą poziomów

w skład analizowanego układu. W związku z tym coraz częściej do analizy i wyznaczania wymaganej niezawodności SIS jest stosowana LOPA. Metoda analizy warstwy zabezpieczeń została przedstawiona w latach 90. ubiegłego wieku. Polega ona na zmodyfikowanej analizie drzewa zdarzeń (Event Tree Analysis – ETA), gdzie ocenie poddaje się zestaw warstw zabezpieczeń, jakie zastosowane zostały do danego procesu. Warstwy te zostały ułożone w kolejności wynikającej z ich aktywacji w przypadku eskalacji zdarzenia niebezpiecznego. Niezadziałanie pierwszej warstwy powinno wywołać reakcję następnej i w efekcie zatrzymanie procesu stwarzającego zagrożenie. Niezadziałanie wszystkich warstw zabezpieczeń doprowadzi do zdarzenia niebezpiecznego mogącego mieć znaczne konsekwencje.

W celu wyznaczenia prawdopodobieństwa wystąpienia zdarzenia niepożądanego w sposób półilościowy określa się wartości prawdopodobieństwa niezadziałania poszczególnych warstw zabezpieczeń na żądanie (PFD). Do oszacowania wartości PFD korzysta się z danych historycznych, tabelarycznych, uproszczonych analiz numerycznych (FTA, FMEA) oraz z oceny eksperckiej. Wraz z rozwojem techniki zabezpieczeniowej równolegle rozwijane są kolejne warstwy zabezpieczeń. Analiza warstw zabezpieczeń jest więc metodą, pozwalającą na ocenę nawet najbardziej zaawansowanych systemów technicznych.

Opisane powyżej metody służą do oszacowania prawdopodobieństwa wystąpienia sytuacji niebezpiecznej oraz do oceny, w jaki sposób SIS może posłużyć do zmniejszenia tego prawdopodobieństwa. W celu oszacowania drugiej części elementu składowego ryzyka – wielkości skutków, konieczne jest podjęcie próby zamodelowania rozpatrywanych uwolnień niebezpiecznych. Rozpatruje się trzy podstawowe cechy substancji używanych w przemyśle procesowym: palność, wybuchowość i toksyczność. Dodatkowo należy wziąć pod uwagę stan skupienia substancji w momencie emisji: ciekły, lotny czy mieszaninę dwufazową. Wreszcie powinno się uwzględnić rodzaj obiektu, z którego nastąpiło uwolnienie. Mogą to być zbiorniki, rurociągi, elementy aparatury kontrolno-pomiarowej, pompy itd. Bezpośrednio z nimi związane są wielkości otworów, przez które następuje wyciek. Te oraz inne zmienne, od których zależy np. natężenie wypływu czy szybkość dyspersji analizowanej substancji, powodują, że modelowanie uwolnień wypływów wymaga zaprzęgnięcia skomplikowanych modeli i równań matematycznych. Tutaj w sukurs przychodzą dostępne na rynku specjalistyczne programy komputerowe wspomagające modelowanie. Dzięki nim można określić zasięgi chmur gazowych, wielkości obszaru rozlewiska, a także ewentualne zapłony czy wybuchy substancji palnych. Przykład zamodelowanego wypływu ciekłego gazu ziemnego LNG został zaprezentowany na rysunku 2. Żółte kontury określają obszar, gdzie istnieje mieszanina LNG i powietrza powyżej dolnej granicy wybuchowości. Na podstawie otrzymanych wyników można określić strefy zagrożone wybuchem (w podanym przykładzie zasięg chmury palnej od miejsca wypływu wynosi prawie 8,5 m).




Rys. 2. Model wycieku LNG z otworu o średnicy 10 mm, na wysokości 0,5 m nad poziomem obsługi

Poprawne wykorzystanie narzędzi komputerowych zależy w dużym stopniu od doświadczenia i wiedzy specjalistycznej użytkownika. Kluczem do otrzymania wiarygodnych wyników jest wybór odpowiedniego modelu używanego do kalkulacji oraz wprowadzenie poprawnych parametrów brzegowych używanych do obliczeń. Ze względu na dużą liczbę niewiadomych, podczas analizy możliwych konsekwencji uwolnienia substancji niebezpiecznej należy bardzo drobiazgowo badać możliwe scenariusze zdarzeń i wszelkie uproszczenia traktować z dużą dozą nieufności.

W powyższym artykule poruszono bardzo pobieżnie problem oceny ryzyka instalacji przemysłowych. Pomimo tego, że analizy stanu bezpieczeństwa są czasochłonne, wymagają specjalistycznej, interdyscyplinarnej wiedzy na pograniczu chemii, inżynierii procesowej czy automatyki, okazuje się, że czas i pieniądze poświęcone w fazie projektowej zwracają się z nawiązką w przyszłości. Brak awarii przemysłowych niejednokrotnie jest kluczem do sukcesu organizacji i firm produkcyjnych, polepszając ich pozycję na rynku pod kątem wizerunkowym dla opinii publicznej, a także pod kątem polepszenia stosunków biznesowych z ich klientami. Z drugiej strony należy pamiętać, że każde uwolnienie substancji niebezpiecznych powoduje mniejsze lub większe konsekwencje w obszarze zdrowia ludzkiego, środowiska oraz zasobów materialnych zakładu przemysłowego.