

LOPA

ANALIZA WARSTW ZABEZPIECZEŃ



**MGR INŻ.
JACEK ŻACZYŃSKI**

Ekspert Urzędzeń Ciśnieniowych
Urząd Dozoru Technicznego
Oddział w Szczecinie



**MGR INŻ.
DAMIAN FIEDOROWICZ**

Kierownik Działu Oceny Zgodności
Urząd Dozoru Technicznego
Oddział w Szczecinie

FUNKCJONOWANIE ZAKŁADÓW PRZEMYSŁOWYCH, ZWŁASZCZA TYCH ZWIĄZANYCH Z PRZEMYSŁEM CHEMICZNYM, PETROCHEMICZNYM CZY NAFTOWO-GAZOWYM, NIESIE ZA SOBĄ NIEODŁĄCZNE RYZYKO ZWIĄZANE Z PRZETWARZANIEM ORAZ MAGAZYNOWANIEM MATERIAŁÓW NIEBEZPIECZNYCH (PALNYCH, WYBUCHOWYCH, TOKSYCZNYCH). DOTYCZY TO SZCZEGÓLNIE PROCESÓW PROWADZONYCH PRZY WYSOKICH CIŚNIENIACH RZĘDU 300–400 BAR ORAZ TEMPERATURACH SIĘGAJĄCYCH RZĘDU 500–600°C. DLATEGO ABY ZAPEWNIĆ BEZPIECZNĄ EKSPLOATACJĘ TYCH INSTALACJI, NALEŻY DOKŁADNIE ZIDENTYFIKOWAĆ I PRZEANALIZOWAĆ POTENCJALNE ZAGROŻENIA JAKIE STWARZA ICH EKSPLOATACJA, POWIĄZANE Z NIMI RYZYKA ORAZ ICH SKUTKI.

Analizy zagrożeń procesowych (PHA - PROCESS HAZARD ANALYSIS), takie jak: Badanie Zagrożeń i Zdolności Operacyjnych (HAZOP - Hazard and Operability Study), Listy Kontrolne (Check-List), Co Jeśli (What-If), Wstępna Analiza Zagrożeń (PrHA - Preliminary Hazard Analysis) są użytecznymi narzędziami do identyfikowania potencjalnych scenariuszy awaryjnych. Analizy te mogą jednak dać tylko jakościową informację, czy zastosowano wystarczające zabezpieczenia w celu złagodzenia skutków zagrożenia. W celu uzyskania dokładniejszych wyników, przeprowadza się czasochłonne oraz bardziej skomplikowane ilościowe analizy ryzyka, takie jak QRA (Quantitative Risk Analysis) czy Bow-Tie. Przeprowadzanie takich analiz ryzyka dla wszystkich scenariuszy awaryjnych, naraża na ogromne problemy oraz kosztów i dlatego jest w większości wypadków nieracjonalne. Konsekwencją tego, było opracowanie oraz wdrożenie półilościowej analizy ryzyka, analizy LOPA (Layer of Protection Analysis).

Analiza warstw zabezpieczeń (LOPA) to ilościowa metoda analizy oraz oceny ryzyka od 20 lat powszechnie stosowana w przemyśle chemicznym czy petrochemicznym. Analiza ta w porównaniu do ilościowych analiz zagrożeń osiąga podobne rezultaty przy równoczesnym ograniczeniu kosztów oraz wykorzystania potencjału ludzkiego. Jednocześnie jest metodą bardziej szczegółową niż analizy jakościowe, a dodatkowo daje zespołowi możliwość odkrycia słabych i mocnych stron stosowanych systemów bezpieczeństwa (warstw zabezpieczeń), aby skuteczniej chronić pracowników, zakład i społeczeństwo.

LOPA to sposób na identyfikację scenariuszy, które stwarzają największe skutki w powiązaniu do wysokiego prawdopodobieństwa ich wystąpienia.

- LOPA pomaga odpowiedzieć na pytanie, czy konsekwencje wystąpienia ryzykownych scenariuszy można ograniczyć poprzez zastosowanie zasad projektowania inherentnego (z natury bezpiecznego).
- LOPA pozwala określić, czy istnieje konieczność stosowania przyrządowych systemów bezpieczeństwa (SIS - Safety Intergyry System) lub innych warstw zabezpieczeń w celu poprawy bezpieczeństwa.



Rys. 1. Zdjęcie wykonane po eksplozji w zakładach Phillips Petroleum Co. w Pasadenie 23.10.1989 r. [1]

UWAGA

Błędnie przeprowadzona analiza metodą LOPA wprowadza poczucie fałszywego bezpieczeństwa, a co za tym idzie, akceptację niedoszacowanego ryzyka, bezpośrednio obniżając całkowity poziom bezpieczeństwa.

Pozorne osiągnięcie ryzyka na poziomie akceptowalnym i tolerowanym może prowadzić do zaniechania stosowania zabezpieczeń rozumianych jako szeroko akceptowana dobra praktyka inżynierska.

RYS HISTORYCZNY

Pierwsze analizy warstw zabezpieczeń (LOPA) zostały przeprowadzone pod koniec lat 90. w kilku firmach przemysłu chemicznego. Ich prekursorami byli między innymi Arthur Dowell i William Bridges, którzy rozpoczęli wdrażanie tej techniki w swoich firmach jako metody dającej możliwość przeprowadzenia analiz z uwzględnieniem niezależnych warstw zabezpieczeń, bez konieczności przeprowadzania skomplikowanych analiz ilościowych QRA.

Zanim przeprowadzono pierwsze analizy LOPA wydane zostały dwie publikacje opisujące genezę tej metody.

1. Pod koniec 1980 r. ówczesne Stowarzyszenie Producentów Chemicznych opublikowało Kodeks praktyk zarządzania bezpieczeństwem procesowym.

2. W 1993 r. CCPS (Center for Chemical Process Safety) opublikowała wytyczne dotyczące bezpiecznej automatyzacji procesów chemicznych *Guidelines for Safe Automation of Chemical Process* (CCPS, 1993) [2], w której jako jedną z metod określania poziomu nienaruszalności bezpieczeństwa dla przyrządowych funkcji bezpieczeństwa (SIF) zaproponowano analizę LOPA (nazywaną metodą poziomu integralności SIS opartą na ryzyku).

Pierwsze publikacje nie opisywały w pełni metodologii LOPA. Dalszy rozwój dotyczył w szczególności opracowania:

- metody do wyznaczania odpowiedniego poziomu nienaruszalności bezpieczeństwa (SIL) przyrządowej funkcji bezpieczeństwa (SIF) - dla niektórych firm był to punkt wyjścia,
- narzędzia w celu zmniejszenia liczby scenariuszy wymagających przeprowadzenia pełnych ilościowych ocen ryzyka (QRA),
- narzędzia identyfikacji osprzętu „krytycznego dla bezpieczeństwa”,
- uproszczonego narzędzia umożliwiającego dokonywanie ilościowych analiz ryzyka.

Przełom nastąpił podczas Międzynarodowej Konferencji i Warsztatów na temat Analizy Ryzyka w Bezpieczeństwie Procesowym, która odbyła się w październiku 1997 r. Skończyła się ona porozumieniem co do konieczności opracowania książki opisującej metodę LOPA. Równoległe z tymi wysiłkami toczyły się dyskusje na temat wymagań dotyczących projektowania przyrządowych systemów bezpieczeństwa (SIS) oraz określenia wymaganego poziomu nienaruszalności bezpieczeństwa (SIL). W normie EN 61511 [3] w części 3 z 1999 r. pierwszy raz wskazano analizę LOPA jako narzędzie do wyznaczania poziomu SIL.

Pierwsza książka *Layer of Protection Analysis, Simplified Process Risk Assessment* zo-

stała opublikowana przez CCPS (Center of Chemical Process Safety/AIChE) w 2001 r. [4]. Współpomysłodawcami i głównymi autorami książki byli Arthur M. Dowell i William G. Bridges. Do opracowania tego przewodnika CCPS utworzyła zespół złożony z następujących firm: A. D. Little, ARCO Chemical, Dow Chemical, DuPont, Factory Mutual, ABS Consulting, International Specialty Products, Procter and Gamble (P&G), Rhodia, Rohm and Haas, Shell (Equilon) oraz Union Carbide.

W kolejnych latach pojawiły się informacje o problemach, jakie napotkały firmy wdrażające tę metodę. CCPS podjęło próbę rozwiązania niektórych z nich, a rezultaty opublikowała w dwóch następnych książkach. W 2013 r. wydano *Guidelines for Conditional Modifiers and Enabling Events* [5], a dwa lata później *Guidelines for Initiating Events and Independent Protection* [6].

Od czasu opublikowania pierwszej książki metoda LOPA szybko zyskiwała na popularności. Obecnie używa się jej zarówno do dokonywania oceny ryzyka, jak i podejmowania decyzji o poziomie SIL dla SIF.

Pomimo upływu 20 lat od wdrożenia tej metody wiele osób nadal nie do końca rozumie intencję jej prekursorów, co powodować może wiele błędów w czasie jej wykonywania. W Polsce ograniczona dostępność polskojęzycznych materiałów dotyczących prowadzenia analizy metodą LOPA, powoduje rzadkie jej stosowanie.

W artykule oraz kolejnych jego częściach przybliżymy tę bardzo skuteczną technikę analizy ryzyka, oraz wskażemy najczęściej popełniane błędy podczas jej stosowania.



Rys. 2. Publikacje CCPS: *Layer of Protection Analysis, Simplified Process Risk Assessment* (2001) [4], *Guidelines for Conditional Modifiers and Enabling Events* (2013) [5], *Guidelines for Initiating Events and Independent Protection* (2015) [6]

METODOLOGIA

LOPA jest uproszczoną formą oceny ryzyka. Metoda ta zazwyczaj wykorzystuje kategorie rzędu wielkości (1/rok) do określenia częstotliwości zdarzeń inicjujących, wielkości skutków oraz prawdopodobieństwa awarii (niezadziałania) „PFD” (Propability Failure of Demand) niezależnych warstw zabezpieczeń (IPL - Independent Protection Layer) w celu oszacowania ryzyka analizowanego scenariusza awaryjnego.

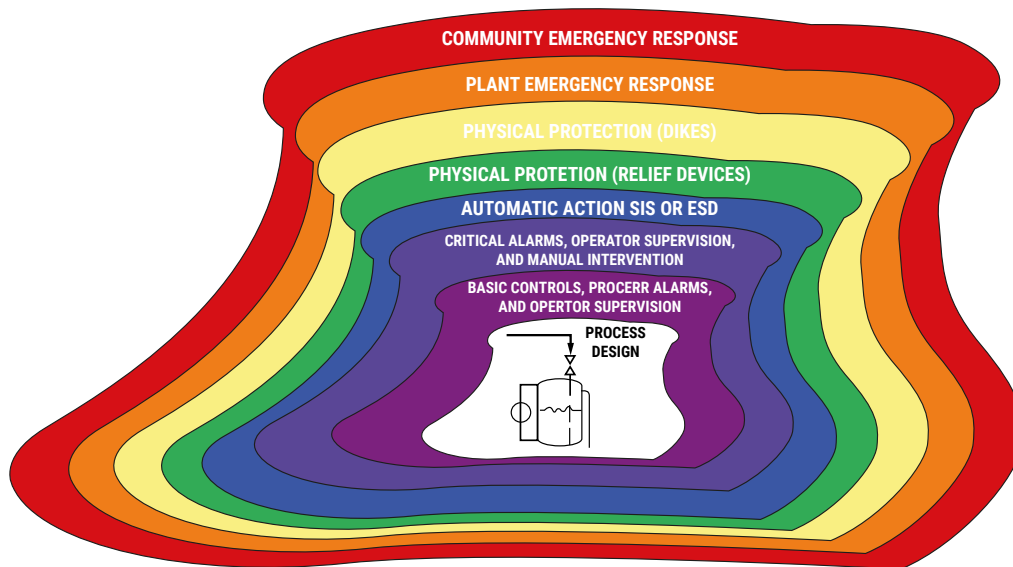
LOPA to narzędzie analityczne, które najczęściej opiera się na informacjach uzyskanych podczas jakościowych analiz zagrożeń (PHA – Proces Hazard Analysis), takich jak np. analiza HAZOP.

Głównym celem analizy LOPA jest określenie, czy istniejące warstwy zabezpieczeń są wystarczające dla danego scenariusza awaryjnego, tzn. czy ryzyko wystąpienia skutków awarii jest tolerowane.

W bezpieczeństwie procesowym istnieje wiele typów warstw zabezpieczeń, które można przedstawić schematycznie (rys. 3) wg CCPS-AIChE [3].

Koncepcja zastosowania warstw zabezpieczających chroniących instalacje i zakłady procesowe, oparta jest siedmiu podstawowych warstwach.

- Warstwa 1: Projekt procesu (np. projekty z natury bezpieczniejsze)
- Warstwa 2: Podstawowe kontrole, alarmy procesowe i nadzór operatora
- Warstwa 3: Alarmy krytyczne, nadzór i interwencja operatora
- Warstwa 4: Automatyka zabezpieczająca (np. SIS lub ESD)
- Warstwa 5: Ochrona fizyczna (np. urządzenia odciążające PSV)
- Warstwa 6: Ochrona fizyczna (np. groble)
- Warstwa 7: Zarządzanie w przypadkach awaryjnych

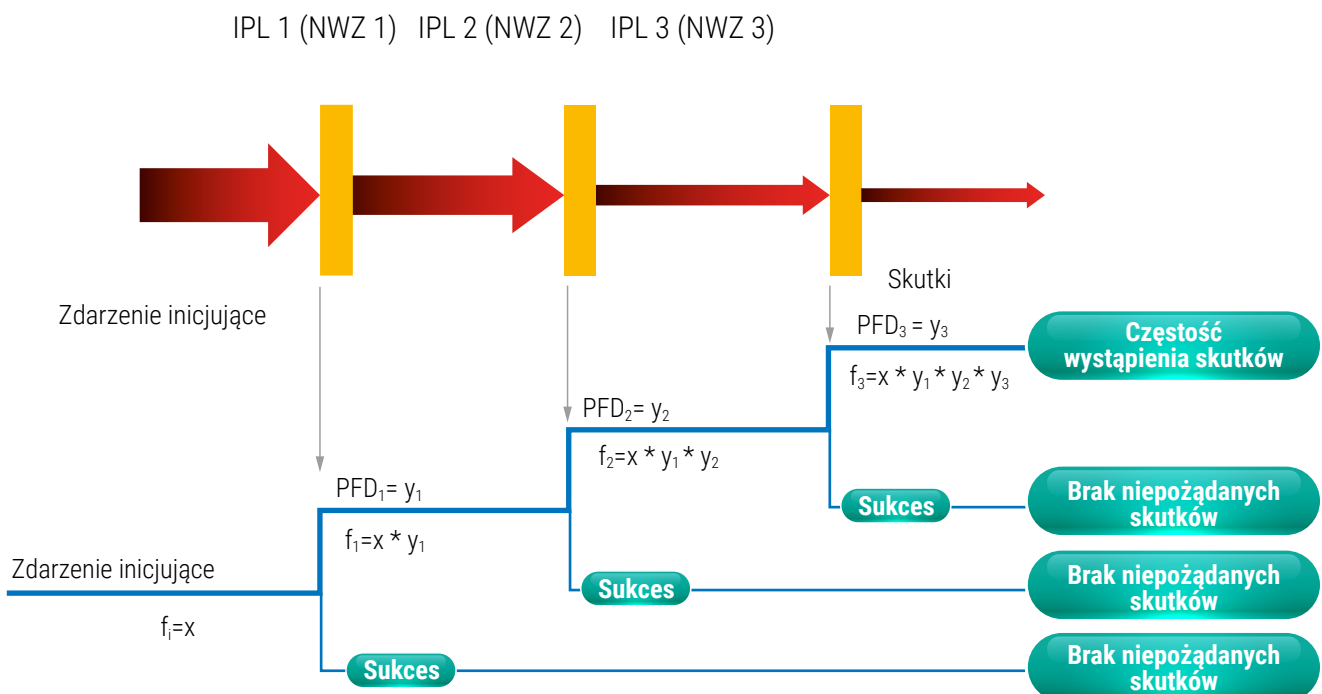


Rys. 3. Warstwy ochrony w przemyśle procesowym [4]

Odpowiednia ochrona przeciw skutkom scenariusza awaryjnego wymaga skuteczności działania jednej lub wielu warstw ochrony. Zależy to od złożoności procesu i wielkości oraz charakteru potencjalnych skutków. Do przerwania rozwijającego się scenariusza awaryjnego, a tym samym zapobiegnięcia skutkom awarii, najczęściej wystarczy już zadziałanie jednej warstwy zabezpieczeń. Żadne zabezpieczenie nie jest jednak całkowicie skuteczne, zatem dąży się do zapewnienia odpowiedniej liczby warstw zabezpieczeń, aby ryzyko poważnej awarii przemysłowej było tolerowane.

Jeżeli w wyniku oceny, poziom ryzyka nie osiągnie poziomu ryzyka tolerowanego, zaleca się, aby przed podjęciem decyzji o zaprojektowaniu dodatkowych lub wzmocnieniu istniejących zabezpieczeń rozważyć zastosowanie rozwiązań z natury bezpiecznych (tzw. bezpieczeństwo inherentne).

LOPA nie sugeruje, które zabezpieczenia należy dodać ani jakie rozwiązanie wybrać, ale pomaga w ocenie alternatywnych rozwiązań w celu ograniczenia ryzyka.



IPL – Independent Protection Layer (Niezależna Warstwa Zabezpieczeń – NWZ)

PFD – Probability of Failure on Demand (Prawdopodobieństwo niezadziałania na żądanie)

f – częstotliwość (1/rok)

Rys. 4. Graficzne porównanie metod LOPA i ETA

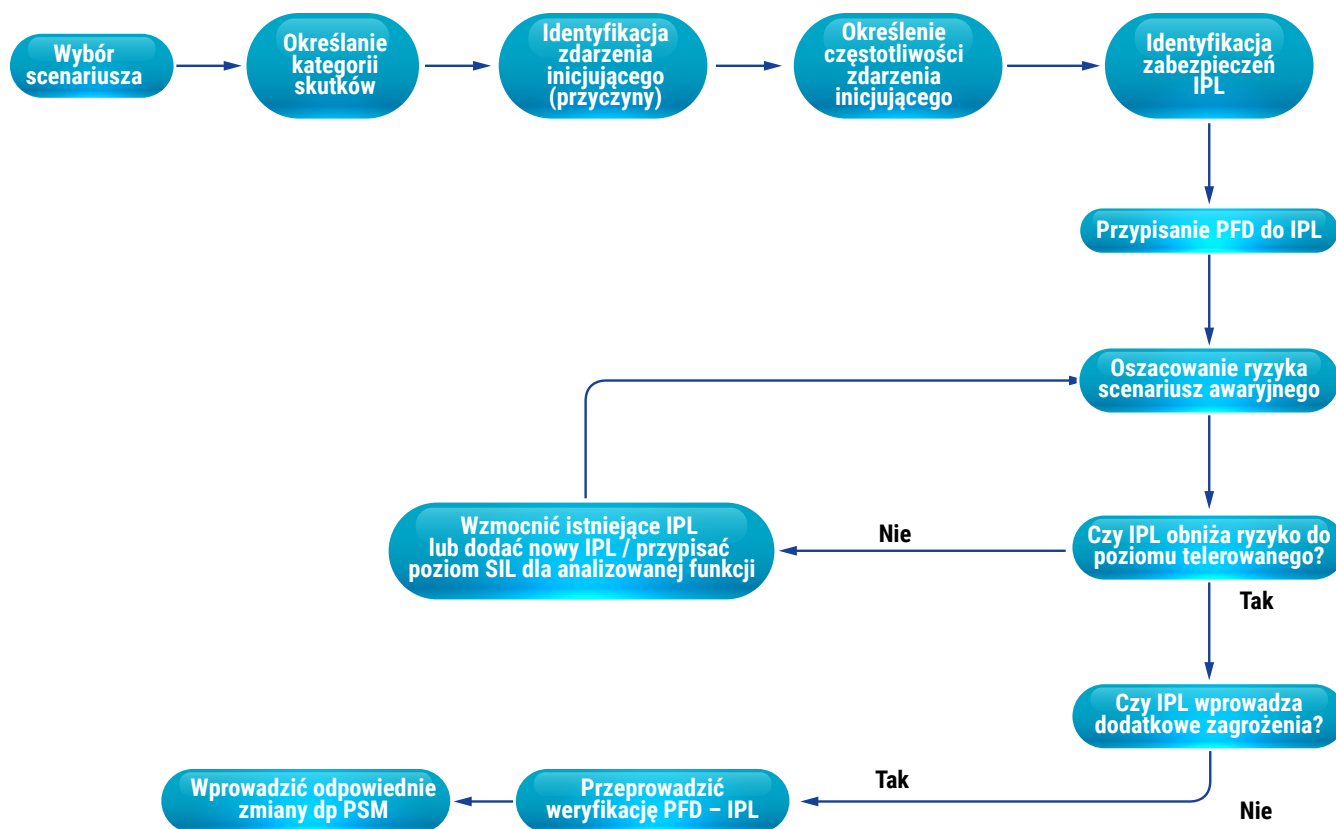
LOPA	ETA
<p>Graficzny model (rys. 4) ilustruje redukcję częstotliwości skutków scenariusza awaryjnego po przejściu przez każdą kolejną niezależną warstwę zabezpieczeń (IPL). Szerokość strzałki przedstawiającej częstotliwość zmniejsza się w miarę przejścia scenariusza awaryjnego przez każdy IPL.</p>	<p>Przedstawiony jest także (rys. 4) model drzewa zdarzeń (ETA) opisujący skuteczne lub nieskuteczne działanie każdej warstwy zabezpieczeń IPL. LOPA koncentruje się na najgorszej ścieżce awarii w drzewie zdarzeń, oznaczonej pogrubioną linią.</p>

Zapamiętaj!

Scenariusz awaryjny analizowany w LOPA opisuje pojedynczą parę przyczyna-skutek.

PROCEDURA PRZEPROWADZANIA ANALIZY LOPA

1. Wybór scenariuszów awaryjnych, określenie rodzaju i ciężkości skutków (ludzie, środowisko, mienie).
2. Identyfikacja przyczyny dla każdego scenariusza awaryjnego.
3. Oszacowanie częstotliwości zdarzenia inicjującego (przyczyny).
4. Identyfikacja wszystkich warstw zabezpieczających, wybór Niezależnych Warstw Zabezpieczających (IPL) dla każdej pary przyczyna-skutek.
5. Określenie PFD (Prawdopodobieństwa Niezadziałania na Żądanie) dla każdej Niezależnej Warstwy Zabezpieczeń IPL.
6. Obliczenie częstotliwości zdarzenia awaryjnego dla każdej pary przyczyna-skutek, jako iloczynu częstotliwości zdarzeń inicjujących oraz PFD każdego odpowiedniego IPL.
7. Porównanie zredukowanej (uwzględniającej PFD wszystkich IPL) częstotliwości zdarzenia awaryjnego z korporacyjnymi kryteriami tolerancji ryzyka.
8. Jeżeli kryteria ryzyka nie są osiągnięte, można dodać dodatkowe IPL, ulepszyć SIL, przeprojektować proces lub przeprowadzić bardziej szczegółową analizę. Bardziej szczegółowe techniki obejmują analizę drzewa błędów (FTA) i ilościową ocenę ryzyka (QRA).
9. Przeanalizowanie, czy ewentualne dodatkowe zabezpieczenia wprowadzają nowe zagrożenia.
10. Przeprowadzenie weryfikacji PFD wybranych zabezpieczeń.
11. W razie potrzeby zaktualizowanie procedury zarządzania bezpieczeństwem procesowym (PSM).



Rys. 3. Graficzne przedstawienie procedury LOPA



W kolejnych częściach cyklu przedstawiona zostanie szczegółowa procedura prowadzenia analizy LOPA z podziałem na kilka głównych kroków. Zaczniemy od wyboru scenariuszy awaryjnych, przez identyfikację zdarzeń inicjujących oraz niezależnych warstw zabezpieczeń, po obliczenia częstotliwości zdarzeń awaryjnych. Następnie przedstawionych zostanie siedem „podstawowych wymagań” (core attributes), które muszą spełnić zabezpieczenia, aby być IPL. Również napiszemy o błędach przy ich stosowaniu oraz odpowiemy na pytanie czy „zakład jest gotowy na zastosowanie analizy LOPA?”. Będziemy mogli też przeanalizować wszystkie kroki w analizie LOPA na podstawie przykładu.

Literatura:

1. <https://tiche.org/wp-content/uploads/2022/10/Safety-Moment-Mr.-Tanaratn-Nurach-GC.pdf> (dostęp 03.2024)
2. Guidelines for Safe Automation of Chemical Processes, AIChE, CCPS, October 1993, <https://www.aiche.org/resources/publications/books/guidelines-safe-automation-chemical-processes>
3. IEC 61511-3 - Bezpieczeństwo funkcjonalne Przynależne systemy bezpieczeństwa do sektora przemysłu procesowego Część 3: Wytyczne do określania poziomów wymaganych nienaruszalności bezpieczeństwa
4. Layer of Protection Analysis: Simplified Process Risk Assessment. New York, NY: Center for Chemical Process Safety, American Institute of Chemical Engineers AIChE 2001.
5. Guidelines for Enabling Conditions and Conditional Modifiers in Layer of Protection Analysis, New York, NY: Center for Chemical Process Safety, American Institute of Chemical Engineers: 2013.
6. 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.
7. Practical SIL Target Selection – Risk Analysis per the IEC 61511 Safety Lifecycle: exida.com LLC; First Edition: 2012.
8. 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 \(udt.gov.pl\)](https://www.udt.gov.pl/).