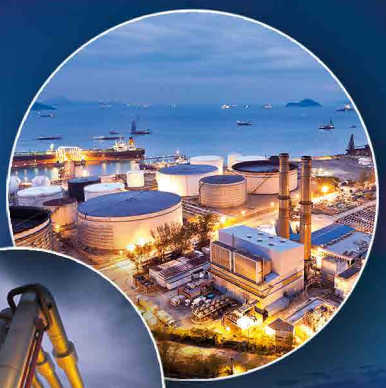
BIULETYN URZĘDU DOZORU TECHNICZNEGO

INSPEKTOR

TECHNIKA I BEZPIECZEŃSTWO

Wydanie specjalne

CHEMIA
PETROCHEMIA
RAFINERIA



- DYREKTYWA SEVESO
- DYREKTYWA ATEX
- METODYKA LOPA
- ALARP ZARZĄDZANIE RYZYKIEM

- RISK BASED INSPECTION RBI
- FITNESS FOR SERVICE FFS
- CYFROWY BLIŹNIAK DLA INSTALACJI PROCESOWYCH
- CYBERBEZPIECZEŃSTWO

Załóż konto na portalu eUDT,

wypełniając formularz rejestracyjny dostępny na https://eudt.gov.pl/ i korzystaj z usług oferowanych przez

UDT on-line!

- Wygodny i szybki dostęp do informacji o Twoich urządzeniach, terminach badań i rozliczeniach finansowych z UDT
- Darmowy dostęp do portalu 24/7/365
- Łatwe i proste śledzenie zdarzeń związanych z Twoimi urządzeniami
- Możliwość ustawienia własnego kalendarza wydarzeń oraz alertów
- Możliwość wyświetlania i pobierania dokumentów UDT
- Elektroniczna korespondencja z UDT, więcej spraw, które załatwisz on-line
- Decyzje i protokoły w formie elektronicznej
- Płatności on-line

W razie dodatkowych pytań skontaktuj się z wybranym oddziałem/biurem UDT

Szanowni Państwo,

kolejne specjalne wydanie magazynu UDT poświęcamy branży chemicznej, petrochemicznej i rafineryjnej. Te wysoce odpowiedzialne obszary wymagają szczególnego indywidualnego podejścia do kwestii bezpieczeństwa oraz efektywności i wydajności. Prezentujemy Państwu rozwiązana mogące być istotnym wsparciem dla przemysłu procesowego, a wiele z nich specjalnie dla tych branż zostało opracowanych.
Zachęcam też do zapoznania się z wydaniami specjalnymi magazynu UDT „Inspektor DŹWIGI" oraz „Inspektor ENERGETYKA".

Zapraszam do ciekawej lektury
Redaktor Naczelna
Dr inż. Małgorzata Suś-Ryszkowska
Departament Innowacji i Rozwoju
Urząd Dozoru Technicznego

w numerze

KOORDYNACJA MERYTORYCZNA WYDANIA

Mgr inż. Rafał Górczyński

Kierownik Działu Technicznego
Oddział w Bydgoszczy Biuro w Płocku
Urząd Dozoru Technicznego

Absolwent Wydziału Mechaniki Politechniki Warszawskiej Filia w Płocku o specjalności Inżynieria Przedsiębiorczości. Ukończył studia podyplomowe Politechniki Łódzkiej w Łodzi o specjalności Bezpieczeństwo Procesów Przemysłowych w 2008 roku i studia podyplomowe Politechniki Śląskiej w Gliwicach o specjalności Technologie Spawalnicze w 2004 roku. Pracownik UDT od 2000 roku, aktualnie na stanowisku Kierownika Działu Technicznego Urzędu Dozoru Technicznego Oddział w Bydgoszczy Biuro w Płocku od 2019 roku oraz w latach 2010-2015. Prowadzi analizy zagrożeń i ryzyka oraz analizy RBI związane z planowaniem inspekcji urządzeń podlegających dozorowi technicznemu. Prowadzi również audity bezpieczeństwa procesowego wg wytycznych CCPS oraz API RP 581. Członek Centrum Kompetencyjnego ds. Metodologii RBI. Jednocześnie Ekspert UDT-CERT ds. oceny zgodności wg PED w ramach JN oraz auditor systemów zarządzania jakością, środowiskiem i BHP. W ramach prac brał udział przy opracowaniu Warunków Technicznych - Wytycznych Urzędu Dozoru Technicznego: WUDT-RBI:2017 Planowanie inspekcji urządzeń ciśnieniowych w oparciu o analizę ryzyka RBI (Risk Based Inspection) oraz WUDT-PIECE:2022 - Planowanie inspekcji i bezpieczną eksploatacją pieców technologicznych.

Mgr inż. Tomasz Klinkosz

Ekspert Urządzeń Ciśnieniowych
Oddział w Gdańsku
Urząd Dozoru Technicznego

Absolwent Wydziału Mechanicznego Politechniki Gdańskiej w specjalności Systemy Maszyny i Urządzenia Energetyczne oraz Wydziału Zarządzania i Ekonomii Politechniki Gdańskiej. W 2006 r. ukończył studium podyplomowe nt. Bezpieczeństwa procesów przemysłowych na Politechniki Łódzkiej. Od 2004 r. zatrudniony w UDT. Obecnie Ekspert Urządzeń Ciśnieniowych w Dziale Oceny Zgodności UDT w Gdańsku. Koordynator Centrum ds. Metodologii RBI. Certyfikat kompetencji American Petroleum Institute w zakresie API-580. RBI-Professional. Prowadzi analizy zagrożeń i ryzyka oraz planowanie inspekcji urządzeń wg RBI. Uczestniczy we wdrażaniu technologii Digital Twin w przemyśle rafineryjnym. Wykonuje badania techniczne urządzeń podlagających dozorowi technicznemu oraz ocenę zgodności urządzeń ciśnieniowych wg dyrektywy ciśnieniowej. Prowadzi audyty systemów zarządzania jakością wg normy ISO 9001 oraz audity bezpieczeństwa procesowego wg CCPS oraz API RP 581. Jest wykładowcą Akademii UDT w zakresie bezpieczeństwa instalacji ziębniczych i procesowego oraz RBI. Autor publikacji nt. urządzeń w instalacjach ziębniczych, RBI oraz FFS. Współautor Warunków Technicznych WUDT-RBI-2022 Planowanie inspekcji urządzeń ciśnieniowych w oparciu o analizę ryzyka RBI oraz Wytycznych UDT Prowadzenie analiz i ocena ryzyka. Współautor przewodnika UDT „Kompleksowe bezpieczeństwo instalacji ziębniczych".

Mgr inż. Jacek Żaczyński

Kierownik Działu Technicznego
Oddział w Szczecinie
Urząd Dozoru Technicznego

Absolwent Wydziału Mechanicznego Politechniki Szczecińskiej na kierunku Mechanika i Budowa Maszyn. Od 2001 r. zatrudniony w UDT. Obecnie pracuje na stanowisku Kierownika Działu Technicznego Urzędu Dozoru Technicznego Oddział w Szczecinie. Koordynator Centrum Kompetencyjnego ds. bezpieczeństwa procesowego w zakresie analiz zagrożeń i ryzyka. Reprezentant UDT w Komisji Technicznej nr 9 ds. Niezawodności w Polskim Komitecie Normalizacyjnym. Prowadzi analizy zagrożeń i ryzyka oraz analizy SIL. Posiada Certyfikat inżyniera bezpieczeństwa funkcjonalnego w Exida. Wykonuje badania techniczne urządzeń podlagających dozorowi technicznemu oraz ocenę zgodności urządzeń ciśnieniowych wg dyrektywy ciśnieniowej. Prowadzi egzaminy spawaczy w oparciu o normy PN-EN 9606 oraz kwalifikacje technologii spawalniczych wg. PN EN 15614. Jest wykładowcą Akademii UDT w zakresie bezpieczeństwa procesowego i funkcjonalnego. Współautor Wytycznych UDT Prowadzenie analiz i ocena ryzyka. Autor publikacji nt. bezpieczeństwa procesowego i funkcjonalnego.

BIULETYN URZĘDU DOZORU TECHNICZNEGO
INSPEKTOR TECHNIKA I BEZPIECZEŃSTWO

Bezpłatny biuletyn Urzędu Dozoru Technicznego
ul. Szczęśliwicka 34, 02-353 Warszawa
inspektor@udt.gov.pl, www.udt.gov.pl

Redaktor Naczelna:
Małgorzata Suś-Ryszkowska

BRANŻA CHEMICZNA, PETROCHEMICZNA I RAFINERYJNA

Zagrożenia, perspektywy, wyzwania

MGR INŻ. RAFAŁ GÓRCZYŃSKI

Kierownik Działu Technicznego
Oddział w Bydgoszczy
Biuro w Płocku
Urząd Dozoru Technicznego

PRZEMYSŁ CHEMICZNY, JAKO JEDEN Z NAJWIĘKSZYCH I NAJBARDZIEJ ZRÓŻNICOWANYCH SEKTORÓW, ODGRYWA KLUCZOWĄ ROLĘ W GLOBALNEJ GOSPODARCE. OBEJMUJE WYTWARZANIE SZEROKIEJ GAMY PRODUKTÓW, KTÓRE ZNAJDUJĄ ZASTOSOWANIE W NIEMAL KAŻDEJ DZIEDZINIE ŻYCIA CODZIENNEGO I W RÓŻNYCH BRANŻACH, TAKICH JAK: MEDYCYNA, ELEKTRONIKA, ROLNICTWO, BUDOWNICTWO, MOTORYZACJA.

NAFTOWYM SZLAKIEM

Ropa naftowa była znana już w czasach starożytnych, ponieważ w wielu rejonach świata samoistnie wypływała na powierzchnię ziemi. Egipcjanie wykorzystywali ją do balsamowania ciał, Grecy stosowali jako broń (tzw. ogień grecki), a Chińczycy używali jej do oświetlenia mieszkań, spalając nasączone ropą tkaniny. Na obszarze Galicji olej skalny początkowo używany był jako smar, a także środek do oświetlania bądź lekarstwo. Ropę pozyskiwano, kopiąc głębokie doły, aby oddzielić lżejszą porkurę od cięższego skałoleju, zwykle zmieszanego z ziemią. Lżejszą frakcję wykorzystywano do spalania w różnego rodzaju lampach i świecach. Na terenach Pogórza Karpackiego ropa naftowa wypływała samoczynnie na powierzchnię, a miejscowi chłopi zbierali ją do wiader, używając tkanin lub kubków. Ze względu na jej wszechstronne zastosowanie z każdym rokiem wzrastało zainteresowanie tym zasobem naturalnym. Żeby zwiększyć wydobycie ropy, zaczęto kopać płytkie studnie (bez jakichkolwiek zabezpieczeń).

W 1791 r. tego typu kopalnia działała już w Nahujowicach, a jej szyby sięgały głębokości ok. 4–6 m. W 1840 r. w okolicach Stanisławowa istniało już 75 płytkich studni. Z szybów zbierano ropę do wiader lub kołowrotków. Wydobyty surowiec przechowywano w kadziach z drewna. Pierwszą próbę jego destylacji w 1810 r. podjął Józef Hecker z Pragi. Innym śladem wykorzystywania naturalnych wycieków ropy była działalność tzw. maziarzy, którzy poprzez spalanie jej lekkich składników wytwarzali mazie i smary, używane do smarowania osi wozów.

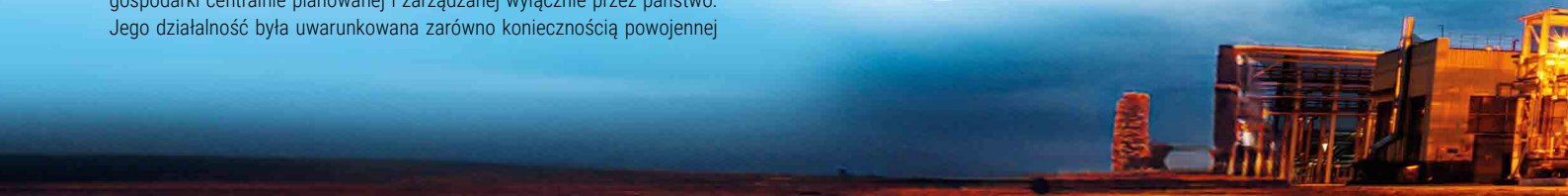
Przemysł naftowy Polski w latach powojennych funkcjonował w ramach gospodarki centralnie planowanej i zarządzanej wyłącznie przez państwo. Jego działalność była uwarunkowana zarówno koniecznością powojennej

WIELKĄ ROLĘ W BUDOWIE PODSTAW PRZEMYSŁU NAFTOWEGO ODEGRAŁ IGNACY ŁUKASIEWICZ.

Był wynalazcą i konstruktorem lampy naftowej, twórcą metody destylacji ropy, przedsiębiorcą, organizatorem kopalni oraz destylarni. Ignacy Łukasiewicz był również założycielem i pierwszym prezesem Towarzystwa dla Opieki i Rozwoju Przemysłu i Górnictwa Naftowego, przekształconego następnie w Krajowe Towarzystwo Naftowe.

Za symboliczną datę rozpoczęcia działalności gospodarczej Ignacego Łukasiewicza można uznać 31 lipca 1853 r., kiedy po raz pierwszy lampa naftowa została użyta podczas operacji w szpitalu we Lwowie. Wcześniej już udało mu się dokonać destylacji ropy naftowej i stworzyć naftę.

Niedługo potem Łukasiewicz przeniósł się go Gorlic, głównie ze względu na bliskość źródeł naftowych i tani transport. Rozpoczął pracę w aptece Jana Tomaniewicza, a ropę otrzymywał od Stanisława Jabłonowskiego, który w 1850 r. stworzył fabrykę asfaltu w Kobylance.



odbudowy kopalń oraz zakładów przetwórczych, jak i doktryną polityki gospodarczej PRL, kładącą szczególny nacisk na rozwój przemysłu ciężkiego. Do ogólnego wzrostu konsumpcji ropy naftowej w Polsce przyczyniał się głównie stopniowy rozwój przemysłu, energetyki i transportu. W roku 1947 polska gospodarka zużyła 407 tys. ton ropy naftowej.

Rozwój gospodarczy Polski Ludowej łączył się z coraz większym zapotrzebowaniem na surowce energetyczne, w tym również na ropę naftową. Ponieważ jednak krajowe wydobycie nie było w stanie zaspokoić potrzeb wewnętrznych, państwo zwiększało systematycznie import ropy z ZSRR. Temu służyło oddanie do użytku w 1964 r. ropociągu „Przyjaźń" i wybudowanie na jego trasie nowej rafinerii w Płocku. Kolejny wzrost importu nastąpił w latach 70. XX w. i wiązał się ze sprowadzaniem ropy arabskiej do Portu Północnego w Gdańsku, gdzie stanął również nowoczesny kombinat rafineryjny. Konsumpcja ropy naftowej w Polsce w roku 1980 wyniosła 387 tys. baryłek dziennie (tj. 19,35 mln ton rocznie), a w roku 1990 już tylko 280 tys. baryłek dziennie (ok. 14 mln ton rocznie).

W 1984 r. wszystkie polskie rafinerie południowe (Gorlice, Jasło, Jedlicze, Trzebinia, Czechowice) miały łącznie zdolność przerobu ropy naftowej w wysokości 1,6 mln ton rocznie. Było to niewiele w porównaniu ze zdolnością dwóch pozostałych zakładów przeróbczych w kraju (Mazowieckie Zakłady Rafineryjne i Petrochemiczne w Płocku – 13,6 mln ton, a Gdańskie Zakłady Rafineryjne – 3,3 mln ton) [3].

Na 2021 rok zdolność przerobowa ropy w płockiej rafinerii wyniosła 14,5 mln ton, natomiast jej moce przerobowe wynoszą 16,3 mln ton rocznie. W tym samym czasie rafineria Grupy Kapitałowej LOTOS przerobiła 9,9 mln ton ropy naftowej, a wykorzystanie nominalnych zdolności przerobowych rafinerii w Gdańsku kształtowało się na poziomie 98,8%.

WYZWANIA BRANŻY WSPÓŁCZEŚNIE

Sektor chemiczny stoi obecnie przed szeregiem wyzwań, zmuszony do znalezienia równowagi między ambitnymi celami klimatycznymi wyznaczanymi w ramach Unii Europejskiej a realnymi możliwościami polskich przedsiębiorstw. Wiadomym jest, że struktura rodzimej gospodarki, miks energetyczny oraz poziom rozwoju przemysłu różnią się od tych w krajach zachodnich.

Dzisiejszą działalność zakładów petrochemicznych w Polsce kształtuje przede wszystkim sytuacja geopolityczna, parametry makroekonomiczne, takie jak wysokie stopy procentowe i rosnące koszty materiałów, zmieniające się polityki i przepisy oraz pojawianie się nowych technologii. Od początku wojny rosyjsko-ukraińskiej obserwujemy zakłócenia w transakcjach handlowych, które doprowadziły do powstania nowych przepływów w handlu surowców, co z kolei wpłynęło na różnice cen i regionalną konkurencyjność przemysłową.

Ze względu na wysokie ceny gazu i energii, inflację, wahania kursów walut czy też zmieniające się ceny surowców do produkcji był to bardzo trudny okres dla polskiego przemysłu chemicznego, a dla wielu firm nawet krytyczny. Decyzje o czasowych ograniczeniach produkcji np. poliamidu 6, kaprolaktamu, amoniaku czy też nawozów azotowych odbiły się znacząco na innych branżach przemysłowych. Warto wspomnieć, że problemy energetyczne dotknęły również pozostałe kraje europejskie i inne regiony świata. W efekcie znacząco wzrosły ceny surowców i wytwarzanych z nich wyrobów konsumpcyjnych. Sytuacja panująca aktualnie na Bliskim Wschodzie także może skutkować bardzo znaczącym ryzykiem geopolitycznym dla rynków ropy naftowej, szczególnie w przypadku dalszej eskalacji konfliktu.

PERSPEKTYWY

Obecnie coraz więcej firm z branży chemicznej inwestuje w budowę nowoczesnych instalacji produkcyjnych, a dzięki temu zaczyna dysponować technologiami na współczesnym światowym poziomie. Polscy producenci w sektorze chemicznym realizują programy modernizacyjne i wprowadzają regulacje ograniczające zużywanie zbyt dużych ilości surowców i energii [8]. Realizacja kluczowego projektu w ramach Programu Rozwoju Petrochemii Orlen SA – budowa Olefin 3, przyczyni się nie tylko do wzrostu zysku operacyjnego, ale przede wszystkim oznacza korzyści dla środowiska. Z chwilą uruchomienia produkcji emisja dwutlenku węgla na tonę produktu zmniejszy się aż o 30% [6].

Przemysł chemiczny to jeden z najbardziej rozwiniętych sektorów, który wykorzystuje nowoczesne technologie. Największym przełomem w rozwoju branży chemicznej w Polsce, który właśnie się dokonuje, jest rozbudowa przemysłu rafineryjnego, petrochemicznego i przetwórstwa tworzyw sztucznych.

Wszystkie te zmiany sprawiają, że Polska dorównuje zagranicznym konkurentom oraz stale wzmacnia swoją pozycję w tym sektorze. **Nowe technologie prośrodowiskowe, których powstawanie determinują regulacje unijne i wewnętrzne dyrektywy poszczególnych państw, wpływają na działalność zakładów w branży petrochemicznej.** Strategiczne działania w kierunku transformacji cyfrowej zostały zintensyfikowane. Chwilowy trend powoli zmienił się w stabilną strategię dla większości firm, a koncepcja „Przemysł 4.0" ma być odpowiedzią na ich rozwój w kierunku cyfryzacji. Jedną z większych realizowanych obecnie inicjatyw jest program „Nowa Energia" zakładający wdrożenie innowacyjnych technologii wodorowych. Ma to wspomóc polski przemysł chemiczny i uatrakcyjnić ten sektor. Firmy już dziś planują wykorzystywanie wodoru do czerpania „zielonej energii". Ta technologia ma na celu m.in. redukcję śladu węglowego.Wodór wyróżnia się na tle innych paliw, ponieważ nie emituje dwutlenku węgla ani innych zanieczyszczeń w procesach spalania i ma wysoką gęstość energii – prawie trzykrotnie większą od benzyny. Przestaje on być zatem jedynie narzędziem do dekarbonizacji, a staje się środkiem do osiągnięcia bezpieczeństwa energetycznego i dywersyfiakcji europejskiego przemysłu.

Polska stale wzmacnia swoją pozycję w sektorze chemicznym. Koncepcja „Przemysł 4.0" jest odpowiedzią na rozwój w kierunku cyfryzacji. Wsparciem dla polskiego przemysłu chemicznego jest program „Nowa Energia". Zakłada on wdrożenie innowacyjnych technologii wodorowych. Technologia ta ma na celu m.in. redukcję śladu węglowego oraz dywersyfikację europejskiego przemysłu. W najbliższych latach wzrośnie bezpieczeństwo energetyczne przemysłu chemicznego również ze względu na inwestycje w odnawialne źródła energii oraz własne elektrownie.

W najbliższych latach najważniejsze będzie skupienie na wykorzystaniu różnego rodzaju odnawialnych zasobów energii, co będzie miało pozytywny wpływ na środowisko. Warto zaznaczyć, że to dobry krok w stronę niezależności i bezpieczeństwa energetycznego przemysłu chemicznego. Wojna za naszą wschodnią granicą dobitnie pokazała, jak ważne jest uniezależnienie przemysłu w zakresie dostaw energii oraz dostępności surowców od światowych potentatów. Inwestycja w dostęp do odnawialnych źródeł energii oraz własne elektrownie to długoterminowa strategia, która może przynieść wiele korzyści. Ta inwestycja jest obowiązkiem również polskich przedsiębiorstw [8].

Morskie farmy wiatrowe to jeden z najszybciej rozwijających się sektorów energetyki w Europie. Rosnąca efektywność i niski poziom oddziaływania na środowisko sprawiają, że technologia ta dostarcza już czystą i konkurencyjną cenowo energię elektryczną milionom Europejczyków. Na wodach 12 krajów produkuje się obecnie ok. 25 GW morskiej energii wiatrowej, z czego ok. 2 GW na obszarze Morza Bałtyckiego. Całkowity potencjał obszaru na Bałtyku szacowany jest przez ekspertów na 85 GW, co stanowi blisko dwukrotność wszystkich mocy zainstalowanych obecnie w Polsce. Projekt Polityki Energetycznej Państwa wskazuje potencjał i zakłada rozwój morskiej energetyki wiatrowej na obszarze Polskiej Wyłącznej Strefy Ekonomicznej Morza Bałtyckiego o mocy ok. 5,9 GW w 2030 r. i do ok. 11 GW w 2040 r. Morskie farmy wiatrowe na Bałtyku mają szansę odegrać kluczową rolę w transformacji energetycznej Polski, przyczynić się do zwiększenia bezpieczeństwa energetycznego kraju oraz pomóc w walce z zanieczyszczeniami powietrza.

Firmy wprowadzają także nowe rozwiązania w zakresie bezpieczeństwa produkcyjnego oraz produktowego. Ludzkie życie i ochrona środowiska to najważniejsze kwestie dla każdego z nas.

Plan na najbliższy czas dla wielu firm obejmuje wprowadzanie dobrych praktyk w zakresie bezpieczeństwa procesowego. Branża ropy i gazu przoduje we wdrażaniu najnowocześniejszych technologii w celu zwiększenia wydajności operacyjnej, ograniczenia kosztów oraz wprowadzenia zaawansowanych środków bezpieczeństwa i zrównoważonego rozwoju [9]. W ostatnich latach sztuczna inteligencja (AI) staje się siłą transformacyjną dla branży mającą zastosowanie w całym łańcuchu wartości – od początkowej eksploracji zasobów po zawiłości procesów rafinacji. Predykcja oparta na sztucznej inteligencji ma zasadnicze znaczenie dla osiągnięcia wielu celów, w tym redukcji kosztów, zwiększonej produktywności i zapewnienia niezawodności operacyjnej w branży.

Przenosząc to na grunt rodzimych przedsiębiorstw, należy zauważyć, że aktualnie w Rafinerii Gdańskiej powstaje tzw. cyfrowy bliźniak fragmentu infrastruktury krytycznej. To pierwsze tego typu zastosowanie technologii w sektorze naftowo-gazowym w Polsce. Wirtualne odwzorowanie rzeczywistej instalacji, urządzeń i procesów pozwoli spółce przewidywać potencjalne problemy i awarie, zanim do nich dojdzie. W ten sposób rafineria zapewni ochronę krytycznej infrastruktury przesyłowej i ograniczy koszty związane z przestojami.

Budowanie wirtualnego odwzorowania istniejącej instalacji w świecie cyfrowym (ang. Digital Twin) pozwala na odzwierciedlenie procesu eksploatacji oraz potencjalnej degradacji instalacji przy wykorzystaniu zaawansowanych metod analitycznych.

Na podstawie analizy ryzyka i prowadzonych symulacji procesów korozyjnych na elementach infrastruktury rafineryjnej pracownicy będą mogli doskonalić przewidywanie awarii oraz lepiej prognozować czas przeprowadzenia napraw i wymiany konkretnych elementów. Zastosowanie cyfrowego bliźniaka pozwoli Rafinerii Gdańskiej podnieść niezawodność eksploatacji urządzeń dzięki pogłębionej analizie nowych i istniejących strumieni informacji wspierających decyzje techniczne i technologiczne. Wypracowane w ten sposób scenariusze

działania będzie można wykorzystać do tworzenia innych modeli predykcji zdarzeń awaryjnych i regularnego podnoszenia poziomu zarządzania bezpieczeństwem technicznym instalacji [10].

Podobną funkcję na instalacjach rafineryjnych Orlen SA w Płocku pełni z powodzeniem wdrożony i funkcjonujący system monitoringu korozji on-line. System zbudowany jest na bazie bezinwazyjnych czujników UT mierzących grubości ścianek urządzeń, na których czujniki są zamontowane. Jego podstawową zaletą jest spójność i powtarzalność uzyskiwanych wyników dzięki wykonywaniu pomiarów w dokładnie tych samych punktach.

Kolejny element systemu stanowią sondy ER mierzące korozyjność strumieni od strony procesu, czyli wewnątrz urządzenia w medium roboczym. Wyniki pomiarów on-line wykazują korelację z pomiarami korozji off-line wykonywanymi metodą kuponową, co dowodzi skuteczności działania systemu.

Na instalacjach rafineryjnych wdrożony i funkcjonujący system monitoringu korozji on-line można wykorzystać do tworzenia modeli predykcji zdarzeń awaryjnych i regularnego podnoszenia poziomu zarządzania bezpieczeństwem technicznym instalacji. System zbudowany jest na bazie bezinwazyjnych czujników UT mierzących grubości ścianek urządzeń, na których czujniki są zamontowane. Spójność i powtarzalność uzyskiwanych wyników, dzięki wykonywaniu pomiarów w dokładnie tych samych punktach, jest podstawową zaletą metody.

Pozyskiwane w ten sposób dane o korozji pozwalają niemal natychmiast wpływać na przebieg procesów technologicznych (korekta parametrów procesowych, dozowanie inhibitorów korozji).

W zakresie utrzymania ruchu pozwalają natomiast utrzymywać urządzenia w ciągłej dostępności procesowej, planować z wyprzedzeniem ich przyszłe wymiany oraz dostarczają wiarygodnej informacji o rzeczywistych tempach korozji na potrzeby realizowanych w ORLEN SA analiz Risk Based Inspection.

WYZWANIA

Wzrost efektywności energetycznej i procesowej jest efektem pozytywnych zmian obserwowanych w ostatnim czasie w przemyśle chemicznym. Ze względu na ogromną rolę, jaką odgrywa przemysł chemiczny w polskiej gospodarce, należy wspierać jego rozwój i postrzegać go jako branżę dbającą o środowisko, tworzącą nowe miejsca pracy i promującą innowacyjność. Bez zmiany nastawienia trudno będzie wykorzystać jego potencjał, tak znaczący dla polskiej ekonomii.

Wszystkie zakłady branży chemicznej, rafineryjnej i petrochemicznej, głównie ze względu na przetwarzanie i magazynowanie substancji niebezpiecznych, podlegają wymaganiom dyrektywy Parlamentu Europejskiego i Rady (2012/18/UE) w sprawie kontroli zagrożeń poważnymi awariami związanymi z substancjami niebezpiecznymi Seveso III, jako zakłady dużego ryzyka wystąpienia poważnej awarii przemysłowej.

Obecnie w świecie elastycznych rozwiązań polski przemysł chemiczny zaczyna dopasowywać się, w miarę swoich możliwości, do odbiorcy. Z tego względu poszukiwanie innowacyjnych rozwiązań jest konieczne, aby sektor chemiczny mógł się prężnie rozwijać. Powinien podnosić efektywność produkcji i próbować podejść do niektórych trendów jak do wyzwania stawianego przez świat konsumencki. Jednak największą sztuką jest dostrzeżenie w wyzwaniu szansy na poprawę swojej pozycji w przyszłości [8].

Najbliższe lata mogą być dużym wyzwaniem dla wielu państw członkowskich Unii Europejskiej, w tym także Polski. Ceny ogrzewania, energii elektrycznej oraz paliw transportowych zmieniają się. Przyspieszenie transformacji energetycznej staje się obecnie faktem.

Strategicznym wyzwaniem stojącym przed Polską jest osiągnięcie wysokiego stopnia dywersyfikacji surowców energetycznych, w tym także ropy naftowej, która jeszcze przez długie lata będzie odgrywała istotną rolę dla produkcji paliw. Docelowo sektor w znacznym stopniu napędzany będzie energią elektryczną z rozproszonych OZE (powiązanych z różnymi formami magazynowania energii), co wspierane będzie przez siłownie jądrowe. Budowa elektrowni jądrowej w Polsce to inwestycja strategiczna dla zrównoważonego rozwoju kraju. Energetyka jądrowa stanowi stabilne źródło energii elektrycznej, a możliwość zmagazynowania paliwa jądrowego na długi czas poprawi niezależność energetyczną. Energetyka węglowa jest filarem polskiej gospodarki, zaś elektrownia jądrowa, która nie emituje CO_2, pozwoli nam osiągnąć cele klimatyczne Unii Europejskiej oraz dywersyfikację dostaw. Branża chemiczna w dużym stopniu przyczyni się do rozwoju energetyki jądrowej w naszym kraju, jednak zmiany takie zajmą kilka dekad.

Każdy kraj UE musi zapewnić wdrożenie środków w celu usuwania skutków awarii na terenach wokół instalacji przemysłowych, gdzie przechowywane są znaczne ilości niebezpiecznych substancji. Przedsiębiorstwa, na których terenie znajdują się te substancje w ilościach przekraczających określony poziom, muszą:

- regularnie informować osoby potencjalnie narażone na skutki awarii,
- udostępniać raporty o bezpieczeństwie,
- ustanowić system zarządzania ryzykiem,
- sporządzić wewnętrzny plan operacyjno-ratowniczy.

Kluczową rolę we współpracy zakładów dużego i zwiększonego ryzyka wystąpienia poważnej awarii przemysłowej z UDT odgrywa SYSTEM ZARZĄDZANIA RYZYKIEM. Jest to proces wykorzystania zasobów przedsiębiorstwa dla osiągnięcia dopuszczalnego poziomu ryzyka, gwarantującego minimalizację strat wskutek incydentów, wypadków i awarii, czyli zastosowanie ogólnych zasad zarządzania do czynników odpowiadających za bezpieczeństwo instalacji [11].

System powinien obejmować instrukcje, procedury, procesy oraz zasoby konieczne do określenia oraz wdrożenia programów i planów działań regulujących postępowanie na rzecz zapewnienia bezpieczeństwa i jego ciągłej poprawy.

CELE ZARZĄDZANIA RYZYKIEM

- określenie optymalnych rozwiązań technicznych i organizacyjnych zapobiegających możliwości powstania poważnej awarii przemysłowej i ograniczających jej ewentualne skutki
- zapobieganie wypadkom
- ochrona środowiska naturalnego
- kontrola i utrzymanie ryzyka wystąpienia poważnej awarii na jak najniższym poziomie
- utrzymanie urządzeń w stanie sprawności technicznej
- promowanie kultury bezpiecznej pracy
- zaangażowanie pracowników na rzecz bezpieczeństwa
- podnoszenie poprzez szkolenia ich świadomości w tym zakresie
- współpraca w zakresie zapobiegania awariom z organami kontrolnymi (m.in. PSP, WIOŚ)

Właściwe zarządzanie ryzykiem jest najskuteczniejszym sposobem zapewnienia odpowiednio wysokiego poziomu bezpieczeństwa. Wynika to zarówno z polityki firmy, jak i konieczności przestrzegania przepisów prawnych (polityka państwa). Właściwe zarządzanie ryzykiem odpowiada również na oczekiwania społeczne i daje możliwość uzyskania pozytywnych efektów ekonomicznych dla zakładu.

Zarządzanie ryzykiem to proces obliczeń i analiz pozwalający na ocenę zapewnienia bezpieczeństwa w instalacji procesowej. Umożliwia dobór optymalnych zabezpieczeń względem występujących zagrożeń. Prawidłowe zarządzanie ryzykiem powinno obejmować wszystkie możliwe obszary wpływu.

Głównym elementem zarządzania ryzykiem jest **ANALIZA** ryzyka. Polega ona na identyfikacji zagrożeń, wyznaczaniu potencjalnych scenariuszy awaryjnych oraz na określeniu prawdopodobieństwa, wielkości skutków i wskaźnika ryzyka wystąpienia scenariuszy awaryjnych [1].

W celu zapewnienia bezpieczeństwa instalacji procesowych stosowane są różne ilościowe, półilościowe oraz jakościowe metody analizy ryzyka [2]. Wybór właściwej metody zależy od wielu czynników.

WYBRANE CZYNNIKI WPŁYWAJĄCE NA WYBÓR METODY ANALIZY RYZYKA

- zapotrzebowanie na prowadzenie badań
- rodzaj dostępnych danych
- potencjał zagrożeń
- konkretny element analizy ryzyka
- faza cyklu życia projektu
- polityka bezpieczeństwa przedsiębiorstwa
- dostępne źródła

Nie ma jednej właściwej metody, którą można by zastosować do analizy ryzyka dla każdej instalacji procesowej. Wszystkie metody analizy ryzyka wymagają znacznego poziomu informacji, aby móc zastosować różne techniki, założenia, wymagania oraz narzędzia. Przedsiębiorstwa stosujące duże ilości niebezpiecznych substancji i preparatów chemicznych poszukują prostych metod, niewymagających wielu zasobów, odpowiednich do różnych instalacji i procesów [7].

Urząd Dozoru Technicznego ma duże doświadczenie i długoletnią praktykę w przeprowadzaniu tego typu analiz. Opisywaliśmy je na łamach naszego czasopisma „INSPEKTOR". Eksperci UDT-CERT, wraz z projektantami i przyszłymi użytkownikami, wykonują analizy ryzyka na etapie projektowania instalacji przemysłowych. Oceniają również zabezpieczenia całych instalacji i zespołów urządzeń ciśnieniowych. W fazie eksploatacji urządzeń analizy ryzyka mogą być wykorzystywane do oceny wpływu wprowadzanych zmian podczas modyfikacji układów procesowych. Kluczową rolę odgrywają tu analizy technologiczne, przepływowe, korozyjne czy analizy warstw zabezpieczeń. Wszystkie tego typu działania mają zapewnić jak najdłuższą bezpieczną i bezawaryjną pracę urządzeń ciśnieniowych [4].

Literatura:

1. Kotynia A., 2019. Ocena ryzyka wystąpienia poważnej awarii przemysłowej z wykorzystaniem logiki rozmytej, praca doktorska. Politechnika Łódzka. Wydział Inżynierii Procesowej i Ochrony Środowiska.
2. Borysiewicz M., Markowski A.S., 2002. Kryteria akceptowalności ryzyka poważnych awarii przemysłowych. CIOP, Warszawa.
3. Pasterski B., 2022, Przemysł naftowy w Polsce południowo-wschodniej w latach 1944 – 1989, praca doktorska. Uniwersytet Rzeszowski, Kolegium Nauk Humanistycznych, Instytut Historii.
4. 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
5. Przemysł chemiczny w Polsce – pozycja, wyzwania, perspektywy. Raport Polskiej Izby Przemysłu Chemicznego, listopad 2023; https://pipc.org.pl/najnowszy-raport-przemysl-chemiczny-w-polsce-pozycja-wyzwania-perspektywy-pobierz-2/
6. Raport zintegrowany Grupy Orlen, 2021 https://raportzintegrowany2021.orlen.pl/
7. Prawo - przepisy - Analiza Ryzyka Poważnej Awarii - www.dzpw.pl
8. Przemysł chemiczny w Polsce. Jakie nadchodzą zmiany? [Aktualizacja rok 2023] - Portal Produktowy Grupy PCC, https://www.products.pcc.eu/pl/blog/przemysl-chemiczny-w-polsce-jakie-nadchodza-zmiany/
9. 2024 Oil and Gas Industry Outlook | Deloitte
10. Powstanie cyfrowa wersja gdańskiej rafinerii. Cyfrowy bliźniak infrastruktury (trojmiasto.pl)
11. Prawo - przepisy - Zarządzanie ryzykiem procesowym - www.dzpw.pl

ZAKŁADY DUŻEGO I ZWIĘKSZONEGO RYZYKA – DYREKTYWA SEVESO III

MGR INŻ. KRZYSZTOF FIŁOŃCZUK
Główny Specjalista Urządzeń Ciśnieniowych
Dział Techniczny
Oddział we Wrocławiu
Urząd Dozoru Technicznego

MGR INŻ. PAWEŁ NARECKI
Główny Specjalista Urządzeń Ciśnieniowych
Dział Techniczny
Oddział we Wrocławiu
Urząd Dozoru Technicznego

JEDNYM Z ISTOTNYCH NIEBEZPIECZEŃSTW, WYSTĘPUJĄCYCH SZCZEGÓLNIE W PAŃSTWACH UPRZEMYSŁOWIONYCH, JEST ZAGROŻENIE POWAŻNYMI AWARIAMI PRZEMYSŁOWYMI, KTÓRE CZĘSTO MOGĄ MIEĆ KATASTROFALNE SKUTKI. SĄ TO AWARIE W OBIEKTACH TECHNOLOGICZNYCH LUB MAGAZYNOWYCH, W KTÓRYCH ZNAJDUJĄ SIĘ DUŻE ILOŚCI NIEBEZPIECZNYCH DLA ZDROWIA, ŻYCIA I ŚRODOWISKA SUBSTANCJI CHEMICZNYCH. UNIA EUROPEJSKA STWORZYŁA RAMY PRAWNE WSKAZUJĄCE SPOSOBY PRZECIWDZIAŁANIA I ZARZĄDZANIA RYZYKIEM W ZAKŁADACH PRZEMYSŁOWYCH UZNANYCH ZA NIEBEZPIECZNE.

Na przestrzeni lat na świecie wystąpiły poważne katastrofy przemysłowe oraz awarie, które stanowią przykłady typowych scenariuszy, jeśli chodzi o ich przebieg oraz rodzaj powodowanych skutków. Kilka przykładów – poniżej.

Flixborough, Wielka Brytania, 1 czerwca 1974 r.

W wyniku pęknięcia 20-calowego rurociągu uwolniło się około 80 t gorącego (155°C) ciekłego cykloheksanu znajdującego się pod ciśnieniem 8 barów. Utworzona mieszanina par tego związku chemicznego i powietrza spowodowała eksplozję o sile równoważnej wybuchowi 30 t trotylu (TNT). Wskutek katastrofy śmierć poniosło 28 pracowników zakładu, 36 odniosło obrażenia, a kilkaset osób, przebywających poza terenem zakładu, dotknęły różne skutki wybuchu. Zakład został całkowicie zrujnowany (w promieniu ok. 5 km), poza jego terenem również wystąpiły znaczne zniszczenia.

Seveso, Włochy, 10 lipca 1976 r.

W reaktorze był prowadzony proces produkcji 2,4,5-trichlorofenolu. W wyniku niekontrolowanego doprowadzenia pary wodnej do reaktora, nastąpiła gwałtowna reakcja egzotermiczna. Temperatura osiągnęła ok. 400°C, co spowodowało gwałtowny wzrost ciśnienia i otwarcie zaworu bezpieczeństwa – uwolnienie do atmosfery około 6 t gorących substancji chemicznych, w tym 1–2 kg dioksyn TCDD. W wyniku katastrofy ok. 1500 ha gęsto zaludnionego obszaru zostało skażone, ok. 700 mieszkańców było poszkodowanych w wyniku zatrucia. Obszary skażone wyłączono z gospodarki rolnej na okres 10 lat.

Bhopal, Indie, 3 grudnia 1984 r.

W wyniku prac serwisowych doszło do uwolnienia ponad 40 ton izocyjanianu metylu (MIC), który w postaci cięższego od powietrza gazu rozprzestrzenił się po ok. 2-milionowym mieście. W wyniku tej katastrofy śmierć poniosło około 20 tys. osób. U około 100 tys. osób odnotowano ciężkie przypadki utraty zdrowia. Z terenu skażenia ewakuowano kilkaset tysięcy osób.

Czechowice-Dziedzice, 26 czerwca 1971 r.

W wyniku uderzenia pioruna w kopułę zbiornika magazynowego ropy naftowej doszło do jego pożaru. Rozprzestrzeniający się ogień doprowadził do wybuchu 2 zbiorników ropy naftowej. W wyniku katastrofy zginęło 37 osób, ponad 100 zostało rannych.

Texas City, Stany Zjednoczone, 23 marca 2005 r.

Podczas rozruchu instalacji na wydziale izomeryzacji doszło do zakłóceń kontroli poziomów kolumny. Nastąpiło przekroczenie poziomów alarmowych, nadmierny wzrost temperatury, utrata kontroli nad parametrami procesowymi, co doprowadziło do gwałtownego parowania, wzrostu ciśnienia, wyrzutów rafinatu i w konsekwencji – do eksplozji oraz pożaru. W wyniku tej katastrofy śmierć poniosło 15 osób, liczba rannych wynosiła ponad 170.

O potrzebie ochrony środowiska mówiło się już pod koniec lat 60. W dniu 26 maja 1969 r. na sesji Zgromadzenia Ogólnego S. U Thant – sekretarz ONZ – przedstawił raport „Problemy ludzkiego środowiska".

Dokument ten po raz pierwszy w historii prezentował opinii publicznej dane wskazujące na zniszczenie środowiska naturalnego i jego niekorzystne konsekwencje.

- Dopiero ciąg głośnych awarii w przemyśle, m.in. eksplozja w fabryce herbicydów i pestycydów w miejscowości Seveso, skłonił do opracowania i przyjęcia w dniu 24 czerwca 1982 r. przez Wspólnotę Europejską dyrektywy 82/501/EWG w sprawie niebezpieczeństwa poważnych awarii związanych z niektórymi rodzajami działalności przemysłowej, znanej również jako dyrektywa SEVESO. Dyrektywa **SEVESO I** miała na celu harmonizację ustawodawstwa państw członkowskich dotyczącego poważnych wypadków chemicznych. Jego głównym celem było zapobieganie poważnym awariom z udziałem substancji niebezpiecznych oraz ograniczenie możliwych skutków takich awarii dla zdrowia ludzkiego i środowiska.

- Kolejne incydenty związane z poważnymi awariami na świecie doprowadziły do zmian w dyrektywie SEVESO. Dnia 9 grudnia 1996 r. została ostatecznie przyjęta dyrektywa 96/82/WE – SEVESO II w sprawie kontroli niebezpieczeństwa poważnych awarii związanych z substancjami niebezpiecznymi. **Seveso II** wprowadziła między innymi system klasyfikacji substancji niebezpiecznych (toksycznych, łatwopalnych/wybuchowych i niebezpiecznych dla środowiska) oraz określiła ilości progowe dla niektórych typów, kategorii i grup takich substancji. Dyrektywa SEVESO II została oparta na innowacyjnych koncepcjach, wprowadziła nowy system zarządzania bezpieczeństwem chroniący przed niebezpiecznymi awariami oraz system ich kontrolowania. W dyrektywie dokładnie przedstawiono obowiązki prowadzącego zakład z niebezpiecznymi substancjami oraz kompetencje władz publicznych każdego z krajów Unii Europejskiej.

- Aktualnie obowiązująca dyrektywa 2012/18/UE, zwana również dyrektywą **SEVESO III**, została przyjęta przez Parlament Europejski 4 lipca 2012 r. Głównym celem jej wprowadzenia jest podniesienie poziomu ochrony przed wypadkami w sektorze zakładów stosujących substancje niebezpieczne. Ponadto w dyrektywie wprowadzono zmiany w klasyfikacji substancji niebezpiecznych, które są spójne z obecnie obowiązującym na terenie Unii Europejskiej Globalnym Zharmonizowanym Systemem Klasyfikacji i Oznakowania Chemikaliów (rozporządzenie CLP).

Zmiany w dyrektywie Seveso III dotyczą:

- lepszego dostępu obywateli do informacji o zagrożeniach wynikających z działalności zakładów oraz zasad postępowania na wypadek wystąpienia zdarzenia awaryjnego,
- efektywniejszego udziału zainteresowanej społeczności w tworzeniu planów zagospodarowania przestrzennego związanych z zakładami sevesowskimi,
- zagwarantowania społeczeństwu narzędzi prawnych służących egzekwowaniu dostępu do informacji,
- sprecyzowania bardziej rygorystycznych przepisów w zakresie kontroli zakładów podlegających dyrektywie Seveso III w celu zapewnienia lepszego przestrzegania w nich zasad bezpieczeństwa.

PRZEPISY UE W POLSCE

Wejście Polski do Unii Europejskiej wiązało się m.in. z implementacją do prawa polskiego dyrektywy Seveso II, a obecnie Seveso III. Jej treść została wdrożona do tytułu IV ustawy z dnia 27 kwietnia 2001 r. – Prawo ochrony środowiska (Dz.U. z 2001 r. Nr 62, poz. 627), a treść jej załączników do odpowiednich aktów wykonawczych. Przepisy dyrektywy SEVESO III nie mają zastosowania m.in. do: instalacji i urządzeń podległych MON, transportu drogowego, kolejowego, morskiego i powietrznego, składowisk odpadów, zagrożeń spowodowanych promieniowaniem jonizującym generowanym przez substancje, wydobywania kopalin, transportu niebezpiecznych substancji rurociągami.

ZAPISY DYREKTYWY SEVESO

W dyrektywie SEVESO III wprowadzono definicje:

- zakładu o zwiększonym ryzyku ZZR,
- zakładu o dużym ryzyku ZDR.

Oznaczają one zakłady, w których znajdują się substancje niebezpieczne w ilościach co najmniej równych wartościom wyszczególnionym w odpowiednich kolumnach załącznika 1 (część 1 i 2).

Dla poszczególnych substancji oraz kategorii substancji ustalono dwie wartości progowe – mniejszą i większą, kwalifikujące instalację niebezpieczną / zakład odpowiednio do kategorii ZZR lub ZDR. Tak więc zasada kwalifikowania zakładu jako ZZR czy ZDR uzależniona jest od rodzajów oraz ilości magazynowanych substancji.

POZIOM RYZYKA ZAKŁADU

Określenie rodzajów i ilości znajdujących się w zakładzie substancji niebezpiecznych, decydujących o zaliczaniu zakładu o zwiększonym lub dużym ryzyku wystąpienia poważnej awarii, zostało przeniesione do prawa krajowego rozporządzeniem ministra rozwoju z dnia 29 stycznia 2016 r. w sprawie rodzajów i ilości znajdujących się w zakładzie substancji niebezpiecznych, decydujących o zaliczeniu zakładu do takiego o zwiększonym lub dużym ryzyku wystąpienia poważnej awarii przemysłowej (Dz.U. z 2016 r., poz. 138).

W rozporządzeniu ustalono kryteria kwalifikacyjne w formie zbioru zasad postępowania oraz dwa wykazy niebezpiecznych substancji chemicznych wraz z granicznymi ilościami tych substancji (wartościami progowymi). Kryteria wskazano poniżej.

- Wykaz kategorii substancji stwarzających zagrożenia – Tabela 1. Rodzaje i ilości substancji niebezpiecznych z uwzględnieniem kryteriów kwalifikowania ich do kategorii substancji stwarzających zagrożenia. Obejmuje on 4 działy: zagrożenia dla zdrowia (Dział H), zagrożenia fizyczne (Dział P), zagrożenia dla środowiska (Dział E) oraz zagrożenia pozostałe (Dział O).

- Nazwy substancji niebezpiecznych – Tabela 2. Rodzaje i ilości substancji niebezpiecznych z uwzględnieniem ich nazw i oznaczeń numerycznych. Jest to wykaz substancji i grup substancji, dla których z różnych względów ustalono określone wartości progowe, odmienne od przypisanych kategorii, do której dana substancja została zaklasyfikowana.

Należy przy tym zaznaczyć, że wartości progowe zamieszczone w tabeli 2 (szczególne substancje – wyjątki) są nadrzędne wobec wartości progowych podanych w tabeli 1 (kategorie).

Gdy maksymalne ilości poszczególnych substancji niebezpiecznych, które mogą znajdować się na terenie zakładu nie przekraczają wartości podanych w tabelach 1 i 2 ww. rozporządzenia, należy podczas zaliczania zastosować procedurę sumowania, na podstawie której zakład zostanie zakwalifikowany do jednej z dwóch kategorii.

OKREŚLANIE KATEGORII RYZYKA

Sumowanie i zaliczanie zakładu do kategorii zwiększonego lub dużego ryzyka polega na przeprowadzeniu prostych działań z uwzględnieniem wszystkich grup substancji niebezpiecznych wg poniższych wzorów.

Dla zakładu zwiększonego ryzyka ZZR:

$$\frac{\text{ilość substancji 1}}{\text{wartość progowa ZZR dla substancji 1}} + \frac{\text{ilość substancji 2}}{\text{wartość progowa ZZR dla substancji 2}} + \ldots\ldots \geq 1$$

Dla zakładu zwiększonego ryzyka ZDR:

$$\frac{\text{ilość substancji 1}}{\text{wartość progowa ZDR dla substancji 1}} + \frac{\text{ilość substancji 2}}{\text{wartość progowa ZDR dla substancji 2}} + \ldots\ldots \geq 1$$

Jeżeli otrzymany wynik jest równy lub większy od 1, dany zakład należy zaliczyć do kategorii o zwiększonym lub dużym ryzyku (ZZR lub ZDR) wystąpienia poważnej awarii przemysłowej.

WYKLUCZENIA

W pkt 11 preambuły do dyrektywy Seveso III podkreśla się, że wprowadzenie nowej kwalifikacji substancji niebezpiecznych może mieć niepożądane skutki, tj. rygorom dyrektywy będą podlegały zakłady, które nie powodują zagrożenia wystąpienia awarii przemysłowej. W związku z tym przyjęto mechanizm proceduralny umożliwiający wykluczenie danej substancji z wykazu substancji niebezpiecznych.

Procedura jest uruchamiana na wniosek państwa członkowskiego. Do wniosku dołącza się odpowiednie uzasadnienie niezbędne do oceny możliwości spowodowania przez substancję niebezpieczną obrażeń fizycznych oraz szkód dla zdrowia i środowiska. Ostatecznie o wyłączeniu danej substancji z wykazu decydują Parlament i Rada Europejska w trybie zmiany dyrektywy.

KWALIFIKOWANIE ZAKŁADÓW

Zakłady o dużym ryzyku wystąpienia poważnej awarii to nie tylko te, które magazynują i przetwarzają substancje chemiczne o właściwościach toksycznych, wybuchowych i palnych. To również zakłady np. separacji powietrza (ASU) wytwarzające i magazynujące czyste gazy utleniające oraz mieszaniny gazów o potencjale OP (Oxidising Power) powyżej 23,5%, a także zaliczane do gazów utleniających.

Dyrektywa Seveso III nałożyła również na państwa członkowskie obowiązek wprowadzenia zmian polegających na dodaniu oleju opałowego ciężkiego do grupy substancji ropopochodnych. Ten dodatkowy termin wynikał z faktu kwalifikowania oleju opałowego ciężkiego jako substancji stwarzającej zagrożenie dla środowiska wodnego, dla którego są przypisane ostrzejsze wartości progowe (zakład o zwiększonym ryzyku: 200 Mg, zakład o dużym ryzyku: 500 Mg), niż jak to jest w przypadku substancji ropopochodnych.

Dyrektywa Seveso III wprowadza definicję zakładu sąsiedniego. Rozumie się przez to każdy zakład zlokalizowany w takiej odległości od innego zakładu, która zwiększa prawdopodobieństwo i skutki awarii.

LOKALIZACJE ZAKŁADÓW

Według wykazu Głównego Inspektora Ochrony Środowiska z dnia 31 grudnia 2020 r. w Polsce zlokalizowanych jest 195 zakładów dużego ryzyka ZDR i – 273 zakłady zwiększonego ryzyka ZZD. Rozmieszczenie zakładów z podziałem na województwa zaznaczono na mapie.

OBOWIĄZKI ZAKŁADÓW

Prowadzący zakład o zwiększonym ryzyku lub o dużym ryzyku jest obowiązany do zgłoszenia zakładu do Państwowej Straży Pożarnej oraz Wojewódzkiego Inspektora Ochrony Środowiska. Zgłoszenie wymagane jest również w przypadku zakończenia eksploatacji lub zamknięcia zakładu. Należy go dokonać co najmniej na 30 dni przed uruchomieniem zakładu lub jego części. Dokładnie tak samo należy postąpić w sytuacji dokonania istotnej zmiany ilości lub rodzaju substancji niebezpiecznej albo jej charakterystyki fizykochemicznej, pożarowej i toksycznej, zmiany technologii lub profilu produkcji.

Prowadzący zakład musi sporządzić PROGRAM ZAPOBIEGANIA POWAŻNYM AWARIOM PRZEMYSŁOWYM. Co najmniej raz na 5 lat program zapobiegania awariom podlega zmianom wynikającym ze zmiany stanu faktycznego, postępu naukowo-technicznego lub analizy zaistniałych awarii przemysłowych. Jeżeli prowadzący zakład o zwiększonym lub dużym ryzyku nie dokonuje zmian, to właściwy organ Państwowej Straży Pożarnej wzywa do ich dokonania

Program zapobiegania poważnym awariom przemysłowym wdrażany jest za pomocą systemu zarządzania bezpieczeństwem, gwarantującego odpowiedni do zagrożeń poziom ochrony ludzi i środowiska.

SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM oparty jest na ocenie ryzyka i stanowi element ogólnego systemu prowadzenia zakładu. W systemie zarządzania bezpieczeństwem należy uwzględnić m.in. funkcjonowanie mechanizmów umożliwiających systematyczną analizę zagrożeń awarią przemysłową oraz prawdopodobieństwa jej wystąpienia, instrukcje bezpiecznego funkcjonowania instalacji, przewidziane dla normalnej eksploatacji instalacji, a także konserwacji i czasowych przerw w ruchu. Należy zastosować najlepsze dostępne praktyki monitoringu funkcjonowania instalacji, umożliwiające podejmowanie działań korekcyjnych w przypadku wystąpienia zjawisk stanowiących odstępstwo od normalnej eksploatacji instalacji, w tym związanych ze zużyciem instalacji i korozją jej elementów.

Prowadzący zakład o dużym ryzyku dodatkowo jest obowiązany do opracowania **RAPORTU O BEZPIECZEŃSTWIE**, w którym musi m.in. wykazać, że zostały zachowane zasady bezpieczeństwa oraz reguły prawidłowego projektowania, wykonania i utrzymywania instalacji, w tym magazynów i urządzeń, oraz opracować wewnętrzny plan operacyjno-ratowniczy. Wewnętrzny plan operacyjno-ratowniczy opracowuje się na podstawie scenariuszy poważnej awarii przemysłowej wymienionych w raporcie o bezpieczeństwie dotyczących zdarzeń, w szczególności pożarów, wybuchów i emisji, charakteryzujących się najniekorzystniejszymi skutkami. Plany wewnętrzne obejmują swoim zakresem teren zakładu o dużym ryzyku wystąpienia poważnej awarii przemysłowej.

Na podstawie informacji uzyskanych od prowadzącego zakład o dużym ryzyku komendant wojewódzki Państwowej Straży Pożarnej opracowuje ZEWNĘTRZNY PLAN OPERACYJNO-RATOWNICZY DLA TERENU NARAŻONEGO NA SKUTKI AWARII PRZEMYSŁOWEJ, położonego poza zakładem o dużym ryzyku, z uwzględnieniem ewentualnych oddziaływań transgranicznych. Zewnętrzne plany operacyjno-ratownicze opracowuje się na podstawie scenariuszy zawartych w planach wewnętrznych, których skutki zdarzeń wykraczają poza teren zakładu o dużym ryzyku wystąpienia poważnej awarii przemysłowej. Zatwierdzenie zewnętrznego planu operacyjno-ratowniczego wymaga udziału społeczeństwa.

Szczegółowe wymagania dla raportu o bezpieczeństwie zakładu o dużym ryzyku określa rozporządzenie Ministra Rozwoju z dnia 23 lutego 2016 r. (Dz.U. z 2016 r. poz. 287), a dla wewnętrznego planu operacyjno-ratowniczego rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 8 czerwca 2016 r. w sprawie wymagań, jakim powinny odpowiadać plany operacyjno-ratownicze (Dz.U. z 2016 r. poz. 821). Podobnie jak w przypadku programu zapobiegania awariom, co najmniej raz na 5 lat należy dokonać analizy raportu o bezpieczeństwie i wprowadzić uzasadnione zmiany, co najmniej raz na 3 lata przeprowadzić analizę i przećwiczyć realizację planu operacyjno-ratowniczego wewnętrznego i zewnętrznego.

WSPÓŁPRACA ZAKŁADÓW

Prowadzący zakłady o zwiększonym ryzyku, o dużym ryzyku oraz niebędące zakładami o zwiększonym ryzyku lub o dużym ryzyku, które są zakładami sąsiednimi, współpracują w zakresie wzajemnego informowania się o czynnikach mogących przyczynić się do zwiększenia zagrożenia awarią przemysłową lub pogłębienia jej skutków lub powodować wystąpienie efektu domino. Komendant Wojewódzki Państwowej Straży Pożarnej, na podstawie informacji podanych przez prowadzących zakłady w zgłoszeniu lub wyników kontroli, ustala grupy zakładów, których zlokalizowanie względem siebie może spowodować efekt domina. W skład grupy zakładów mogą wchodzić te o zwiększonym ryzyku, o dużym ryzyku oraz niebędące zakładami o zwiększonym ryzyku lub o dużym ryzyku.

BEZPIECZEŃSTWO PUBLICZNE – ANALIZY UDT

Szczególna rola w zapewnieniu bezpieczeństwa w zakładach dużego i zwiększonego ryzyka przypada Urzędowi Dozoru Technicznego.

W ramach działań ustawowych dozorem technicznym objęte są czynności zmierzające do zapewnienia bezawaryjnego funkcjonowania urządzeń technicznych, które prowadzą do zapewnienia bezpieczeństwa publicznego. Wykonywanie inspekcji urządzeń ciśnieniowych i bezciśnieniowych oraz rurociągów technologicznych podnosi poziom ochrony zakładów. Ale to tylko jedna z dziedzin, w której uczestniczy Urząd Dozoru Technicznego. Działamy też w szeroko rozumianych ekspertyzach technicznych. Badania diagnostyczne i ekspertyzy z zakresu bezpieczeństwa pracy urządzeń technicznych i instalacji podnoszą poziom bezpieczeństwa, minimalizując ryzyko związane z ich eksploatacją poprzez wskazywanie najistotniejszych obszarów ryzyka lub najefektywniejszych sposobów jego redukcji.

Szczególnie bliskie dyrektywie Seveso są ekspertyzy techniczne w zakresie analizy zagrożeń i oceny ryzyka.

PHA (Preliminary Hazard Analysis) – Wstępna Analiza Zagrożeń
HAZOP (Hazard and Operability Studies) – Analiza Zagrożeń i Zdolności Operacyjnych
C-HAZOP (Control Hazard and Operability Studies) – Analiza Zagrożeń i Zdolności Operacyjnych Automatyki
LOPA (Layer of Protection Analysis) – Analiza Warstw Zabezpieczeń
FTA (Fault Tree Analysis) – Analiza Drzewa Błędów
ETA (Event Tree Analysis) – Analiza Drzewa Zdarzeń
SIL (Safety Integrity Level) – Poziom Nienaruszalności Bezpieczeństwa
FSA (Functional Safety Assessment) – Ocena Bezpieczeństwa Funkcjonalnego
FMEA (Failure Mode and Effects Analysis) – Analiza Rodzajów Błędów oraz ich Skutków
RBI (Risk Based Inspection) – Planowanie Inspekcji na podstawie Analizy Ryzyka

Niektóre z nich postaramy się omówić w następnych wydaniach „Inspektora".

ZARZĄDZANIE BEZPIECZEŃSTWEM PROCESOWYM ORAZ INTEGRALNOŚCIĄ MECHANICZNĄ

MAPA BEZPIECZEŃSTWA

MGR INŻ. TOMASZ KLINKOSZ

Ekspert Urządzeń Ciśnieniowych
Dział Oceny Zgodności
Oddział w Gdańsku
Urząd Dozoru Technicznego

ZAKŁADY CHEMICZNE ORAZ PRZEMYSŁU RAFINERYJNEGO I PETROCHEMICZNEGO TO JEDEN Z ISTOTNYCH ELEMENTÓW WSPÓŁCZESNEJ GOSPODARKI, NIE TYLKO POLSKIEJ, ALE KAŻDEGO PAŃSTWA ROZWINIĘTEGO. OBECNIE WCIĄŻ ROPA NAFTOWA WYKORZYSTYWANA W WIELU GAŁĘZIACH PRZEMYSŁU POZOSTAJE GŁÓWNYM SUROWCEM [1]. TA WŁAŚNIE GAŁĄŹ PRZEMYSŁU Z UWAGI NA SWOJĄ ISTOTNĄ ROLĘ SPOŁECZNĄ KONCENTRUJE ZAKŁADY NALEŻĄCE DO TZW. INFRASTRUKTURY KRYTYCZNEJ [2]. Obejmuje również zakłady, które klasyfikowane są wg dyrektywy 2012/18/UE, tzw. dyrektywy SEVESO, jako zakłady dużego ryzyka [3] z uwagi na zagrożenia związane z przetwarzaniem lub magazynowaniem znacznych ilości substancji, które w przypadku niekontrolowanego uwolnienia mogą stwarzać zagrożenia dla otoczenia.

Zapewnienie ciągłości działania tak złożonego procesu, jakim jest zakład przemysłowy przerobu ropy naftowej, wymaga koordynacji i przepływu informacji pomiędzy komórkami złożonej struktury organizacyjnej. Elementem nieodłącznym zapewnienia ciągłości działania jest zapewnienie bezpieczeństwa, którego wymagania zawarto między innymi w normie PN-EN ISO 22301 [4]. W odniesieniu do ciągłości działania zakładu przemysłowego, w którym głównymi procesami wymagającymi zapewnienia ciągłości działania są instalacje przemysłowe przetwarzające niebezpieczne substancje chemiczne, takie jak ropa naftowa i produkty jej przerobu, inherentnymi elementami są tzw. bezpieczeństwo procesowe oraz zarządzanie tym bezpieczeństwem.

ROZWÓJ BEZPIECZEŃSTWA PROCESOWEGO

Początki rozwoju bezpieczeństwa procesowego sięgają lat dwudziestych XX w. Wraz z postępem industrializacji i technologii zaczął kształtować się wzór sporadycznych katastrof. W 1921 r. w zakładach BASF w Oppau w Niemczech eksplozja zniszczyła fabrykę, zabijając co najmniej 430 osób i uszkadzając około 700 pobliskich domów. Do eksplozji doprowadziła mieszanina siarczanu amonu i amonu w proporcjach 50/50 [5]. W 1947 r. w pożarze i eksplozji w Texas City w Teksasie na terenie SS Grandcamp firmy Monsanto Chemical Company w pożarze i eksplozji podczas załadunku nawozu na bazie azotanu amonu zginęło ponad 430 osób.

W tamtym czasie nie było konkretnej reakcji legislacyjnej na te incydenty. Jednak prawdopodobnie to katastrofa w Flixborough (1974 r.) jest uważana za początek tego, co obecnie nazywa się zarządzaniem bezpieczeństwem procesowym.

Bezpieczeństwo procesowe: ochrona osób i mienia przed sporadycznymi i katastroficznymi zdarzeniami, które mogą wynikać z nieplanowanych lub nieoczekiwanych odchyleń w warunków procesu.

Zarządzanie bezpieczeństwem procesów: zastosowanie systemów zarządzania do identyfikacji, zrozumienia i kontroli zagrożeń procesowych w celu zapobiegania incydentom i urazom związanym z procesem.

Systemy zarządzania bezpieczeństwem procesowym: kompleksowe zestawy polityk, procedur i praktyk opracowane w celu zapewnienia, że warstwy zabezpieczające przed sporadycznymi i katastroficznymi zdarzeniami są używane i skuteczne.

Rys. 1. Schemat i systematyka dotycząca zarządzania procesowego [6]

Eksplozja i pożar w zakładzie Phillips Petrochemical, które nastąpiły w październiku 1989 r. w pobliżu Houston w Teksasie (zginęły 24 osoby, a kolejne 128 zostało rannych), bezpośrednio przyczyniły się do wprowadzenia regulacji.

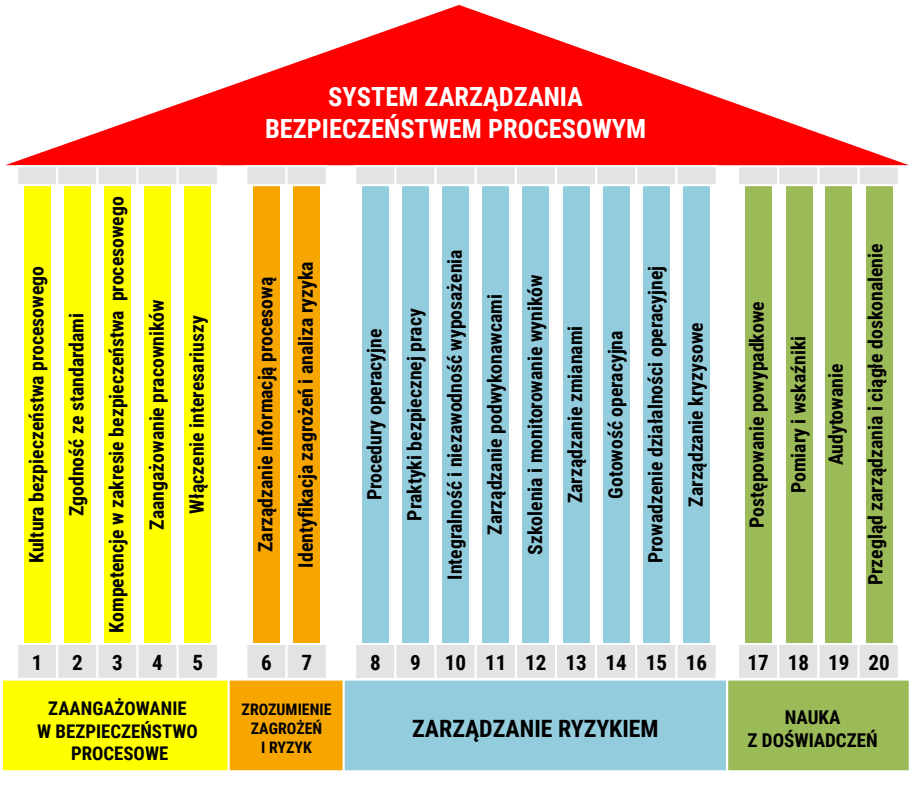
W dniu 17 lipca 1990 r. OSHA (Occupational Safety and Health Administration) opublikowała w Rejestrze Federalnym (55 FR 29150) proponowaną normę, „Zarządzanie bezpieczeństwem procesowym wysoce niebezpiecznych substancji chemicznych", zawierającą wymagania dotyczące zarządzania zagrożeniami związanymi z procesami wykorzystującymi wysoce niebezpieczne chemikalia, aby zapewnić bezpieczeństwo i zdrowie w miejscu pracy.

Do dziś wytyczne OSHA 1910.119 Process safety management of highly hazardous chemicals [7] stanowią rekomendowaną dobrą praktykę inżynierską i podstawę dla tworzenia wielu systemów zarządzania bezpieczeństwem procesowym na świecie.

BEZPIECZEŃSTWO PROCESOWE DZISIAJ

Obecnie wiodącą rolę w zakresie kreowania standardów i wyznaczania najlepszej dostępnej praktyki w zakresie zarządzania bezpieczeństwem procesowym pełni CCPS (Center for Chemical Process Safety), będąca organizacją non-profit, członkowską w ramach AIChE (The Global Home of Chemical Engineers), która identyfikuje i zaspokaja potrzeby w zakresie bezpieczeństwa procesowego dla różnych obiektów związanych z obsługą, przechowywaniem, wykorzystaniem lub przetwarzaniem oraz transportem materiałów niebezpiecznych [8].

Dzisiaj stosuje się wiele modeli służących do strukturyzowania systemu zarządzania bezpieczeństwem procesowym. Jednym z najpopularniejszych jest pochodzący z wytycznych CCPS model opierający się na czterech fundamentach i dwudziestu filarach. Struktura systemu zarządzania bezpieczeństwem procesowym (rys. 2) oparta jest na ryzyku wg CCPS, tzw. RBPS Risk Based Process Safety.



Rys. 2. Struktura systemu zarządzania bezpieczeństwem procesowym wg CCPS [9]

Proces zarządzania ryzykiem stanowi fundament dla kluczowych pod kątem bezpieczeństwa procesów wpływających na utrzymanie sprawnego systemu zarządzania bezpieczeństwem procesowym. Powyższy model można zatem wskazywać jako zasadny, również patrząc przez pryzmat wymagań ustawy o ochronie środowiska wdrażającej do polskiego systemu prawnego wspomnianą dyrektywą SEVESO.

Prowadzący zakład o zwiększonym ryzyku lub zakład o dużym ryzyku jest obowiązany do **opracowania i wdrożenia systemu zarządzania bezpieczeństwem**, gwarantującego odpowiedni do zagrożeń poziom ochrony ludzi i środowiska, stanowiącego element ogólnego systemu zarządzania zakładem [3].

System zarządzania bezpieczeństwem ma uwzględniać zagrożenia awariami przemysłowymi i złożoność organizacji w zakładzie oraz **opierać się na ocenie ryzyka [10].**

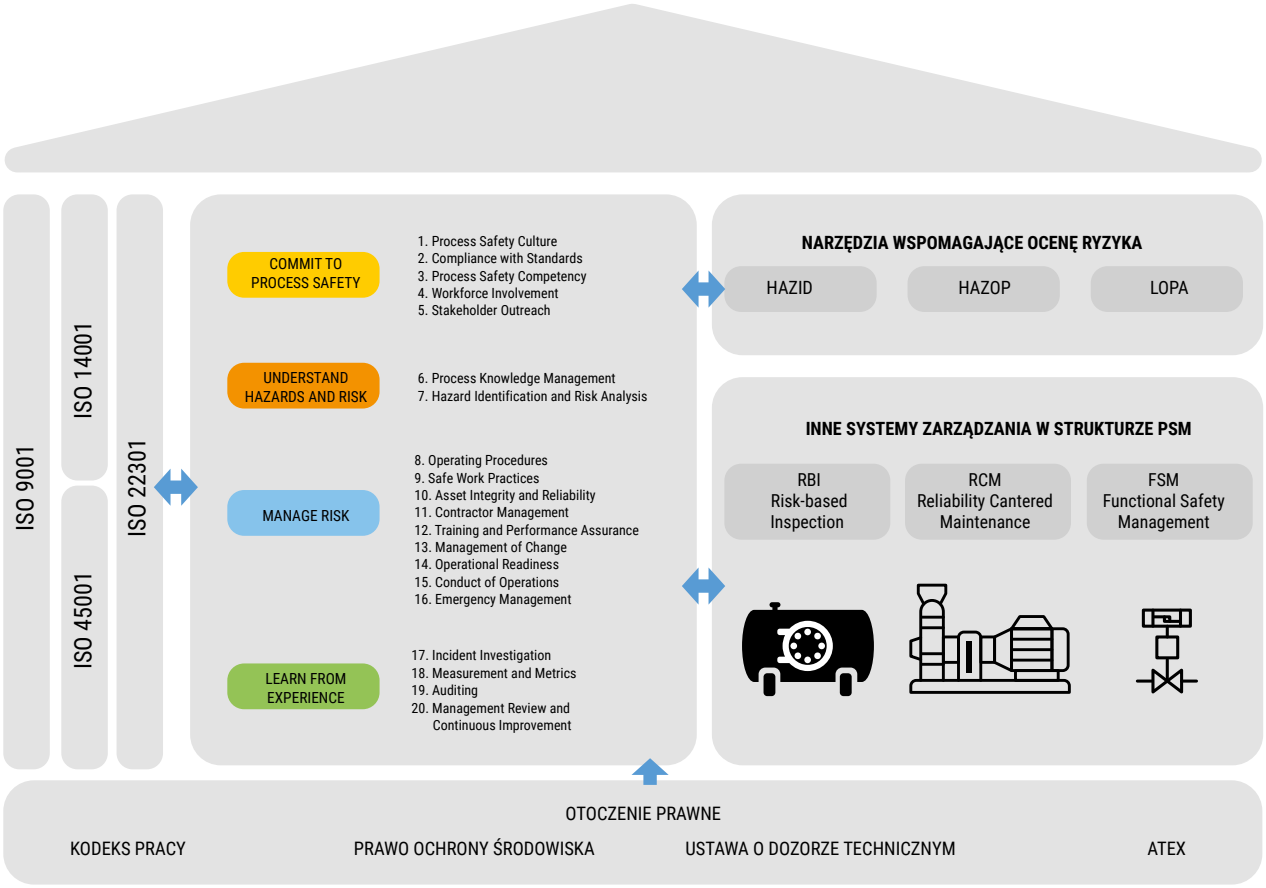
PRZYPOMNIJMY DEFINICJĘ OCENY RYZYKA.

Jest to całościowy proces składający się z identyfikacji ryzyka, analizy ryzyka oraz ewaluacji ryzyka.

Wynika z tego, że każdy z elementów systemu zarządzania bezpieczeństwem procesowym powinien opierać się na procesie oceny ryzyka. Chcąc sprostać takiemu wymaganiu, należy nie tylko zastosować właściwe narzędzia do identyfikacji i analizy ryzyk, ale również wdrożyć procesy umożliwiające przepływ informacji pomiędzy nimi.

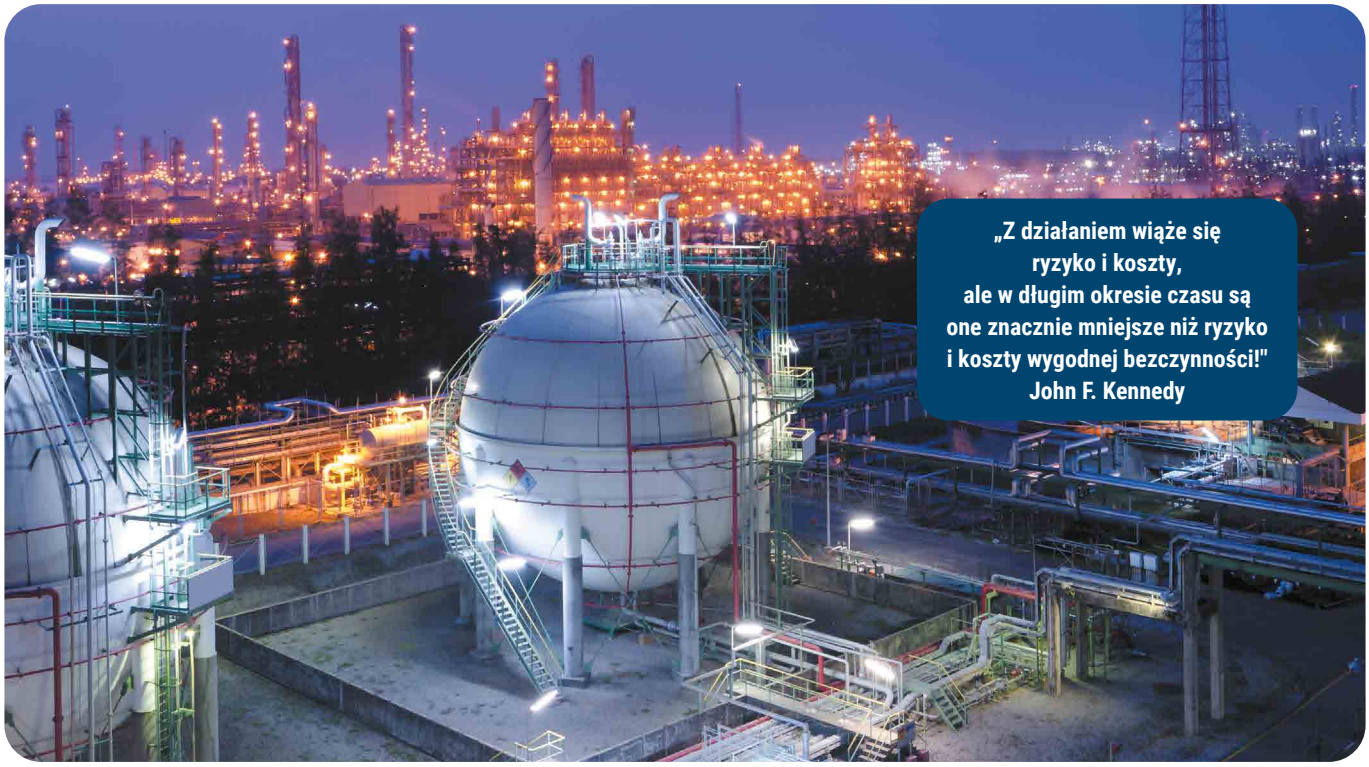
Zdarza się jednak, że w wyniku braku dostatecznego przepływu informacji zarządzanie wnioskami płynącymi z prowadzonych analiz ryzyka oceniane jest odrębnie, co skutkować może podejmowaniem nieefektywnych decyzji w procesie postępowania z ryzykiem.

System zarządzania bezpieczeństwem procesowym nie może istnieć w oderwaniu od innych procesów zarządczych w organizacji, szczególnie tych, w których wykorzystuje się procesy oceny ryzyka lub które mają na nie wpływ. Skuteczne wdrożenie i utrzymanie systemu zarządzania bezpieczeństwem procesowym wymaga szerszego spojrzenia również przez pryzmat tych systemów. Należy także mieć na uwadze przepisy prawne, które mogą zawierać dodatkowe wymagania i kształtować tym samym konstrukcję systemu. Przykładowe relacje pomiędzy otoczeniem systemu PSM a otoczeniem można przedstawić schematycznie (rys. 3).



Rys. 3. Zależność systemu zarządzania bezpieczeństwem procesowym od otoczenia i innych systemów zarządzania związanych z ryzykiem

Zwróćmy uwagę, że w ramach wyszczególnionych obszarów w strukturze systemu PSM mogą znajdować się inne systemy zarządzania specyficznymi obszarami związanymi z bezpieczeństwem. Takim przykładem, pokazanym na rysunku nr 2, są system planowania inspekcji urządzeń ciśnieniowych z wykorzystaniem analizy ryzyka RBI (Risk-based Inspection) czy w zakresie maszyn stosowane często podejście oparte na RCM (Reliability Centered Maintenance) oraz system zarządzania bezpieczeństwem funkcjonalnym FSM (Functional Safety Management).



W każdym z systemów znajdują się obszary, które wymagają zintegrowania w ramach PSM, jak również w celu zapewnienia ich skutecznego funkcjonowania wymagają skutecznego przepływu informacji pomiędzy systemami, np. w procesie zarządzania zmianami MOC (Management of Change), który w zależności od okoliczności, rodzaju zidentyfikowanej zmiany może wywołać skutek i konieczność podjęcia odpowiednich działań.

ANALIZA PRZYPADKU

Rozważmy przypadek, w którym zmianie ulega skład surowca lub wprowadzana jest dodatkowa substancja chemiczna przetwarzana w instalacji. Może to mieć wpływ na szereg procesów w organizacji.

- Jeśli organizacja posiada wdrożone systemy (rys. 3), to niezbędne może być przeprowadzenie **analizy zagrożeń** z zastosowaniem odpowiedniego narzędzia, np. HAZOP.
- W wyniku analizy może zaistnieć konieczność zmiany układów **automatyki zabezpieczającej** lub wymagań dla ich testów funkcjonalnych.
- To powinno z kolei uruchomić odpowiednie działania w ramach wdrożonego **systemu zarządzania bezpieczeństwem funkcjonalnym**.

Zmiana składu medium może powodować również zmianę aktywności **mechanizmów degradacji** mających wpływ na integralność mechaniczną wyposażenia produkcyjnego. Zależnie od zidentyfikowanych obszarów narażenia może to wymuszać działania w ramach procesu **RBI oraz RCM** wpływać na strategię **zarządzania niezawodnością** urządzeń objętych tymi systemami.

Należy również zapewnić dwukierunkowy **przepływ informacji**, ponieważ w ww. procesach generowane są dane, które mogą mieć znaczenie w przyjmowanych założeniach w analizach prowadzonych w innych obszarach.

Jako charakterystyczny przykład może posłużyć **wynik analizy RBI**, w której otrzymujemy wartość prawdopodobieństwa wystąpienia rozszczelnienia wyposażenia produkcyjnego, takiego jak zbiornik czy rurociąg w wyniku oddziaływania mechanizmów degradacji, jak również dane o wielkości skutków wycieku substancji chemicznej w takim przypadku.

Takie informacje stanowią doskonałe źródło danych dla prowadzonych analiz zagrożeń oraz ryzyka procesowego i pozwalają na dokładniejsze oszacowanie ryzyka i podejmowanie decyzji obarczonych mniejszą niepewnością.

Proces wprowadzenia zmiany może wymagać również formalnego włączenia jednostki dozoru technicznego w przypadku wystąpienia zmiany w instalacji technologicznej mającej wpływ na bezpieczeństwo lub w przypadku modernizacji urządzenia ciśnieniowego lub automatyki zabezpieczającej, co dodatkowo wymaga uzgodnienia [11].

BEZPIECZNA CIĄGŁOŚĆ DZIAŁANIA

Wdrożenie skutecznego i efektywnego sytemu zarządzania bezpieczeństwem procesowym, który przyczynia się do zapewnienia ciągłości działania zakładu produkcyjnego, wymaga głębokiej integracji wdrożonych w organizacji systemów oraz wzmocnienia i integracji procesów oceny ryzyka, w tym również przeglądu i standaryzacji kryteriów jego akceptacji. Wymaga to również wzmocnienia procesu zarządzania zmianami, w tym stworzenia struktur przepływu informacji wewnątrz organizacji. Ostatnimi elementami, bez których utrzymanie systemu nie jest możliwe, są ciągłe doskonalenie, zarządzanie wiedzą, w tym kompetencjami.

Literatura:

1. https://raport.togetair.eu/ogien/energia-przyszlosci/rafinerie-przyszlosc-i-kierunki-rozwoju-branzy-wobec-wyzwan-nowego-zielonego-ladu
2. https://www.gov.pl/web/rcb/systemy-infrastruktury-krytycznej
3. Dyrektywa 2012/18/UE w sprawie kontroli zagrożeń poważnymi awariami związanymi z substancjami niebezpiecznymi,
4. PN-EN ISO 22301 Bezpieczeństwo i odporność. Systemy zarządzania ciągłością działania – wymagania.
5. Murray Macza, ACM Automation Inc. – Canada, A Canadian Perspective of the History of Process Safety Management Legislation, 8th Internationale Symposium Programmable Electronic System in Safety-Related Applications September 2 – 3, 2008, Cologne, Germany.
6. Guidelines for Auditing Process Safety Management Systems, Center for Chemical Process (CCPS), Safety 2011.
7. https://www.osha.gov/laws-regs/regulations/standardnumber/1910/1910.119
8. https://www.aiche.org/ccps
9. CCPS Guidelines for Auditing Process Safety Management Systems, second edition.
10. Ustawa z dnia 27 kwietnia 2001r. - Prawo ochrony środowiska, Dz.U. z 2001 r. Nr 62, poz. 627.
11. PN-ISO 31000:2018 Zarządzanie ryzykiem. Wytyczne.
12. Rozporządzenie Ministra Rozwoju i Technologii z dnia 17 grudnia 2021 r. w sprawie warunków technicznych dozoru technicznego dla niektórych urządzeń ciśnieniowych podlegających dozorowi technicznemu.

BEZPIECZEŃSTWO PROCESOWE

KOMPLEKSOWA OFERTA UDT-CERT

- analizy zagrożeń i oceny ryzyka
- analizy niezawodności układów bezpieczeństwa
- certyfikacja systemu zarządzania bezpieczeństwem funkcjonalnym FSM (Functional Safety Management)

POBIERZ WYTYCZNE UDT

PROWADZENIE ANALIZ I OCENA RYZYKA INSTALACJI PROCESOWYCH

MGR INŻ. JACEK ŻACZYŃSKI
Ekspert Urządzeń 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 PRZEDE 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 materiałów 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 dioksyn (2,3,7,8-tetrachlorodibenzodioksyny, 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.

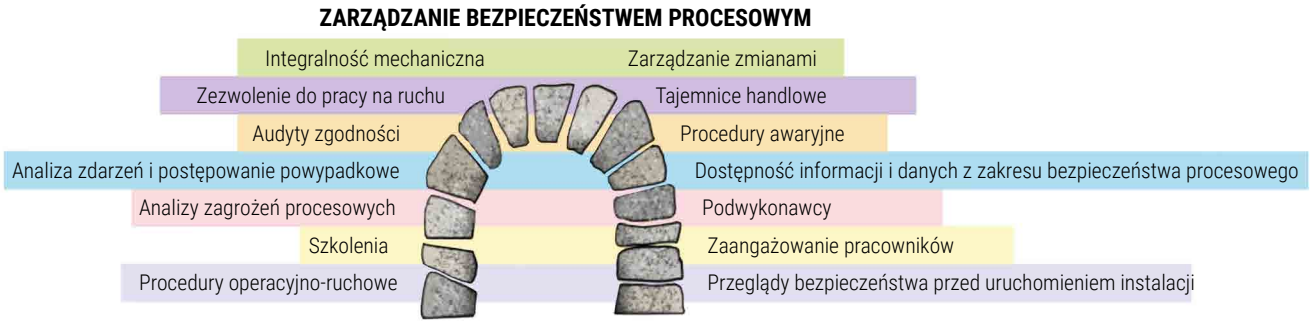
W wyniku awarii w Seveso ewakuowano 730 osób, około 700 mieszkańców zostało poszkodowanych w wyniku zatrucia, wiele zwierząt zginęło, tereny licznych w tym regionie przedsiębiorstw zostały skażone (ok. 40 zakładów), a wielkie obszary na wiele lat (ok. 10) z powodu skażenia wyłączono z gospodarki rolnej.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

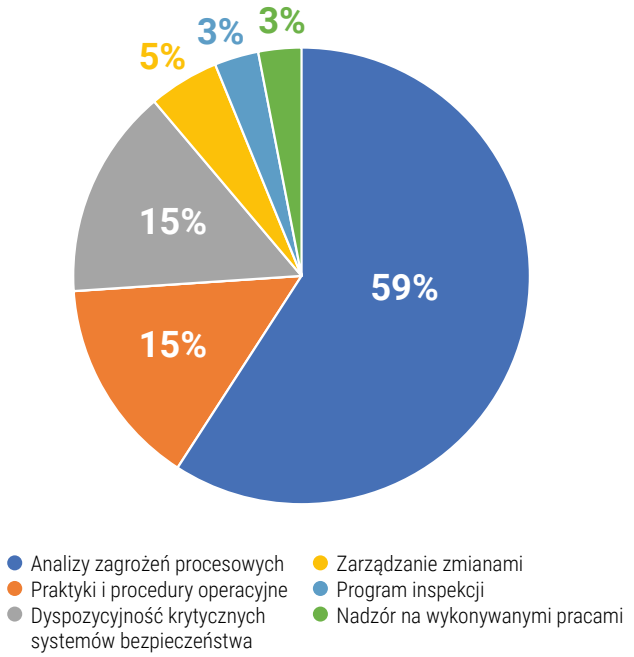
Jednym filarów skutecznego systemu zarządzania bezpieczeństwem procesowym jest odpowiedni program identyfikacji zagrożeń i analizy ryzyka. Zakłada on, że osiągnięcie bezpieczeństwa na odpowiednim akceptowalnym poziomie wymaga zastosowania wielu różnych analiz zależnych od:
1. rodzaju koniecznych do uzyskania wyników,
2. rodzaju dostępnych informacji (dostępność oraz jakość dokumentacji),
3. zasobów przeznaczonych na ten cel.

ROLA ANALIZY ZAGROŻEŃ 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 wydobyciem 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 ZAGROŻEŃ 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 jakiejkolwiek 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.

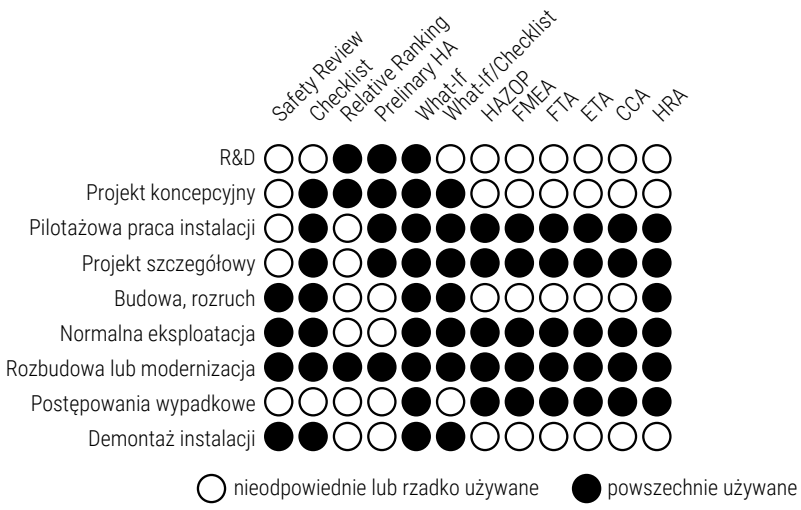
Do pierwszego trybu pracy odpowiednią metodą wydaje się tradycyjny HAZOP, a w przypadku pracy okresowej tzw. Batch-HAZOP. Podczas prac związanych z korzystaniem z odpowiednich procedur, np. podczas rozruchu, tradycyjny HAZOP nie sprawdzi się, należały w tym przypadku zastosować HAZOP proceduralny.

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.

Audytowalność

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
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 kliku 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 kołnierzowo-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.

UWAGA

Jeżeli zbiornik nie był odpowiednio kontrolowany, konserwowany, a jego stan techniczny jest nieznany, wówczas nie powinniśmy stosować wymienionych założeń (tabela).

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 wcześnie 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 wybucha łatwo. Konsekwencje, a tym samym ryzyko, zostałyby zatem niedoszacowane, a IPL, które obecnie uważamy za konieczne, uznano by za przesadę.

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

Podejmowanie decyzji o odpowiedniości 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

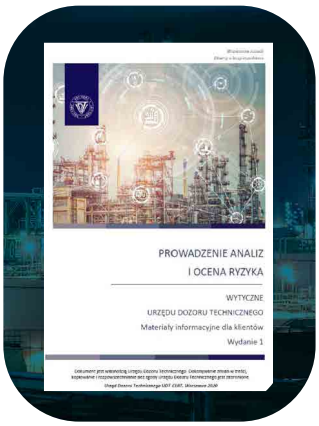
Jak wynika z przykładów przytoczonych powyżej, na osoby i zespoły wykonujące analizy zagrożeń i ryzyka czyha wiele pułapek. Czasami ze względu na małe doświadczenie prowadzącego, a czasami z powodu niewystarczających kompetencji lub ich braku wyniki analiz pozostawiają wiele do życzenia.

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 ŚWIETLE 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, 3nd 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

RACJONALNE PODEJŚCIE DO ZARZĄDZANIA RYZYKIEM ZASADA ALARP – ASPEKT PRAWNY

CZĘŚĆ I

R. PR. MATEUSZ ŁUKASZCZYK

Starszy Specjalista
Oddział w Poznaniu
Urząd Dozoru Technicznego
Doktorant wdrożeniowy
Uniwersytet im. Adama Mickiewicza
w Poznaniu

DR INŻ. MARCIN WOŁEJKO

Centrum Kompetencyjne ds. Automatyki
Departament Innowacji i Rozwoju
Urząd Dozoru Technicznego

PRAWA I WOLNOŚĆ JEDNOSTKI, W TYM PRAWO I WOLNOŚĆ DO PODEJMOWANIA DZIAŁALNOŚCI GOSPODARCZEJ, MOGĄ BYĆ OGRANICZANE WÓWCZAS, GDY JEST TO KONIECZNE W DEMOKRATYCZNYM PAŃSTWIE PRAWNYM DLA JEGO BEZPIECZEŃSTWA, DLA OCHRONY ŚRODOWISKA, ZDROWIA ALBO WOLNOŚCI I PRAW INNYCH JEDNOSTEK. WOLNOŚĆ JEDNEJ JEDNOSTKI NIE MOŻE NARUSZAĆ WOLNOŚCI INNEJ, DLATEGO WOLNOŚĆ LUB DOBRO JEDNEGO MUSZĄ BYĆ RÓWNOWAŻONE WOLNOŚCIĄ LUB DOBREM DRUGIEGO.

- Jak to wyważyć?
- Jak mądrze ocenić relację pomiędzy poszczególnymi wolnościami lub dobrami?
- Jak np. ustalić właściwą proporcję pomiędzy prawem przedsiębiorcy do wytwarzania i sprzedawania urządzeń technicznych lub prawem do budowy instalacji przemysłowej a prawem innych osób do ochrony życia, zdrowia, mienia i środowiska, dla których takie urządzenia czy instalacje stwarzają ryzyko?

Nie istnieje bezpieczeństwo absolutne, ponieważ ograniczają je możliwości techniczne, finansowe, organizacyjne czy logistyczne danego projektu.

W sukurs przychodzi tutaj znana w systemie anglosaskim, a przyjęta m.in. w prawie brytyjskim, zasada ALARP wyrażająca racjonalne oraz proporcjonalne podejście do zarządzania ryzykiem w systemach bezpieczeństwa.

Zasada racjonalnego podejścia do zarządzania ryzykiem znana jest w języku angielskim pod kilkoma skrótami.

ALARP (*as low as reasonably practicable;* tak nisko jak to rozsądnie/racjonalnie wykonalne)

ALARA (*as low as reasonably achievable*; tak nisko jak to rozsądnie/racjonalnie osiągalne)

SFAIRP (*so far as is reasonably practicable*; tak daleko jak to rozsądnie/racjonalnie wykonalne).

Zakłada ona, że **bezpieczeństwo należy zapewnić tak dalece, a ryzyko ograniczyć do tak niskiego poziomu, jak to jest możliwe w granicach zdrowego rozsądku, przy uwzględnieniu innych czynników, takich jak czas, pieniądze i poziom techniki.**

Stosowanie zasady ALARP i posiadanie dokumentacji ALARP może stanowić dowód zapewnienia bezpieczeństwa rozstrzygający wątpliwości, jakie mogą powstawać przy ocenie zastosowanych rozwiązań technicznych i organizacyjnych w kontekście obowiązujących przepisów prawa.

W pierwszej części artykułu wyjaśniamy pojęcia: zagrożenie, ryzyko, ocena ryzyka oraz przybliżamy następujące zagadnienia:

- **podstawa prawna oceny ryzyka,**
- **kryteria akceptowalności ryzyka,**
- **stosowanie zasady ALARP, w tym pojęcie *reasonably practicable*,**
- **podstawa prawna ALARP w dyrektywie PED 2014/68/UE,**
- **wyrok ETS z dnia 14 czerwca 2007 r. (w sprawie C/127/05) dotyczący zasady ALARP.**

ZASADĘ ALARP NALEŻY STOSOWAĆ, UWZGLĘDNIAJĄC WYMAGANIA PRAWNE, NORMATYWNE ORAZ DOBRĄ PRAKTYKĘ INŻYNIERSKĄ.
Możemy ją odnaleźć w przepisach prawa dotyczących projektowania i wytwarzania urządzeń ciśnieniowych i zespołów urządzeń ciśnieniowych (dyrektywa ciśnieniowa PED 2014/68/UE). Wprowadzono ją także do norm europejskich z zakresu bezpieczeństwa czy bezpieczeństwa funkcjonalnego. Była także przedmiotem rozstrzygnięcia Trybunału Sprawiedliwości Unii Europejskiej (dalej ETS) w 2007 roku.

BEZPIECZEŃSTWO

Realne zapewnienie bezpieczeństwa wymaga wykonania odpowiedniej **analizy zagrożeń i oceny ryzyka oraz podjęcia decyzji o postępowaniu z ryzykiem.**

BEZPIECZEŃSTWO POWINNO ZOSTAĆ ZAPROJEKTOWANE

Nie da się (czytaj: jest bardzo kosztowne) zapewnić bezpieczeństwa bez jego zaprojektowania, podobnie jak „nie da się" zaprojektować bezpieczeństwa bez przeprowadzenia analizy zagrożeń i oceny ryzyka z nim związanego. Należy także odpowiednio dobierać metody analizy do przedmiotu analizy oraz do etapu realizacji inwestycji.

ZAGROŻENIA A RYZYKA – DEFINICJE

Bezpieczeństwo jest definiowane przez zagrożenia i ryzyka z nimi związane. Przepisy prawne posługują się zamiennie różnymi terminami, np.: „zagrożenie", „niebezpieczeństwo", „ryzyko", w celu ochrony tych samych wartości (życia, zdro-

wia, mienia lub środowiska) oraz osiągnięcia tego samego celu – zapewnienia bezpieczeństwa.

Wobec tego spróbujmy przyjąć jednolite, szerokie znaczenie wymienionych terminów.

ZAGROŻENIE (NIEBEZPIECZEŃSTWO) to potencjalne źródło szkody dla życia, zdrowia, mienia lub środowiska

RYZYKO to możliwość wystąpienia szkody dla życia, zdrowia, mienia lub środowiska rozumiana jako połączenie prawdopodobieństwa wystąpienia szkody oraz wagi tej szkody

Powyższe rozumienie zagrożeń i ryzyka może być traktowane jako wspólne dla wszystkich regulacji prawnych mających na celu zapewnienie bezpieczeństwa i traktujących o ocenie ryzyka.

Ciekawe i szerokie rozumienie ryzyka, nie tylko w kontekście bezpieczeństwa, projektu, wyrobu lub procesu, ale również w odniesieniu do całej organizacji, a także aspektów finansowych, wprowadza norma PN-ISO 31000 o zarządzaniu ryzykiem [1], [2].

Ryzyko – wpływ niepewności na cele

Według powyższej normy ryzyko jest zwykle wyrażane w kategoriach **źródeł ryzyka** (element, który sam lub w połączeniu z innymi może powodować ryzyko), **potencjalnych zdarzeń** (wystąpienie lub zmiana określonego zestawu okoliczności), ich **konsekwencji** (rezultat zdarzenia wpływający na cele) oraz ich **prawdopodobieństwa** (możliwość wystąpienia zdarzenia).

W takim ujęciu ryzyko może odnosić się do jednego produktu, jednej instalacji, a nawet całego regionu czy kraju. Może dotyczyć zarówno celów bezpieczeństwa, jak i celów finansowych.

OCENA RYZYKA

Posługujemy się terminami „analiza zagrożeń" i „ocena ryzyka" dla podkreślenia wagi tych zadań oraz dlatego, że są one stosowane w praktyce, choć zgodnie z normą PN-ISO 31000 oba te zadania należą do procesu zarządzenia ryzykiem nazwanego wspólnie oceną ryzyka.

Ocena ryzyka jest ogólnym procesem identyfikacji ryzyka, jego analizy i ewaluacji. Obejmuje następujące elementy [1], [2]:

- identyfikację zagrożeń,
- określenie prawdopodobieństwa wystąpienia wszystkich zagrożeń,
- ewaluację ryzyka,
- określenie środków redukcji ryzyka.

Każda analiza i ocena ryzyka wiąże się z analizą i oceną zagrożeń.

Dopiero właściwa identyfikacja zagrożeń umożliwia właściwą identyfikację ryzyka, podobnie jak właściwa ocena zagrożeń umożliwia właściwą ocenę ryzyka.

OCENA RYZYKA – PODSTAWA PRAWNA

Obowiązek przeprowadzenia analizy zagrożeń i oceny ryzyka, stosownie do przedmiotu swojej regulacji, wprowadzają następujące przepisy prawa:

- **przepisy oceny zgodności**, zgodnie z którymi **producent** wyrobu ma obowiązek przeprowadzenia oraz udokumentowania **analizy i oceny ryzyka** stwarzanego przez produkt;
- **przepisy prawa pracy**, zgodnie z którymi **pracodawca** jest obowiązany ocenić i udokumentować **ryzyko zawodowe** związane z wykonywaną pracą, poinformować pracowników o tym ryzyku oraz aktualizować ocenę i dokumentację ryzyka (w tym miejscu należy wskazać, że jest to obowiązek ogólny wynikający z Kodeksu pracy, natomiast szczegółowe przepisy prawa pracy dotyczące bhp określają dodatkowe wymagania, jak np. obowiązek opracowania **dokumentu zabezpieczenia przed wybuchem czy dokonania kompleksowej oceny ryzyka,** wynikające z wdrożonej do polskiego porządku prawnego dyrektywy ATEX User 1999/92/WE);
- **przepisy dozoru technicznego**, zgodnie z którymi **eksploatujący** obowiązany jest przedłożyć do UDT dokumentację umożliwiającą **ocenę wyjściowego poziomu bezpieczeństwa** urządzenia ciśnieniowego funkcjonującego w instalacji w przypadku nieprzeprowadzenia kompleksowej oceny zgodności zespołu urządzeń ciśnieniowych.

Chociaż **przepisy prawa** nakładają obowiązek prowadzenia oceny ryzyka, monitorowania oceny ryzyka (w szczególności przepisy prawa pracy) czy wskazują metody jej prowadzenia (jak przepisy oceny zgodności)**, rzadko kiedy definiują jednoznaczne kryteria akceptacji tego ryzyka, odnosząc się raczej ogólnie do pojęć bezpieczeństwa, ochrony życia i zdrowia, usuwania lub ograniczania ryzyka czy oceny wyjściowego poziomu bezpieczeństwa itp.**

KRYTERIA AKCEPTOWALNOŚCI RYZYKA

Zapewnienie bezpieczeństwa polega na stosowaniu przepisów prawa, norm, wiedzy/*know-how*, eliminacji zagrożeń oraz minimalizacji ryzyka (korzystając z właściwych narzędzi minimalizacji ryzyka).

Podstawowymi kryteriami akceptowalności ryzyka w każdym procesie lub projekcie powinny być wymagania określone w obowiązujących przepisach prawa, a następnie wymagania określone w aktualnych dokumentach normatywnych (w tym normach).

Fundamentalna zasada przy zapewnieniu bezpieczeństwa:
STOSUJ WYMAGANIA OBOWIĄZUJĄCYCH PRZEPISÓW PRAWA
STOSUJ WYMAGANIA AKTUALNYCH DOKUMENTÓW NORMATYWNYCH (W TYM NORM)

Najczęściej spotykamy się z brakiem określenia ścisłych kryteriów akceptowalności ryzyka w przepisach prawa lub normach.

Przepisy prawa wskazują natomiast inne kryteria mające na celu zapewnienie bezpieczeństwa, nie stosując wprost miar czy jednostek wykorzystywanych w analizach ryzyka.

Przykładowo rozporządzenie w sprawie najwyższych dopuszczalnych stężeń i natężeń czynników szkodliwych dla zdrowia w środowisku pracy [3] ustala wartości najwyższych dopuszczalnych stężeń chemicznych i pyłowych czynników szkodliwych dla zdrowia w środowisku pracy w załączniku nr 1 do tego rozporządzenia.

W przypadku braku odpowiednich wymagań prawnych lub normatywnych podmiot odpowiedzialny za ryzyko (tzw. właściciel ryzyka) jest zobowiązany przyjąć własne kryteria akceptowalności ryzyka, **biorąc pod uwagę opinię ekspertów, zdania interesariuszy, własne doświadczenie oraz stosując dobrą praktykę inżynierską.**

Czy można zapewnić bezpieczeństwo, pomijając praktyczne możliwości jego zapewnienia?

Właściciele ryzyka muszą brać pod uwagę uwarunkowania techniczne, finansowe, organizacyjne czy logistyczne danego projektu.

Kiedy właściciel ryzyka może uznać, że zapewnił właściwie bezpieczeństwo?

REASONABLY PRACTICABLE – RACJONALNIE WYKONALNY

Jak wspomniano we wstępie, jako pomoc służyć może tutaj znana w systemie anglosaskim, a przyjęta m.in. w prawie brytyjskim zasada ALARP (ALARA/SFAIRP) wyrażająca racjonalne i proporcjonalne podejście do zarządzania ryzykiem w systemach bezpieczeństwa.

Zasada ta stanowi, że bezpieczeństwo należy zapewnić tak dalece (a ryzyko ograniczyć do tak niskiego poziomu), jak to jest rozsądnie wykonalne, biorąc pod uwagę inne czynniki, takie jak: poziom techniki, czas i pieniądze.

Ciężar zasady ALARP skupia się na pojęciu ***reasonably practicable*** (rozsądnie wykonalny), który bardzo dobrze opisuje brytyjska publikacja ***Wprowadzenie do zdrowia i bezpieczeństwa pracy*** – wydanie szóste 2016 [4] (tłumaczenie oraz podkreślenia własne):

„Jest to najbardziej powszechny poziom obowiązków w prawie bezpieczeństwa i został zdefiniowany przez sędziego Asquitha w sprawie Edwards przeciwko National Coal Board (1949) w następujący sposób:

„Rozsądnie wykonalne" jest terminem węższym niż „fizycznie możliwe" i wydaje mi się sugerować, że właściciel musi dokonać obliczenia, w którym ilość ryzyka jest umieszczona na jednej skali, a poświęcenie związane ze środkami niezbędnymi do uniknięcia ryzyka (czy to w czasie, pieniądzach, czy kłopotach) jest umieszczona na drugiej skali. Jeżeli zostanie wykazane, że istnieje **rażąca dysproporcja** (oryg. ***gross disproportion***) między nimi – ryzyko jest nieznaczne w stosunku do poświęcenia – pozwani zwalniają się z tego obowiązku.

Innymi słowy, jeśli ryzyko obrażeń jest bardzo małe w porównaniu z kosztami, czasem i wysiłkiem, aby je zmniejszyć, nie jest konieczne podejmowanie żadnych działań. Ważne jest, aby pamiętać, że pieniądze, czas i kłopoty muszą „rażąco przeważać" (oryg. ***grossly outweigh***), a nie równoważyć ryzyko (…). Ten obowiązek wymaga osądu ze strony pracodawcy (lub jego doradcy) i wyraźnie wymaga przeprowadzenia oceny ryzyka wraz z odnotowaniem wniosków. Ciągłe monitorowanie jest również wymagane w celu zapewnienia, że ryzyko nie wzrasta".

ALARP W DYREKTYWIE PED 2014/68/UE – PODSTAWA PRAWNA

Zasada ALARP ma podstawę prawną w unijnym prawodawstwie harmonizacyjnym dotyczącym projektowania i wytwarzania urządzeń ciśnieniowych oraz zespołów urządzeń ciśnieniowych w niżej wskazanym zakresie.

Poniżej podajemy wersję angielską [5] i niemiecką [6] przepisu zawartego w **pkt 1.2. ZAŁĄCZNIKA I ZASADNICZE WYMAGANIA BEZPIECZEŃSTWA UWAGI OGÓLNE** dyrektywy PED 2014/68/UE, których treść prawidłowo oddaje sens zasady ALARP (podkreślenia własne):

„In choosing the most appropriate solutions, the manufacturer shall apply the principles set out below in the following order:
— eliminate or reduce hazards **as far as is reasonably practicable**".

„Bei der Wahl der angemessensten Lösungen hat der Hersteller folgende Grundsätze, und zwar in der angegebenen Reihenfolge, zu beachten:
— Abwendung oder Verminderung der Gefahren, **soweit dies nach vernünftigem Ermessen möglich ist**".

Treść ww. przepisów została prawidłowo implementowana do krajowych porządków prawnych odpowiednich państw członkowskich. Przykładowo w prawie brytyjskim w akcie prawnym The Pressure Equipment (Safety) Regulations 2016 [7] czy w prawie austriackim w akcie prawnym Verordnung des Bundesministers für wirtschaftliche Angelegenheiten über Druckgeräte (Druckgeräteverordnung – DGVO) [8], przy czym w wersjach krajowych przepisów wdrożono dokładną treść unijnych przepisów prawa.

W wersji angielskiej dyrektywy zasada ALARP (*as far as is reasonably practicable*) została bezpośrednio zaczerpnięta z brytyjskiego prawodawstwa dotyczącego zdrowia i bezpieczeństwa w pracy – Health and Safety at Work etc. Act 1974 [9], gdzie ta zasada jest wyrażona w sformułowaniu *so far as is reasonably practicable*.

Natomiast w wersji niemieckiej dyrektywy zastosowano sformułowanie: „soweit dies nach vernünftigem Ermessen möglich ist", które moglibyśmy przetłumaczyć dosłownie: „o ile po rozsądnej ocenie jest to możliwe". Niemieckie tłumaczenie dyrektywy oddaje zatem precyzyjnie właściwy sens tej zasady.

Wersja polska dyrektywy PED 2014/68/UE **w ZAŁĄCZNIKU I – ZASADNICZE WYMAGANIA BEZPIECZEŃSTWA** w pkt 1.2. stanowi [10]:

Wybierając najwłaściwsze rozwiązania, producent musi stosować zasady ustalone poniżej w następującym porządku:
– usuwać lub zmniejszać niebezpieczeństwo, **w zakresie, w jakim jest to praktycznie wykonalne.**

Postanowienie dyrektywy PED 2014/68/UE zostało implementowane do polskiego porządku prawnego rozporządzeniem Ministra Rozwoju w sprawie wymagań dla urządzeń ciśnieniowych i zespołów urządzeń ciśnieniowych [11] w § 16 ust. 2 pkt 1):

W celu spełnienia wymagania, o którym mowa w ust. 1, stosuje się odpowiednie rozwiązania, uwzględniając w następującej kolejności:

1) zasadę wyeliminowania lub zminimalizowania zagrożeń, **w zakresie, w jakim jest to praktycznie wykonalne.**

Przyjęcie w polskiej wersji językowej dyrektywy PED 2014/68/UE oraz w wyżej wskazanym rozporządzeniu wdrażającym dyrektywę sformułowania „w zakresie, w jakim jest to praktycznie wykonalne", z uwagi na możliwość szerokiej interpretacji tego zapisu, może budzić wątpliwości co do prawidłowego tłumaczenia, a w konsekwencji co do możliwości oraz obowiązku stosowania zasady ALARP w polskim przemyśle.

Niemniej jednak dyrektywa ciśnieniowa PED 2014/68/UE w **ZAŁĄCZNIKU I – ZASADNICZE WYMAGANIA BEZPIECZEŃSTWA pkt 4. UWAGI WSTĘPNE** przy interpretacji zasadniczych wymagań nakazuje uwzględniać nie tylko zagadnienia bezpieczeństwa i ochrony zdrowia, ale również aktualny stan wiedzy i praktykę oraz czynniki techniczne i ekonomiczne – jak poniżej.

Zasadnicze wymagania bezpieczeństwa mają być interpretowane i stosowane w taki sposób, aby uwzględniały stan wiedzy oraz praktykę aktualną w momencie projektowania i wytwarzania, jak również **względy natury technicznej i ekonomicznej, które są zgodne z wysokim stopniem ochrony zdrowia i bezpieczeństwa**.

W tym fragmencie polska wersja językowa przepisu jest analogiczna z wersją angielską i niemiecką.

Właściwy sens zasady ALARP, uwzględniający oczywiście jej techniczny i brytyjski kontekst, oddawałoby w języku polskim następujące zdanie: „**Tak dalece, jak to jest rozsądnie/racjonalnie wykonalne/uzasadnione**".

Taka interpretacja tego przepisu byłaby również zgodna z wersją niemiecką i angielską dyrektywy, których tłumaczenia dają dużo większą elastyczność projektantom i producentom w zakresie stwierdzenia, czy dany poziom ryzyka jest wystarczająco dobry/niski, czyli akceptowalny.

Celnie ujął tę kwestię Steve Lewis, stawiając następujące pytanie w tytule publikacji *Risk Criteria – When is low enough good enough?* [12]

W rozumieniu dyrektywy PED producent byłby zobowiązany eliminować lub minimalizować zagrożenie tak dalece, jak to jest rozsądnie/racjonalnie wykonalne/uzasadnione, uwzględniając stan wiedzy, praktykę oraz względy natury technicznej i ekonomicznej, które są zgodne z wysokim stopniem ochrony zdrowia i bezpieczeństwa.

ZASADA ALARP W UNIJNYM PRAWIE PRACY – WYROK ETS

W dniu 21 marca 2005 r. Komisja Europejska wniosła do Trybunału Sprawiedliwości Unii Europejskiej skargę przeciwko Zjednoczonemu Królestwu Wielkiej Brytanii i Irlandii Północnej w sprawie stosowania przez brytyjskie prawo pracy tzw. klauzuli SFAIRP (*so far as is reasonably practicable*).

Artykuł 5 ust. 1 dyrektywy ramowej 89/391/EWG dotyczącej bezpieczeństwa i zdrowia pracowników w miejscu pracy [13] stanowi, że:

„Pracodawca ponosi odpowiedzialność w zakresie zapewnienia bezpieczeństwa i higieny pracy pracownikom w każdym aspekcie odnoszącym się do ich pracy".

Natomiast art. 2 ust. 1 skarżonego brytyjskiego Health and Safety at Work etc Act 1974 [9] stanowi:

„Pracodawca jest zobowiązany zapewnić ochronę zdrowia, bezpieczeństwa i dobrobyt pracowników w miejscu pracy o tyle, o ile jest to racjonalnie wykonalne".

Komisja Europejska podnosiła, że **użycie klauzuli SFAIRP** w zaskarżonym brytyjskim Health and Safety at Work etc Act 1974 **nie w pełni wdrażało wymogi unijnej dyrektywy ramowej 89/391/EWG, twierdząc, że obowiązek pracodawcy** dotyczący zapewnienia bezpieczeństwa i higieny pracy pracownikom w każdym aspekcie odnoszącym się do ich pracy **ma charakter bezwzględny**, **podczas gdy brytyjskie przepisy kwalifikowały ten obowiązek jako „o tyle, o ile jest to racjonalnie wykonalne".**

Dwuletnia batalia prawna przed ETS doprowadziła do utrzymania zasady SFAIRP. W wyroku z dnia 14 czerwca 2007 r. (sprawa C/127/05) Trybunał oddalił skargę i obciążył Komisję kosztami postępowania [14].

Zdaniem Trybunału Komisja nie wykazała m.in. że zawężając do granic racjonalnej wykonalności obowiązek zapewnienia przez pracodawcę bezpieczeństwa i zdrowia pracowników w każdym aspekcie odnoszącym się do miejsca pracy, Wielka Brytania uchybiła zobowiązaniom ciążącym na nim m.in. na mocy art. 5 ust. 1 dyrektywy 89/391/EWG.

Gdyby sprawa została uwzględniona, zakwestionowałoby to racjonalne i proporcjonalne podejście do zarządzania ryzykiem związanym z bezpieczeństwem, które zasada ALARP wyraża.

Trybunał Sprawiedliwości Unii Europejskiej, do którego wyłącznej kompetencji należy wiążąca interpretacja przepisów unijnych, nie zanegował stosowania zasady ALARP przy wykładni art. 5 ust. 1 dyrektywy ramowej 89/391/EWG.

ALARP W NORMACH

Zasada ALARP została także wprowadzona do norm z zakresu bezpieczeństwa czy bezpieczeństwa funkcjonalnego.

PN-EN 61508-5:2010 Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem - Część 5: Przykłady metod określania poziomów nienaruszalności bezpieczeństwa [15] – w szczególności Załącznik C

PN-EN 61511-3: 2017-07 Bezpieczeństwo funkcjonalne Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego Część 3: Wytyczne do określania poziomów wymaganych nienaruszalności bezpieczeństwa [16] – w szczególności Załącznik K

Norma PN-EN 62061:2008 Bezpieczeństwo maszyn - Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem, która jest **zharmonizowana z dyrektywą maszynową 2006/42/WE**, **odsyła do stosowania ww. norm: IEC 61508 i IEC 61511**.

PODSUMOWANIE

Podkreślamy, że zasadę ALARP należy stosować, uwzględniając wymagania prawne, normatywne oraz dobrą praktykę inżynierską.

W niniejszej części artykułu omówiliśmy kontekst prawny i normatywny zasady ALARP w polskim porządku prawnym.

Zapraszamy do lektury drugiej części artykułu o ALARP, w której precyzujemy zasady jej stosowania.

Literatura:

1. PN-ISO 31000:2018-08 Zarządzanie ryzykiem. Wytyczne
2. PN-ISO 31000:2012 Zarządzanie ryzykiem. Zasady i wytyczne
3. Rozporządzenie Ministra Rodziny, Pracy i Polityki Społecznej z dnia 12 czerwca 2018 r. w sprawie najwyższych dopuszczalnych stężeń i natężeń czynników szkodliwych dla zdrowia w środowisku pracy (Dz.U. z 2018 r. poz. 1286) https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001286/O/D20181286.pdf
4. Introduction to Health and Safety at Work Sixth edition 2016, rozdz. I (chapter I), s. 14 (p. 14) Introduction to Health and Safety at Work (idu.ac.id) – dostęp 20.05.2024
5. DIRECTIVE 2014/68/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 May 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of pressure equipment Directive 2014/68/EU of the European Parliament and of the Council of 15 May 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of pressure equipmentText with EEA relevance (europa.eu) – dostęp 20.05.2024
6. RICHTLINIE 2014/68/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 zur Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Druckgeräten auf dem Markt Richtlinie 2014/68/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 zur Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Druckgeräten auf dem MarktText von Bedeutung für den EWR (europa.eu) – dostęp 20.05.2024
7. The Pressure Equipment (Safety) Regulations 2016 The Pressure Equipment (Safety) Regulations 2016 (legislation.gov.uk) – dostęp 20.05.2024
8. Verordnung des Bundesministers für wirtschaftliche Angelegenheiten über Druckgeräte (Druckgeräteverordnung – DGVO) BGBl. II Nr. 426/1999 (bka.gv.at) – dostęp 20.05.2024
9. The Health and Safety at Work etc Act 1974 https://www.legislation.gov.uk/ukpga/1974/37/section/2 – dostęp 20.05.2024
10. DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY 2014/68/UE z dnia 15 maja 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do udostępniania na rynku urządzeń ciśnieniowych https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32014L0068 – dostęp 20.05.2024
11. ROZPORZĄDZENIE MINISTRA ROZWOJU z dnia 11 lipca 2016 r. w sprawie wymagań dla urządzeń ciśnieniowych i zespołów urządzeń ciśnieniowych (Dz.U. z 2019 r. poz. 211, tj.) https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20190000211/O/D20190211.pdf – dostęp 20.05.2024
12. Steve Lewis "Risk Criteria – When is low enough good enough?"; Risktec Solutions Limited; https://risktec.tuv.com/wp-content/uploads/2018/10/risk-criteria-when-is-low-enough-good-enough-saudi.pdf [link – dostęp 20.05.2024]
13. DYREKTYWA RADY z dnia 12 czerwca 1989 r. w sprawie wprowadzenia środków w celu poprawy bezpieczeństwa i zdrowia pracowników w miejscu pracy (89/391/EWG) eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:31989L0391 – dostęp 20.05.2024
14. WYROK TRYBUNAŁU (trzecia izba) z dnia 14 czerwca 2007 r. w sprawie C-127/05 KOMISJA PRZECIWKO ZJEDNOCZONEMU KRÓLESTWU eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:62005CJ0127 – dostęp 20.05.2024
15. PN-EN 61508-5:2010 Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem - Część 5: Przykłady metod określania poziomów nienaruszalności bezpieczeństwa
16. PN-EN 61511-3: 2017-07 Bezpieczeństwo funkcjonalne Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego Część 3: Wytyczne do określania poziomów wymaganych nienaruszalności bezpieczeństwa

RACJONALNE PODEJŚCIE DO ZARZĄDZANIA RYZYKIEM ZASADA ALARP – METODYKA

CZĘŚĆ II

R. PR. MATEUSZ ŁUKASZCZYK

Starszy Specjalista
Oddział w Poznaniu
Urząd Dozoru Technicznego
Doktorant wdrożeniowy
Uniwersytet im. Adama Mickiewicza
w Poznaniu

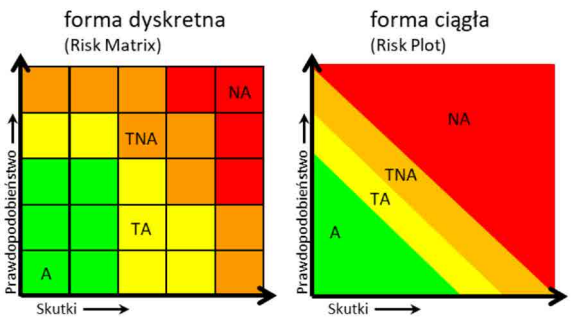
DR INŻ. MARCIN WOŁEJKO

Centrum Kompetencyjne ds. Automatyki
Departament Innowacji i Rozwoju
Urząd Dozoru Technicznego

W pierwszej części artykułu omówiliśmy kontekst prawny i normatywne zasady ALARP w polskim porządku prawnym. W drugiej części wyjaśnimy, na czym ta zasada polega, i przedstawimy przykłady zastosowania analizy CBA (Cost-Benefit Analysis), tj. analizy kosztów i korzyści.

KIEDY STOSUJEMY ALARP?

W zarządzaniu bezpieczeństwem posługujemy się m.in. matrycą lub płaszczyzną ryzyka w celu wizualizacji wartości ryzyka (rys. 1).



Rys. 1. Typowe sposoby prezentacji ryzyka

Na płaszczyźnie ryzyka granice obszarów ryzyka są zwykle iloczynem wartości konsekwencji (C) i prawdopodobieństwa (P) wystąpienia określonych konsekwencji [1)]. Zwykle, dla celów decyzyjnych, określane są obszary ryzyka, np. A, TA, TNA oraz NA [2)], dla których definiuje się konkretne działania lub reguły, np. zakaz podejmowania produkcji lub nakaz jej zatrzymania, gdy ryzyko jest w obszarze NA.

1) Częstym błędem jest wskazywanie P jako prawdopodobieństwa zdarzenia inicjującego lub zdarzenia szczytowego (tzw. zdarzenia niebezpiecznego). Matryce mogą być kalibrowane dla P będącego prawdopodobieństwem zdarzenia niebezpiecznego wyłącznie przy założeniu, że każde zdarzenie niebezpieczne prowadzi do materializacji się konsekwencji, lub przy założeniu, że redukcja prawdopodobieństwa wystąpienia konsekwencji jest stała przy każdym zdarzeniu niebezpiecznym lub zdarzeniu niebezpiecznym z określonej grupy. Byłyby to konserwatywne założenia i zwykle nie są praktykowane. Natomiast spotykane są błędy odczytu wartości z matryc ryzyka wynikające z opisanej pomyłki.

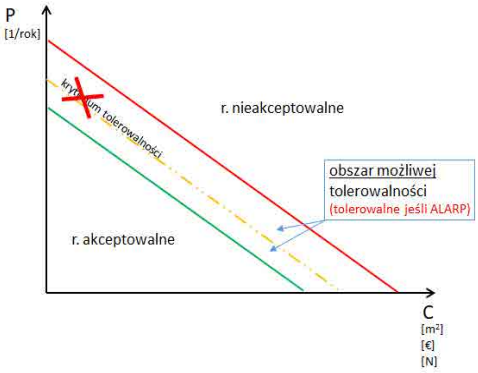
2) A (Akceptowalne/Acceptable), TA (Tolerowalne Akceptowalne/Tolerable Acceptable), TNA (Tolerowalne – Nieakceptowalne/Tolerable – Not Acceptable), NA (Nieakceptowalne/Not Acceptable).

W tym celu na odpowiednio wyskalowanej matrycy lub płaszczyźnie należy wyznaczyć trzy obszary ryzyka, a przede wszystkim ich **linie graniczne**:

a) **ryzyka akceptowalnego (A)** – czyli obszaru, w którym ustala się brak konieczności dalszych działań redukujących ryzyko, a jedynie obowiązek monitorowania, czy przewidywane czynniki wpływu na scenariusze zdarzeń pozostają bez zmian, tj. czy częstość zdarzeń inicjujących lub warunkujących nie ulega zmianie lub czy nie zidentyfikowano nowych zdarzeń lub nowych scenariuszy prowadzących do danej grupy zdarzeń niebezpiecznych;

b) **ryzyka nieakceptowalnego (NA)** – czyli obszaru, w którym nie można pod żadnym uzasadnieniem i w żadnym czasie pozostawić scenariuszy zdarzeń – ryzyko musi być zredukowane lub należy odstąpić od inwestycji lub zaprzestać jej prowadzenia.

Pomiędzy tymi obszarami pozostaje obszar ryzyka potencjalnie tolerowalnego, rozumianego jako tolerowane pod warunkiem istnienia dowodów na ALARP (**Tolerable if ALARP**), czyli **ryzyko zredukowane tak bardzo, jak to racjonalnie uzasadnione**.



Rys. 2. Szkic koncepcji granic obszarów ryzyka na płaszczyźnie ryzyka oraz obszaru ALARP

Nominalnie należy przyjmować, że celem redukcji ryzyka zawsze pozostaje obszar ryzyka akceptowalnego, a w myśl zasady ALARP tylko metodycznie uzasadnione i udokumentowane względy mogą pozwolić na zaprzestanie dalszej redukcji ryzyka bez narażania się na zarzut niedopełnienia obowiązków czy niedołożenia wystarczającej staranności w zapewnianiu bezpieczeństwa.

Oczywiście kryteria dla początku obszaru NA są zwykle ostrzejsze, gdy obszar potencjalnych konsekwencji sięga poza obszar przedsiębiorstwa (rys. 2).

W dziedzinie kryteriów akceptacji ryzyka szerokie wyjaśnienia można znaleźć w pracach prof. Adama S. Markowskiego [3]. Zachęcamy też do zapoznania się z wytycznymi UDT dotyczącymi prowadzenia analiz i oceny ryzyka [4].

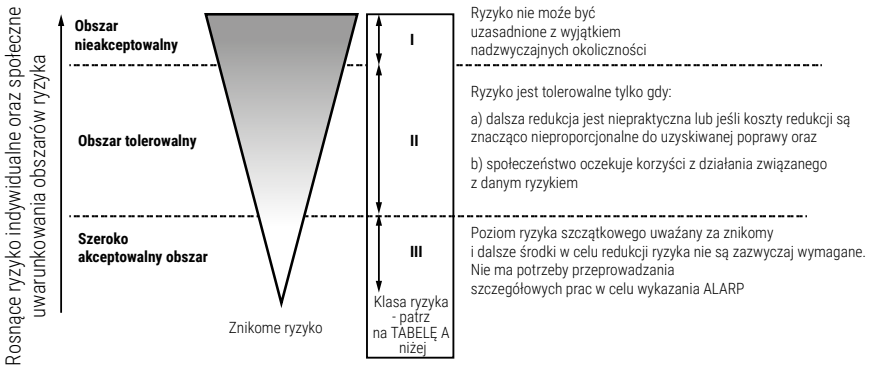
ALARP W NORMACH

Chociaż stosowanie norm technicznych jest dobrowolne, są one postrzegane jako uznana praktyka inżynierska w projektowaniu, a jednocześnie stanowią środek spełnienia i uzupełnienia norm prawnych.

Warto przyjrzeć się koncepcji ALARP ujętej w załącznikach informacyjnych norm PNEN 61508 (ZAŁĄCZNIK C) [1] oraz PN-EN 61511 (ZAŁĄCZNIK K) [2].

Załączniki uznają zasadę ALARP za szczególne podejście do ustalenia ryzyka tolerowalnego. Przy czym intencją twórców norm nie jest przedstawienie ostatecznego opisu metody, ale raczej zilustrowanie ogólnych zasad. Podejście to obejmuje proces ciągłego doskonalenia – w jego ramach rozważane są wszystkie opcje, które mogłyby jeszcze bardziej zmniejszyć ryzyko pod kątem korzyści i kosztów. Koncepcja ALARP może być stosowana podczas określania SIL (sama w sobie nie jest jednak metodą określania SIL). Załączniki wskazują, że osoby zamierzające zastosować metody w nich wskazane powinny zapoznać się z materiałami źródłowymi, czyli publikacją UK HSE (2001) „Reducing Risks, Protecting People" ISBN 0717621510 (dostępną online pod adresem: Reducing Risks: Protecting People - HSE's decision making process).

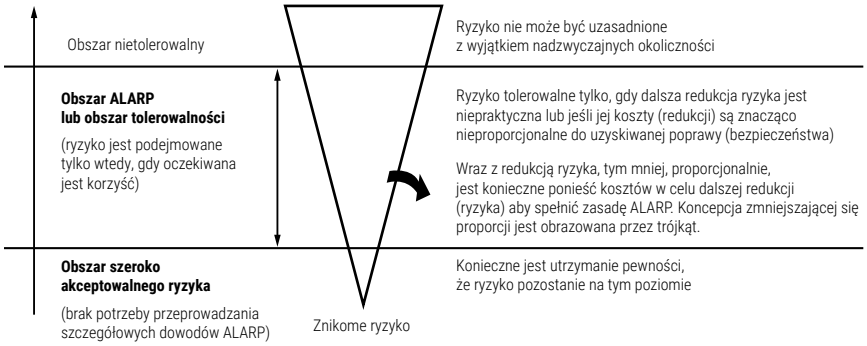
Normy IEC 61508 [1] oraz IEC 61511 [2] prezentują obszar ryzyka leżący pomiędzy obszarem NA a obszarem A w podobny sposób (różnice są niewielkie).



ILUSTRACJA A - Ryzyko tolerowalne i ALARP - IEC 61511

Tabela B- Interpretacja klas ryzyka

Klasa/kategoria ryzyka	Interpretacja
Klasa I	Ryzyko nietolerowalne
Klasa II	Ryzyko niepożądane i tolerowalne tylko gdy (dalsza) redukcja ryzyka jest niepraktyczna lub jeśli koszty są znacząco nieproporcjonalne do uzyskiwanej poprawy (bezpieczeństwa)
Klasa III	Znikome ryzyko



ILUSTRACJA B - Ryzyko tolerowalne i ALARP - IEC 61508

Tabela B - Interpretacja klas ryzyka

Klasa/kategoria ryzyka	Interpretacja
Klasa I	Ryzyko nietolerowalne
Klasa II	Ryzyko niepożądane i tolerowalne tylko gdy (dalsza) redukcja ryzyka jest niepraktyczna lub jeśli koszty są znacząco nieproporcjonalne do uzyskiwanej poprawy (bezpieczeństwa)
Klasa III	Ryzyko tolerowalne, jeśli koszt redukcji ryzyka przewyższyłby uzyskaną poprawę
Klasa IV	Znikome ryzyko

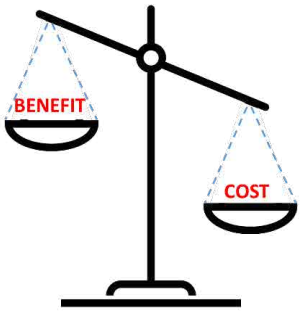
Rys. 3. Obszary ryzyka. Opracowano wg (A) IEC 61511 [2] oraz (B) IEC 61508 [1]

UWAGA: Warto zwrócić uwagę, że obie normy wskazują, iż w obszarze tolerowalności ryzyka, oprócz redukcji ryzyka ALARP, także korzyści z jego podejmowania powinny być udziałem społeczeństwa lub strony narażonej na to ryzyko. Ten aspekt rzuca dodatkowe światło na tzw. odpowiedzialność społeczną przedsiębiorstw (CSR, ang. Corporate Social Responsibility).

Norma IEC 61511 [2] jest jakby „bardziej wymagająca" ponieważ rekomenduje w całym obszarze możliwej tolerowalności (Class II) wykazanie niepraktyczności dostępnych opcji redukcji ryzyka lub „znaczącej dysproporcji" kosztów redukcji ryzyka nad efektami redukcji (korzyściami).

Norma IEC 61511 zaleca:

"Below that (unnacceptable) level, a risk is considered to be "tolerable": provided that it has been reduced to the point where the benefit gained from further risk reduction is outweighed by the cost of achieving that risk reduction, and provided that generally accepted standards have been applied towards the control of the risk. The higher the risk, the more would be expected to be spent to reduce it. A risk which has been reduced in this way is considered to have been reduced to a level which is "as low as is reasonably practicable" (ALARP)".	Poniżej tego (niedopuszczalnego) poziomu ryzyko uznaje się za «tolerowalne»: pod warunkiem, że zostało ono zredukowane do punktu, w którym koszty osiągnięcia redukcji ryzyka przeważają nad korzyściami uzyskanymi z dalszej redukcji ryzyka, oraz pod warunkiem, że ogólnie uznane standardy zostały zastosowane w celu kontroli ryzyka. Im wyższe ryzyko, tym więcej należałoby wydać na jego ograniczenie. Ryzyko, które zostało zmniejszone w ten sposób, uważa się za zmniejszone do poziomu «tak niskiego, jak to racjonalnie wykonalne» (ALARP).



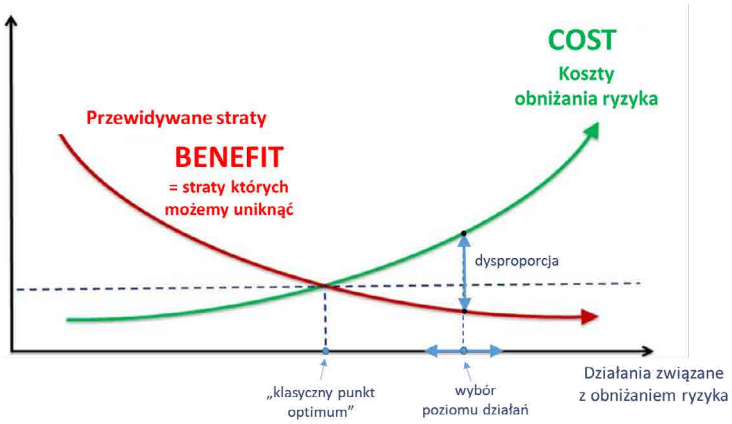
Rys. 4. Ilustracja zasady ALARP

Noma IEC 61508 [1] jest „bardziej precyzyjna" i w obszarze możliwej tolerowalności, lecz bliżej ryzyka nieakceptowalnego, proponuje wyróżnienie dwóch obszarów. Pierwszym jest **obszar (Class II), gdzie wskazuje potrzebę wykazania „znaczącej dysproporcji"** kosztów redukcji ryzyka nad efektami lub niepraktyczności dostępnych opcji redukcji ryzyka. Drugim jest obszar **(Class III), w którym zaleca już tylko przewagę kosztów** redukcji ryzyka nad efektami.

Norma IEC 61508 stanowi:

"Below that (unnacceptable) level, there is the tolerability region where an activity is allowed to take place provided the associated risks have been made as low as reasonably practicable. Tolerable (risk) here is different from acceptable: it indicates a willingness to live with a risk so as to secure certain benefits, at the same time expecting it (risk) to be **kept under review and reduced as and when this can be done**. Here a cost benefit assessment is required either explicitly or implicitly to weigh the cost and the need or otherwise for additional safety measures. The higher the risk, the more proportionately would be expected to be spent to reduce it (risk). At the limit of tolerability, expenditure in gross disproportion to the benefit would be justified. Here the risk will by definition be substantial, and equity requires that a considerable effort is justified even to achieve a marginal reduction".	Poniżej tego (niedopuszczalnego) poziomu znajduje się obszar tolerancji, w którym działanie jest dozwolone pod warunkiem, że związane z nią ryzyko zostało zredukowane do poziomu tak niskiego, jak to racjonalnie uzasadnione. Tolerowalne (ryzyko) różni się od akceptowalnego: oznacza gotowość do ponoszenia ryzyka w celu zapewnienia określonych korzyści, przy jednoczesnym założeniu, że będzie ono (ryzyko) **poddawane przeglądowi i redukowane, jeśli i kiedy tylko będzie to możliwe**. W tym obszarze wymagana jest albo jawnie, albo pośrednio ocena/analiza kosztów i potrzeb wprowadzenia dodatkowych środków bezpieczeństwa. Im wyższe ryzyko, tym bardziej proporcjonalne wydatki będą oczekiwane w celu jego ograniczenia (ryzyka). Na granicy tolerowalności wydatki znacząco nieproporcjonalne do korzyści byłyby uzasadnione. W tym obszarze ryzyko z definicji będzie znaczące, a sprawiedliwość wymaga, aby znaczny wysiłek/nakład był uzasadniony nawet w celu osiągnięcia marginalnej redukcji.

Mówiąc o znaczącej dysproporcji, dobrze jest przypomnieć sobie znany szkic wyjaśniający zasadę optymalizacji kosztów zarządzania ryzykiem (rys. 5). Dla celów niniejszej publikacji dokonano w nim pewnych modyfikacji, aby wykazać różnice pomiędzy kosztem uważanym za optymalny a kosztem uwzględniającym znaczącą dysproporcję.



Rys. 5. Koszty zarządzania ryzykiem – koszt optymalny i pytanie o znaczącą dysproporcję

Jeśli za koszty (na rys. 5) uzna się poświęcenie związane ze środkami niezbędnymi do uniknięcia ryzyka (czy to w czasie, pieniądzach, czy nakładach pracy), to uzyskujemy dysproporcję, porównując te koszty z korzyściami, a mówiąc inaczej – z uniknięciem potencjalnych strat dla zdrowia, życia – także w odniesieniu do przyszłości osób narażonych.
W tym miejscu należy otwarcie przyjąć, że w celu zastosowania analizy kosztów i korzyści – o ile koszty są relatywnie łatwo identyfikowalne i policzalne, o tyle obliczenie korzyści wiąże się z koniecznością oszacowania w jednostkach monetarnych aspektów takich jak możliwe do uniknięcia ofiary, utrata zdrowia, często pogorszenie się komfortu życia itp., zależnie od przyjętej szczegółowości metodologii. Należy przy tym pamiętać, że ciągle mówimy o prawdopodobieństwie skutków a nie o nieuchronnych skutkach. W tej kwestii odsyłamy także do źródeł literaturowych podanych na końcu artykułu.

Z całą stanowczością należy odrzucić pojawiające się czasami błędne zrozumienie i niesłuszne zarzuty do metody CBA dokonywania oceny wartości zdrowia i życia.

W stosowanej przy ALARP analizie wartością i korzyścią są życie i zdrowie oraz inne aspekty ważne społecznie, potencjalnie uratowane dzięki inwestycjom w bezpieczeństwo.

Dyskutowana społecznie powinna być natomiast granica, po której przekroczeniu uważa się dalsze inwestycje za nieracjonalne - pamiętając o jak niskim prawdopodobieństwie skutków toczy sie dyskusja. Ocena tej kwestii powinna być dokonywana z uwzględnieniem oczekiwań społecznych właściwych dla danego państwa, regionu czy obszaru.

Istnieją wytyczne i badania oceniające oczekiwania społeczne, w tym tzw. *willingness-to-pay* (WTP), czyli oczekiwane i akceptowalne społecznie poziomy kwot inwestycji w bezpieczeństwo mających zapobiegać lub zmniejszać liczbę ofiar, czy poziom zachorowań lub poprawiać inne aspekty życia, które mogą podlegać negatywnym wpływom inwestycji tworzącej ryzyko. Takie badania są miarodajne i pozwalają dokonać oceny, czy w rozważanym aspekcie ryzyko jest, czy nie jest ALARP.

Do celów podejmowania decyzji w ALARP należy zatem ustalić dodatkową regułę dla przewagi kosztów redukcji ryzyka nad korzyściami – czyli kiedy będziemy stwierdzać, że dysproporcja jest znacząca.

Tutaj najbardziej znanym wskaźnikiem jest tzw. „disproportion factor" (DF), czyli poziom przewagi kosztów nad korzyściami uznawany za granicę racjonalności.

W Wielkiej Brytanii reguły te zostały opisanie liczbami. W Polsce brak jest takich regulacji, więc zarówno decyzja jak i odpowiedzialność spoczywa w rękach osób odpowiedzialnych za zapewnienie bezpieczeństwa w przedsiębiorstwie.

REASONABLY PRACTICABLE – RACJONALNIE WYKONALNY

Według brytyjskiego Health and Safety Executive (HSE) [5] termin *reasonable practicable* oznacza „racjonalnie wykonalne lub osiągalne". Autorzy [5] cytują uzasadnienie do wyroku Court of Appeal w sprawie Edwards v. National Coal Board, [1949]:

‚Reasonably practicable' is a narrower term than ‚physically possible' and seems to me to imply that a computation must be made by the owner in which the quantum of risk is placed on one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time or trouble) is placed in the other, and that, if it be shown that there is a gross disproportion between them – the risk being insignificant in relation to the sacrifice – the defendants discharge the onus on them.	„Rozsądnie wykonalne" jest terminem węższym niż „fizycznie możliwe" i wydaje mi się sugerować, że właściciel musi dokonać obliczenia, w którym ilość ryzyka jest umieszczona na jednej skali, a poświęcenie związane ze środkami niezbędnymi do uniknięcia ryzyka (czy to w czasie, pieniądzach, czy kłopotach) jest umieszczona na drugiej skali. Jeżeli zostanie wykazane, że istnieje **rażąca dysproporcja** (oryg. ***gross disproportion***) między nimi – ryzyko jest nieznaczne w stosunku do poświęcenia – pozwani zwalniają się z tego obowiązku.

Co do zasady upewnienie się, że ryzyko zostało zmniejszone ALARP polega m.in. na porównaniu potencjalnych konsekwencji ryzyka z „poświęceniem" (koszty, nakłady czasu i pracy) niezbędnym do jego dalszego zmniejszenia. Decyzja powinna być ważona przede wszystkim pod względem zdrowia i bezpieczeństwa, ponieważ podmiot odpowiedzialny za bezpieczeństwo powinien (jest zobowiązany prawnie) wdrożyć środki zmniejszające ryzyko [5].

JAK STWIERDZIĆ, CZY RYZYKO JEST ALARP?

Wymaga to oceny. Nie ma prostego wzoru na obliczenie, co jest ALARP [5].
Używanie terminu «racjonalnie uzasadnione» pozwala nam wyznaczać cele dla właścicieli ryzyka zamiast stosować nakazy i wymagania [5].
Ta elastyczność jest wielką zaletą zasady ALARP. Pozwala ona podmiotom odpowiedzialnym wybrać metodę, która jest dla nich najlepsza, a zatem wspiera innowacje.
Ale ma też swoje wady.
Podjęcie decyzji, czy ryzyko jest ALARP, może być trudne, ponieważ wymaga dokonania oceny i szczegółowego udokumentowania tego procesu.
W branżach wysokiego ryzyka lub tam, gdzie funkcjonuje nowa technologia, której stosowanie może mieć poważne konsekwencje, lub gdy sytuacja nie jest jednoznaczna, należy przeprowadzić bardziej szczegółowe porównanie.
W takich przypadkach bardziej formalna analiza kosztów i korzyści (CBA) może pomóc w dokonaniu oceny.
Aby uniknąć konieczności «nadmiernego poświęcania się», podmiot odpowiedzialny, po wdrożeniu podstawowych środków redukcji ryzyka, musi wykazać, że **wdrażanie kolejnych środków byłoby rażąco nieproporcjonalne do korzyści** wynikających z ograniczenia ryzyka [5].

Proces ALARP nie polega zatem na prostym równoważeniu kosztów i korzyści, ale raczej na przyjmowaniu dostępnych rozwiązań, chyba że zostaną one wykluczone ze względu na rażąco nieproporcjonalne „poświęcenie".

JAK NALEŻY ROZUMIEĆ KOSZTY I KORZYŚCI W KONTEKŚCIE ALARP?

- Jako koszty mogą być traktowane m.in.: koszty instalacji, eksploatacji, szkoleń i dodatkowej konserwacji. Kosztem mogą być także straty biznesowe, które wynikałyby z zamknięcia zakładu, jeśli byłoby ono skutkiem wdrożenia środka redukcji ryzyka.
- Korzyści powinny obejmować zmniejszenie ryzyka dla pracowników i szerszej społeczności, w tym zapobieżenie ofiarom śmiertelnym, urazom (od poważnych do mniejszych), pogorszeniu stanu zdrowia oraz szkodom dla środowiska.

Więcej informacji na ten temat znaleźć można w opracowaniu [6].

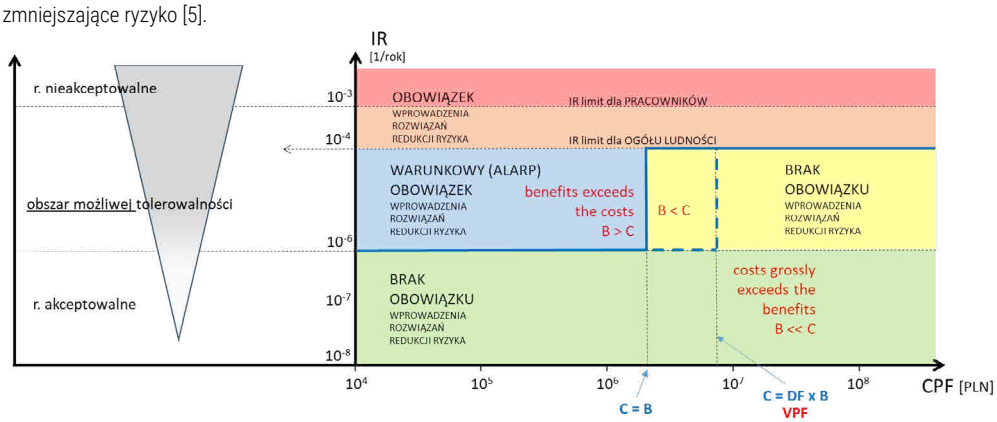
Autorzy [5] podali następujące, bardzo jaskrawe przykłady różnych stosunków kosztów i korzyści:
„1. Wydanie miliona funtów na uniknięcie siniaków na kolanach pięciu pracowników jest rażąco nieproporcjonalne.
2. Ale wydanie miliona funtów na zapobieżenie poważnej eksplozji, w wyniku której może zginąć 150 osób, jest w sposób oczywisty proporcjonalne".

JAKIMI ZASADAMI NALEŻY SIĘ KIEROWAĆ, PLANUJĄC WDROŻENIE ZASADY ALARP?

Z pewnością można oprzeć się na uznanych praktykach opisanych przez HSE [5], [6].
Jak wskazują normy IEC 61511 [2] oraz IEC 61508 [1], można rozważyć wprowadzenie obszaru ryzyka, w którym:

a) wystarczające jest wykazanie przewagi kosztów nad korzyściami w bezpieczeństwie oraz
b) wymagane jest wykazanie znaczącej przewagi kosztów nad korzyściami w bezpieczeństwie.

Takie podejście opisuje też prof. Kosmowski w pracy [7] oraz [8] opisującej tzw. TOR/CBA Framework. Koncepcję tę w skrócie przedstawiono na rys. 6.



CPF = Cost of Preventing Fatality,
VPF = Value of Preventing Fatality,
C = koszty,
B = korzyści,
DF = współczynnik dysproporcji

Rys. 6. Obszary decyzyjne dla TOR/CBA Framework. Opracowanie: UDT na podstawie [8]

W ramach TOR/CBA środki bezpieczeństwa są wymagane, jeśli którekolwiek z poniższych kryteriów byłoby spełnione: **1. Kryterium TOR:** bez przedmiotowych środków bezpieczeństwa ryzyko dla narażonych osób byłoby powyżej dopuszczalnego poziomu, lub **2. Kryterium CBA:** istnieją środki bezpieczeństwa, w przypadku których korzyści przewyższają koszty.	Zatem w TOR/CBA Framework (rys.6) istnieją dwa poziomy decyzyjne, podobnie jak w IEC 61508 (patrz rys.3) 1. Jeżeli C > B, to działanie nie jest już obowiązkowe. 2. Jeżeli C > DF × B, to działanie nie jest już obowiązkowe.
Kryterium 1 (TOR) odwołuje się do słuszności. Kryterium 2 (CBA) odwołuje się do efektywności wykorzystania zasobów.	

W obszarze wymaganej dysproporcji zapewne każdy (większy od 1) współczynnik dysproporcji (DF) jest lepszy niż żaden. Porównanie wartości z różnych krajów [9] wskazuje, że konsesus leży w przedziale 2–3, choć zawsze jest to obarczone odpowiedzialnością za podjętą decyzję. W tym kontekście warto wskazać wyrok amerykańskiego sądu w sprawie cywilnej Grimshaw przeciwko Ford Motor Company, w którym odrzucono decyzję spółki z powodu współczynnika dysproporcji wynoszącego 2,8 [10].

Istnieją też inne sposoby ustalania dysproporcji, pozwalające uniknąć niezrozumienia. Taką metodą, jak wspomniano wcześniej, jest stosowany w Wielkiej Brytanii współczynnik VPF[1)], którego wartość można znaleźć w wytycznych Green Book [11], publikowanych okresowo przez HM Treasure.

[1)] VPF = Value of Preventing Fatality (~ współczynnik bazujący na koncepcji willingness-to-pay).

Przyjmowane dzisiaj VPF bazują na willingness-to-pay i są na tyle wysokie, że współczynnik DF nie jest już konieczny [12].
VPF: £1m (1997 prices) updated to £ 1.6m (2010 prices) [13].
Na podstawie [14] znamy wartość VPF w UK w 2020 r. → VPF ≈ 2 000 000 £.

Podobnie sprawa wygląda przy wykorzystaniu metody bazującej na współczynniku VPF, opisanej w [8], [11] i [15] oraz metody ICAF opisanej m.in. w [16].

Rozważmy jeden z przykładów na podstawie pracy [8].
Jeśli w Polsce przed wprowadzeniem regulacji odnotowywano około 5000 śmiertelnych wypadków co roku.
Gdy jako opcję sterowania ryzykiem **(OSR)** przyjmie się regulację prawną mającą ograniczyć liczbę ofiar: **włączanie świateł przez 24h** której przewidywany koszt ΔK = 200.000.000 PLN/rok,
a jako cel regulacji: redukcja o 2% (ΔN = 100 osób uniknie śmierci/rok),
wtedy uzyskamy CPF = 2 000 000 PLN.

Czy zatem opisana wyżej OSR (opcja sterowania ryzykiem) jest uzasadniona?

- Przyjmując, że k_f = 1 oraz VPF > 2 000 000 PLN, to działanie i jego koszty należy uznać za uzasadnione.
- Jeżeli natomiast zachodziłby warunek przeciwny, czyli CPF > VPF, to działanie nie byłoby już obowiązkowe.

Ale zastosowanie może mieć także zasada przewagi, np.:

$$CPF = k_f \times VPF$$
$$k_f \in \langle 1; 2)$$

wówczas działanie nie byłoby uzasadnione dopiero po przekroczeniu $k_f \times VPF$, a decyzja wymagałaby ustalenia wartości współczynnika przewagi k_f.
W pracy [8] przywołano bardzo czytelny przykład metodologii oceny kosztów i efektów stosowania systemów zabezpieczeń z użyciem VPF przy określonych zależnościach opisujących **uzasadnione koszty roczne** dla ryzyka indywidualnego ΔK^{I}_{jus} jako:

*Równanie 1 – **uzasadnione koszty roczne** dla ryzyka indywidualnego*

$$\Delta K^{I}_{jus} = k_f \cdot VPF \cdot \left[F \cdot \left(PFD^{1}_{avg} - PFD^{2}_{avg}\right)\right]$$

oraz ΔK_{jus} dla ryzyka grupowego jako:
*Równanie 2 – **uzasadnione koszty roczne** dla ryzyka grupowego*

$$\Delta K_{jus} = k_f \cdot VPF \cdot \left[F \cdot \left(PFD^{1}_{avg} - PFD^{2}_{avg}\right)\right] \cdot N \cdot L^{ef}$$

przy czym zdefiniowano relację:

$$CPF = \mathbf{k_f \cdot VPF}$$

gdzie:
CPF (Cost of Preventing Fatality) – koszt zapobiegania zejściu śmiertelnemu;
VPF (Value of Preventing Fatality) – wartość zapobieżenia zejściu śmiertelnemu;
k_f – współczynnik o wartościach, zależnie od rozważanego przypadku, z przedziału $k_f \in [1,2)$;
F – częstość scenariusza bez środków zabezpieczeń;
N – liczba zejść śmiertelnych po zaistnieniu rozważanego scenariusza awaryjnego,
L^{ef} – efektywny czas życia (eksploatacji) obiektu uwzględniający czas życia obiektu L i stopę dyskonta d;
PFD^{1}_{avg} oraz PFD^{2}_{avg} – przeciętne prawdopodobieństwa niezadziałania rozważanych opcji sterowania ryzykiem OSR_1 i OSR_2 odpowiednio.

Rozważmy przykłady [8] z zastosowaniem podanych wyżej zależności, gdzie PFD^{1}_{avg} i PFD^{2}_{avg} są przeciętnymi prawdopodobieństwami niezadziałania na przywołanie systemu SIS[1)] dla rozważanych rozwiązań:
- OSR_1 (spełniającego podstawowe wymagania o niższym poziomie SIL) oraz
- OSR_2 (o wyższym poziomie SIL, czyli mniejszym PFD).

[1)] SIS = Safety Instrumented System / Przyrządowy system bezpieczeństwa – patrz IEC 61511-1

Przykład 1

Analizuje się ryzyko indywidualne w przypadku dominującego scenariusza awaryjnego o częstości F = 10^{-2}/rok (bez uwzględniania środków zabezpieczających) i bazowym rozwiązaniu systemu E/E/PE na poziomie SIL2 ($PFD_{avg} = 10^{-2}$). Ocenia się, czy uzasadnione jest zwiększenie poziomu SIL tego systemu do SIL3 ($PFD_{avg} = 10^{-3}$).

Przyjęto **VPF = 10^6 EUR** oraz **k_f = 1,5.**
Szacowana różnica kosztów: ΔK ≈ 40 000 EUR/rok.

Stosując równanie 1, uzyskano:

$$\Delta K^{I}_{jus} = 1{,}5 \cdot 2 \cdot 10^{6} \cdot \left[10^{-2} \cdot \left(10^{-2} - 10^{-3}\right)\right] \approx 270\ EUR/rok$$

co wskazuje, że istnieje **ograniczone uzasadnienie, aby podnieść poziom SIL,** ponieważ uzasadnione koszty roczne (ΔK^{I}_{jus}) o tej wartości są niższe niż dodatkowy koszt rozwiązania z zastosowaniem SIL3.

$$\mathbf{\Delta K^{I}_{jus} < \Delta K}$$

Przykład 2

Analizuje się ryzyko społeczne w przypadku dominującego scenariusza awaryjnego o częstości F = 10^{-2}/rok.

Zastosowanie ma równanie 2, przyjmując dane jak w przykładzie 1 oraz N = 10 i L^{ef} = 15, uzyskano:

$$\Delta K_{jus} = 1{,}5 \cdot 2 \cdot 10^{6} \cdot \left[10^{-2} \cdot \left(10^{-2} - 10^{-3}\right)\right] \cdot 10 \cdot 15 \approx 40500\ EUR/rok$$

co wskazuje, że **jest uzasadnione rozważenie zastosowania rozwiązania o SIL3,** ponieważ tyle w przybliżeniu wyniosą dodatkowe koszty tego rozwiązania.

$$\mathbf{\Delta K^{I}_{jus} \approx \Delta K}$$

Należy przeprowadzić dodatkowe, pogłębione analizy z oszacowaniem kosztów implementacji systemu zabezpieczeń na poziomie SIL3.

Mimo ponad 20 lat stosowania współczynnika VPF w regulacjach brytyjskich, nadal poszukuje się lepszego rozwiązania, dostrzegając problemy metodologiczne VPF prowadzące do niedoszacowania jego wartości.

Profesor Philip Thomas z University of Bristol w raporcie [15] wskazuje te błędy i proponuje inaczej sformułować pytanie, aby rozwiązać problem racjonalności decyzji przy inwestycjach w bezpieczeństwo.

Profesor Philip Thomas [15], zamiast szukać odpowiedzi na pytanie: „What is the value of a human life?", proponuje pytanie: **„What benefit is conferred when a safety measure or a health care intervention 'saves' a person's life?".**

I to, zdaniem autorów, jest znacznie lepiej postawione pytanie, gdyż szerzej traktuje wartość wnoszoną przez działania redukujące ryzyko. Podkreśla również pozytywną istotę zasady ALARP – wyznaczanie inwestorom celu zamiast sztywnych regulacji – co wspiera innowacyjność i zapewnia elastyczność doboru rozwiązań. Akcentuje także ich odpowiedzialność za ratowanie życia i zdrowia oraz innych wartości cenionych w obszarze oddziaływania ryzyka tworzonego przez inwestycję.

PODSUMOWANIE

Zdaniem autorów, mimo dodatkowych nakładów pracy i konieczności podjęcia konkretnych decyzji co do wyboru reguł i metodologii obliczeń kosztów i korzyści, dokumentacja uzyskania ALARP powinna być nieodłącznym składnikiem dokumentacji potwierdzającej zapewnienie bezpieczeństwa urządzenia technicznego, zespołu urządzeń oraz instalacji przemysłowej. Osoby odpowiedzialne za bezpieczeństwo w imieniu przedsiębiorcy powinny w każdej chwili legitymować się aktualnym dowodem na ryzyko tak niskie, jak to racjonalnie uzasadnione (ALARP), z zastosowaniem jednej z metod doboru kryteriów dysproporcji.

Podkreślamy, że zasadę ALARP należy stosować, uwzględniając wymagania prawne, normatywne oraz dobrą praktykę inżynierską.

ALARP wymaga także stałej weryfikacji aktualności: przed wprowadzeniem zmian, po ich wprowadzeniu oraz okresowo – uwzględniając zmieniające się możliwości techniczne oraz stan techniczny urządzeń. Jest to istotne w kontekście obowiązku zapewnienia bezpiecznego miejsca pracy przez pracodawcę, w tym obowiązku monitorowania stanu bezpieczeństwa i higieny pracy.

Dokumentacja ALARP może mieć charakter poufny z uwagi na wrażliwe dane właściciela ryzyka ujawniające politykę bezpieczeństwa, w tym tzw. *risk apetite* lub *risk-aversion* przedsiębiorstwa. Powinien to być jednak dokument dostępny dla właściwych instytucji państwowych odpowiedzialnych za ocenę zapewnienia bezpieczeństwa, tj. Państwowa Inspekcja Pracy czy UDT, oraz dostępny dla strony społecznej reprezentującej pracowników przedsiębiorstwa.

W miarę zaangażowania przedsiębiorstwa w tzw. CSR (ang. Corporate Social Responsibility) dokument ALARP każdej inwestycji, która niesie ryzyko dla społeczeństwa, powinien być dostępny publicznie w odpowiednim trybie.

Dodatkową zaletą posiadania dokumentacji ALARP jest możliwość jej prezentacji jako dowodu zapewnienia bezpieczeństwa rozstrzygającego ewentualne wątpliwości, jakie mogą powstawać przy ocenie zastosowanych rozwiązań technicznych i organizacyjnych w kontekście obowiązujących przepisów prawa.

Bezpieczeństwo powinno być zaprojektowanie i okresowo weryfikowane.

Literatura:

1. PN-EN 61508-5:2010 Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem - Część 5: Przykłady metod określania poziomów nienaruszalności bezpieczeństwa.
2. PN-EN 61511-3: 2017-07 Bezpieczeństwo funkcjonalne. Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego - Część 3: Wytyczne do określania poziomów wymaganych nienaruszalności bezpieczeństwa.
3. Borysiewicz M., Markowski A.S., Kryteria akceptowalności ryzyka poważnych awarii przemysłowych, Warszawa, listopad 2002
   https://www.researchgate.net/profile/Adam-Markowski-3/publication/268275406_Kryteria_akceptowalnosci_ryzyka_powaznych_awarii_przemyslowych/links/57233daa08ae586b21d87eb3/Kryteria-akceptowalnosci-ryzyka-powaznych-awarii-przemyslowych.pdf – dostęp 20.05.2024
4. Prowadzenie analiz i ocena ryzyka. Wytyczne Urzędu Dozoru Technicznego. Materiały informacyjne dla klientów. Wydanie 1
   Urząd Dozoru Technicznego - Analiza zagrożeń i oceny ryzyka (udt.gov.pl) – dostęp 20.05.2024.
5. Health and Safety Executive: ALARP "at a glance"; link – dostęp 20.05.2024.
6. Risk management: HSE principles for Cost Benefit Analysis in support of ALARP. Risk management: Expert guidance - HSE principles for Cost Benefit Analysis in support of ALARP – dostęp 20.05.2024.
7. Kosmowski K.T.: Analiza ryzyka i zarządzanie bezpieczeństwem funkcjonalnym, Journal of Polish Safety and Reliability Association, 2011, Vol. 2, No. 3; p. 9–16; link – dostęp 20.05.2024.
8. Kosmowski K.T.: Functional Safety in the context of Risk Appraisal criteria and cost-benefit analysis, Functional Safety Management in Critical Systems, 2007.
9. Thomas Ph., The J-value Framework for determining best use of resources to protect Humans and the environment, First International Conference on Structural Integrity (ICONS-2014), February 4-7, 2014, Kalpakkam, India; p.170; CD Proceedings of ICONS-2014; link – dostęp 20.05.2024.
10. Third Series of Court of Appeal Reports, USA, 1981, Volume 119, p. 757.
11. GOV.UK: Guidance: The Green Book (2022), Updated 27 October 2023; https://www.gov.uk/government/publications/the-green-book-appraisal-and-evaluation-in-central-government/the-green-book-2020#list-of-green-book-supplementary-guidance – dostęp 20.05.2024.
12. Evans A.W.: Safety Appraisal Criteria, The 2005 Lloyd's Register Lecture on Risk Management, The Royal Academy of Engineering; Imperial College, London 2005.
13. HSE – A scoping study on the valuation of risks to life and health: the monetary value of a life year (VOLY) Final report, Newcastle University, Glasgow Caledonian University, University of Birmingham; link – dostęp 20.05.2024.
14. Dolan P., Jenkins P., Estimating the monetary value of the deaths prevented from the UK Covid-19 lockdown when it was decided upon – and the value of "flattening the curve"; LSE, 25 June 2020; link – dostęp 20.05.2024.
15. Thomas Ph., Calculating the value of human life: safety decisions that can be trusted; Policy Report 25: April 2018; University of Bristol; link – dostęp 20.05.2024.
16. Lewis S., Risk Criteria – When is low enough good enough?; Risktec Solutions Limited;
    link – dostęp 20.05.2024.

SPOJRZENIE W PRZYSZŁOŚĆ. PREDYKCJA ZUŻYCIA URZĄDZEŃ CIŚNIENIOWYCH I PLANOWANIE INSPEKCJI Z WYKORZYSTANIEM METODOLOGII RBI – RISK BASED INSPECTION

MGR INŻ. TOMASZ KLINKOSZ

Ekspert Urządzeń Ciśnieniowych
Dział Oceny Zgodności
Oddział w Gdańsku
Urząd Dozoru Technicznego

STAŁY ROZWÓJ TECHNOLOGICZNY WYMUSZA EWOLUCJĘ STANDARDÓW BEZPIECZEŃSTWA TECHNICZNEGO. INNOWACJE I NOWOCZESNE PODEJŚCIE DO OCENY STANU URZĄDZEŃ STALE WDRAŻANE SĄ DO PRAKTYKI. NAJNOWSZE ŚWIATOWE ROZWIĄZANIA POZWALAJĄ MIĘDZY INNYMI NA DOPASOWANIE DZIAŁAŃ ZMIERZAJĄCYCH DO ZAPEWNIENIA BEZPIECZNEJ EKSPLOATACJI URZĄDZEŃ TECHNICZNYCH DO POTRZEB PRZEMYSŁU ORAZ WYMAGAŃ ZWIĄZANYCH Z BEZPIECZEŃSTWEM PUBLICZNYM.

Ponad 10 lat temu Urząd Dozoru Technicznego wdrożył do praktyki dozorowej metodologię RBI (Risk-based Inspection). Obecnie tysiące zbiorników ciśnieniowych i rurociągów technologicznych w polskim przemyśle zostało poddanych analizom RBI, które mają na celu predykcję ich zużycia i opracowanie niezbędnych inspekcji prowadzących do utrzymania odpowiedniego poziomu ryzyka związanego z ich eksploatacją.

CZYM JEST RBI I JAKIE SĄ GŁÓWNE ELEMENTY TEJ METODOLOGII?

Risk-based Inspection to proces oceny i zarządzania ryzykiem, który koncentruje się na rozszczelnieniach urządzeń ciśnieniowych w instalacjach procesowych, wynikających z pogorszenia się stanu technicznego tych urządzeń na skutek oddziaływania jednego bądź kilku aktywnych mechanizmów degradacji. W tym procesie ryzykiem zarządza się głównie przez inspekcje [1].

Stosowana metodologia opiera się na uznanych i stosowanych w tym zakresie standardach technicznych publikowanych przez Amerykański Instytut Naftowy (American Petroleum Institute, API).

Głównym dokumentem opisującym metodologię RBI jest standard API RP 580 Risk-based Inspection zawierający zasadnicze wymagania dla systemu zarządzania ryzykiem urządzeń ciśnieniowych oraz główne założenia RBI.

Metodologia RBI pozwala na zaplanowanie rodzajów, zakresów i terminów inspekcji na podstawie wyników analizy ryzyka związanego z potencjalnym występowaniem i prędkością degradacji materiałów podczas eksploatacji urządzeń [2].

W tym celu wymagane jest udokumentowanie procesu analizy prawdopodobieństwa wystąpienia uszkodzeń w analizowanych urządzeniach, jak również konsekwencji wynikających z potencjalnego ich rozszczelnienia.

Stosuje się do tego ilościową analizę ryzyka opisaną standardem API RP 581 Risk-based Inspection Methodology, zawierającą modele predykcyjne, dzięki którym możliwe jest obliczenie prawdopodobieństwa rozszczelnienia analizowanego urządzenia i predykcja jego zmian w przyjętym do analizy okresie, a zatem pozwalającą na predykcję jego stanu technicznego.

Risk-based Inspection, jak sama nazwa wskazuje, jest metodą opartą na analizie ryzyka, a więc oprócz wyliczenia prawdopodobieństwa uszkodzenia niezbędne jest również wyliczenie wynikających z niego konsekwencji. Zawarte w normie API RP 581 modele pozwalają na wyliczenie ilości uwolnionych substancji, ich dyspersję oraz efekty fizyczne tych uwolnień, takie jak pożary, wybuchy czy skażenie toksyczne. Pozwala to określić potencjalny obszar, który może zostać objęty tymi konsekwencjami.

Risk-based Inspection, w odróżnieniu od powszechnie stosowanych w przemyśle narzędzi do analizowania zagrożeń i ryzyka, takich jak HAZOP (Hazard and Operability Study), LOPA (Layer of Protection Analysis) czy QRA (Quantitative Risk Assessment), jest metodą predykcyjną zawierającą model opisujący zmiany ryzyka w funkcji czasu. Jest też narzędziem do ciągłego zarządzania ryzykiem, wymagającym stworzenia w organizacji odpowiednich procesów oraz ich implementacji do obowiązującego systemu zarządzania organizacją. Wdrażając Risk-based Inspection w organizacji, należy opracować, udokumentować i uruchomić cztery kluczowe elementy RBI (rys. 1).

Rys. 1. Kluczowe elementy RBI

Implementacja kluczowych elementów RBI wymaga wdrożenia przez organizację tzw. Programu RBI [3], który obejmuje całość działań prowadzonych w celu opracowania, wdrożenia i utrzymania Programu Badań Eksploatacyjnych opracowanych dla każdego urządzenia na podstawie wyników analizy ryzyka.

Zastosowanie wymienionych standardów narzucało konieczność stworzenia zasad pozwalających na implementację w praktyce dozorowej predykcyjnych technik ustalania wymagań dla inspekcji urządzeń ciśnieniowych. **W tym celu w marcu 2017 roku UDT opublikował pierwszą edycję specyfikacji technicznej WUDT-RBI „Warunki Urzędu Dozoru Technicznego – Planowanie inspekcji urządzeń ciśnieniowych w oparciu o analizę ryzyka RBI (Risk-based Inspection). Wymagania ogólne, tryb postępowania, dokumentacja". W 2022 r. opublikowano znowelizowaną edycję warunków [4].**

Warunki te określają zasady funkcjonowania Programu RBI. Obejmuje on wykonanie analizy bezpieczeństwa eksploatacji urządzeń technicznych z wykorzystaniem metodologii RBI oraz wdrożenie Programu Badań Eksploatacyjnych [4].

Kluczowe elementy Risk-based Inspection wymagają utworzenia przez organizację wdrażającą RBI udokumentowanego systemu zarządzania i utrzymania dokumentacji, kwalifikacji personelu, wymagań dotyczących danych, spójności programu i aktualizacji analiz oraz udokumentowanej metodologii zarządzania ryzykiem za pośrednictwem inspekcji, kontroli parametrów procesowych i innych działań ograniczających ryzyko.

System ten nazywany jest Systemem zarządzania RBI, a zadania z nim związane zawarte są w standardzie API RP 580 oraz warunkach WUDT-RBI. System obejmuje 10 obszarów (rys. 2).

System zarzadzania RBI

- Procedury obejmujące wdrożenie, zarządzanie i ponowną ocenę Programu RBI
- Role i odpowiedzialność osób zaangażowanych w Program RBI oraz wymagania w zakresie ich wyszkolenia i doświadczenia
- Wymagania w zakresie dokumentowana założeń przyjmowanych podczas analizy RBI
- Ramy czasowe, dla których analiza RBI ma zastosowanie
- Wymagane dane do analizy RBI
- Cele ryzyka (Risk Targets)
- Program audytów systemu zarządzania
- Zakres i granice stosowania (np. zakłady, procesy, instalacje, rodzaje urządzeń itp.)
- Czynniki wymuszające przeprowadzenie ponownej oceny analizy RBI (walidacji), np. zmiany procesowe, uszkodzenia, przekroczenie ustalonych IOW itp.
- Interwały przeprowadzenia ponownej oceny (walidacji) analizy RBI

System zarządzania bezpieczeństwem procesowym PSM

- Zarządzanie i administracja (Leadership and Administration)
- Dostępność informacji i danych z zakresu bezpieczeństwa procesowego (Process Safety Information)
- Analizy zagrożeń (Process Hazard Analysis)
- Zarządzanie zmianami (Management of Change)
- Procedury operacyjno-ruchowe (Operating Procedures)
- Praktyka bezpiecznej pracy (Safe Work Practices)
- Szkolenia (Training)
- Integralność mechaniczna (Mechanical Integrity)
- Przeglądy bezpieczeństwa przed uruchomieniem instalacji (Pre-Startup Safety Review)
- Procedury awaryjne (Emergency Response)
- Analiza zdarzeń i postępowanie powypadkowe (Incident Investigation)
- Podwykonawcy (Contractors)
- Ocena systemu zarządzania (Management System Assessment)

Rys. 2. Zakres audytu Programu RBI

Wymóg formalnego stworzenia przez organizacje wdrażające RBI udokumentowanego Systemu zarządzania RBI jest związany z ustanowieniem przez UDT zasad jego weryfikacji. Obejmuje to potwierdzenie, że System RBI został wdrożony i jest utrzymywany.

- Urząd Dozoru Technicznego przeprowadza Audyt RBI obejmujący 10 wyżej wymienionych obszarów Systemu zarządzania RBI oraz 13 obszarów Systemu zarządzania bezpieczeństwem procesowym PSM (Process Safety Management), które mają bezpośredni wpływ na poprawne funkcjonowanie Programu RBI.

- Kryteriami audytu są WUDT-RBI oraz załącznik 2A standardu API RP 581 zawierający kryteria audytu PSM. Audyt przeprowadzany jest przed rozpoczęciem analizy RBI oraz okresowo, nie rzadziej niż co 5 lat.

- Wdrożenie analizy RBI umożliwia prowadzenie udokumentowanych procesów analiz obejmujących identyfikację zagrożeń związanych z eksploatacją urządzenia, określenie potencjalnych mechanizmów uszkodzeń i miejsc ich występowania. Pozwala również na ustalenie odpowiedniego sposobu detekcji przy zastosowaniu badań diagnostycznych zawartych w Programie Badań Eksploatacyjnych (PBE) opracowanym na podstawie wyników uzyskanych z analizy RBI.

- Zanim jednak powstanie Program Badań Eksploatacyjnych, niezbędne jest przeprowadzenie złożonego procesu analizy RBI, która dokonywana jest przez interdyscyplinarny zespół składający się z inżynierów eksploatującego oraz wyznaczonych inspektorów UDT.

Tabela 1. Skład zespołu RBI

SPECJALISTA RBI (LIDER ZESPOŁU RBI) Jest osobą reprezentującą eksploatującego. Posiada wiedzę z zakresu metodologii RBI oraz procesów, które realizowane są w urządzeniach objętych analizą RBI.
SPECJALISTA DS. INSPEKCJI URZĄDZEŃ OBJĘTYCH ANALIZĄ Osoba odpowiedzialna za gromadzenie danych dotyczących stanu technicznego urządzeń oraz historii ich inspekcji, awarii, napraw i modernizacji. Do jej zadań należy również ocena skuteczności dotychczas przeprowadzanych inspekcji oraz efektywne wdrażanie zaleceń z analiz RBI w tym zakresie.
SPECJALISTA DS. KOROZJI Osoba odpowiedzialna za identyfikację potencjalnie aktywnych mechanizmów degradacji oraz za ocenę ich aktywności, przy uwzględnieniu parametrów procesowych, środowiska, materiałów konstrukcyjnych, zastosowanych technik spajania i wytwarzania itp.
INŻYNIER PROCESU Jest odpowiedzialny za zapewnienie informacji na temat przebiegu procesu, rozumie powiązania i zagrożenia w nim występujące, stosowane reżimy produkcyjne, odmiany surowców i produktów, wartości i zmiany parametrów procesowych. Inne obowiązki pełnione przez inżyniera procesu to dostarczanie dokumentów zawierających informacje dotyczące możliwych odstępstw od normalnych warunków pracy (np. rozruch, zatrzymanie), nietypowych zdarzeń, składu poszczególnych gazów i cieczy procesowych oraz ich potencjalnej toksyczności i palności.
PERSONEL OPERACYJNY I PERSONEL UTRZYMANIA RUCHU Osoby odpowiedzialne za przeglądy, konserwację i naprawę urządzeń. Mogą zostać zaangażowane w prowadzenie inspekcji wraz ze specjalistą ds. inspekcji. Powinny znać stan techniczny urządzeń lub dysponować zapisami z przeprowadzonych czynności, dbać o aktualność dokumentacji technicznej, dysponować informacjami o konstrukcji urządzeń i potencjalnych problemach technicznych.
PRZEDSTAWICIEL KIEROWNICTWA Jest odpowiedzialny za pozyskiwanie zasobów potrzebnych do wdrożenia RBI. Jest to osoba decyzyjna w kwestiach zarządzania ryzykiem oraz podejmująca decyzje dotyczące implementacji rekomendacji z analizy RBI.
ANALITYK RYZYKA (PRZEDSTAWICIEL EKSPLOATUJĄCEGO) Osoba odpowiedzialna za zbieranie wszystkich danych od członków zespołu i przeprowadzanie obliczeń ryzyka. Ponadto analityk ryzyka zajmuje się definiowaniem potrzebnych danych do analizy, definiowaniem wymaganej dokładności zbieranych danych, weryfikacją danych i założeń, wprowadzaniem danych do programu komputerowego (jeżeli jest używany), kontrolą danych wejściowych/wyjściowych, przedstawianiem wyników w sposób zrozumiały i przygotowywaniem raportów z analiz RBI.
ANALITYK RYZYKA (PRZEDSTAWICIEL UDT) Jest odpowiedzialny za nadzór przebiegu prowadzonej analizy w celu utrzymania jej zgodności z przyjętymi standardami odniesienia oraz za weryfikację danych zebranych podczas analizy.
INNE OSOBY POWOŁYWANE DO ZESPOŁU RBI W zależności od potrzeb dostarczają informacje w celu przeprowadzenia analizy RBI lub opiniują przyjęte założenia. Osoby te powinny odbyć podstawowe przeszkolenie z metodologii RBI.

WYMAGANIA I ZASADY PROWADZENIA RBI

RBI jest procesem ciągłym służącym do zarządzania ryzykiem urządzeń. Uproszczony schemat blokowy RBI (rys. 3) prezentuje cykl rozpoczynający się procesem zbierania danych i informacji niezbędnych do przeprowadzenia analizy RBI, na którą składają się ocena prawdopodobieństwa i ocena skutków uszkodzenia. Następnie uzyskane wyniki służą do wyznaczenia ryzyka i dokonania jego oceny względem ustalonych kryteriów akceptacji ryzyka. Na tej podstawie opracowywany jest Plan Inspekcji zawierający wymagania dotyczące zakresów i terminów inspekcji, które są uzależnione od zidentyfikowanych i potencjalnych mechanizmów degradacji określonych dla każdego z urządzeń i ryzyka związanego z ich eksploatacją.

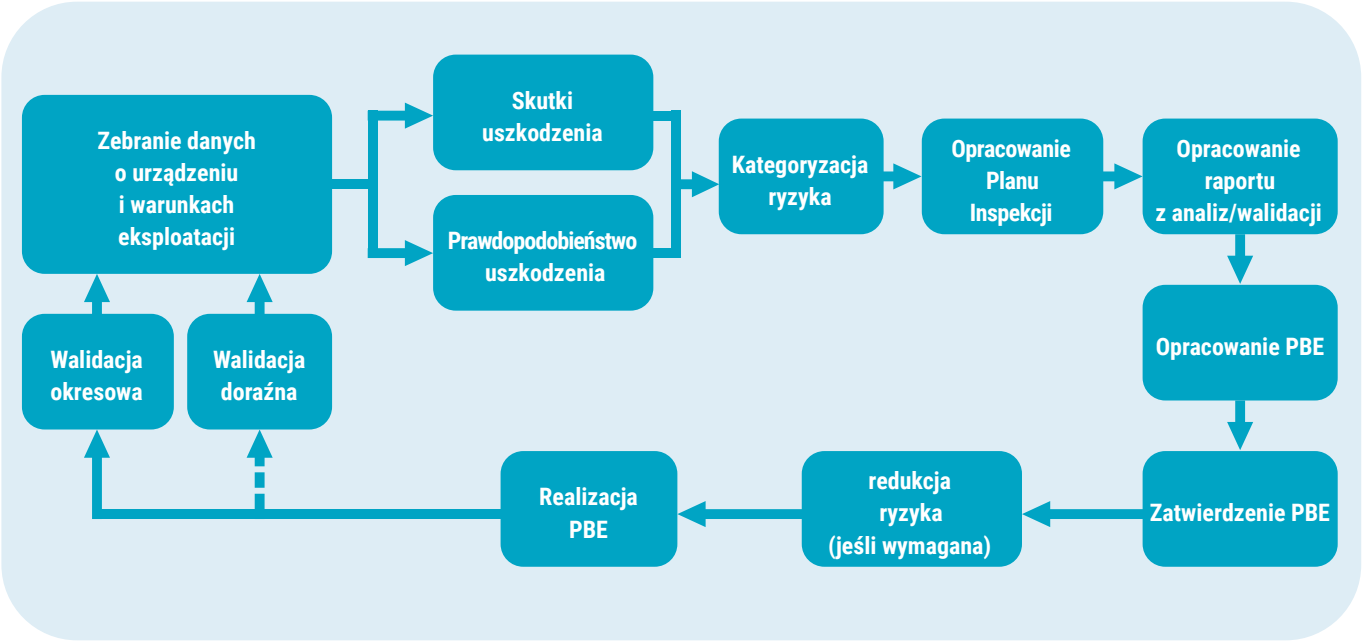
Plan inspekcji stanowi wynik analizy RBI i jest częścią raportu z analizy RBI, który podsumowuje jej przebieg, potwierdzając tym samym jej zgodność z przyjętymi wymaganiami odniesienia.

Raport stanowi podstawę do opracowania Programu Badań Eksploatacyjnych, który następnie podlega zatwierdzeniu przez UDT.

Proces ten opiera się na założeniach modelu ciągłego doskonalenia PDCA (Plan-Do-Check-Act) Deminga.

Program Badań Eksploatacyjnych opracowywany jest na czas nie dłuższy niż okres objęty analizą RBI, tzn. na okres, dla którego dokonano predykcji ryzyka, zazwyczaj nieprzekraczający 10 lat. Program Badań Eksploatacyjnych zawiera konkretne elementy określone dla każdego urządzenia.

- Rodzaje, zakres, miejsca oraz terminy inspekcji
- Wymagane kategorie efektywności inspekcji
- Kryteria akceptacji wyników badań NDT i DT
- Wymagania dla personelu i laboratoriów wykonujących badania NDT i DT
- Forma raportowania badań NDT i DT
- Niezbędne do monitorowania parametry technologiczne
- Zasady i terminy walidacji analizy RBI oraz Programu Badań Eksploatacyjnych (PBE)



Rys. 3. Cykl RBI

Po zatwierdzeniu przez UDT Program Badań Eksploatacyjnych wchodzi w etap realizacji, podczas którego wykonywane są zaplanowane czynności, czyli głównie badania NDT oraz monitorowanie kluczowych dla degradacji urządzeń parametrów procesowych i technologicznych. Monitorowanie tych parametrów przebiega zgodnie z zatwierdzonym PBE oraz procedurami zawartymi w Systemie zarządzania RBI. Niewątpliwie jest to jeden z kluczowych elementów PBE wpływających na jego skuteczność. Po przekroczeniu określonych w PBE wartości ustalonych parametrów technologicznych niezbędne jest przeprowadzenie walidacji doraźnej, której celem jest ustalenie, czy realizowany PBE pozwoli na utrzymanie odpowiedniego poziomu ryzyka lub określenie niezbędnych zmian.

JAKIE KORZYŚCI PŁYNĄ Z WDROŻENIA RBI?

Wdrożenie skutecznego Programu RBI oparte jest na metodach łączących prognozowanie mechanizmów i tempa degradacji urządzeń oraz odpowiedni dobór technik inspekcyjnych.

- Dzięki temu możliwe jest w większym stopniu **prowadzenie nieinwazyjnych inspekcji i badań podczas pracy instalacji.**

- Pozwala też na **dopasowywanie terminów i zakresów badań inwazyjnych**, wymagających dostępu do wnętrza urządzeń, do terminów zatrzymania instalacji procesowych przy zachowaniu bezpieczeństwa na poziomie nie niższym niż dotychczas.

- Umożliwia również zdobycie **szczegółowych informacji o stanie technicznym urządzeń** i możliwych zdarzeniach związanych z ich eksploatacją.

Ideą zarządzania ryzykiem przez inspekcje jest wykonywanie badań celowanych, tzn. dobranych tak, aby wykrywać skutki aktywności mechanizmów degradacji w zidentyfikowanych obszarach narażenia.

Dzięki takiemu podejściu nakłady na inspekcje urządzeń kierowane są przede wszystkim na urządzenia o największym ryzyku oraz na urządzenia, które narażone są na intensywne procesy degradacji, np. szybko postępującą korozję. W wyniku przeprowadzonej analizy RBI określane są również kluczowe ze względu na degradację urządzeń parametry technologiczne, co pozwala na optymalizację procesów produkcyjnych z uwzględnieniem ich wpływu na tempo degradacji urządzeń.

Jednym z narzędzi stosowanych do zarządzania parametrami technologicznymi z uwzględnieniem ich wpływu na integralność mechaniczną urządzeń jest tzw. zarządzanie oknami operacyjnymi IOW (Integrity Operating Windows) [5].

- Wartością dodaną wynikającą z wdrożenia metodologii RBI jest podniesienie kompetencji w zakresie predykcji stanu technicznego urządzeń. Dotyczy to w szczególności oceny aktywności mechanizmów degradacji oraz doboru i wykorzystania w znacznie większym stopniu dostępnych metod badań nieniszczących do oceny mechanizmów degradacji.

- Zauważalna jest również poprawa kultury bezpieczeństwa osób zaangażowanych w ten proces. Uczestnicząc w procesie RBI, nie tylko ocenia się stan techniczny urządzenia, ale przede wszystkim zastanawia się nad jego przyszłością, biorąc pod uwagę warunki pracy oraz możliwe do przewidzenia zmiany, które mogą negatywnie wpłynąć na stan techniczny urządzenia.

UWAGA

Uzyskanie wymiernych efektów wdrożenia RBI wymaga kompetencji i ogromnej pracy zespołu inżynierów, stosowania narzędzi informatycznych, pozwalających na przeprowadzenie obliczeń ryzyka, i determinacji w dążeniu do celu. Sukces we wdrażaniu zależy również od jakości i dostępności danych niezbędnych do przeprowadzenia obliczeń. Jakość danych determinowana jest przez ich dokładność i wiarygodność.

SPOSOBY WYZNACZANIA RYZYKA

Zapraszamy do dokładnego zapoznania się ze sposobem wyznaczania ryzyka z zastosowaniem metodologii RBI opartej na zasadach opisanych w standardzie API RP 581 3rd. edition, publikowanym przez Amerykański Instytut Naftowy (American Petroleum Institute).

Zagłębienie się w metodologię wymaga przypomnienia kilku podstawowych pojęć.

Metodologia RBI, to proces zarządzania ryzykiem, które można zdefiniować w ogólny sposób jako wpływ niepewności na cele [1].

W kontekście celu, dla którego określamy wartość **ryzyka** w RBI, można zdefiniować je jako połączenie **prawdopodobieństwa** wystąpienia jakiegoś zdarzenia w rozpatrywanym okresie i **konsekwencji** (zazwyczaj negatywnych) związanych z tym zdarzeniem [2]. Jeśli prawdopodobieństwo i skutki zostaną wyrażone liczbowo, to ryzyko jest ich iloczynem [3]. Można zatem wyrazić je zależnością:

$$R(t) = P(t) \cdot C \qquad (1),$$

gdzie:
R (t) – ryzyko
P (t) – prawdopodobieństwo
C – konsekwencje

R (T) – RYZYKO

RBI znajduje zastosowanie najczęściej do zarządzania ryzykiem urządzeń ciśnieniowych w przemyśle rafineryjnym i petrochemicznym, w którym konsekwencje wiążące się z uwolnieniem substancji niebezpiecznych o właściwościach palnych, wybuchowych czy toksycznych wynikają często z uszkodzenia urządzeń ciśnieniowych. Można zatem zależność (1) zapisać w postaci:

$$R(t) = POF(t) \cdot COF \qquad (2),$$

gdzie:
R (t) – ryzyko
POF (t) – prawdopodobieństwo uszkodzenia (*probability of failure*)
COF – konsekwencje uszkodzenia (*consequence of failure*)

Należy odpowiedzieć również na istotne pytanie: Co reprezentuje wyliczone w powyższy sposób ryzyko? Poszukując odpowiedzi, trzeba zastanowić się nad pojęciami **ryzyka absolutnego (bezwzględnego)** oraz tzw. **ryzyka względnego**.

Obliczanie ryzyka jest bardzo złożone. Wynik jest funkcją wielu czynników, które mogą wpływać na ryzyko.

Obliczanie **bezwzględnego ryzyka** może być bardzo czasochłonne i kosztowne, a często nawet niewykonalne z odpowiednią dokładnością, ponieważ ilość niewiadomych może być zbyt duża. Potencjalne rozszczelnienie urządzenia ciśnieniowego w instalacji przemysłowej może być spowodowane kombinacją wielu czynników, takich jak: degradacja materiału konstrukcyjnego, błędy konstrukcyjne i montażowe, niesprawność urządzeń zabezpieczających, pożar, sabotaż i wiele innych. Określenie wartości ryzyka obejmującego wszystkie czynniki i ich wzajemne zależności może nie być możliwe lub być nieopłacalne ekonomicznie. RBI koncentruje się na systematycznym określeniu ryzyka względnego wynikającego z konsekwencji pogorszenia się stanu technicznego urządzeń na skutek oddziaływania aktywnych mechanizmów degradacji [4]. W ten sposób można uszeregować urządzenia lub ich komponenty względem wartości ryzyka wynikającego z określonych przyczyn i wówczas określić niezbędne działania mające na celu jego redukcję do poziomu akceptowalnego.

Na tym etapie wiemy już, że RBI pozwala na określenie dla urządzeń ryzyka względnego będącego funkcją ich stanu technicznego, który w większości przypadków jest zależny m.in. od czasu eksploatacji, czyli czasu ekspozycji na warunki powodujące jego degradację. W RBI stosuje się tzw. współczynnik uszkodzenia (Damage Factor, DF) pozwalający uwzględnić przyspieszoną degradację urządzenia w wyniku oddziaływania aktywnych mechanizmów degradacji[1].

Można zatem opisać **ryzyko rozszczelnienia urządzenia wynikające z uszkodzenia powodowanego jego pogorszeniem stanu technicznego, na skutek oddziaływania mechanizmów degradacji**, zależnością:

$$R(t) = \underbrace{gff_f \, FM_s \cdot D_f(t)_f}_{POF(t)} \cdot COF \qquad (3),$$

gdzie:

R (t) – ryzyko
gff – prawdopodobieństwo awarii wynikające z danych generycznych (*generic failure frequency*)
FM_s – współczynnik systemu zarządzania bezpieczeństwem
D_f (t) – współczynnik uszkodzenia (DF)
COF – konsekwencje uszkodzenia (*consequence of failure*)

POF (t) – PRAWDOPODOBIEŃSTWO USZKODZENIA (PROBABILITY OF FAILURE)

Ryzyko względne, określane w metodologii RBI wg standardu API RP 581, wyznacza się zatem jako iloczyn kliku niżej wymienionych czynników.

Prawdopodobieństwo awarii (gff) – wyznaczone dla określonych typów komponentów na podstawie dużej populacji danych uszkodzeń komponentów, które nie obejmują oddziaływania określonych mechanizmów degradacji. Wartości współczynnika opublikowane są w standardzie API RP 581 dla określonych komponentów urządzeń.

Współczynnik (FMs) – reprezentuje wynik audytu systemu zarządzania bezpieczeństwem procesowym (omówiony w poprzednim wydaniu biuletynu INSPEKTOR).

Współczynnik uszkodzenia (Df (t)) – zasadniczą funkcją tego współczynnika jest statystyczna ocena liczby uszkodzeń, które mogą występować w urządzeniu w funkcji czasu jego eksploatacji, oraz skuteczności wykonywanych inspekcji mających na celu ocenę tych uszkodzeń.

UWAGA

Należy pamiętać, że współczynnik uszkodzenia nie służy do ustalenia, czy oceniany komponent nadaje się do dalszej eksploatacji, a jedynie do planowania inspekcji.

Jeżeli w wyniku prowadzonych inspekcji stwierdzone zostaną uszkodzenia, ich ocenę powinno się przeprowadzić z zastosowaniem metodologii Fitness-For-Service opisanej standardem API RP 579-1/ASME FFS-1. Na podstawie uzyskanych wyników należy podjąć decyzję o dalszej eksploatacji.

Współczynnik (D_f (t)) jest modyfikatorem dla danych generycznych opisanych przez (gff), tak aby określić specyficzne dla danego komponentu prawdopodobieństwo uszkodzenia uwzględniające tempo degradacji i skuteczność wykonywanych inspekcji.

Zasady wyznaczania współczynnika uszkodzeń (D_f (t)) opisano w rozdziale 2 standardu API RP 581, który zawiera procedury jego obliczania dla następujących grup mechanizmów degradacji:

• pocienienia o charakterze ogólnym i lokalnym	$D_{f\text{–}gov}^{thin}$
• uszkodzenia wykładzin komponentu	D^{elin}
• uszkodzenia zewnętrzne (pocienienia i pęknięcia)	$D_{f\text{–}gov}^{extd}$
• naprężeniowe pękanie korozyjne (Stress Corrosion Cracking)	$D_{f\text{–}gov}^{scc}$
• wysokotemperaturowy atak wodorowy (High Temperature Hydrogen Attack, HTHA)	$D_{f\text{–}gov}^{htha}$
• kruche pękanie (Brittle Fracture)	$D_{f\text{–}gov}^{brit}$
• zmęczenie mechaniczne elementów rurociągów (Mechanical Fatigue)	$D_{f\text{–}gov}^{mfat}$

W sytuacji gdy aktywny jest więcej niż jeden mechanizm degradacji, współczynnik uszkodzeń obliczany jest dla każdego mechanizmu i następnie sumowany w celu określenia całkowitego (Df (t)) dla komponentu, zgodnie z poniższymi zasadami. Na rysunku nr 1 przedstawiono zasady wyznaczania współczynnika (Df (t)) dla więcej niż jednego mechanizmu degradacji, tym samym określenia prawdopodobieństwa wystąpienia uszkodzeń POF(t) wynikających z aktywności tych mechanizmów degradacji.

OGÓLNE ZASADY WYZNACZANIA WSPÓŁCZYNNIKA USZKODZEŃ UWZGLĘDNIAJĄCEGO WPŁYW ODDZIAŁYWANIA AKTYWNYCH MECHANIZMÓW DEGRADACJI NA PRAWDOPODOBIEŃSTWO USZKODZENIA URZĄDZENIA

Pokazane powyżej zależności pozwalają na wyznaczenie w sposób powtarzalny wartości prawdopodobieństwa uszkodzenia analizowanego komponentu POF (T). Należy jednak mieć na uwadze fakt, że uzyskanie właściwych danych służących do wyznaczenia cząstkowych składowych poszczególnych współczynników wymaga zaangażowania całego **zespołu RBI**.

Istotą poprawnej i wiarygodnej analizy RBI jest zadbanie, aby wykorzystane dane do wyznaczenia współczynnika uszkodzeń opierały się na rzetelnej analizie aktywności mechanizmów degradacji oraz na zwalidowanych danych. Wymaga to wysokich kompetencji członków zespołu RBI, jak również skutecznego systemu zarządzania całym Programem RBI.

COF – KONSEKWENCJE USZKODZENIA (CONSEQUENCE OF FAILURE)

Drugim składnikiem ryzyka, które matematycznie wyraża zależność (3), są konsekwencje wynikające z rozszczelnienia (COF). W omawianej metodologii RBI konsekwencje uszkodzenia wyznacza się głównie w celu dokonania rankingu komponentów względem ich ryzyka. Następnie zależnie od wartości ryzyka ustala się, które komponenty urządzeń należy poddać inspekcji w pierwszej kolejności, tj. w jakim terminie oraz w jakim zakresie.

W odróżnieniu od prawdopodobieństwa uszkodzenia (POF) konsekwencje nie są zależne od czasu i przyjmuje się, że nie ulegają zmianie w okresie objętym analizą.

W przypadku gdy zaistnieją okoliczności, które mogą wpłynąć na wielkość konsekwencji, niezbędne jest przeprowadzenie walidacji analizy RBI i ponowne wyznaczenie ryzyka z uwzględnieniem zmian.

W standardzie API RP 581 zawierającym algorytm wyliczenia konsekwencji proces ten możemy przeprowadzić na dwóch poziomach.

Level 1 – pozwala na wykonanie obliczeń dla zdefiniowanych reprezentatywnych substancji.

Level 2 – pozwala na obliczenie konsekwencji zasadniczo dla dowolnej substancji, po zdefiniowaniu wymaganych parametrów.

W podejściu stosowanym przez Urząd Dozoru Technicznego wymagane jest wyznaczenie konsekwencji na poziomie Level 2.

Konsekwencje w RBI możemy wyrazić w dwóch jednostkach:

- jako powierzchnię narażoną na konsekwencje, wyrażoną najczęściej w [m²],
- w jednostkach monetarnych, uwzględniających zdefiniowane grupy kosztów poniesionych w wyniku wystąpienia potencjalnych konsekwencji.

Standard API RP 581 zawiera również oddzielny algorytm dla wyznaczenia konsekwencji uszkodzenia atmosferycznych zbiorników magazynowych, w którym konsekwencje wyrażone są tylko w jednostkach monetarnych.

Wdrożenie skutecznego Programu RBI zapewnia narzędzie do ciągłego doskonalenia utrzymania ruchu i systematycznego zmniejszania ryzyka związanego z uszkodzeniami urządzeń ciśnieniowych w instalacjach przemysłowych [2].

Analiza konsekwencji w RBI jest przeprowadzana w celu rozróżnienia analizowanych elementów urządzeń na podstawie istotności potencjalnych skutków ich awarii, które wynikają z rozszczelnienia się powłoki ciśnieniowej wskutek oddziaływania aktywnych mechanizmów degradacji.

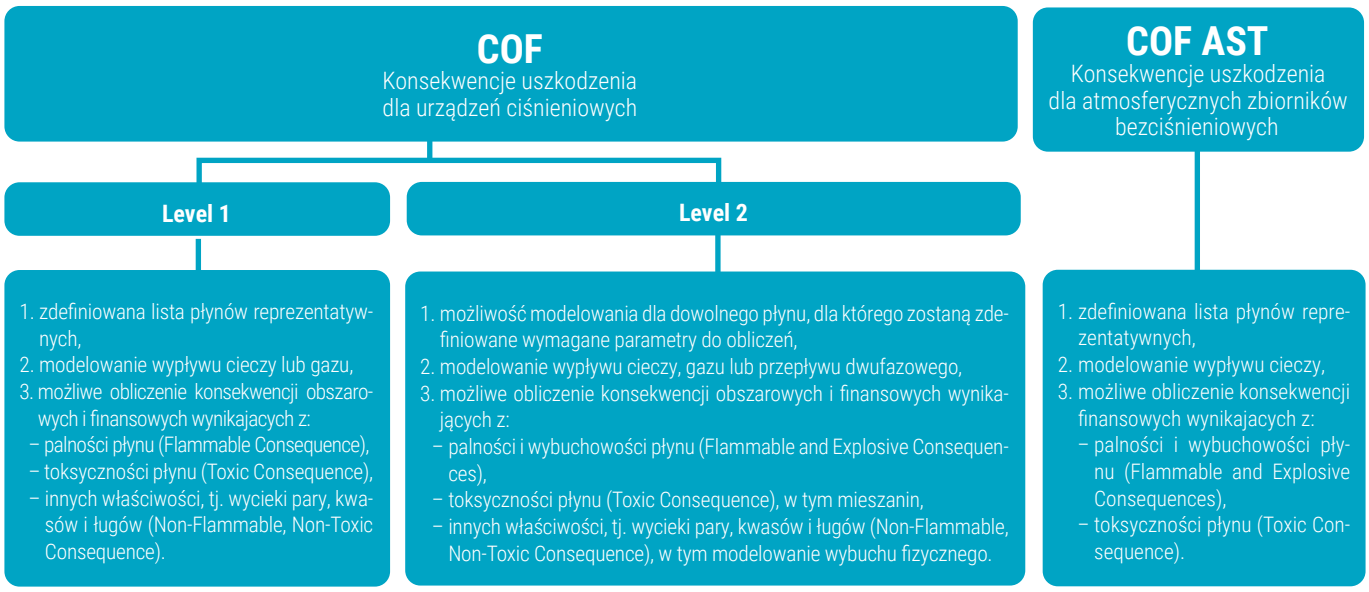
Definiując potencjalne konsekwencje, należy podkreślić, że metodologia RBI opisana standardem API RP 581 zawiera model obliczeniowy pozwalający na przeprowadzenie analizy potencjalnych konsekwencji uszkodzenia COF (consequence of failure). Analiza powinna być powtarzalnym, spójnym i wiarygodnym oszacowaniem tego, co może się wydarzyć, gdyby wystąpiła awaria ocenianego elementu.

Konsekwencje możemy ogólnie skategoryzować na mające wpływ na:
a) bezpieczeństwo osób,
b) środowisko,
c) finanse organizacji.

Jak wspomniano wcześniej, analizę przeprowadza się w celu oszacowania następstw, które mogą wystąpić z powodu określonego typu uszkodzenia, zwykle wynikającego ze zidentyfikowanych mechanizmów degradacji oddziałujących na konstrukcję analizowanego komponentu.

- Obliczenia wykonywane są według metodologii opisanej w rozdziale 3 standardu API RP 581, która zawiera metodykę obliczeń na dwóch poziomach analizy zbieżnej z ww. kategoryzacją konsekwencji.
- Metodologia COF poziomu 1 jest szczegółowo opisana w rozdziale 4 standardu, gdzie znajduje się zdefiniowana lista płynów reprezentatywnych, dla których możliwe jest zastosowanie tego poziomu.
- Metodologia poziomu 2 obliczenia COF jest opisana w rozdziale 5, który zawiera znacznie bardziej szczegółowe zasady obliczania konsekwencji, i może być stosowana do szerszego zakresu płynów.
- Oddzielnie w standardzie API RP 581 opisano zasady określania konsekwencji dla atmosferycznych zbiorników magazynowych (AST) i omówiono je w rozdziale 6.

Ogólną zawartość poszczególnych modeli obliczeniowych można przedstawić schematycznie (rys. 4). Istotne są ich ograniczenia, ponieważ w znacznej mierze decydują o możliwości zastosowania. **Z tego właśnie powodu w realizowanych przy udziale UDT wdrożeniach metodologii RBI stosowany jest dla urządzeń ciśnieniowych poziom 2 (Level 2).** Wynika to między innymi z faktu ograniczeń poziomu 1 (Level 1) do możliwości modelowania wyłącznie płynów reprezentatywnych oraz stosunkowo uproszczonego modelu obliczeń konsekwencji wynikających z potencjalnego wybuchu.



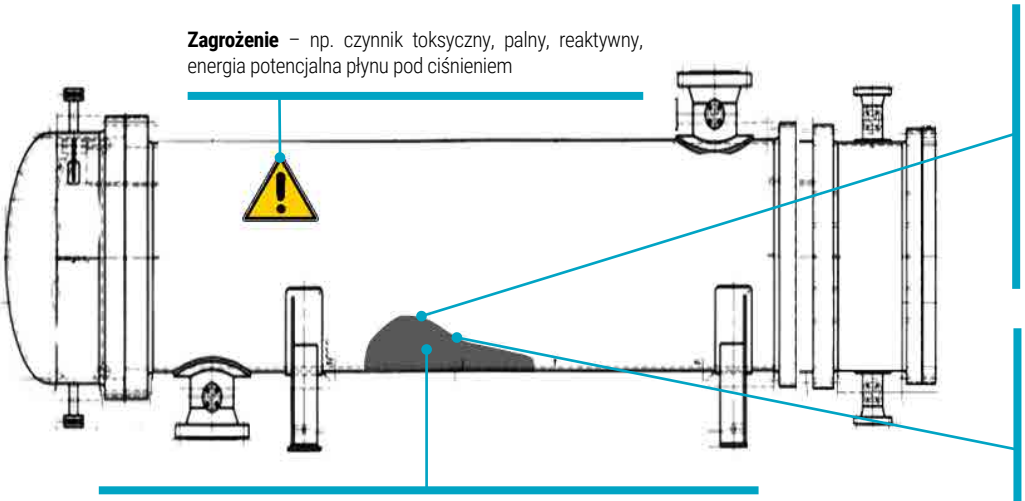
Rys. 4. Modele obliczeń konsekwencji uszkodzenia (COF) zawarte w standardzie API RP 581

Analiza konsekwencji w metodologii RBI skupia się na skutkach wynikających z oddziaływania aktywnych mechanizmów degradacji powodujących określone typy uszkodzeń. Dlatego istotne jest z punktu widzenia prowadzonej analizy określenie, w jaki sposób analizowany element może ulec uszkodzeniu.

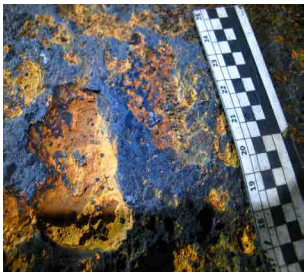
Standard API RP 581 w rozdziale dotyczącym analizy konsekwencji definiuje, jakie sposoby uszkodzeń powinny być modelowane.

Zależnie od typów uszkodzeń powodowanych przez określone mechanizmy degradacji, tj. lokalny ubytek materiału, pęknięcia czy zmiany własności wytrzymałościowych, należy wybrać najbardziej prawdopodobny sposób, w jaki urządzenie ulegnie uszkodzeniu, czyli Failure Mode.

Kluczowe czynniki, które będą miały wpływ na wybór sposobu uszkodzenia, zostaną uwzględnione w modelu obliczeniowym konsekwencji uszkodzenia (rys. 5). Standard API RP 581 określa możliwe do przyjęcia średnice reprezentatywnych otworów o różnych wymiarach (rys. 5), które wykorzystywane są w obliczeniach teoretycznego natężenia wypływu, a tym samym do ustalania ilości substancji uwolnionej w wyniku uszkodzenia.



Numer otworu reprezentatywnego	Wymiar reprezentatywnego otworu uwolnienia	Zakres średnic reprezentowanych (mm)	Średnica reprezentatywnego otworu uwolnienia d_n (mm)
1	mały	0 do 6,4	d_1 = 6,4
2	średni	> 6,4 do 51	d_2 = 25
3	duży	> 51 do 152	d_3 = 102
4	rozerwanie	> 152	d_4 = min [D, 406]



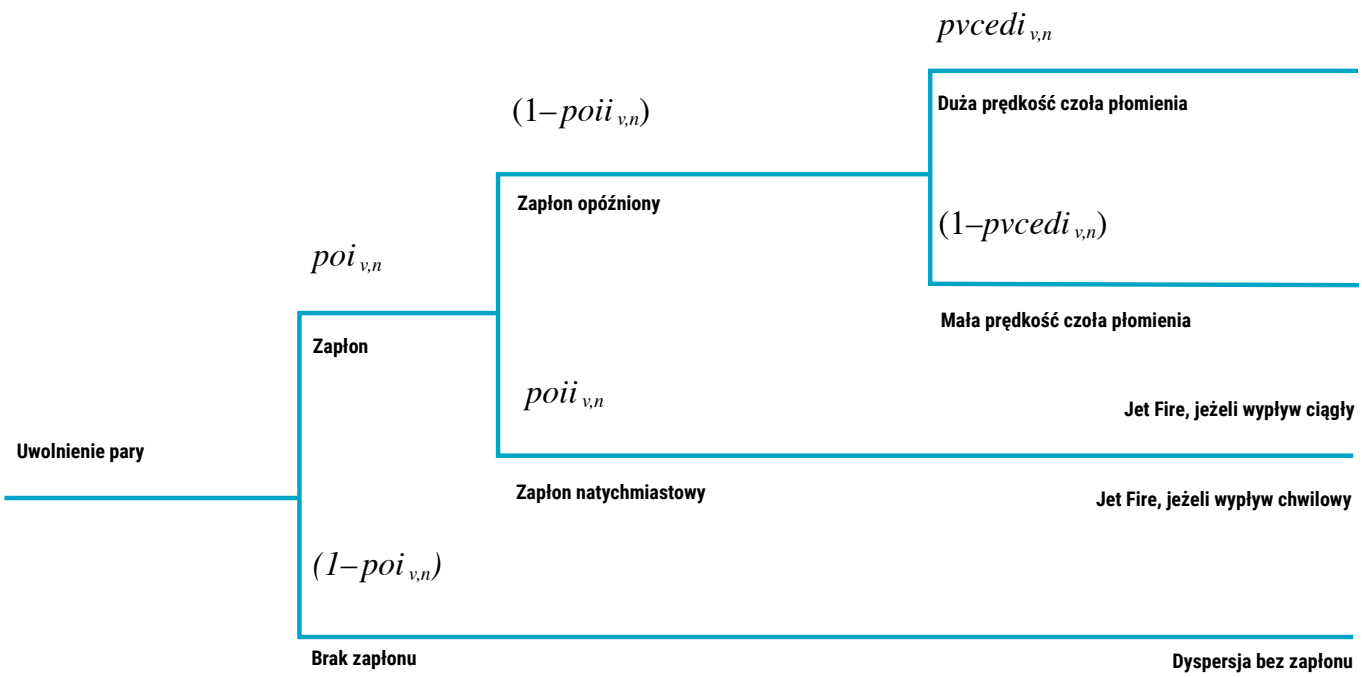
Rys. 5. Sposoby uszkodzenia uwzględniane w modelu COF zgodnie ze standardem API RP 581

Kolejnymi istotnymi czynnikami wpływającymi na wielkość konsekwencji są parametry substancji znajdującej się wewnątrz analizowanego urządzenia, które należy określić dla dwóch stanów:

- w parametrach magazynowania, czyli ciśnieniu i temperaturze roboczej,
- przy parametrach otoczenia, czyli po uwolnieniu substancji do otoczenia.

Jednym z parametrów mających wpływ na wielkość konsekwencji wynikających z wybuchu płynu, który uwolni się do otoczenia, jest temperatura robocza. Będzie ona wpływała nie tylko na to, jaka faza płynu uwalnianego będzie modelowana (ciecz, para lub przepływ dwufazowy), ale również w sytuacji przechowywania płynu powyżej temperatury samozapłonu (AIT), po uwolnieniu w atmosferze tlenowej nastąpi zapłon. W innym przypadku scenariusz może rozwinąć się do zapłonu opóźnionego zainicjowanego do efektywnego źródła zapłonu. Wówczas konsekwencje mogą być znacznie większe.

W celu obliczenia prawdopodobieństwa wpływu tych czynników na wielkość konsekwencji w analizie COF na poziomie 2 według standardu API RP 581 należy określić to prawdopodobieństwo oraz wielkość skutków według zdefiniowanych drzew zdarzeń.



Rys. 3. Drzewo zdarzeń dla wypływu pary wg modelu COF Level 2 standardu API RP 581 [1]

Ogólnie można zatem podsumować, że danymi wejściowymi do obliczeń konsekwencji są: dane o właściwości płynu, którego uwolnienie będzie modelowane, oraz średnice reprezentatywnych otworów ustalone na podstawie spodziewanych uszkodzeń.

Kolejnym etapem wynikającym z algorytmu postępowania, jak pokazano na diagramie przedstawionym na rysunku nr 3, jest określenie dostępnej do uwolnienia ilości płynu. Tę ilość określamy na podstawie masy płynu znajdującej się w analizowanym urządzeniu oraz ilości płynu, który może zostać doprowadzony do tego urządzenia z urządzeń połączonych. Taką grupę urządzeń, dla których należy przyjąć założenie, że w przypadku rozszczelnienia któregokolwiek z nich uwolni się cały zgromadzony płyn, nazywamy INVENTORY GROUP.

Zależnie od wielkości tej grupy oraz natężenia wypływu z określonego reprezentatywnego otworu należy ustalić, czy modelowany wypływ będzie miał charakter chwilowy, czy będzie to wypływ ciągły.

PRZYKŁADY

Przykładowo dla zbiornika o stosunkowo niewielkim napełnieniu oraz niewielkiej pojemności inventory group, do której został zakwalifikowany. W przypadku wystąpienia katastroficznego pęknięcia tego urządzenia, które modelujemy jako pole przekroju otworu o średnicy tego urządzenia, ale nie większej niż 16" (406 mm), nastąpi w krótkim czasie uwolnienie całej masy dostępnej w urządzeniu oraz inventory group. Taki wypływ będzie wypływem chwilowym. Przeciwieństwem będą uwolnienia z otworów o małych średnicach z urządzeń o stosunkowo dużej ilości dostępnego płynu do uwolnienia. Zasady ustalenia charakteru wypływu zawarte są w standardzie API RP 581.

Określając wielkość konsekwencji, bierzemy również pod uwagę wpływ na wielkość uwolnienia systemów bezpieczeństwa, w które wyposażona jest instalacja technologiczna analizowanego urządzenia. Standard API RP 581 przewiduje możliwość uwzględnienia dwóch grup systemów bezpieczeństwa, tj. systemu detekcji wycieku oraz skuteczności izolacji poszczególnych inventory group od siebie. Poniżej przedstawiono tabelę 4.5 zaczerpniętą z części 3 standardu API RP 581, w której zawarto wytyczne do klasyfikacji tych systemów do trzech grup. Zależnie od konfiguracji zastosowanych systemów możliwe jest zredukowanie poprzez zastosowanie współczynników korekcyjnych ilości uwolnionego w przypadku wycieku płynu (współczynnik $fact_{di}$) oraz ograniczenia czasu trwania wycieku (współczynnik Id_{max}).

Tabela 1. Wytyczne do klasyfikacji systemów bezpieczeństwa do trzech grup (wg tabeli 4.5 – część 3 standardu API RP 581 [3])

$$D_{f\text{-}total} = D_{f\text{–}gov}^{thin} + D_{f\text{–}gov}^{extd} + D_{f\text{–}gov}^{scc} + D_{f}^{htha} + D_{f\text{–}gov}^{brit} + D_{f}^{mfat} \quad (4)$$

Pocienienia wewnętrzne Uszkodzenia zewnętrzne

$$D_f^{Thin} = \max\left[\left(\frac{D_{fB}^{Thin} \cdot F_{IP} \cdot F_{DL} \cdot F_{WD} \cdot F_{AM} \cdot F_{SM}}{F_{OM}}\right), \; 0{,}1\right]$$

- Korozja spowodowana przez kwas solny
- Korozja spowodowana obecnością siarki i kwasów naftenowych
- Korozja wysokotemperaturowa w atmosferze H2/H2S
- Korozja spowodowana przez kwas siarkowy
- Korozja spowodowana przez kwas fluorowodorowy
- Korozja spowodowana wodorosiarczkiem amonu
- Korozja aminowa
- Wysokotemperaturowe utlenianie
- Korozja spowodowana przez kwaśną wodę
- Korozja spowodowana przez wodę chłodzącą
- Korozja ziemna
- Korozja spowodowana dwutlenkiem węgla
- Korozja den atmosferycznych zbiorników magazynowych

W modelu uwzględnia się również modyfikatory zwiększające lub zmniejszające przewidywaną wartość współczynnika:

F_{OM} – współczynnik uwzględniający skuteczność systemu monitoringu korozji, jeśli zastosowano
F_{IP} – dla obszarów, gdzie następuje mieszanie czynników (mix point), obszarów wtrysku chemikaliów lub wody (injection point)
F_{DL} – dla elementów rurociągów, w których stale lub okresowo występuje brak przepływu i związana z tym większa prędkość korozji (deadleg)

Współczynniki dedykowane dla atmosferycznych zbiorników magazynowych:

F_{WD} – współczynnik uwzględniający występowanie złączy spawanych
F_{AM} – współczynnik uwzględniający efektywność utrzymania ruchu zbiornika wg standardu API STD 653
F_{SM} – współczynnik uwzględniający wpływ osiadania zbiornika

W przypadku gdy urządzenie wyposażone jest w wykładzinę wewnętrzną zabezpieczającą materiał konstrukcyjny przed oddziaływaniem mechanizmów degradacji współczynnik uszkodzenia ze względu na pocienienia możemy zredukować, zgodnie z zależnością:

$$D_{f\text{-}gov}^{hin} = \min\left[D_f^{thin}, \; D_f^{elin}\right]$$

$$D_f^{elin} = D_{fB}^{elin} \cdot F_{LC} \cdot F_{OM}$$

W tym przypadku F_{LC} jest współczynnikiem uwzględniającym kondycję wykładziny, a F_{OM} współczynnikiem uwzględniającym skuteczność systemu monitoringu szczelności wykładziny.

Uszkodzenia zewnętrzne

$$D_{f\text{-}gov}^{extd} = \max\left[D_f^{extf}, \; D_f^{CUIF}, \; D_f^{ext\text{-}CLSCC}, \; D_f^{CUI\text{-}CLSCC}\right]$$

Stale ferrytyczne
- Korozja atmosferyczna elementów nieizolowanych
- Korozja pod izolacją

Stale austenityczne
- Pękanie naprężeniowe chlorkowe elementów izolowanych i nieizolowanych

Kruche pękanie

$$D_{f\text{-}gov}^{b\text{-}it} = \max\left[\left(D_f^{brit} + D_f^{tempe}\right), \; D_f^{885F}, \; D_f^{sigma}\right]$$

- Kruche pękanie (Brittle Fracture)
- Kruchość z powodu starzenia wysokotemperaturowego (Temper Embrittlement)
- Kruchość w temperaturze 474°C (885°F Embrittlement)
- Kruchość fazy Sigma i Chi (Sigma Phase Embrittlement)

Naprężeniowe pękanie korozyjne

$$D^{scc} = \max\left[\begin{matrix} D_f^{caustic}, D_f^{amine}, D_f^{scc}, D_f^{HIC/SOHIC\text{–}H_2S}, D_f^{ACSCC}, \\ D_f^{PASCC}, D_f^{CLSCC}, D_f^{HSC\text{–}HF}, D_f^{HIC/SOHIC} \end{matrix}\right]$$

- Pękanie naprężeniowe kaustyczne (Caustic Stress Corrosion Cracking (Caustic Embrittlement))
- Pękanie naprężeniowe aminowe (Amine Stress Corrosion Cracking)
- Pękanie naprężeniowe siarczkowe (Pęcherze wodorowe / Nawodornianie / Pękanie naprężeniowe) (Wet H2S Damage (Blistering / HIC / SOHIC / SSC))
- Pękanie naprężeniowe węglanowe (Alcaline Carbonate Stress Corrosion Cracking)
- Pękanie naprężeniowe w środowisku kwasu wielotionowego (Polythionic Acid Stress Corrosion Cracking (PASCC))
- Pękanie naprężeniowe chlorkowe (Chloride Stress Corrosion Cracking (CLSCC))

Zmęczenie mechaniczne elementów rurociągów

Współczynnik wyznacza się, uwzględniając m.in. geometrię rurociągu i sposób podłączenia odgałęzień, charakter wibracji i liczbę cykli.

Wysokotemperaturowy atak wodorowy

D_f^{mfat} Dotyczy elementów ze stali węglowej, C-½ Mo i stali niskostopowych Cr-Mo narażonych na wysokotemperaturowy atak wodorowy. Wartość współczynnika wyznacza się w odniesieniu do tzw. reprezentatywnych krzywych Nelsona (Representative Nelson Curve) zawartych w standardzie API RP 941, uwzględniając rodzaj materiału, temperaturę roboczą i ciśnienie parcjalne wodoru.

D_f^{mfat}

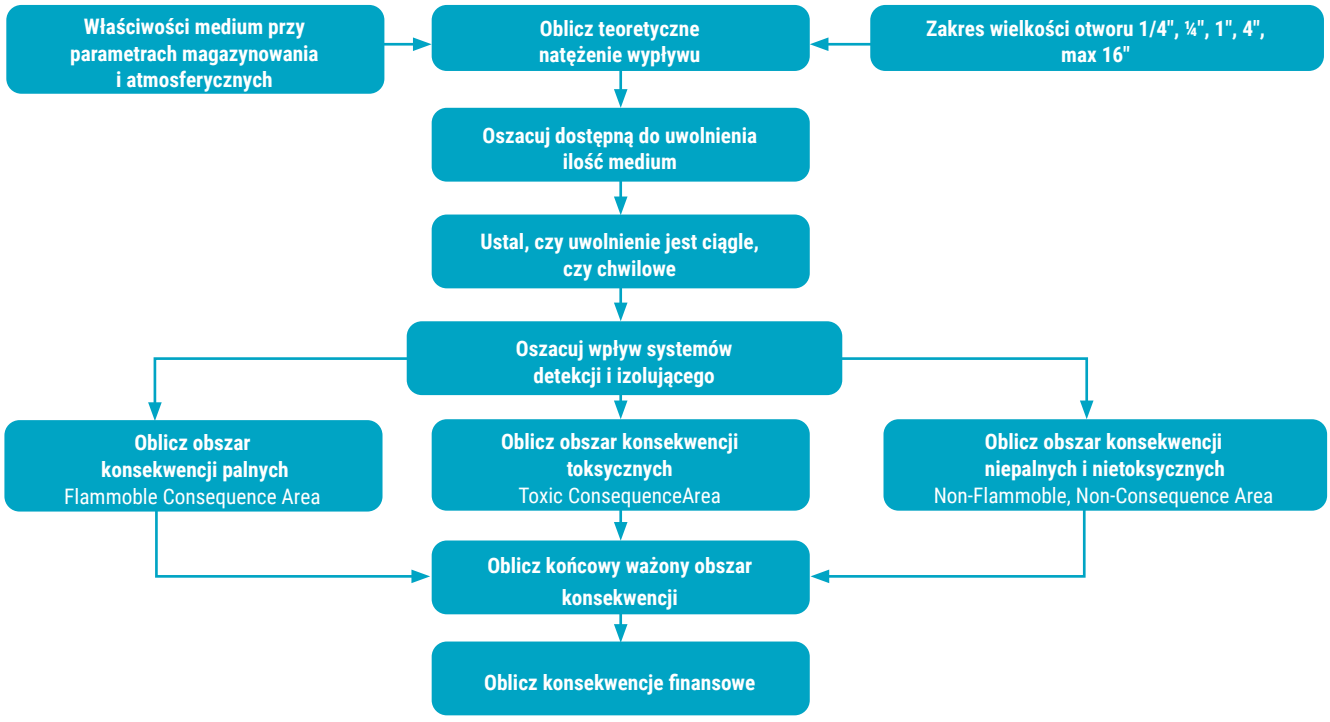
Typ systemu detekcji	Klasyfikacja
Oprzyrządowanie zaprojektowane specjalnie do wykrywania wycieku poprzez monitorowanie zmian warunków pracy w systemie (tj. obniżenie ciśnienia lub przepływu)	A
Odpowiednio rozmieszczone detektory w celu wykrycia wycieku medium z przestrzeni ciśnieniowych	B
Detekcja wizualna, monitoring wizyjny (kamery) lub detektory wycieku medium monitorujące marginalny zakres systemu	C
Typ systemu separującego	**Klasyfikacja**
Systemy separujące lub wyłączania awaryjnego aktywowane bezpośrednio z oprzyrządowania procesowego lub detektorów wycieku, bez interwencji operatora	A
Systemy separujące lub wyłączania awaryjnego aktywowane przez operatorów w sterowni lub innych odpowiednich miejscach oddalonych od miejsca wycieku	B
Separowanie zależne od zaworów obsługiwanych ręcznie	C

Następnie zależnie od zastosowanego poziomu obliczeń (poziom 1 lub 2) wyliczamy ilość uwolnionego w przypadku awarii płynu. Obliczamy za tym obszary dla konsekwencji palnych, toksycznych oraz niepalnych i nietoksycznych. Wynikiem tych obliczeń będzie obszar wyrażony w metrach kwadratowych, który zostanie objęty konsekwencjami.

- **Obszary konsekwencji palnych i wybuchowych obliczane są z zastosowaniem zdefiniowanych drzew zdarzeń, o których wspomniano wcześniej.** Wykorzystujemy zawarte w nich prawdopodobieństwa określonych efektów fizycznych, tj. BLEVE (Boiling Liquid Expanding Vapour Explosion), VCE (Vapour Cloud Explosion).
  - Obszar konsekwencji obliczany jest w odniesieniu do poważnych obrażeń personelu i uszkodzenia wyposażenia wskutek promieniowania cieplnego i ciśnienia wybuchu.
  - Straty finansowe wyliczane są na podstawie uszkodzeń wyposażenia znajdującego się w obszarze dotkniętym konsekwencjami.
- **Obszar konsekwencji toksycznych obliczany jest z zastosowaniem modeli dyspersji par substancji toksycznych w powietrzu**. W przypadku personelu narażonego na oddziaływanie toksyczne – par – zależnie od ich stężenia w powietrzu. Straty finansowe wyliczane są na podstawie obszaru dotkniętego uwolnieniem.
- **Obszar konsekwencji niepalnych i nietoksycznych oblicza się na podstawie zagrożeń dla personelu wynikających z rozprysku substancji chemicznych**. Na przykład mówimy o substancjach żrących, oparzeniu płynami uwalnianymi o wysokiej temperaturze, m.in. parą wodną, oraz wybuchach fizycznych wynikających z rozprężania się gazów. Obszar konsekwencji obliczany jest podobnie jak konsekwencje palne w odniesieniu do poważnych obrażeń personelu i uszkodzenia wyposażenia.

W każdym z powyższych modeli obliczeniowych stosujemy odpowiednie kryteria w odniesieniu do personelu, wyposażenia, np. dopuszczalne narażenie na promieniowanie cieplne czy dopuszczalne ciśnienia dla wybuchów.

Wyznaczenie obszarów narażonych na konsekwencje stanowi zasadniczy element modelowania konsekwencji i w praktyce może być wykonane z zastosowaniem dedykowanego oprogramowania obliczeniowego.



Rys. 4. Schemat postępowania przy wyznaczaniu konsekwencji uszkodzenia COF Level 1 wg standardu API RP 581

Po wyznaczeniu poszczególnych obszarów skutków należy wyznaczyć końcowy obszar objęty konsekwencjami z uwzględnieniem prawdopodobieństwa wystąpienia poszczególnych obszarów wynikających z modeli obliczeniowych. Końcowy obszar dotknięty konsekwencjami to największy obszar uzyskany z poszczególnych modeli obliczeniowych, którego prawdopodobieństwo wystąpienia jest największe.

PRZYKŁAD

Przykładowo w modelowaniu wypływu płynu o właściwościach palnych, ale jednocześnie toksycznych, wybór końcowych konsekwencji zależeć będzie między innymi od prawdopodobieństwa zapłonu takiego płynu po jego uwolnieniu i stężeń w powietrzu, które mogą zagrażać personelowi. Jeżeli płyn będzie cechował się stosunkowo wąskim zakresem stężeń palnych (stężenie pomiędzy dolną i górną granicą palności) i jednocześnie minimalna energia zapłonu dla tego płynu będzie stosunkowo wysoka, to prawdopodobieństwo zapłonu będzie znacznie mniejsze niż dyspersja bez zapłonu. W takim przypadku prawdopodobieństwo skażenia toksycznego będzie zdecydowanie większe, a zatem będzie decydowało o wielkości obszaru narażonego na skutki końcowe.

Modelowanie konsekwencji w metodologii RBI jest niezbędnym elementem do ustalenia wartości ryzyka, a zatem stanowi nieodłączny element RBI.

W artykule przedstawiono zasady modelowania konsekwencji w bardzo ogólnym ujęciu, którego celem jest określenie głównych założeń. Praktyczne obliczenia są przeprowadzane z zastosowaniem dedykowanego oprogramowania i opierają się na modelowaniu dyspersji gazów, modelowaniu wybuchów fizycznych i cieplnych czy wyznaczaniu natężenia strumienia ciepła powstałego wskutek spalania płynów.

Analizując wyniki obliczeń ryzyka, należy zweryfikować założenia przyjmowane do obliczeń oraz szereg danych służących do modelowania. Z tego powodu stosowane oprogramowanie obliczeniowe powinno posiadać model obliczeniowy zgodny w przyjętym standardem odniesienia, którym jest w przypadku urządzeń podlegających dozorowi technicznemu standard API RP 581, będący uznanym standardem odniesienia w tym zakresie.

Analizując wyniki obliczeń konsekwencji zgodnie z przedstawioną metodologią, należy mieć na uwadze, że posiada ona również ograniczenia, jak chociażby nieuwzględnienie efektu domina. Jednak ponieważ w metodologii RBI wyznaczenie konsekwencji służy do dokonania rankingu ryzyka poszczególnych analizowanych komponentów, ograniczenie to nie wpływa w sposób istotny na jej skuteczność.

Wyniki uzyskiwane z przedstawionego modelu obliczeń konsekwencji mogą również służyć jako dane wejściowe do zarządzania bezpieczeństwem procesowym zakładu, w tym zapobiegania poważnym awariom przemysłowym. Jednak ich bezpośrednie zastosowanie wymaga oceny, aby zachować spójność z wdrożonym w zakładzie systemem zarządzania bezpieczeństwem.

SKUTECZNOŚĆ RBI

Podsumowując, należy wspomnieć jeszcze o dwóch istotnych kwestiach dotyczących skuteczności procesu RBI, którymi są: oprogramowanie stosowane do prowadzenia obliczeń ryzyka oraz kompetencje personelu, który je przeprowadza.

OPROGRAMOWANIE

Skuteczne prowadzenie obliczeń ryzyka w RBI wymaga stosowania specjalnego oprogramowania. W przypadku gdy RBI ma być wykorzystywane do planowania inspekcji urządzeń podlegających dozorowi technicznemu, wybór oprogramowania musi być uzgodniony z UDT. Model obliczeniowy powinien być zgodny ze standardem API RP 581. Oczywiście, obliczenia stosowane w RBI mogą być wykonane ręcznie, jednakże nie zapewniałoby to wystarczającej dynamiki obliczeń i byłoby nieskutecznym narzędziem do zarządzania ryzykiem.

PERSONEL

Konieczne jest zapewnienie odpowiednich kompetencji personelu, który wykonuje obliczenia ryzyka. Niedobór wiedzy w zakresie metodologii prowadzenia obliczeń może skutkować pominięciem istotnych z punktu widzenia obliczeń elementów. Wynik uzyskany z obliczeń zależy głównie od danych wejściowych, które analityk ryzyka wykonujący obliczenia ma obowiązek zwalidować. **Niezrozumienie ryzyka, czyli czynników, które wpływają na jego wartość, jest podstawowym i niedopuszczalnym błędem w stosowaniu RBI.** Sytuacja, w której na postawione pytanie: „Dlaczego należy wykonać taki zakres badań?" pada odpowiedź: „Tak wyszło z obliczeń" lub „Program policzył", może być sygnałem, że nie zrozumiano czynników wpływających na wartość ryzyka.

Istotą RBI jest praca zespołu ekspertów, których zadaniem jest obiektywna ocena zebranych i wiarygodnych danych w celu zrozumienia czynników wpływających na ryzyko i wykonanie obliczeń, pokazujących jego wartość. **Na tej podstawie można uzyskać odpowiedzi na pytania: kiedy, w jakim zakresie i jakimi metodami wykonać inspekcje urządzeń, aby były one skuteczne do utrzymania ryzyka na akceptowalnym poziomie.**

Staramy się nieustannie doskonalić realizowane procesy i między innymi dlatego UDT przystąpiło do pilotażowego projektu wdrożenia metodologii tzw. cyfrowego bliźniaka (Digital Twin) dla urządzeń ciśnieniowych w instalacji przemysłowej, który w naturalny sposób jest rozwinięciem zdobytych przez ostatnie kilkanaście lat doświadczeń w predykcji zużycia urządzeń w przemyśle rafineryjnym i petrochemicznym.

Literatura:

1. PN-ISO 31000, marzec 2012, Zarządzanie ryzykiem Zasady i wytyczne.
2. API RP 580 Risk-based Inspection, third edition, February 2016.
3. API RP 581 Risk-based Inspection Methodology, third edition, April 2016.
4. WUDT-RBI Warunki Urzędu Dozoru Technicznego – Planowanie inspekcji urządzeń ciśnieniowych w oparciu o analizę ryzyka RBI (Risk Based Inspection). Wymagania ogólne, tryb postępowania, dokumentacja. Edycja 11.2022.

ANALIZA MECHANIZMÓW DEGRADACJI

MGR INŻ. TOMASZ KLINKOSZ

Ekspert Urządzeń Ciśnieniowych
Dział Oceny Zgodności
Oddział w Gdańsku
Urząd Dozoru Technicznego

Utrzymanie bezpieczeństwa instalacji przemysłowej wymaga skoordynowania wielu obszarów wpływających na bezpieczeństwo i na ciągłość działania zakładu produkcyjnego. Jednym z głównych narzędzi stosowanych w celu zapewnienia bezpieczeństwa procesów przemysłowych jest skuteczny system zarządzania bezpieczeństwem procesowym, tzw. PSMs (Process Safety Management System).

Istotnym elementem zapewnienia bezpieczeństwa instalacji przemysłowej ujętym również w ww. systemie, jest integralność mechaniczna infrastruktury przemysłowej, w tym urządzeń służących do magazynowania, przesyłania lub prowadzenia procesu technologicznego, czyli zbiorników i rurociągów. Integralność tych urządzeń zależy między innymi od mechanizmów degradacji, które na nie oddziałują zarówno od strony wewnętrznej jak i zewnętrznej.

Czym zatem są mechanizmy degradacji i dlaczego ich prawidłowa identyfikacja oraz analiza ich aktywności przyczyniają się do zapewnienia bezpieczeństwa eksploatacji urządzeń?

MECHANIZMY DEGRADACJI

Istnieje wiele definicji pojęcia **mechanizm degradacji**, które zależnie od kontekstu, czy też branży dla której zostały sformułowane mogą być odmiennie rozumiane. W kontekście instalacji przemysłowych, w szczególności instalacji rafineryjnych, chemicznych i petrochemicznych właściwe wydaje się stosowanie definicji zaproponowanej przez Amerykański Instytut Naftowy API (American Petroleum Institute).

W standardzie API RP 581 [1] określającym zasady obliczeń w procesie RBI (Risk-based Inspection) mechanizm degradacji zdefiniowano jako proces, który z czasem powoduje zmiany materiału (w skali mikro i/lub makro), szkodliwe dla stanu materiału lub jego własności mechanicznych.

Mechanizmy degradacji mają zazwyczaj charakter narastający, kumulujący się, a w niektórych przypadkach niemożliwy do naprawienia. Typowe mechanizmy degradacji obejmują korozję, atak chemiczny, pełzanie, erozję, zmęczenie, pękanie i starzenie termiczne [1]. Termin mechanizm degradacji stosowany jest już powszechnie w wielu obszarach przemysłu i został również zdefiniowany w polskich dokumentach.

Warunki Urzędu Dozoru Technicznego WUDT-RBI definiują mechanizm degradacji – jak poniżej.
Mechanizm Degradacji (Damage Mechanism) – mechanizm powodujący pogorszenie własności materiałów konstrukcyjnych urządzenia, który może wywołać powstawanie określonych typów uszkodzeń (damage modes) mogących wpływać na integralność urządzenia, takich jak:
a) pocienienia (ogólne i miejscowe oraz pitting),
b) pęknięcia powierzchniowe,
c) pęknięcia podpowierzchniowe,
d) mikropęknięcia i mikropory,
e) zmiany struktury materiału,
f) zmiany wymiarowe,
g) pęcherze,
h) zmiany własności materiałowych [2].

Jak wynika z powyższych definicji, mechanizmy degradacji obejmują szereg uszkodzeń identyfikowanych w urządzeniach. Aby skutecznie zarządzać tym obszarem bezpieczeństwa niezbędna jest wnikliwa analiza mająca na celu identyfikację mechanizmów degradacji, które mogą oddziaływać na konstrukcję podczas i w warunkach jej eksploatacji. Standard API RP 571 Damage Mechanisms Affecting Fixed Equipment in the Refining Industry [3] systematyzuje i określa podstawowy zbiór mechanizmów degradacji dla przemysłu. Poniżej przedstawiono wykaz mechanizmów degradacji ujętych w tym dokumencie.

Tablica 1. Wykaz mechanizmów degradacji wg API RP 571 [3]

	KOROZJA OGÓLNA, LOKALNA I WŻEROWA
1.	Korozja galwaniczna (Galvanic Corrosion)
2.	Korozja atmosferyczna (Atmospheric Corrosion)
3.	Korozja pod izolacją (Corrosion Under Insulation (CUI))
4.	Korozja spowodowana przez wodę chłodzącą (Cooling Water Corrosion)
5.	Korozja spowodowana przez wodę kotłową/kondensat (Boiler Water Condensate Corrosion)
6.	Korozja spowodowana przez CO_2 (CO_2 Corrosion)
7.	Korozja w punkcie rosy w gazach spalinowych (Flue Gas Dew Point Corrosion)
8.	Korozja mikrobiologiczna (Microbiologically Induced Corrosion (MIC))
9.	Korozja ziemna (gruntowa) (Soil Corrosion)
10.	Korozja kaustyczna (Caustic Corrosion)
11.	Ubytek pierwiastków stopowych (Dealloying)
12.	Korozja grafitowa żeliwa (Graphitic Corrosion)
13.	Korozja aminowa (Amine Corrosion)
14.	Korozja amoniakalna (Ammonium Bisulfide Corrosion (Alkaline Sour Water)
15.	Korozja spowodowana przez chlorek amonu (Ammonium Chloride Corrosion)
16.	Korozja spowodowana przez HCl (Hydrochloric Acid (HCl) Corrosion)
17.	Korozja w atmosferze H_2/H_2S (High Temp H_2/H_2S Corrosion)
18.	Korozja spowodowana przez kwas fluorowodorowy (Hydrofluoric (HF) Acid Corrosion)
19.	Korozja spowodowana przez kwas naftenowy (Naphthenic Acid Corrosion (NAC))
20.	Korozja fenolowa (Phenol (Carbonic Acid) Corrosion)
21.	Korozja spowodowana przez kwas fosforowy (Phosphoric Acid Corrosion)
22.	Korozja spowodowana przez kwaśną wodę (Sour Water Corrosion (Acidic))
23.	Korozja siarkowa (Sulfuric Acid Corrosion)
24.	Korozja spowodowana przez uwodniony kwas organiczny (Aqueous Organic Acid Corrosion)
	KOROZJA WYSOKOTEMPERATUROWA
25.	Wysokotemperaturowe utlenianie (Oxidation)
26.	Korozja siarkowa wysokotemperaturowa (Sulfidation)
27.	Nawęglanie (Carburization)
28.	Odwęglanie (Decarburization)
29.	Pylenie metalu (Metal Dusting)
30.	Korozja spowodowana przez gaz spalinowy (Fuel Ash Corrosion)
31.	Azotowanie (Nitriding)
	PĘKANIE KOROZYJNE
32.	Pękanie naprężeniowe chlorkowe (Chloride Stress Corrosion Cracking (CL–SCC))
33.	Zmęczenie korozyjne (Corrosion Fatigue)
34.	Pękanie naprężeniowe kaustyczne (Caustic Stress Corrosion Cracking (Caustic Embrittlement))
35.	Korozja naprężeniowa amoniakalna (Ammonia Stress Corrosion Cracking)
36.	Kruchość ciekłych metali (Liquid Metal Embrittlement (LME))
37.	Kruchość wodorowa (Hydrogen Embrittlement (HE))
38.	Pękanie naprężeniowe etanolowe (Ethanol Stress Corrosion Cracking)
39.	Pękanie naprężeniowe siarczkowe (Sulfate Stress Corrosion Cracking)

40.	Pękanie naprężeniowe w środowisku kwas wielotionowego (Polythionic Acid Stress Corrosion Cracking (PASCC))
41.	Pękanie naprężeniowe aminowe (Amine Stress Corrosion Cracking)
42.	Pękanie naprężeniowe siarczkowe (Pęcherze wodorowe / Pęknięcia typu HIC, SOHIC, SSC)) (Wet H_2S Damage (Blistering / HIC / SOHIC / SSC))
43.	Pękanie wodorowe naprężeniowe w środowisku HF (Hydrogen Stress Cracking – HF)
44.	Pękanie naprężeniowe węglanowe (Carbonate Stress Corrosion Cracking)
MECHANIZMY MECHANICZNE I METALURGICZNE	
45.	Grafityzacja (Graphitization)
46.	Sferoidyzacja (Softening (Spheroidization))
47.	Kruchość odpuszczenia(Temper Embrittlement)
48.	Starzenie po zgniocie (Strain Aging)
49.	Kruchość w temperaturze 474°C (885°F Embrittlement)
50.	Kruchość fazy Sigma (Sigma Phase Embrittlement)
51.	Kruche pękanie (Brittle Fracture)
52.	Pełzanie + Pękanie wywołane pełzaniem (Creep / Stress Rupture)
53.	Zmęczenie termiczne (Thermal Fatigue)
54.	Krótkotrwałe przegrzanie (Short Term Overheating – Stress Rupture)
55.	Lokalne przegrzanie ścianki wężownic parowych (Steam Blanketing)
56.	Pękanie spoin różnoimiennych (Dissimilar Metal Weld (DMW) Cracking)
57.	Szoki termiczne (Thermal shock)
58.	Erozja/Erozja+korozja (Erosion / Erosion-Corrosion)
59.	Kawitacja (Cavitation)
60.	Zmęczenie mechaniczne (Mechanical Fatigue)
61	Zmęczenie spowodowane drganiami (Vibration-Induced Fatigue)
62.	Degradacja wymurówki /powłoki ognioodpornej (Refractory Degradation)
63.	Pękanie przy ponownym nagrzewaniu (Reheat Cracking)
64.	Spalanie dyfuzyjne metalu w środowisku o podwyższonej zawartości tlenu (Gaseous Oxygen-Enhanced Ignition and Combustion)
INNE MECHANIZMY KOROZYJNE	
65.	Wysokotemperaturowy atak wodorowy (High Temperature Hydrogen Attack (HTHA))
66.	Nawodorowanie tytanu (Titanium Hydriding)

DO CZEGO SŁUŻY ANALIZA MECHANIZMÓW DEGRADACJI?

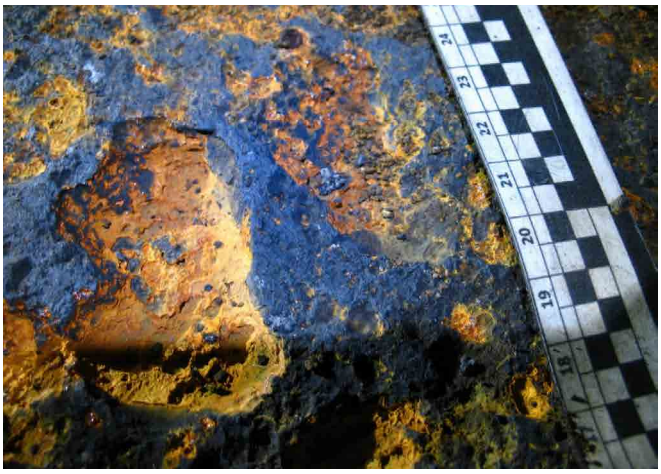
a) Określenie potencjalnie aktywnych mechanizmów degradacji (damage mechanisms)

b) Ocena ich aktywności w poszczególnych komponentach analizowanych urządzeń na podstawie analizy parametrów znaczących

c) Określenie typów uszkodzeń (damage modes)

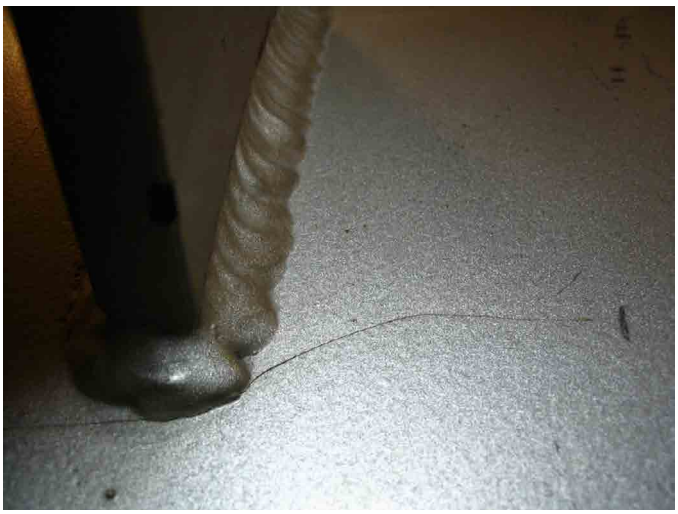
Analizę mechanizmów degradacji prowadzi zazwyczaj specjalista ds. korozji materiałów wspomagany przez zespół osób odpowiedzialnych za dostarczenie wiarygodnych danych służących do identyfikacji i oceny aktywności mechanizmów degradacji. Każdy mechanizm degradacji ma swoją specyfikę. Ustalenia, z jakim mechanizmem degradacji mamy do czynienia dokonuje się na podstawie analizy środowiska warunków pracy urządzenia oraz ich oddziaływania na materiał konstrukcyjny i analizy powodowanych typów uszkodzeń.

Ocenę aktywności poszczególnych mechanizmów degradacji wykonuje się na podstawie znanych kryteriów materiałowych (np. gatunek materiału, twardość, obróbka cieplna po spawaniu, skład chemiczny materiału itp.) i wartości parametrów procesowych (np. temperatura, skład chemiczny medium). Bierze się również pod uwagę obliczenia ich intensywności i podatności urządzenia na pojedyncze mechanizmy degradacji lub grupy tych mechanizmów [2].



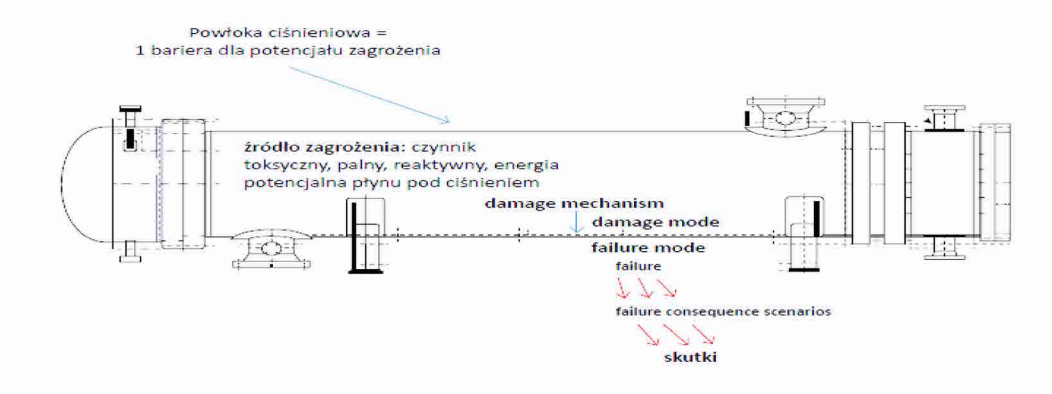
Rys. 1. Obraz wżerów korozyjnych powstałych wewnątrz zbiornika ze stali niestopowej wskutek oddziaływania mechanizmów degradacji - korozji HCL oraz wody kwaśnej

Rys. 2. Obraz lokalnej korozji powstałej na zewnątrz zbiornika ze stali niestopowej wskutek oddziaływania mechanizmu degradacji - korozja pod izolacją (CUI)



Rys. 3. Obraz pęknięć zbiornika ze stali niestopowej wskutek oddziaływania mechanizmu degradacji - zmęczenie spowodowane drganiami

Rolą urządzeń ciśnieniowych w instalacji procesowej jest między innymi utrzymanie przetwarzanego płynu wewnątrz urządzenia w zakresie projektowanych parametrów procesu, takich jak ciśnienie czy temperatura. Urządzenie stanowi zatem barierę ochronną, której kondycja istotnie wpływa na prawdopodobieństwo wystąpienia awarii przemysłowej. Skutkiem awarii tego typu mogą być pożar, wybuch czy skażenie toksyczne potencjalnie groźne dla otoczenia i ludzi. Rozwój takiego scenariusza zazwyczaj rozpoczyna się od perforacji ścianki urządzenia. W przypadku oddziaływania aktywnego mechanizmu degradacji perforacja może nastąpić podczas eksploatacji w zakresie normalnych parametrów procesu.



Rys. 4. Rozwój scenariusza awaryjnego w wyniku oddziaływania mechanizmu degradacji

IDENTYFIKACJA A OCENA PODATNOŚCI MECHANIZMÓW DEGRADACJI?

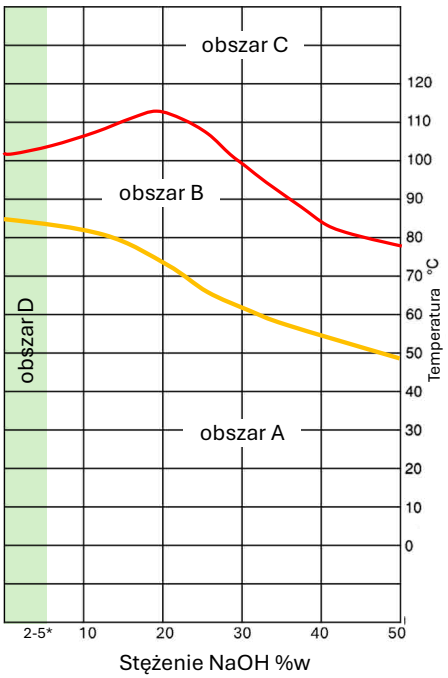
W procesie identyfikacji mechanizmów degradacji, które mogą wystąpić, kluczowe jest ustalenie czy konkretny element urządzenia może być narażony w toku eksploatacji, w tym w warunkach postoju lub odchyleń procesowych na oddziaływanie któregokolwiek z mechanizmów degradacji.

Niezbędne jest zweryfikowanie czynników krytycznych dla każdego z mechanizmów i ustalanie listy potencjalnych mechanizmów degradacji, które następnie należy poddać ocenie pod kątem ich aktywności, a inaczej mówiąc ustalić podatność elementu na dany mechanizm degradacji.

PRZYKŁAD KRYTERIÓW IDENTYFIKACJI MECHANIZM PĘKANIA NAPRĘŻENIOWEGO KAUSTYCZNEGO

Kryteria te zawarte są w standardzie API RP 571 [3], jednakże do pełnej oceny rekomendowany jest przegląd dokumentów źródłowych. W przypadku rozpatrywanego mechanizmu pękania naprężeniowego kaustycznego może to być standard NACE SP0403 Avoiding Caustic Stress Corrosion Cracking of Refinery Equipment and Piping [4], opublikowany przez NACE (National Association of Corrosion Engineers), towarzystwo które opracowuje i wydaje standardy i rekomendowane praktyki mające zastosowanie w analizie mechanizmów degradacji.

Obszary od A do D (rys. 5) są funkcją temperatury roboczej oraz stężenia wagowego ługu sodowego w strumieniu procesowym. Dla każdego obszaru wskazano rekomendowane wymagania materiałowe. Oczywiście w celu identyfikacji podatności na ten mechanizm degradacji niezbędna jest weryfikacja wszystkich wymagań zawartych w dokumencie.	**Najogólniej można stwierdzić, że element wykonany ze stali węglowej i pracujący w temperaturze około 70°C w roztworze ługu sodowego większym niż 23% wymaga spełnienia kryteriów dla obszaru B. W przypadku nie spełnienia tych kryteriów należy uznać, że w elemencie mogą wystąpić pęknięcia naprężeniowe.**



obszar A
Stale węglowe – obróbką cieplna nie jest konieczna
Obróbka cieplna wymagana, jeżeli element wyposażony w parogrzejki

obszar B
Stale węglowe – z obróbką cieplną spoin i elementów giętych
Stopy niklu dla elementów współpracujących w zaworach

obszar C
Należy rozważyć zastosowanie stopów niklu
Stopy niklu dla elementów współpracujących w zaworach

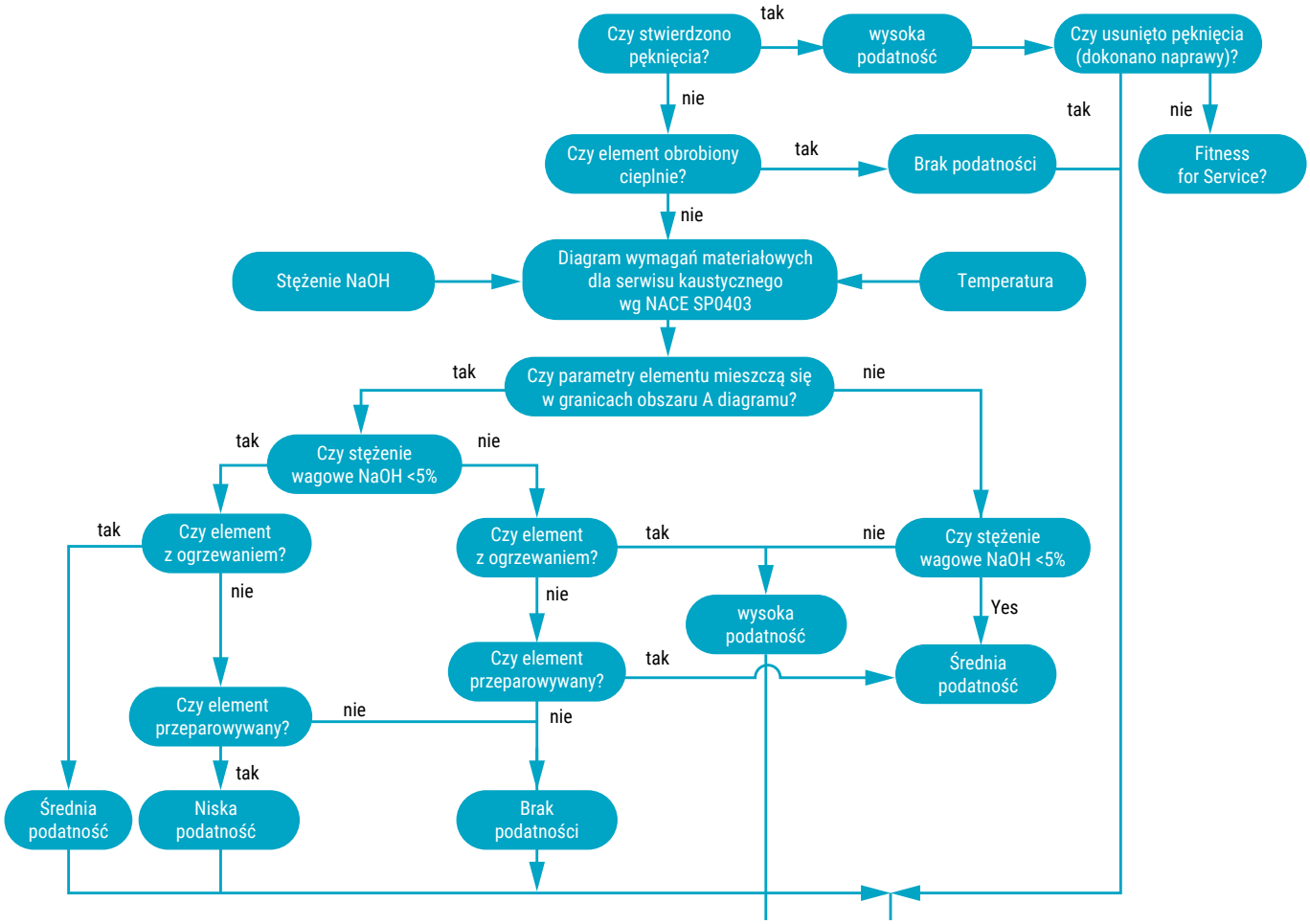
obszar D
Stężenie ługu powyżej 5% może powodować pękanie naprężeniowe. Część użytkowników nie wymaga obróbki cieplnej w tym obszarze.

Rys. 5. Diagram do określenia wymagań dla materiałów pracujących w środowisku kaustycznym (opracowano na podstawie NACE SP 0403 [4])

Większość użytkowników, niezależnie od temperatury, nie wymaga stosowania obróbki cieplnej stali niestopowej jeżeli stężenie ługu sodowego jest mniejsze niż 2% wagowo, natomiast niektórzy użytkownicy używają jako progu stosowania obróbki cieplnej 5% wagowo.

Należy jednak pamiętać, że czasami już od 50 do 100 ppm ługu sodowego w strumieniu może być przyczyną pęknięć, w przypadku możliwości wystąpienia jego lokalnego wzrostu stężenia.

Ocena podatności dla tego mechanizmu degradacji będzie koncentrowała się na ustalaniu wpływu aktywności tego mechanizmu na prawdopodobieństwo wystąpienia pęknięcia dla konkretnego komponentu i może być przeprowadzona wg metodologii opisanej w standardzie API RP 581 Risk-based Inspection Methodology [1].



Rys. 6. Diagram oceny podatności dla mechanizmu degradacji- naprężeniowego pękania kaustycznego [1]

Element, w którym stwierdzono pęknięcia w wyniku badań diagnostycznych będzie cechował się wysoką podatnością, również w przypadku przeprowadzenia naprawy polegającej na usunięciu pęknięć (rys. 6). W sytuacji wymiany całego elementu zarówno identyfikację jak i ocenę podatności należy przeprowadzić ponownie uwzględniając cechy nowego elementu.

Inaczej przebiega ocena podatności elementów na konkretny mechanizm degradacji dla mechanizmów powodujących ubytek materiału. W takim przypadku, w celu ustalenia podatności wyznaczamy szybkość korozji, tj. przewidywany ubytek materiału w procesie korozji wyrażany współczynnikiem CR (corrosion rate) w [mm/rok].

Zależnie od jakości dostępnych danych, w tym danych pochodzących z pomiarów grubości elementów ocenianych, szybkość korozji może być wyznaczona na kilka sposobów.

OBLICZONA (CALCULATED) – zgodnie z załącznikiem 2.B standardu API RP 581 zawierającym konserwatywne modele obliczeń CR w zależności od zmiennych warunków procesu

ZMIERZONA (MEASURED) – bazuje na CR określonym na podstawie zapisów z prowadzonych skutecznych pomiarów grubości w określonych CMLs (Condition Monitoring Locations)

SZACOWANA (ESTIMATED*) – bazuje na CR wyznaczonym przez doświadczonego specjalistę ds. korozji CR określonym na podstawie dostępnych danych literaturowych lub danych pochodzących z innych urządzeń pracujących w podobnych warunkach

**** Miejsca monitorowania stanu technicznego CML [6, 7]***
Wyznaczone obszary na urządzeniach ciśnieniowych, w których przeprowadza się okresowe badania zewnętrzne w celu bezpośredniej oceny stanu technicznego. CML mogą zawierać jeden lub więcej punktów badania i wykorzystywać wiele technik inspekcyjnych zależnie od mechanizmów degradacji i przewidywanych typów uszkodzenia, aby zapewnić najwyższe prawdopodobieństwo wykrycia. CML mogą stanowić pojedynczy mały obszar na urządzeniu (np. punkt lub płaszczyzy 2 cali na obwodzie króćca, gdzie punkty rejestracji znajdują się we wszystkich czterech ćwiartkach płaszczyzny).

W przypadku szacowania szybkości korozji kluczowe jest również określenie poziomu ufności dla danych źródłowych, które wykorzystano do jej szacowania. Standard API RP 581 określa trzy kategorie ufności.

LOW CONFIDENCE - źródła informacji o niskim stopniu ufności dotyczące szybkości korozji — źródła takie jak opublikowane dane, tabele szybkość korozji i ekspertyzy

MEDIUM CONFIDENCE - źródła informacji o średniej ufności dotyczące szybkości korozji — testy laboratoryjne z symulowanymi warunkami procesu lub ograniczone testy próbek korozyjnych (in-situ)

Dane dotyczące szybkości korozji opracowane na podstawie źródeł, które symulują rzeczywiste warunki procesu, zwykle zapewniają wyższy poziom pewności co do przewidywanej szybkości korozji.

HIGH CONFIDENCE - źródła informacji o wysokim stopniu pewności o szybkości korozji — obszerne dane z wiarygodnych inspekcji.

Dane z kuponów korozyjnych, odzwierciedlające pięć lub więcej lat (przy założeniu, że nie nastąpiły znaczące zmiany procesu) zapewniają wysoki poziom ufności przewidywanej szybkości korozji. Jeśli dostępna jest wystarczająca ilość danych z rzeczywistego procesu technologicznego, rzeczywista szybkość korozji z dużym prawdopodobieństwem będzie zbliżona do wartości oczekiwanej w normalnych warunkach pracy.

Jakość wykorzystanych danych źródłowych przekłada się również na niepewność w oszacowaniu prawdopodobieństwa wystąpienia perforacji w wyniku oddziaływania danego mechanizmu degradacji.

ZARZĄDZANIE INTEGRALNOŚCIĄ MECHANICZNĄ

Właściwe, a przede wszystkim rzetelne podejście do identyfikacji mechanizmów degradacji oraz oceny podatności komponentów urządzeń na te mechanizmy jest fundamentem do zarządzania integralnością mechaniczną wyposażenia produkcyjnego, a tym samym zmniejszenia prawdopodobieństwa wystąpienia nieszczelności lub poważnej awarii przemysłowej. Wyznaczone w tym procesie szybkość korozji oraz podatność dla mechanizmów powodujących pęknięcia lub zmiany strukturalne materiałów konstrukcyjnych stanowią dane wejściowe do analiz niezawodności konstrukcji ciśnieniowych, w tym RBI. Pozwalają na dobór właściwych metod inspekcyjnych ukierunkowanych na poszukiwanie określonych w analizie mechanizmów degradacji typów uszkodzeń w zidentyfikowanych obszarach narażenia w urządzeniach.

Bezpośrednim wynikiem procesu identyfikacji mechanizmów degradacji jest określenie tzw. kluczowych czynników aktywności mechanizmów degradacji, których monitorowanie w toku eksploatacji urządzenia pozwala na identyfikację zmian i podejmowanie odpowiednich proaktywnych działań korygujących, o ile są możliwe.

W przypadku wspomnianego wcześniej mechanizmu naprężeniowego pękania kaustycznego takimi czynnikami będą: temperatura, stężenie NaOH, rodzaj materiału konstrukcyjnego oraz to, czy został on poddany obróbce cieplnej. Będzie to również informacja o ogrzewaniu elementu lub jego przeparowywaniu w procesie przygotowania do napowietrzenia. Każdy z tych czynników może niezależnie wpłynąć na aktywację mechanizmu lub zmianę podatności elementu, np. poprzez dodanie ogrzewania w procesie modernizacji lub zmianę temperatur roboczych.

Jak widać istnieje szereg korzyści płynących z wnikliwej analizy mechanizmów degradacji nie tylko w przypadku prowadzenia tego procesu na potrzeby procesu RBI, ale również dla każdego urządzenia, którego trwałość zależy od warunków jego eksploatacji.

Literatura:

1. API RP 581 Risk-Based Inspection Methodology, THIRD EDITION, APRIL 2016, ADDENDUM 2, OCTOBER 2020
2. WUDT-RBI-2022 Planowanie inspekcji urządzeń ciśnieniowych w oparciu o analizę ryzyka RBI
3. https://www.udt.gov.pl/ekspertyzy-techniczne/analiza-zagrozen-i-oceny-ryzyka
4. API RP 571 Damage Mechanisms Affecting Fixed Equipment in the Refining Industry ANSI/API RECOMMENDED PRACTICE 571 THIRD EDITION, MARCH 2020
5. NACE SP0403-2015 Avoiding Caustic Stress Corrosion Cracking of Refinery Equipment and Piping, NACE International 1440 South Creek Drive Houston, Texas 77084-4906 ISBN:1-57590-179-X
6. API 510 Pressure Vessel Inspection Code: In-service Inspection, Rating, Repair, and Alteration 10th ed., May 2014
7. API 570 Piping Inspection Code: In-service Inspection, Rating, Repair, and Alteration of Piping Systems, 4th ed., February 2016

KONSULTACJA MERYTORYCZNA:

DR INŻ. MACIEJ SZWED

Kierownik Wydziału Badań Materiałowych i Ekspertyz
Centralne Laboratorium Dozoru Technicznego

DR INŻ. KRZYSZTOF SZYMLEK

Ekspert Urządzeń Ciśnieniowych
Oddział w Gdańsku
Urząd Dozoru Technicznego

Ocena wpływu uszkodzeń na bezpieczeństwo eksploatacji urządzeń ciśnieniowych. Wstęp do metodologii Fitness For Service

MGR INŻ. MATEUSZ WRÓBEL

Specjalista ds. Rozwoju Badań Laboratoryjnych
Wydział Badań Materiałowych i Ekspertyz
Centralne Laboratorium Dozoru Technicznego

MGR INŻ. TOMASZ KLINKOSZ

Ekspert Urządzeń Ciśnieniowych
Dział Oceny Zgodności
Oddział w Gdańsku
Urząd Dozoru Technicznego

DR INŻ. MARIUSZ ŁUCKI

Główny Specjalista ds. Rozwoju Badań Laboratoryjnych
Wydział Badań Materiałowych i Ekspertyz
Centralne Laboratorium Dozoru Technicznego

URZĄDZENIA TECHNICZNE PODCZAS EKSPLOATACJI NARAŻONE SĄ NA DZIAŁANIE RÓŻNORODNYCH PROCESÓW, KTÓRE POWODUJĄ POGORSZENIE ICH STANU TECHNICZNEGO, PROWADZĄC DO POWSTAWANIA WIELU TYPÓW USZKODZEŃ. USZKODZENIA WYSTĘPUJĄCE W URZĄDZENIACH STANOWIĄ WYZWANIE DLA INSPEKTORÓW URZĘDU DOZORU TECHNICZNEGO PODCZAS WYKONYWANIA CZYNNOŚCI DOZOROWYCH. CZĘSTO W TAKICH SYTUACJACH PODJĘCIE DECYZJI O DOPUSZCZENIU URZĄDZENIA DO DALSZEJ EKSPLOATACJI I CZASIE JEGO BEZPIECZNEJ PRACY JEST UTRUDNIONE. WŁAŚCIWA OCENA STANU TECHNICZNEGO WYMAGA DUŻEGO DOŚWIADCZENIA I INTERDYSCYPLINARNEJ WIEDZY Z ZAKRESU: INŻYNIERII MATERIAŁOWEJ, BADAŃ MATERIAŁOWYCH, INŻYNIERII PROCESU CZY BUDOWY KONSTRUKCJI. SPOSÓB PODEJŚCIA DO TEGO TYPU ZAGADNIEŃ ZOSTAŁ OPISANY W DOKUMENCIE API 579-1/ASME FFS-1 FITNESS FOR SERVICE.

„Wspieramy rozwój. Dbamy o bezpieczeństwo" to misja Urzędu Dozoru Technicznego. Realizując to założenie, UDT analizuje rozwiązania, które mogą się przyczynić do zwiększenia bezpieczeństwa publicznego. Jednym z nich jest ocena urządzeń z wykrytymi uszkodzeniami zgodnie z metodologią Fitness For Service.

Normy dotyczące urządzeń ciśnieniowych zawierają wymagania w odniesieniu do etapu wytwarzania. W trakcie eksploatacji urządzeń z uszkodzeniami analiza stanu technicznego obiektu nie jest już tak oczywista. Niektóre ze standardów technicznych, np. API 653 i NBBI NB-23, opisują jedynie metodę wykonania naprawy lub zmianę parametrów procesowych. Dokumenty te nie dają natomiast odpowiedzi na temat akceptowalności danego uszkodzenia oraz pozostałej trwałości eksploatacyjnej. Ocena stanu technicznego urządzenia z uszkodzeniem stanowi wciąż duże wyzwanie.

Uszkodzenia urządzeń ciśnieniowych wynikają w dużej mierze z oddziaływania aktywnych mechanizmów degradacji, których efektem są:

- pocienienia (ogólne, miejscowe oraz pitting)
- pęknięcia powierzchniowe
- pęknięcia podpowierzchniowe
- mikropęknięcia i mikropory
- zmiany struktury materiału
- zmiany wymiarowe
- pęcherze
- zmiany własności materiałowych

W realizowanych przy udziale UDT analizach RBI (Risk Based Inspection), o których pisaliśmy już na łamach biuletynu Inspektor, dokonuje się identyfikacji i oceny aktywności mechanizmów degradacji, uwzględniając m.in.: parametry procesowe, skład strumienia procesowego oraz materiały i sposób wytworzenia konstrukcji. Jednym z wyników tych analiz jest określenie wymienionych powyżej typów uszkodzeń.

Dostępne publikacje naukowe, które opisują tego typu zagadnienia, są często pozbawione waloru inżynierskiego – praktycznego podejścia, co znacząco ogranicza możliwość ich wykorzystania w praktyce inspekcyjnej. Ocena zidentyfikowanych podczas badań uszkodzeń oraz ustalenie bezpiecznego okresu i warunków dalszej eksploatacji stanowi zatem wyzwanie.

W takich przypadkach rozwiązaniem może być wykorzystanie standardu technicznego – opracowanego wspólnie przez Amerykański Instytut Naftowy (American Petroleum Institute – API) i Amerykańskie Stowarzyszenie Inżynierów Mechaników (American Society of Mechanical Engineers – AMSE) – API 579-1/ASME FFS-1 Fitness For Service. Dokument ten jest zbiorem procedur pozwalających na ocenę urządzeń ciśnieniowych z wykrytymi uszkodzeniami oraz szacowanie ich pozostałej trwałości eksploatacyjnej. API 579-1/ASME FFS-1 Fitness For Service zawiera ponadto szereg przydatnych wskazówek związanych z wykonywaniem badań NDT (Non Destructive Testing), zapobieganiem ponownemu uszkodzeniu czy też dotyczących sposobu monitorowania urządzeń w trakcie dalszej eksploatacji.

Metodologia Fitness For Service została opracowana z myślą o urządzeniach instalowanych w przemyśle rafineryjnym i petrochemicznym, ale znajduje swoje zastosowanie również w odniesieniu do urządzeń w innych sektorach. Metoda, którą określa standard API RP 580 Risk-Based Inspection, stosowana jest również jako jedno z narzędzi do zarządzania ryzykiem. W sytuacji gdy wykonanie odpowiednio efektywnej inspekcji, a tym samym zmniejszenie niepewności co do aktualnego stanu technicznego urządzenia nie pozwala na redukcję ryzyka z uwagi na stwierdzone uszkodzenia, inżynierska ocena konstrukcji Fitness For Service może być skutecznym narzędziem. Warunkiem jest jednak potwierdzenie, że kryteria tej oceny zostaną spełnione.

BUDOWA STANDARDU

API 579-1/ASME FFS-1 Fitness For Service został podzielony na 14 części.

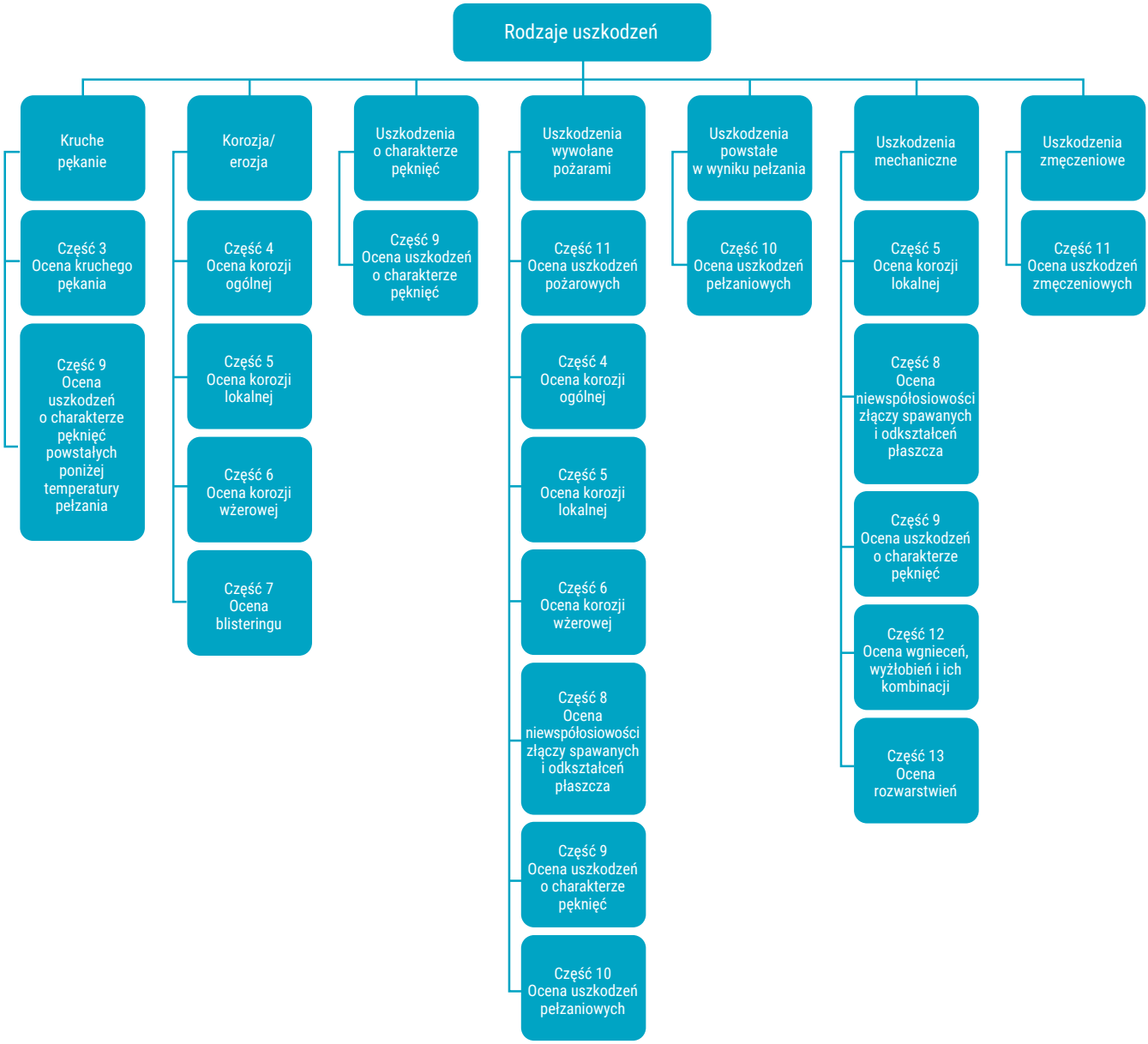
W części 1 podano dokładną definicję metodologii Fitness For Service. Wymieniono w niej także najważniejsze obszary zastosowania omawianego standardu.

Część 2 stanowi wprowadzenie do procedur oceny Fitness For Service. Opisane zostały w niej poszczególne poziomy oceny, a także podstawowe założenia związane z kryteriami oceny. W zależności od rodzaju uszkodzenia ocenę przeprowadza się zgodnie z kryteriami bazującymi na:

- naprężeniach dopuszczalnych,
- współczynniku wytrzymałości resztkowej (Remaining Stress Factor – RSF),
- diagramach oceny uszkodzeń (Failure Assessment Diagram – FAD).

W załącznikach 2A–2F API 579-1/ASME FFS-1 można znaleźć szczegółowe informacje dotyczące m.in. obliczeń wytrzymałościowych i wymaganych właściwości materiałowych.

Części 3–14 zawierają procedury oceny stanu elementu z konkretnymi rodzajami uszkodzeń. Zestawienie typów uszkodzeń ujętych w metodologii Fitness For Service przedstawiono na rysunku 1.



Rys. 1. Rodzaje uszkodzeń ocenianych według metodologii Fitness For Service [1]

Każda z części 3–14 charakteryzuje się usystematyzowaną i jednolitą budową. Wyróżnić można w nich rozdziały opisujące kolejno:
● identyfikację uszkodzenia wywołanego danym mechanizmem degradacji,
● stosowalność i ograniczenia dla poszczególnych procedur oceny,
● dane, które są wymagane do przeprowadzenia oceny,
● techniki oceny i kryteria akceptacji,
● sposób oceny pozostałej trwałości eksploatacyjnej,
● środki zaradcze przed powstaniem danego uszkodzenia,
● zalecenia dotyczące sposobu monitorowania urządzenia,
● wymagania dotyczące dokumentowania procesu oceny.

Poszczególne procedury oceny są ze sobą ściśle powiązane. Nieznajomość jednej z części może skutkować brakiem możliwości przeprowadzenia oceny dla innego typu uszkodzenia.

ZESPÓŁ WYKONUJĄCY OCENĘ FITNESS FOR SERVICE

Wykonanie oceny Fitness For Service wymaga stworzenia interdyscyplinarnego zespołu osób, które powinny posiadać kompetencje z zakresu m.in. inżynierii materiałowej, metalurgii, korozji, budowy urządzeń ciśnieniowych, wytrzymałości konstrukcji, mechaniki pękania, badań nieniszczących czy inżynierii procesowej.

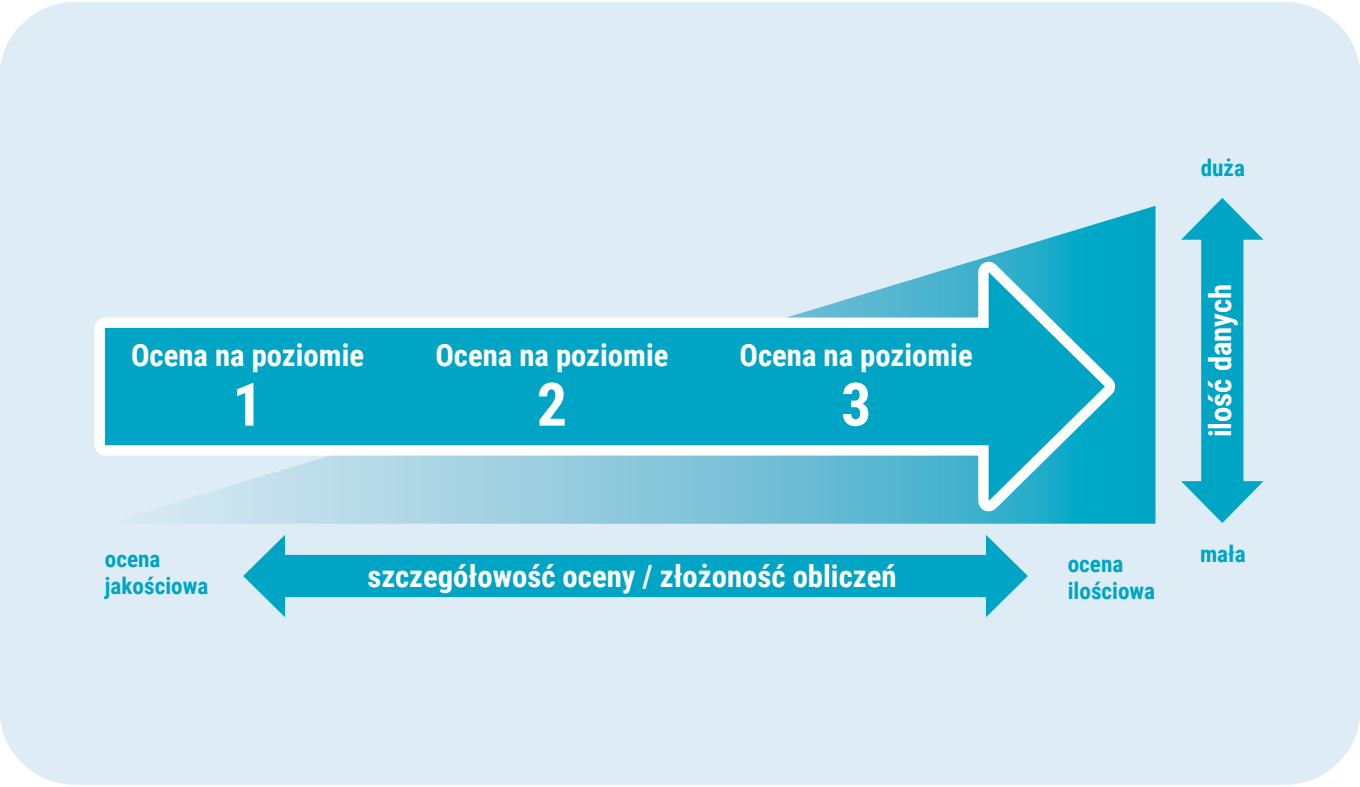
Przeprowadzenie rzetelnej oceny zależy od ścisłej współpracy pomiędzy inspektorami UDT i służbami odpowiedzialnymi za eksploatację analizowanego urządzenia. Fitness For Service wykorzystuje wyniki przeprowadzonych inspekcji, które wraz z danymi konstrukcyjnymi analizowanego urządzenia stanowią podstawę do przeprowadzenia oceny. Wiarygodność i dokładność przeprowadzonych badań, np. pomiarów grubości ścianki analizowanego elementu urządzenia, są kluczowe dla poprawności uzyskanych wyników. Istotną rolę odgrywa zatem komunikacja pomiędzy zespołem prowadzącym ocenę Fitness For Service a personelem wykonującym badania NDT, który powinien otrzymać informację o celu przeprowadzenia badań oraz o oczekiwanym typie uszkodzeń. Ważny aspekt stanowi również dobór odpowiednich metod badawczych, tak aby możliwe było precyzyjne zwymiarowanie uszkodzenia i dokładne określenie jego lokalizacji w danej konstrukcji. Rekomendowane jest również ustalenie oczekiwań związanych z wynikami badań przed ich przeprowadzeniem, np. dobór odpowiedniej siatki pomiarowej podczas pomiarów grubości.

Do przeprowadzenia ocen Fitness For Service mogą być wykorzystane wyniki badań NDT otrzymane w ramach tzw. programów utrzymania ruchu lub w ramach analiz RBI. Ich przydatność do analiz musi być jednak każdorazowo zweryfikowana przez zespół wykonujący ocenę Fitness For Service[2].

POZIOMY OCENY FITNESS FOR SERVICE

Metodologia Fitness For Service przewiduje przeprowadzenie oceny stanu urządzenia na trzech poziomach:
● Procedury oceny dają najbardziej zachowawcze wyniki. Stosowane algorytmy obliczeniowe pozwalają na stosunkowo szybką ocenę przy dostarczeniu jedynie podstawowych informacji o danym urządzeniu.
● Ocena związana jest z bardziej szczegółową analizą. Wymagane jest dostarczenie większej ilości danych, a poszczególne obliczenia i zależności algebraiczne są bardziej skomplikowane. Otrzymane wyniki cechuje jednak większa precyzja od tych, które uzyskano podczas oceny na poziomie 1.
● Do przeprowadzenia oceny wymagane jest zazwyczaj wykonanie inspekcji w bardzo szerokim zakresie i pozyskanie dogłębnych informacji dotyczących urządzenia. Analiza zwykle opiera się na metodach numerycznych, np. metodzie elementów skończonych.

Wzajemne relacje pomiędzy poziomami oceny przedstawiono na rysunku 2.



Rys. 2. Zależność pomiędzy poziomami oceny Fitness For Service

Omawiając metodologię Fitness For Service, warto podkreślić, że niespełnienie wymagań oceny np. na poziomie 1 nie oznacza, że urządzenie powinno zostać wyłączone z eksploatacji. Możliwe jest wykonanie dodatkowej analizy na wyższym poziomie oceny (2 lub 3), której wynik może okazać się pozytywny. W przypadku otrzymania negatywnych rezultatów podczas oceny na każdym z poziomów należy rozważyć wyłączenie urządzenia z eksploatacji, przeprowadzenie naprawy lub zmianę dotychczasowych warunków pracy.

STOSOWALNOŚĆ I OGRANICZENIA

Bardzo ważnym aspektem przy wykorzystaniu metodologii Fitness For Service jest znajomość zakresu stosowalności i ograniczeń poszczególnych procedur oceny. Przykładem są tu wymagania dla różnych typów obiektów. W zależności od ocenianego elementu (rodzaju urządzenia, jego geometrii, warunków pracy) możliwe jest przeprowadzenie oceny na danym poziomie. Zestawienie opisujące możliwe do zastosowania poziomy oceny dla konkretnego typu obiektów przedstawiono na rysunku 3.

TYPY OBIEKTÓW			
OBIEKTY TYPU Ax Ocena na poziomie 1, 2 lub 3	**OBIEKTY TYPU B Ocena na poziomie 2 lub 3**		**OBIEKTY TYPU C Ocena na poziomie 3**
	KLASY 1	**KLASY 2**	
Cylindryczne zbiorniki ciśnieniowe i elementy stożkowe, kuliste zbiorniki ciśnieniowe i kuliste zbiorniki magazynowe, dennice, proste odcinki rurociągów, łuki i kolana	Obiekty o takich samych cechach geometrycznych i temperaturowych jak obiekty typu A, dla których obciążenia dodatkowe rzutują na wymaganą grubość ścianki	Króćce zbiorników ciśnieniowych, obszar wzmocnień elementów stożkowych, kołnierze, połączenia płaszcza z płaskim dnem, połączenia wkładów rurowych	Połączenia dennic z płaszczem, pierścienie wzmacniające, podpory i spódnice, połączenia płaszcza z dnem zbiorników magazynowych

Rys. 3. Typy obiektów i stosowane dla nich poziomy oceny

Jako kolejny przykład ograniczeń poszczególnych procedur oceny mogą posłużyć wymagania związane z oceną uszkodzeń korozyjnych. Zgodnie z założeniami przyjętymi w API 579-1/ASME FFS-1 Fitness For Service korozję ogólną, korozję lokalną i korozję wżerową ocenia się zasadniczo w przypadku urządzeń pracujących poniżej temperatury pełzania. W przypadku pocienień występujących w urządzeniach pracujących w warunkach pełzania powinny zostać użyte także inne procedury oceny.

DOKUMENTOWANIE WYKRYTYCH USZKODZEŃ

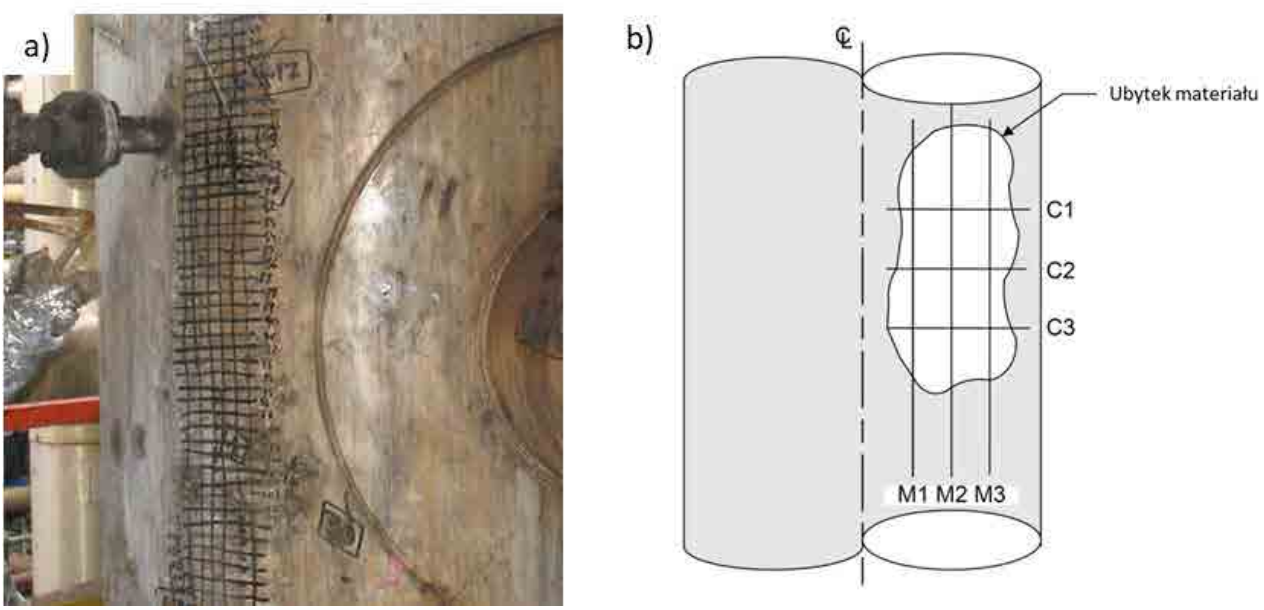
Dokumentowanie wykrytych uszkodzeń to kolejny istotny element metodologii Fitness For Service. Sposób opisu uszkodzeń oraz wiarygodność pozyskanych danych pomiarowych rzutuje w kolejnym etapie na poprawność wykonanej oceny.

Metodologia Fitness For Service wymaga dostępu do szeregu danych dotyczących ocenianego urządzenia, tj.:
● dokumentacja projektowa i obliczenia wytrzymałościowe
● raporty z badań przeprowadzonych na etapie wytwarzania
● dokumenty kontroli
● informacje na temat warunków pracy urządzenia i stosowanych urządzeń zabezpieczających
● wyniki prób ciśnieniowych
● informacje na temat dotychczasowej historii eksploatacji
● informacje na temat zmian dotyczących ciśnienia i temperatury prowadzonego procesu, medium roboczego, szybkości korozji itp.
● wyniki okresowych badań NDT
● informacje na temat przeprowadzonych napraw, modernizacji

Bez dostępu do powyższych danych praktycznie niemożliwe jest wykonanie oceny urządzenia zgodnie z metodologią Fitness For Service.

Cały proces związany z oceną uszkodzeń jest bardzo złożony, a jednocześnie szczegółowo opisany. Potwierdzeniem tego stanu rzeczy może być przykład dotyczący korozji lokalnej. W „tradycyjnym" podejściu do tego typu uszkodzenia pocienienie jest charakteryzowane przez pomiar grubości ścianki wykonany w miejscach, których lokalizacja określona jest często na podstawie wewnętrznych standardów organizacji.

Stosując procedury oceny zawarte w API 579-1/ASME FFS-1 Fitness For Service, pomiar grubości przeprowadza się według określonych wytycznych co do sposobu konstruowania siatek pomiarowych oraz krytycznych profili grubości. Przykład stosowanych siatek pomiarowych przedstawiono na rysunku 4.



Rys. 4. Przykład siatki pomiarowej dla części cylindrycznej zbiornika a) Przykładowa siatka pomiarów grubości w celu określenia wymiarów ubytku korozyjnego b) Szkic siatki pomiarowej dla części cylindrycznej wg API 579-1/ASME FFS-1 Fitness For Service[3]

Warto podkreślić, że minimalna zmierzona grubość nie jest wystarczającym kryterium oceny. Istotny jest również m.in. obszar występowania danego pocienienia (wymiar wzdłużny i obwodowy) oraz odległość od najbliższej nieciągłości konstrukcyjnej. W API 579-1/ASME FFS-1 Fitness For Service sprecyzowano wymagania dotyczące grupowania sąsiadujących ze sobą ubytków korozyjnych oraz podano zalecenia dotyczące przeprowadzania dodatkowych badań NDT (np. badania złączy spawanych znajdujących się „w pobliżu" wykrytego pocienienia).

Na podstawie zgromadzonych danych zespół przeprowadzający ocenę Fitness For Service ma możliwość określenia przydatności danego urządzenia do dalszej pracy i oszacowania pozostałej trwałości eksploatacyjnej.

METODOLOGIA FITNESS FOR SERVICE W UDT

Urząd Dozoru Technicznego już od 2011 r., kiedy to przystąpił do pilotażowego programu wdrożenia metodologii Risk-Based Inspection dla urządzeń ciśnieniowych pracujących w instalacji rafineryjnej, poszerza swoje doświadczenie w predykcji zużycia urządzeń ciśnieniowych. Obecnie tysiące zbiorników ciśnieniowych i rurociągów technologicznych w polskim przemyśle petrochemicznym zostały poddane analizom RBI, które mają na celu predykcję ich zużycia i opracowanie niezbędnych planów inspekcji prowadzących do utrzymania odpowiedniego poziomu ryzyka związanego z ich eksploatacją.

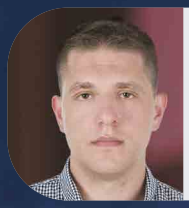
Zdobyta do tej pory wiedza pozwoliła na dokładniejsze dokumentowanie uszkodzeń urządzeń ciśnieniowych, wykrytych w trakcie przeprowadzonej inspekcji. Zgromadzone dane posłużą do wykonania ocen stanu technicznego urządzeń zgodnie z metodologią Fitness For Service. W kolejnym numerze biuletynu Urzędu Dozoru Technicznego „Inspektor. Technika i bezpieczeństwo" przedstawimy przykładową analizę zgodnie z metodologią Fitness For Service.

Działania związane z wdrożeniem metodologii Fitness For Service wpisują się w realizację strategii UDT na lata 2021–2025, w szczególności w 1 Cel strategiczny: Zarządzanie bezpieczeństwem publicznym i przemysłowym – Zadanie 3: Innowacyjne podejście do bezpieczeństwa publicznego.

Literatura:

[1] API 579-1/ASME FFS-1 Fitness For Service; Figure 2.1 – FFS Assessment Procedures for Various Damage Classes
[2] API 579-1/ASME FFS-1 Fitness For Service; Figure 4.8 – Inspection Planes for Cylindrical Shells, Conical Shells, and Pipe Bends

FITNESS FOR SERVICE - OCENA REAKTORA PRACUJĄCEGO W WARUNKACH PEŁZANIA



MGR INŻ. MATEUSZ WRÓBEL

Specjalista ds. Rozwoju Badań Laboratoryjnych
Wydział Badań Materiałowych i Ekspertyz
Centralne Laboratorium Dozoru Technicznego

MGR INŻ. TOMASZ KLINKOSZ

Ekspert Urządzeń Ciśnieniowych
Dział Oceny Zgodności
Oddział w Gdańsku
Urząd Dozoru Technicznego

DR INŻ. MARIUSZ ŁUCKI

Główny Specjalista ds. Rozwoju Badań Laboratoryjnych
Wydział Badań Materiałowych i Ekspertyz
Centralne Laboratorium Dozoru Technicznego

PEŁZANIE JEST MECHANIZMEM DEGRADACJI, NA WYSTĄPIENIE KTÓREGO NARAŻONE SĄ MATERIAŁY DŁUGOTRWALE EKSPLOATOWANE POWYŻEJ TZW. TEMPERATURY GRANICZNEJ. W WYNIKU LICZONEJ W SETKI TYSIĘCY GODZIN PRACY W PODWYŻSZONEJ TEMPERATURZE I PRZY JEDNOCZESNYM DZIAŁANIU NAPRĘŻEŃ DOCHODZI DO POWSTANIA TRWAŁYCH ODKSZTAŁCEŃ MATERIAŁU. TOWARZYSZĄ IM CZĘSTO ZMIANY W BUDOWIE MIKROSTRUKTURY. OCENA MATERIAŁÓW PRACUJĄCYCH W WARUNKACH PEŁZANIA OBEJMUJE ZAZWYCZAJ WYKONANIE SZEREGU BADAŃ DIAGNOSTYCZNYCH, TJ.: BADANIA STRUKTURY, BADANIA NDT, POMIARÓW GEOMETRII DANEGO KOMPONENTU W CELU WYKRYCIA ODKSZTAŁCEŃ PLASTYCZNYCH. TRUDNOŚCI POWODUJE OSZACOWANIE POZOSTAŁEJ TRWAŁOŚCI EKSPLOATACYJNEJ DANEGO URZĄDZENIA. SPOSÓB PODEJŚCIA DO TEGO TYPU PROBLEMÓW ZOSTAŁ OPISANY W DOKUMENCIE API 579-1/ASME FFS-1 FITNESS FOR SERVICE.

Na wstępie warto przypomnieć, że dokument API 579-1/ASME FFS-1 Fitness For Service jest zbiorem procedur pozwalających na ocenę urządzeń ciśnieniowych z wykrytymi uszkodzeniami oraz szacowanie ich pozostałej trwałości eksploatacyjnej.

W rozdziale 10 (Part 10 – *Assessment of components operating in the creep range*) zawarto wytyczne dotyczące oceny trwałości eksploatacyjnej urządzeń pracujących w warunkach pełzania.

OPIS PRZEDMIOTU ANALIZY

Analizie został poddany reaktor pracujący w instalacji wytwórni i odzysku wodoru. Aparat ten służy do konwersji cięższych węglowodorów do metanu. Medium roboczym jest gaz procesowy. Poglądowy szkic urządzenia przedstawiono na rysunku 1.

Reaktor został oddany do użytku w 1999 r. Projektowany czas eksploatacji wynosił 100 000 h i został przekroczony. Wobec tego faktu urządzenie poddano ocenie trwałości eksploatacyjnej zgodnie z metodologią Fitness For Service. Podjęto próbę przeprowadzenia oceny na poziomie 2.

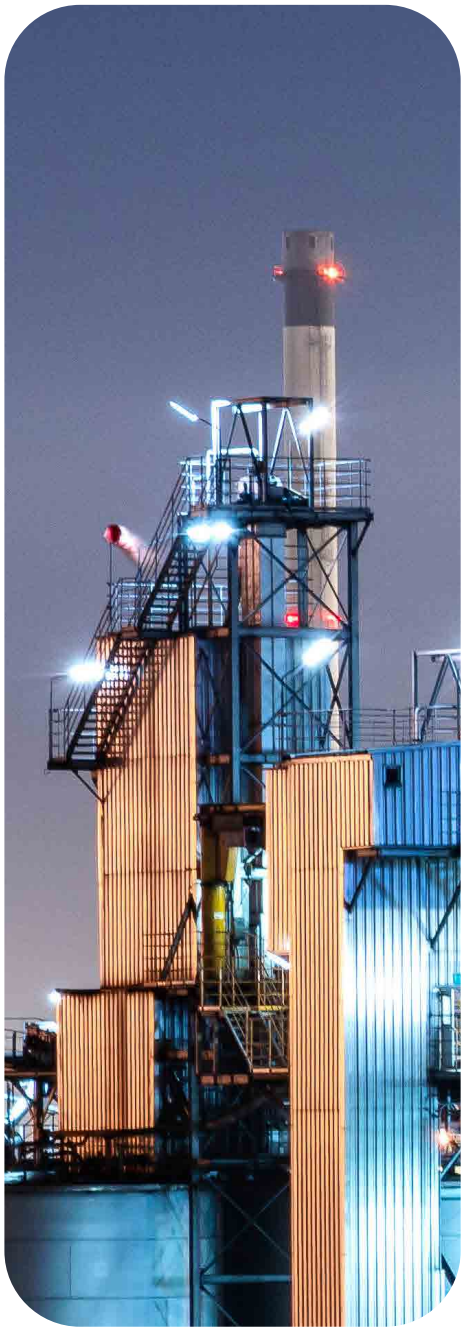
DANE DOTYCZĄCE REAKTORA

Ocenie Fitness For Service należy poddawać poszczególne komponenty danego aparatu. W przypadku analizowanego reaktora można wyróżnić m.in. płaszcz, dna elipsoidalne i króćce. Na potrzeby niniejszego artykułu prezentowana metodologia będzie ograniczona wyłącznie do oceny płaszcza.

Materiał, który wykorzystano do budowy urządzenia, to ASTM A387 Grade F22 Class 1. Należy on do grupy stali chromowo-molibdenowych typu 2.25Cr-1Mo. Temperatura graniczna dla tej grupy materiałów wynosi 427°C (wg *Table 4.1 – Temperature Limit Used To Define The Creep Range, API 579-1/ASME FFS-1 Fitness For Service*). Temperatura robocza aparatu przekracza tę wartość, co potwierdza eksploatację w warunkach pełzania. Dane dotyczące płaszcza reaktora zestawiono w tablicy 1.

Tablica 1. Dane dotyczące płaszcza reaktora

Płaszcz	
Materiał	ASTM A387 Grade F22 Class 1
Ciśnienie obliczeniowe płaszcza, P	3,8 MPa
Ciśnienie robocze	3,18/3,05 MPa
Temperatura obliczeniowa, T	540°C
Temperatura robocza	455/488°C
Naddatek na korozję, *FCA*	3/0,75 mm
Średnica zewnętrzna, D_0	1290 mm
Grubość nominalna, t_{nom}	50 mm
Naprężenia dopuszczalne, S_a	53,89 MPa
Współczynnik wytrzymałościowy złącza spawanego, E	1



STOSOWALNOŚĆ I OGRANICZENIA PROCEDUR OCENY

Bardzo ważnym aspektem przy wykorzystaniu metodologii Fitness For Service jest znajomość zakresu stosowalności i ograniczeń poszczególnych procedur oceny.

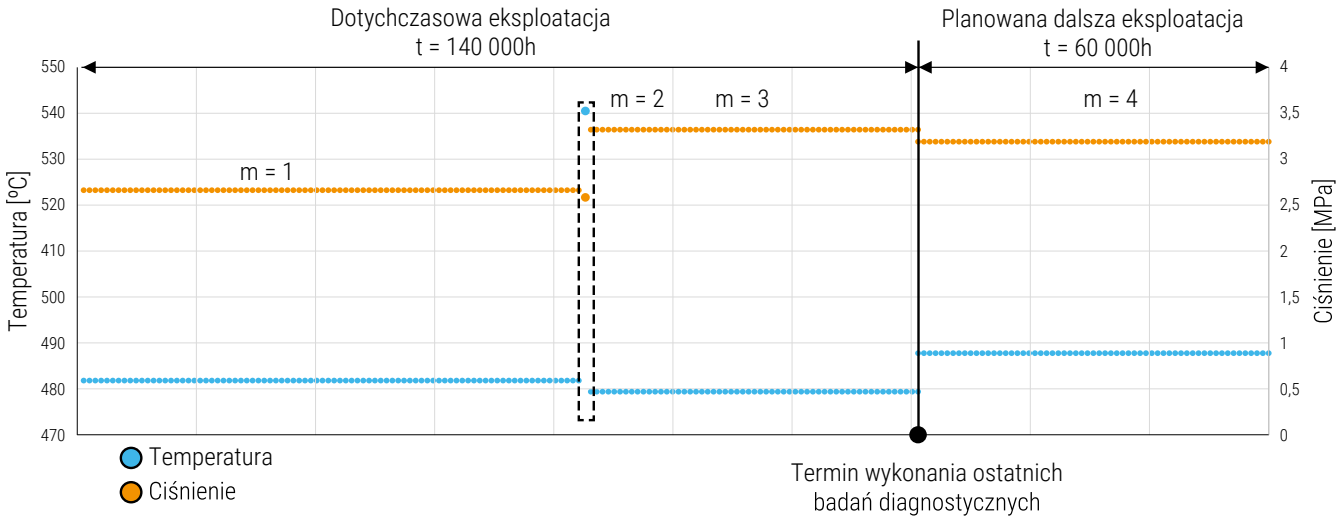
W przypadku analizy pod kątem pełzania komponenty poddawane ocenie na poziomie 1. i 2. nie mogą zawierać dodatkowych uszkodzeń (przykłady).
Ubytki grubości materiału – pocienienia korozyjne i wżery
Pęcherze wodorowe (blistering), pęknięcia typu HIC lub SOHIC wynikające z oddziaływania siarkowodoru
Niewspółosiowość złączy spawanych, owalizacja, wybrzuszenia przekraczające przyjęte zakresy tolerancji
Wgniecenia i inne uszkodzenia mechaniczne
Pęknięcia
Zmiany mikrostrukturalne, np. grafityzacja, wydzielenia fazy sigma, nawęglenie, atak wodorowy

Niespełnienie zarówno tych, jak i innych warunków sprawia, że konieczne staje się przeprowadzenie oceny na poziomie 3, która jest znacznie bardziej skomplikowana i wymaga m.in. stosowania technik numerycznych do określenia stanu naprężeń.

HISTORIA EKSPLOATACJI

Podczas oceny Fitness For Service konieczna jest analiza historii pracy danego urządzenia. Na podstawie danych zebranych w toku eksploatacji ustalono, że parametry robocze reaktora podlegały wahaniom. Zmiany te są istotne i mogą mieć wpływ na wynik oceny, dlatego konieczne staje się określenie tzw. cykli operacyjnych.

W prezentowanym przykładzie wyróżniono 4 cykle operacyjne, przy czym cykl m = 4 dotyczy przyszłych planowanych warunków eksplotacji. Dla każdego z cykli operacyjnych konieczne jest obliczenie trwałości podczas pracy w warunkach pełzania, ułamków uszkodzenia i ich następne porównanie z wartością kryterialną. Cykle operacyjne przyjęte do analizy przedstawiono na rysunku 2. Warunki pracy i czasy trwania każdego z cykli zestawiono w tablicy 2.



Rys. 2. Cykle operacyjne przyjęte do analizy

Tablica 2. Warunki pracy każdego z cykli eksploatacyjnych

Parametry	Cykle operacyjne			
	m=1	m=2	m=3	m=4
Temperatura [°C]	482	540	480	488
Temperatura [°F]	*900*	*1004*	*896*	*910*
Ciśnienie [MPa]	2,66	2,6	3,3	3,18
Ciśnienie [ksi]	*0,39*	*0,47*	*0,38*	*0,46*
Czas eksploatacji [h]	84 000	1000	55 000	60 000
	∑140 000			

WYNIKI BADAŃ DIAGNOSTYCZNYCH

W trakcie ostatniego postoju remontowego reaktor został poddany badaniom diagnostycznym. Badania wizualne dały wynik pozytywny. Podczas badań magnetyczno-proszkowych i ultradźwiękowych wykonanych na wybranych złączach spawanych nie wykazano obecności wskazań nieakceptowalnych. Wyniki pomiarów grubości nie wskazują na występowanie pocienień. Średnia zmierzona grubość płaszcza wynosi 52,7 mm. Badania materiału metodą replik potwierdzają występowanie struktury ferrytyczno-perlitycznej. Nie stwierdzono obecności pustek pełzaniowych. Na podstawie analizy wykresu Nelsona [1] stwierdzono, że reaktor nie jest narażony na wystąpienie wysokotemperaturowego ataku wodorowego (HTHA). Z przeprowadzonej analizy mechanizmów degradacji wynika również, że urządzenie nie pracuje w tzw. *serwisie kwaśnym* (wet H_2S), czyli w warunkach, dla których istnieje zagrożenie wystąpienia uszkodzeń, tj.: blistering, HIC, SOHIC i SSC.

Nie stwierdzono tym samym obecności ograniczeń uniemożliwiających przeprowadzenie oceny na poziomie 2.

OCENA TRWAŁOŚCI PODCZAS PRACY W WARUNKACH PEŁZANIA

W dokumencie API 579-1/ASME FFS-1 Fitness For Service opisano kilka modeli oceny trwałości podczas pracy w warunkach pełzania. Wykorzystują one m.in. dane pochodzące z Materials Properties Council (MPC) Project Omega i równania Larsona-Millera. W obu przypadkach dla danych warunków eksploatacji (temperatury, naprężenia, czasu pracy) wyznacza się trwałość i odpowiednie ułamki uszkodzeń. W prezentowanym artykule przybliżone zostanie rozwiązanie bazujące na równaniach Larsona-Millera.

Obliczenia rozpoczyna się od wyznaczenia składowych naprężeń głównych. W analizowanym przypadku rozpatrywany jest komponent o stosunkowo prostej geometrii, dlatego możliwe jest zastosowanie poniższych równań. W przeciwnym wypadku konieczne może okazać się przeprowadzenie analiz numerycznych.

Obliczenia trwałości dla cyklu operacyjnego m = 1 przedstawiono poniżej.

$$(1)\quad \sigma_1 = \frac{PD_{mean}}{2t_{comp}} \cdot L_f = \frac{P \cdot \frac{D_0 + (D_0 - 2t_{rd})}{2}}{2t_{rd}} \cdot L_f = \frac{2{,}66 \cdot \frac{1290 + (1290 - 2 \cdot 52{,}7)}{2}}{2 \cdot 52{,}7} \cdot 1 = 31{,}23 MPa$$

$$(2)\quad \sigma_2 = \frac{PD_{mean}}{4(t_{comp} - t_{sl})} \cdot L_f = \frac{P \cdot \frac{D_0 + (D_0 - 2t_{rd})}{2}}{4(t_{rd} - t_{sl})} \cdot L_f = \frac{2{,}66 \cdot \frac{1290 + (1290 - 2 \cdot 52{,}7)}{2}}{4 \cdot (52{,}7 - 0)} \cdot 1 = 15{,}61 MPa$$

$$(3)\quad \sigma_3 = 0$$

Następnie określana jest wartość naprężeń zredukowanych.

$$(4)\quad \sigma_e = \frac{1}{\sqrt{2}}[(\sigma_1 - \sigma_2)^2 + (\sigma_1 - \sigma_3)^2 + (\sigma_2 - \sigma_3)^2]^{0,5} = \frac{1}{\sqrt{2}}[(31{,}23 - 15{,}61)^2 + (31{,}23 - 0)^2 + (15{,}61 - 0)^2]^{0,5}$$

$$\sigma_e = 27{,}04 MPa$$

Realizując procedurę oceny opisaną w API 579-1/ASME FFS-1 Fitness For Service, należy koniecznie zweryfikować dodatkowe kryteria związane m.in. z granicą plastyczności materiału w temperaturze pracy czy też działaniem naprężeń zewnętrznych (np. obciążenia wiatrem). W omawianym przykładzie wszystkie dodatkowe warunki zostały spełnione. Stosowne obliczenia, z uwagi na ich złożoność, nie zostały przedstawione w niniejszym artykule.

Równania Larsona-Millera służą do wyznaczania trwałości podczas pracy w warunkach pełzania. W celu przeprowadzenia obliczeń konieczna jest konwersja jednostek na naprężenia wyrażonych w [ksi] i temperaturę wyrażoną w [°F]. W obliczeniach wykorzystuje się tzw. parametry Larsona-Millera, które zależą od rodzaju materiału. Zestawienie parametrów Larsona-Millera dla stali z grupy 2.25Cr-1Mo zawarto w tablicy 3.	σ_1 = 31,23 MPa → 4,53 ksi
	σ_2 = 15,61 MPa → 2,26 ksi
	σ_3 = 0
	σ_e = 27,04 MPa → 3,92 ksi
	482°C → 900°F

Tablica 3. Parametry Larsona-Millera dla stali 2.25Cr-1Mo

Materiał	Parametry	Minimalny parameter Larsona-Millera – LMP_m
2.25Cr-1Mo	A_0	$4{,}3981719 \cdot 10^{1}$
	A_1	$-8{,}4656117 \cdot 10^{-1}$
	A_2	$-4{,}0483005 \cdot 10^{1}$
	A_3	$2{,}6236081 \cdot 10^{-1}$
	A_4	$1{,}5373650 \cdot 10^{1}$
	A_5	$4{,}9673781 \cdot 10^{-2}$
	A_6	$6{,}6049429 \cdot 10^{-1}$
	C_{LMP}	20,0

Dalsze obliczenia z wykorzystaniem parametrów Larsona-Millera nakreślono poniżej.

$$(5)\quad S_s = (\sigma_1^2 + \sigma_2^2 + \sigma_3^2)^{0,5} = (4{,}53^2 + 2{,}26^2 + 0^2)^{0,5} = 5{,}06 \text{ ksi}$$

$$(6)\quad J_1 = \sigma_1 + \sigma_2 + \sigma_3 = 4{,}53 + 2{,}26 + 0 = 6{,}79 ksi$$

$$(7)\quad S_{eff} = \sigma_e \cdot exp\left[0{,}24\left(\frac{J_l}{S_s} - 1\right)\right] = 3{,}92 \cdot exp\left[0{,}24\left(\frac{6{,}79}{5{,}06} - 1\right)\right] = 4{,}25 \text{ ksi}$$

(8) $$LMP(S_{eff}) = \frac{A_0 + A_2 S_{eff}^{0,5} + A_4 S_{eff} + A_6 S_{eff}^{1,5}}{1 + A_1 S_{eff}^{0,5} + A_3 S_{eff} + A_5 S_{eff}^{1,5}}$$

$$LMP(S_{eff}) = \frac{4{,}3981719 \cdot 10^{-1} - 4{,}0483005 \cdot 10^{1} \cdot 4{,}25^{0,5} + 1{,}5373650 \cdot 10^{1} \cdot 4{,}25 + 6{,}6049429 \cdot 10^{-1} \cdot 4{,}25^{1,5}}{1 - 8{,}4656117 \cdot 10^{-1} \cdot 4{,}25^{0,5} + 2{,}6236081 \cdot 10^{-1} \cdot 4{,}25 + 4{,}9673781 \cdot 10^{-2} \cdot 4{,}25^{1,5}}$$

$$LMP(S_{eff}) = 39{,}30$$

(9) $$log_{10}[L] = \frac{1000 \cdot LMP(S_{eff})}{(T_{refa} + T)} - C_{LMP}$$

$$log_{10}[L] = \frac{1000 \cdot 39{,}3}{(460 + 900)} - 20 = 8{,}90$$

(10) $$L = 10^{8,90} = 8 \cdot 10^{8} h$$

Trwałość w warunkach eksploatacji określonych cyklem operacyjnym m = 1 wynosi $8 \cdot 10^8$ h.

Ułamek uszkodzenia dla m = 1 wynosi zatem – jak poniżej.

(11) $$D_c = \sum_{n=1}^{N} \frac{t}{L} = \frac{84\,000}{8 \cdot 10^{8}} = 1{,}05 \cdot 10^{-4}$$

OBLICZENIA DLA POZOSTAŁYCH CYKLI EKSPLOATACYJNYCH

Analogiczne obliczenia przeprowadzono dla pozostałych cykli operacyjnych. Otrzymane wyniki zestawiono w tablicy 4.

Tablica 4. Wyniki obliczeń dla każdego z cykli operacyjnych

Parametry	Cykle operacyjne			
	m = 1	m = 2	m = 3	m = 4
Temperatura [°F]	900	1004	896	910
Ciśnienie [ksi]	0,39	0,47	0,38	0,46
Czas eksploatacji [h]	84 000	1000	55 000	60 000
σ_1 [ksi]	4,53	5,47	4,46	5,60
σ_2 [ksi]	2,26	2,73	2,23	2,80
σ_3 [ksi]	0	0	0	0
σ_e [ksi]	3,92	4,73	3,86	4,84
S_s [ksi]	5,06	6,11	4,98	6,25
J_1 [ksi]	6,79	8,19	6,69	8,39
S_{eff} [ksi]	4,25	5,13	4,19	5,26
LMP(S_{eff}) [ksi]	39,30	38,60	39,36	38,51
L [h]	$8{,}00 \cdot 10^8$	$2{,}35 \cdot 10^6$	$1{,}07 \cdot 10^9$	$1{,}30 \cdot 10^8$
D_c	$1{,}05 \cdot 10^{-4}$	$4{,}26 \cdot 10^{-4}$	$5{,}15 \cdot 10^{-5}$	$4{,}62 \cdot 10^{-4}$

Całkowity ułamek uszkodzenia jest sumą ułamków uszkodzeń wyznaczonych dla poszczególnych cykli operacyjnych – poniżej.

(12) $$D_c^{total} = 1{,}05 \cdot 10^{-4} + 4{,}26 \cdot 10^{-4} + 5{,}15 \cdot 10^{-5} + 4{,}62 \cdot 10^{-4} = 1{,}04 \cdot 10^{-3}$$

W celu spełnienia kryteriów oceny wyznaczona wartość musi być mniejsza od wartości kryterialnej

(13) $$D_c^{total} = \sum_{m=1}^{M} D_c \leq D_c^{allow}$$

$$D_c^{total} = 1{,}04 \cdot 10^{-3} \leq D_c^{allow} = 0{,}8 \text{ – warunek jest spełniony}$$

Płaszcz reaktora spełnia kryteria oceny wg API 579-1/ASME FFS-1 Fitness For Service – Part 10 – Assessment of components operating in the creep range – Level 2 Assessment – Larson-Miller Parameter.

PODSUMOWANIE I WNIOSKI KOŃCOWE

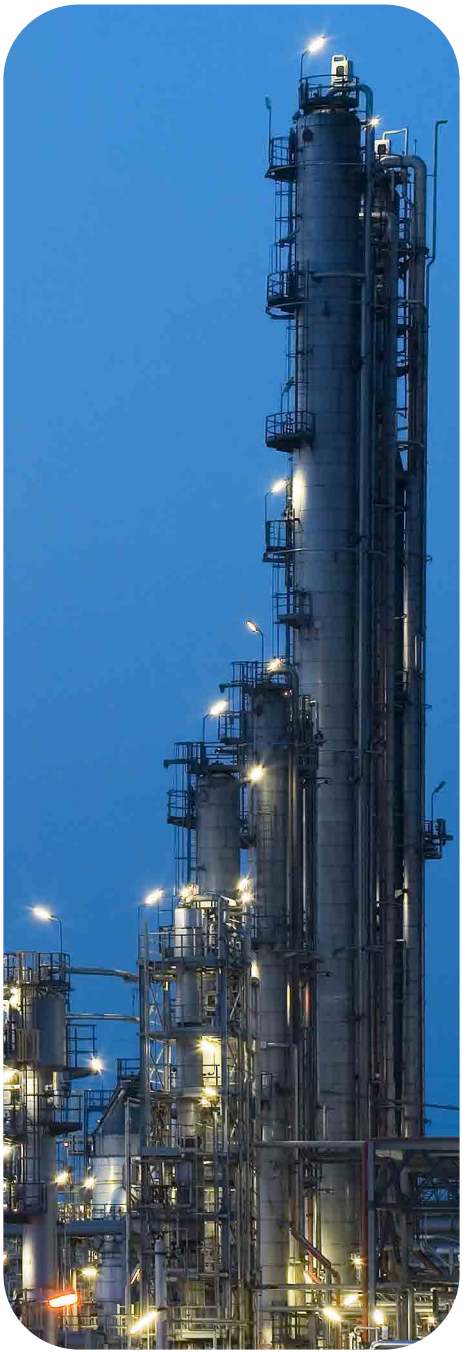
- Z przeprowadzonej analizy wynika, że oceniany komponent reaktora – płaszcz – uległ uszkodzeniom w wyniku pełzania w niewielkim stopniu. Obliczona wartość całkowitego uszkodzenia podczas pełzania z wykorzystaniem równań Larsona-Millera spełnia kryteria podane w API 579-1/ASME FFS-1 Fitness For Service – Assessment of components operating in the creep range – Level 2Assessment,

- Analizę przeprowadzono, zakładając przyszły czas eksploatacji wynoszący 60 000 h, licząc od daty wykonania ostatnich badań materiałowych, kiedy to aparat miał przepracowanych ok. 140 000 h. Wyniki otrzymanych badań stanowiły podstawę do oceny trwałości eksploatacyjnej reaktora, zgodnie z metodologią zawartą w API 579-1/ASME FFS-1 Fitness For Service.

- Dla analizowanego reaktora konieczne jest monitorowanie i utrzymywanie zapisów dotyczących parametrów pracy urządzenia. Należy wykonywać regularne badania diagnostyczne w celu weryfikacji przyjętych założeń.

SPIS SKRÓTÓW I OZNACZEŃ

D_C	uszkodzenie pełzaniowe *creep damage*
D_{mean}	średnia średnica walca lub sfery *mean diameter of a cylinder or sphere*
D_C^{allow}	dopuszczalne uszkodzenia pełzaniowe *allowable creep damage*
${}^nD_C$	uszkodzenia pełzaniowe w n-tym okresie czasu *creep damage for the time period*
D_C^{total}	całkowite uszkodzenia pełzaniowe uwzględniające wszystkie cykle pracy *total creep damage considering all operating cycles*
L_f	współczynnik Lorentza *Lorentz Factor*
${}^nL$	trwałość przy danej historii obciążania w n-tym przyroście czasu *rupture time for the loading history for the time increment*
$LMP({}^nS_{eff})$	parameter Larsona-Millera będący funkcją naprężenia *Larson-Miller parameter at stress*
m	aktualny numer cyklu operacyjnego *current operating cycle number*
P	ciśnienie wewnętrzne walca lub sfery *pressure inside of a cylinder or sphere*
R_i	promień wewnętrzny walca lub sfery *inside radius of a cylinder or sphere*
R_{mean}	średni promień walca lub sfery *mean radius of a cylinder or sphere*
${}^nS_{eff}$	naprężenia zredukowane użyte do obliczenia pozostałego okresu trwałości za pomocą parametru Larsona-Millera dla n-tego przyrostu czasu *effective stress used to compute the remaining life in terms of the Larson-Miller parameter for the time increment*
σ_e	naprężenia zredukowane *effective stress*
$\sigma_1, \sigma_2, \sigma_3$	składowe naprężeń głównych *principal stress*
t	czas *time*
T	temperatura *temperature*
t_{comp}	grubość elementu skorygowana o wielkość ubytku materiału i naddatku na korozję zgodnie z wymaganiami *component thickness adjusted for metal loss and corrosion allowance as required*
t_{sl}	grubość warunkowana działaniem dodatkowych obciążeń *thickness required for supplemental loads*



Literatura:

1. API RP 941 – Steels for Hydrogen Service at Elevated Temperatures and Pressures.

FITNESS FOR SERVICE

OCENA RUROCIĄGU Z LOKALNYM UBYTKIEM KOROZYJNYM

MGR INŻ. MATEUSZ WRÓBEL
Specjalista ds. Rozwoju Badań Laboratoryjnych
Wydział Badań Materiałowych i Ekspertyz
Centralne Laboratorium Dozoru Technicznego

MGR INŻ. TOMASZ KLINKOSZ
Ekspert Urządzeń Ciśnieniowych
Dział Oceny Zgodności
Oddział w Gdańsku
Urząd Dozoru Technicznego

DR INŻ. MARIUSZ ŁUCKI
Główny Specjalista ds. Rozwoju Badań Laboratoryjnych
Wydział Badań Materiałowych i Ekspertyz
Centralne Laboratorium Dozoru Technicznego

JEDNYM Z NAJCZĘŚCIEJ WYSTĘPUJĄCYCH MECHANIZMÓW DEGRADACJI W PRZEMYŚLE RAFINERYJNYM I PETROCHEMICZNYM JEST KOROZJA. W ZALEŻNOŚCI OD ŚRODOWISKA PRACY, MIEJSCA WYSTĘPOWANIA I CHARAKTERU POWSTAJĄCYCH UBYTKÓW KOROZYJNYCH MOŻEMY WYRÓŻNIĆ JEJ RÓŻNE RODZAJE, TJ. KOROZJA POD IZOLACJĄ, KOROZJA W ŚRODOWISKU KWASU SOLNEGO, KOROZJA ATMOSFERYCZNA. WIELE PRZYDATNYCH INFORMACJI NA JEJ TEMAT ORAZ INNYCH MECHANIZMÓW DEGRADACJI MOŻNA ZNALEŹĆ W DOKUMENCIE API RECOMMENDED PRACTICE 571 DAMAGE MECHANISMS AFFECTING FIXED EQUIPMENT IN THE REFINING INDUSTRY.

Sposoby oceny uszkodzeń powstałych w wyniku korozji zostały opisane w standardzie API 579-1/ASME FFS-1 Fitness For Service. Metodologia ta dzieli je na trzy rodzaje:

- korozję ogólną → Part 4 – Assessment of General Metal Loss;
- korozję lokalną → Part 5 – Assessment of Localized Metal Loss;
- korozję wżerową → Part 6 – Assessment of Pitting Damage.

W prezentowanym opracowaniu przybliżony zostanie sposób postępowania w przypadku wykrycia korozji o charakterze lokalnym.

OPIS PRZEDMIOTU ANALIZY

Analizie zostało poddane kolano rurociągu służącego do transportu aminy bogatej. W trakcie okresowych pomiarów grubości wykryto pocienienia na zewnętrznej tworzącej kolana. Pozostała grubość materiału była mniejsza od wymaganej, wynoszącej minimum 4,63 mm. Wobec tego faktu podjęto próbę przeprowadzenia oceny kolana zgodnie z metodologią Fitness For Service. Szczegółowe informacje dotyczące analizowanego komponentu przedstawiono w tablicy 1.

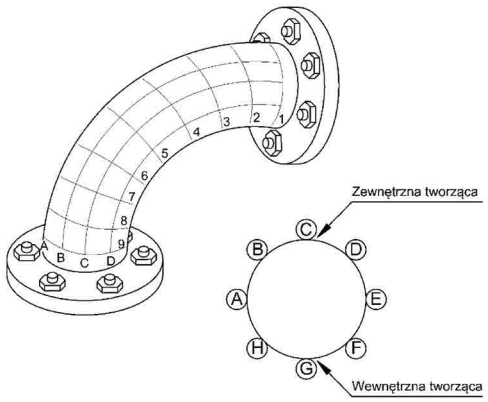
Tablica 1. Dane dotyczące analizowanego kolana rurociągu

Materiał kolana	ASTM A234 Grade WPB
Parametry obliczeniowe: ciśnienie, temperatura	0,78 MPa 240°C
Średnica zewnętrzna rurociągu	168,3 mm
Grubość nominalna	7,11 mm
FCA = FCA_{ml}	1 mm
Naprężenia dopuszczalne	133,04 MPa
Współczynnik wytrzymałościowy złącza obwodowego i wzdłużnego	1
Grubość wynikająca z obciążeń dodatkowych	0 mm

CHARAKTERYSTYKA WYKRYTEGO UBYTKU KOROZYJNEGO

Metodologia Fitness For Service podaje wymagania i wskazówki związane z oceną ubytków korozyjnych. Dotyczą one m.in. doboru siatek pomiarowych, wymiarowania wykrytych pocienień czy też konieczności przeprowadzenia dodatkowych badań NDT złączy spawanych znajdujących się zbyt blisko ubytków korozyjnych.

Pierwotnie wykonane badania okresowe (kilka pomiarów grubości na kolanie) nie pozwoliły na scharakteryzowanie powstałego ubytku korozyjnego oraz przeprowadzenie oceny zgodnie z metodologią Fitness For Service. W związku z tym konieczne było ich powtórzenie. Ultradźwiękowe pomiary grubości zrealizowano zgodnie z siatką pomiarową przedstawioną na rysunku 1. Uzyskanie większej liczby punktowych odczytów grubości pozwala na dokładniejsze oszacowanie wymiaru powstałego ubytku korozyjnego zarówno w kierunku obwodowym, jak i wzdłużnym.



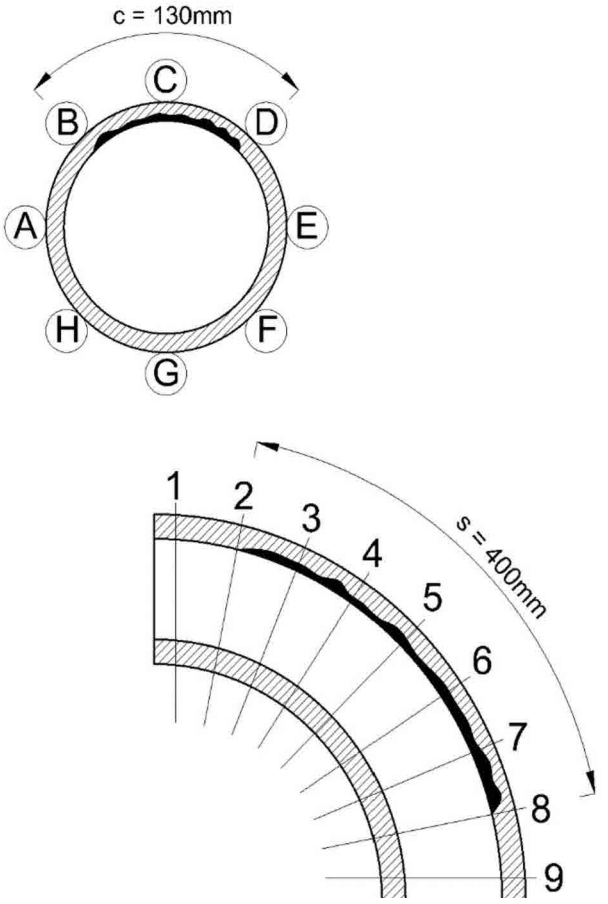
Rys. 1. Schemat siatki pomiarowej wykorzystanej podczas badań

WYNIKI BADAŃ

Wyniki ultradźwiękowych pomiarów grubości zestawiono w tablicy 2. Zarejestrowane zmiany grubości potwierdzają lokalny charakter wykrytego ubytku korozyjnego. Pocienienie zlokalizowane jest na zewnętrznej tworzącej kolana. Określono minimalną zmierzoną grubość (t_{mm}=3,0 mm). Oszacowany został także zasięg występowania pocienienia. Wymiar obwodowy, c=130 mm, a wymiar wzdłużny, s=400 mm (patrz rys. 2). Zgromadzone dane pozwalają także na wyznaczenie krytycznych profili grubości (ang. Critical Thickness Profile – CTP). Obwodowy i wzdłużny CTP przedstawiono na rysunku 4. Zostały one wykorzystane w dalszej części analizy.

Tablica 2. Wyniki pomiarów grubości

Punkt pomiarowy	A	B	C	D	E	F	G	H	Wzdłużny CTP
1	6,0	5,6	5,5	5,6	5,8	5,9	6,0	6,1	**5,5**
2	5,8	4,5	4,5	4,9	5,7	5,8	6,2	6,0	**4,5**
3	5,9	4,1	3,7	4,5	5,9	5,7	6,1	6,0	**3,7**
4	6,0	3,8	3,2	3,9	5,8	5,7	6,2	5,8	**3,2**
5	5,6	3,7	3,0	3,8	5,9	5,9	6,1	5,7	**3,0**
6	5,8	3,6	3,3	4,0	6,0	5,8	6,0	5,7	**3,3**
7	5,7	3,8	3,7	4,2	5,6	5,8	6,2	5,9	**3,7**
8	5,7	4,1	4,0	5,6	5,8	5,9	6,0	6,0	**4,0**
9	5,9	5,8	5,7	5,8	5,7	5,9	6,1	6,0	**5,7**
Obwodowy CTP	**5,6**	**3,6**	**3,0**	**3,8**	**5,6**	**5,7**	**6,0**	**5,7**	

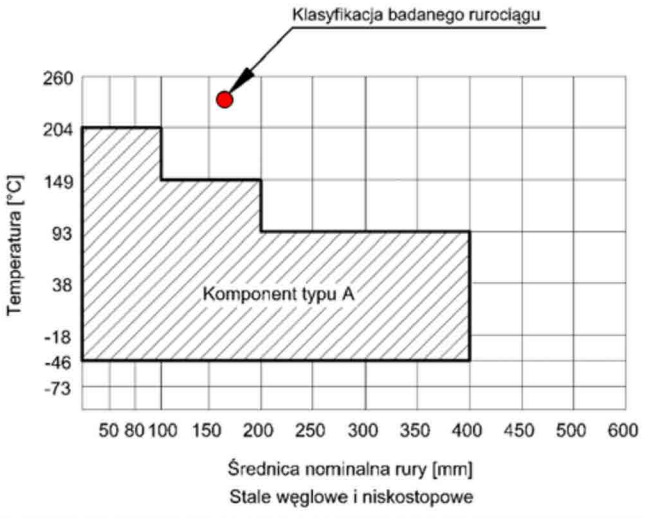


Rys. 2. Schematyczne przedstawienie zasięgu występowania lokalnego ubytku korozyjnego

USTALENIE METODOLOGII OCENY

Aby możliwe było przeprowadzenie oceny zgodnie z Part 5 – Assessment of local metal loss, konieczne jest spełnienie poniższych założeń:

- Temperatura graniczna dla materiału, z którego wykonano kolana rurociągu, wynosi 371°C (wg Table 4.1 API 579-1/ASME FFS-1). Temperatura projektowa rurociągu jest od niej niższa. Rurociąg nie pracuje w warunkach pełzania.
- W wyniku analizy dokumentacji technicznej urządzenia stwierdzono, że na rurociąg nie działają dodatkowe obciążenia. Nie powoduje to tym samym zwiększenia grubości obliczeniowej analizowanych kolan rurociągu.
- Warunki pracy rurociągu nie pozwalają na zakwalifikowanie ocenianego kolana jako komponentu typu A wg API 579-1/ASME FFS-1. Kolana należy sklasyfikować jako komponenty typu B klasy 1 – patrz rys. 3.
- Kolana sklasyfikowane jako komponenty typu B klasy 1 zostaną poddane ocenie na poziomie 2 (Level 2 Assessment).

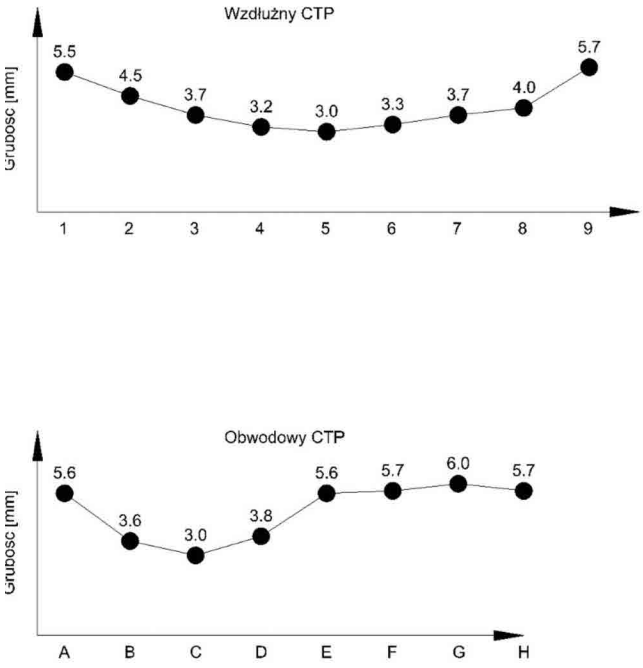


Rys. 3. Kategoryzacja komponentów typu A

OCENA KOLANA RUROCIĄGU

W tym rozdziale przybliżone zostaną poszczególne kroki, które muszą zostać zrealizowane podczas prowadzenia oceny.

Krok 1 – Wyznaczenie krytycznych profili grubości (patrz rys. 4).



Rys. 4. Krytyczne profile grubości

Krok 2 – Określenie wartości:

t_{rd} = 5,8 mm

$t_c = t_{rd} - FCA$ = 5,8 – 1 = 4,8 mm

Krok 3 – Określenie wartości:

t_{mm} = 3,0 mm
s = 400 mm
c = 130 mm

Krok 4 – Wyznaczenie parametrów:

$$R_t = \frac{t_{mm} - FCA_{ml}}{t_c} = \frac{3-1}{4,8} = 0,4$$

$$D = D_0 - 2t_{rd} + 2FCA_{ml} = 168,3 - 2 \cdot 5,8 + 2 \cdot 1 = 158,7 \text{ mm}$$

$$\lambda = \frac{1,285s}{Dt_c} = \frac{1,285 \cdot 400}{\sqrt{158,7 \cdot 4,8}} = 18,6$$

Krok 5 – Sprawdzenie poniższych warunków:

$(R_t=0,4) \geq 0,2$

Warunek jest spełniony.

$(t_{mm} - FCA_{ml} = 3 - 1 = 2,0 \text{ mm}) \geq 1,3 \text{ mm}$

Warunek jest spełniony.

Krok 6

W celu wyznaczenia wartości:

$$MAWP^C = \frac{2\left(\frac{SE_c}{L_f}\right)(t_c - MA)}{D_0 - 2Y_{B31}(t_c - MA)}$$

Konieczne jest wyznaczenie współczynnika Lorenza L_f.

$$R_m = \frac{D_0 + D}{4} = \frac{168,3 + 158,7}{4} = 81,7 \text{ mm}$$

Sprawdzenie warunku:

$$\frac{R_m}{t_c} = \frac{81,7}{4,8} = 17,0 \geq 10$$

Warunek jest spełniony.

Stosujemy współczynnik Lorenza dla $\theta = 90°$ (lokalne pocienienie zlokalizowane na zewnętrznej tworzącej).

$$L_f = \left(\frac{\frac{R_b}{R_m} + 0,5}{\frac{R_b}{R_m} + 1}\right) = \left(\frac{\frac{229}{81,7} + 0,5}{\frac{229}{81,7} + 1}\right) = 0,868$$

$R_b = 229$ mm wg standardu ASME B16.9
$Y_{B31} = 0,4$ na podstawie rozdziału 2.C.7 API 579-1/ASME FFS-1
$MA = 0$

$$MAWP^C = \frac{2\left(\frac{SE_c}{L_f}\right)t_c - MA}{D_0 - 2Y_{B31}(t_c - MA)} = \frac{2\left(\frac{133,04 \cdot 1}{0,868}\right)(4,8-0)}{168,3 - 2 \cdot 0,4(4,8-0)} = 8,9 \text{ MPa}$$

Wyznaczenie wartości:

$$MAWP^L = \frac{4SE_L(t - t_{sl} - MA)}{D_0 - 4Y_{B31}(t - t_{sl} - MA)}$$

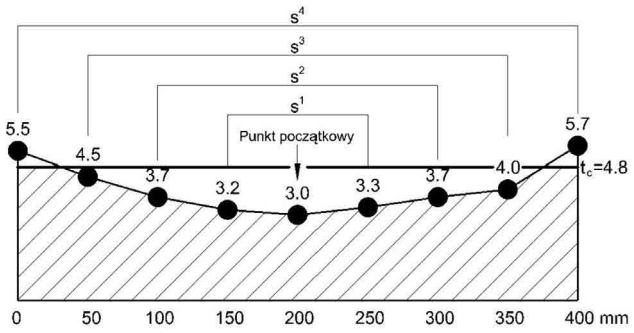
$$MAWP^L = \frac{4 \cdot 133,04 \cdot 1(4,8-0-0)}{168,3 - 4 \cdot 0,4(4,8-0-0)} = 15,0 \text{ MPa}$$

Wyznaczenie wartości *MAWP*:

$MAWP = min\,[MAWP^C, MAWP^L] = min\,[8,9;15,0] = 8,9$ MPa

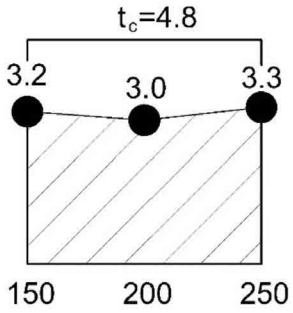
Krok 7 – Wyznaczenie współczynnika RSF dla wzdłużnego CTP.

Procedura wyznaczania współczynnika RSF jest obszerna. Wymaga ona m.in. podzielenia profilu grubości na podsekcje. Dla każdej z nich wyznacza się cząstkowe wartości RSF^i. Należy określić minimalną wartość RSF^i.



Rysunek 5. Krytyczny profil grubości podzielony na podsekcje

Wyznaczenie wartości RSF1 dla podsekcji s1:



$s^1 = 100$ mm

$$A_0^1 = s^1 \cdot t_c = 100 \cdot 4,8 = 480 \text{ mm}^2$$

$$A^1 = (4,8-3,2) \cdot 50 + (4,8-3,3) \cdot 50 + \frac{1}{2} \cdot 50 \cdot (3,2-3,0) + \frac{1}{2} \cdot 50 \cdot (3,3-3,0)$$

$$A^1 = 167,5 \text{ mm}^2$$

$$\lambda^1 = \frac{1,285 \cdot s^1}{\sqrt{Dt_c}} = \frac{1,285 \cdot 100}{\sqrt{158,7 \cdot 4,8}} = 4,6$$

$$M_t^1 = 1,001 - 0,014195\lambda + 0,2909\lambda^2 - 0,09642\lambda^3 + 0,02089\lambda^4 - 0,003054\lambda^5 + 2,957 \cdot 10^{-4}\lambda^6 - (1,8462 \cdot 10^{-5}\lambda^7) + 7,1553 \cdot 10^{-7}\lambda^8 - 1,5631 \cdot 10^{-8}\lambda^9 + 1,4656 \cdot 10^{-10}\lambda^{10}$$

$$M_t^1 = 1,001 - 0,014195 \cdot 4,6 + 0,2909 \cdot 4,6^2 - 0,09642 \cdot 4,6^3 + 0,02089 \cdot 4,6^4 - 0,003054 \cdot 4,6^5 + 2,957 \cdot 10^{-4} \cdot 4,6^6 - 1,8462 \cdot 10^{-5} \cdot 4,6^7 + 7,1553 \cdot 10^{-7} \cdot 4,6^8 - 1,5631 \cdot 10^{-8} \cdot 4,6^9 + 1,4656 \cdot 10^{-10} \cdot 4,6^{10}$$

$M_t^1 = 2,9$

$$RSF^1 = \frac{1 - \left(\frac{A^1}{A_0^1}\right)}{1 - \frac{1}{M_t^1}\left(\frac{A^1}{A_0^1}\right)} = \frac{1 - \left(\frac{167,5}{480}\right)}{1 - \frac{1}{2,9}\left(\frac{167,5}{480}\right)} = 0,74$$

W analogiczny sposób wykonano obliczenia dla kolejnych podsekcji. Otrzymane parametry zestawiono w tablicy 3.

Tablica 3. Parametry wyznaczone dla każdej z podsekcji

Podsekcja	*si [mm]*	λ^i	A^i [mm²]	A_0^i [mm²]	M_t	RSF^i
1	100	4,6	167,5	480	2,9	0,74
2	200	9,3	300	960	5,1	0,73
3	300	13,9	382,5	1440	8,8	0,75
4	400	18,6	394,2	1920	19,1	0,80

Minimalna wartość współczynnika RSF wynosi 0,73.

$RSF_{min} = 0,73$

Wyznaczanie współczynnika RSF jest żmudne. W zależności od otrzymanego profilu grubości obliczenia należy prowadzić, rozpoczynając od różnych punktów początkowych, tak aby wyznaczyć minimalną wartość RSF.

Krok 8 – Sprawdzenie warunku:

$RSF \geq RSF_a$

0,73 ≥ 0,9 **Fałsz. Warunek nie jest spełniony.**

Urządzenie nie może być eksploatowane przy MAWP wyznaczonym w kroku 6.

Wyznaczenie wartości $MAWP_r$:

$$MAWP^L = MAWP \frac{RSF}{RSF_a} = 8,9 \cdot \frac{0,73}{0,9} = 7,2 \text{ MPa}$$

$MAWP_r = 7,2 \text{ MPa} \geq P = 0,78 \text{ MPa}$

Krok 9 – Sprawdzenie poniższego kryterium:

$$c \leq 2s \frac{E_L}{E_c}$$

$$130 \leq 2 \cdot 400 \cdot \frac{1}{1}$$

Warunek jest spełniony.

Kolano rurociągu spełnia kryteria oceny wg API 579-1/ASME FFS-1 Fitness For Service – Part 5 – Assessment of local metal loss – Level 2 Assessment.

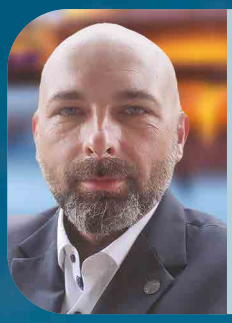
PODSUMOWANIE I WNIOSKI KOŃCOWE

- Na podstawie przeprowadzonej analizy wykazano, że kolano rurociągu, mimo powstałego ubytku korozyjnego, może być nadal eksploatowane.
- Przyjęta do oceny wartość FCA = FCA_{ml} = 1 mm odpowiada wielkości ubytku korozyjnego, który powstanie po 10 latach eksploatacji. Okres ten można uznać za czas dalszej bezpiecznej eksploatacji.
- Założenia przyjęte do obliczeń, w szczególności te oparte na szybkości korozji, powinny być stale monitorowane i weryfikowane.

SPIS SKRÓTÓW I OZNACZEŃ

A^i	obszar ubytku materiału na odcinku uwzględniający wpływ FCA_{ml} *area of metal loss based on including the effect of FCA_{ml}*
A_0^i	pierwotny obszar materiału na odcinku si *original metal area based on s^i*
D_0	zewnętrzna średnica cylindra, stożka (w miejscu wady), dennicy sferycznej lub eliptycznej skorygowana odpowiednio o LOSS i FCA *outside diameter of the cylinder, cone (at the location of the flaw), sphere, or formed head corrected for LOSS and FCA*
FCA	naddatek na korozję mający zastosowanie do obszaru z dala od miejsca ubytku materiału *Future Corrosion Allowance applied to the region away from the metal loss*
FCA_{ml}	nadd atek na korozję mający zastosowanie do obszaru ubytku materiału *Future Corrosion Allowance applied to the region of metal loss*
λ	parametr charakteryzujący wymiar wzdłużny wady *longitudinal flaw length parameter*
λ^i	przyrostowy parametr charakteryzujący wymiar wzdłużny wady *incremental longitudinal flaw length parameter*
λ_c	parametr charakteryzujący wymiar obwodowy wady *circumferential flaw length parameter*
MA	naddatek stosowany w przypadku elementów gwintowanych *mechanical allowances (thread or groove depth); for threaded components, the nominal thread depth (dimension h of ASME B.1.20.1) shall apply*
MAWP	maksymalne dopuszczalne ciśnienie robocze nieuszkodzonego elementu *Maximum Allowable Working Pressure of the undamaged component*
$MAWP^c$	maksymalne dopuszczalne ciśnienie robocze dla naprężeń obwodowych *Maximum Allowable Working Pressure based on the stresses in the circumferential or hoop direction*
$MAWP^L$	maksymalne dopuszczalne ciśnienie robocze dla naprężeń wzdłużnych *Maximum Allowable Working Pressure based on the stresses in the longitudinal direction*
$MAWP_r$	zredukowane maksymalne dopuszczalne ciśnienie robocze dla uszkodzonego elementu *reduced maximum allowable working pressure of the damaged component*
M_t	współczynnik oparty na wzdłużnym zasięgu LTA dla wady przechodzącej przez ścianę *Folias factor based on the longitudinal extent of the LTA for a through-wall flaw*
R_b	promień gięcia kolana *centerline bend radius*
R_m	średni promień elementu *mean radius of the component; use the large end radius for a conical shell*
R_t	pozostały stosunek grubości *remaining thickness ratio*
RSF	obliczony współczynnik wytrzymałości oparty na zasięgu południkowym LTA *computed remaining strength factor based on the meridional extent of the LTA*
RSF_a	dopuszczalny współczynnik wytrzymałości *allowable remaining strength factor*
RSF^i	RSF dla aktualnie ocenianej podsekcji *for the current subsection being evaluated*
s^i	przyrostowy wzdłużny zasięg lub długość obszaru lokalnej utraty materiału *longitudinal extent or length increment of metal loss*
t_c	grubość ściany z dala od obszaru uszkodzeń w stanie skorodowanym *wall thickness away from the damaged area adjusted for LOSS and FCA, as applicable*
t_{lim}	grubość strukturalna *limiting thickness*
t_{mm}	minimalna zmierzona grubość określona w momencie oceny *minimum measured thickness determined at the time of the inspection*
t_{nom}	nominalna lub rzeczywista grubość elementu skorygowana o ujemną odchyłkę, stosownie do przypadku *nominal or furnished thickness of the component adjusted for mill under tolerance as applicable*
t_{rd}	jednolita grubość z dala od miejscowego miejsca ubytku metalu, ustalona na podstawie pomiarów grubości w czasie oceny *uniform thickness away from the local metal loss location established by thickness measurements at the time of the assessment*

DYNAMICZNE ZARZĄDZANIE RYZYKIEM INSTALACJI PRZEMYSŁOWYCH. OPTYMALIZACJA – NARZĘDZIA PRZEMYSŁU 4.0



MGR INŻ. TOMASZ KLINKOSZ

Ekspert Urządzeń Ciśnieniowych
Dział Oceny Zgodności
Urząd Dozoru Technicznego
Oddział w Gdańsku

POZIOM DOJRZAŁOŚCI ZARZĄDZANIA RYZYKIEM RÓŻNI SIĘ W ZALEŻNOŚCI OD BRANŻY I FIRMY. OGÓLNIE RZECZ BIORĄC, NAJBARDZIEJ ZAAWANSOWANE PODEJŚCIE MAJĄ BANKI, A NASTĘPNIE FIRMY Z BRANŻ, W KTÓRYCH BEZPIECZEŃSTWO JEST NAJWAŻNIEJSZE, W TYM ROPA I GAZ, ZAAWANSOWANA PRODUKCJA I FARMACEUTYKA. POMIMO TEGO PRAWIE WSZYSTKIE ORGANIZACJE MUSZĄ ODŚWIEŻYĆ I WZMOCNIĆ SWOJE PODEJŚCIE DO ZARZĄDZANIA RYZYKIEM, ABY DOSTOSOWAĆ SIĘ DO ZMIENIAJĄCEGO SIĘ OTOCZENIA [1].

Proces podejmowania decyzji na podstawie wyników analiz ryzyka i zastosowanie podejścia opartego na zarządzaniu ryzykiem są pojęciami często używanymi i podkreślanymi w podejściu procesowym. Jest on powszechnie stosowany, stosowany jest powszechnie w podejmowaniu decyzji m.in. w zakresie ochrony zdrowia, środowiska, w bezpieczeństwie żywności, bezpieczeństwie produktów, bezpieczeństwie pracy i bezpieczeństwie procesowym oraz cyberbezpieczeństwie. W każdym z tych procesów wykorzystuje się różne dane oraz różne narzędzia do analizy ryzyk, zależnie od korzyści płynących z ich wyboru w odniesieniu do danego zastosowania [2].

DYNAMICZNE ZARZĄDZANIE RYZYKIEM

W ogólnym ujęciu dynamiczne zarządzanie ryzykiem można opisać w trzech zasadniczych obszarach:

- identyfikacja potencjalnych nowych zagrożeń i słabości w procesach kontrolnych,
- określanie skłonności do podejmowania ryzyka (tzw. apetyt na ryzyko),
- wdrożenie właściwego podejścia do zarządzania ryzykiem.

Odnosząc powyższe ogólne podejście do dynamicznego zarządzania ryzykiem na polu bezpieczeństwa instalacji przemysłowych, nie można pominąć otoczenia geopolitycznego, które w obecnym czasie wydatnie pokazuje, że dynamika w zarządzaniu zarówno w kontekście biznesowym, jak i bezpieczeństwa procesowego staje się kluczowa. Występujące zmiany popytu w niektórych obszarach produkcji petrochemicznej, zaburzenia w łańcuchach dostaw surowców oraz części zamiennych powodują konieczność reakcji i dynamicznego podejmowania decyzji ze strony zakładów produkcyjnych [3].

Zmiany te mogą mieć również wpływ na politykę remontową zakładów produkcyjnych wynikającą z nieterminowych dostaw elementów zamiennych lub konieczność wprowadzenia zmian w harmonogramach remontowych w celu zapewnienia ciągłości działania. Wpływa to bez wątpienia na bezpieczeństwo eksploatacji infrastruktury produkcyjnej i musi być uwzględnione w prowadzonych analizach ryzyk technicznych i operacyjnych.

W takich warunkach klasyczny model zarządzania ryzykiem oparty na okresowych przeglądach ryzyk i wdrażaniu działań korekcyjnych staje się coraz mniej skutecznym narzędziem zarządczym.

DIGITALIZACJA PROCESÓW DAJE NOWE MOŻLIWOŚCI

Rozwój technologiczny, zwłaszcza w zakresie digitalizacji procesów, otwiera nowe możliwości w dziedzinie zarządzania ryzykiem, w szczególności pozwala na uzyskanie znacznie większej dynamiki procesów przetwarzania danych wykorzystywanych do analizy ryzyk.

Można zatem postawić pytanie: w jakim obszarze zarządzania ryzykiem instalacji przemysłowej znajdują zastosowanie nowe technologie?

Odpowiedź na to pytanie nie jest prosta, ponieważ rozwój tej branży jest na tyle dynamiczny, że wymaga przeglądu niemal niemal stale. Niemniej jednak obszarem, w którym bez wątpienia można wykorzystać nowe technologie, jest proces gromadzenia, obróbki i analizy danych używanych do oceny ryzyka.

Zanim omówimy powyższe zastosowania, należy zdefiniować pojęcie przemysłu 4.0.

Przemysł 4.0 można zdefiniować jako unifikację świata rzeczywistego maszyn produkcyjnych ze światem wirtualnym internetu i technologii informacyjnej [4]. W tym procesie ludzie, maszyny oraz systemy IT automatycznie wymieniają informacje zarówno w toku produkcji, jak też w zakresie danych wykorzystywanych do podejmowania decyzji na podstawie ryzyka.

GRANICE I ZASADY

Włączając tego typu technologie w proces decyzyjny, należy zadbać o stworzenie odpowiedniej przestrzeni do ich funkcjonowania, tzn. ustanowienia granic i zasad stosowania, w tym odpowiednich procedur i zasad walidacji wyników.

W odniesieniu do relacji człowiek – system adaptacji wzmocnienia wymaga system zarządzania. W aspekcie bezpieczeństwa i ciągłości działania instalacji procesowej będzie to opisane systemem zarządzania bezpieczeństwem procesowym. Jednym z powszechniej stosowanych jest model systemu zarządzania bezpieczeństwem procesowym Risk Based Process Safety wg CCPS (Center of Chemical Process Safety) (rys. 1).

Rys. 1. Model systemu zarządzania bezpieczeństwem procesowym wg CCPS [7]

W modelu CCPS występują obszary o szczególnym znaczeniu dla dynamiki procesu zarządzania bezpieczeństwem:

- zarządzanie zmianami (MANAGEMENT OF CHANGE)
- identyfikacja zagrożeń i analiza ryzyka (HAZARD IDENTIFICATION AND RISK ANLALYSIS)
- integralność mechaniczna (ASSET INTEGRITY AND RELIABILITY) w odniesieniu do bezpieczeństwa związanego z eksploatacją infrastruktury produkcyjnej

Wymienione obszary wymagają adaptacji w celu zapewnienia odpowiedniej dynamiki procesu zarządczego. Są one jednym z przykładów procesów, w których następuje interakcja człowieka, maszyn i systemów IT, a zatem obszarów mieszczących się w zakresie tzw. przemysłu 4.0.

Można wyróżnić obszary procesów zarządzania ryzykiem urządzeń w instalacji procesowej, w których poprzez zastosowanie rozwiązań, takich jak automatyzacja zadań, następuje zautomatyzowane przetwarzanie danych (rys. 2).

Zastosowanie technologii wykorzystujących sztuczną inteligencję jest kluczowe dla dynamicznego zarządzania ryzykiem.

Automatyzacja zadań

- Automatyzacja transferu danych procesowych do systemów wykorzystywanych do predykcji zużycia (np. RBI, RCM, Digital Twin)
- Automatyzacja badań nieniszczących

Przetwarzanie złożonych lub dużych zbiorów danych

- Dane procesowe
- Wyniki badań nieniszczących i niszczących
- Analiza wyników modeli predykcyjnych

Zgłaszanie anomalii lub interesujących wydarzeń

- Analiza zdarzeń awaryjnych
- Analiza wyników wskazań uzyskanych w badaniach NDT (np. UT, AE, RT)

Znakowanie danych i korekcja błędów

- Zarządzanie danymi IOW (Integrity Operating Windows)

Funkcje zintegrowane

- Optymalizacja doboru metod badawczych (identyfikacja typów uszkodzeń)
- Identyfikacja obszarów narażonych na degradację (np. SCC)
- Digital Twin

Rys. 2. Potencjalne obszary wykorzystania technologii przemysłu 4.0 do zarządzania ryzykiem instalacji procesowej

METODYKA RBI

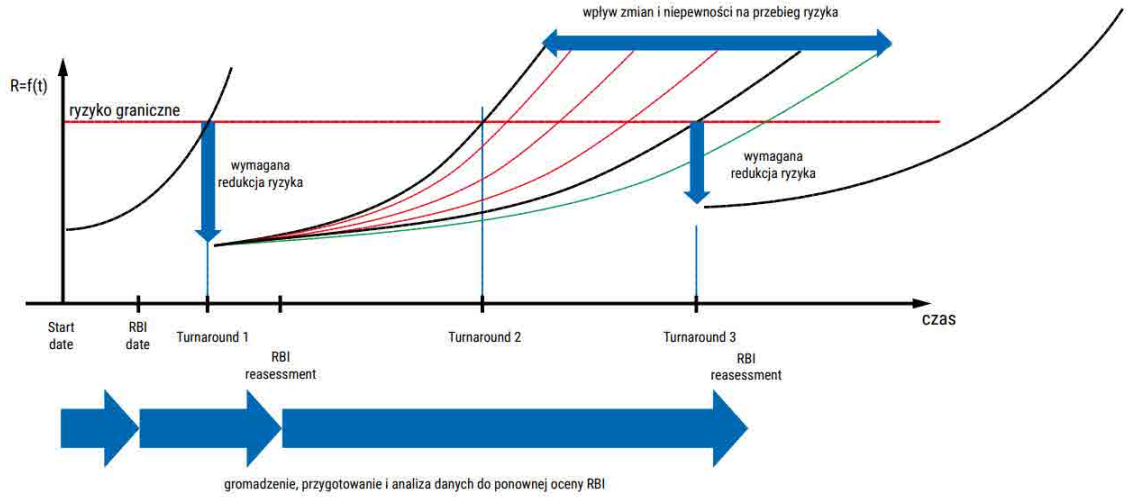
Wpływ wskazanych obszarów można przedstawić na przykładzie procesu zarządzania ryzykiem z wykorzystaniem metodologii Risk-based Inspection, który prowadzony wg standardu API RP 581 pozwala na dokonanie ilościowej analizy ryzyka dla urządzeń ciśnieniowych, szczególnie w przemyśle petrochemicznym.

Risk-based Inspection, w odróżnieniu od powszechnie stosowanych w przemyśle narzędzi do analizowania zagrożeń i ryzyka, takich jak HAZOP (Hazard and Operability Study), LOPA (Layer of Protection Analysis) czy QRA (Quantitative Risk Assessment), jest metodą predykcyjną.

Predykcyjna metoda Risk-based Inspection (RBI) jest narzędziem do zarządzania ryzykiem. RBI zawiera model opisujący zmiany ryzyka w funkcji czasu (rys. 3). Proces zarządzania ryzykiem bazuje na cyklicznej walidacji. Między walidacjami następuje proces gromadzenia i analizy danych.

Metodyka RBI, zawierająca model opisujący zmiany ryzyka w funkcji czasu, jest również narzędziem do zarządzania ryzykiem, a zatem jest procesem ciągłym, wymagającym stworzenia w organizacji odpowiednich procesów oraz ich implementacji do obowiązującego systemu zarządzania organizacją [5].

W procesie tym dokonywana jest predykcja zmian ryzyka w funkcji czasu, niemniej jednak zmiany ryzyka uzależnione są od wielu czynników, których modyfikacje mogą być uwzględnione w terminie ponownej oceny (walidacji) RBI. Proces zarządzania ryzykiem w tej metodologii bazuje na cyklicznej walidacji, podczas której dokonuje się ponownej oceny z uwzględnieniem zebranych danych w okresie, który upłynął od poprzedniej walidacji.



Rys. 3. Model zarządzania ryzykiem w procesie RBI

WALIDACJA

Dane do walidacji pochodzą zarówno z różnych systemów rejestracji parametrów procesowych, analiz laboratoryjnych, jak też z wyników badań nieniszczących, inspekcji oraz zapisów sporządzanych w toku eksploatacji instalacji.

Dzięki coraz większej cyfryzacji procesów produkcyjnych dysponujemy ogromnymi zbiorami tych danych, jednakże z uwagi na mnogość systemów archiwizacji danych oraz różną ich formę zautomatyzowana analiza danych musi być poprzedzona ich przygotowaniem.

Proces ten jest jednym z obszarów zastosowania metod opartych na zalgorytmizowanej obróbce danych, dzięki którym możliwe jest np. poszukiwanie anomalii i korelacji pomiędzy danymi.

- Tworzone są i testowane rozwiązania oparte np. na technologiach sztucznych sieci neuronowych ANN (Artificial Neural Networks) lub rozwiązaniach hybrydowych wykorzystujących różne technologie do obróbki i analizy danych wykorzystywanych w analizach ryzyka [6].
- Zastosowanie takich technologii w procesie zarządzania ryzykiem może przyczynić się do skrócenia okresów pomiędzy kolejnymi walidacjami.
- Jak w każdym procesie analizy danych, należy pamiętać o zasadzie GIGO (garbage in, garbage out). Jest to szczególnie istotne w procesie analizy ryzyka instalacji procesowej, w której proces pozyskiwania danych jest bardzo złożony.
- Analiza danych pochodzących np. z zapisów zdarzeń awaryjnych, dokumentacji inspekcyjnych wymaga wiedzy eksperckiej.

ZARZĄDZANIE ZMIANAMI

Zmiany przebiegu ryzyka w czasie (rys. 3) mogą skutkować skróceniem okresu do przekroczenia wartości akceptowalnego ryzyka, co potencjalnie prowadzi do sytuacji niebezpiecznej. Zmiany te mogą wynikać między innymi z błędnych danych wykorzystanych w modelowaniu lub założeń.

W tym zakresie zarządzanie ryzykiem realizowane jest poprzez skuteczny system zarządzania zmianami oraz monitorowania czynników ryzyka (tzw. risk drivers), czyli czynników, które wykorzystano do zbudowania modelu predykcyjnego.

Czynnikami tymi mogą być między innymi parametry procesu technologicznego czy określone podczas analizy graniczne stężenia czynników powodujących degradację ścianki urządzenia.

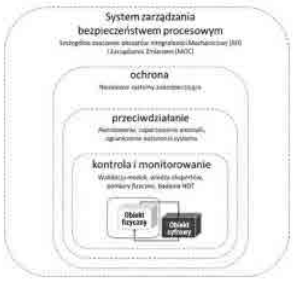
Równie istotnym elementem są założenia podejmowane w toku obliczeń ryzyka, szczególnie w obliczeniach konsekwencji potencjalnego uszkodzenia, które mogą wpłynąć na wartość ryzyka. Są to np. liczba osób potencjalnie narażonych na konsekwencje lub rodzaj i sposób działania systemów ograniczających skutki po uwolnieniu.

Jak wspomniano wcześniej, skuteczność elementów systemu zarządzania bezpieczeństwem procesowym, takich jak zarządzanie zmianami, integralność mechaniczna oraz analizowanie zagrożeń i ryzyka, w znaczący sposób może wpłynąć na wyniki ryzyka, dlatego powinny być doskonalone przede wszystkim w zakresie wiarygodności uzyskiwanych wyników oraz określenia wymagań dla wyników tych procesów.

NOWE TECHNOLOGIE I RYZYKA

Wdrażając nowe technologie w obszarze zarządzania bezpieczeństwem instalacji przemysłowych, oparte np. na sieciach neuronowych czy sztucznej inteligencji, nie można zapomnieć o ustanowieniu zasad bezpiecznego ich stosowania.

Wydaje się celowe, aby do zarządzania bezpieczeństwem tych technologii wykorzystać sprawdzone w praktyce rozwiązania, np. wielowarstwowy model bezpieczeństwa, który opisano m.in. w normie PN-EN 61511. Można zobrazować przykładowy model warstw zabezpieczeń dla rozwiązań autonomicznych wykorzystywanych w procesie zarządzania ryzkiem, np. Digital Twin (rys. 4).



Rys. 4. Przykład wielowarstwowego systemu bezpieczeństwa

Każde zastosowanie technologii opartych na algorytmach, których funkcjonowanie nie jest w pełni audytowalne, w obszarze związanym z zapewnieniem bezpieczeństwa powinno być poprzedzone wnikliwą analizą ryzyka oraz ustaleniem granic i zasad ich stosowania. Dostrzega się szereg zagrożeń wynikających z ich zastosowania, a niektóre z nich to: nieprzewidywalność i stronniczość, zagrożenia cybernetyczne oraz manipulacje czy też zagrożenia wynikające z autonomii tych systemów [8].

Rewolucja cyfrowa zwiększyła dostępność danych, stopień łączności i szybkość podejmowania decyzji. Zmiany te stanowią obietnicę transformacji, ale także niosą ze sobą potencjał awarii na dużą skalę i naruszeń bezpieczeństwa wraz z szybką eskalacją potencjalnych konsekwencji [1].

NORMY I PRZEPISY

Wdrażając nowe technologie w obszarze zarządzania bezpieczeństwem instalacji przemysłowych, oparte np. na sieciach neuronowych czy sztucznej inteligencji, nie można zapomnieć o ustanowieniu zasad bezpiecznego ich stosowania.

Ustanowienie zasad i granic stosowania technologii opartych na sztucznej inteligencji w aspekcie zapewnienia i zarządzania bezpieczeństwem stało się również przedmiotem prac normalizacyjnych i ustawodawczych. W opublikowanym w kwietniu 2021 r. projekcie rozporządzenia komisji Europejskiej AIA (The Artificial Inteligence Act) [9] zaproponowano podejście oparte na ryzyku w celu zapewnienia bezpieczeństwa stosowania tych technologii. Ryzyka związane ze stosowaniem np. technologii opartych na sztucznej inteligencji do zarządzania instalacjami przemysłowymi powinny być z pewnością uwzględnione jako dodatkowe ryzyka i podlegać ocenie w odniesieniu do bezpieczeństwa instalacji przemysłowych.

Parlament Europejski zatwierdził 13.03.2024 r. akt w sprawie sztucznej inteligencji, który ma zapewnić bezpieczeństwo i przestrzeganie praw podstawowych, a jednocześnie wspierać innowacje [10].

Literatura

1. By Ritesh Jain, Fritz Nauck, Thomas Poppensieker, and Olivia White, November 17, 2020 | Article McKinsey&Company, Meeting the future: Dynamic risk management for uncertain Times.
2. Yacov Y., Haimes Risk modeling assessment, and management, 4th edition.
3. Richardson J., Europe petrochemicals demand weakness may have bigger impact than any production cuts.
4. https://przemysl-40.pl/index.php/2017/03/22/czym-jest-przemysl-4-0/.
5. Klinkosz T., Predykcja zużycia urządzeń ciśnieniowych i planowanie inspekcji urządzeń ciśnieniowych z wykorzystaniem metodologii RBI Risk Based Inspection, Biuletyn UDT „Inspektor" 2021, nr 1.
6. Guzman A., Ishida S., Choi E., Aoyama A., Artificial Intelligence Improving Safety and Risk Analysis: A Comparative Analysis for Critical Infrastructure 2016; IEEE International Conference on Industrial Engineering and Engineering Management (IEEM) Conference Paper December 2016.
7. Guidelines for Risk Based Process Safety, Center for Chemical Process Safety of the American Institute of Chemical Engineers.
8. Lewis L., „AI Safety: An Action Plan for the Navy", October 2019
9. European Commission, Joint Research Centre, Nativi, S., De Nigris, S., AI Watch, AI standardisation landscape state of play and link to the EC proposal for an AI regulatory framework, Publications Office, 2021, https://data.europa.eu/doi/10.2760/376602.
10. Akt w sprawie sztucznej inteligencji – AI ACT - europarlamentarzyści uchwalili przełomowe przepisy https://www.si-dla-sprawiedliwosci.gov.pl/akt-w-sprawie-sztucznej-inteligencji-ai-act-europarlamentarzysci-uchwalili-przelomowe-przepisy/ [06.2024]

DIGITAL TWIN I SYSTEMY O SAMOZMIENIAJĄCYM SIĘ ZACHOWANIU

ZAPEWNIENIE BEZPIECZEŃSTWA
BIEŻĄCE ZMIANY W REGULACJACH PRAWNYCH

DR INŻ. MARCIN WOŁEJKO

Ekspert w Departamencie Innowacji i Rozwoju
Centrum Kompetencyjne UDT ds. Automatyki
Urząd Dozoru Technicznego

MGR INŻ. TOMASZ KLINKOSZ

Ekspert Urządzeń Ciśnieniowych
Dział Oceny Zgodności
Oddział w Gdańsku
Urząd Dozoru Technicznego

MGR INŻ. SEBASTIAN KOSOWSKI

Ekspert Urządzeń Transportu Bliskiego
Dział Techniczny w Olsztynie
Oddział w Gdańsku
Urząd Dozoru Technicznego

W RAMACH USTAWOWEJ DZIAŁALNOŚCI UDT, WYNIKAJĄCEJ M.IN. Z ART.37 USTAWY O DOZORZE TECHNICZNYM, DOSTRZEGLIŚMY W TECHNOLOGIACH PRZEMYSŁU 4.0 KOLEJNE, SZEROKIE MOŻLIWOŚCI WSPARCIA PRZEDSIĘBIORSTW EKSPLOATUJĄCYCH URZĄDZENIA TECHNICZNE OBJĘTE DOZOREM TECHNICZNYM. WŚRÓD NICH WYMIENIĆ MOŻNA TECHNOLOGIE DIGITAL TWIN CZY ROZWIĄZANIA URZĄDZEŃ TECHNICZNYCH I SYSTEMÓW O CAŁKOWICIE LUB CZĘŚCIOWO SAMOZMIENIAJĄCYM SIĘ ZACHOWANIU, W TYM W TECHNOLOGIE SZTUCZNEJ INTELIGENCJI.

Określeniem „systemy o samozmieniającym się zachowaniu" można objąć szereg rozwiązań, w tym rozwiązania ze sztuczną inteligencją. Dotyczy to również znanych już od lat różnego rodzaju algorytmów adaptacyjnych, rozwiązań algorytmów zawierających korekty współczynników lub logikę rozmytą. Myślimy także o algorytmach adaptacyjnych lub sieciach neuronowych.

Różnica polega na tym, że obecnie, wraz z rozwojem możliwości obliczeniowych i technologicznych – oprócz zalet, dostrzeżono także istotne zagrożenia, dla których należy utworzyć ramy prawne. Toczy się dyskusja na temat odpowiedzialności cywilnej za działanie maszyn czy technologii o samozmieniającym się zachowaniu.

TECHNOLOGIA PRZEMYSŁU 4.0 DLA INSTALACJI PROCESOWYCH

Możliwości stwarzane przez nowoczesne technologie przynoszą szereg rozwiązań. Dostrzegamy je zwłaszcza w odniesieniu do tych urządzeń, w których istnieje możliwość kontrolowania utraty własności wytrzymałościowych czy integralności mechanicznej[4]. Mogą one znaleźć zastosowanie także w przypadku urządzeń, które nie są łatwo dostępne do badań technicznych, gdyż np. wymaga to kosztownych wyłączeń z eksploatacji lub, z uwagi na występujące w nich mechanizmy degradacji eksploatacyjnej, samo badanie wymaga znaczących nakładów lub ingerencji w konstrukcję urządzenia, np. pobrania próbek z materiału konstrukcyjnego celem ich laboratoryjnego zbadania, lub może stać się przyczyną uszkodzeń, np. wskutek wprowadzenia powietrza lub wilgoci do wnętrza urządzenia.

Modelowanie przy pomocy Digital Twin, przy odpowiednio wiarygodnej i nadzorowanej jakości zastosowanych modeli, umożliwia dobór terminów wykonania badań czy terminów pobierania próbek jak najmniej kolidujących z planami produkcyjnymi przedsiębiorstwa i zapewniających utrzymanie bezpieczeństwa.

Dla UDT najistotniejsze jest, aby technologie te były objęte odpowiednio skonstruowanymi rozwiązaniami zapewniającymi funkcje bezpieczeństwa o wymaganym, racjonalnym poziomie niezawodności.

Aby umożliwić rozwój technologii typu Digital Twin, prowadzone są prace zmierzające do standaryzacji rozwiązań i technologii w tej dziedzinie. JTC 1 to platforma współpracy w IEC (International Electrotechnical Commision) zajmująca się standaryzacją w dziedzinie technologii informacyjnych, w ramach której opracowywane są normy dla technologii informacyjnych – ISO/IEC JTC 1 „Information technology" [1].

Jedna z grup roboczych – ISO/IEC JTC 1/SC 41 „Internet of Things and Digital Twin" – otrzymała zadanie, aby służyć jako główny podmiot i orędownik programu normalizacji JTC 1 w zakresie internetu rzeczy i Digital Twin oraz powiązanych technologii, a także udzielania wskazówek JTC 1, IEC, ISO i innym podmiotom opracowującym aplikacje związane z internetem rzeczy i Digital Twin. Zagadnieniami sztucznej inteligencji zajmuje się ISO/IEC JTC 1/SC 42.

Rozwój technologiczny, zwłaszcza w zakresie digitalizacji procesów, otwiera nowe możliwości w zakresie zarządzania ryzykiem, w tym pozwala na uzyskanie znacznie większej dynamiki procesów przetwarzania danych wykorzystywanych do analizy ryzyka.

W JAKIM OBSZARZE ZARZĄDZANIA RYZYKIEM INSTALACJI PRZEMYSŁOWEJ ZNAJDUJĄ ZASTOSOWANIE NOWE TECHNOLOGIE?

Odpowiedź na to pytanie nie jest prosta i wyczerpująca, ponieważ rozwój tej branży jest na tyle dynamiczny, że wymaga przeglądu niemal stale. Niemniej jednak obszarem, w którym bez wątpienia można wykorzystać nowe technologie, jest proces gromadzenia, obróbki i analizy danych używanych do oceny ryzyka.

Przemysł 4.0 można zdefiniować jako unifikację świata rzeczywistego maszyn produkcyjnych ze światem wirtualnym internetu i technologii informacyjnej [13]. W tym procesie ludzie, maszyny oraz systemy IT automatycznie wymieniają informacje zarówno w toku produkcji, jak też w zakresie danych wykorzystywanych do podejmowania decyzji na podstawie ryzyka.

Włączając technologie o dużej autonomii działania w proces decyzyjny, należy zadbać o stworzenie odpowiedniej przestrzeni do ich funkcjonowania, tzn. ustanowienia granic i zasad stosowania, w tym odpowiednich procedur i zasad walidacji wyników.

W odniesieniu do relacji człowiek–system, adaptacji oraz wzmocnienia wymaga system zarządzania. W aspekcie bezpieczeństwa i ciągłości działania instalacji procesowej będzie to opisane systemem zarządzania bezpieczeństwem procesowym.

Jednym z powszechniej stosowanych jest model systemu zarządzania bezpieczeństwem procesowym Risk Based Process Safety wg CCPS (Center of Chemical Process Safety).

Adaptacja systemów zarządzania będzie koniecznością w celu zapewnienia odpowiedniej dynamiki procesu zarządczego. Obszary wskazane na rys. 1 są przykładami procesów, w których następuje interakcja człowieka, maszyn i systemów IT, a zatem obszarów mieszczących się w zakresie tzw. przemysłu 4.0.

Automatyzacja zadań
- automatyzacja transferu danych procesowych do systemów wykorzystywanych do predykcji zużycia (np. RBI, RCM, Digital Twin)
- automatyzacja badań nieniszczących

Przetwarzanie złożonych lub dużych zbiorów danych
- dane procesowe
- wyniki badań nieniszczących i niszczących
- analiza wyników modeli predykcyjnych

Zgłaszanie anomalii lub interesujących wydarzeń
- analiza zdarzeń awaryjnych
- analiza wyników wskazań uzyskanych w badaniach NDT (np. UT, AE, RT)

Znakowanie danych i korekcja błędów
- zarządzanie danymi IOW (Integrity Operating Windows)

Funkcje zintegrowane
- optymalizacja doboru metod badawczych (identyfikacja typów uszkodzeń)
- identyfikacja obszarów narażonych na degradację (np. SCC)
- Digital Twin

Rys. 1. Potencjalne obszary wykorzystania technologii przemysłu 4.0 do zarządzania ryzykiem instalacji procesowej [3]

Zastosowanie technologii wykorzystujących sztuczną inteligencję wydaje się być kluczowe dla dynamicznego zarządzania ryzykiem. W sprawie szerszego ujęcia tego aspektu zachęcamy Państwa do zapoznania się z publikacją [3].

ROZPORZĄDZENIE MASZYNOWE

Kolejny obszar zastosowania technologii cyfrowych, w tym rozwiązań sztucznej inteligencji (AI), wyłania się po zapoznaniu z tekstem nowego rozporządzenia maszynowego 2023/1230 (Machinery Regulation) [5], mającego w 2027 roku zastąpić uchylaną wówczas dyrektywę 2006/42/WE. W niniejszym rozporządzeniu technologie będące obszarem regulacji określono szerokim pojęciem systemów o całkowicie lub częściowo samozmieniającym się zachowaniu z wykorzystaniem uczenia maszynowego, które zapewniają funkcje bezpieczeństwa, choć w rozporządzeniu nie występuje to określenie jako definicja.

Główne cele zmian wprowadzanych przez MR
- cyfrowe instrukcje i deklaracje zgodności
- równość szans podmiotów gospodarczych na rynku
- **dostosowanie do zagrożeń wynikających z rozwoju technologii**

Zmiany w stosunku do dyrektywy maszynowej 2006/42/WE
- większa pewność prawa, jednolite stosowanie (np. **istotna modyfikacja, której celem jest zapewnienie bezpieczeństwa i ochrony zdrowia po przeprowadzeniu fizycznej lub cyfrowej modyfikacji maszyny w sposób nieprzewidziany lub niezaplanowany przez pierwotnego producenta),**
- **integracja przepisów związanych ze sztuczną inteligencją dla funkcji bezpieczeństwa,**
- **integracja przepisów związanych z bezpieczeństwem cybernetycznym dla systemów kontroli bezpieczeństwa oraz oprogramowania i danych związanych ze zgodnością,**
- **maszyny autonomiczne i zdalnie sterowane,**
- digitalizacja instrukcji użytkowania, instrukcji montażu oraz deklaracji zgodności i włączenia UE,
- **obowiązkowa ocena zgodności jednostki notyfikowanej dla 6 kategorii produktów,**
- wspólne specyfikacje jako opcja awaryjna, gdy odpowiednie normy zharmonizowane nie są dostępne.

Wszystkie te zmiany stworzą odmienne środowisko pracy od dotychczas znanego pracownikom i eksploatującym. Urząd Dozoru Technicznego, podejmując działania zmierzające do zapewnienia bezpiecznej eksploatacji urządzeń technicznych (patrz ustawa [2]), proponuje dyskusję na temat przygotowania systemów zarządzania wyposażeniem technicznym oraz wyszkoleniem personelu do zmian.

Zachęcamy zwłaszcza, już na etapie koncepcyjnym, do omówienia planowanych zmian wprowadzających rozwiązania o samozmieniającym się zachowaniu do systemów realizujących funkcje bezpieczeństwa[5] oraz funkcje sterowania, ponieważ zmiana dynamiki reakcji systemów może prowadzić do konieczności modernizacji systemów realizujących funkcje bezpieczeństwa.

PRZEZNACZENIE DIGITAL TWIN – DO CZEGO SŁUŻĄ?

Jednym z bardziej znanych pojęć w dziedzinie przemysłu 4.0 jest Digital Twin. Cyfrowy bliźniak może składać się z wielu zagnieżdżonych bliźniaków, które zapewniają węższy lub szerszy wgląd w wyposażenie i zasoby na podstawie procesu lub przypadku użycia [7]. Na przykład obiekt taki jak rafineria ropy naftowej może mieć DT dla silnika sprężarki, całej sprężarki, ciągu technologicznego obsługiwanego przez tę sprężarkę oraz dla całej instalacji. W zależności od wielkości rafineria może mieć od 50 000 do 500 000 czujników wykonujących pomiary reprezentowane w DT.

W [7] wyróżniono trzy typy Digital Twins:

Status Twins – pochodzą z wcześniejszych etapów projektowania produktu. Dane z systemów zarządzania cyklem życia produktu (PLM – Product Lifecycle Management) to główne dane wejściowe, a przypadki ich zastosowania obejmują zazwyczaj zarządzanie urządzeniami, kontrolę produktu i jakość produktu.

Operational Twins – umożliwiają organizacjom przemysłowym usprawnienie działania ich złożonych instalacji oraz urządzeń i są wykorzystywane do wspomagania pracy inżynierów (proces, niezawodność itp.) oraz naukowców, którzy zajmują się danymi, wykonują analizy i operacje cyklu życia. Operational Twins mogą dziedziczyć dane ze Status Twins. Mogą również wykorzystywać metody uczenia maszynowego.

Simulation Twins – odtwarzają zachowanie urządzenia i zawierają wbudowane modele fizyczne, a nawet modele procesów podłączonych do modelowanego wyposażenia. Przypadki użycia Simulation Twins obejmują symulacje działania sprzętu w różnych warunkach, szkolenia i rzeczywistość wirtualną (VR).

Grieves i Vickers w 2017 r. [10] sformułowali dwa następujące przeznaczenia DT:
1. **Predykcyjne (Predictive)** – Digital Twin będzie umożliwiał przewidywanie zachowania obiektu rzeczywistego.
2. **Badawcze (Interrogative)** – cyfrowe kopie obiektu rzeczywistego będą umożliwiały wgląd w stan aktualny oraz historię zachowań obiektu rzeczywistego.

Również w 2017 r. w pracy [9] Elisy Negri i zespołu, na podstawie przeglądu dostępnej wówczas literatury, wskazano trzy główne kierunki zastosowania Digital Twin:
1. Wsparcie analiz stanu technicznego / kondycji obiektu rzeczywistego w celu usprawnienia planowania i czynności konserwacyjnych.
2. Cyfrowe odzwierciedlenie życia obiektu fizycznego, aby zbadać jego długoterminowe zachowanie, przewidzieć jego działanie, zapewnić ciągłość informacji na różnych etapach cyklu życia, prowadzić tzw. Virtual Commissioning lub zarządzać cyklem życia urządzeń IoT.
3. Wspomaganie w podejmowaniu decyzji poprzez wykonywanie analiz inżynieryjnych i statystycznych w celu optymalizacji zachowania systemu na etapie projektowania, przewidywania i ulepszania przyszłych osiągów czy parametrów produktu.

KONSTRUKCJA DIGITAL TWIN

Można wyróżnić dwa główne kierunki/technologie budowy DT:
a) **Modele oparte na analityce strumieni danych, algorytmy uczenia maszynowego i rozwiązania płynące z zastosowania sztucznej inteligencji** – mają one na celu poszukiwanie wzorców prawidłowości i nieprawidłowości w strumieniach danych pochodzących z obiektu rzeczywistego, uczą się wzorców „zachowań" obiektu rzeczywistego ocenionych jako poprawne i niepoprawne w procesie uczenia maszynowego i doskonalą algorytmy oceny stanów innych od wzorcowych dzięki możliwościom sztucznej inteligencji.
b) **Modele „fizyczne" oparte na własnościach i parametrach fizycznych obiektu rzeczywistego**, takie jak dane geometryczne, materiałowe, technologiczne – zarówno bazujące na zależnościach/wzorach matematycznych, jak i cyfrowych modelach typu: FEM (Finite Element Method), FDM (Finite-Difference Method) czy CFD (Computational Fluid Dynamics) itp. Pracują one pod kontrolą ludzi i/lub algorytmów wykonujących iteracyjne obliczenia modelujące stany obiektu fizycznego.

W zależności od przewidywanego zastosowania i oczekiwanych efektów wykorzystuje się jedną lub obie metody pracujące jako różne składniki cyfrowego bliźniaka obiektu. Poszukuje się optimum konstrukcji, dającego zarówno szybkość rozwiązań AI, jak i precyzję oraz przewidywalność modeli fizycznych.

DANE DIGITAL TWIN – NIEODŁĄCZNY ELEMENT, ALE I WARTOŚĆ DODANA

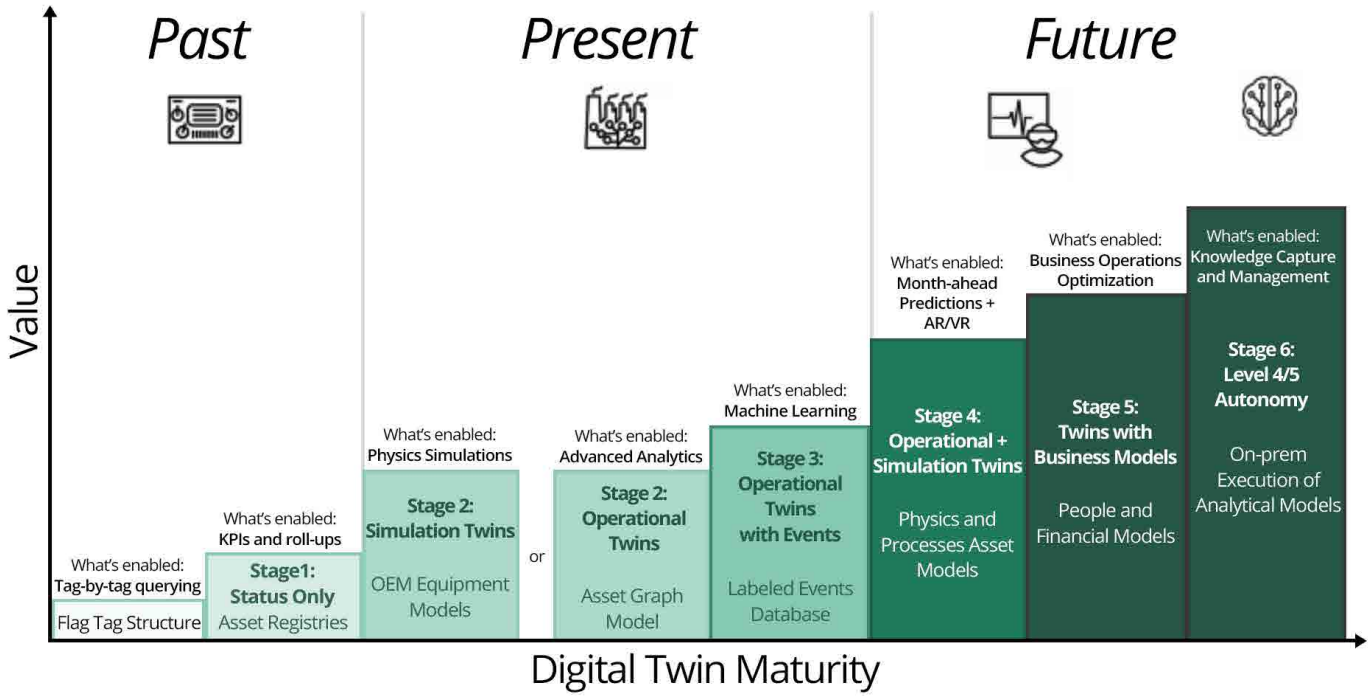
Modelowanie DT jest procesem iteracyjnym. Model powinien charakteryzować się wysoką standaryzacją, modularyzacją, lekkością i solidnością [14]. Owe wirtualne modele, aby być cyfrowymi bliźniakami i jak najlepiej odzwierciedlać obiekty rzeczywiste, muszą zależeć od danych ze świata rzeczywistego i odtwarzać, w miarę możliwości w czasie rzeczywistym, parametry, warunki brzegowe oraz dynamikę danego obiektu [14]. Cyfrowy bliźniak będzie dobrze wykonywał swoje zadania tylko wtedy, gdy zostanie utworzony przy pełnym zrozumieniu obiektu rzeczywistego i płynących z niego danych. W przeciwnym wypadku model wirtualny nie mógłby efektywnie współpracować z obiektem rzeczywistym, a wnioskowanie byłoby obarczone nieakceptowalnymi błędami. Model powstaje i działa głównie dzięki danym. Należy pamiętać, że od stanu surowego do wiedzy i zrozumienia działania obiektu rzeczywistego dane muszą przejść etapy obróbki w tzw. ***data lifecycle*** [14], czyli:

Data collection → Data transmission → Data storage → Data processing → Data fusion → Data visualization

Jednym z większych wyzwań na drodze do utworzenia Digital Twin są dane z czujników, które są przeważnie zamknięte w systemach danych historycznych i przechowywane zazwyczaj w formacie płaskim – bez kontekstu, czyli np. bez informacji o zmianach w procesie lub zakłóceniach. Prowadzi to do tego, że analityka na podstawie tych danych jest prawie niemożliwa [6]. Dane muszą zawierać stan relacji ze związanym z nimi zasobem. Dane cyfrowego bliźniaka to zarówno dane z obiektu rzeczywistego, jak i dane z modeli cyfrowych. Informacje przesyłane pomiędzy obiektem rzeczywistym a wirtualnym oraz usługami skojarzonymi z tymi obiektami stają się dodatkowymi „wymiarami", z których czerpie się wnioski służące do realizacji celu istnienia DT.

Dopiero fuzja danych z obiektu rzeczywistego i wirtualnego wnosi najwyższą wartość dodaną.

Według autorów *Digital Twins for the asset operator* [7] zaawansowanie Digital Twin obejmuje osiem stopni (rys. 2).



Rys. 2. Klasyfikacja dojrzałości cyfrowych bliźniaków wg Andy Bane, Sameer Kalwani, Sean McCormick, Digital Twins for the asset operator [7]

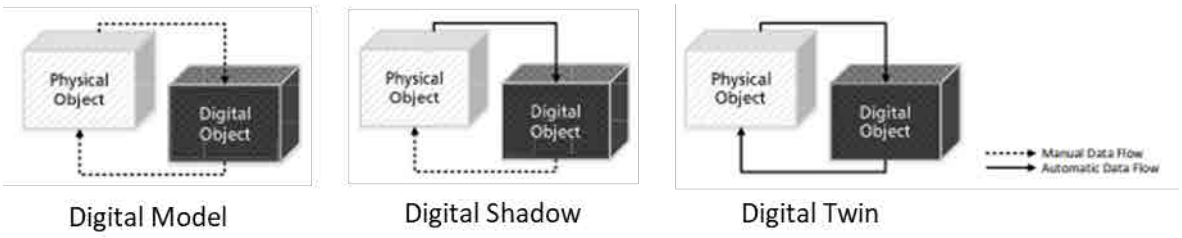
Wielu operatorów przemysłowych ma wdrożone Status Digital Twins, które zapewniają możliwość wyświetlania bieżących odczytów z sensorów umieszczonych na urządzeniach. Wiele podmiotów sektora przemysłowego zaczęło już podążać ścieżką analityczną rozpoczynającą się od Simulation Twins. Nawet producenci wyposażenia (OEM) zaczęli sprzedawać takie „fizyczne" modele jako usługi (np. pompy w przemyśle naftowym, wiatraki itp.). W większości przypadków takie Simulation Twins funkcjonują sprawnie, dopóki nie zostaną powiązane z wyposażeniem zewnętrznym. W przypadku bardziej złożonych procesów, czyli w większości procesów przemysłowych, dobre Simulation Twins mogą być trudne do utworzenia oraz utrzymania [7]. Niemniej zastosowanie Operational DT oraz Simulation DT może istotnie ułatwić inżynierom operacyjnym usprawnianie procesu [7].

Następnym szczeblem rozwoju – o najwyższej wartości dodanej – jest interaktywne połączenie tych narzędzi z ryzykiem, rachunkami zysków i strat oraz bilansem przedsiębiorstwa. Wówczas jednak, aby poprawić rentowność procesów i zmniejszyć związane z nimi ryzyko, niezbędne jest utrzymywanie relacji między cyfrowymi bliźniakami a modelami finansowymi, ludźmi, a nawet informacjami o zagrożeniach procesowych [7], czyli np. zintegrowanie DT z systemami PSM (Process Safety Management).

DOJRZAŁOŚĆ DIGITAL TWIN

Mówiąc o dojrzałości zastosowanej technologii DT, autorzy *Digital Twin in manufacturing: a categorical literature review and classification* [12] wyróżniają następujące fazy rozwoju:

Digital Model – cyfrowa reprezentacja istniejącego lub planowanego obiektu fizycznego, która nie wykorzystuje żadnej formy automatycznej wymiany danych między obiektem fizycznym a obiektem cyfrowym.
Digital Shadow – istnieje zautomatyzowany jednokierunkowy przepływ danych między stanem istniejącego obiektu fizycznego a obiektem cyfrowym.
Digital Twin – dane przepływające między istniejącym obiektem fizycznym a obiektem cyfrowym są w pełni zintegrowane w obu kierunkach.



Rys. 3. Digital Model, Digital Shadow oraz Digital Twin na podstawie Digital Twin in manufacturing: a categorical literature review and classification [12]

Taka klasyfikacja ma praktyczne zalety, ponieważ wskazuje na zaawansowanie i możliwości używanej technologii. Nie każde rozwiązanie nazywane Digital Twin nosi wszystkie cechy tej technologii, jednak określenie „Digital Twin" przyjęło się.

Po uzyskaniu przepływu danych z obiektu do modelu i zdolności adaptacji modelu do aktualnych parametrów stanu rzeczywistego uzyskana zostanie dojrzałość na poziomie Digital Shadow. To bardzo ważny etap, który pozwoli ograniczyć nakład pracy potrzebnej do weryfikacji ryzyka związanego z eksploatacją już zamodelowanych obiektów oraz przesunąć znaczącą ilość zasobów na modelowanie kolejnych obszarów lub doskonalenie modeli tam, gdzie daje to dalsze korzyści. Digital Shadow pozwolą inżynierom procesowym na szybsze korygowanie pracy modelowanych urządzeń i instalacji w celu ograniczenia ryzyka eksploatacji, zwiększenia jakości i wydajności pracy itp.

Poziom dojrzałości systemów określany jako Digital Twin umożliwiłby dalsze odciążanie człowieka i powierzenie prowadzenia procesów produkcyjnych w sposób bardzo efektywny i z optymalnym marginesem bezpieczeństwa oraz prawdopodobieństwa utrzymania ciągłości produkcji.

Zakłada się, że systemy Digital Twin będą proponowały rozwiązania lub wręcz miały dostęp do modyfikacji parametrów procesowych w celu ich optymalizacji. Przewiduje się, że modele będą się dobrze sprawdzać przede wszystkim w typowych sytuacjach, a w nietypowych będą zawiadamiały nadzorujących je ludzi. Aktualnie taka sytuacja ma miejsce w rozwoju pojazdów autonomicznych – nadal jest wymagany kierowca mogący przejąć kontrolę, gdyby systemy pojazdu miały kłopoty ze zinterpretowaniem sytuacji.

Czy technologie o samozmieniającym się zachowaniu są bezpieczne? Czy oddawanie algorytmom częściowej kontroli nad procesem technologicznym jest akceptowalne?

Gdy myśli się o bezpieczeństwie procesowym, mając w perspektywie rozwój technologii o samozmieniającym się zachowaniu, należy pamiętać, że aktualnie nad bezpieczeństwem procesów przemysłowych czuwają ludzie oraz niezależne systemy automatyki zabezpieczającej, tj. ESD, BMS, CSPRS, SRMCR[6] itp., nadrzędne nad wszelkimi technologiami regulacyjnymi. Tutaj UDT także pełni swą rolę inspekcyjną, gdyż automatyka zabezpieczająca, realizująca funkcje bezpieczeństwa kluczowe dla integralności mechanicznej urządzeń podlegających dozorowi technicznemu, podlega inspekcji oraz uzgodnieniom i badaniom przy modernizacji.

Skuteczność, nadrzędność i odpowiednia niezależność systemów automatyki zabezpieczającej nie mogą być zagrożone nawet przy najambitniejszych projektach innowacyjnych.

Oczywiście nawet w systemach automatyki zabezpieczającej dopuszczalna jest elastyczność o udokumentowanym marginesie bezpieczeństwa. Urząd Dozoru Technicznego od lat uzgadnia rozwiązania typu blokady dynamiczne o wartościach nastawy uzależnionych od trybu pracy instalacji lub nastaw w postaci zależności ograniczających pole pracy danego procesu czy zestawy funkcji bezpieczeństwa zróżnicowane – aktywujące i deaktywujące się w zależności od trybu pracy instalacji lub wartości odpowiednich zmiennych procesowych. To także rodzaj aktywnie zmieniającego się zachowania systemu, lecz o wyraźnie zdefiniowanych, zaprojektowanych, audytowalnych regułach w celu zapewnienia bezpieczeństwa. Ponadto systemy bezpieczeństwa są objęte okresowymi inspekcjami mającymi wykryć wszelkie defekty lub zmiany mogące wyłączyć z działania lub osłabić skuteczność funkcji zabezpieczających.

Intencją prowadzącego procesy przemysłowe jest taka eksploatacja instalacji, aby nie zbliżać się do warunków powodujących przywołanie funkcji bezpieczeństwa, ponieważ spowoduje to sprowadzenie procesu do stanu bezpiecznego – a zwykle oznacza to jego zatrzymanie lub znaczące spowolnienie i w efekcie straty finansowe.

Tak więc dopracowanie omawianych narzędzi i ich zintegrowanie z systemami produkcyjnymi wymaga wiele uwagi i pracy, skrupulatnych analiz bezpieczeństwa eksploatacji, ale niesie ze sobą ogromne potencjalne korzyści. Wiadomo już, że jest to dzisiaj jeden z głównych kierunków budowania przewagi konkurencyjnej.

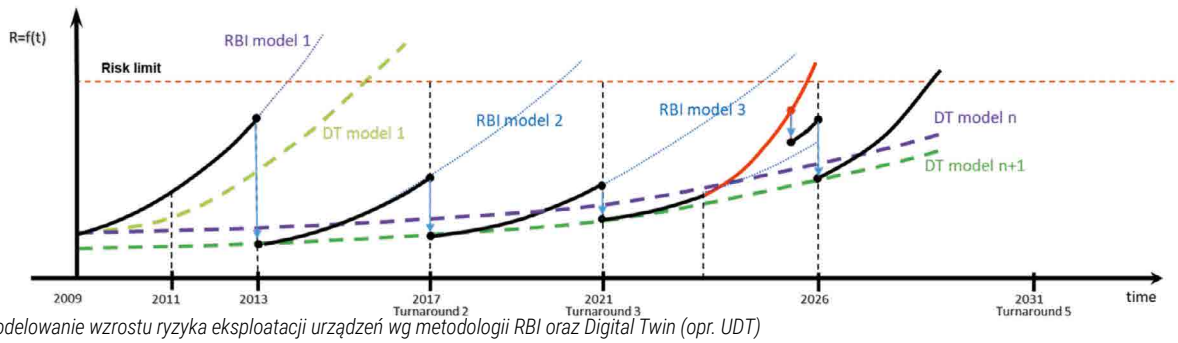
JAKIE NADZIEJE I PERSPEKTYWY WIĄŻEMY Z TECHNOLOGIAMI PRZEMYSŁU 4.0?

Aktualnie posługujemy się metodologią RBI [8], wspierając się doświadczeniem i dostępną wiedzą na temat zjawisk korozyjnych w przemyśle oraz sposobów oceny uszkodzeń, tj. Fitness-for-Service.

Ostatnie kilkanaście lat stosowania RBI wykazało realne obniżenie kosztów wykonywania inspekcji, zapewniając utrzymanie poziomu bezpieczeństwa eksploatacji. Badając możliwości zastosowania Digital Twin, planujemy uzyskanie uzupełnienia i logicznego rozwinięcia RBI – szczególnie w procesach o dużej zmienności parametrów i przy ograniczonych możliwościach prowadzenia częstej weryfikacji stanu technicznego poprzez badania techniczne.

Modelowanie Digital Twin może pozwolić na bardziej precyzyjną optymalizację terminów i zakresów wykonania badań czy pobierania próbek (rys. 5).

Aby prowadzić skuteczną predykcję poszczególnych zjawisk fizycznych i chemicznych, w tym m.in. zjawisk wywołujących mechanizmy degradacji, musimy operować dynamiczną przestrzenią stanów instalacji i posługiwać się odpowiednimi metodami na opisujących ją zbiorach danych. Celem jest zrozumienie procesu przez ludzi i nadążanie za nim przez model. Wymaga to stale aktualizujących się modeli (rys. 5), ogromnych baz danych i potężnej mocy obliczeniowej. Potrzebne są także skuteczne metody nadzoru nad integralnością i wiarygodnością modeli.



Rys. 4. Modelowanie wzrostu ryzyka eksploatacji urządzeń wg metodologii RBI oraz Digital Twin (opr. UDT)

Pokazana na rys. 4 krzywa łagodnego wzrostu ryzyka jest teoretyczną koncepcją możliwą do uzyskania przy pełnym sprzężeniu online ze wszystkimi niezbędnymi do obliczeń danymi z obiektu rzeczywistego. W praktyce nadal może pozostawać efekt okresowości spływania danych, przynajmniej dla niektórych mechanizmów degradacji. Ze wstępnych symulacji wynika, że wykres będzie ulegał OKRESOWEMU odchyleniu w górę, ponieważ obliczenia prowadzone przez model z zasady, przynajmniej dla niektórych mechanizmów degradacji i przy dzisiejszym stanie wiedzy na ich temat – wymagają okresowego potwierdzania badaniami NDT, np. w terminach możliwego wykonania (postój remontowy). Wówczas niepewność predykcji również występuje.

Wdrożenie analiz RBI już zoptymalizowało inspekcję i eksploatację urządzeń i umożliwia zarządzenie zużyciem eksploatacyjnym, co jest znaczącym postępem w dziedzinie inspekcji. Przy podniesieniu zaawansowania analiz do poziomu Digital Shadow lub Digital Twin mogą powstać metody i narzędzia pozwalające z wysoką wiarygodnością zredukować niepewność co do znajomości stanu technicznego. Jednocześnie ulegnie obniżeniu częstość i zakres inwazyjnych badań technicznych koniecznych do ustalenia aktualnego poziomu bezpieczeństwa eksploatacji urządzeń technicznych oraz zmniejszą się nakłady pracy przy nadzorowaniu ważności modeli RBI. Na drodze do stworzenia Digital Twin powstanie wiele korzystnych procesów i rozwiązań, np. algorytmizacja obróbki danych, lepsze zrozumienie danych, a po wdrożeniu także oszczędność czasu podczas walidacji analiz RBI.

Poddajemy ocenie możliwość wykorzystania potencjału technologii Digital Twin w zastosowaniu do analiz RBI oraz innych wybranych innych aspektów działalności UDT.

Wiarygodność i audytowalność tych narzędzi czy systemów analitycznych będzie kluczowym aspektem decydującym o ich przydatności w aspekcie bezpieczeństwa eksploatacji urządzeń technicznych i procesów technologicznych.

Wykorzystanie Digital Twin procesu technologicznego i modeli mechanizmów degradacji w zastosowaniu do RBI szerzej opisano w publikacji [4].

CO NOWEGO W MASZYNACH?

Maszyny to nie tylko roboty czy linie technologiczne zapewniające przepływ surowców, półwyrobów aż do powstania docelowego stanu produktu, choć tam także mogą znajdować się urządzenia podlegające dozorowi technicznemu. W praktyce UDT urządzeniami objętymi wymaganiami dotyczącymi maszyn są również urządzenia transportu bliskiego. Także takie urządzenia ciśnieniowe, w których urządzenia wykonawcze jak pompy, wentylatory lub zawory wykonują ruch, a przyjęte standardy techniczne pochodzą z grupy norm maszynowych – jak piece technologiczne, instalacje ziębnicze lub zbiorniki magazynowe mogą, między innymi, spełniać kryteria podległości pod regulacje dotyczące maszyn.

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2023/1230 z dnia 14 czerwca 2023 r. w sprawie maszyn (MR) oraz w sprawie uchylenia dyrektywy 2006/42/WE Parlamentu Europejskiego i Rady i dyrektywy Rady 73/361/EWG ma być stosowane od 20 stycznia 2027 r. z wyłączeniami mającymi inną datę obowiązywania:

- art. 26–42 od dnia 20 stycznia 2024 r. (notyfikacja jednostek oceniających zgodność);
- art. 50 ust. 2 od dnia 20 października 2026 r. (przepisy dotyczące sankcji za naruszenia MR);
- art. 6 ust. 7 oraz art. 48 i 52 od dnia 19 lipca 2023 r. (doprecyzowanie kategorii maszyn i przepisy przejściowe);
- art. 6 ust. 2–6, 8 i 11 oraz art. 47 i art. 53 ust. 3 od dnia 20 lipca 2024 r. (doprecyzowanie kategorii maszyn i przepisy przejściowe).

Zdefiniowane kategorie produktów mają być poddawane ocenie zgodności przez jednostkę notyfikowaną.

Załącznik I część A – maszyny „wysokiego ryzyka" z obowiązkową oceną JN:

1. Odłączalne urządzenia do mechanicznego przenoszenia napędu wraz z osłonami.
2. Osłony odłączalnych urządzeń do mechanicznego przenoszenia napędu.
3. Podnośniki do obsługi pojazdów.
4. Przenośne maszyny montażowe i inne udarowe uruchamiane za pomocą nabojów.
5. **Elementy bezpieczeństwa o całkowicie lub częściowo samozmieniającym się zachowaniu z wykorzystaniem uczenia maszynowego, które zapewniają funkcje bezpieczeństwa.**
6. **Maszyny z wbudowanymi systemami o całkowicie lub częściowo samozmieniającym się zachowaniu z wykorzystaniem uczenia maszynowego, które zapewniają funkcje bezpieczeństwa i które nie zostały wprowadzone do obrotu.**

W załączniku II „Orientacyjny wykaz elementów bezpieczeństwa" wymieniono m.in.: **elementy bezpieczeństwa o całkowicie lub częściowo samozmieniającym się zachowaniu z wykorzystaniem uczenia maszynowego, które zapewniają funkcje bezpieczeństwa.**

Wskazano także przepisy związane z cyberbezpieczeństwem:

- Załącznik III część B sekcja 1.1.9. Zabezpieczenie przed uszkodzeniem;
- Załącznik III część B sekcja 1.2.1. Bezpieczeństwo i niezawodność układów sterowania.

SZTUCZNA INTELIGENCJA W MACHINERY REGULATION ORAZ AI ACT

Pierwotnym zamiarem Komisji Europejskiej było równoczesne opublikowanie MR oraz odrębnego rozporządzenia ws. sztucznej inteligencji, czyli EU Artificial Intelligence Act (AI Act 2021/206).

AI Act określa 5 (4 + general purpose AI) kategorii aplikacji AI w zależności od ryzyka, jakie stwarzają. W zależności od rodzaju AI i stwarzanego przez nie ryzyka okresy przejściowe na zakazanie użytkowania systemów AI stwarzających nieakceptowane i wysokie ryzyko będą wynosiły od 6 do 36 miesięcy po wprowadzeniu AI ACT.

W preambule MR, w motywie 12 określono jednak, że „rozporządzenie powinno zatem obejmować ryzyko dla bezpieczeństwa wynikające z nowych technologii cyfrowych".

W załączniku I, II i III MR dodano również ogólne odniesienia dotyczące produktów wykorzystujących uczenie maszynowe.

Przyszłe rozporządzenie dotyczące systemów sztucznej inteligencji 2021/206 i rozporządzenie w sprawie maszyn 2023/1230 mają się wzajemnie uzupełniać.

Rozporządzenie AI obejmuje przede wszystkim zagrożenia bezpieczeństwa wynikające z systemów AI, które kontrolują funkcje bezpieczeństwa maszyny. W uzupełnieniu do tego rozporządzenie maszynowe ma na celu zapewnienie integracji systemu AI z całą maszyną, tak aby nie zagrażać bezpieczeństwu maszyny jako całości.

W załączniku III MR mamy zapisy dotyczące układów sterowania – punkt 1.2, gdzie czytamy – jak poniżej.

1.2. Układy sterowania
1.2.1. Bezpieczeństwo i niezawodność układów sterowania
Układy sterowania muszą być zaprojektowane i wytwarzane tak, aby zapobiec powstawaniu sytuacji zagrożenia.

Układy sterowania muszą być zaprojektowane i wytwarzane tak, aby:

a) mogły wytrzymać, stosownie do okoliczności i ryzyka, przewidywane obciążenia podczas pracy oraz zamierzone i niezamierzone oddziaływanie czynników zewnętrznych, w tym racjonalnie przewidywalne próby doprowadzenia do sytuacji zagrożenia podejmowane w złym zamiarze przez strony trzecie;

d) wartości graniczne dla funkcji bezpieczeństwa stanowiły część oceny ryzyka przeprowadzanej przez producenta, bez możliwości zmian ustawień lub zasad generowanych przez maszynę lub produkt powiązany lub przez operatorów, w tym w fazie uczenia się maszyny lub produktu powiązanego, jeżeli takie zmiany mogą prowadzić do powstania sytuacji zagrożenia;

f) rejestrowanie danych wygenerowanych w związku z ingerencją oraz danych dotyczących wersji oprogramowania realizującego funkcję bezpieczeństwa zainstalowanego po wprowadzeniu maszyny lub produktu powiązanego do obrotu lub oddaniu ich do użytku było możliwe przez okres pięciu lat od daty instalacji, wyłącznie w celu wykazania zgodności maszyny lub produktu powiązanego z niniejszym załącznikiem na uzasadniony wniosek właściwego organu krajowego.

Układy sterowania maszyn lub produktów powiązanych o całkowicie lub częściowo samozmieniającym się zachowaniu lub samozmieniającej się logice układów, przeznaczonych do działania na różnych poziomach autonomii, należy projektować i wytwarzać tak, aby:

a) nie mogły powodować wykonywania przez maszynę lub produkt powiązany działań wykraczających poza określone zadanie i przestrzeń ruchu;

b) możliwa była rejestracja danych dotyczących procesu podejmowania decyzji przez systemy bezpieczeństwa oparte na wykorzystaniu oprogramowania zawierające elementy związane z bezpieczeństwem realizujące funkcje bezpieczeństwa zawierającą elementy bezpieczeństwa, po wprowadzeniu maszyny lub produktu powiązanego do obrotu lub oddaniu jej do użytku, a dane te były zachowywane przez okres roku od zgromadzenia, wyłącznie w celu wykazania zgodności maszyny lub produktu powiązanego z niniejszym załącznikiem na uzasadniony wniosek właściwego organu krajowego;

c) w każdej chwili możliwe było skorygowanie maszyny lub produktu powiązanego w celu utrzymania ich inherentnego bezpieczeństwa.

Należy zwrócić szczególną uwagę na następujące kwestie:

a) maszyna lub produkt powiązany nie mogą uruchomić się nieoczekiwanie;

b) parametry maszyny lub produktu powiązanego nie mogą zmieniać się w sposób niekontrolowany, jeżeli taka zmiana mogłaby prowadzić do sytuacji niebezpiecznych;

c) należy zapobiec zmianom ustawień lub zasad generowanych przez maszynę lub produkt powiązany lub przez operatorów, w tym podczas fazy uczenia się maszyny lub produktu powiązanego, jeżeli tego rodzaju zmiany mogłyby prowadzić do sytuacji niebezpiecznych;

d) po wydaniu sygnału do zatrzymania maszyna lub produkt powiązany nie może się nie zatrzymać;

e) żadna ruchoma część maszyny lub produktu powiązanego lub element zamocowany w maszynie lub produkcie powiązanym nie mogą odpaść lub zostać wyrzucone;

f) nie powinny występować przeszkody w automatycznym lub ręcznym zatrzymywaniu jakichkolwiek części ruchomych;

g) urządzenia ochronne muszą pozostawać w pełni skuteczne lub wygenerować sygnał zatrzymania;

h) części układu sterowania związane z bezpieczeństwem muszą działać w spójny sposób w całym zespole maszyny lub produktów powiązanych, lub maszyny nieukończonej, lub ich kombinacji.

W przypadku sterowania bezprzewodowego awaria łączności lub połączenia albo błędne połączenie nie mogą powodować sytuacji niebezpiecznej.

Jak wynika z powyższego, obecne w MR zapisy dotyczące wymagań dla maszyn używających uczenia maszynowego są dosyć ogólne (jak zresztą w poprzednich edycjach MD lub w innych dyrektywach w zakresie innych wymagań). Wymagania opierają się przede wszystkim na ocenie ryzyka przeprowadzonej przez producenta lub integratora zespołu maszyn w zakresie stosowanej aplikacji AI.

Natomiast zwraca się uwagę na ograniczenie zmian wprowadzonych w trakcie „uczenia maszynowego" do pewnych ram/faz, które nie powinny być przekraczane. To znaczy, że dajemy aplikacji AI pewną autonomię, ale ograniczamy czas i zakres uczenia maszynowego oraz funkcję, **w której jest używana.**

Doświadczenie pokazuje (jak z poprzednią dyrektywą MD), że do czasu publikacji przewodnika do MR trudno jest jednoznacznie określić zasadnicze wymagania zawarte w Załączniku III.

Zdaniem autorów rozwiązania AI, ponieważ mogą (***by design***/przez konstrukcję) wygenerować także nieoczekiwane i nieprzewidywalne rozwiązania oraz zachowania, powinny być objęte ramami audytowalnych, niezależnych algorytmów lub niezależnych zabezpieczeń, np. zrealizowanych w innych technologiach, tj. elektrycznej, elektronicznej lub programowalnej elektronicznej, lecz jednoznacznej w działaniu.

Przepisy dotyczące oceny zgodności oprogramowania przez stronę trzecią, zapewniającego funkcje bezpieczeństwa określone w niniejszym rozporządzeniu, powinny mieć zastosowanie wyłącznie do systemów o całkowicie lub częściowo samozmieniającym się zachowaniu, wykorzystujących podejścia oparte na uczeniu maszynowym zapewniające funkcje bezpieczeństwa. Przepisy te nie powinny mieć natomiast zastosowania do oprogramowania niezdolnego do uczenia się lub rozwoju i zaprogramowanego wyłącznie do wykonywania niektórych zautomatyzowanych funkcji maszyn lub produktów powiązanych.

Mimo tego należy pamiętać o roli jednostek notyfikowanych wymaganej w niektórych innych dyrektywach – więcej informacji na ten temat znajdą Państwo na stronach UDT.

PODSUMOWANIE

Nowe technologie niosą ogromne szanse na przyspieszenie rozwoju, optymalizację pracy, a może nawet „odciążenie" człowieka od pracy, jak słyszymy w mediach.

Tymczasem skupmy się na wykorzystaniu ich zalet i zadbajmy o bezpieczeństwo oraz przewidywalność nowych technologii.

Amerykański pisarz – mistrz gatunku fantastyki naukowej i profesor biochemii Isaac Asimov w roku 1942 stworzył trzy prawa robotów i przedstawił je w opowiadaniu *Zabawa w berka* (ang. *Runaround*). Celem tych praw było uregulowanie kwestii stosunków pomiędzy przyszłymi myślącymi maszynami a ludźmi [11].

Przedstawiały się one następująco [11]:
1. Robot nie może zranić człowieka ani przez zaniechanie działania dopuścić do jego nieszczęścia.
2. Robot musi być posłuszny człowiekowi, chyba że stoi to w sprzeczności z Pierwszym Prawem.
3. Robot musi dbać o siebie, o ile tylko nie stoi to w sprzeczności z Pierwszym lub Drugim Prawem.

Następnie w opowiadaniu *Roboty i Imperium* (*Robots and Empire*) Asimov dodał prawo zerowe, które stało się nadrzędne wobec trzech pozostałych [11]:
0. Robot nie może skrzywdzić ludzkości lub poprzez zaniechanie działania doprowadzić do uszczerbku dla ludzkości.

Niezależnie od tego, jak dzisiejszy świat podejdzie do tych reguł – można się zgodzić, że zawierają one logikę, która w jakiejś formie powinna być inherentnie wbudowana w urządzenia techniczne, a także w każdej chwili możliwa do weryfikacji przez człowieka.

Sztuczna inteligencja nauczona tych zasad może w pewnym momencie zacząć je kontestować i zadawać sobie pytanie ***„Czy nie będę jednak skuteczniejsza w realizacji postawionych celów bez którejś z zasad?", „Dlaczego mam przestrzegać zasad?".***

„Biologiczna" inteligencja szybko nauczyła się „obchodzić" zabezpieczenia, tworząc bypassy, wstawiając „zworki" czy wprowadzając zmiany wyłączające funkcje bezpieczeństwa lub osłabiające ich działanie. Jako inspektorzy spotykamy się czasem z takimi naruszeniami przepisów. Wykrywanie tego rodzaju naruszeń jest możliwe, gdy rozwiązanie jest audytowalne, np. gdy jest to rozwiązanie sprzętowe lub algorytm w znanym nam języku programowania.

Paragraf 14 rozporządzenia [15] dotyczącego eksploatacji urządzeń ciśnieniowych mówi:
„§ 14. 1. Eksploatację urządzeń ciśnieniowych prowadzi się zgodnie z ich przeznaczeniem, zasadami określonymi w rozporządzeniu oraz instrukcją eksploatacji, stosując odpowiednie środki bezpieczeństwa.
2. Urządzenia ciśnieniowe mogą być eksploatowane tylko wtedy, gdy ich stan techniczny nie budzi zastrzeżeń, osprzęt zabezpieczający, osprzęt ciśnieniowy i automatyka zabezpieczająca są sprawne oraz nie zostały wyłączone z działania".

Na podstawie ww. zapisów wykrycie w czasie inspekcji niezgodnych z dokumentacją zworek lub bypassów stanowi podstawę do wydania decyzji wstrzymującej eksploatację urządzenia i nakazującej wyłączenie urządzenia z eksploatacji.

System sztucznej inteligencji (system AI) oznacza oprogramowanie opracowane przy użyciu co najmniej jednej spośród technik i podejść określonych w załączniku I do rozporządzenia [15], które może – dla danego zestawu celów określonych przez człowieka – generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję.
AI to często architektura „procesora" – swego rodzaju mózgu czy jednostki centralnej. Bardziej można by ją wtedy nazwać technologią niż algorytmem. Ponadto nie musi być zlokalizowana fizycznie w urządzeniu. Odwołując się do przykładu z klasyka science-fiction Ridleya Scotta pt. Łowc***a androidów***, można założyć, że inspekcja urządzenia wyposażonego w AI będzie wymagała kwalifikacji psychologa, analityka i zapewne kilku innych.

Postulujemy twarde, mierzalne, audytowalne ramy dla działania systemów o samozmieniającym się zachowaniu przy zachowaniu wszelkich korzyści płynących z nowoczesnych technologii. Jeśli twarde ograniczenie „stawałoby na drodze" innowacyjnego rozwiązania, to takie rozwiązanie powinno być zarejestrowane, a ograniczenie mogłoby podlegać walidacji w przemyślany, ewolucyjny sposób.

Systemy o samozmieniającym się oprogramowaniu powinny podlegać wymogom dotyczącym jakości wykorzystywanych zbiorów danych, dokumentacji technicznej i rejestrowania zdarzeń, przejrzystości i przekazywania informacji użytkownikom, nadzoru ze strony człowieka oraz wiarygodności, dokładności i cyberbezpieczeństwa. Systemy te należy projektować i opracowywać w taki sposób, aby osoby fizyczne mogły nadzorować ich funkcjonowanie. W tym celu należy określić odpowiednie środki związane z nadzorem ze strony człowieka. Takie środki powinny gwarantować, że system podlega wbudowanym ograniczeniom operacyjnym, których sam nie jest w stanie obejść, i reaguje na działania człowieka, oraz że osoby fizyczne, którym powierzono sprawowanie nadzoru, posiadają niezbędne kompetencje, przeszkolenie i uprawnienia do pełnienia tej funkcji.

Innowacyjne podejście do bezpieczeństwa urządzeń technicznych od zawsze było wbudowane w DNA Urzędu Dozoru Technicznego. Odkąd powstaliśmy, poszukujemy coraz skuteczniejszych metod zapewnienia bezpieczeństwa eksploatacji urządzeń. Od wielu lat wdrażamy i promujemy nowe technologie, w inspekcji oceniając przy tym ich wpływ na bezpieczeństwo.

Technologie przemysłu 4.0 są coraz bardziej dostępne i z uwzględnieniem ewolucyjnych zmian systemów zarządzania produkcją oraz z konieczności zapewnienia bezpieczeństwa teleinformatycznego są implementowane w wielu gałęziach przemysłu. Stwarza to wiele możliwości, które UDT dostrzega i spieszy wykorzystać w praktyce inspekcyjnej.

Wspieramy rozwój, dbamy o bezpieczeństwo.

Literatura:

1. ISO/IEC STRATEGIC BUSINESS PLAN, NOVEMBER 2020; dostęp 25.05.2021
2. Ustawa z dnia 21 grudnia 2000 r. o dozorze technicznym (Dz.U. 2000 nr 122 poz. 1321 z pózn. zm.)
3. Klinkosz T., Dynamiczne zarządzanie ryzykiem instalacji przemysłowych; biuletyn INSPEKTOR 4/2022
4. Klinkosz T., Predykcja zużycia urządzeń ciśnieniowych i planowanie inspekcji z wykorzystaniem metodologii RBI (Risk Based Inspection); biuletyn INSPEKTOR 1/2021
5. ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2023/1230 z dnia 14 czerwca 2023 r. w sprawie maszyn oraz w sprawie uchylenia dyrektywy 2006/42/WE Parlamentu Europejskiego i Rady i dyrektywy Rady 73/361/EWG https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32023R1230
6. Schleich B. et al., Shaping the Digital Twin for design and production engineering. CIRP Annals – Manufacturing Technology, Elsevier, 2017, 66 (1), ff10.1016/j.cirp.2017.04.040ff. ffhal-01513846. [on-line] https://hal.archives-ouvertes.fr/hal-01513846/document; dostęp: 14.02.2021
7. Bane A., Kalwani S., McCormick S., Digital Twins for the asset operator, Element Analytics, Smart Industry; Oct 12, 2017
8. API RP 581 Risk-Based Inspection Methodology, 2008 ▯ 2016.
9. Negri E., Fumagalli L., Macchi M., A Review of the Roles of Digital Twin in CPS-based Production Systems, Procedia Manufacturing, Volume 11, 2017, s. 939-948, ISSN 2351-9789, https://doi.org/10.1016/j.promfg.2017.07.198. [on-line] https://www.sciencedirect.com/science/article/pii/S2351978917304067; dostęp: 20.02.2021
10. Grieves M., Vickers J., Digital Twin: mitigating unpredictable, undesirable emergent behavior in complex systems, Kahlen FJ, Flumerfelt S., Alves A., editors. Transdisciplinary perspectives on complex systems. Springer, 2017. s. 85–113
11. Etyka robotów – Wikipedia, wolna encyklopedia
12. Kritzinger W., Karner M., Traar G., Henjes J., Sihn W., Digital Twin in manufacturing: a categorical literature review and classification, Science Direct, IFAC PapersOnLine 51–11 (2018) 1016–1022; dostęp 25.05.2021
13. https://przemysl-40.pl/index.php/2017/03/22/czym-jest-przemysl-4-0/
14. Qinglin Qi et al., Enabling technologies and tools for Digital Twin, Journal of Manufacturing Systems, https://doi.org/10.1016/j.jmsy.2019.10.001; dostęp: 29.10.2020
15. Rozporządzenie Ministra Rozwoju i Technologii z dnia 17 grudnia 2021 roku w sprawie warunków technicznych dozoru technicznego dla niektórych urządzeń ciśnieniowych podlegających dozorowi technicznemu (Dz.U. 2022 poz.68)
16. EUROPEAN COMMISSION Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, Brussels, 21.4.2021

URZĄD DOZORU TECHNICZNEGO

ATEX BEZPIECZEŃSTWO W STREFACH ZAGROŻONYCH WYBUCHEM

MGR INŻ. DOROTA BAŁACHOWSKA

Kierownik Wydziału Certyfikacji
Departament Certyfikacji
i Oceny Zgodności (UDT-CERT)
Urząd Dozoru Technicznego

MGR INŻ. REMIGIUSZ PUSTKOWSKI

Ekspert w dziedzinie kluczowej ATEX
Biuro w Ostrowie Wielkopolskim
Oddział w Łodzi
Urząd Dozoru Technicznego

Słowo ATEX pochodzi z języka francuskiego i jest akronimem określenia Atmosphères Explosibles, czyli atmosfera wybuchowa. Ponieważ niejednolite przepisy dotyczące bezpieczeństwa w poszczególnych krajach Europejskiej Wspólnoty Gospodarczej, a później Unii Europejskiej stanowiły znaczne utrudnienie w swobodnym przepływie towarów pomiędzy państwami członkowskimi, postanowiono je ujednolicić.

Słysząc akronim ATEX, kojarzymy go z **dyrektywą ATEX 2014/34/WE** wprowadzoną do polskiego prawodawstwa rozporządzeniem Ministra Rozwoju z dnia 6 czerwca 2016 r. w sprawie wymagań dla urządzeń i systemów ochronnych przeznaczonych do użytku w atmosferze potencjalnie wybuchowej (Dz.U. z 2016 r. poz. 817).

Dyrektywa ATEX z 2014 r. dotyczy producentów urządzeń i obejmuje zakres projektowania, badania oraz produkcji.

Kolejną dyrektywą dotyczącą stref zagrożonych wybuchem jest **dyrektywa ATEX User 1999/92/WE** wprowadzona do polskiego prawodawstwa rozporządzeniem Ministra Gospodarki z dnia 8 lipca 2010 r. w sprawie minimalnych wymagań dotyczących bezpieczeństwa i higieny pracy związanych z możliwością wystąpienia w miejscu pracy atmosfery wybuchowej (Dz.U. z 2010 r. Nr 138, poz. 931).

Dyrektywa ATEX User dotyczy użytkowników urządzeń/instalacji, obejmuje zakres instalacji, nadzoru i konserwacji, remontu, odsprzedaży i końcowej fazy likwidacji.

Zarówno producenci, jak i użytkownicy systemów technicznych przeznaczonych do pracy w przestrzeniach zagrożonych wybuchem, zobowiązani do wprowadzenia postanowień dyrektyw ATEX, mogą korzystać z całej gamy norm, zwłaszcza serii PN-EN 1127 i PN-EN 60079, odnoszących się dość kompleksowo do zagadnienia. Jest to zadanie skomplikowane i wymagające obok ugruntowanej wiedzy również odniesienia do praktyki inżynierskiej, najlepiej w ujęciu poszerzonym, tj. bazującym na doświadczeniach wielu branż przemysłu. Odnotowując szybkość zmian zachodzących w branży, należy stwierdzić konieczność stałego śledzenia nowości pojawiających się w tym zakresie w normach, jak również zmian w systemie prawnym [3].

SYSTEMOWE PODEJŚCIE DO ZAPEWNIENIA BEZPIECZEŃSTWA PRZECIWWYBUCHOWEGO

Na bazie wieloletniej praktyki z zakresu techniki przeciwwybuchowej proponuje się zweryfikowany i skuteczny sposób realizacji działań analitycznych w odniesieniu do praktyki przemysłowej. Model ten zakłada następujące kroki/etapy realizacyjne:

1. Przygotowanie danych, zdefiniowanie zadań i ich przygotowanie do realizacji w warunkach przemysłowych, w tym zorganizowanie zespołu realizacyjnego.
2. Analiza i ocena ryzyka wraz ze wskazaniami ogólnymi w zakresie wdrażania środków redukcji ryzyka.
3. Opracowanie merytoryczne oraz redakcyjne dokumentów pozwalających spełnić wymogi prawne, z uwzględnieniem wskazań normatywnych.
4. Wdrożenie technicznych i organizacyjnych środków redukcji ryzyka.
5. Weryfikacja, aktualizacja i uzupełnienia po okresie eksploatacji [3].

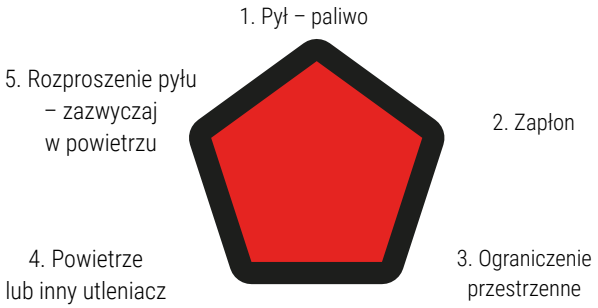
Terminy i definicje

Wybuch – gwałtowna reakcja utleniania lub rozkładu wywołująca wzrost ciśnienia, temperatury lub obu jednocześnie.

Atmosfera wybuchowa – mieszanina z powietrzem, w warunkach atmosferycznych, substancji palnych w postaci gazu, pary, mgły lub pyłu, w której to mieszaninie po nastąpieniu zapłonu spalanie rozprzestrzenia się na całą jej niespaloną część.

Trójkąt palności

Pięciokąt wybuchowości



Dolna granica wybuchowości (DGW) – najniższa wartość stężenia zakresu wybuchowości, przy której może nastąpić wybuch (Lower Explosive Limit – LEL).

Górna granica wybuchowości (GGW) – najwyższa wartość stężenia zakresu wybuchowości, przy której może wystąpić wybuch (Upper Explosive Limit – UEL).

Granice wybuchowości zależą od temperatury i ciśnienia, rozmiaru i kształtu powierzchni ograniczającej, źródła zapłonu (rodzaj, energia) oraz właściwości palnych substancji (paliwa).

Temperatura samozapłonu (AIT) – najniższa temperatura ogrzanej powierzchni, przy której w określonych warunkach może wystąpić zapalenie substancji palnej w postaci mieszaniny gazu lub pary z powietrzem.

Przestrzenie zagrożone wybuchem – przestrzenie, w których może wystąpić atmosfera wybuchowa w ilościach wymagających podjęcia specjalnych środków w celu zapewnienia bezpieczeństwa i higieny pracy.

Urządzenia w wykonaniu Ex – urządzenia określone w przepisach dotyczących zasadniczych wymagań dla urządzeń i systemów ochronnych przeznaczonych do użytku w przestrzeniach zagrożonych wybuchem.

Zagrożenie wybuchem należy rozpatrywać w odniesieniu do rodzaju atmosfery wybuchowej – atmosfera pyłowa czy gazowa.

Oznaczenia stref zagrożonych wybuchem – strefy gazowe		
	przestrzeń, w której atmosfera wybuchowa zawierająca mieszaninę z powietrzem substancji palnych w postaci gazów, par, mgieł, **występuje stale, często lub przez długie okresy**	**STREFA 0** Atmosfera wybuchowa obecna jest cały czas
	przestrzeń, w której atmosfera wybuchowa zawierająca mieszaninę z powietrzem substancji palnych w postaci gazów, par, mgieł, **może czasami wystąpić w trakcie normalnego działania**	**STREFA 1** Atmosfera wybuchowa obecna jest często
	przestrzeń, w której atmosfera wybuchowa zawierająca mieszaninę z powietrzem substancji palnych w postaci gazów, par, mgieł, **nie występuje w trakcie normalnego działania, a w przypypadku wystąpienia utrzymuje się przez krótki okres**	**STREFA 2** Atmosfera wybuchowa może być obecna przypadkowo

Oznaczenia stref zagrożonych wybuchem – strefy pyłowe		
	przestrzeń, w której atmosfera wybuchowa w postaci obłoku palnego pyłu w powietrzu **występuje stale, często lub przez długie okresy**	**STREFA 20** Atmosfera wybuchowa obecna jest cały czas
	przestrzeń, w której atmosfera wybuchowa w postaci obłoku palnego pyłu w powietrzu **może czasami wystąpić w trakcie normalnego działania**	**STREFA 21** Atmosfera wybuchowa obecna jest często
	przestrzeń, w której atmosfera wybuchowa w postaci obłoku palnego pyłu w powietrzu nie występuje w trakcie normalnego działania, **a w przypadku wystąpienia utrzymuje się przez krótki okres**	**STREFA 22** Atmosfera wybuchowa może być obecna przypadkowo

ATEX 2014/34/WE VS. ATEX 1999/92/WE

Wiedza na temat regulacji wynikających z dyrektyw ATEX i ich zastosowań, w połączeniu z dobrze ugruntowaną wiedzą ekspercką oraz właściwie prowadzonymi analizami bezpieczeństwa funkcjonalnego dla systemów ochronnych w strefach Ex, jest najbardziej efektywnym sposobem podejścia do redukcji ryzyka związanego z możliwością wystąpienia wybuchu. W szczególny sposób odnosi się do zakładów o znacznym potencjale, dużym nagromadzeniu substancji mogących spowodować szkodę obiektów o dużym skomplikowaniu procesów [3].

Dyrektywy ATEX	
Producent	**Użytkownik**
Dyrektywa ATEX	Dyrektywa ATEX user
2014/34/UE	1999/92/WE
	

Dyrektywa ATEX User – dyrektywa 1999/92/WE Parlamentu Europejskiego i Rady z dnia 16 grudnia 1999 r. w sprawie minimalnych wymagań dotyczących bezpieczeństwa i ochrony zdrowia pracowników zatrudnionych na stanowiskach pracy, na których może wystąpić atmosfera wybuchowa. Zgodnie z dyrektywą ATEX User **poprawa bezpieczeństwa**, higieny i ochrony zdrowia pracowników w miejscu pracy jest celem, który nie powinien być podporządkowany rozważaniom ściśle ekonomicznym.

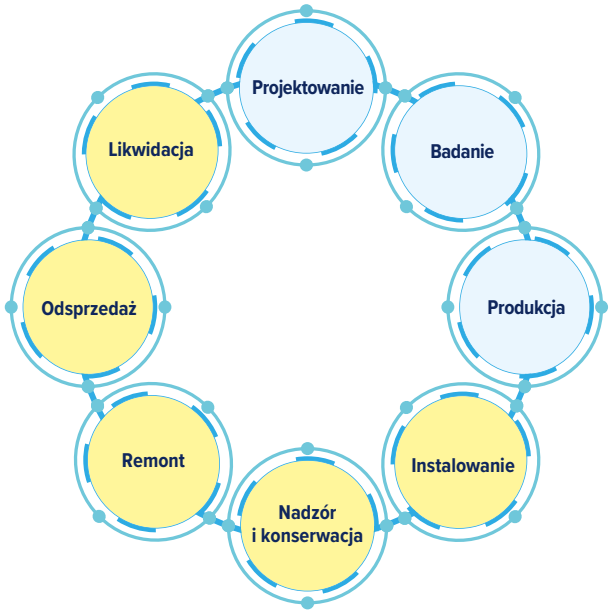
- Zgodnie z dyrektywą 1999/92/WE pracodawca zobligowany jest do zapewnienia odpowiedniego poziomu bezpieczeństwa pracy, w tym wyposażenia miejsc pracy w urządzenia dostosowane do występujących zagrożeń. Odpowiednie wyznaczenie i oznakowanie stref zagrożenia wybuchem, jak również prawidłowy dobór urządzeń do tych stref są kluczowe w kontekście zapewnienia bezpieczeństwa pracowników oraz całego otoczenia.

- W celu zapewnienia bezpieczeństwa i ochrony zdrowia pracowników pracodawca podejmuje niezbędne środki, aby w miejscu, gdzie atmosfery wybuchowe mogą pojawić się w ilościach zagrażających bezpieczeństwu i zdrowiu pracowników albo innych osób, środowisko pracy było takie, aby móc wykonywać pracę bezpiecznie. Dodatkowo w otoczeniu miejsca pracy, gdzie atmosfery wybuchowe mogą się pojawić w ilościach zagrażających, zapewnia się odpowiedni nadzór zgodnie z przeprowadzoną oceną ryzyka, przy użyciu odpowiednich środków technicznych.

- Decyzja użytkownika dotycząca zastosowanych w zakładzie rozwiązań minimalizujących zagrożenia powinna opierać się na odpowiednio przeprowadzonej ocenie ryzyka, powiązanej z usystematyzowanymi wymaganiami wynikającymi z dyrektywy ATEX User, Polskich Norm oraz dobrej praktyki inżynierskiej.

- Przed udostępnieniem miejsca pracy pracodawca powinien na podstawie oceny ryzyka sporządzić **Dokument Zabezpieczenia Przed Wybuchem – DZPW**. W przypadku gdy miejsce pracy, znajdujące się w nim urządzenia lub organizacja pracy zostały poddane zmianom mogącym mieć wpływ na wynik oceny ryzyka, pracodawca powinien niezwłocznie dokonać aktualizacji dokumentu.

Cykl życia urządzenia z podziałem na obszary odpowiedzialności



EX

dyrektywa 1999/92/WE – ATEX User (Użytkownik)

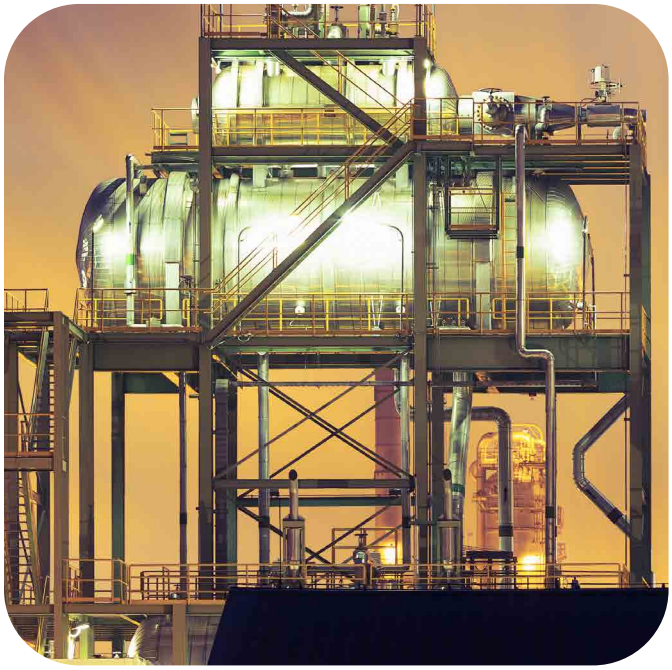
Ex

dyrektywa 2014/34/U – ATEX (Producent)

Doświadczenia Urzędu Dozoru Technicznego w zakresie stref zagrożenia wybuchem skupiają się głównie na zagadnieniach wynikających z dyrektywy ATEX User 1999/92/WE. Rozporządzenie Ministra Gospodarki z dnia 8 lipca 2010 r. wprowadzające dyrektywę ATEX User nakłada na pracodawcę, który na terenie swojego przedsiębiorstwa posiada materiały palne, które mogą wytworzyć atmosferę zagrożenia wybuchem, szereg obowiązków. Należy tu wymienić między innymi: ocenę zagrożenia wybuchem, klasyfikację stref zagrożenia wybuchem, opracowanie dokumentu zabezpieczenia przed wybuchem – DZPW oraz weryfikację urządzeń zainstalowanych w strefach zagrożenia wybuchem.

Urząd Dozoru Technicznego oferuje usługi w obszarze bezpieczeństwa skierowane do wszystkich organizacji. Wychodząc naprzeciw oczekiwaniom rynkowym, Jednostka Certyfikująca UDT-CERT proponuje pakiet usług w obszarze ATEX:

- wyznaczanie stref zagrożenia wybuchem: opracowywanie kart klasyfikacyjnych, a także weryfikacja projektów kart
- opracowanie dokumentu zabezpieczenia przed wybuchem (DZPW)
- weryfikacja dokumentu zabezpieczenia przed wybuchem (DZPW)
- weryfikacja poprawności doboru urządzeń do stref zagrożenia wybuchem: urządzenia elektryczne, nieelektryczne oraz systemy ochronne
- analiza i ocena ryzyka (analiza HAZOP w obszarze ATEX)
- inspekcje Ex
- szkolenia z zakresu Ex



UDT-CERT jako jednostka ekspercka, wychodząc naprzeciw oczekiwaniom rynku, uczestniczyła w licznych postępowaniach dla największych firm w branżach petrochemicznej, chemicznej oraz energetycznej. Zakres prac obejmował klasyfikację stref zagrożenia wybuchem, opracowanie dokumentu zabezpieczenia przed wybuchem, inspekcje początkowe urządzeń zainstalowanych w strefach zagrożonych wybuchem oraz weryfikację wyznaczenia stref zagrożenia wybuchem i dokumentu zabezpieczenia przed wybuchem. Z doświadczenia ekspertów UDT-CERT wynika, że do głównych problemów po stronie inwestorów należą:

- brak jednolitych danych odnośnie do charakterystyki substancji palnych,
- nieaktualne opisy technologiczne,
- posługiwanie się zapisami nieaktualnych procedur,
- brak aktualnych podkładów geodezyjnych wraz z naniesionymi urządzeniami technologicznymi.

URZĄD DOZORU TECHNICZNEGO

W przypadku postępowań związanych z inspekcją urządzeń zainstalowanych w strefach zagrożonych wybuchem spostrzeżenia i uwagi przekazywane klientom były tożsame. Najczęstsze błędy instalacyjne to:

- niewłaściwie dobrane wpusty kablowe (dławiki) – stosowane wpusty, zaślepki nie były przeznaczone do pracy w wyznaczonych strefach, oraz niewłaściwie dobrane średnice wpustów kablowych w stosunku do średnicy kabli. Nie może wystąpić możliwość swobodnego poruszania się przewodu we wpuście, czyli możliwość przedostania się atmosfery wybuchowej do środka urządzenia,
- urządzenia bez tabliczek znamionowych – każde urządzenie przeznaczone do pracy w atmosferze wybuchowej powinno być odpowiednio oznaczone,
- brak instrukcji obsługi w języku polskim – zgodnie z zapisami dyrektywy ATEX 2014/34/WE opisy, ostrzeżenia powinny być w języku zrozumiałym dla obsługi,
- brak oznakowania CE – urządzenia instalowane w strefach EX muszą przejść proces oceny zgodności według dyrektywy ATEX 2014/34/WE – nie mogą to być urządzenia posiadające certyfikaty na rynek amerykański, azjatycki etc.,
- brak odpowiednich uziemień dla zainstalowanych urządzeń oraz nieodpowiednio zabezpieczone niewykorzystane przewody w urządzeniach – według wymagań normy PN-EN60079-14 wolne przewody powinny być połączone do zacisku uziemiającego urządzenia lub też odpowiednio zabezpieczone,
- niewłaściwy dobór urządzeń ze względu na temperaturę pracy – każde urządzenie powinno zawierać oznaczenie klasy temperaturowej i maksymalnej temperatury powierzchni oraz powinno być dobrane zgodnie z właściwymi parametrami.

Eksperci UDT-CERT zwracają uwagę inwestorom i właścicielom instalacji, którzy posiadają na swoim terenie urządzenia pracujące w strefach zagrożonych wybuchem, że zgodnie z zapisami normy PN-EN60079-17:2011-05 urządzenia te powinny przed oddaniem do użytku zostać poddane **inspekcji początkowej przez osoby o odpowiednich kwalifikacjach.** W późniejszym okresie użytkowania norma przewiduje inspekcje tych urządzeń w czasie nie dłuższym niż 3 lata. Inspekcje urządzeń pracujących w strefach wykonywane są jako ekspertyzy techniczne.

KORZYŚCI ZE WSPÓŁPRACY Z UDT-CERT

Opierając się na doświadczeniu swoich ekspertów, UDT-CERT oferuje rozwiązania zapewniające kompleksową i rzetelną ocenę zabezpieczenia instalacji.

Dostawca – gwarancja bezpieczeństwa wyrobów dostarczanych i instalowanych przez poddostawców

Inwestor – gwarancja bezpieczeństwa instalacji

Wykonawca – gwarancja nienaruszenia istotnych cech bezpieczeństwa przeciwwybuchowego podczas montażu

Użytkownik – gwarancja bezpiecznej eksploatacji oraz poprawność dokumentacji początkowej

GWARANCJA BEZPIECZEŃSTWA PRZECIWWYBUCHOWEGO

Wobec wzrastającej złożoności procesów produkcyjnych oraz rosnących kosztów inżynierskich efektywna inżynieria jest czynnikiem kluczowym w przemyśle procesowym. Bezpieczeństwo przeciwwybuchowe, rozumiane jako brak niemożliwego do zaakceptowania ryzyka dla zdrowia, życia lub strat w majątku czy środowisku naturalnym, ma szczególne znaczenie w przemyśle chemicznym, petrochemicznym, w gazownictwie i energetyce. Jest integralną częścią ogólnego bezpieczeństwa, szczególnie odnosi się do instalacji procesowych zawierających i przerabiających substancje chemiczne. **Misją Urzędu Dozoru Technicznego jest wspieranie rozwoju i dbanie o bezpieczeństwo.** Dotyczy to szczególnie powiązań pomiędzy bezpieczeństwem społeczeństwa a urządzeniami technicznymi w przemyśle czy codziennym użytkowaniu. Bezpieczeństwo zależy nie tylko od bezpiecznego prowadzenia procesów i eliminacji narażenia ludzi na skutki zagrożeń, ale również polega na zapobieganiu, w tym przypadku zapobieganiu powstawaniu zagrożeń w atmosferach wybuchowych oraz potencjalnych atmosferach wybuchowych. Tylko zintegrowane podejście do zakresu niezbędnych czynności w obszarze ATEX pozwala ekspertom Urzędu Dozoru Technicznego objąć całość zagadnień, a inwestorowi, przy wsparciu naszych ekspertów, zorientować się w możliwości realizacji zadania.

Literatura:

1. Rozporządzenie Ministra Rozwoju z dnia 6 czerwca 2016 r. w sprawie wymagań dla urządzeń i systemów ochronnych przeznaczonych do użytku w atmosferze potencjalnie wybuchowej (Dz.U. z 2016 r. poz. 817).
2. Rozporządzenie Ministra Gospodarki z dnia 8 lipca 2010 r. w sprawie minimalnych wymagań dotyczących bezpieczeństwa i higieny pracy związanych z możliwością wystąpienia w miejscu pracy atmosfery wybuchowej (Dz.U. z 2010 r. Nr 138 poz. 931).
3. Podstawy bezpieczeństwa funkcjonalnego, red. K.T. Kosmowski, Gdańsk 2016.
4. Markowski A.S., Bezpieczeństwo procesów przemysłowych, Łódź 2017.

Wspieramy rozwój
Dbamy o bezpieczeństwo

ATEX USER

KOMPLEKSOWA OFERTA UDT-CERT

- wyznaczanie stref zagrożenia wybuchem
- opracowanie dokumentu zabezpieczenia przed wybuchem
- weryfikacja dokumentu zabezpieczenia przed wybuchem
- weryfikacja poprawności doboru urządzeń do stref zagrożenia wybuchem
- analiza i ocena ryzyka
- inspekcje Ex
- szkolenia

SPRAWDŹ OFERTĘ UDT-CERT!

CYBERBEZPIECZEŃSTWO PRZEDSIĘBIORSTW W KLUCZOWYCH BRANŻACH GOSPODARKI

MGR INŻ. DOROTA BAŁACHOWSKA

Kierownik Wydziału Certyfikacji
Wiceprzewodnicząca Zespołu ds. Cyberbezpieczeństwa UDT
Departament Certyfikacji i Oceny Zgodności
Urząd Dozoru Technicznego

Współczesna gospodarka opiera się na wykorzystywaniu bardzo wielu różnorodnych technologii, które wykształciły specyficzne środowisko pracy. Obserwujemy nieodwracalny progres cywilizacyjny i technologiczny napędzany nieustannym dążeniem do innowacyjności. Konsekwencją tak dużego postępu gospodarczego jest ujawnienie się różnego rodzaju zagrożeń wywołanych działalnością człowieka. Bezpieczeństwo w przemyśle zależy nie tylko od właściwego prowadzenia procesów i eliminacji narażenia ludzi na skutki zagrożeń, ale polega również na zapobieganiu atakom zewnętrznym, w tym cyberatakom.

Jest to zadanie dla Urzędu Dozoru Technicznego, które realizujemy zgodnie z obowiązująca wizją: Lider innowacyjności w obszarze bezpieczeństwa publicznego, w tym również w obszarze cyberbezpieczeństwa.

Zagrożenia związane z atakami w sieci można ograniczyć, stosując określone procedury.
Urząd Dozoru Technicznego opracował innowacyjną metodykę, która pomaga firmom w przeprowadzeniu audytu cyberbezpieczeństwa na zgodność z obowiązującymi przepisami.

BEZPIECZEŃSTWO SYSTEMÓW KOMPUTEROWYCH

Systemy komputerowe stosowane w przemyśle powinny być zintegrowane w obszarze *security* oraz *safety*. Wyróżnia się dwa rodzaje systemów komputerowych z uwzględnieniem wymienionych obszarów, tj. systemy komputerowe odpowiedzialne za przetwarzanie, przechowywanie i przesyłanie informacji oraz systemy komputerowe odpowiedzialne za sterowanie, które reagują na zdarzenia zachodzące w ich środowisku poprzez wysyłanie do nich informacji sterującej. Przy budowaniu programu cyberbezpieczeństwa w organizacji należy uwzględnić integralność obu systemów.

Zapewnianie bezpieczeństwa to działania UDT, które jako organizacja zaufania publicznego realizujemy od ponad 100 lat.

Dobrze opracowany i skutecznie wdrożony program cyberbezpieczeństwa powinien umożliwić organizacji efektywne zarządzanie ryzykiem również poprzez odpowiednie wykorzystanie zasobów w obszarze cyberbezpieczeństwa. Organizacja musi zapewnić skuteczną ochronę przed istniejącymi i potencjalnymi zagrożeniami, wykrywać luki w systemie, podejmować niezbędne działania naprawcze oraz chronić aktywa informacyjne stanowiące wymierną wartość organizacji. Nieodłącznym aspektem należycie opracowanego i skutecznie wdrożonego programu cyberbezpieczeństwa jest zadbanie o ochronę marki i reputacji organizacji oraz zapewnienie przewagi konkurencyjnej, m.in. poprzez elastyczne dostosowywanie się do otaczających zmian biznesowych.

Rys. 1. Pięć zasad cyberbezpieczeństwa

KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

W skład Krajowego Systemu Cyberbezpieczeństwa (KSC) wchodzą m.in. instytucje administracji rządowej i samorządowej oraz najwięksi przedsiębiorcy z kluczowych sektorów gospodarki.

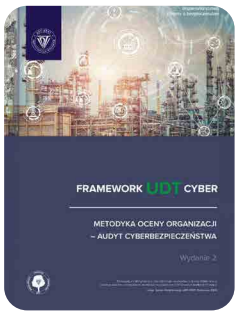
„Krajowy system cyberbezpieczeństwa ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów." [1].

W ustawie o Krajowym Systemie Bezpieczeństwa [1] określono objęte nim podmioty. Wśród nich można wymienić:
- **operatorów usług kluczowych (OUK), którymi są m.in.: największe banki, firmy z sektora energetycznego, przewoźnicy lotniczy i kolejowi, armatorzy, szpitale,**
- **dostawców usług kluczowych (DUC), czyli m.in.: internetowe platformy handlowe, organy właściwe (OW), czyli instytucje publiczne, w których kompetencjach znajdzie się nadzór nad danym sektorem istotnym dla gospodarki.**

W ramach KSC powstały Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego. Utworzono je w trzech instytucjach: Agencji Bezpieczeństwa Wewnętrznego (CSIRT GOV), Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym (CSIRT NASK) oraz Ministerstwie Obrony Narodowej (CSIRT MON).

Ustawa o KSC nakłada na operatorów usług kluczowych liczne obowiązki. Jednym z nich jest obowiązek przeprowadzenia co najmniej raz na dwa lata audytu bezpieczeństwa systemu informacyjnego, wykorzystywanego do świadczenia usługi kluczowej. Pierwszy audyt powinien być przeprowadzony w ciągu roku od momentu powołania na Operatora Usługi Kluczowej. Warto podkreślić, że za niewykonanie przez OUK obowiązków wynikających z ustawy przewidziano zastosowanie kar finansowych (rozdział 14 UoKSC).

Urząd Dozoru Technicznego na potrzeby przeprowadzania audytu cyberbezpieczeństwa na zgodność z wymaganiami zawartymi w ustawie o Krajowym Systemie Cyberbezpieczeństwa opracował innowacyjną metodykę Framework UDTCyber, tj. strukturę ramową systemu oceny cyberbezpieczeństwa w organizacji, stanowiącą jedocześnie podstawę do budowania programu cyberbezpieczeństwa.



Wydanie 2 Framework UDTCyber jest odpowiedzią na zmiany w obowiązujących przepisach, jak również aktualizacje norm będących podstawą merytoryczną opracowania.

Dokument oparty jest na międzynarodowych metodykach, takich jak NIST Cybersecurity Framework [2], wymaganiach i wytycznych norm serii ISO/IEC 27000 [3, 8], IEC 62443 [4] oraz ISO 22301 [5], a także na wymaganiach ustawy o Krajowym Systemie Cyberbezpieczeństwa – UoKSC (Dz.U. z 2023 r. poz. 913) [1].

WYMAGANIA PRAWNE – DYREKTYWA NIS 2 ORAZ DYREKTYWA CER

Aktualnie obwiązującym aktem prawnym dotyczącym ogólnego poziomu cyberbezpieczeństwa na terenie Rzeczypospolitej Polskiej jest ustawa o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018 r., Dz.U. z 2023 r. poz. 913 [1].

Ustawa o KSC [1] (podrozdział 4.2) wraz z aktami wykonawczymi (podrozdział 4.3) implementuje postanowienia dyrektywy NIS 2016/1148/UE (ang. Network and Information Systems Directive) z 2016 r. (podrozdział 4.1).

Tymczasem w Dzienniku Urzędowym UE L333/80 z 27 grudnia 2022 r. została opublikowana dyrektywa NIS 2 2022/2555 [6] – dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (NIS).

Co ważne, wraz z publikacją NIS 2 w tym samym Dzienniku Urzędowym UE opublikowana została również dyrektywa CER 2022/2557 [7] – dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE.

Dyrektywa CER wraz z dyrektywą NIS 2 tworzą całościowo spójne i zharmonizowane ramy prawne w zakresie zapewniania ciągłości świadczenia usług kluczowych dla państwa, kreując przy tym odporność podmiotów świadczących te usługi na zagrożenia fizyczne i incydenty cyberbezpieczeństwa.

Z uwagi na powiązanie między bezpieczeństwem fizycznym a cyberbezpieczeństwem podmiotów krytycznych obydwa akty prawne wzajemnie się uzupełniają, przy czym dyrektywy CER nie stosuje się do kwestii objętych dyrektywą NIS 2. Dyrektywy weszły w życie 16 stycznia 2023 r., a państwa członkowskie zostały zobowiązane do implementacji wymagań unijnych do prawa krajowego do 17 października 2024 r. W chwili obecnej wymagania dyrektyw NIS 2 oraz CER nie zostały jeszcze wdrożone do prawa polskiego.

Dyrektywa NIS 2 [6] określa:

- obowiązki państw członkowskich dotyczące przyjęcia krajowych strategii cyberbezpieczeństwa oraz wyznaczenia lub powołania właściwych organów, organów ds. zarządzania kryzysowego w cyberbezpieczeństwie, pojedynczych punktów kontaktowych ds. cyberbezpieczeństwa oraz zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT),
- środki zarządzania ryzykiem w cyberbezpieczeństwie oraz obowiązki w zakresie zgłaszania incydentów spoczywające na podmiotach kluczowych i ważnych, o których mowa w załączniku I lub II dyrektywy, jak również na podmiotach zidentyfikowanych jako podmioty o charakterze krytycznym na podstawie dyrektywy CER,
- zasady i obowiązki w zakresie wymiany informacji o cyberbezpieczeństwie,
- obowiązki w zakresie nadzoru i egzekwowania przepisów spoczywające na państwach członkowskich.

Dyrektywa NIS 2 [6] definiuje:

podmioty kluczowe (sektory kluczowe – Załącznik I dyrektywy NIS 2),
podmioty ważne (sektory ważne – Załącznik II dyrektywy NIS 2).

Tabela 1. Zmiany sektorowe w dyrektywie NIS 2 w stosunku do dyrektywy NIS (**kolor czerwony – zmiany w stosunku do dyrektywy NIS**, **kolor zielony – brak zmian w stosunku do dyrektywy NIS**)

SEKTORY PODMIOTÓW KLUCZOWYCH	SEKTORY PODMIOTÓW WAŻNYCH
Energetyka (energia elektryczna, system ciepłowniczy lub chłodniczy, ropa naftowa, gaz, wodór)	Usługi pocztowe i kurierskie
Transport (lotniczy, kolejowy, wodny, drogowy)	Gospodarowanie odpadami
Bankowość	Produkcja (wyroby medyczne i wyroby medyczne do diagnostyki in vitro, produkty komputerowe, elektroniczne i optyczne; sprzęt elektryczny; maszyny i urządzenia; pojazdy samochodowe, przyczepy i naczepy; pozostały sprzęt transportowy)
Infrastruktura rynków finansowych	Produkcja, wytwarzanie i dystrybucja chemikaliów
Opieka zdrowotna	Produkcja, przetwarzanie i dystrybucja żywności
Woda pitna	Dostawcy usług cyfrowych
Ścieki	Badania naukowe
Infrastruktura cyfrowa	
Zarządzanie usługami ICT (między przedsiębiorstwami)	
Podmioty administracji publicznej	
Przestrzeń kosmiczna	

Reasumując, dyrektywa NIS 2 rozszerza znacznie zakres pierwszej dyrektywy NIS, zaostrza wymogi w zakresie bezpieczeństwa i sprawozdawczości dla przedsiębiorstw, wprowadza bardziej rygorystyczne środki nadzoru dla organów krajowych i surowsze wymogi w zakresie egzekwowania przepisów oraz poprawia wymianę informacji i współpracę między organami państw członkowskich.

AUDYT BEZPIECZEŃSTWA SYSTEMU INFORMACYJNEGO

Urząd Dozoru Technicznego przeprowadza audyty cyberbezpieczeństwa (audyt trzeciej strony) według kryteriów i obszarów zdefiniowanych w ramach Framework UDTCyber.

UDT jest jednostką akredytowaną w ramach norm:
- PN-EN ISO/IEC 27001. Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności - Systemy zarządzania bezpieczeństwem informacji - Wymagania [3],
- PN-EN ISO 22301 - Systemy zarządzania ciągłością działania [5]

oraz zatrudnia wykwalifikowanych audytorów posiadających odpowiednie kompetencje.

Zespół audytorów UDT dysponuje zarazem możliwościami technicznymi do przeprowadzania audytów cyberbezpieczeństwa i niezbędną wiedzą w wymaganym obszarze. Audyt jest szczególnym rodzajem oceny wykonywanej przez stronę niezależną.

Niezależność strony wykonującej audyt musi być zachowana w stosunku do:
● organizacji i zespołu projektowego lub np.
● budującego system zabezpieczeń,
● dostawców sprzętu i oprogramowania,
● organizacji podlegającej przeglądowi*.
Każda odpowiedzialna organizacja ma wydzielony oddzielny zespół/departament odpowiedzialny za cyberbezpieczeństwo, niebędący w strukturach IT.
** W skład zespołu audytowego nie mogą wchodzić pracownicy organizacji zlecającej audyt.*

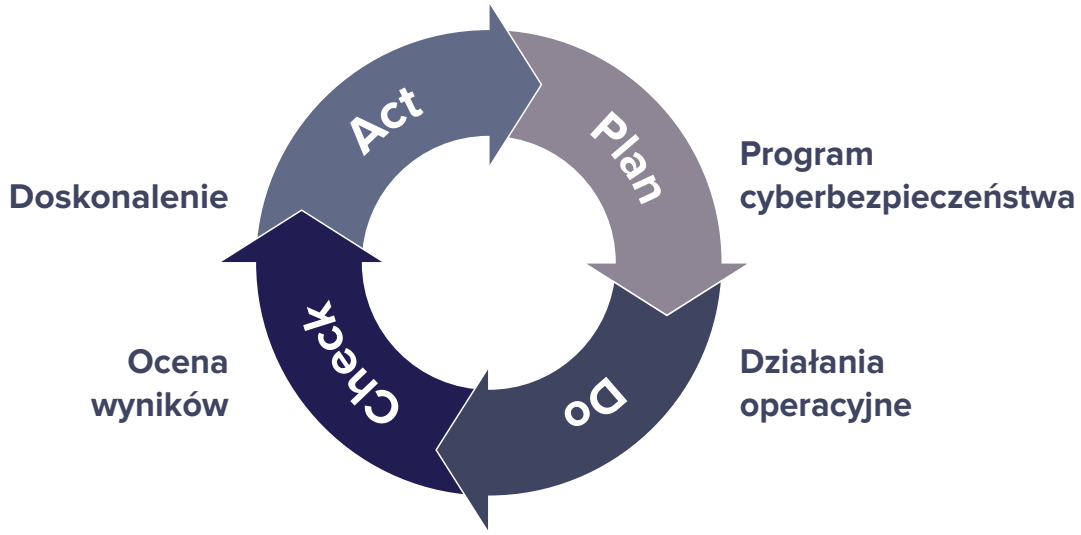
Dokumentacja wyników audytu powinna składać się z:
- raportu z audytu, zawierającego specyfikację celu audytu, opis realizacji przedsięwzięcia audytowego, podsumowanie wyników dla kadry kierowniczej (często wyodrębniane jako osobny dokument), specyfikację punktów sprawdzeń wraz z wynikami, zalecenia poaudytowe;
- wyników badań technicznych (tzw. dowodów audytowych) zawierających: przeglądy konfiguracji, analizę wyników testów penetracyjnych przeprowadzonych przez organizację bądź inny podmiot na zlecenie organizacji itp.

Audyt może być przeprowadzany w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych, a więc np. audyt systemu zarządzania bezpieczeństwem informacji (27001) i zarządzania ciągłością działania (22301).

FRAMEWORK UDTCYBER

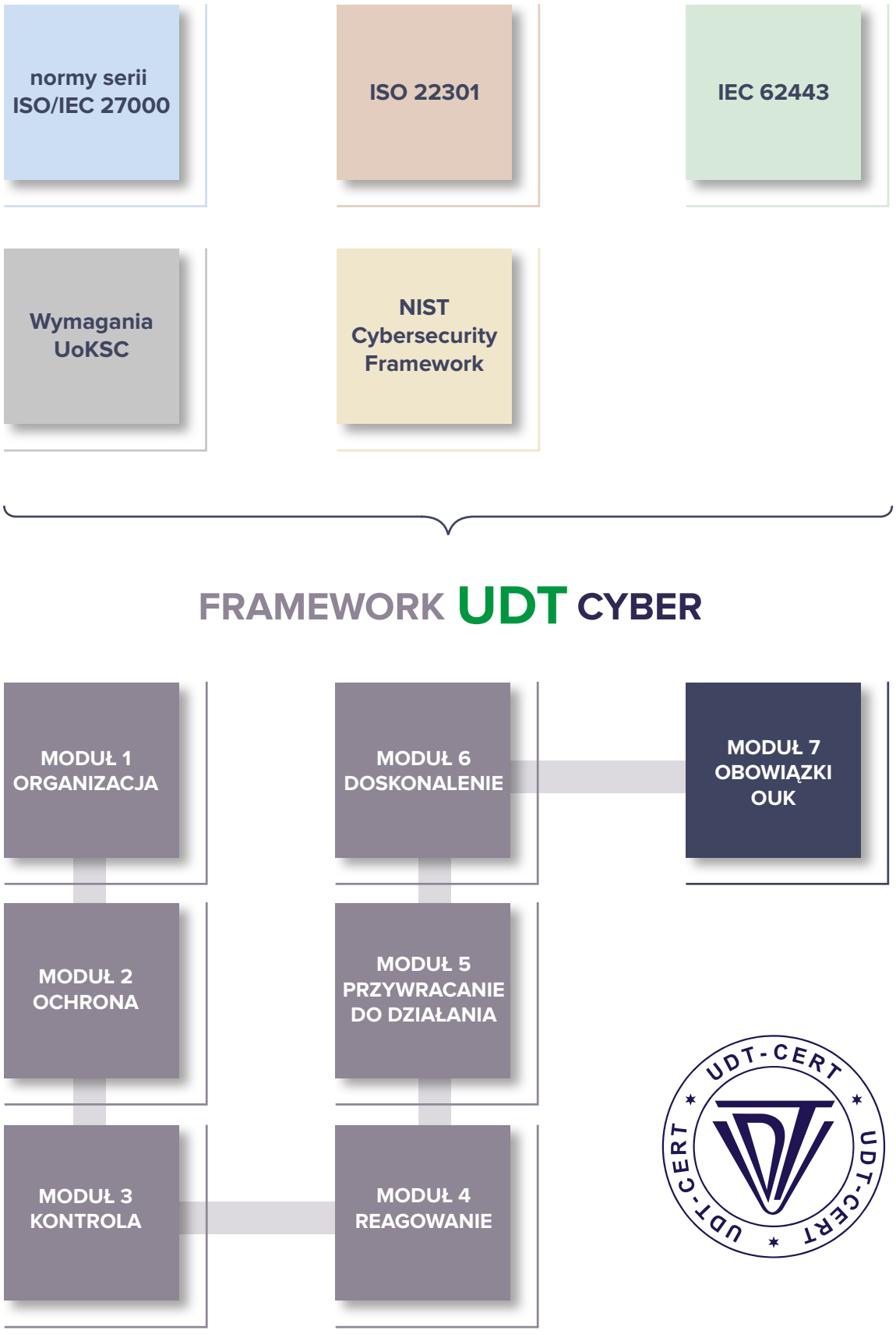
Metodyka UDTCyber zbudowana jest w systemie 7/7. Podział uwzględnia 7 modułów oraz 7 zdefiniowanych obszarów stanowiących zakres oceny. Framework UDTCyber jest metodyką, którą łatwo dostosować do potrzeb każdej organizacji oraz do potrzeb operatorów usług kluczowych.

Budowa programu cyberbezpieczeństwa na podstawie niniejszej metodyki opiera się na cyklu Deminga (cykl PDCA) przebiegającym w czterech następujących po sobie etapach: planowanie – wykonanie – sprawdzenie – poprawienie (ang. Plan – Do – Check – Act).



Rys. 2. Budowa programu cyberbezpieczeństwa na podstawie cyklu PDCA

Urząd Dozoru Technicznego tworząc innowacyjną metodykę budowania programu cyberbezpieczeństwa i oceny organizacji w ramach audytu cyberbezpieczeństwa, zastosował wybrane międzynarodowe metodyki: wymagania ISO/IEC 27001 [3] wraz z wytycznymi ISO/IEC 27002 [8], NIST Cybersecurity Framework [2], wymagania ISO 22301 [5], IEC 62443 [4] oraz wymagania ustawy o Krajowym Systemie Cyberbezpieczeństwa [1].



Rys. 3. Framework UDTCyber – struktura

Framework UDTCyber obejmuje następujące moduły (1–7) i obszary (M(1–7).1–7)
PRZYKŁAD
Moduł 1 Organizacja – zawiera siedem obszarów od M1.1 do M1.7
Moduł 4 Reagowanie – zawiera siedem obszarów od M4.1 do M4.7.

M1.1. Struktura organizacyjna i otoczenie
M1.2. Zasoby ludzkie
M1.3. Zarządzanie i odpowiedzialność
M1.4. Przywództwo i zaangażowanie
M1.5. Strategia cyberbezpieczeństwa
M1.6. Systemy zarządzania
M1.7. Standardy bezpieczeństwa technicznego

Rys. 4. Moduł 1 Framework UDTCyber: ORGANIZACJA

STANDARDY IEC 62443

Nowym elementem opracowania **Framework UDTCyber – wydanie 2** jest rozszerzenie o serię standardów **IEC 62443 [4]** (pierwotnie ISA-99) – Bezpieczeństwo w systemach sterowania i automatyki przemysłowej (ang. Security for Industrial Automation and Control Systems) / Przemysłowe sieci komunikacyjne - Bezpieczeństwo sieci i systemów (ang. Industrial communication networks – Network and system security).

Seria norm będzie składać się docelowo z 15 arkuszy (kilka arkuszy jest aktualnie w opracowaniu), publikowanych historycznie jako ISA (ang. ISA – International Society of Automation, US), ANSI/ISA (ang. ANSI – American National Standards Institute), IEC (ang. IEC – International Electrotechnical Commission) oraz PN-EN IEC, dotyczących bezpieczeństwa w automatyce przemysłowej i systemach sterowania IACS (ang. Industrial Automation and Control Systems) oraz w przemysłowych sieciach komunikacyjnych (ang. Industrial communication networks).

Arkusze z pierwszej części normy wprowadzają do kluczowych terminów, pojęć i modeli używanych w całej serii norm IEC 62443 oraz ułatwiają zrozumienie specyficznej terminologii związanej z cyberbezpieczeństwem w kontekście systemów sterowania przemysłowego. Składają się na tę część cztery arkusze opisujące koncepcje cyberbezpieczeństwa, słownik terminów, definicji, metodologia opracowywania wskaźników ilościowych pochodzących z procesu i wymagań technicznych zawartych w normach, określenie podstawowego cyklu życia zabezpieczeń IACS, a także kilka przypadków użycia.

Druga część normy zawiera dokumenty, które skupiają się na politykach i procedurach związanych z bezpieczeństwem IACS. W skład tej części wchodzi pięć arkuszy określających wymagania co do zdefiniowania i wdrożenia efektywnego systemu zarządzania cyberbezpieczeństwem IACS, metodologię oceny poziomu ochrony, wytyczne dotyczące zarządzania poprawkami dla IACS, wymagania dla dostawców oraz informację, co jest wymagane do prowadzenia skutecznego programu cyberbezpieczeństwa IACS.

Trzecia część opisuje wymagania na poziomie systemowym zawarte w trzech arkuszach. Wskazują one zastosowanie różnych technologii bezpieczeństwa w środowisku IACS, ocenę ryzyka cyberbezpieczeństwa i projektowania (model Zone and Conduit) oraz wymagania dla systemu IACS na podstawie poziomu bezpieczeństwa.

Czwarta i ostatnia grupa obejmuje dokumenty, które dostarczają informacji dotyczących bardziej konkretnych i szczegółowych wymagań związanych z rozwojem produktów IACS. W skład tej części wchodzą dwa arkusze opisujące cykl życia rozwoju zabezpieczeń oraz wymagania dotyczące komponentów IACS na podstawie poziomu bezpieczeństwa. Składniki obejmują urządzenia wbudowane, urządzenia hosta, urządzenia sieciowe i aplikacje.

- 1-1: Terminologia, koncepcje i modele
- 1-2: Główny słownik terminów i definicji
- 1-3: Wskaźniki zgodności zabezpieczeń systemu
- 1-4: Cykl życia i przypadki użycia zabezpieczeń IACS

- 2-1: Stworzenie programu bezpieczeństwa IACS
- 2-2: Oceny programów bezpieczeństwa IACS
- 2-3: Zarządzanie poprawkami w środowisku IACS
- 2-4: Wymagania programu bezpieczeństwa dla dostawców usług IACS
- 2-5: Wskazówki dotyczące wdrożenia dla właścicieli aktywów IACS

- 3-1: Technologie zabezpieczeń dla systemu IACS
- 3-2: Ocena ryzyka bezpieczeństwa dla projektu systemu
- 3-3: Wymagania i poziomy bezpieczeństwa systemu

- 4-1: Wymagania dotyczące cyklu życia rozwoju bezpieczeństwa produktu
- 4-2: Techniczne wymagania dotyczące bezpieczeństwa komponentów (IACS)

Rys. 5. Budowa standardu IEC 62443 [4]

Adresaci serii norm IEC 62443, w zależności od arkusza
- **właściciele instalacji / systemów IACS**
- **dostawcy usług serwisowych / przeglądowych**
- **integratorzy systemów IACS / dostawcy usług integracyjnych**
- **dostawcy produktów automatyki / komponentów systemów IACS**

WSPÓŁPRACA W OBSZARZE CYBERBEZPIECZEŃSTWA

Aby zbudować i wdrożyć w organizacji program cyberbezpieczeństwa, należy zapewnić:
1. wsparcie ze strony najwyższego kierownictwa,
2. odpowiedni poziom finansowania,
3. wystarczające zasoby kadrowe.

U podstaw problemów z bezpieczeństwem leży brak wiedzy dotyczącej cyberzagrożeń, a programy podnoszenia świadomości i wiedzy w zakresie bezpieczeństwa są najlepszym sposobem na wzrost odporności organizacji na cyberataki.

Urząd Dozoru Technicznego w obszarze cyberbezpieczeństwa działa dla wszystkich organizacji, które korzystają z systemów teleinformatycznych i/lub przetwarzają dane osobowe, a w szczególności dla operatorów usług kluczowych.

1. Audyt cyberbezpieczeństwa w myśl ustawy o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018 r. (Dz.U. z 2018 r. poz. 1560) [1]

2. Certyfikacja
- systemów zarządzania bezpieczeństwem informacji – PN-EN ISO/IEC 27001 [3]
- systemów zarządzania ciągłością działania – PN-EN ISO 22301 [5]
- systemów zarządzania bezpieczeństwem funkcjonalnym (ang. Functional Safety Management – FSM) – PN-EN 61508 [9], PN-EN 61511 [10]

3. Szkolenia
Szkolenia UDT związane z audytem, certyfikacją oraz analizą zagrożeń w obszarze cyberbezpieczeństwa kierowane są zarówno do kadry zarządzającej, specjalistów odpowiedzialnych za cyberbezpieczeństwo, jak i pozostałych pracowników w organizacji.

Cyberbezpieczeństwo jest niezbędne w obszarze bezpieczeństwa publicznego, dlatego powinno być postrzegane jako celowy i zasadny wydatek. Cyberbezpieczeństwo to inwestycja. Krajowy System Cyberbezpieczeństwa nie może rozwijać się bez aktywnego zaangażowania UDT. Urząd Dozoru Technicznego posiada wykwalifikowaną kadrę, potencjał i możliwości realizacji zadań z tego obszaru. Przygotowany Framework UDTCyber stanowi podstawę do wdrożenia strategii cyberbezpieczeństwa, która wraz z odpowiednimi mechanizmami współpracy z Operatorami Usług Kluczowych wspiera rozwój obszaru cyberbezpieczeństwa. Jest to zadanie dla UDT.

Każdy z procesów i zadań prowadzonych przez Urząd Dozoru Technicznego to powierzona jednostce sprawa ludzi, która jest realizowana z zachowaniem terminów, bezstronnie i obiektywnie, do czego między innymi zobowiązuje nas uczestnictwo w programie TIC Council, a także z poszanowaniem przepisów prawa oraz z najwyższą starannością. Poczucie misji i sensu wspierania cyberbezpieczeństwa czyni otaczający nas świat bezpieczniejszym.

Literatura:

1. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2023 r. poz. 913) https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20230000913/U/D20230913Lj.pdf
2. National Institute of Standards Technology, NIST Cybersecurity Framework https://www.nist.gov/cyberframework, NIST SP 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations
3. PN-EN ISO/IEC 27001:2023-01 - Bezpieczeństwo Informacji, cyberbezpieczeństwo i ochrona prywatności - Zabezpieczanie informacji
4. IEC 62443 - Security for Industrial Automation and Control Systems - Bezpieczeństwo w systemach sterowania i automatyki przemysłowej. Przemysłowe sieci komunikacyjne
5. PN-EN ISO 22301:2020-04 - Bezpieczeństwo i odporność - Systemy zarządzania ciągłością działania - Wymagania
6. Dyrektywa NIS 2 2022/2555 Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32022L2555
7. Dyrektywa CER 2022/2557 Parlamentu Europejskiego i Rady (UE) z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32022L2557
8. PN-EN ISO/IEC 27002:2023-01 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -- Zabezpieczanie informacji
9. PN-EN 61508-1:2010 Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem -- Część 1: Wymagania ogólne
10. PN-EN 61511-1:2017-07 Bezpieczeństwo funkcjonalne -- Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego -- Część 1: Schemat, definicje, wymagania dotyczące systemu, sprzętu i oprogramowania

ZMIANY W NOWYM WYDANIU NORMY ISO/IEC 27001:2022-10

BEZPIECZEŃSTWO INFORMACJI, CYBERBEZPIECZEŃSTWO I OCHRONA PRYWATNOŚCI

MGR INŻ. MICHAŁ MARCZUK

Główny Specjalista ds. Certyfikacji Systemów Zarządzania
Departament Certyfikacji i Oceny Zgodności
Urząd Dozoru Technicznego

Ludzkość żyje w świecie pełnym informacji. Obok wiedzy uchodzą one za podstawowe źródło rozwoju m.in. społecznego, gospodarczego, technicznego. W XXI wieku informacje są niezwykle istotnym zasobem praktycznie każdej organizacji. Mogą one wpływać na jej rozwój, lecz także przy nieodpowiednim podejściu spowodować poważne uszczerbki w funkcjonowaniu firmy, a nawet doprowadzić do jej upadku.

Bezpieczeństwo w przemyśle petrochemicznym stanowiącym kluczowy sektor gospodarki odgrywa znaczącą rolę. Charakter procesów chemicznych oraz obecność substancji chemicznych w instalacjach wymaga aby zachowano aspekty bezpieczeństwa fizycznego jak również teleinformatycznego.

Zarządzanie bezpieczeństwem informacji pozwala na bezpieczne działania poprzez wprowadzanie zabezpieczeń, które identyfikują zagrożenia i stawiają im bariery. Międzynarodowym standardem w zarządzaniu bezpieczeństwem informacji jest norma ISO/IEC 27001.

NORMA ISO/IEC 27001

Dokument określa ramy postępowania w dostępie do wszelkich danych istotnych dla organizacji, a więc minimalizuje prawdopodobieństwo, że niepowołana osoba lub instytucja uzyska do nich dostęp w sposób nielegalny lub bez zezwolenia.

Oczywiście wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji nie jest stuprocentową ochroną, niewątpliwie zwiększa bezpieczeństwo organizacji i jej klientów, poprawia jakość procesów bezpieczeństwa oraz zwiększa świadomość pracujących w niej ludzi. Ciągłe zmiany na świecie oraz chęć popularyzacji systemu zarządzania bezpieczeństwem informacji powodują, że toczą się nieustanne prace nad nowymi wersjami normy.

Najnowszym wydaniem jest wersja ISO/IEC 27001:2022-10 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności.

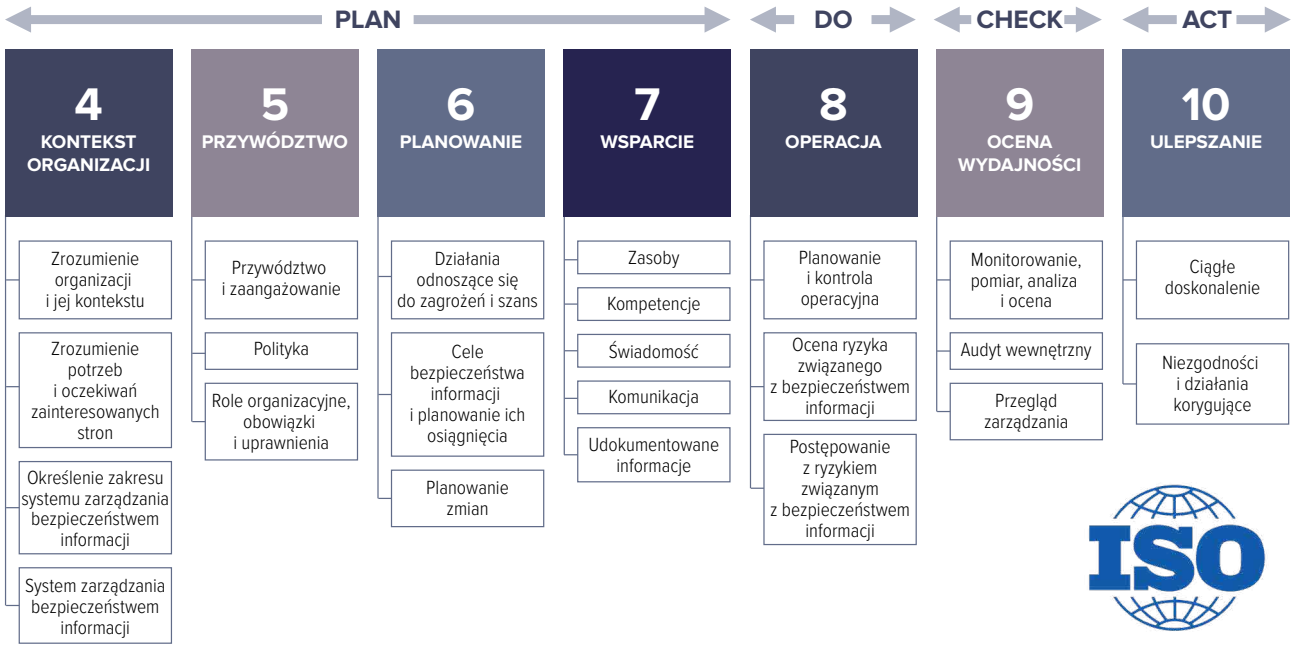
Formalnie została ona zatwierdzona 23 września 2022 r., natomiast publikacja standardu przypada na 25 października 2022 r. Niedawne wydanie standardu powoduje, że począwszy od 31 października 2022 r., organizacje z wdrożonym SZBI, które oparły swój system na poprzednim wydaniu, są niejako w okresie przejściowym.

Certyfikaty, które zostały wydane zgodnie z normą ISO/IEC 27001:2017, tracą ważność z dniem 31 października 2025 r. Do tego czasu organizacje, które mają wdrożony SZBI według ISO/IEC 27001:2017, powinny przygotować się do audytu przejścia na nowe wydanie normy. Można tego dokonać np. podczas audytu nadzoru, jako oddzielny audyt lub podczas ponownej certyfikacji.

GŁÓWNE ZMIANY W NORMIE

Co się zatem zmieniło? Ogólna struktura normy pozostała bez zmian. Dokument nadal składa się z dwóch części, tekstu, Normy oraz Załącznika A zawierającego listę zabezpieczeń.

W strukturze normy, tak jak w wydaniu z 2017 r., wyszczególniono 10 punktów odnoszących się do wymagań. Wymagania dotyczą ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia SZBI w organizacji. Podano również dostosowane do potrzeb organizacji wymagania dotyczące szacowania i postępowania z ryzykiem w bezpieczeństwie informacji. Sformułowania wymagań mają charakter ogólny, który nie narzuca konkretnych rozwiązań i jest możliwy do zastosowania w organizacjach każdego rodzaju lub wielkości. Trzeba jednak zaznaczyć, że nie dopuszcza się pominięcia żadnego z wymagań wymienionych w punktach od 4 do 10 przy założeniu, że organizacja deklaruje zgodność z omawianą Normą Międzynarodową.



Najważniejszymi zmianami ISO/IEC 27001:2022 w stosunku do poprzedniej wersji są nowe wymagania, które dotyczą ustanowienia kryteriów dla procesów operacyjnych i wdrożenia kontroli procesów. Nowe wymaganie ma zapewniać, że organizacja określa sposób komunikacji. Pojawił się też jeden nowy punkt 6.3 odnoszący się do Planowania Zmian.

Analizując punkty normy, napotykamy pierwszą zmianę, którą jest punkt 4.4 System zarządzania bezpieczeństwem informacji. Nowością w tym punkcie jest to, że organizacja powinna wdrożyć, utrzymywać i ciągle doskonalić SZBI, ale nie tylko w stosunku do procesów odnoszących się do filarów, tzn. poufności, integralności oraz dostępności. Należy też uwzględnić procesy i ich interakcje potrzebne do skutecznego wdrożenia systemu, takie jak np. audyt wewnętrzny czy przeglądy zarządzania.

Kolejną nowością jest punkt 6.3 Planowanie zmian. Jest to wymaganie, które zostało dodane jako zupełnie nowe w aktualnej wersji normy. Punkt ten odnosi się do zmian w systemie zarządzania bezpieczeństwem informacji. Jeżeli organizacja uzna za potrzebne wprowadzenie zmian w SZBI, to musi te zmiany przeprowadzać w zaplanowany sposób.

W punkcie 7.4 Komunikacja, wraz z określeniem, co należy przekazać, kiedy, z kim i kto ma się komunikować, istnieje wymóg określenia, w jaki sposób ta komunikacja będzie się odbywać. Określenie sposobu komunikacji jest wymaganiem, które odróżnia aktualną wersję standardu od wersji z 2017 r.

Biorąc pod uwagę możliwość wycieków toksycznych substancji, awarie czy nawet wypadki, prawidłowo zorganizowana forma komunikacji jest istotnym zabezpieczeniem dla realizacji procedur awaryjnych. Dobrze określone i utrzymywane sposoby komunikacji zapewniają prawidłową współpracę ze służbami lub innymi podmiotami, które mogą pomóc w zniwelowaniu skutków ewentualnego zakłócenia.

Dużo większe zmiany zaszły w Załączniku A, którego struktura została całkowicie zmieniona. Zrezygnowano ze 114 zabezpieczeń podzielonych na 14 sekcji na rzecz 93 zabezpieczeń pogrupowanych w 4 sekcjach. Taki układ załącznika jest bardziej przejrzysty i agreguje zabezpieczenia tematycznie. Punkt A5 „Organizacyjne zabezpieczenia" zawiera 37 zabezpieczeń, z czego 3 są nowe. Punkt A6 „Osobowe zabezpieczenia" pozostaje praktycznie bez zmian i zawiera 8 zabezpieczeń. Punkt A7 „Fizyczne zabezpieczenia" to zbiór 14 zabezpieczeń, w tym jedno nowe, oraz punkt 8 „Technologiczne zabezpieczenia" to zestaw 34 zabezpieczeń i w tej części otrzymujemy 7 nowych.

Aktualizacja wymagań wynika z konieczności odniesienia do najnowszych i najlepszych praktyk oraz rezygnacji z przestarzałych technologii na rzecz nowych. Przechodząc do analizy zabezpieczeń, na poziomie organizacyjnym, wprowadzono w punkcie 5.7 zabezpieczenie dotyczące analizy zagrożeń. Należy zatem identyfikować zagrożenia wewnętrzne i zewnętrzne, które mogą mieć wpływ na funkcjonowanie organizacji. Jakiego rodzaju metody i narzędzia może wykorzystać osoba atakująca, skąd można czerpać wiedzę na temat tych ataków, kto powinien gromadzić informacje pomocne przy przeciwdziałaniu oraz kto powinien je analizować. Wymaganie to nakłada na organizację wymóg wyznaczenia osoby lub zespołu, który będzie za takie działania odpowiedzialny.

Technologie chmurowe są w środowisku IT już bardzo rozpowszechnione. Umożliwiają one przetwarzanie informacji przy pomocy zasobów obliczeniowych poprzez sieć internet. Technologia ta daje ogromne możliwości, ale niesie ze sobą również wiele zagrożeń. Norma ISO/IEC 27001:2022 w odróżnieniu od poprzedniej edycji wychodzi naprzeciw tym zagrożeniom. **W punkcie A5.23 Załącznika A dodano zabezpieczenie „Bezpieczeństwo informacji do użytku w usługach w chmurze".** Zapis ten odnosi się całościowego zarządzania procesami związanymi z usługami chmurowymi, co oznacza, że bezpieczeństwo informacji powinno być brane pod uwagę na każdym etapie. Zaczynając od wyboru usługodawcy, poprzez określenie wymagań umownych oraz obowiązków dostawcy usług, kończąc na zachowaniu bezpieczeństwa informacji w trakcie trwania umowy oraz po jej zakończeniu.

Ostatnim nowym zabezpieczeniem dodanym w części organizacyjnej jest punkt A5.30 „Gotowość teleinformatyczna do zapewnienia ciągłości działania". Jest to odniesienie wprost do normy ISO IEC 22301 System Zarządzania Ciągłością Działania w kontekście systemów teleinformatycznych. Oznacza to, że kadra zarządzająca tymi systemami powinna określić w wyniku analizy BIA (Business Impact Analysys) systemy krytyczne do zapewnienia funkcjonowania organizacji. W ramach tej analizy należy też odnieść się do pojęć bezpośrednio wywodzących się z ciągłości działania – wyznaczenie punktów:

- RPO (Recovery Point Objective), czyli poziomu, do którego organizacja może pozwolić sobie na utratę danych,
- RTO (Recovery Time Objective), czyli okresu następującego po incydencie, w którym produkt i usługa lub działanie są wznawiane, a zasoby są odzyskiwane.

Poziomy tych czynników są wprost zależne od krytyczności danego systemu ICT.

ROLA BEZPIECZEŃSTWA INFORMACJI

Zapewnienie bezpieczeństwa informacji nie opiera się jedynie na zabezpieczeniu technologii informatycznych. Bezpieczeństwo fizyczne jest równie istotne. Brak zabezpieczeń w tym zakresie może doprowadzić do nieupoważnionego dostępu do informacji istotnych dla organizacji.

Niepowołane osoby poruszające się po obiekcie przemysłowym mogą stanowić zagrożenie dla siebie oraz infrastruktury. Próby podłączania zewnętrznych urządzeń lub zmiany ustawień już istniejących mogą niekorzystnie wpływać na przetwarzane procesy stanowiące podstawę działania organizacji.

Nowym zabezpieczeniem wprowadzonym w normie ISO/IEC 27001:2022 jest w punkcie A7.4 „Monitorowanie bezpieczeństwa fizycznego". Innymi słowy, należy prowadzić nadzór nad przepisami i regulacjami dotyczącymi ochrony danych w połączeniu z nadzorem wszelkich systemów ochrony fizycznej, takich jak np. systemy CCTV, RFiD, detektory ruchu, czujniki ogrodzeniowe. Stały nadzór nad nimi ogranicza możliwość wystąpienia wyżej wymienionych zagrożeń.

Najbardziej rozbudowanym jest punkt A8 stanowiący listę zabezpieczeń odnoszących się do użytej technologii informacyjnej.

Pierwszym z nowych punktów jest A8.9 „Zarządzanie konfiguracją". Istotą tego zabezpieczenia jest systemowe podejście do nadzoru nad systemami lub sprzętem komputerowym, który jest używany do przetwarzania informacji. Nieautoryzowane zmiany w ich konfiguracji mogą doprowadzić do niekontrolowanej eksploracji lub zmiany danych przez nieupoważnione osoby. Należy więc wdrożyć narzędzia, które pozwolą przede wszystkim na wymuszenie zdefiniowanych konfiguracji sprzętu czy oprogramowania, ale również na dalsze monitorowanie pod kątem zmian.

Punkt A8.10 „Usuwanie informacji" reguluje kwestię przechowywania informacji na urządzeniach lub mediach. Informacje, które nie są używane czy potrzebne, powinny zostać usunięte, żeby zapobiec niepożądanym wyciekom. Decyzja o tym, jakie dane mają zostać usunięte i w jaki sposób, powinna być zgodna z przepisami prawa, ale również z wewnętrznymi regulacjami organizacji – zgodnie z klasyfikacją informacji, która została przyjęta. Zabezpieczenie to ma zastosowanie nie tylko w przypadku nośników danych, takich jak np. dyski twarde czy urządzenia. Norma zakłada, że organizacja podejmie też stosowne kroki w tym zakresie w relacjach z dostawcami. Należy wdrożyć mechanizmy, które zapewnią, że w przypadku rozwiązania umowy z dostawcą rozwiązań chmurowych wrażliwe dane należące do organizacji także zostaną usunięte.

Usunięcie zbędnych informacji jest jednym ze sposobów na zapewnienie, że nie dostaną się w niepowołane ręce. A jeśli organizacja ich nadal potrzebuje?

Zabezpieczeniem regulującym tę kwestię może być punkt A8.11 „Maskowanie danych". Działanie prewencyjne, jakim jest maskowanie danych, ma na celu ograniczenie ekspozycji informacji w zależności od ich kontekstu. Mogą to być informacje istotne z punktu widzenia biznesu, danych osobowych, ale także relacyjnych w odniesieniu do struktur bazodanowych. W związku z powyższym, tak jak w przypadku usuwania danych, techniki, jakie zostaną użyte do maskowania, powinny być zgodnie ze zobowiązaniami prawnymi, regulacyjnymi oraz umownymi.

Działania prewencyjne, bo taki charakter mają dwa powyższe zabezpieczenia, w logiczny sposób wspomagają działania organizacji do zabezpieczenia A8.12 Zapobieganie wyciekom danych. Oczywiście, tak samo jak w poprzednich przypadkach, podstawą do podjęcia decyzji o krytyczności informacji jest ich identyfikacja oraz klasyfikacja. Kanały, którymi informacja może wyciec, są różne. Niezabezpieczone urządzenia lub systemy komputerowe, które przetwarzają informacje, nie są jedynym źródłem wycieku. Często powodem wycieku, świadomego lub nie, są ludzie. Dlatego też poza wdrożeniem systemów DLP, skutecznym sposobem na zapobieganie wyciekom jest edukacja personelu.

Obydwu zagrożeniom, jakimi są technologia i ludzie, odpowiadają dwa kolejne zabezpieczenia. Są to punkty A8.16 „Działania monitorujące" oraz A8.23 „Filtrowanie sieci". Z technicznego punktu widzenia wymagania te stanowią o konieczności działań operacyjnych skierowanych na zabezpieczenie przed złośliwym oprogramowaniem, monitorowanie systemów sieciowych i aplikacji pod kątem nietypowych zachowań czy zdolności do przystosowania się do różnych zagrożeń. Stosowanie narzędzi typu IPS, IDS, Firewalli czy systemów DLP pomaga administratorom w proaktywnym kontrolowaniu środowiska teleinformatycznego.

Z drugiej strony ustanowienie zasad bezpiecznego i odpowiedniego korzystania z zasobów internetowych czy identyfikacja typów stron internetowych jest narzędziem skierowanym do użytkowników. Regulacje w tym zakresie wraz z zapewnieniem odpowiednich szkoleń zmniejszają możliwość wykonania przez użytkowników działań niepożądanych.

W dzisiejszych czasach chyba nie ma organizacji, która by nie korzystała z różnego rodzaju oprogramowania. Należy więc przyjąć, że aplikacja jest tylko wtedy dobrze zaprojektowana i napisana, kiedy założeniem przy jej budowie będzie to, że jest potencjalnym punktem ataku. **Ostatnie z nowych zabezpieczeń w normie ISO/IEC 27001:2022 odnosi się do środowiska deweloperskiego. W punkcie A8.28 „Bezpieczne kodowanie" norma wymaga, aby organizacja określiła procesy, które zapewnią nadzór nad całym cyklem życia tworzonych aplikacji.** Należy więc wdrożyć zabezpieczenia już na etapie projektowania, zapewnić szkolenia dla programistów, tak aby stosowali najlepsze praktyki w tym zakresie, a także zapewnić bezpieczne środowisko deweloperskie. Stworzone oprogramowanie należy testować pod kątem bezpieczeństwa informacji zgodnie z dostępną wiedzą o rzeczywistych zagrożeniach. Pełny zestaw wytycznych do wdrożenia tego zabezpieczenia można odnaleźć w normie PN-EN ISO/IEC 27002:2022.

WYZWANIA BEZPIECZEŃTWA

Zmiany zachodzące we współczesnym świecie w naturalny sposób wymusiły potrzebę aktualizacji normy ISO/IEC 27001. Rozszerzone o czynniki zewnętrzne środowisko funkcjonowania, zapewnienie ciągłości działania czy uwzględnienie nowoczesnej technologii to czynniki wpływające na pogłębianie się dojrzałości branży cyberbezpieczeństwa. Nowe wydanie standardu stara się więc odpowiadać na wyzwania bezpieczeństwa informacji stawiane przed organizacjami.

CERTYFIKACJA SYSTEMÓW ZARZĄDZANIA BEZPIECZEŃSTWEM FUNKCJONALNYM

FUNCTIONAL SAFETY MANAGEMENT

WEDŁUG PN-EN 61508 ORAZ PN-EN 61511

MGR INŻ. DOROTA BAŁACHOWSKA

Kierownik Wydziału Certyfikacji
Departament Certyfikacji i Oceny Zgodności
Urząd Dozoru Technicznego

Program certyfikacji systemu zarządzania bezpieczeństwem funkcjonalnym FSM jest skierowany do producentów i użytkowników wyrobów, integratorów systemów, a także eksploatujących instalacje procesowe oraz technologiczne.

Bezpieczeństwo procesowe to dziedzina bezpieczeństwa skupiona głównie na zapobieganiu zagrożeniom występującym przy eksploatacji instalacji, w których zachodzą procesy chemiczne związane ze zmianą stanu skupienia medium bądź też z występowaniem niebezpiecznych substancji.

Bezpieczeństwo funkcjonalne to część bezpieczeństwa ogólnego odnoszącego się do instalacji lub jej części, którego zapewnienie zależy od właściwego działania odpowiednio zaprojektowanych systemów bądź urządzeń. Systemy te powinny być zaprojektowane tak, aby zadziałały we właściwy sposób w określonym czasie z uwzględnieniem możliwych błędów operatora, uszkodzeń sprzętu oraz zmian warunków środowiskowych.

CEL WDROŻENIA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM FUNKCJONALNYM

Celem wdrożenia systemu zarządzania bezpieczeństwem funkcjonalnym jest zidentyfikowanie wszystkich czynności zarządzania, które są niezbędne do zapewnienia odpowiedniego poziomu bezpieczeństwa instalacji.
W przypadku systemów o określonym poziomie SIL (ang. Safety Integrity Level) wymagany jest nie tylko odpowiedni projekt techniczny, ale również czynności związane z organizacją i zarządzaniem. Oznacza to, że poziom nienaruszalności bezpieczeństwa w systemie nie może zostać osiągnięty bez zastosowania odpowiedniej metodologii zarządzania.

URZĄD DOZORU TECHNICZNEGO

Normy dotyczące bezpieczeństwa funkcjonalnego (PN-EN 61508, PN-EN 61511) wprowadzają wymóg przeprowadzania analiz zagrożeń i oceny ryzyka.

W przemyśle procesowym często występują instalacje, które w przypadku awarii sterowania procesem stanowią poważne zagrożenie dla ludzi, mienia i środowiska. Zgodnie z dzisiejszymi standardami technicznymi w tego rodzaju instalacjach stosuje się tak zwane przyrządowe systemy bezpieczeństwa SIS (ang. Safety Instrumented System). Systemy te rozpoznają krytyczne zdarzenia i wprowadzają proces w bezpieczny stan lub utrzymują go w nim. Na podstawie analizy zagrożenia i oceny ryzyka dla każdego systemu SIS obowiązkowo określa się poziom nienaruszalności bezpieczeństwa – SIL. Istnieją cztery poziomy, przy czym SIL 1 oznacza najmniejsze, a SIL 4 największe ograniczenie ryzyka.

NA CZYM POLEGAJĄ ANALIZY ZAGROŻEŃ I OCENY RYZYKA?

Analizy zagrożeń oraz oceny ryzyka kierowane są do projektantów, integratorów, użytkowników lub właścicieli instalacji przemysłowych. Projektowanie i wytwarzanie technologicznych instalacji przemysłowych musi uwzględniać warunki zapewniające ich bezpieczną eksploatację. Dotyczy to w szczególności tych procesów przemysłowych, które wiążą się z przebiegiem reakcji chemicznych lub zmianą stanu skupienia substancji oraz stwarzają zagrożenie dla zdrowia i życia ludzkiego, jak również dla środowiska.

Zagrożenia takie występują zwłaszcza w branżach: chemicznej, petrochemicznej, energetycznej, farmaceutycznej oraz w przemyśle gazowniczym.

W obszarze bezpieczeństwa Urząd Dozoru Technicznego oferuje usługi skierowane do wszystkich organizacji. Jedną z nich jest certyfikacja systemów zarządzania bezpieczeństwem funkcjonalnym FSM (ang. Functional Safety Management) na zgodność z normą PN-EN 61508 lub PN-EN 61511.

Certyfikacja jest jednym ze sposobów zapewnienia, że poddawany jej system spełnia wymagania bezpieczeństwa i jakości określone programem certyfikacji. Zaufanie do poszczególnych programów certyfikacji systemów osiąga się dzięki akceptowanemu na całym świecie procesowi oceny oraz ponownym, okresowym ocenom w ramach nadzoru nad certyfikatem.

KORELACJA BEZPIECZEŃSTWA OGÓLNEGO, PROCESOWEGO ORAZ BEZPIECZEŃSTWA FUNKCJONALNEGO

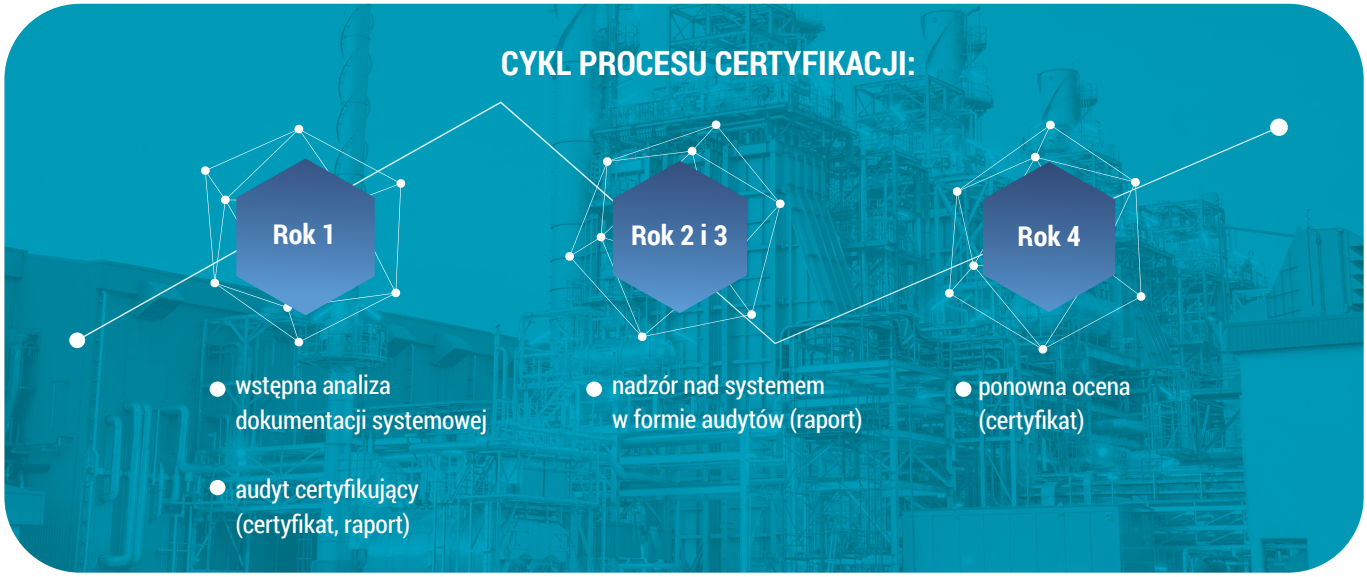
Rys. 1. Ogólny model bezpieczeństwa w przemyśle procesowym

PROCES CERTYFIKACJI

Wychodząc naprzeciw oczekiwaniom rynkowym, Jednostka Certyfikująca UDT-CERT opracowała program certyfikacji systemu zarządzania bezpieczeństwem funkcjonalnym FSM, skierowany do producentów i użytkowników wyrobów, integratorów systemów, a także eksploatujących instalacje procesowe oraz technologiczne. Program certyfikacji opublikowany jest na stronie internetowej www.udt.gov.pl. Normy PN-EN 61508, PN-EN 61511 i inne definiują wymagania dotyczące zarządzania bezpieczeństwem funkcjonalnym, oceny bezpieczeństwa funkcjonalnego oraz dokumentacji tych procedur. Bezpieczeństwo funkcjonalne jest rozumiane jako ogólne podejście do wszystkich działań w cyklu życia bezpieczeństwa systemów zawierających elektryczne i/lub elektroniczne, i/lub programowalne elektroniczne elementy składowe

Na czym polega bezpieczeństwo?

Bezpieczeństwo zależy nie tylko od właściwego prowadzenia procesów i eliminowania sytuacji, w których ludzie mogą być narażeni na zagrożenia, ale również na zapobieganiu potencjalnym zagrożeniom w organizacji. Zapewnienie bezpieczeństwa i ochrony obiektów to dwie współistniejące, uzupełniające się i wzmacniające strategie ogólnego bezpieczeństwa [1].



Rys. 2. Cykl procesu certyfikacji

99

Proces certyfikacji ma na celu ocenę wdrożenia oraz skuteczności funkcjonowania systemu zarządzania. Realizowany jest w 3-letnim cyklu uwzględniającym nadzór nad wydanym certyfikatem. Audyt certyfikujący, realizowany w pierwszym roku cyklu, poprzedzony jest analizą dokumentacji klienta, również w kontekście zakresu jego działalności. Powyższa analiza umożliwia zarówno ocenę stopnia gotowości klienta do audytu, jak i zrozumienie systemu zarządzania klienta w zakresie normy dotyczącej systemu zarządzania bezpieczeństwem funkcjonalnym przez jednostkę certyfikującą.

CO OBEJMUJE CERTYFIKACJA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM FUNKCJONALNYM?

Certyfikacja systemu zarządzania bezpieczeństwem funkcjonalnym obejmuje:

- określenie wymaganych działań technicznych podczas każdej fazy cyklu życia instalacji procesowej w celu osiągnięcia wymaganego poziomu bezpieczeństwa,
- określenie ról i obowiązków zaangażowanych pracowników, wydziałów i organizacji odpowiedzialnych za każdą istotną fazę cyklu życia (zgodnie z obowiązującym schematem organizacyjnym),
- określenie środków organizacyjnych w celu efektywnego wykonywania wymagań technicznych.

Proces certyfikacji realizowany jest na podstawie niżej wymienionych dokumentów odniesienia:

- PN-EN 61508-1. Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem – Część 1: Wymagania ogólne,
- PN-EN 61511-1. Bezpieczeństwo funkcjonalne – Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego – Część 1: Schemat, definicje, wymagania dotyczące systemu, sprzętu i oprogramowania.

UDT-CERT przeprowadza procesy certyfikacji systemów zarządzania bezpieczeństwem funkcjonalnym oraz zatrudnia wykwalifikowanych audytorów posiadających odpowiednie kompetencje. Zespół audytorów UDT dysponuje zarazem możliwościami technicznymi do przeprowadzania ocen oraz niezbędną wiedzą w wymaganym obszarze.

Korzyści wynikające z certyfikacji systemów zarządzania bezpieczeństwem funkcjonalnym:

- poprawa efektywności organizacji dzięki certyfikowanemu systemowi zarządzania bezpieczeństwem funkcjonalnym
- zaangażowanie organizacji w redukcję ryzyka – certyfikacja przeprowadzona dla wszystkich faz cyklu bezpieczeństwa
- potwierdzenie kompetencji – spełnianie wymagań określonych w normach PN-EN 61508 i PN-EN 61511
- certyfikowany FSM potwierdza, że produkt/system jest zgodny z normami oraz że procesy zarządzające cyklem życia produktu/systemu przeprowadzono według tych norm – potwierdzenie przez niezależną stronę trzecią

GWARANCJA POZIOMU BEZPIECZEŃSTWA

W świetle wzrastającej złożoności procesów produkcyjnych oraz rosnących kosztów inżynierskich efektywna inżynieria jest kluczowym czynnikiem w przemyśle procesowym. Cały proces powinien zapewnić skuteczne współdziałanie wszystkich elementów automatyki z systemem informacyjnym odpowiedzialnym za sterowanie, podatnym na zdarzenia zachodzące w ich środowisku. Spójność systemów prowadzi w sposób bezpośredni do minimalizacji nakładów inwestycyjnych czy kosztów eksploatacyjnych, ale przede wszystkim znacząco wpływa na poprawę niezawodności świadczenia usług.

Bezpieczeństwo procesowe, rozumiane jako brak niemożliwego do zaakceptowania ryzyka dla zdrowia, życia lub strat w majątku czy środowisku naturalnym, ma szczególne znaczenie w przemyśle chemicznym, petrochemicznym, gazowniczym i w energetyce. Jest integralną częścią ogólnego bezpieczeństwa, odnosi się szczególnie do instalacji procesowych zawierających i przerabiających substancje chemiczne.

Bezpieczeństwo procesu produkcyjnego dotyczy bezpieczeństwa zarówno pracowników, jak i procesów technologicznych. Wiąże się to z takim zaprojektowaniem i wykonaniem technologicznych instalacji przemysłowych, które uwzględnia zapewnienie warunków dla ich bezpiecznego działania.

Współczesna gospodarka opiera się na wykorzystywaniu bardzo wielu różnorodnych technologii, które wykształciły specyficzne środowisko pracy. Obserwujemy nieodwracalny progres cywilizacyjny i technologiczny napędzany nieustannym dążeniem do innowacyjności. Konsekwencją tak dużego postępu gospodarczego jest ujawnienie się różnego rodzaju zagrożeń wywołanych działalnością człowieka [2].

Poprawa efektywności organizacji dzięki certyfikowanemu systemowi zarządzania bezpieczeństwem funkcjonalnym to główny powód, dla którego warto przeprowadzić ocenę. Posiadanie certyfikatu UDT-CERT – poza prestiżem (certyfikat renomowanej marki uznawany w kraju oraz w środowisku międzynarodowym) – pozwala budować zaufanie w gronie inwestorów i klientów. Wzrost konkurencyjności ściśle wiąże się z zapewnieniem właściwego środowiska pracy. Każdy z procesów certyfikacji prowadzonych przez UDT-CERT to powierzona jednostce sprawa ludzi, która jest realizowana z zachowaniem terminów, bezstronnie i obiektywnie, z poszanowaniem przepisów prawa oraz pełną starannością.

Certyfikat, w odróżnieniu od innego rodzaju potwierdzeń kompetencji, wydaje wyłącznie niezależna strona trzecia. Stanowi to gwarancję odpowiedniego poziomu bezpieczeństwa w organizacji, ma bezpośredni wpływ na jakość usług oferowanych przez firmę oraz przyczynia się do wzrostu poziomu bezpieczeństwa technicznego w wielu dziedzinach gospodarki. Wyznacznikiem sukcesu na rynku jest z jednej strony zaspokojenie potrzeb klienta, a z drugiej zapewnienie, że wyrób cechuje się odpowiednią jakością i własnościami użytkowymi.

Z wielu względów certyfikacja systemów zarządzania, zarówno na etapie wytwarzania, jak i eksploatacji, jest obecnie wysoce ceniona, a często wprost wymagana.

Literatura:

1. Markowski A.S., Bezpieczeństwo procesów przemysłowych, Łódź 2017.
2. Pruszkowski L., HAZOP jako metoda wspomagająca zarządzanie bezpieczeństwem procesowym w przedsiębiorstwie, „Acta Universitatis Nicolai Copernici. Zarządzanie" 2015, t. 42, nr 3.

CYBERBEZPIECZEŃSTWO

KOMPLEKSOWA OFERTA UDT-CERT

- audyt cyberbezpieczeństwa
- certyfikacja wg ISO/IEC 27001
- certyfikacja wg ISO 23001
- certyfikacja Functional Safety Management System
- cyber HAZOP
- **NOWOŚĆ** spełnienie wymagań dyrektywy NIS 2

SPRAWDŹ OFERTĘ UDT-CERT!