CHEMIA 4.0

BIULETYN PROJEKTU

nr 2/2023 | grudzień 2023

Przemysłowa sztuczna inteligencja: jakie przyniesie zmiany i korzyści? s. 2

Planowane regulacje w obszarze wykorzystywania sztucznej inteligencji s. 4

NIS 2 – nowe oblicze cyberbezpieczeństwa w Unii Europejskiej s. 10

PIPC POLSKA IZBA PRZEMYSŁU CHEMICZNEGO 1988-2023 35 lat

www.pipc.org.pl/projekt-chemia-4-0/ | www.pipc.org.pl

WIĘCEJ INFORMACJI:
www.pipc.org.pl/projekt-chemia-4-0/

PROJEKT CHEMIA 4.0 2023

PIPC POLSKA IZBA PRZEMYSŁU CHEMICZNEGO 1988-2023 35 lat

Chemia 4.0

Partner Strategiczny

ABB

Partner Główny

Dräger

Patroni Merytoryczni

NASK

URZĄD DOZORU TECHNICZNEGO

Więcej o Projekcie Chemia 4.0

www.pipc.org.pl/projekt-chemia-4-0/

W numerze

Przemysłowa sztuczna inteligencja: jakie przyniesie zmiany i korzyści?
ABB POLSKA **2**

Planowane regulacje w obszarze wykorzystywania sztucznej inteligencji
KANCELARIA SKS **4**

NIS 2 – nowe oblicze cyberbezpieczeństwa w Unii Europejskiej
NASK **10**

Ocena ryzyka a odporność sieci i systemów informatycznych na incydenty cyberbezpieczeństwa
URZĄD DOZORU TECHNICZNEGO **14**

Smart Safety: Więcej danych to większe bezpieczeństwo
DRÄGER POLSKA **20**

Predykcja zużycia urządzeń ciśnieniowych i planowanie inspekcji z wykorzystaniem metodologii RBI (*Risk-based Inspection*)
URZĄD DOZORU TECHNICZNEGO **26**

Cyfrowa i bezpieczna chemia – pierwsza edycja formatu „Workshops&Networking PIPC" za nami
POLSKA IZBA PRZEMYSŁU CHEMICZNEGO. **32**

Biuletyn Projektu Chemia 4.0 2/2023

Wydawca:
Polska Izba Przemysłu Chemicznego,
ul. Śniadeckich 17, 00-654 Warszawa
e-mail: pipc@pipc.org.pl, media@pipc.org.pl
www.pipc.org.pl/projekt-chemia-4-0/
www.pipc.org.pl

Redakcja: Zespół PIPC

Realizacja projektu i skład: IT WORKS / itworks.net.pl

Wydawca wyraża zgodę na nieograniczone wykorzystywanie publikowanych treści przez Partnerów Projektu Chemia 4.0 oraz Członków Polskiej Izby Przemysłu Chemicznego.

Warunkiem wykorzystania treści przez podmioty wymienione w zdaniu poprzednim jest wskazanie źródła cytowania wraz z linkiem do publikacji.

PRZEMYSŁOWA SZTUCZNA INTELIGENCJA: JAKIE PRZYNIESIE ZMIANY I KORZYŚCI?

Dynamiczny rozwój sztucznej inteligencji (AI) sprawia, że stoimy u progu wkroczenia w erę przemysłu 5.0. Choć wiele mówi się o zagrożeniach, to w praktyce wykorzystanie technologii AI może przynieść wiele korzyści: od zwiększenia efektywności energetycznej po nową jakość w utrzymaniu ruchu. Wszystko za sprawą wsparcia w analizie danych, co pomoże w podejmowaniu lepszych decyzji, zapobiegających m.in. awariom i przestojom.

W dynamicznie zmieniającym się świecie przemysłu cyfryzacja staje się jednym z kluczowych czynników sukcesu. Jeszcze kilka lat temu sztuczna inteligencja była traktowana jako kolejna niedojrzała technologia, za to dziś jest to rozwiązanie, na które zwrócone są oczy całego świata. Priorytety i cele biznesowe, które wcześniej napędziły rozwój Przemysłowego Internetu Rzeczy (IIoT), ukazują prawdziwy potencjał tej rewolucji cyfrowej.

Eksperci firmy ABB zapowiadają, że wdrożenie AI usprawni eksploatację oraz umożliwi holistyczne zarządzanie aktywami i efektywne wykorzystanie dostępnych zasobów. To nie tylko zmieni procesy biznesowe, ale również przyniesie nowe możliwości w zakresie zrównoważonego rozwoju, operacyjnej doskonałości i optymalizacji.

W praktyce oznacza to, że organizacje, które szybciej wyjdą poza etap koncepcji oraz zaangażują się we wdrożenie przemysłowej sztucznej inteligencji i aplikacji IIoT, nie tylko zwiększą swoją konkurencyjność, ale także przystosują się do dynamicznie zmieniającego się otoczenia biznesowego.

Klucz do sukcesu? Jeszcze więcej wartości z danych

Potęga sztucznej inteligencji tkwi bowiem w jej zdolności do analizy ogromnych ilości danych, generowanych m.in. przez urządzenia i systemy w zakładach przemysłowych. Obecnie większość z tych informacji nie jest skutecznie wykorzystywana. By to zmienić, AI dla przemysłu rozwija się w dwóch kluczowych kategoriach: sztucznej inteligencji analitycznej i sztucznej inteligencji generatywnej (GenAI).

Pierwszy rodzaj AI obejmuje uczenie maszynowe, umożliwiające przetwarzanie danych, analizę wzorców i podejmowanie decyzji na podstawie historii danych. To kluczowe narzędzie do prognozowania, optymalizacji procesów i zarządzania aktywami. Z kolei, GenAI koncentruje się na generowaniu treści, takich jak: teksty czy obrazy. Zastosowanie GenAI, podobnie jak w przypadku algorytmów wykorzystywanych w asystencie ChatGPT, może rewolucjonizować sposób, w jaki korzystamy z danych w przemyśle, wprowadzając innowacje i tworząc nowe perspektywy dla rozwoju.

Firm ABB razem z koncernem Microsoft pracują nad wdrożeniem nowej platformy dla przemysłu, która łączy w sobie wspomniane, dwa rodzaje sztucznej inteligencji. Technologia usprawni zarówno zbieranie, weryfikację i analizę danych, jak i zautomatyzuje na ich podstawie proces wnioskowania. By tego dokonać, ABB zintegruje cyfrową platformę dla przemysłu ABB Ability™ Genix z usługami Azure OpenAI Microsoftu.

Mowa o dużych modelach językowych *(Large Language Model* – LLM), takich jak GPT-4, na którym bazuje asystent ChatGPT Plus. ABB zasili je wiedzą technologiczną na temat funkcjonowania aplikacji przemysłowych z całego świata oraz informacjami m.in. o tym, jak działają urządzenia, jakie symptomy świadczą o zbliżającej się awarii, czy w jaki sposób optymalizować procesy, by obniżyć koszty produkcji.

Z połączenia ABB Ability™ Genix oraz Azure Open AI Service powstanie platforma Genix Copilot, naszpikowana zaawansowanymi narzędziami do wnioskowania oraz algorytmami uczenia maszynowego. Warstwa GenAI oparta na GPT-4 umożliwi

generowanie kodów, obrazów i tekstów w czasie rzeczywistym na bazie otrzymanych danych z aplikacji przemysłowych. – *W kontekście przemysłu, połączenie tych dwóch rodzajów sztucznej inteligencji może przyspieszyć innowacje, usprawnić procesy produkcyjne, a także zrewolucjonizować obszary takie jak: utrzymanie ruchu, zwiększenie wydajności urządzeń, a także zmniejszenie zużycia energii* – **mówi Piotr Szkoda, dyrektor biznesu Automatyki Procesowej ABB w Polsce.**

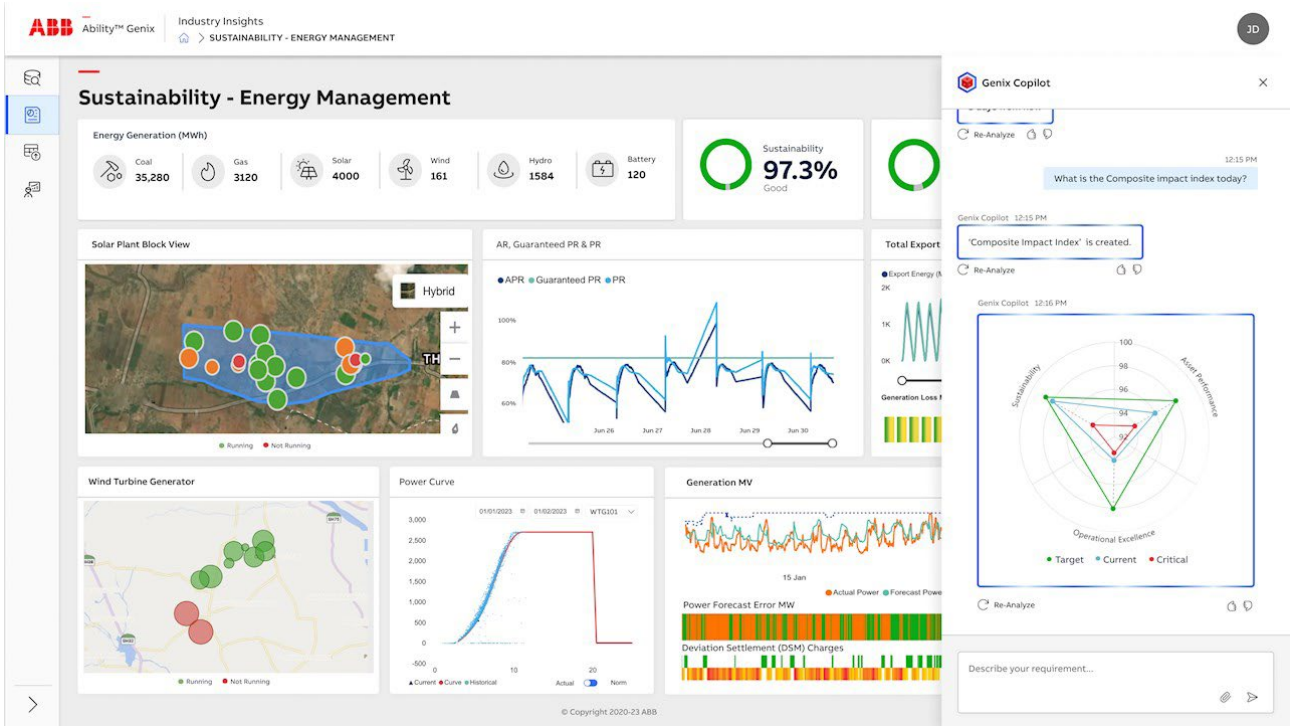
Genix będzie tworzyć modele pracy poszczególnych urządzeń wykorzystywane do skuteczniejszego monitoringu, predykcji i przewidywania awarii. Wśród możliwości tej technologii będzie także podpowiadanie operatorowi, jak powinien zachować się w danej sytuacji, by usprawnić i zoptymalizować proces technologiczny – *Inną korzyścią, w której widzę duży potencjał, są funkcje doradcze, czyli doradzanie serwisantowi lub operatorowi, w jaki sposób prowadzić proces i co należy zrobić „krok po kroku", by uzyskać pożądany efekt* – dodaje Piotr Szkoda.

Nieograniczone możliwości i mierzalne efekty

ABB ocenia, że platforma Genix Copilot dostarczy informacji zwrotnych w zakresie monitoringu i predykcji, które przełożą się na mierzalne efekty w postaci wydłużenia cyklu życia urządzeń o 20 proc. oraz zmniejszenie nieplanowanych przestojów aż do 60. proc. co jednocześnie pomoże przedsiębiorstwom uniknąć ogromnych strat finansowych. Narzędzie może być również wsparciem w procesie transformacji energetycznej w ramach monitoringu i optymalizacji w zakresie zużycia energii oraz emisji, a także wspomoże bezpieczny przepływ informacji wewnątrz przedsiębiorstwa.

W rozwoju platformy największym wyzwaniem będzie pozyskanie wartościowych informacji do jej zasilenia. – *Punktem wyjścia do analizy i wnioskowania AI są dane, podobnie, jak w przypadku asystenta ChatGPT. Jednak, gdy mówimy o platformie Genix, musimy pamiętać, że potrzebujemy specjalistycznej wiedzy, która nie jest powszechnie dostępna np. w Internecie. Ponadto chcemy, by nasze narzędzie czerpało z doświadczenia specjalistów i producentów urządzeń. Im większą ilością danych zasilimy platformę, tym lepsze wnioski i funkcjonalności otrzymamy* – mówi Piotr Szkoda z ABB.

Platforma Genix integruje dane z trzech obszarów: operatorskiego (OT – systemy sterowania), informatycznego (IT – systemy ERP) i inżynieryjnego (ET – narzędzia projektowe). Będzie można uruchomić ją w chmurze, na konkretnej maszynie lub w infrastrukturze IT przedsiębiorstwa.



Genix Copilot interfejs użytkownika

PLANOWANE REGULACJE W OBSZARZE WYKORZYSTYWANIA SZTUCZNEJ INTELIGENCJI

Ostatnio bardzo dużo mówi się o sztucznej inteligencji („**SI**") i jej wpływie na transformację cyfrową przemysłu. Projektowane europejskie regulacje w obszarze wykorzystania SI są niezwykle istotne dla całej europejskiej gospodarki. W nowych technologiach i usługach opartych o SI upatruje się szansy na rozwój przemysłowy oraz badawczy gospodarek Unii Europejskiej. Przewiduje się, że SI może przynieść oszczędności w wielu sektorach oraz pobudzić unijną gospodarkę. Istnieją jednakże duże obawy, aby nowe planowane akty prawne nie zaszkodziły rozwojowi SI i nie spowolniły jej potencjału innowacyjnego.

Ujednolicenie przepisów o SI

Ustawodawca unijny dąży do ujednolicenia podejścia do stworzenia standardów wykorzystania SI w Europie (a może i na świecie), w konsekwencji czego powstał pakiet (projektów) aktów prawnych odnoszący się do SI. Projektowane unijne akty prawne można podzielić na akty zawierające: (a) podstawowe przepisy dotyczące systemów SI (projekt Rozporządzenia w sprawie SI), (b) nowe przepisy dotyczące kwestii odpowiedzialności za SI (projekt Dyrektywy o Odpowiedzialności za SI) czy (c) aktualizację sektorowych przepisów w zakresie SI np. dot. odpowiedzialności za produkty wadliwe.

Rozporządzenie w sprawie SI

Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji i zmieniające niektóre akty ustawodawcze Unii Europejskiej[1] („**Rozporządzenie w sprawie SI**") ma być odpowiedzią UE na wyzwania i ryzyka związane z rozwojem SI. W chwili pisania tego artykułu trwają intensywne prace – w ramach tzw. trilogu (tj. trójstronnych negocjacji międzyinstytucjonalnych, w których biorą udział przedstawiciele Parlamentu Europejskiego, Rady Unii Europejskiej i Komisji Europejskiej) – nad projektem Rozporządzenia w sprawie SI. Data

1 Tekst projektu opublikowanego na dzień 14 czerwca 2023r.: https://www.europarl.europa.eu/doceo/document/TA-9-2023-06-14_EN.html#sdocta6 (dostęp: 1.12.2023 r.)

zakończenia negocjacji nie jest znana, ale **oczekuje się, że przyjęcie Rozporządzenia w sprawie SI nastąpi jeszcze w tym roku lub na początku 2024 roku**. **W takim przypadku Rozporządzenie w sprawie SI weszłoby w życie w połowie 2024 r., po czym rozpocząłby się dwuletni okres przejściowy**. Ze względu na toczące się nadal burzliwe dyskusje w ramach trilogu, również w odniesieniu do takich kluczowych kwestii jak definicja systemu SI, trudno przewidzieć jaki będzie ostateczny kształt Rozporządzenia w sprawie SI.

Celem Rozporządzenia w sprawie SI jest ustanowienie przepisów horyzontalnych dotyczących systemów SI oraz zapewnienie, aby systemy te wprowadzane do obrotu w UE były bezpieczne i zgodne z obowiązującym prawem w obszarze praw podstawowych oraz z unijnymi wartościami. Obecne podejście do systemów SI opiera się na stworzeniu czterech kategorii poziomów ryzyka w SI: **niedopuszczalnego, wysokiego, ograniczonego lub minimalnego (braku) ryzyka**. Najbardziej restrykcyjnie mają być traktowane systemy niedopuszczalnego ryzyka, których użycie ma być całkowicie zakazane. Wśród takich systemów (**zakazanych praktyk w zakresie systemów SI**) wymienia się:

- techniki podprogowe, manipulacyjne i wprowadzające w błąd, wpływające na decyzje użytkowników
- implementujące „scoring społeczny"
- kategoryzujące biometrycznie osoby fizyczne według ich cech
- wspomagające identyfikację biometryczną w miejscach publicznych
- tworzące bazy danych na podstawie rozpoznawania twarzy w internecie i kamerach CCTV
- rozpoznające emocje w obszarze kontroli granic
- ocena ryzyka zachowań karalnych.

Natomiast za **systemy SI wysokiego ryzyka** uznane zostały te, które mogą wpływać negatywnie na bezpieczeństwo lub chronione prawa podstawowe, jeżeli taki system SI jest przeznaczony do wykorzystywania jako związany z bezpieczeństwem element produktu objętego unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku II lub sam jest takim produktem; oraz produkt, którego związanym z bezpieczeństwem elementem jest system SI, lub sam system SI jako produkt podlegają – na podstawie unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku II – ocenie zgodności przeprowadzanej przez osobę trzecią w celu wprowadzenia tego produktu do obrotu lub oddania go do użytku. Oprócz systemów SI wysokiego ryzyka, o których mowa powyżej, za systemy wysokiego ryzyka uznaje się również systemy SI, wspomniane w załączniku III. **Systemami SI wysokiego ryzyka mogą być zatem:**

- SI jako komponent bezpieczeństwa w niektórych produktach
- identyfikacja biometryczna (za wyjątkiem potwierdzenia tożsamości)
- zarządzanie niektórą infrastrukturą krytyczną
- rekrutacja, awanse i zakończenie umów z pracownikami
- ocena kredytowa
- ocena na potrzeby ubezpieczeń i ochrony zdrowia
- ocena wiarygodności zgłoszeń alarmowych
- systemy wspierające stosowanie prawa przez organy sądowe i administracyjne
- systemy rekomendacji treści dla bardzo dużych platform społecznościowych[2]
- wpływanie na zachowania wyborców

Rozporządzenie w sprawie SI określa również **obowiązki, które mają zastosowanie do wszystkich systemów SI**, takie jak:

- przewodnia i nadzorcza rola człowieka
- techniczna solidność i bezpieczeństwo
- prywatność i należyte zarządzanie danymi
- przejrzystość – identyfikowalność i wyjaśnialność procesów
- badanie długotrwałego wpływu na środowisko, jednostkę, społeczeństwo i demokrację
- niedyskryminacja

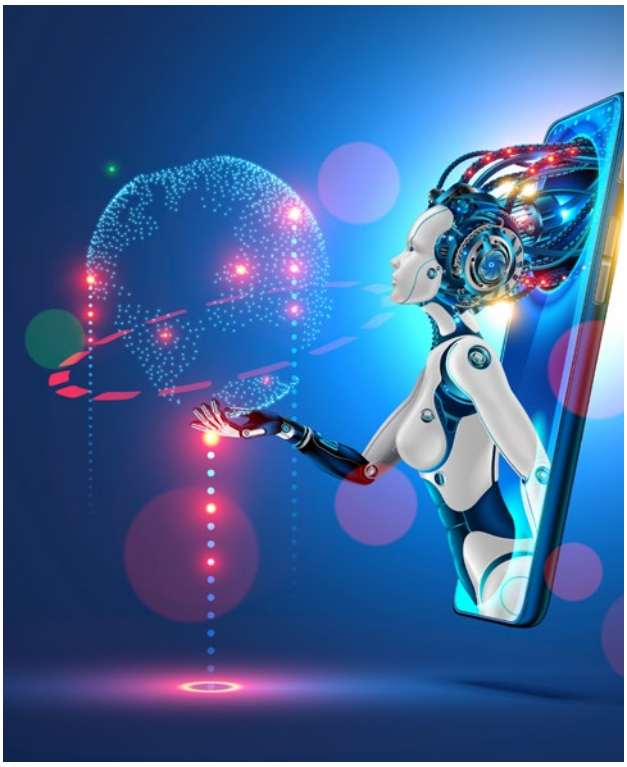
oraz (liczne) **obowiązki, które mają zastosowanie do dostawców oraz operatorów systemów wysokiego ryzyka**. **Na dostawców systemów wysokiego ryzyka nałożono przede wszystkim obowiązek** wdrożenia systemów zarządzania ryzykiem w całym cyklu życia SI, prowadzenia dokumentacji technicznej i rejestrowanie zdarzeń, zarządzanie danymi treningowymi, walidacyjnymi i testowymi, dostarczania zrozumiałych instrukcji (transparentność działania), wdrożenia nadzoru człowieka (kompetentnej osoby),

2 Alibaba, Amazon, Booking, Facebook, Google, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, Zalando

rejestracji w unijnej bazie danych czy informowania o niezgodnościach i incydentach. **Na operatorów SI nałożono m.in. obowiązek** zapewnienia używania SI zgodnie z instrukcją, informowania dostawców o incydentach, prowadzenia stałego monitoringu odporności i cyberbezpieczeństwa, wdrożenia nadzoru człowieka czy zapewnienia adekwatności danych wejściowych.

Rozporządzenie w sprawie SI będzie miało zastosowanie do:

- dostawców (eng. *provider*) wprowadzających do obrotu lub oddających do użytku systemy SI w UE, niezależnie od tego, czy dostawcy ci mają siedzibę w UE, czy w państwie trzecim;
- operatorów SI (eng. *deployer*), którzy mają siedzibę w UE;
- dostawców i operatorów SI, którzy znajdują się w państwie trzecim, jeżeli wyniki działania systemu SI są wykorzystywane w UE.



Dyrektywa o Odpowiedzialności za SI

Celem projektu dyrektywy Parlamentu Europejskiego i Rady w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji (dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję,[3] „**Dyrektywa o Odpowiedzialności za SI**") jest harmonizacja prawa dotyczącego **niektórych aspektów pozaumownej odpowiedzialności cywilnej za szkody powstałe w wyniku działania systemów SI** (szkody spowodowane wynikiem uzyskanym przez system SI lub faktem nieuzyskania przez taki system wyniku, jeżeli należało go uzyskać). Podmiotem odpowiedzialnym może być zarówno dostawca jak i operator SI. Obecne krajowe przepisy dotyczące odpowiedzialności cywilnej nie są dostosowane do kwestii roszczeń z tytułu odpowiedzialności za szkody spowodowane przez produkty i usługi wykorzystujące systemy SI.

Projekt Dyrektywy o Odpowiedzialności za SI odnosi się do dwóch ważnych kwestii, ustanawiając wspólne zasady dotyczące:

- **ujawniania dowodów dotyczących systemów SI wysokiego** ryzyka, aby umożliwić powodowi uzasadnienie pozaumownego cywilnoprawnego roszczenia odszkodowawczego **opartego na zasadzie winy**. Regulacja ta ma na celu umożliwienie identyfikacji osób potencjalnie ponoszących odpowiedzialność oraz odpowiednich dowodów na potrzeby roszczenia. Sąd w takim przypadku będzie mógł nakazać ujawnienie odpowiednich dowodów dotyczących konkretnych systemów SI wysokiego ryzyka, co do których istnieje podejrzenie, że spowodowały szkodę – jednakże tylko w ograniczonym zakresie, tj. wyłącznie w zakresie niezbędnym do uzasadnienia takiego roszczenia. W przypadku, gdy pozwany nie zastosuje się do nakazu ujawnienia dowodów **sąd zastosuje domniemanie, że pozwany nie zastosował się do obowiązku dochowania należytej staranności (sąd domniemywa winę pozwanego)**.
- **ciężaru dowodu** w przypadku pozaumownych cywilnoprawnych roszczeń odszkodowawczych opartych na zasadzie winy wnoszonych do sądów krajowych z tytułu szkód spowodowanych przez system sztucznej inteligencji (**domniemanie istnienia związku przyczynowego** w przypadku winy polegającej na niedopełnieniu obowiązku dochowania należytej staranności zgodnie z prawem unijnym lub krajowym).

3 Tekst projektu dostępny na: https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52022PC0496; (dostęp: 1.12.2023 r.)

W przypadku wejścia w życie Dyrektywy o Odpowiedzialności za SI każde państwo członkowskie będzie zobowiązane do implementacji nowych regulacji do swojego porządku krajowego **w ciągu dwóch lat**. Co istotne, projekt Dyrektywy o Odpowiedzialności za SI dopuszcza, że państwa członkowskie mogą przyjąć lub utrzymać w mocy przepisy krajowe, które są korzystniejsze dla powodów w zakresie uzasadniania pozaumownego cywilnoprawnego roszczenia odszkodowawczego z tytułu szkody spowodowanej przez system SI, pod warunkiem, że takie przepisy są zgodne z prawem UE. **Projekt Dyrektywy o Odpowiedzialności za SI nie zawiera przepisów dotyczących odpowiedzialności karnej**.

Dyrektywa w sprawie odpowiedzialności za produkty wadliwe

Celem projektu dyrektywy Parlamentu Europejskiego i Rady w sprawie odpowiedzialności za produkty wadliwe[4] („**Dyrektywa w sprawie odpowiedzialności za produkty wadliwe**") jest dostosowanie istniejących przepisów do zmian wynikających m.in. z trwającej transformacji ekologicznej i cyfrowej, w szczególności w kontekście nieadekwatności istniejących obecnie definicji i pojęć do nowoczesnych produktów występujących na rynku, w szczególności produktów cyfrowych oraz produktów materialnych wspieranych przez usługi cyfrowe.

Ustawodawca unijny zdecydował się – dla celów stosowania odpowiedzialności na zasadzie ryzyka – na uzupełnienie definicji „produktu" o **oprogramowanie** (takie jak systemy operacyjne, oprogramowanie układowe, programy komputerowe, **aplikacje lub systemy AI) i cyfrowe pliki produkcyjne**. Doprecyzowano także w jakich przypadkach usługa cyfrowa związana z produktem będzie stanowić jego część składową. **Za produkt wadliwy będzie mógł zostać zatem uznany nie tylko przedmiot, ale też produkt elektroniczny.**

Na gruncie Rozporządzenia odpowiedzialnością zostali objęci: (a) producenci produktu/części składowej; (b) importerzy; (c) podmioty modyfikujące produkt; lub (d) dystrybutorzy.

Ustawodawca unijny – aktualizując sektorowe przepisy – nie zapomina również o odniesieniu się do kwestii wykorzystania SI w produktach czy usługach. Warto przywołać w tym miejscu rozporządzenie w sprawie ogólnego bezpieczeństwa produktów oraz rozporządzenie w sprawie maszyn.

Rozporządzenie w sprawie ogólnego bezpieczeństwa produktów

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/988 z dnia 10 maja 2023 r. w sprawie ogólnego bezpieczeństwa produktów, zmieniające rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 i dyrektywę Parlamentu Europejskiego i Rady (UE) 2020/1828 oraz uchylające dyrektywę 2001/95/WE Parlamentu Europejskiego i Rady i dyrektywę Rady 87/357/EWG[5] („**Rozporządzenie w sprawie ogólnego bezpieczeństwa produktów**") weszło w życie 12 czerwca 2023 r., a **będzie bezpośrednio stosowane w państwach członkowskich od 13 grudnia 2024 r.** Rozporządzenie ma sprostać wyzwaniom związanym z bezpieczeństwem produktów związanym z zastosowaniem nowych technologii, w tym wykorzystaniem sztucznej inteligencji i urządzeń podłączonych do sieci.

Zgodnie z motywem 23 Rozporządzenia w sprawie ogólnego bezpieczeństwa produktów „(…) w ocenie bezpieczeństwa produktów należy uwzględnić ryzyko dla zdrowia stwarzane przez cyfrowo połączone produkty, w tym dla zdrowia psychicznego, zwłaszcza konsumentów podatnych na zagrożenia, w szczególności dzieci. *W związku z tym podczas oceny bezpieczeństwa cyfrowo połączonych produktów, które mogłyby mieć wpływ na dzieci, producenci powinni zapewnić, aby produkty, które udostępniają na rynku, spełniały* już w fazie projektowania *najwyższe normy bezpieczeństwa, ochrony i prywatności, w najlepszym interesie dzieci. Ponadto jeżeli dla zapewnienia bezpieczeństwa produktów dla danej kategorii osób niezbędne są szczegółowe informacje,* w ocenie bezpieczeństwa produktów należy uwzględnić obecność tych informacji i ich dostępność. *Bezpieczeństwo wszystkich produktów należy oceniać z uwzględnieniem konieczności*

4 Tekst projektu dostępny na: EUR-Lex - 52022PC0495 - EN - EUR-Lex (europa.eu); (dostęp: 1.12.2023 r.)

5 Tekst Rozporządzenia dostępny na: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32023R0988; (dostęp: 1.12.2023 r.)

zapewnienia bezpieczeństwa produktu przez cały okres jego używania."

Ustawodawca unijny uznał również, że nowe technologie mogą istotnie zmodyfikować oryginalny produkt, na przykład w drodze aktualizacji oprogramowania; należy go zatem poddać **nowej ocenie ryzyka jeżeli ta istotna modyfikacja miałaby wpływ na bezpieczeństwo produktu**.

Rozporządzenie w sprawie maszyn

Nowe 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[6] („**Rozporządzenie w sprawie maszyn**"), które weszło w życie 19 lipca 2023 r., a **będzie bezpośrednio stosowane w państwach członkowskich od 20 stycznia 2027 r**. ma na celu m.in. dostosowanie przepisów do szybko rozwijających się technologii, takich jak digitalizacja i SI.

Zgodnie z założeniami ustawodawcy unijnego Rozporządzenie w sprawie maszyn oraz projektowane Rozporządzenie w sprawie SI powinny się wzajemnie uzupełniać. Zgodnie z motywem 12 Rozporządzenia w sprawie maszyn, Rozporządzenie to powinno *„obejmować ryzyko dla bezpieczeństwa wynikające z nowych technologii cyfrowych"*. Rozporządzenie zawiera również ogólne odniesienia dotyczące produktów wykorzystujących uczenie maszynowe.

Ustawodawca unijny nakłada na producentów również obowiązek w zakresie ochrony przed przypadkowym lub zamierzonym uszkodzeniem, tj. wymaga, aby podłączenie do maszyny (np. poprzez pamięć przenośną), jak również łączenie z „urządzeniami zdalnymi", tj. przez Internet było chronione, nie mogło prowadzić do powstania sytuacji zagrożenia (pkt 1.1.9 „Zabezpieczenie przed uszkodzeniem" Załącznika III).

Polskie „podwórko"

W projektowanej nowelizacji ustawy o związkach zawodowych (skierowana do prac w komisji we wrześniu 2022 r.[7]) został przewidziany obowiązek pracodawcy udzielania, na wniosek zakładowej organizacji związkowej, informacji dotyczących parametrów, zasad i instrukcji, na których opierają się algorytmy lub systemy SI, które mają wpływ na podejmowanie decyzji, a które mogą mieć wpływ na warunki pracy i płacy, dostęp do zatrudnienia i jego utrzymanie, w tym profilowanie. Obecnie nie są prowadzone dalsze prace nad tym projektem.

Zgodnie z informacjami zawartymi w odpowiedzi na interpelację poselską z marca 2023 r. wydaje się, że Ministerstwo Sprawiedliwości nie prowadzi prac nad przepisami dot. SI[8]. W odpowiedzi na interpelację poselską Ministerstwo Sprawiedliwości wskazało tylko prace prowadzone nad projektami aktów prawnych na poziomie unijnym.

Nowe, dynamicznie zmieniające się ustawodawstwo unijne (a w ślad za nim polskie) wymusza na przedsiębiorcach konieczność bieżącego monitorowania wprowadzanych zmian. Niejednokrotnie bowiem zmiany te będę wymagały dokonywania zasadniczych zmian w produktach czy świadczonych usługach, a co się z tym wiąże będą wymagały czasu.

Sylwia Macura-Targosz
radczyni prawna, starszy prawnik w kancelarii Sołtysiński Kawecki & Szlęzak

6 Tekst Rozporządzenia dostępny na: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=uriserv%3AOJ.L_.2023.165.01.0001.01.POL&toc=OJ%3AL%3A2023%3A165%3ATOC; (dostęp: 1.12.2023 r.)

7 Tekst projektu dostępny na: https://www.sejm.gov.pl/sejm9.nsf/PrzebiegProc.xsp?id=F1D9C32EE2AB85BDC12588CB0031A801; (dostęp: 1.12.2023 r.)

8 Tekst interpelacji poselskiej oraz odpowiedzi dostępny na: https://www.sejm.gov.pl/Sejm9.nsf/interpelacja.xsp?typ=INT&nr=38607&view=null; (dostęp: 1.12.2023 r.)

ABB Ability™ Genix Copilot

Zaawansowana platforma AI dla przemysłu

ABB, światowy lider w automatyce i elektryfikacji, nawiązał strategiczne partnerstwo z Microsoft, wprowadzając Genix Copilot - zaawansowaną platformę AI dla przemysłu. Rozwiązanie uzbrojone w narzędzia wnioskujące i algorytmy uczenia maszynowego ułatwiają analizę danych oraz pomagają podjąć właściwe decyzje, dzięki którym możemy zwiększyć wydajność urządzeń, zmniejszyć zużycie energii i przede wszystkim zapobiec awariom i niezaplanowanym przestojom.
Przyspiesz cyfrową transformację swojego przedsiębiorstwa oraz osiągnij nowe standardy wydajności i innowacyjności.
abb.com

NIS 2 – NOWE OBLICZE CYBERBEZPIECZEŃSTWA W UNII EUROPEJSKIEJ

NIS 2 – czyli dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii – zaktualizowała do tej pory obowiązujące przepisy dyrektywy NIS z 2016 r. Nowa regulacja weszła w życie na początku tego roku i aktualnie znajduje się na etapie wdrażania do krajowych porządków prawnych państw członkowskich. Mają one na to czas do 17 października 2024 r. W poniższym artykule dokonany został przegląd najważniejszych zmian, które niesie za sobą dyrektywa.

Nowe sektory

Jedną z kluczowych zmian, które wprowadza NIS 2 w stosunku do NIS, jest rozszerzenie katalogu sektorów i podsektorów, do których ma ona zastosowanie. Do zakresu obowiązywania nowej dyrektywy dodany został szereg zupełnie nowych obszarów działalności, takich jak administracja publiczna, gospodarowanie odpadami czy też produkcja, wytwarzanie i dystrybucja chemikaliów. Kompletny wykaz sektorów objętych przepisami NIS 2 można znaleźć w Załączniku I i II do dyrektywy.

Zmianie ulega także obowiązujące na gruncie poprzednich przepisów rozdzielenie podmiotów objętych regulacją na operatorów usług kluczowych i dostawców usług cyfrowych. Dyrektywa NIS 2 wprowadza w tym zakresie nowy podział – na podmioty kluczowe i podmioty ważne. Przynależność do jednej lub drugiej kategorii nie wpływa na rodzaj obowiązków nałożonych na podmiot na gruncie dyrektywy – w przypadku obydwu grup są one dokładnie takie same. Ma ona jednak znaczenie przy stosowaniu środków nadzoru i egzekwowania przepisów, ponieważ w przypadku podmiotów kluczowych są one bardziej restrykcyjne.

Kryterium wielkości

Dyrektywa NIS 2, co do zasady, ma zastosowanie do tych podmiotów publicznych lub prywatnych, które kwalifikują się jako przedsiębiorstwa średnie lub większe niż średnie. Zgodnie z definicją z zalecenia 2003/361/WE, do którego odwołuje się dyrektywa, są to podmioty, które zatrudniają co najmniej 50 pracowników i których roczny obrót lub bilans wynosi co najmniej 10 mln euro.

Od tej zasady istnieją jednak wyjątki. W przepisach dyrektywy znajduje się katalog przypadków, w których są one stosowane również do mikro- lub małych przedsiębiorstw. Może się tak stać na przykład, gdy podmiot jest jedynym w danym państwie członkowskim dostawcą usługi, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej. Dodatkowo, niezależnie od wielkości, dyrektywa będzie miała zastosowanie do podmiotów zidentyfikowanych przez państwo jako mające charakter krytyczny na mocy dyrektywy (UE) 2022/2557 oraz świadczących usługi rejestracji nazw domen.

Zmiana sposobu identyfikacji

Zgodnie z obowiązującą wcześniej dyrektywą NIS, obowiązek identyfikacji podmiotów objętych przepisami spoczywał na państwach członkowskich. NIS 2 nie zawiera takich zapisów – a to oznacza, że podmioty będą musiały, co do zasady, same zidentyfikować się jako kluczowe lub ważne na podstawie wskazanych w regulacji kryteriów. Oczywiście państwa mają możliwość odrębnego uregulowania tej kwestii w ramach wdrażania dyrektywy do porządku krajowego. Mogą więc zadecydować o pozostawieniu obowiązku identyfikacji przy organach administracji publicznej. W związku z tym, że do tej pory w Polsce nie opublikowano projektu wdrożenia, warto na

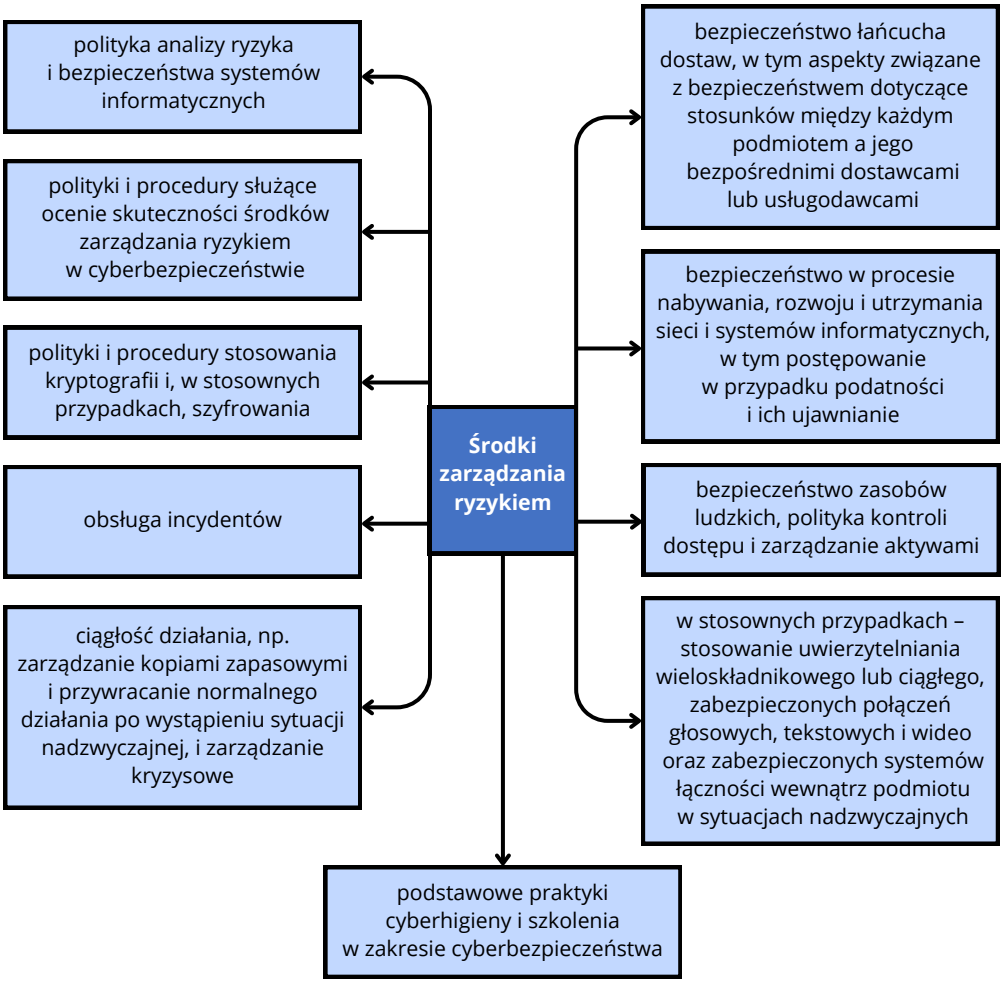
ten moment odnosić się do przepisów samego NIS 2 i przyjąć ostrożniejsze założenie - czyli że podmioty kluczowe i ważne muszą dokonać samoidentyfikacji.

Nowe obowiązki

Dyrektywa NIS 2 nakłada na objęte nią podmioty kluczowe i ważne szereg nowych obowiązków. Jednym z najistotniejszych jest konieczność wprowadzenia odpowiednich i proporcjonalnych środków w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych oraz zapobiegania bądź minimalizowania wpływu incydentów na odbiorców usług lub na inne usługi.

Istotą tego obowiązku jest wprowadzenie przez podmiot takich środków technicznych, operacyjnych i organizacyjnych, które pozwolą na zrealizowanie wskazanych wyżej celów. Środki te muszą zapewniać poziom bezpieczeństwa odpowiedni do ryzyka przy uwzględnieniu m.in. najnowszego stanu wiedzy, kosztów wdrożenia czy, w stosownych przypadkach, odpowiednich norm europejskich i międzynarodowych. Z kolei ocena ich proporcjonalności dokonywana jest w oparciu o wielkość podmiotu, stopień narażenia na ryzyko oraz prawdopodobieństwa wystąpienia u niego incydentów i ich dotkliwości, w tym skutków społecznych i gospodarczych.

W przepisach znajduje się także katalog obowiązkowych elementów, które muszą zostać włączone do wspomnianych wyżej środków. Należą do nich: odpowiednie polityki i procedury (np. służące analizie ryzyka lub ocenie skuteczności wprowadzonych środków), zapewnianie bezpieczeństwa w określonych obszarach (np. łańcucha dostaw, zasobów ludzkich), obsługa incydentów, zachowanie ciągłości działania i zarządzanie kryzysowe, stosowanie zabezpieczenia połączeń i systemów łączności, wprowadzanie podstawowych praktyk cyberhigieny oraz szkolenia w zakresie cyberbezpieczeństwa.



Rys. 1 Środki zarządzania ryzykiem

Dodatkowe obowiązki spoczywają na organach zarządzających podmiotów kluczowych i ważnych. Są one odpowiedzialne za zatwierdzanie środków zarządzania ryzykiem w cyberbezpieczeństwie oraz monitorują ich wdrożenia w organizacji. W przypadku naruszeń mogą one zostać pociągnięte do odpowiedzialności. Oprócz tego, członkowie organu zarządzającego mają obowiązek odbywać regularne szkolenia w celu zdobycia wiedzy i umiejętności pozwalających na rozpoznanie ryzyka oraz ocenę praktyk zarządzania nim w podmiocie i ich wpływu na świadczone usługi.

Kolejnym istotnym obowiązkiem wynikającym z NIS 2 jest zgłaszanie incydentów poważnych. Zgodnie z dyrektywą, za incydent poważny uznaje się incydent, który spowodował lub może spowodować dotkliwe zakłócenia operacyjne usług lub straty finansowe dla danego podmiotu oraz wpłynął lub jest w stanie wpłynąć na inne osoby fizyczne lub prawne, powodując znaczne szkody majątkowe i niemajątkowe.

Jeżeli podmiot stanie się ofiarą incydentu poważnego, ma on obowiązek niezwłocznego zgłoszenia incydentu do odpowiedniego CSIRT (lub właściwego organu). Nie dłużej niż w ciągu 24 godzin od uzyskania informacji o wystąpieniu incydentu, podmiot jest zobowiązany do wydania wczesnego ostrzeżenia, a w czasie nie dłuższym niż 72 godziny do zgłoszenia incydentu oraz wskazania wstępnej oceny tego incydentu. Podmiot ma również obowiązek złożyć okresowe sprawozdanie (na wniosek CSIRT) oraz końcowe sprawozdanie, które powinno zawierać dokładny opis incydentu, prawdopodobną przyczynę wystąpienia incydentu, środki jakie zostały wdrożone oraz, jeśli ma to zastosowanie, transgraniczne skutki incydentu. Termin złożenia sprawozdania końcowego wynosi miesiąc od zgłoszenia incydentu. Jednak w sytuacji, gdy incydent nie zakończył się w wyżej określonym czasie, sprawozdanie powinno być złożone w ciągu miesiąca od zakończenia incydentu.

Środki nadzoru

Zgodnie z Dyrektywą NIS 2 państwa członkowskie wyznaczają lub ustanawiają co najmniej jeden organ właściwy, który ma być odpowiedzialny za cyberbezpieczeństwo oraz zadania nadzorcze określone w dyrektywie. Podmioty kluczowe i podmioty ważne podlegają podobnym środkom nadzoru. Niewielkie różnice występują w kwestii kontroli - dla podmiotów kluczowych przewidywane są kontrole wyrywkowe, w przypadku podmiotów ważnych wskazane są kontrole i nadzór ex post („po fakcie").

Drugą różnicą jest możliwość przeprowadzenia audytu doraźnego w podmiocie kluczowym, co nie zostało wskazane w przypadku podmiotu ważnego. Pozostałe wymienione w dyrektywie środki nadzoru są dla obu podmiotów takie same i są to m.in. audyty i skany bezpieczeństwa, wnioski organów właściwych o udzielenie informacji, dostępu do danych, dokumentów czy o przedstawienie dowodów realizacji polityki cyberbezpieczeństwa.

Środki egzekwowania przepisów

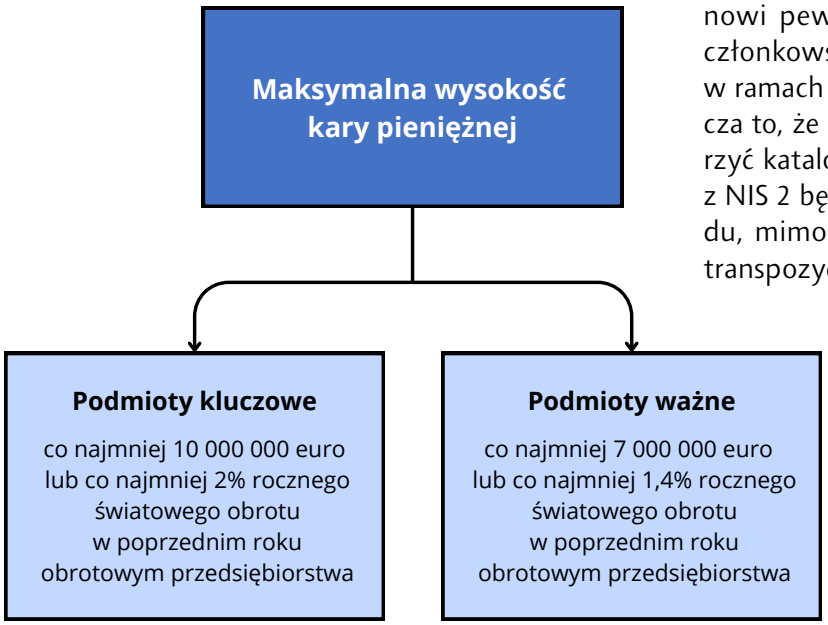
Organy właściwe mają również uprawnienia do stosowania środków egzekwowania przepisów wobec podmiotów kluczowych i ważnych, jednak wykorzystując te uprawnienie muszą każdą sprawę potraktować indywidualnie oraz uwzględnić skalę naruszenia i postawę podmiotu, który się go dopuścił.

Dyrektywa NIS 2 oferuje organom właściwym katalog środków egzekwowania przepisów, takich jak: wydawanie ostrzeżenia dotyczącego działań naruszających dyrektywę i wystosowanie wiążącego polecenia oraz nakazy: zaprzestania działań, które naruszają dyrektywę, zagwarantowania zgodnych z dyrektywą środków zarządzania ryzykiem w cyberbezpieczeństwie, poinformowania odbiorców usług o charakterze zagrożenia i zalecanych środkach naprawczych i ochronnych, wdrożenie zaleceń wydanych przez audytora oraz przekazania informacji o wykrytym naruszeniu do wiadomości publicznej. Dodatkowo, w przypadku podmiotów kluczowych może zostać wyznaczony urzędnik monitorujący.

W sytuacji, gdy środki nałożone przez organ właściwy nie są wystarczająco skuteczne i podmiot nie podjął zaleconych działań w celu usunięcia uchybień, organ wyznacza termin, w którym podmiot kluczowy jest zobowiązany do podjęcia koniecznych działań. Jeżeli jednak tego nie wykona, organ właściwy jest uprawniony do zastosowania bardziej restrykcyjnych środków. Pierwszym z nich jest tymczasowe zawieszenie certyfikacji lub zezwolenia na świadczone usługi lub działalność podmiotu. Drugim jest tymczasowy zakaz pełnienia funkcji zarządczej,

na który należy zwrócić szczególną uwagę, ponieważ jest nakładany na osobą fizyczną. Wszystkie wyżej opisane środki przestają mieć zastosowanie w momencie podjęcia przez podmiot działań wymaganych przez organ właściwy.

W dyrektywie NIS 2 przewidziano również możliwość nakładania na podmioty kluczowe i ważne administracyjnych kar pieniężnych. Maksymalną wysokość kary w zależności od rodzaju podmiotu przedstawia poniższa grafika.



Rys. 2 Maksymalna wysokość kar pieniężnych

Przygotowanie organizacji na NIS 2

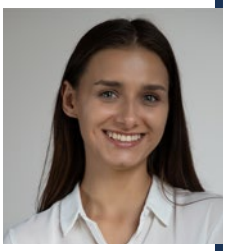
Na koniec warto odpowiedzieć na pytanie w jaki sposób organizacja może przygotować się na zmiany, które wprowadza dyrektywa NIS 2.

Podstawowym krokiem w tym procesie będzie wspomniana już samoidentyfikacja. W tym celu niezbędne jest określenie, czy podmiot spełnia kryteria podlegania pod stosowanie przepisów NIS 2 – czyli czy prowadzi działalność w którymś z wymienionych w załącznikach sektorów i jest wielkości przynajmniej średniego przedsiębiorstwa (uwaga na wspomniane wcześniej wyjątki!). Jeżeli wynikiem tej oceny jest stwierdzenie, że regulacja na pewno lub z wysokim prawdopodobieństwem będzie dotyczyć organizacji, warto już teraz zastanowić się, w jaki sposób może ona zacząć przygotowania do nowych obowiązków i wymagań.

Zadanie utrudnia fakt, że przepisy NIS 2 są dość ogólne, a ich doprecyzowanie stanowić będą dopiero regulacje wdrażające tę dyrektywę do porządku krajowego. Jak już wcześniej wspomniano, Polska jeszcze nie opublikowała projektu takich przepisów. Z tego powodu niezwykle ważnym działaniem, które powinny podjąć wszystkie podmioty, które wiedzą lub podejrzewają, że mogą podlegać pod NIS 2, jest bieżące monitorowanie prac legislacyjnych w tym zakresie.

Warto też mieć na uwadze, że dyrektywa stanowi pewne minimum, do którego państwa członkowskie mogą dołożyć własne elementy w ramach swoich porządków krajowych. Oznacza to, że polski ustawodawca może np. rozszerzyć katalog podmiotów, do których obowiązki z NIS 2 będą miały zastosowanie. Z tego powodu, mimo że ostateczny termin na dokonanie transpozycji dyrektywy jest jeszcze odległy, to warto zachować czujność i obserwować bieżącą sytuację w obszarze wdrażania dyrektywy.

Emilia Zalewska-Czajczyńska
Prawniczka
Specjalistka ds. analiz strategicznych z obszaru cyberbezpieczeństwa



Paulina Popow
Młodsza Specjalistka ds. analiz strategicznych z obszaru cyberbezpieczeństwa

Dział Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni, Państwowy Instytut Badawczy NASK

OCENA RYZYKA A ODPORNOŚĆ SIECI I SYSTEMÓW INFORMATYCZNYCH NA INCYDENTY CYBERBEZPIECZEŃSTWA

Bezpieczeństwo sieci i systemów informatycznych zdefiniowane jest w dyrektywie NIS 2 2022/2555/UE jako: „odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie zdarzenia, które mogą naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez te sieci i systemy informatyczne lub dostępnych za ich pośrednictwem" [1].

Definicja systemu informatycznego (a także teleinformatycznego, który połączony jest z innymi za pomocą sieci telekomunikacyjnych) mówi natomiast, że SYSTEM INFORMATYCZNY to ta część systemu informacyjnego, w której do przetwarzania informacji wykorzystywane są środki techniki komputerowej [3]. Definicja ta obejmuje również przemysłowe systemy sterowania *(Industrial Control Systems*, ICS) występujące wszędzie tam, gdzie mamy do czynienia z fizyczną realizacją procesów produkcyjnych, przesyłowych, magazynowych czy transportu bliskiego. Podstawowe definicje przedstawia rys. 1.

Rys. 1. Definicje systemów informacyjnych

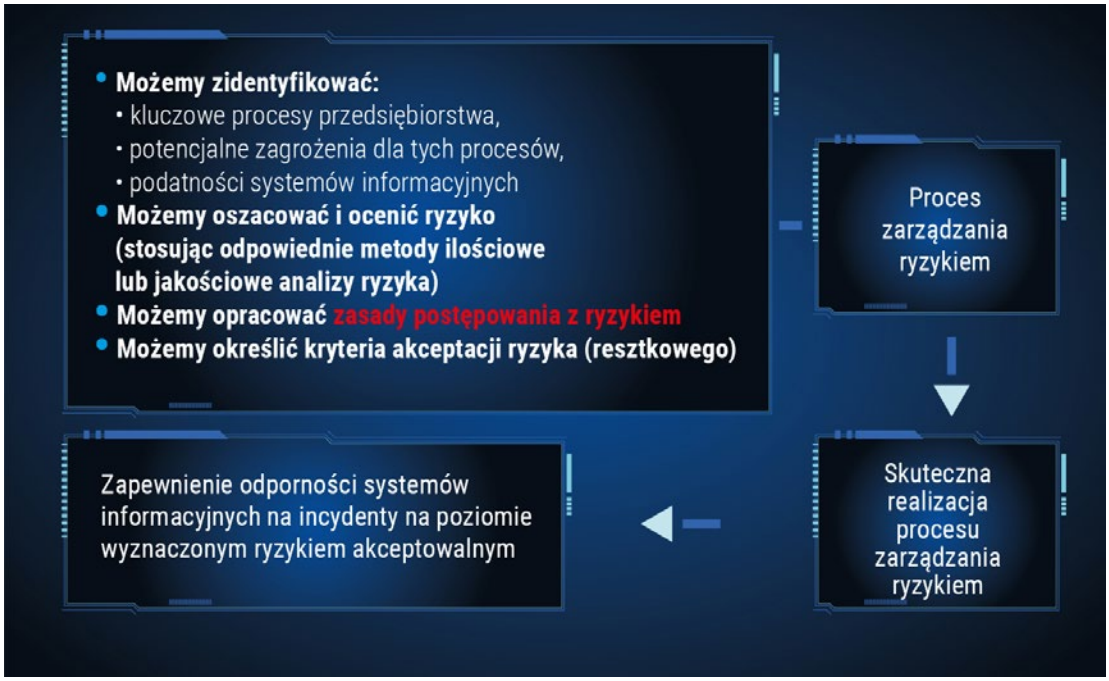
Czym zatem jest odporność systemów i sieci informatycznych? Czy możemy z całą pewnością stwierdzić, że nasze aktywa są wystarczająco bezpieczne i odporne?

Niestety nie, nigdy bowiem nie będziemy pewni, że nasze sieci i systemy mają w danym momencie odpowiedni (wystarczający) poziom bezpieczeństwa i odporności na zagrożenia. Wynika to z faktu, że bezpieczeństwo oraz odporność (sieci i systemów) na incydenty są wartościami niemierzalnymi, występującymi najczęściej jako pojęcia jakościowe.

Jak zatem zwiększać bezpieczeństwo i budować odporność?

Z pomocą przychodzi nam proces zarządzania ryzykiem w organizacji, podczas którego możemy zidentyfikować kluczowe procesy przedsiębiorstwa, potencjalne zagrożenia dla tych procesów (w tym potencjalne

incydenty dotyczące sieci i systemów informatycznych) oraz opracować zasady postępowania ze zbyt wysokim ryzykiem materializacji zagrożenia czy konsekwencji. Proces ten przedstawia rys. 2.



Rys. 2. Zarządzanie ryzykiem a odporność sieci i systemów informatycznych na incydenty

Budowanie odporności sieci i systemów informatycznych zarówno biurowych IT (Information Technology, IT), jak i sterowania przemysłowego OT (Operational Technology, OT) na incydenty cyberbezpieczeństwa jest procesem ciągłym i wynikającym z poziomu ryzyka wystąpienia incydentu (wartości prawdopodobieństwa materializacji zagrożenia i wielkości jego potencjalnych konsekwencji).

Skuteczne prowadzenie procesu zarządzania ryzykiem w przedsiębiorstwie pozwala na zapewnienie odporności sieci i systemów informatycznych na poziomie wyznaczonym ryzykiem zaakceptowanym przez przedsiębiorstwo, np. najwyższe kierownictwo, zarząd. Oznacza to, że odporność naszych sieci i systemów wyznacza poziom ryzyka zaakceptowany przez organizację.

Zagrożenie (dla bezpieczeństwa informacji) to materialny i/lub niematerialny czynnik mogący spowodować niepożądaną zmianę wymaganych wartości istotnych kryteriów jakości informacji [3].

Umiejętne zarządzanie ryzykiem jest podstawą bezpiecznego funkcjonowania przedsiębiorstwa

Zarówno atak zdalny (zwany potocznie atakiem hakerskim), jak i fizyczny na systemy informatyczne i sieci definiowane są jako jeden ze sposobów realizacji zagrożenia poprzez nieuprawnione, celowe działanie człowieka powodujące niepożądaną zmianę wymaganych wartości istotnych kryteriów jakości informacji. Zagrożenie natomiast jest pojęciem szerszym i tak powinno być rozpatrywane podczas oceny ryzyka w przedsiębiorstwie.

PODSTAWOWE ELEMENTY PROCESU ZARZĄDZANIA RYZYKIEM

- Prawidłowa identyfikacja kluczowych procesów w przedsiębiorstwie
- Identyfikacja potencjalnych zagrożeń dla tych procesów
- Identyfikacja podatności sieci i systemów informatycznych
- Szacowanie i ocena ryzyka (z wykorzystaniem odpowiednich metod ilościowych i jakościowych analizy ryzyka)
- Opracowanie zasad postępowania ze zbyt wysokim ryzykiem (unikanie ryzyka, transfer ryzyka, kontrola ryzyka, retencja/zatrzymanie ryzyka)
- Określenie kryteriów jego akceptacji

Należy mieć na uwadze, że zarządzanie ryzykiem cyberbezpieczeństwa, zdarzeń zagrażających przedsiębiorstwu jako potencjalne incydenty cyberbezpieczeństwa, występuje jako wymaganie i dobra praktyka.

WYMAGANIE

- w obowiązującej jeszcze ustawie o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018 r. [7] na podstawie dyrektywy NIS 2016/1148/UE (dotyczy operatorów usług kluczowych) [2]
- w dyrektywie NIS 2 2022/2555/UE [1] (dla podmiotów kluczowych, w tym administracji publicznej oraz podmiotów ważnych – znacznie szerszy zakres niż w dyrektywie NIS 2016/1148/UE); listę sektorów kluczowych i ważnych przedstawia tab. 1

DOBRA PRAKTYKA w normach wskazanych w uzasadnieniu do obowiązującej ustawy o KSC.

- PN-EN ISO/IEC 27001:2017-06 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania (obecnie: PN-EN ISO/IEC 27001:2023-08 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji – Wymagania) [5]
- PN-EN ISO 22301:2020-04 Bezpieczeństwo i odporność – Systemy zarządzania ciągłością działania – Wymagania [4]

Oprócz prewencji, należy pamiętać o zapewnieniu ciągłości działania poprzez przygotowanie planów odtwarzania systemów i stosowanie zaleceń standardu PN-EN ISO 22301:2020-04 [4].

Tabela 1. Sektory podmiotów kluczowych i ważnych według dyrektywy NIS 2 (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	

Ocena ryzyka powinna być przeprowadzana cyklicznie, co najmniej raz w roku, oraz po każdej istotnej planowanej lub występującej niespodziewanie zmianie w działalności przedsiębiorstwa. Prawidłowo przeprowadzona ocena definiuje konieczność wdrożenia brakujących bądź rozbudowy istniejących zabezpieczeń / środków ochronnych organizacyjnych, fizycznych i technicznych.

Przykłady zabezpieczeń i środków ochronnych:

Zabezpieczenia organizacyjne (wspierające skuteczność zabezpieczeń fizycznych i technicznych)

- **Polityka bezpieczeństwa**
- Zintegrowany system zarządzania
- Cykliczne audyty bezpieczeństwa
- SOC wewnętrzny i/lub zewnętrzny (ang. *Security Operation Center*)
- Edukacja i budowanie świadomości pracowników
- Weryfikacja dostawców

Zabezpieczenia fizyczne (obiektów, łączy i urządzeń)

- **Ochrona osobowa – straż, firma ochroniarska**
- **Służby wewnętrzne**
- **Ogrodzenia, przegrody budowlane**
- **Bunkry**
- **Drzwi, zamki, kraty**
- **Sejfy, szafy pancerne**

Zabezpieczenia techniczne

- **Obiektów, łączy i urządzeń systemy ppoż/pgaz.**
- systemy ppoż/pgaz.
- systemy sygnalizacji napadu i włamania
- systemy kontroli dostępu
- systemy rejestracji czasu pracy
- systemy nadzoru wizyjnego
- **Sprzętowo-programowe – produkty realizujące funkcje ochronne**
- segmentacja sieci (model Purdue, DMZ, VLAN)
- monitorowanie sieci (SIEM, IDS/IPS, SOAR)
- komunikacja jednokierunkowa (*data diodes*)
- firewall
- oprogramowanie antywirusowe
- szyfrowanie transmisji danych oraz plików
- bezpieczne metody uwierzytelniania
- regularne kopie bezpieczeństwa
- terminowe aktualizacje
- ograniczone wykorzystanie pamięci przenośnych

W przypadku oceny ryzyka sieci i systemów informatycznych sterowania i kontroli (OT) warto skorzystać z opracowanych dla tego sektora standardów. Popularną serią standardów przemysłowych, wywodzącą się z tej samej amerykańskiej organizacji normalizacyjnej ISA (*International Society of Automation*), w której opracowano serię standardów dotyczącą bezpieczeństwa funkcjonalnego dla przemysłu procesowego (seria IEC 61511), jest seria IEC 62443 (ISA-99) Security for Industrial Automation and Control Systems.

Zaletą serii jest uzupełnienie zagadnień bezpieczeństwa funkcjonalnego safety o zagadnienia dotyczące cyberbezpieczeństwa security (No safety without security). W polskim wydaniu arkuszu normy PN-EN IEC 62443-3-2:2021-03 Bezpieczeństwo w systemach sterowania i automatyki przemysłowej – Część 3-2: Ocena ryzyka w bezpieczeństwie i projektowaniu systemu [6] znajdziemy przydatne informacje dotyczące oceny ryzyka sieci i systemów sterowania przemysłowego, budynkowego, transportowego, wodno-kanalizacyjnego czy też medycznego.

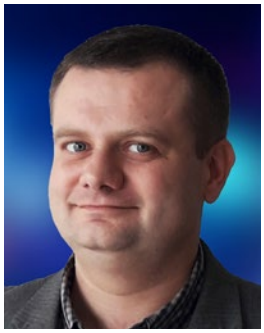
Podstawowe etapy oceny ryzyka dla systemów sterowania, opisane w standardzie:

- identyfikacja rozważanego systemu (*System Under Consideration*, SUC) – zdefiniowanie ocenianego systemu w ramach systemu automatyki i sterowania przemysłowego *(Industrial Automation and Control Systems*, IACS),
- przeprowadzenie wstępnej (zgrubnej) oceny ryzyka cyberbezpieczeństwa,
- podzielenie SUC na strefy i kanały – grupowanie aktywów w strefy i kanały, przy czym priorytetem jest zidentyfikowanie tych aktywów, które mają wspólne wymagania dotyczące bezpieczeństwa, i umożliwienie identyfikacji wspólnych środków bezpieczeństwa (zabezpieczeń) wymaganych do ograniczenia ryzyka,
- wykonanie szczegółowej oceny ryzyka cyberbezpieczeństwa dla każdej strefy i kanału oraz określenie docelowego poziomu bezpieczeństwa SL-T (*Security Level-Target*) dla każdej strefy i kanału,
- udokumentowanie zaktualizowanych wymagań cyberbezpieczeństwa dla szczegółowego projektu (specyfikacja wymagań cyberbezpieczeństwa – *Cybersecurity Requirements Specifications*, CRS).

Standard wskazuje ponadto, aby podczas oceny ryzyka szczególną uwagę poświęcić systemom bezpieczeństwa, systemom automatyki zabezpieczającej, przyrządowym systemom bezpieczeństwa SIS (Safety Instrumented Systems), systemom łączności bezprzewodowej, systemom połączonym bezpośrednio do punktów końcowych sieci internet, systemom będących interfejsem do IACS, ale zarządzanych przez zewnętrzne podmioty (w tym systemom zewnętrznym) i urządzeniom mobilnym.

Z uwagi na poziom ryzyka wynikający z pozostającej zawsze większej bądź mniejszej możliwości wystąpienia incydentu (ryzyko resztkowe / szczątkowe) każde przedsiębiorstwo powinno być przygotowane na jego wystąpienie. Kluczowym procesem, obok procesu zarządzania ryzykiem w organizacji, jest zatem proces zarządzania incydentami, a w szczególności proces ich obsługi. Należy przy tym pamiętać, że całkowita eliminacja występowania incydentów nie jest możliwa, a proces zarządzania ryzykiem ich wystąpienia i konsekwencji powinien być stałym elementem działalności organizacji.

Michał Łoniewski
Kierownik Wydziału Rozwoju Technicznego Przewodniczący Zespołu Zadaniowego ds. Cyberbezpieczeństwa Departament Innowacji i Rozwoju Urząd Dozoru Technicznego



Literatura:

1. 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 (dyrektywa NIS 2).
2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa NIS).
3. Liderman K. (2017). Bezpieczeństwo informacyjne. Nowe wyzwania. Warszawa: Wydawnictwo Naukowe PWN.
4. PN-EN ISO 22301:2020-04 Bezpieczeństwo i odporność – Systemy zarządzania ciągłością działania – Wymagania.
5. PN-EN ISO/IEC 27001:2023-08 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -- Systemy zarządzania bezpieczeństwem informacji – Wymagania.
6. PN-EN IEC 62443-3-2:2021-03 Bezpieczeństwo w systemach sterowania i automatyki przemysłowej – Część 3-2: Ocena ryzyka w bezpieczeństwie i projektowaniu systemu.
7. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369 oraz z 2021 r. poz. 2333 i 2445 oraz z 2022 r. poz. 655).

Znasz już nasz najnowszy system pomiarowy?

—

Dräger X-node

Dräger

Technika dla Życia

SMART SAFETY: WIĘCEJ DANYCH TO WIĘKSZE BEZPIECZEŃSTWO

Cyfrowe monitorowanie gazów przy pomocy platform IoT lub automatyczne zarządzanie urządzeniami przy użyciu oprogramowania chmurowego to potencjalne kamienie milowe na drodze do digitalizacji procesów bezpieczeństwa i generowania nowej wiedzy. Już dziś sieciowe systemy sprzętowe i platformy danych zapewniają większą przejrzystość stanu przemysłowych zakładów i miejsc pracy. Te i inne rozwiązania z zakresu Smart Safety mogą zagwarantować bezpieczeństwo, przejrzystość i efektywność działalności w branży surowcowej i przetwórczej.

Zdigitalizowane procesy bezpieczeństwa związane z sieciową technologią pomiaru gazów

W procesie wypalania wapienia w wapiennikach Fels-Werke GmbH przekazywana od pokoleń wiedza o surowcach łączy się z technologią przyszłości. Wytwarzanie tlenku wapnia (CaO) to proces znany i rozwijany od starożytności. W jego trakcie węglan wapnia ($CaCO_3$) pod postacią wapienia jest podgrzewany do temperatury około 1000 stopni Celsjusza przy użyciu paliwa stałego, ciekłego lub gazowego. Tak powstaje wapno palone, które po gaszeniu wodą przekształca się w wapno gaszone ($CA(OH)_2$). Stabilizuje się ono w trakcie przetwarzania, tworząc węglan wapnia. Obecnie w nowoczesnych zakładach produkcyjnych wykorzystujących zaawansowane procesy powstają różne materiały budowlane i surowce przemysłowe. Oferta Fels-Werke obejmuje białe wapno, sproszkowane białe wapno, białe wapno hydratyzowane, mleko wapienne oraz różne specjalne rodzaje wapna w postaci produktów palonych. W trakcie wytwarzania tych surowców mobilne urządzenia do pomiaru gazów zapewniają wysoki poziom bezpieczeństwa pracowników.

Firma z siedzibą w niemieckim Goslar, założona 85 lat temu pod nazwą „Stein und Erden GmbH", od

2021 roku realizuje cyfrową transformację. Do zarządzania flotą detektorów gazu Fels-Werke wykorzystuje chmurowe oprogramowanie Gas Detection Connect firmy Dräger. Określenie „Smart Safety" (inteligentne bezpieczeństwo) stosuje się do opisywania **digitalizacji procesów i zadań związanych z bezpieczeństwem.** Podstawą tego podejścia jest dostępność szerokiego zakresu danych, która daje cenną, płynącą z wiedzy przewagę w działalności gospodarczej. Innowacyjne usługi związane z technologią pomiarową, sprzętem ochronnym i akcesoriami tworzą wartość dodaną i odciążają użytkowników, bazując na danych z urządzeń, wartościach wskazywanych przez czujniki, obrazach i mapach lub informacjach lokalnych. Celem gromadzenia i analizy danych jest często konserwacja predykcyjna (przewidywanie potrzeb konserwacyjnych i zapobieganie samoistnemu zużyciu i awariom). Firmy ze wszystkich branż mogą rozwijać się w sposób zrównoważony pod względem ekonomicznym i ekologicznym przy pomocy w pełni zdigitalizowanych procesów korzystających z systemów sieciowych. Thomas Ullrich potwierdza to, opowiadając o codziennej pracy z technologią detekcji gazów Dräger. Jako technik pomiarowy w firmie Fels-Werke Ullrich odpowiada za flotę około 150 detektorów gazu Dräger i stacji testowych X-dock rozproszonych po sześciu zakładach. Od zeszłego roku do zarządzania tym zespołem urządzeń wykorzystywany jest system Gas Detection Connect. Wcześniej urządzenia były monitorowane przy pomocy klasycznego oprogramowania X-dock Management firmy Dräger. „Już w tamtym systemie w ciągu kilku sekund było widoczne, że pracownik skorzystał z detektora gazu do konkretnego zadania, że został on uprzednio przetestowany i że jest gotowy do użytku" – mówi Ullrich.

Oprogramowanie chmurowe zmniejsza obciążenia

Wprowadzając **Dräger Gas Detection Connect,** firma Fels-Werke zdecydowała się na kolejny poziom digitalizacji w zarządzaniu technologią pomiaru gazów. „Oprogramowanie zniknęło z komputerów, a urządzenia zawsze są aktualne dzięki chmurze i jej bazie danych" – mówi specjalista, opisując zalety widoczne w codziennej pracy. Ullrich nie jest jedynym użytkownikiem, który dostrzega pozytywne rezultaty. Zadowolony jest również dział IT klienta, ponieważ działania, które wcześniej były niezbędne do aktualizowania oprogramowania sprzętowego przy użyciu lokalnego serwera, teraz przebiegają automatycznie. Dodatkowo terminy kalibracji i wymogi konserwacyjne, uruchomione alarmy oraz status urządzeń są dokumentowane w jasny i szczegółowy sposób, a każda uprawniona do tego osoba może Rozwiązania chmurowe nie są jeszcze standardem w branży, chociaż pod względem cyberbezpieczeństwa i bezpieczeństwa danych w niczym nie ustępują oprogramowaniu instalowanemu na miejscu. Firma Fels-Werke, która należy do CRH, ustanawia nowy wzorzec w obrębie swojej grupy. Korzyści są szczególnie widoczne w ramach procesów wyższego poziomu, takich jak testowanie, konserwacja i zarządzanie sprzętem. „W tym projekcie scentralizowana kontrola i centralizacja aktualizacji oprogramowania sprzętowego przy użyciu stacji X-dock były dla naszego klienta kluczowe ze względu na rozproszenie geograficzne zakładów" – mówi Sonja During, inżynier ds. sprzedaży Dräger, która asystowała przy wprowadzeniu Gas Detection Connect w firmie Fels-Werke. Wyjaśnia, że lepsze planowanie zasobów zapewnia optymalną dostępność utrzymanego w doskonałym stanie sprzętu, co może zainteresować także innych producentów. „Technologia detekcji gazów w ramach cyfrowej sieci odegra w przyszłości decydującą rolę w branży" – przewiduje chemiczka. Jej zdaniem celem jest dalsza poprawa bezpieczeństwa dzięki danym czasu rzeczywistego.

„W pięciu odkrywkach, z których wydobywamy wapień, gazy zazwyczaj nie stanowią problemu" – twierdzi Ullrich. Znacznie istotniejsze jest ciągłe monitorowanie atmosfery podczas dalszego przetwarzania w 37 pracujących wapiennikach. Działają one na zasadzie ciągłego spalania. Dopóki się żarzą, technologia pomiaru gazów jest niezbędna, przede wszystkim po to, by chronić pracowników przed tlenkiem węgla, którego poziom jest nieustannie monitorowany przy pomocy ostrzegawczych mierników pojedynczego gazu Dräger Pac. „Nikt nie wejdzie do górnej części szybu bez tego urządzenia" – mówi Ullrich. Fels-Werke wykorzystuje również cenione urządzenia do pomiaru wielu gazów z **serii Dräger X-am.** Są one stosowane do kontrolowania emisji i uzyskiwania jasnych pomiarów. Ullrich wykorzystuje te urządzenia do pomiarów przed regulacją. Dla firmy Fels-Werke wyposażono je w czujniki do wykrywania tlenu (O_2), tlenku węgla (CO), dwutlenku węgla (CO_2) i metanu (CH_4).

Przewyższyć standardy bezpieczeństwa

Testy urządzeń do pomiaru gazów w firmie Fels-Werke odbywają się nie tylko każdego dnia roboczego, ale też przed każdym użyciem. „W ten sposób wykraczamy poza wymogi instrukcji T 021 i T 023 BG RCI" – mówi Ullrich. T 021 („Detektory gazu i sprzęt do gazów toksycznych / par i tlenu – użycie i korzystanie") oraz T 023 („Detektory gazu i sprzęt do ochrony przed wybuchem – użycie i korzystanie") określają obowiązujące w Niemczech standardy w zakresie korzystania z detektorów gazu w celu zapewnienia bezpieczeństwa w miejscu pracy. Taka decyzja firmy znacząco poprawia to ostatnie, na co mają pozytywny wpływ także połączone stacje testowe z infrastrukturą cyfrową. W Fels-Werke dostępnych jest w sumie osiem stacji dokujących Dräger i odpowiednich gazów testowych do testów gazowania. Oprócz tego stacje za pośrednictwem istniejącej sieci przekazują do chmury rejestratory danych wszystkich mobilnych detektorów gazu oraz wyniki testów. Automatycznie przesyłają także aktualizacje do oprogramowania sprzętowego. Wymagana dokumentacja wszystkich testów, w tym rejestratorów danych urządzeń, prowadzona jest cyfrowo i dostępna dla każdego użytkownika w dowolnym momencie. Niezależnie od sieci stacji X-dock, zmierzone wartości i lokalizacje można przesłać do chmury, korzystając z urządzeń pomiarowych w połączeniu ze smartfonem. Same stacje X-dock także pobierają aktualizacje oprogramowania sprzętowego z oprogramowania chmurowego Gas Detection Connect po naciśnięciu guzika, dzięki czemu trwająca 15 minut aktualizacja nie zakłóca pracy. Tradycyjny proces wymagał, by pracownik udał się osobiście do każdego z zakładów. Dzisiaj wystarczy, że wykwalifikowani pracownicy ręcznie wymienią jedynie butle z gazem testowym.

Cyfrowe monitorowanie na żywo w miejscu pracy

Cyfrowe zarządzanie flotą urządzeń pomiarowych stanowi jakościowy skok w zarządzaniu technologią, ale portfolio Smart Safety obejmujące systemy monitorowania na żywo prowadzi także do znaczącej poprawy bezpieczeństwa. Urządzenia do pomiaru gazów są połączone przez Bluetooth z odpornym na wybuchy smartfonem, co pozwala na monitorowanie wariantu, gazu i zanieczyszczenia przy użyciu oprogramowania Gas Detection Connect. W zależności od regulaminu działalności aplikacja mobilna przesyła do chmury takie dane jak wartości pomiarowe, współrzędne GPS, alarmy oraz, jeśli taka jest wola użytkownika, imię i nazwisko osoby korzystającej z urządzenia. Zaletą tego rozwiązania jest to, że po uruchomieniu alarmu jest on zapisywany w czasie rzeczywistym w pomieszczeniu kontrolnym, w systemie ochrony przed gazem oraz w dziale straży pożarnej kopalni lub fabryki, a także wizualizowany na mapie. Dzięki temu odpowiednie osoby mogą szybko poddać ocenie i automatycznie udokumentować

wystąpienia gazu, wycieki, incydenty, skażenia i zanieczyszczenia miejsca pracy. W sytuacji awaryjnej można podjąć szybkie i bezpieczne działanie.

„W wielu sytuacjach możliwe są lepsze decyzje, jeśli dane są dostępne w powiązanym kontekście lokalnym" – mówi Sven Schmellenkamp, specjalista ds. rozwoju biznesowego w firmie Dräger, który kieruje strategicznym Inkubatorem Smart Safety oraz technologicznym Systems Center, starając się sprostać potrzebom klientów związanym z digitalizacją. Jak mówi Schmellenkamp, Dräger nieustannie znajduje nowe zastosowania dla usług opartych na danych. Często polega to na zwiększeniu efektywności wykorzystania czasu i zasobów ludzkich w trakcie stosowania prewencyjnych środków bezpieczeństwa w złożonych procesach lub zakładach przemysłowych, co ogranicza do minimum opóźnienia lub zakłócenia procesów budujących wartość.

Schmellenkamp podaje kilka przykładów:

- Przed rozpoczęciem pracy inteligentny system monitorowania niezależnie sprawdza gotowość indywidualnego detektora gazu. Pracownik zostaje automatycznie poinformowany o stanie urządzenia i w momencie wejścia do zakładu nie musi się już o nic martwić.
- Można połączyć ze sobą informacje o lokalizacji pracownika, dane o czujnikach, w jakie wyposażone jest urządzenie, oraz informacje przechowywane w bazie danych na temat zakładu, do którego ma wejść pracownik. Następnie inteligentny system automatycznie sprawdza, czy technologia czujników na wyposażeniu odpowiada wymogom bezpieczeństwa obowiązującym w zakładzie.
- Analiza zbiorów danych zgromadzonych we wskazanych okresach służy do identyfikacji anomalii, które są wizualizowane przy pomocy tzw. map cieplnych.
- Dane gromadzone przez roboty i drony w ramach autonomicznych procesów pomiarowych są włączane do systemów chmurowych i kojarzone z odpowiednimi informacjami.

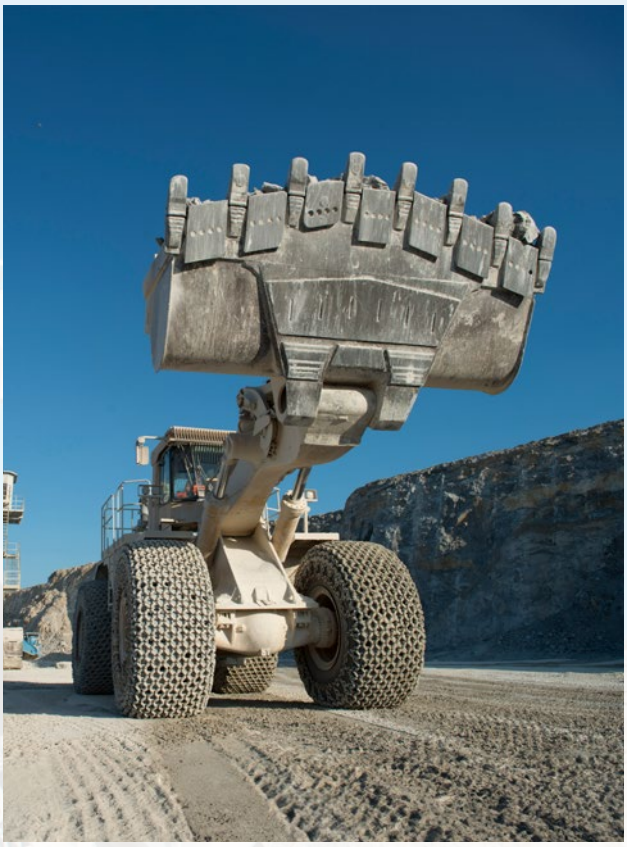
- Procesy zyskują na efektywności bez uszczerbku dla bezpieczeństwa, na przykład poprzez cyfrowe przesyłanie zezwoleń na pracę po przeprowadzeniu pomiaru dopuszczającego lub dokumentacji. Włączenie w ten sposób wyników pomiarów w procesy klienta pozwala znacząco zaoszczędzić czas w porównaniu z przekazywaniem papierowego formularza w biurze i zapobiec błędom w trakcie tej procedury.

Koncentracja na usłudze

Smart Safety to więcej niż suma sprzętu i oprogramowania. W istocie jest to nowa strategia, polegająca na śmiałym tworzeniu rozwiązań wspólnie z klientami. „Nasze systemy muszą być jak najbardziej elastyczne" – mówi Schmellenkamp. „To nie klient ma się dostosować do naszego rozwiązania, tylko rozwiązanie jest opracowywane wspólnie z klientem" – podkreśla. Dodaje, że z tego powodu istotną częścią działalności Dräger jest jak najlepsze dopasowanie wybranych usług do konkretnych indywidualnych potrzeb i struktury spółki przemysłowej. Zakres tych potrzeb jest bardzo szeroki, począwszy od znaczącego skalowania obciążenia pracą, a skończywszy na takich środkach jak przejście do długoterminowego, bezpiecznego dokumentowania działalności. Pierwszy przykład to znakomita ilustracja potencjału Smart Safety nawet w szczególnych sytuacjach. Gdy na kilka tygodni liczba pracowników w zakładzie zwiększa się ponad dziesięciokrotnie, wydajne i bezpieczne procesy wypożyczania sprzętu pomiarowego, zarządzania nim i testowania go mają szczególną wartość. Drugi przykład pokazuje rosnące znaczenie, jakie ma dla firm możliwość udowodnienia, że pracują w sposób bezpieczny. Wiele spółek przemysłowych pragnie aktywnie dokumentować ten fakt. Może to objąć także automatyczną dokumentację określonego indywidualnie narażenia na substancje niebezpieczne pracowników i usługodawców.

Droga do przyszłości wymaga zrobienia pierwszego kroku

Nie ulega wątpliwości, że inteligentne systemy bezpieczeństwa, zautomatyzowane procesy i technologie autonomiczne wywrą istotny wpływ na przyszłość wszystkich branż. Coraz więcej firm szuka rozwiązań, dzięki którym świat pracy i prowadzona przez nie produkcja staną się bezpieczniejsze,



wydajniejsze i bardziej zrównoważone. Pójście tą drogą wymaga zrobienia pierwszego kroku, tak jak w latach 2021–2022 uczyniła to firma Fels-Werke GmbH, wprowadzając Gas Detection Connect.

Internet rzeczy dzięki sieci LoRa

Nowe urządzenie monitorujące Dräger X-node przesyła w trybie ciągłym wartości pomiarowe dotyczące m.in. obecności gazu, wilgotności, ciśnienia powietrza i temperatury na platformę Internetu rzeczy (IoT). Przejrzyste pulpity online podają istotne informacje o środowisku pracy. Inteligentne urządzenie bezprzewodowe można zawiesić w miejscu, w którym wykryto zagrożenie obecnością gazu. Mocny akumulator i wrażliwe czujniki oparte na technologii stacjonarnych ostrzegawczych mierników gazu pozwalają na bezobsługowe monitorowanie obszaru przez wiele miesięcy. Dane są przesyłane do aplikacji na telefon przez Bluetooth albo na platformę danych przez efektywną energetycznie sieć LoRa-Wan (sieć wielkoobszarową dalekiego zasięgu). Oprócz celów związanych jedynie z dokumentacją i monitorowaniem dane mogą posłużyć do wpływania na inne systemy IoT lub sterowania nimi, na przykład do uruchomienia automatycznych systemów wentylacji, klimatyzacji lub mechanizmów czyszczących.

Dräger Gas Detection Connect

Chmurowe oprogramowanie Gas Detection Connect to potężna platforma cyfrowa opracowana przez firmę Dräger z myślą o technologii detekcji gazów. Głównym celem było zbudowanie efektywnej sieci urządzeń oraz kompleksowe wykorzystanie i kontekstualizacja danych. Informacje, od pojedynczych odczytów poziomu gazów i wyników testów po certyfikaty, są przesyłane przez stacje Dräger X-dock. Do systemu można podłączyć także automat wypożyczeniowy Dräger Rental Robot 3.0 z interfejsem opartym na sieci internetowej i adapterem IoT. Zarządzanie cyfrową flotą zostaje w ten sposób wzbogacone o kolejny poziom informacji. Podczas prac nad oprogramowaniem priorytetem była ochrona danych. Kopia zapasowa wszystkich danych jest zapisywana w europejskiej chmurze Microsoft Azure. Dzięki jasnemu przypisywaniu ról i uprawnień użytkownik może zdecydować, którzy pracownicy mogą wyświetlać określone dane. Można na przykład ustalić, czy na mapie będzie widoczna lokalizacja GPS pracowników oraz czy będą oni wyświetlać się anonimowo.

Dräger Gas Detection Connect opracowano, koncentrując się w całym procesie na tym, by rozwiązanie było przyjazne dla użytkownika. Uruchomienie i aktualizacje nie wymagają już wsparcia działu IT, ponieważ wszystkie aplikacje są oparte na sieci internetowej. Zakup licencji uprawnia do hostingu danych, regularnych aktualizacji oprogramowania i wsparcia. W ten sposób Dräger z powodzeniem realizuje w ramach Smart Safety koncepcję „oprogramowania jako usługi" (Software-as-a-Service, SaaS).

Fels-Werke GmbH

Firma z siedzibą w niemieckim Goslar specjalizuje się w wydobyciu wapienia i wytwarzaniu wapna oraz wyrobów wapiennych. Należy do obecnej na całym świecie irlandzkiej grupy Cement Roadstone Holding plc (CRH). W Niemczech Fels-Werke GmbH ma sześć zakładów przetwarzających wapień, jeden zakład przetwarzający dolomit i jedną fabrykę zapraw. Dodatkowo prowadzi zakład przetwarzający wapień w Czechach. W samych Niemczech firma produkuje rocznie około 5 mln ton wapna i wapienia do różnych zastosowań. Roczna wydajność wapienników wynosi około 2 mln ton. Wapienniki pracują w temperaturze od 900 do 1200 stopni Celsjusza na różnych paliwach.

Zdjęcia: Dräger / Fels-Werke GmbH

PREDYKCJA ZUŻYCIA URZĄDZEŃ CIŚNIENIOWYCH I PLANOWANIE INSPEKCJI Z WYKORZYSTANIEM METODOLOGII RBI (RISK-BASED INSPECTION)

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.

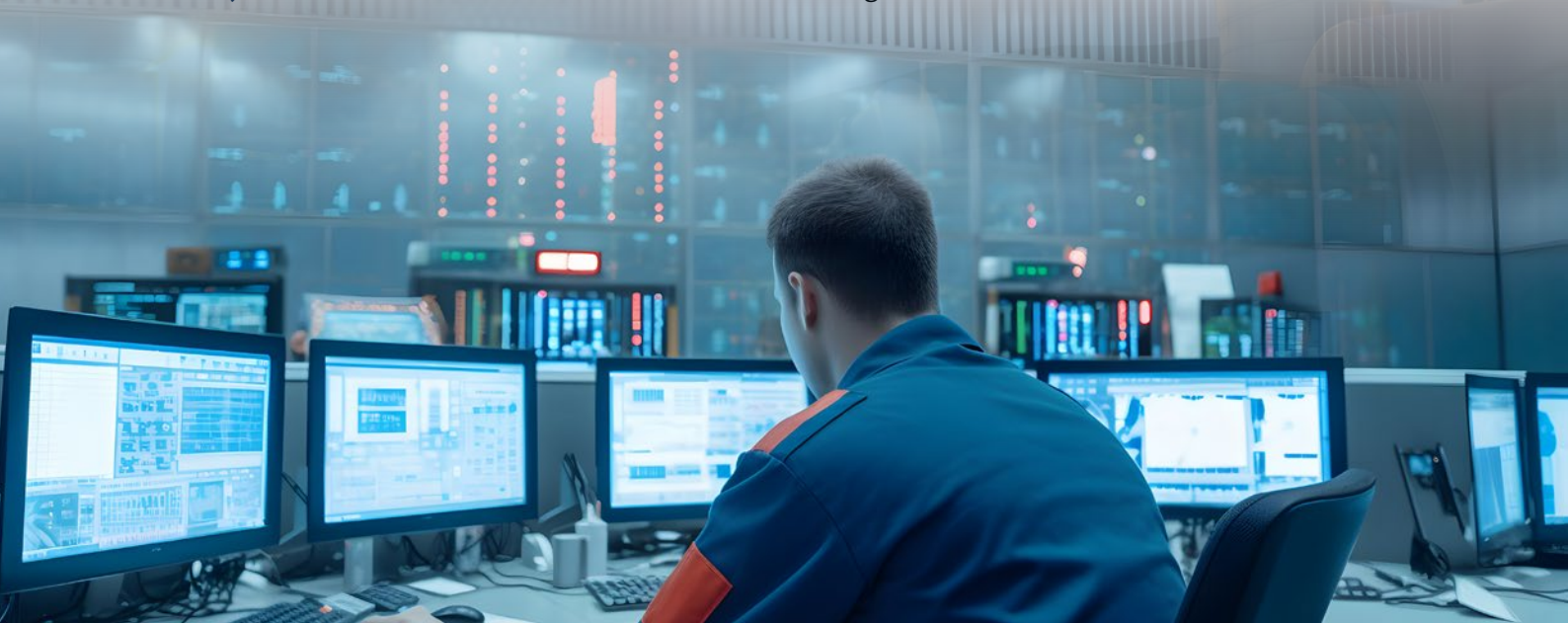
Ponad 10 lat temu Urząd Dozoru Technicznego wdrożył w praktykę dozorową metodologię RBI (Risk-based Inspection). Obecnie tysiące zbiorników ciśnieniowych i rurociągów technologicznych w polskim przemyśle zostało poddanych analizom RBI, które mają na celu predykcję ich zużycia i opracowanie niezbędnych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

Metodologię RBI, chociaż pierwotnie dedykowaną dla urządzeń ciśnieniowych eksploatowanych w przemyśle petrochemicznym i rafineryjnym, można wykorzystać, w całości lub częściowo, w planowaniu inspekcji urządzeń ciśnieniowych eksploatowanych w przemyśle chemicznym i energetycznym. Będzie to uzależnione miedzy innymi od tego, czy znane są mechanizmy degradacji materiału wywołane środowiskiem pracy i możliwe czy możliwe jest modelowanie konsekwencji uszkodzenia.

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*).

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 ta 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].

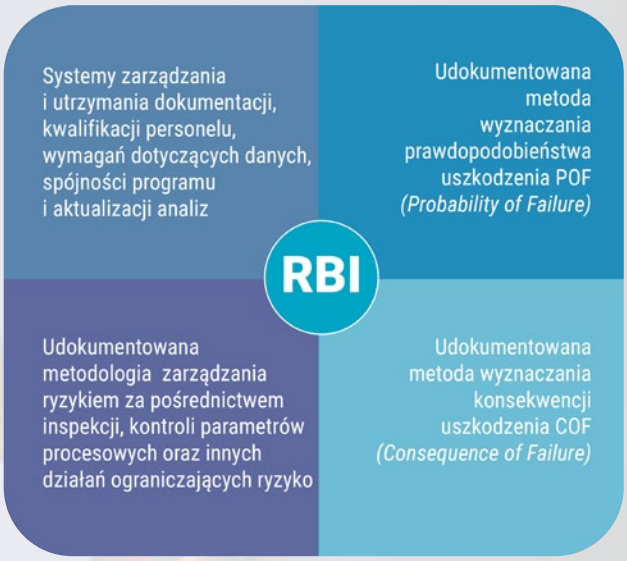
W tym celu wymagane jest udokumentowanie procesu analizy prawdopodobieństwa wystąpienia uszkodzeń w analizowanych urządzeniach, jak również konsekwencji wynikających z potencjalnego ich rozszczelnienia.

Do tego celu stosuje się 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 we wspomnianej wcześniej 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 zarządzania ryzykiem, a zatem jest analizą ciągłą wymagającą 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).

Implementacja kluczowych elementów RBI wymaga wdrożenia przez organizację tzw. Programu RBI [3], który obejmuje całość działań prowadzonych w celu opracowania, wdrożenia i utrzymania Programu



Rys. 1. Kluczowe elementy RBI

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 specyfikację techniczną WUDT-RBI-2017 „Warunki Urzędu Dozoru Technicznego – Planowanie inspekcji urządzeń ciśnieniowych w oparciu o analizę ryzyka RBI (Risk-based Inspection). Wymagania ogólne, tryb postępowania,** dokumentacja". W roku 2022 opublikowano znowelizowane wydanie warunków.

Celem opracowanych warunków jest ustalenie zasad funkcjonowania Programu RBI, który obejmuje 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-2022. System obejmuje 10 obszarów (rys. 2).

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.

W tym celu UDT 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-2017 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.

Celem wdrożenia analizy RBI jest prowadzenie udokumentowanych procesów analiz obejmujących identyfikację zagrożeń związanych z eksploatacją urządzenia, określenie potencjalnych mechanizmów uszkodzeń i miejsc ich występowania oraz 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 prowadzona jest przez interdyscyplinarny zespół składający się z inżynierów eksploatującego oraz wyznaczonych inspektorów UDT.

RBI jest procesem ciągłym służącym do zarządzania ryzykiem urządzeń. Uproszczony schemat blokowy RBI (rys. 3) prezentuje swojego rodzaju 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

System zarządzania 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

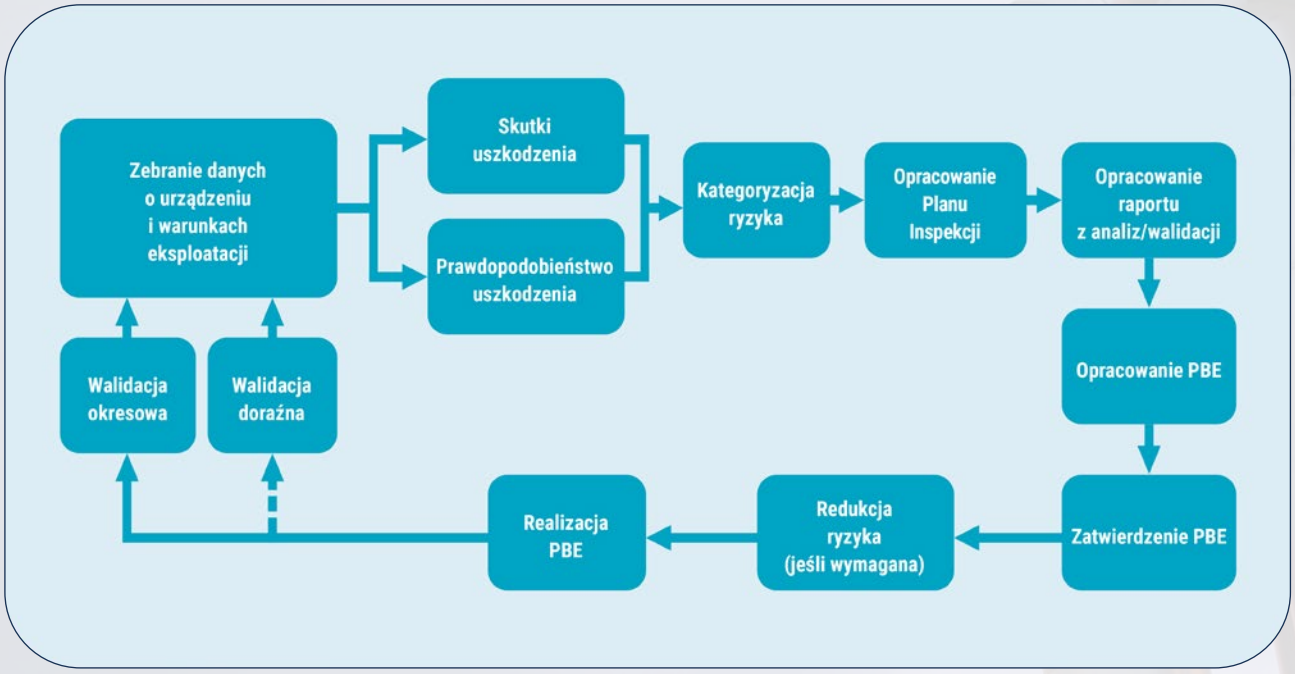
Tabela 1. Skład zespołu RBI

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 **Odpowiedzialna osoba 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 wzajemne 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 posiadać podstawowe przeszkolenie z metodologii RBI**

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. Jak widać, 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 nie dłuższy niż 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**
• **Formę raportowania badań NDT i DT**
• **Niezbędne do monitorowania parametry technologiczne**
• **Zasady i terminy walidacji analizy RBI oraz Programu Badań Eksploatacyjnych**



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 jest realizowane 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.

- Pozwala to również na 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, patrzy się na urządzenie ciśnieniowe, nie tylko oceniając jego stan techniczny, ale przede wszystkim zastanawiając się nad jego przyszłością i mając na uwadze warunki pracy oraz możliwe do przewidzenia zmiany, które mogą negatywnie wpłynąć na jego stan techniczny.

UWAGA

Uzyskanie wymiernych efektów z 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 oznacza ich dokładność i wiarygodność.

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 ponad 10 lat doświadczeń w predykcji zużycia urządzeń w przemyśle rafineryjnym, chemicznym i petrochemicznym.

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

Literatura:

1. API RP 580 Risk-based Inspection, Third Edition, February 2016.
2. RBI (Risk Based Inspection) – planowanie Inspekcji na podstawie Analizy Ryzyka https://www.udt.gov.pl/ekspertyzy-techniczne/analiza-zagrozen-i-oceny-ryzyka/rbi-risk-based-inspection-planowanie-inspekcji-na-podstawie-analizy-ryzyka
3. WUDT-RBI-2022 Warunki Urzędu Dozoru Technicznego – Planowanie inspekcji urządzeń ciśnieniowych w oparciu o analizę ryzyka RBI (Risk Based Inspection). Wymagania ogólne, tryb postępowania, dokumentacja.
4. WUDT-RBI-2022 Warunki Urzędu Dozoru Technicznego - Planowanie inspekcji urządzeń ciśnieniowych w oparciu o analizę ryzyka RBI (Risk Based Inspection). Wymagania ogólne Tryb postępowania, dokumentacja.
5. API Recommended Practise 584. Integrity Operating Windows, May 2014.

CYFROWA I BEZPIECZNA CHEMIA – PIERWSZA EDYCJA FORMATU „WORKSHOPS&NETWORKING PIPC" ZA NAMI

W dobie wszechobecnej transformacji kluczowe miejsce zajmuje przemysł chemiczny, który ze względu na swoje ogromne znaczenie dla gospodarki, dotykany jest przez wiele wyzwań. Wśród nich można wskazać zmienność regulacyjną, potrzebę finansowania, zapewnienie odpowiednich kadr, dostępność do technologii czy infrastruktury. To właśnie wokół zagadnienia transformacji i towarzyszących jej wyzwań odbywało się wydarzenie Polskiej Izby Przemysłu Chemicznego „Workshops&Networking PIPC: Cyfrowa i bezpieczna – transformacja przemysłu chemicznego", które odbyło się 20–21 września 2023 r. w Hotelu Novotel w Katowicach. Tym razem nie była to tradycyjna konferencja, ale platforma wymiany wiedzy w formule warsztatów, pokazów, otwartych dyskusji, zwiększonego czasu na networking, zwieńczona dyskusjami moderowanymi w formule round-table

Największe wyzwania w transformacji przemysłu chemicznego? Regulacje i dostępność technologii

Wydarzenie rozpoczęło się od wspólnej dyskusji moderowanej przez **Marcina Przygudzkiego, Koordynatora Pionu Projektów i Komunikacji, Senior Eksperta, Polska Izba Przemysłu Chemicznego**, w której uczestniczyły ekspertki **Agnieszka Majchrzak, Kierownik Biura Bezpieczeństwa Procesowego, ORLEN** oraz **Barbara Makowska, Health&Safety Manager, CIECH**, a także wszyscy uczestnicy spotkania, którzy mieli okazję odpowiadać na te same pytania w ankiecie „na żywo". Agnieszka Majchrzak z Grupy ORLEN podkreśliła, że jednym z głównych wyzwań jest połączenie nowoczesnych technologii z obowiązującymi regulacjami bezpieczeństwa, jak np. Dyrektywa SEVESO III, podczas gdy Barbara Makowska z Grupy CIECH wskazała, że w całym procesie transformacji nie można zapominać o człowieku, jego roli i konieczności ciągłego szkolenia personelu w zakresie nowych technologii. Z kolei ankietowani dostrzegli, że największe wyzwanie stanowią dwa elementy – regulacje oraz dostęp do technologii. W kolejnej części dyskusji ekspertki podzieliły się szeregiem aktywności, które wdrażają reprezentowane przez nie przedsiębiorstwa, aby sprostać wymaganiom transformacji, która jest wieloaspektowa – zielona, energetyczna, cyfrowa, a jednocześnie powinna być bezpieczna i niewpływająca na konkurencyjność rynkową. W odpowiedzi na zadane pytanie „Co może pomóc przemysłowi w transformacji?" wiele osób wskazało cyfryzację, digitalizację czy wykorzystanie sztucznej inteligencji. Oznacza to, że przedstawiciele branży chemicznej są świadomi, że droga transformacji wiedzie przez wdrażanie rozwiązań przemysłu 4.0. Drugim ciekawym aspektem, na który zwróciły uwagę zarówno prelegentki, jak i biorący udział w ankiecie goście, było odpowiednie zarządzanie w przedsiębiorstwach i umiejętności miękkie – co kryło się pod takimi hasłami jak: świadomość, elastyczność, komunikacja, zrozumienie problemów, społeczna świadomość i zmiana mentalności. Dyskusja wyraźnie pokazała, że cała branża jest świadoma konieczności adaptacji do zmieniających się warunków, lecz aby to zrobić skutecznie, firmy muszą równie mocno skupić się na ludziach, jak i na technologii. Ostatecznie to połączenie wiedzy, technologii i ludzkich kompetencji będzie decydować o konkurencyjności i sukcesie przemysłu chemicznego w przyszłości.

Cyfrowa i bezpieczna chemia „idą pod rękę"

Kolejną część wydarzenia stanowiły warsztaty, które odbywały się w równoległych sesjach. Jeden blok poświęcony został zagadnieniom realizowanym w ramach **Programu Bezpieczna Chemia**, drugi

Panel otwierający w formie standingowej

poświęcony został **Projektowi Chemia 4.0**. **Autorami obydwu inicjatyw jest Polska Izba Przemysłu Chemicznego**, która projekt o bezpieczeństwie zapoczątkowała w latach 2013-2014, zaś zagadnieniem przemysłu 4.0 zajmuje się już od dawna, a w ramach projektu – od 2018 r. Coraz częściej jednak w wyzwaniach dotyczących zapewnienia bezpieczeństwa procesowego czy BHP wykorzystuje się możliwości narzędzi cyfrowych. Bezpieczna chemia to także bezpieczna transformacja przemysłu chemicznego, a więc prowadzona w stabilny i zrównoważony sposób, dlatego możliwość wykorzystania digitalizacji widoczna jest również w obszarach, które optymalizują działania przedsiębiorstwa, poprawiają efektywność energetyczną czy monitorują emisyjność. W opublikowanym przez Komisję Europejską dokumencie „Transition pathway for chemical industry" („Ścieżka transformacji przemysłu chemicznego w UE") wskazano, że przemysł chemiczny, jako czwarty co do wielkości przemysł w Unii Europejskiej, odgrywa kluczową rolę w europejskiej „bliźniaczej" transformacji, czyli zielonej i cyfrowej. Wśród rekomendacji zawartych w przytoczonym dokumencie znalazło się także m.in. wykorzystywanie potencjału narzędzi 4.0 na rzecz realizowania Strategii ds. Zrównoważonych Chemikaliów (CSS), co również jest przedmiotem prac zarówno Komisji Bezpieczeństwa i Techniki PIPC, jak i Programu Bezpieczna Chemia. Można powiedzieć, że ostatnie lata wskazują, że Projekt Chemia 4.0 stał się niejako odpowiedzią na wyzwania omawiane w Programie Bezpieczna Chemia, stąd połączenie obydwu tematów w ramach jednego wydarzenia.

Potęga transformacji cyfrowej a cyberbezpieczeństwo

Warsztaty w ramach Projektu Chemia 4.0 otworzyło spotkanie z firmą **ABB**, które poświęcone zostało optymalizacji kosztów pracy zakładów przemysłowych przy użyciu zaawansowanego systemu klasy EMS (*Energy Management System*). Sesja miała na celu pogłębienie wiedzy na temat mechanizmów optymalizacyjnych oraz utrzymania ciągłości działania zakładów energochłonnych. Uczestnicy zapoznali się z praktycznymi aspektami tego podejścia, bazującymi na realnych przykładach z różnorodnych problemów – od liniowych po bardziej skomplikowane nieliniowe zagadnienia. Szkolenie podkreślało znaczenie skutecznego monitorowania produkcji oraz utraty energii, podnosząc zdolność do adaptacji do dynamicznie zmieniających się warunków rynkowych. Spotkanie prowadzone było przez **Marka Sulewskiego, Area Sales Managera i Marcina Bartosza, System Engineera z ABB Polska,** którzy dzielili się wiedzą i doświadczeniem na temat wdrażania EMS w przemyśle chemicznym.

Kolejna sesja zorganizowana została przez **Enxoo we współpracy z Salesforce i CIECH Sarzyna**. Spotkanie było poświęcone prezentacji case-study dotyczącego wdrożenia nowoczesnych technologii w przedsiębiorstwie chemicznym. Uczestnicy warsztatów mogli zgłębić wiedzę w zakresie najnowszych trendów i innowacyjnych technologii, które kształtują przyszłość branży chemicznej. Kluczowym elementem spotkania była prezentacja dotycząca sposobu,

w jaki CIECH Sarzyna usprawniła procesy sprzedaży i obsługi klienta dzięki zaawansowanym narzędziom cyfrowym. **Magdalena Forkasiewicz, Product Owner i Salesforce Consultant, Enxoo** dzieliła się wiedzą na temat roli technologii w osiągnięciu większej sprawności biznesowej w przemyśle chemicznym. W warsztacie towarzyszyli jej także **Krzysztof Rachwalski, Account Executive, Salesforce** oraz **Elżbieta Żórawska-Gałuszka, Kierownik Aplikacji Digitalowych, CIECH Services**.

Sesja warsztatowa w ramach Projektu Chemia 4.0

Inny przykład case-study z wykorzystania technologii 4.0 omówił ekspert od urządzeń ciśnieniowych Urzędu Dozoru Technicznego – **Tomasz Klinkosz, Specjalista Risk Based Inspection**. Prelegent skupił się na prezentacji technologii cyfrowego bliźniaka (*Digital Twin*) i jej kluczowych korzyści dla przemysłu. Uczestnicy mieli okazję poznać technologię Digital Twin jako narzędzie służące do zarządzania produktem, utrzymania ciągłości jego działania oraz wsparcia dla inżynierów w analizie całego cyklu życia urządzeń. Przybliżone zostały możliwości technologii w odtwarzaniu rzeczywistych zachowań urządzeń, przewidywaniu ich funkcjonowania oraz monitorowaniu ich aktualnego stanu. Uczestnicy mogli zrozumieć, jak technologia Digital Twin może przyczynić się do optymalizacji procesów konserwacji, zwiększenia niezawodności, ograniczenia kosztów i poprawy bezpieczeństwa.

Korzystanie z cyfrowych rozwiązań niesie za sobą również ryzyko. W ostatnich latach cyberataki na firmy w Polsce oraz w Europie stały się częstym zjawiskiem, co sprawiło, że kwestie związane z cyberbezpieczeństwem zajęły kluczowe miejsce w strategiach bezpieczeństwa przedsiębiorstw. Jako odpowiedź na rosnące zagrożenia w cyberprzestrzeni, Unia Europejska wprowadziła Dyrektywę NIS2. Ta zaktualizowana regulacja skupia się na ochronie danych przedsiębiorstw działających w obszarze Unii Europejskiej i narzuca bardziej rygorystyczne wymagania dla podmiotów biznesowych. W związku z nowymi regulacjami, kraje członkowskie UE musiały dostosować krajowe przepisy, a firmy poddane zostały presji, by przystosować się do zaostrzonych wymogów w ograniczonym czasie. Aby poruszyć kluczowe wyzwania związane z wdrażaniem Dyrektywy NIS2 oraz skutecznymi strategiami dla przedsiębiorstw został zorganizowany specjalny warsztat. Podczas tej sesji, **Emilia Zalewska, ekspert ds. Cyberpolicy oraz Paulina Popow, Młodsza Specjalistka ds. analiz strategicznych z obszaru cyberbezpieczeństwa z Naukowej i Akademickiej Sieci Komputerowej (NASK) – Państwowego Instytutu Badawczego**, podzieliły się swoją wiedzą, oferując praktyczne porady i wskazówki dla firm dążących do zwiększenia swojego poziomu cyberbezpieczeństwa.

Bezpieczna przyszłość przemysłu chemicznego

Równolegle odbywały się warsztaty i spotkania w ramach Programu Bezpieczna Chemia. Na pierwszy z nich zaprosili eksperci **Dräger Polska**. Warsztat skupił się na jednym z kluczowych aspektów w bezpieczeństwie przemysłu chemicznego – detekcji gazów. Uczestnicy warsztatu mieli okazję zgłębiać najnowsze osiągnięcia w dziedzinie stacjonarnej detekcji gazów, z naciskiem na cechy zapewniające najwyższe standardy bezpieczeństwa w obszarach chronionych. Ponadto, przedstawione zostało, jak w praktyce wygląda współdziałanie stacjonarnych i mobilnych systemów detekcji gazów. Zasadniczą część warsztatu stanowiło omówienie konfiguracji systemów oraz krytycznych procedur reakcji na wykrycie gazów niebezpiecznych. Całość prowadzona była przez **Michała Motykę, Dyrektora Sprzedaży i Marketingu oraz Tomasza Domżalskiego, Lidera Sekcji Systemów Detekcji Gazowej z Dräger Polska**.

Zagadnienia związane z detekcją gazów kontynuował przedstawiciel firmy **Atest Gaz, Marek Hiero, Dyrektor Działu Sprzedaży**. W trakcie warsztatu poświęconego problematyce wycieków gazów niebezpiecznych w zakładach chemicznych, uczestnicy zgłębiali kluczowe aspekty zapobiegania i minimalizacji strat związanych z takimi wyciekami. Poruszano kwestie związane z komunikacją zagrożeń oraz eksploatacją urządzeń w strefach o podwyższonym ryzyku. Uczestnicy mieli okazję dowiedzieć się o historii systemów detekcji gazów, zrozumieć pojęcia takie jak ryzyko, zagrożenie czy LOPC oraz poznać konkretne wymagania stawiane tym systemom. Wspólne refleksje i obserwacje skupiały się na budowie niezawodnych systemów detekcji, które gwarantują minimalizację strat, zwiększają bezpieczeństwo personelu oraz są pewne w działaniu. Jednym z kluczowych pytań poruszanych podczas warsztatu było, czy wykrycie wycieku gazu niebezpiecznego powinno prowadzić do zatrzymania instalacji procesowej, aby uniknąć przestojów i dodatkowych kosztów.

Warsztat nt. klasyfikacji litu

Inne specjalistyczne warsztaty prowadzone były przez **Climbex** we współpracy z firmą **Dekonta** z Czech. W tej sesji skupiono się na nowoczesnych rozwiązaniach pro-ekologicznych oraz dekontaminacji substancji PFAS. Uczestnicy mieli okazję zgłębić tematykę koncentratów piany gaśniczej stosowanej przez przemysłową straż pożarną, poznając najnowsze metody zastępowania i dekontaminacji tych substancji. Dodatkowo omówiono innowacyjne techniki badania terenów zanieczyszczonych chemikaliami, w tym zaawansowane metody bezpośredniego wiercenia, wtryskiwania oraz monitorowania zanieczyszczeń w gruncie. Omówiono również biotechnologiczne podejście do oczyszczania powietrza w przemyśle z uwzględnieniem wykorzystania biofiltrów. Na koniec zaprezentowano skuteczne strategie zarządzania kryzysowego oraz innowacyjne rozwiązania opracowane przez Dekonta w sytuacjach awaryjnych. Wiedza była przekazywana przez ekspertów z obu firm: **Grzegorza Szymańskiego, International Business Develompent Directora z Climbex oraz Vojtecha Musila, Business Directora z Dekonta**.

Duże zainteresowanie wzbudziło spotkanie na temat energetyki jądrowej. W ramach warsztatu „Atom w zakładzie przemysłowym" opowiedziano o możliwościach wprowadzenia technologii HTGR (*High Temperature Gas cooled R*eactor) oraz jej potencjale w kontekście przemysłu chemicznego. Uczestnicy dowiedzieli się, jak technologia reaktorów wysokotemperaturowych, będąca jednym z innowacyjnych podejść w energetyce jądrowej, może przynieść znaczące korzyści przemysłowi chemicznemu. Kluczowym atutem tej technologii jest zdolność do wytwarzania zarówno energii elektrycznej, jak i ciepła, co ma szczególne zastosowanie w procesach technologicznych przemysłu chemicznego, takich jak produkcja wodoru. Technologia HTGR, ze względu na jej unikalne właściwości bezpieczeństwa, takie jak samoistne ochładzanie w przypadku awarii i użycie gazu helowego do chłodzenia, stała się obiektem intensywnych badań w wielu krajach. W Polsce za badania nad tą technologią odpowiadało **Narodowe Centrum Badań Jądrowych (NCBJ),** którego przedstawiciele podzielili się wiedzą i doświadczeniem na temat potencjału technologii HTGR w kontekście krajowego przemysłu chemicznego.

Spośród wszystkich równoległych spotkań dwa z nich dostępne były dla wszystkich uczestników jednocześnie. Jednym z nich był **okrągły stół pt. „Niepewna przyszłość litu. Co czeka produkcję i recykling baterii?" organizowany we współpracy PIPC z BASF Polska oraz Polskim Stowarzyszeniem Paliw Alternatywnych (PSPA).** Skupiając się na propozycji Komisji Europejskiej dotyczącej klasyfikacji soli litu jako substancji reprotoksycznej, omawiane były potencjalne skutki tej decyzji dla przemysłu. Uczestnicy warsztatu zdobyli wiedzę na temat szerokiego spektrum zastosowań litu w różnych sektorach, od energetyki po kosmonautykę. Zwrócono uwagę na znaczenie Polski jako wiodącej siły w europejskim łańcuchu dostaw baterii, podkreślając, że baterie litowo-jonowe stanowiły ponad 2,4% polskiego eksportu w 2022 roku. Spotkanie prowadzili **Szymon Domagalski, Radca ds. Regulacji, Pion Rzecznictwa i Legislacji, Polska Izba Przemysłu Chemicznego oraz dr inż. Anna Zalewska, Advocacy Manager, BASF Polska**. W wydarzeniu wzięli udział reprezentanci sektora chemicznego, motoryzacyjnego i bateryjnego. Głos w dyskusji zabierali m.in. **Jérémy Pinte, Policy Officer – CLP, GHS and Fertilising Products w Komisji Europejskiej, dr Paul Xaver Schuster, Senior Manager Regulatory Affairs, Catalysts Division – ERT, BASF, Maria Majewska, New Mobility Manager, PSPA, Marcin Witaszek, Radca Prawny, Polski Związek Przemysłu Motoryzacyjnego.**

Pierwszy dzień agendy premierowego wydarzenia Workshops&Networking PIPC zwieńczyło szkolenie praktyczne w siedzibie Dräger Polska. W ramach warsztatu zostały omówione procedury i dobre praktyki przed rozpoczęciem pracy w przestrzeniach zamkniętych, a w ramach części praktycznej wszyscy chętni, pod okiem doświadczonych ekspertów, mieli możliwość przeprowadzenia ewakuacji osoby poszkodowanej z takiego miejsca, korzystając ze sprzętu ucieczkowego oraz izolującego drogi oddechowe firmy Dräger. Wielu uczestników warsztatu podkreślało, że to właśnie praktyczne ćwiczenia dały im pewność w działaniu oraz przekonanie o nieocenionej wartości profesjonalnego wyposażenia w trudnych i nieprzewidywalnych warunkach pracy.

Dokąd zmierza przemysł chemiczny w erze transformacji?

Podsumowaniem wydarzenia była organizacja platformy do dalszych rozmów w formule

Warsztat praktyczny w siedzibie Dräger Polska

Dyskusje podczas śniadania biznesowego w formule round table

moderowanego śniadania biznesowego drugiego dnia spotkania. W round-table uczestniczyło sześciu moderatorów, którzy poruszali różne zagadnienia związane z transformacją przemysłu chemicznego i obecnymi trendami. **Tomasz Bukowski (go&biogas)** poruszył zagadnienia związane z realizacją założeń transformacyjnych poprzez inwestycje w biogazownie. **Paulina Flasińska (Instytut Przemysłu Organicznego Sieci Badawczej Łukasiewicz)** skupiła się na zrównoważonych chemikaliach i ich roli w bezpiecznej transformacji przemysłu. Z kolei **dr inż. Julian Malaka (Platforma Przemysłu Przyszłości)** zastanawiał się nad tym, czy przemysł chemiczny jest odpowiednio przygotowany na zmiany pod kątem kadr – luk kompetencyjnych w obszarze zawodów „cyfrowych" i „zielonych". **Janusz Malesa (Narodowego Centrum Badań Jądrowych)** podjął ważny temat energii jądrowej jako potencjalnego rozwiązania dla przemysłu chemicznego w kierunku bardziej zrównoważonej transformacji energetycznej. **Sylwia Macura-Targosz (Kancelaria SKS)** przybliżyła uczestnikom aspekty prawne związane z transformacją cyfrową przemysłu. Jej analiza skupiła się na tym, jak wygląda stan regulacyjny w obszarze wykorzystywania sztucznej inteligencji oraz jakie wyzwania prawne mogą się pojawić w nadchodzących latach. **Kamil Laskowski (WiseEuropa)** skierował uwagę na dekarbonizację przemysłu, analizując jej wpływ na konkurencyjność firm. Uczestnicy jego stolika zastanawiali się, czy można zrównoważyć dążenie do redukcji emisji z potrzebą bycia konkurencyjnym na globalnym rynku.

Każdy z moderatorów stolików wnosił unikalną perspektywę na temat przyszłości przemysłu chemicznego, co sprawiło, że dyskusje były żywiołowe i pełne różnorodnych punktów widzenia. Wszyscy uczestnicy śniadania biznesowego opuścili salę z nową wiedzą i inspiracją do dalszych działań w swoich organizacjach.

Artykuł opracowany przez Zespół Polskiej Izby Przemysłu Chemicznego

PIPC
POLSKA IZBA PRZEMYSŁU CHEMICZNEGO

1988-2023 35 lat

chemHR

PROGRAM ChemHR

- Wspieranie rozwoju współpracy nauka-przemysł;
- Dialog branży chemicznej z przedstawicielami uczelni;
- Promocja osiągnięć naukowych na wydarzeniach PIPC;
- Kampanie informacyjne dla studentów i pracowników naukowych;
- Bezpłatne uczestnictwo w Programie.

Więcej o Programie ChemHR:

www.chemhr.pl

PIPC
POLSKA IZBA PRZEMYSŁU CHEMICZNEGO

1988-2023
35
lat

BEZPIECZNA chemia

PROGRAM
BEZPIECZNA CHEMIA

- Seminaria, warsztaty, szkolenia;
- Prezentacje rozwiązań i najlepszych praktyk;
- Monitorowanie zmian prawnych;
- Współpraca z ekspertami i największymi firmami przemysłu chemicznego;
- Biuletyn Bezpieczna Chemia.

Więcej o Programie Bezpieczna Chemia:

www.programbezpiecznachemia.pl