

SYSTEMY SZTUCZNEJ INTELIGENCJI (AI) W PROCESIE ZARZĄDZANIA INTEGRALNOŚCIĄ MECHANICZNĄ URZĄDZEŃ CIŚNIENIOWYCH

CZY MOŻLIWE JEST ZAPEWNIENIE BEZPIECZEŃSTWA?



TOMASZ KLINKOSZ

Ekspert Urzędów
Ciśnieniowych
Urząd Dozoru Technicznego
Oddział w Gdańsku

SZTUCZNA INTELIGENCJA (AI) TO SZYBKO ROZWIJAJĄCA SIĘ RODZINA TECHNOLOGII, KTÓRA MOŻE PRZYNIEŚĆ WACHLARZ KORZYŚCI EKONOMICZNYCH I SPOŁECZNYCH W CAŁYM SPEKTRUM BRANŻ I DZIAŁAŃ SPOŁECZNYCH. MOŻE POPRAWIĆ PRZEWIDYWANIA, OPTYMALIZACJĘ OPERACJI I ALOKACJĘ ZASOBÓW, A TAKŻE PERSONALIZACJĘ ŚWIADCZENIA USŁUG. WYKORZYSTANIE SZTUCZNEJ INTELIGENCJI MA POTENCJAŁ WSPIERANIA SPOŁECZNYCH I ŚRODOWISKOWYCH ZMIAN. JEST TEŻ ŹRÓDŁEM KLUCZOWEJ PRZEWAGI KONKURENCYJNEJ PRZEDSIĘBIORSTW I GOSPODARKI EUROPEJSKIEJ.

Jednak te same elementy i techniki, które napędzają korzyści społeczno-ekonomiczne z zastosowania AI, mogą również wiązać się z nowymi zagrożeniami i negatywnymi konsekwencjami dla jednostek i społeczeństwa, czego dowodem mogą być tak niedawne doniesienia prasowe związane z zastosowaniem innowacyjnego rozwiązania, którym jest ChatGPT wdrożony przez firmę OpenAI. Włoski rząd wprowadził ograniczenia w dostępie do tej technologii, jak pisze portal money.pl [1]. Komisarz ds. rynku wewnętrznego Thierry Breton powiedział: „Sztuczna inteligencja jest środkiem, a nie celem. Ta technologia istnieje od kilkudziesięciu lat, ale osiągnęła nowe możliwości dzięki dostępnej obecnie mocy obliczeniowej. Oferuje ona ogromne możliwości w tak różnorodnych dziedzinach jak zdrowie, transport, energia, rolnictwo, turystyka czy bezpieczeństwo cybernetyczne, to wiąże się jednak również z szeregiem zagrożeń” [2].

W świetle tempa zmian technologicznych Unia Europejska jest zdecydowana dążyć do wyważonego podejścia w zakresie AI [3]. W tym celu w kwietniu 2021 r. powstał projekt rozporządzenia Parlamentu Europejskiego, dotyczącego ustanowienia zharmonizowanych przepisów odnoszących się do sztucznej inteligencji, tzw. **ARTIFICIAL INTELLIGENCE ACT**.

Tworzony akt prawny ma być stosowany bezpośrednio, czyli w ten sam sposób we wszystkich państwach członkowskich. W akcie tym w celu zapewnienia bezpieczeństwa AI przyjęto podejście oparte na analizie ryzyka.

Pojęcie sztucznej inteligencji nie jest jednoznaczne i może być interpretowane różnie. W tym celu w projekcie ww. rozporządzenia podjęto próbę zdefiniowania AI jako „**systemu sztucznej inteligencji**”. Określono, że oznacza on **OPROGRAMOWANIE**, które zostało opracowane z wykorzystaniem jednej lub kilku technik i podejść wymienionych w załączniku I do rozporządzenia i które może, dla danego zestawu celów określonych przez człowieka, generować dane wyjściowe, takie jak treści, prognozy, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję.

Projekt Rozporządzenia Unii Europejskiej [3] dotyczy ustanowienia:

- zharmonizowanych przepisów dotyczących wprowadzania do obrotu, oddawania do użytku i użytkowania systemów sztucznej inteligencji („systemów sztucznej inteligencji”) w Unii,
- zakazów niektórych praktyk związanych ze sztuczną inteligencją,
- szczególnych wymogów dotyczących systemów sztucznej inteligencji wysokiego ryzyka oraz obowiązków operatorów takich systemów,
- zharmonizowanych przepisów dotyczących przejrzystości systemów sztucznej inteligencji przeznaczonych do interakcji z osobami fizycznymi, systemów rozpoznawania emocji i systemów kategoryzacji biometrycznej oraz systemów sztucznej inteligencji wykorzystywanych do generowania treści obrazowych, dźwiękowych lub wideo oraz manipulowania nimi,
- przepisów dotyczących monitorowania i nadzoru rynku.

JAKIE TECHNOLOGIE OBJĘTE SĄ DEFINICJĄ SYSTEMU SZTUCZNEJ INTELIGENCJI?

W załączniku pierwszym do projektu rozporządzenia znajdziemy technologie mieszczące się w definicji systemu sztucznej inteligencji:

- podejścia oparte na uczeniu maszynowym, w tym uczeniu nadzorowanym, nienadzorowanym i uczeniu wzmacniającym, z wykorzystaniem szerokiej gamy metod obejmujących uczenie głębokie (Deep Learning),
- podejścia oparte na logice i wiedzy, w tym reprezentacja wiedzy, programowanie indukcyjne (logiczne), bazy wiedzy, mechanizmy wnioskowania i dedukcji, wnioskowanie (symboliczne) i systemy eksperckie,
- podejścia statystyczne, estymacja bayesowska, metody wyszukiwania i optymalizacji.



Jak widać, w definicji ujęto dość szeroką gamę technologii, w tym technologii stosowanych już obecnie w wielu gałęziach przemysłu. Definicja ta, a szczególnie uwzględnione w niej technologie, obecnie budzi szereg kontrowersji i może ulec modyfikacji w trakcie dalszych prac nad tym aktem prawnym. Istotne jest jednak uwzględnienie ryzyka, które niesie wdrażanie i stosowanie nowych technologii. Ważne jest wdrożenie odpowiednich rozwiązań konstrukcyjnych, organizacyjnych oraz prawnych mających na celu wyeliminowanie lub ograniczenie ryzyka.

Zastosowanie ww. technologii w przemyśle, a zwłaszcza w zakresie mającym wpływ na bezpieczeństwo i ciągłość działania infrastruktury krytycznej, wymaga zwrócenia szczególnej uwagi na zastosowania w elementach związanych z bezpieczeństwem.

Omawiany projekt rozporządzenia UE w części trzeciej zawiera wymagania dla tzw. systemów AI wysokiego ryzyka. Systemy kwalifikuje się do tej kategorii niezależnie od tego, czy są wprowadzane do obrotu, czy do użytku.

SYSTEM SZTUCZNEJ INTELIGENCJI UZNAJE SIĘ ZA SYSTEM WYSOKIEGO RYZYKA, JEŻELI SPEŁNIONE SĄ OBA NASTĘPUJĄCE WARUNKI:

- a) system AI ma być stosowany jako element bezpieczeństwa produktu lub sam jest produktem objętym unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku II projektu,
- b) produkt, którego elementem zabezpieczającym jest system AI, lub sam system AI jako produkt, musi przejść ocenę zgodności przeprowadzoną przez stronę trzecią w celu wprowadzenia tego

produktu do obrotu lub oddania do użytku zgodnie z prawodawstwem harmonizacyjnym wymienionym w załączniku II projektu.

WŚRÓD AKTÓW PRAWA ZHARMONIZOWANEGO WYMIENIONYCH W ZAŁĄCZNIKU II ZNALAZŁY SIĘ MIĘDZY INNYMI DYREKTYWA 2014/68/UE DOTYCZĄCA URZĄDZEŃ CIŚNIENIOWYCH ORAZ DYREKTYWA MASZYNOWA 2006/42/WE.

Systemy AI stanowiące elementy zabezpieczające lub mające wpływ na bezpieczeństwo produktów objętych m.in. wspomnianymi dyrektywami, zgodnie z projektem rozporządzenia dotyczącego AI, będą musiały spełniać wymagania określone dla systemów AI wysokiego ryzyka.

Jako systemy AI wysokiego ryzyka uznaje się również systemy AI wymienione w załączniku III projektu rozporządzenia, do których zalicza się między innymi systemy AI w obszarze **zarządzania i eksploatacji infrastruktury krytycznej** przeznaczone do stosowania jako elementy bezpieczeństwa w zarządzaniu ruchem drogowym i prowadzeniu go oraz w dostawie wody, gazu, ogrzewania i energii elektrycznej.

W załączniku III do projektu rozporządzenia wymieniono część obszarów zaliczanych do infrastruktury krytycznej, jednak lista może zostać rozszerzona, jeżeli systemy sztucznej inteligencji stwarzają zagrożenie dla zdrowia i bezpieczeństwa. Również wtedy, gdy ryzyko niekorzystnego wpływu na prawa podstawowe jest równoważne lub większe niż ryzyko stwarzane przez systemy sztucznej inteligencji wysokiego ryzyka, o których mowa w załączniku III projektu rozporządzenia.

Analizując powyższe zapisy, można wnioskować, że wymagania te mogą objąć również instalacje chemiczne, rafineryjne i petrochemiczne, systemy gazowe – szeroko pojęta energetyka – zaklasyfikowane jako systemy infrastruktury krytycznej.

Komisja Europejska w projekcie rozporządzenia UE określiła główne obszary wymagań dla systemów AI wysokiego ryzyka.

- Zgodność z wymaganiami
- System zarządzania ryzykiem
- Dane i zarządzanie danymi
- Dokumentacja techniczna
- Utrzymywanie zapisów
- Przejrzystość i dostarczanie informacji użytkownikom
- Nadzór ludzki
- Dokładność, solidność i cyberbezpieczeństwo

Poza wymaganiami dla procesu oceny zgodności, oznakowania znakiem CE, wymagań dla producentów, importerów czy dystrybutorów, projekt rozporządzenia określa obowiązki i wymagania dla użytkowników systemów AI wysokiego ryzyka.

Obszary wymagań wskazane w projekcie rozporządzenia nie odbiegają co do zasady od praktyki stosowanej w zarządzaniu bezpieczeństwem instalacji z zastosowaniem metodologii Risk Based Inspection, opisanej standardem API RP 580, uzupełnionej wymaganiami zawartymi w Warunkach Technicznych Urzędu Dozoru Technicznego WUDT-RBI. Ogólne informacje dotyczące tej metodologii można znaleźć w serii artykułów zamieszczonych w Biuletynie „Inspektor” [4] wydawanym przez Urząd Dozoru Technicznego oraz artykule „Dynamiczne zarządzanie ryzykiem instalacji przemysłowych. Optymalizacja procesu zarządzania ryzykiem z wykorzystaniem narzędzi przemysłu 4.0 [5].

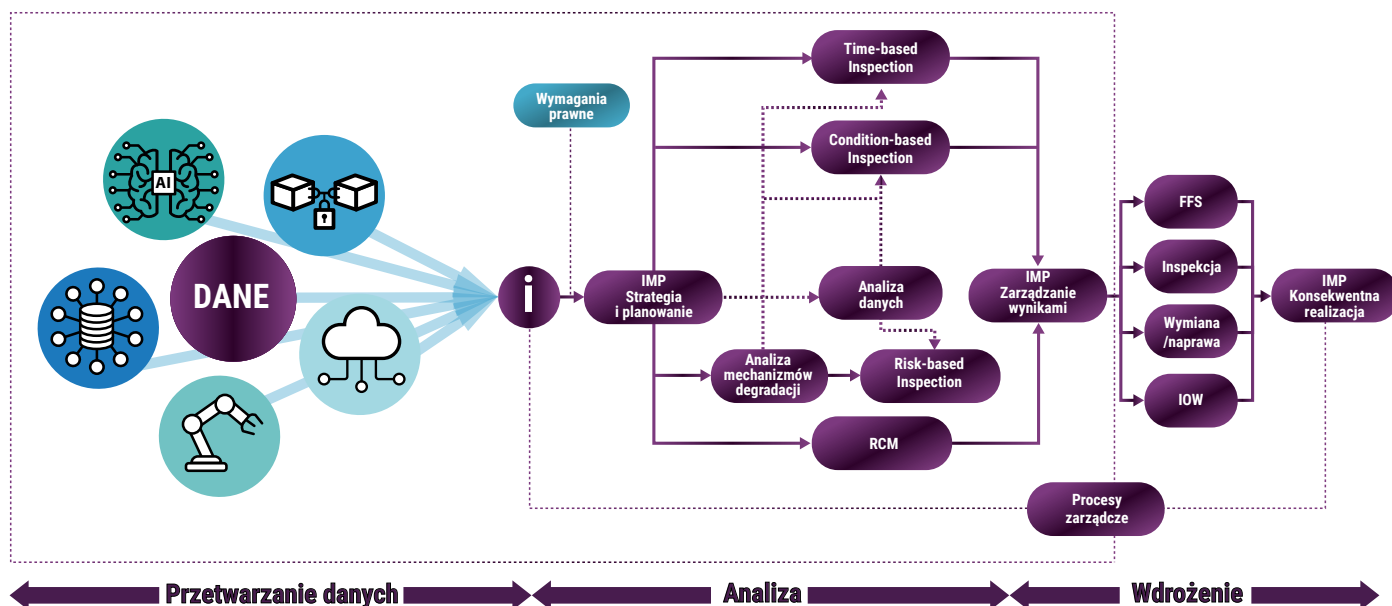
Rozwój technologii, a wraz z nim gromadzenie danych, ich zautomatyzowane analizowanie i wnioskowanie muszą być uwzględnione w procesie analizy i oceny ryzyka. **Ryzyka te będą zależały od konkretnego zastosowania.**

Jednym z zastosowań, w których technologie te są wdrażane, jest predycyjne utrzymanie ruchu urządzeń i instalacji technologicznych, w tym dynamiczne przewidywanie uszkodzeń oraz planowanie niezbędnych działań w celu monitorowania ryzyka.

Przykładem takiego systemu może być tzw. **cyfrowy bliźniak (Digital Twin)**. Rozwiązanie to szeroko stosowane jest w zarządzaniu niezawodnością i optymalizacji kosztów eksploatacji maszyn, takich jak turbozespoły, wieże wiatrowe, a coraz częściej również stosowane jest dla urządzeń i instalacji ciśnieniowych w wielu gałęziach przemysłu energetycznego. UDT również rozwija swoje kompetencje w zakresie tej technologii, uczestnicząc jako partner merytoryczny w pilotażowym wdrożeniu cyfrowego bliźniaka dla części instalacji procesowej Rafinerii Gdańskiej [6, 7].

Jednym z największych wyzwań aplikacji cyfrowych bliźniaków jest często omawiany problem silosów danych. W branżach związanych z energetyką generowana jest ogromna różnorodność danych, którymi trzeba zarządzać za pomocą kilku różnych narzędzi programowych, baz danych i dokumentów. Wiąże się to z brakiem ustandaryzowanych struktur danych. Konieczna jest poprawa integracji danych w całym cyklu życia instalacji oraz zapewnienie ujednoliconego standardu danych i jednego wiarygodnego ich źródła do wymiany i udostępniania [8]. Wyzwanie to, poza dokładnością i wiarygodnością zastosowanych modeli predycyjnych, ma zasadniczy wpływ na wiarygodność uzyskanych danych oraz możliwość ich wykorzystania w procesie podejmowania decyzji.

Kluczowe jest dostarczenie właściwych informacji w odpowiednim czasie do odpowiednich adresatów. Na poniższym rysunku przedstawiono przykładową strukturę przepływu danych i informacji w procesie podejmowania decyzji podczas tworzenia i realizacji programu zarządzania integralnością mechaniczną (IMP Integrity Management Program) urządzeń w ciśnieniowych w przemyśle rafineryjnym.



Przedstawiony proces stanowi uzupełnienie stosowanej obecnie metodologii RBI przy dążeniu do optymalizacji procesu pozyskiwania danych i generowania informacji. Należy szczególnie odróżnić dane od informacji.

Niektóre dane mogą bezpośrednio stanowić nośnik informacji, jak np. rodzaj materiału konstrukcyjnego urządzenia ciśnieniowego czy wymiary geometryczne.

Inaczej jest w przypadku informacji niezbędnej do wyznaczenia prawdopodobieństwa uszkodzenia urządzenia, którą jest m.in. szybkość korozji wynikająca z aktywności mechanizmów degradacji oraz jej charakter (tzw. Corrosion Rate, CR).

W przypadku informacji o wartości prędkości korozji CR, która ma zostać przyjęta do wyliczenia prawdopodobieństwa uszkodzenia, niezbędne jest pozyskanie niekiedy wielu danych takich jak:

- gatunek materiału konstrukcyjnego,
- rodzaj konstrukcji i jego cechy geometryczne,
- dane o uszkodzeniach i naprawach,
- rodzaj medium procesowego oraz rodzaj i ilość zawartych tzw. zanieczyszczeń przyczyniających się do aktywności konkretnego mechanizmu degradacji,
- temperatura robocza,
- ciśnienie robocze,
- zakres i efektywność przeprowadzonych inspekcji,
- wyniki przeprowadzonych inspekcji, w tym pomiarów grubości ścianek urządzenia, mapowania korozji, badań wizualnych, ocena dokumentacji fotograficznej uszkodzeń korozyjnych,
- zakres i efektywność przeprowadzonych inspekcji,
- dane o zaburzeniach i odchyleniach procesowych.

Zakres danych, które należy wziąć pod uwagę, jest w tym przypadku obszerny.

W każdym indywidualnym przypadku wpływ poszczególnych danych może być różny. W procesie RBI dane te są gromadzone, dokumentowane i analizowane przez inżyniera ds. korozji, a następnie informacja weryfikowana jest przez **zespół RBI** [9]. Proces ten jest jednak czasochłonny i wymaga zaangażowania specjalistów z kilku branż. Jego optymalizacja jest jednym z obszarów, w których np. algorytmy oparte na uczeniu maszynowym mogą stanowić wsparcie w poszukiwaniu korelacji pomiędzy danymi pozyskiwanymi z systemów monitorowania procesu.

Kluczowe jest ustalenie wiarygodności uzyskanej na podstawie danych informacji o CR. Procesy korozyjne są złożone, zmienne w czasie, a w przypadku procesów rafineryjnych również trudne do monitorowania. Zatem niepewność wynikająca z oszacowania prędkości korozji oraz charakteru spodziewanych uszkodzeń, tzn. czy spodziewamy się ubytków o charakterze np. lokalnym czy ogólnym, zależy od tego, jaka strategia planowania zarządzania integralnością urządzenia zostanie przyjęta.

W przypadku urządzeń objętych dozorem technicznym UDT wymagania dla tego procesu, w tym jego dokumentowania, zawarto w warunkach WUDT-RBI [10]. Gdy proces ten realizowany jest przy wsparciu

systemów sztucznej inteligencji, może istnieć również konieczność uwzględnienia wymagań wspomnianego wcześniej projektu rozporządzenia UE.

Czy zatem można zapewnić bezpieczeństwo, stosując rozwiązania oparte na systemach AI? Obecny stan wiedzy nie pozwala na jednoznaczną ocenę. Zależy to od zastosowanej technologii oraz zakresu jej zastosowania. W znacznym stopniu bezpieczeństwo AI zależy również od sposobu jego wykorzystania. Istotne jest, aby w dążeniu do optymalizacji z wykorzystaniem systemów AI zachować szczególną ostrożność i analizować potencjalne ryzyka. Systemy te należy traktować jako wsparcie, a nie zastąpienie doświadczenia i wiedzy inżynierskiej, które szczególnie w początkowym procesie wdrażania odgrywają kluczową rolę. Ważne jest również odpowiednie dokumentowanie wszystkich przyjmowanych założeń dotyczących danych, ich obróbki oraz założeń i „uproszczeń” w stosowanych modelach. Aspekt ten został uwzględniony w projekcie wymagań prawnych UE [3].



Literatura:

1. <https://www.money.pl/gospodarka/chatgpt-zablokowany-kolejne-kraje-mysla-o-podobnym-kroku-wlosi-dali-sygnal-6884970980604832a.html>.
2. https://ec.europa.eu/commission/presscorner/api/files/document/print/pl/ip_21_1682/IP_21_1682_PL.pdf.
3. EUROPEAN COMMISSION Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, Brussels, 21.4.2021.
4. <https://www.udt.gov.pl/inspektor-on-line>.
5. https://www.kierunekbmp.pl/Resources/magazyn/3_2022_chemia_portal.pdf.
6. Powstanie cyfrowa wersja gdańskiej rafinerii. Cyfrowy bliźniak infrastruktury, <https://biznes.trojmiasto.pl/Powstanie-cyfrowa-wersja-gdanskiej-rafinerii-Cyfrowy-blizniak-infrastruktury-n169178.html>.
7. Microsoft stworzy cyfrowego bliźniaka rafinerii LOTOS, <https://www.computerworld.pl/news/Microsoft-stworzy-cyfrowego-blizniaka-rafinerii-LOTOS,440136.html>.
8. Libing Gaoorcid, Mengda Jia, Dongqing Liu, Process Digital Twin and Its Application in Petrochemical Industry, Journal of Software Engineering and Applications, Vol.15 No.8, August 2022.
9. T. Klinkosz Biuletyn „Inspektor” 1/2021 predykcja zużycia urządzeń ciśnieniowych i planowanie inspekcji urządzeń ciśnieniowych z wykorzystaniem metodologii RBI Risk Based Inspection.
10. <https://www.udt.gov.pl/warunki-wudt-2/115-udt/baza-wiedzy/warunki-wudt/2138-warunki-urzedu-dozeru-technicznego-specyfikacja-techniczna-wydanie-11-2022-planowanie-inspekcji-urazden-cisnieniowych-w-oparciu-o-analize-ryzyka-rbi-risk-based-inspection>.