

# DIGITAL TWIN I SYSTEMY O SAMOZMIENIAJĄCYM SIĘ ZACHOWANIU

## ZAPEWNIENIE BEZPIECZEŃSTWA BIEŻĄCE ZMIANY W REGULACJACH PRAWNYCH



**DR INŻ. MARCIN WOLEJKO**

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



**MGR INŻ. TOMASZ KLINKOSZ**

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



**MGR INŻ. SEBASTIAN KOSOWSKI**

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



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

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

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

## TECHNOLOGIA PRZEMYSŁU 4.0 DLA INSTALACJI PROCESOWYCH

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

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

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

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

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

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

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

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

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

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

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

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

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

### Automatyzacja zadań

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

### Przetwarzanie złożonych lub dużych zbiorów danych

- dane procesowe
- wyniki badań niszczących i niszczących
- analiza wyników modeli predykcyjnych

### Zgłaszanie anomalii lub interesujących wydarzeń

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

### Znakowanie danych i korekcja błędów

- zarządzanie danymi IOW (Integrity Operating Windows)

### Funkcje zintegrowane

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

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

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

## ROZPORZĄDZENIE MASZYNOWE

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

### Główne cele zmian wprowadzanych przez MR

- cyfrowe instrukcje i deklaracje zgodności
- równość szans podmiotów gospodarczych na rynku
- dostosowanie do zagrożeń wynikających z rozwoju technologii

### Zmiany w stosunku do dyrektywy maszynowej 2006/42/WE

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

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

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

### PRZEZNACZENIE DIGITAL TWIN – DO CZEGO SŁUŻĄ?

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

#### W [7] wyróżniono trzy typy Digital Twins:

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

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

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

Grieves i Vickers w 2017 r. [10] sformułowali dwa następujące przeznaczenia DT:

1. **Predykcyjne (Predictive)** – Digital Twin będzie umożliwiał przewidywanie zachowania obiektu rzeczywistego.

2. **Badawcze (Interrogative)** – cyfrowe kopie obiektu rzeczywistego będą umożliwiały wgląd w stan aktualny oraz historię zachowań obiektu rzeczywistego.

Również w 2017 r. w pracy [9] Elisy Negri i zespołu, na podstawie przeglądu dostępnej wówczas literatury, wskazano trzy główne kierunki zastosowania Digital Twin:

1. Wsparcie analiz stanu technicznego / kondycji obiektu rzeczywistego w celu usprawnienia planowania i czynności konserwacyjnych.
2. Cyfrowe odzwierciedlenie życia obiektu fizycznego, aby zbadać jego długoterminowe zachowanie, przewidzieć jego działanie, zapewnić ciągłość informacji na różnych etapach cyklu życia, prowadzić tzw. Virtual Commissioning lub zarządzać cyklem życia urządzeń IoT.
3. Wspomaganie w podejmowaniu decyzji poprzez wykonywanie analiz inżynierskich i statystycznych w celu optymalizacji zachowania systemu na etapie projektowania, przewidywania i ulepszania przyszłych osiągnięć czy parametrów produktu.

### KONSTRUKCJA DIGITAL TWIN

Można wyróżnić dwa główne kierunki/technologie budowy DT:

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

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

### DANE DIGITAL TWIN – NIEODŁĄCZNY ELEMENT, ALE I WARTOŚĆ DODANA

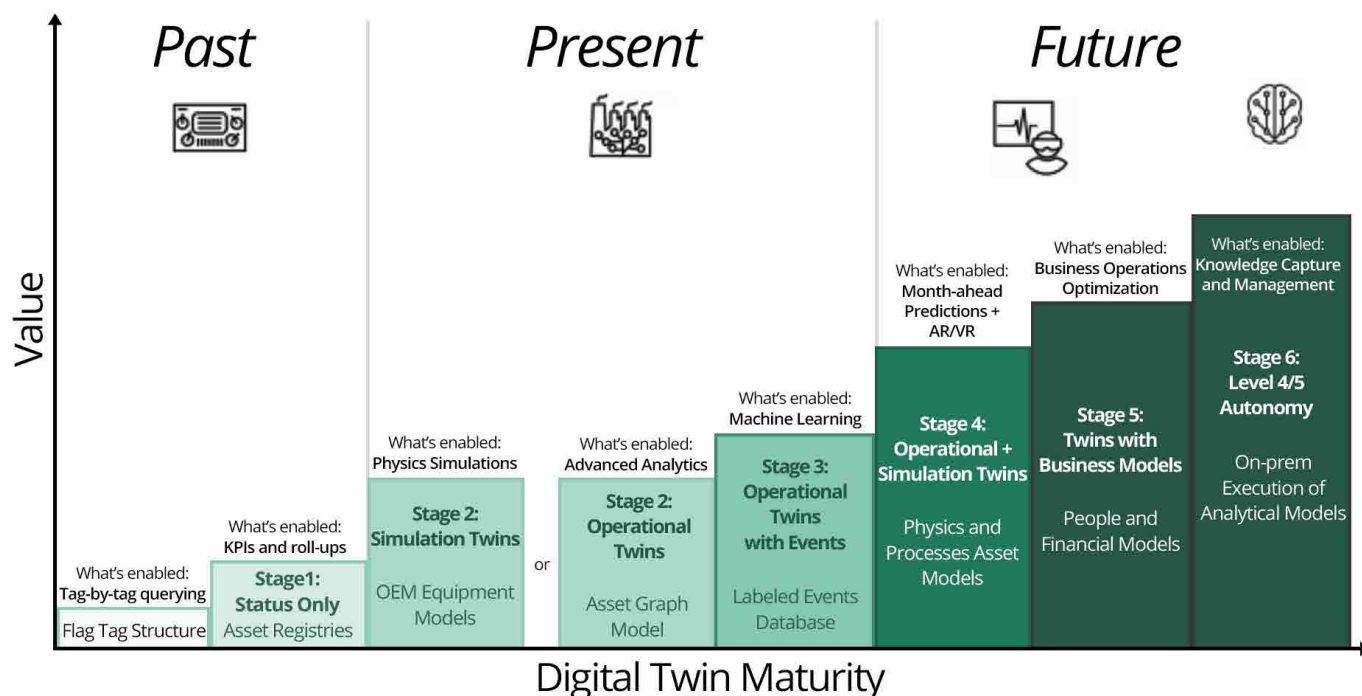
Modelowanie DT jest procesem iteracyjnym. Model powinien charakteryzować się wysoką standaryzacją, modularyzacją, lekkością i solidnością [14]. Owe wirtualne modele, aby być cyfrowymi bliźniakami i jak najlepiej odzwierciedlać obiekty rzeczywiste, muszą zależeć od danych ze świata rzeczywistego i odtwarzać,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

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

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

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

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



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

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

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

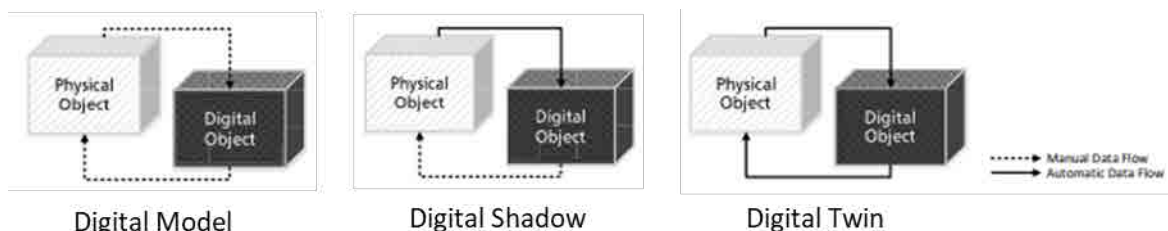
### DOJRZAŁOŚĆ DIGITAL TWIN

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

**Digital Model** – cyfrowa reprezentacja istniejącego lub planowanego obiektu fizycznego, która nie wykorzystuje żadnej formy automatycznej wymiany danych między obiektem fizycznym a obiektem cyfrowym.

**Digital Shadow** – istnieje zautomatyzowany jednokierunkowy przepływ danych między stanem istniejącego obiektu fizycznego a obiektem cyfrowym.

**Digital Twin** – dane przepływające między istniejącym obiektem fizycznym a obiektem cyfrowym są w pełni zintegrowane w obu kierunkach.



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

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

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

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

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

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

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

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

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

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

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

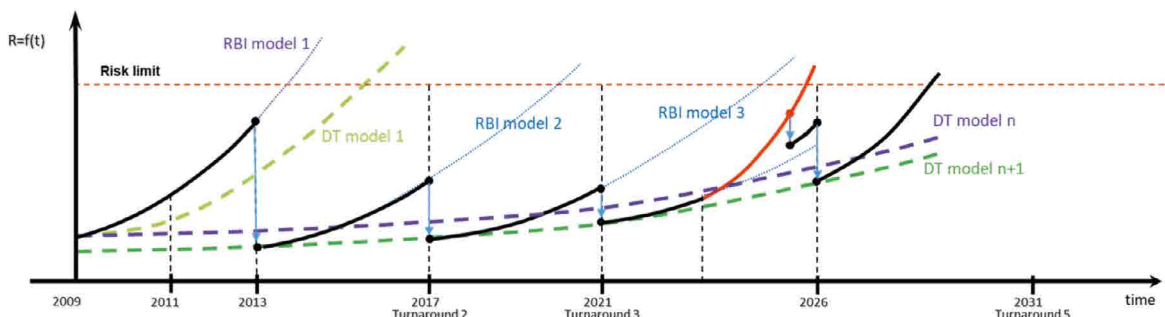
## JAKIE NADZIEJE I PERSPEKTYWY WIĄŻEMY Z TECHNOLOGIAMI PRZEMYSŁU 4.0?

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

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

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

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



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

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

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

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

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

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

## CO NOWEGO W MASZYNACH?

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

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

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

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

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

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

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

Wskazano także przepisy związane z cyberbezpieczeństwem:

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

## SZTUCZNA INTELIGENCJA W MACHINERY REGULATION ORAZ AI ACT

Pierwotnym zamiarem Komisji Europejskiej było równoczesne opublikowanie MR oraz odrębnego rozporządzenia ws. sztucznej inteligencji, czyli EU Artificial Intelligence Act (AI Act 2021/206).

AI Act określa 5 (4 + general purpose AI) kategorii aplikacji AI w zależności od ryzyka, jakie stwarzają. W zależności od rodzaju AI i stwarzanego przez nie ryzyka okresy przejściowe na zakazanie użytkowania systemów AI stwarzających nieakceptowane i wysokie ryzyko będą wynosiły od 6 do 36 miesięcy po wprowadzeniu AI ACT.

W preambule MR, w motywie 12 określono jednak, że „rozporządzenie powinno zatem obejmować ryzyko dla bezpieczeństwa wynikające z nowych technologii cyfrowych”.

W załączniku I, II i III MR dodano również ogólne odniesienia dotyczące produktów wykorzystujących uczenie maszynowe.

Przyszłe rozporządzenie dotyczące systemów sztucznej inteligencji 2021/206 i rozporządzenie w sprawie maszyn 2023/1230 mają się wzajemnie uzupełniać.

Rozporządzenie AI obejmuje przede wszystkim zagrożenia bezpieczeństwa wynikające z systemów AI, które kontrolują funkcje bezpieczeństwa maszyny. W uzupełnieniu do tego rozporządzenie maszynowe ma na celu zapewnienie integracji systemu AI z całą maszyną, tak aby nie zagrażało bezpieczeństwu maszyny jako całości.

W załączniku III MR mamy zapisy dotyczące układów sterowania – punkt 1.2, gdzie czytamy – jak poniżej.

1.2. Układy sterowania  
1.2.1. Bezpieczeństwo i niezawodność układów sterowania  
Układy sterowania muszą być zaprojektowane i wytwarzane tak, aby zapobiec powstawaniu sytuacji zagrożenia.

Układy sterowania muszą być zaprojektowane i wytwarzane tak, aby:

a) mogły wytrzymać, stosownie do okoliczności i ryzyka, przewidywane obciążenia podczas pracy oraz zamierzone i niezamierzone oddziaływanie czynników zewnętrznych, w tym racjonalnie przewidywalne próby doprowadzenia do sytuacji zagrożenia podejmowane w złym zamiarze przez strony trzecie;

d) wartości graniczne dla funkcji bezpieczeństwa stanowiły część oceny ryzyka przeprowadzanej przez producenta, bez możliwości zmian ustawień lub zasad generowanych przez maszynę lub produkt powiązany lub przez operatorów, w tym w fazie uczenia się maszyny lub produktu powiązanego, jeżeli takie zmiany mogą prowadzić do powstania sytuacji zagrożenia;

f) rejestrowanie danych wygenerowanych w związku z ingerencją oraz danych dotyczących wersji oprogramowania realizującego funkcję bezpieczeństwa zainstalowanego po wprowadzeniu maszyny lub produktu powiązanego do obrotu lub oddaniu ich do użytku było możliwe przez okres pięciu lat od daty instalacji, wyłącznie w celu wykazania zgodności maszyny lub produktu powiązanego z niniejszym załącznikiem na uzasadniony wniosek właściwego organu krajowego.

Układy sterowania maszyn lub produktów powiązanych o całkowicie lub częściowo samozmieniającym się zachowaniu lub samozmieniającej się logice układów, przeznaczonych do działania na różnych poziomach autonomii, należy projektować i wytwarzać tak, aby:

**a) nie mogły powodować wykonywania przez maszynę lub produkt powiązany działań wykraczających poza określone zadanie i przestrzeń ruchu;**

**b) możliwa była rejestracja danych dotyczących procesu podejmowania decyzji** przez systemy bezpieczeństwa oparte na wykorzystaniu oprogramowania zawierające elementy związane z bezpieczeństwem realizujące funkcje bezpieczeństwa zawierającą elementy bezpieczeństwa, po wprowadzeniu maszyny lub produktu powiązanego do obrotu lub oddaniu jej do użytku, a dane te były zachowywane przez okres roku od zgromadzenia, wyłącznie w celu wykazania zgodności maszyny lub produktu powiązanego z niniejszym załącznikiem na uzasadniony wniosek właściwego organu krajowego;

**c) w każdej chwili możliwe było skorygowanie** maszyny lub produktu powiązanego w celu utrzymania ich inherentnego bezpieczeństwa.

**Należy zwrócić szczególną uwagę na następujące kwestie:**

a) maszyna lub produkt powiązany nie mogą uruchomić się nieoczekiwanie;

b) parametry maszyny lub produktu powiązanego nie mogą zmieniać się w sposób niekontrolowany, jeżeli taka zmiana mogłaby prowadzić do sytuacji niebezpiecznych;

**c) należy zapobiec zmianom ustawień lub zasad generowanych przez maszynę lub produkt powiązany lub przez operatorów, w tym podczas fazy uczenia się maszyny lub produktu powiązanego, jeżeli tego rodzaju zmiany mogłyby prowadzić do sytuacji niebezpiecznych;**

d) po wydaniu sygnału do zatrzymania maszyna lub produkt powiązany nie może się nie zatrzymać;

e) żadna ruchoma część maszyny lub produktu powiązanego lub element zamocowany w maszynie lub produkcie powiązanym nie mogą odpaść lub zostać wyrzucone;

f) nie powinny występować przeszkody w automatycznym lub ręcznym zatrzymywaniu jakichkolwiek części ruchomych;

g) urządzenia ochronne muszą pozostawać w pełni skuteczne lub wygenerować sygnał zatrzymania;

**h) części układu sterowania związane z bezpieczeństwem muszą działać w spójny sposób w całym zespole maszyny lub produktów powiązanych, lub maszyny nieukończonych, lub ich kombinacji.**

W przypadku sterowania bezprzewodowego awaria łączności lub połączenia albo błędne połączenie nie mogą powodować sytuacji niebezpiecznej.

Jak wynika z powyższego, obecne w MR zapisy dotyczące wymagań dla maszyn używających uczenia maszynowego są dosyć ogólne (jak zresztą w poprzednich edycjach MD lub w innych dyrektywach w zakresie innych wymagań). Wymagania opierają się przede wszystkim na ocenie ryzyka przeprowadzonej przez producenta lub integratora zespołu maszyn w zakresie stosowanej aplikacji AI.

Natomiast zwraca się uwagę na ograniczenie zmian wprowadzonych w trakcie „uczenia maszynowego” do pewnych ram/faz, które nie powinny być przekraczane. To znaczy, że dajemy aplikacji AI pewną autonomię, ale ograniczamy czas i zakres uczenia maszynowego oraz funkcję, **w której jest używana.**

Doświadczenie pokazuje (jak z poprzednią dyrektywą MD), że do czasu publikacji przewodnika do MR trudno jest jednoznacznie określić zasadnicze wymagania zawarte w Załączniku III.

Zdaniem autorów rozwiązania AI, ponieważ mogą (*by design*/przez konstrukcję) wygenerować także nieoczekiwane i nieprzewidywalne rozwiązania oraz zachowania, powinny być objęte ramami audytowalnych, niezależnych algorytmów lub niezależnych zabezpieczeń, np. zrealizowanych w innych technologiach, tj. elektrycznej, elektronicznej lub programowalnej elektronicznej, lecz jednoznacznej w działaniu.

Przepisy dotyczące oceny zgodności oprogramowania przez stronę trzecią, zapewniającego funkcje bezpieczeństwa określone w niniejszym rozporządzeniu, powinny mieć zastosowanie wyłącznie do systemów o całkowicie lub częściowo samozmieniającym się zachowaniu, wykorzystujących podejścia oparte na uczeniu maszynowym zapewniające funkcje bezpieczeństwa. Przepisy te nie powinny mieć natomiast zastosowania do oprogramowania niezdolnego do uczenia się lub rozwoju i zaprogramowanego wyłącznie do wykonywania niektórych zautomatyzowanych funkcji maszyn lub produktów powiązanych.

Mimo tego należy pamiętać o roli jednostek notyfikowanych wymaganej w niektórych innych dyrektywach – więcej informacji na ten temat znajdują Państwo na stronach UDT.

## PODSUMOWANIE

Nowe technologie niosą ogromne szanse na przyspieszenie rozwoju, optymalizację pracy, a może nawet „odciążenie” człowieka od pracy, jak słyszymy w mediach.

Tymczasem skupmy się na wykorzystaniu ich zalet i zadbajmy o bezpieczeństwo oraz przewidywalność nowych technologii.

**Amerykański pisarz – mistrz gatunku fantastyki naukowej i profesor biochemii Isaac Asimov w roku 1942 stworzył trzy prawa robotów i przedstawił je w opowiadaniu *Zabawa w berka* (ang. *Ru-naround*). Celem tych praw było uregulowanie kwestii stosunków pomiędzy przyszłymi myślącymi maszynami a ludźmi [11].**

Przedstawiły się one następująco [11]:

1. Robot nie może zranić człowieka ani przez zaniechanie działania dopuścić do jego nieszczęścia.
2. Robot musi być posłuszny człowiekowi, chyba że stoi to w sprzeczności z Pierwszym Prawem.
3. Robot musi dbać o siebie, o ile tylko nie stoi to w sprzeczności z Pierwszym lub Drugim Prawem.

**Następnie w opowiadaniu *Roboty i Imperium* (*Robots and Empire*) Asimov dodał prawo zerowe, które stało się nadrzędne wobec trzech pozostałych [11]:**

0. Robot nie może skrzywdzić ludzkości lub poprzez zaniechanie działania doprowadzić do uszczerbku dla ludzkości.

Niezależnie od tego, jak dzisiejszy świat podejdzie do tych reguł – można się zgodzić, że zawierają one logikę, która w jakiejś formie powinna być inherentnie wbudowana w urządzenia techniczne, a także w każdej chwili możliwa do weryfikacji przez człowieka.

**Sztuczna inteligencja nauczona tych zasad może w pewnym momencie zacząć je kontestować i zadawać** sobie pytanie „**Czy nie będę jednak skuteczniejsza w realizacji postawionych celów bez którejs z zasad?**”, „**Dlaczego mam przestrzegać zasad?**”.

„Biologiczna” inteligencja szybko nauczyła się „obchodzić” zabezpieczenia, tworząc bypassy, wstawiając „zworki” czy wprowadzając zmiany wyłączające funkcje bezpieczeństwa lub osłabiające ich działanie. Jako inspektorzy spotykamy się czasem z takimi naruszeniami przepisów. Wykrywanie tego rodzaju naruszeń jest możliwe, gdy rozwiązanie jest audytowalne, np. gdy jest to rozwiązanie sprzętowe lub algorytm w znanym nam języku programowania.

**Paragraf 14 rozporządzenia [15] dotyczącego eksploatacji urządzeń ciśnieniowych mówi:**

**„§ 14. 1. Eksploatację urządzeń ciśnieniowych prowadzi się zgodnie z ich przeznaczeniem, zasadami określonymi w rozporządzeniu oraz instrukcją eksploatacji, stosując odpowiednie środki bezpieczeństwa.**

**2. Urządzenia ciśnieniowe mogą być eksploatowane tylko wtedy, gdy ich stan techniczny nie budzi zastrzeżeń, osprzęt zabezpieczający, osprzęt ciśnieniowy i automatyka zabezpieczająca są sprawne oraz nie zostały wyłączone z działania”.**

Na podstawie ww. zapisów wykrycie w czasie inspekcji niezgodnych z dokumentacją zworek lub bypassów stanowi podstawę do wydania decyzji wstrzymującej eksploatację urządzenia i nakazującej wyłączenie urządzenia z eksploatacji.

**System sztucznej inteligencji (system AI)** oznacza oprogramowanie opracowane przy użyciu co najmniej jednej spośród technik i podejść określonych w załączniku I do rozporządzenia [15], które może – dla danego zestawu celów określonych przez człowieka – generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję.

AI to często architektura „procesora” – swego rodzaju mózgu czy jednostki centralnej. Bardziej można by ją wtedy nazwać technologią niż algorytmem. Ponadto nie musi być zlokalizowana fizycznie w urządzeniu. Odwołując się do przykładu z klasycznej science-fiction Ridleya Scotta pt. *Łowca androidów*, można założyć, że inspekcja urządzenia wyposażonego w AI będzie wymagała kwalifikacji psychologa, analityka i zapewne kilku innych.

**Postulujemy twarde, mierzalne, audytowalne ramy dla działania systemów o samozmieniającym się zachowaniu przy zachowaniu wszelkich korzyści płynących z nowoczesnych technologii. Jeśli twarde ograniczenie „stawałoby na drodze” innowacyjnego rozwiązania, to takie rozwiązanie powinno być zarejestrowane, a ograniczenie mogłoby podlegać walidacji w przemyśle, ewolucyjny sposób.**

Systemy o samozmieniającym się oprogramowaniu powinny podlegać wymogom dotyczącym jakości wykorzystywanych zbiorów danych, dokumentacji technicznej i rejestrowania zdarzeń, przejrzystości i przekazywania informacji użytkownikom, nadzoru ze strony człowieka oraz wiarygodności, dokładności i cyberbezpieczeństwa. Systemy te należy projektować i opracowywać w taki sposób, aby osoby fizyczne mogły nadzorować ich funkcjonowanie. W tym celu należy określić odpowiednie środki związane z nadzorem ze strony człowieka. Takie środki powinny gwarantować, że system podlega wbudowanym ograniczeniom operacyjnym, których sam nie jest w stanie obejść, i reaguje na działania człowieka, oraz że osoby fizyczne, którym powierzono sprawowanie nadzoru, posiadają niezbędne kompetencje, przeszkolenie i uprawnienia do pełnienia tej funkcji.

Innowacyjne podejście do bezpieczeństwa urządzeń technicznych od zawsze było wbudowane w DNA Urzędu Dozoru Technicznego. Odkąd powstał, poszukujemy coraz skuteczniejszych metod zapewnienia bezpieczeństwa eksploatacji urządzeń. Od wielu lat wdrażamy i promujemy nowe technologie, w inspekcji oceniając przy tym ich wpływ na bezpieczeństwo.

Technologie przemysłu 4.0 są coraz bardziej dostępne i z uwzględnieniem ewolucyjnych zmian systemów zarządzania produkcją oraz z konieczności zapewnienia bezpieczeństwa teleinformatycznego są implementowane w wielu gałęziach przemysłu. Stwarza to wiele możliwości, które UDT dostrzega i spieszy wykorzystać w praktyce inspekcyjnej.

**Wspieramy rozwój, dbamy o bezpieczeństwo.**



Literatura:

1. ISO/IEC STRATEGIC BUSINESS PLAN, NOVEMBER 2020; dostęp 25.05.2021
2. Ustawa z dnia 21 grudnia 2000 r. o dozorcze technicznym (Dz.U. 2000 nr 122 poz. 1321 z późn. zm.)
3. Klinkosz T., Dynamiczne zarządzanie ryzykiem instalacji przemysłowych; biuletyn INSPEKTOR 4/2022
4. Klinkosz T., Predykcja zużycia urządzeń ciśnieniowych i planowanie inspekcji z wykorzystaniem metodologii RBI (Risk Based Inspection); biuletyn INSPEKTOR 1/2021
5. ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2023/1230 z dnia 14 czerwca 2023 r. w sprawie maszyn oraz w sprawie uchylecia dyrektywy 2006/42/WE Parlamentu Europejskiego i Rady i dyrektywy Rady 73/361/EWG <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32023R1230>
6. Schleich B. et al., Shaping the Digital Twin for design and production engineering. CIRP Annals – Manufacturing Technology, Elsevier, 2017, 66 (1), ff10.1016/j.cirp.2017.04.040ff. fhal-01513846. [on-line] <https://hal.archives-ouvertes.fr/hal-01513846/document>; dostęp: 14.02.2021
7. Bane A., Kalwani S., McCormick S., Digital Twins for the asset operator, Element Analytics, Smart Industry; Oct 12, 2017
8. API RP 581 Risk-Based Inspection Methodology, 2008 11 2016.
9. Negri E., Fumagalli L., Macchi M., A Review of the Roles of Digital Twin in CPS-based Production Systems, Procedia Manufacturing, Volume 11, 2017, s. 939-948, ISSN 2351-9789, <https://doi.org/10.1016/j.promfg.2017.07.198>. [on-line] <https://www.sciencedirect.com/science/article/pii/S2351978917304067>; dostęp: 20.02.2021
10. Grieves M., Vickers J., Digital Twin: mitigating unpredictable, undesirable emergent behavior in complex systems, Kahlen FJ, Flumerfelt S., Alves A., editors. Transdisciplinary perspectives on complex systems. Springer, 2017. s. 85–113
11. Etyka robotów – Wikipedia, wolna encyklopedia
12. Kritzinger W., Karner M., Traar G., Henjes J., Sihl W., Digital Twin in manufacturing: a categorical literature review and classification, Science Direct, IFAC PapersOnLine 51–11 (2018) 1016–1022; dostęp 25.05.2021
13. <https://przemysl-40.pl/index.php/2017/03/22/czym-jest-przemysl-4-0/>
14. Qinglin Qi et al., Enabling technologies and tools for Digital Twin, Journal of Manufacturing Systems, <https://doi.org/10.1016/j.jmsy.2019.10.001>; dostęp: 29.10.2020
15. Rozporządzenie Ministra Rozwoju i Technologii z dnia 17 grudnia 2021 roku w sprawie warunków technicznych dozoru technicznego dla niektórych urządzeń ciśnieniowych podlegających dozorowi technicznemu (Dz.U. 2022 poz.68)
16. EUROPEAN COMMISSION Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, Brussels, 21.4.2021