Jan Maciej Kościelny
Politechnika Warszawska
Wydział Mechatroniki
Instytut Automatyki i Robotyki
jan.koscielny@pw.edu.pl

Automatyczna detekcja i diagnostyka zagrożeń – nowoczesna metoda podwyższania bezpieczeństwa procesów przemysłowych

1. Przyczyny stanów awaryjnych

Wiele instalacji technologicznych stwarza ryzyko wystąpienia poważnej awarii przemysłowej. Instalacje takie określane są jako krytyczne lub wysokiego ryzyka. W przypadku takich systemów bezpieczeństwo jest podstawowym wymogiem stawianym w okresie czwartej transformacji przemysłowej, określanej jako Przemysł 4.0.

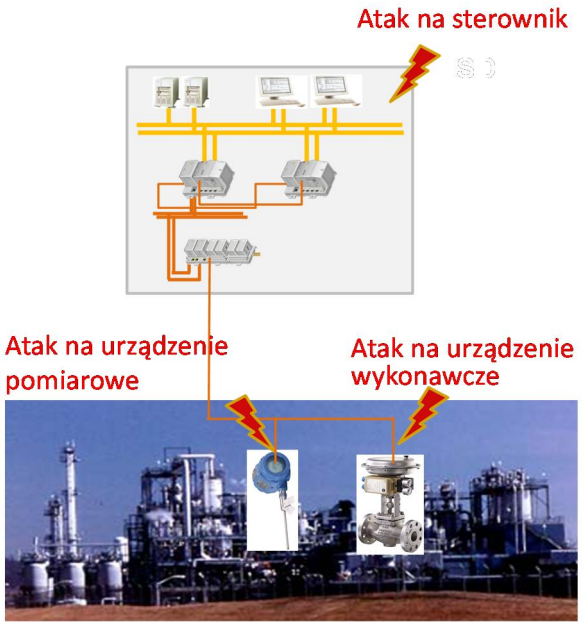
Prawidłowe funkcjonowanie przemysłowych systemów sterowania (ICS – Industrial Control Systems) narażone jest na dwa rodzaje zagrożeń:

- zagrożenia typu hazards związane z uszkodzeniami urządzeń i błędami ludzkimi, które wchodzą w obszar bezpieczeństwa określanego jako safety,
- zagrożenia typu threats, dotyczące celowych destrukcyjnych działań jakimi są cyberataki, znajdujące się w obszarze bezpieczeństwa określanego jako security (rys.1).

Powyższe zagrożenia były przyczyną wielu poważnych awarii przemysłowych. Przykładowo:

- Pęknięcie rurociągu spowodowało 1 czerwca 1974 r. awarię w Flixborough w Wielkiej Brytanii, w instalacji produkującej kaprolaktam. Zginęło 28 pracowników zakładu, poważne obrażenia poniosło 89 osób.
- Pęknięcie nadziemnego gazociągu zasilającego odbiorców w propan-butan było prawdopodobnie przyczyną katastrofy w San Juanico – Ixhuatepec na przedmieściach Meksyku 19 listopada 1984 r. Śmierć poniosło około 550 osób, ciężkie poparzenia i inne urazy odniosło ponad 2000 osób, ewakuowanych zostało 60 000 mieszkańców.
- Uszkodzenie zaworu spowodowało awarię w cukrowni Głogów, Polska, 1 listopada 1992 r. W wyniku eksplozji śmierć poniosło siedmiu pracowników zakładu, dziesięciu zostało okaleczonych.
- Uszkodzenie czujnika poziomu doprowadziło do przepełnienia zbiornika z paliwem, a następnie zapłon w bazie paliw Buncefield, Anglia, 11 grudnia 2005 r. Nnastąpiła seria wybuchów i pożar paliwa lotniczego. Był to największy pożar w Europie. Skutki: 43 osoby ranne i poważne straty materialne (1 mld £).
- Uszkodzenie przetwornika pomiarowego poziomu i błędy operatorów były przyczyną katastrofy w rafinerii Statoil w Texas City w Stanach Zjednoczonych w dniu 23 marca 2005 roku. Wypadek spowodował 15 ofiar śmiertelnych, 180 rannych oraz około 3 miliardy dolarów odszkodowań.

- Błędy popełnione przez operatorów elektrowni oraz przestarzała konstrukcja reaktora RBMK była przyczyną awarii w Czarnobylu, ZSRR (obecnie Ukraina), 26 kwietnia 1986 r. Zginęło 38 osób, dziesiątki tysięcy zostały napromieniowane, ewakuowano i przesiedlono ponad 350 000 osób. Nastąpiło skażenie gleby i wód. Elektrownia została zniszczona.
- Naruszenie przez operatora procedur operacyjnych było przyczyną incydentu (eksplozji) w wieży destylacyjnej nitrobenzenu Jilin Petrochemical w Chinach 13 listopada 2005 r. Zginęło 8 osób, 60 zostało rannych.
- Możliwą przyczyną katastrofy w Bhopalu, Indie, 3 grudnia 1984 r. mogło być doprowadzenie wody do zbiornika produktu, w wyniku sabotażu lub nieszczelności zaworu. Była to największa katastrofa na świecie pod względem liczby ofiar, której dokładnie nie ustalono. Zginęło około 15-20 tys. ludzi, a 560 tys. zostało poszkodowanych, w tym 120 tys. ciężko.
- Cyberataki spowodowały m.in: wybuch ropociągu Baku – Tbilisi – Ceyhan w dniu 6 sierpnia 2008 r. we Wschodniej Turcji, zniszczenie wirówek do wzbogacania uranu w irańskich instalacjach nuklearnych w Natanz w 2010 r., ogromne zniszczenia w infrastrukturze huty w Niemczech w 2014 r., wyłączenia zasilania dla 225 000 klientów w Ukrainie w 2015 r. i 2016 r.



Rys.1. Ataki cybernetyczne na ICS.

Mimo różnych przyczyn skutki groźnych uszkodzeń, błędów operatorów i cyber-ataków mogą być takie same: np. pożar, eksplozja, skażenie środowiska, zniszczenie instalacji, zatrzymanie procesu.

Aby można było skutecznie przeciwdziałać skutkom uszkodzeń konieczna jest wiedza o ich wystąpieniu. Im ta wiedza jest szybciej pozyskana i bardziej precyzyjna, tym skuteczniejsze mogą być działania zabezpieczające [1,2,3]. Wynika stąd wysoka ranga automatycznej detekcji i diagnostyki uszkodzeń oraz cyberataków [4,5,6,7], a także stałego nadzoru diagnostycznego nad działaniami operatorów procesów przemysłowych. W pracy [8]

podkreślono, że zapobieganie wypadkom jest jedną z dziesięciu zasad bezpieczeństwa, a zasada ta jest osiągana poprzez wczesne wykrywanie i dokładną diagnozę uszkodzeń.

O ile diagnostyka uszkodzeń i cyberataków jest tematem badań od wielu lat, to automatyczna detekcja i diagnostyka błędów ludzkich była dotychczas tematem zaledwie kilku publikacji. Jest to pewien paradoks, ponieważ błędy ludzkie są najczęstszymi przyczynami awarii.

Zakres detekcji i izolacji anomalii powinien obejmować wszystkie zdarzenia zagrażające, a więc uszkodzenia aparatury technologicznej oraz urządzeń automatyki i pomiarów, cyberataki a także błędy operatorów i akcje sabotażowe. Powyższe anomalie wpływają destrukcyjnie na działanie układów sterowania i przebieg procesu. W związku z tym powstają rozbieżności między normalną pracą systemów sterowania związaną z prawidłowym przebiegiem kontrolowanego procesu a przebiegiem zaburzonym. Te rozbieżności, stanowiące symptomy anomalii, mogą być wykrywane w sposób automatyczny, na podstawie rejestracji i analizy mierzonych zmiennych procesowych i sygnałów sterujących z wykorzystaniem modeli reprezentujących stan normalny diagnozowanego obiektu.

2. Systemy alarmowe versus systemy automatycznej detekcji i diagnostyki zagrożeń.

W systemach automatyki procesów przemysłowych (SCADA, DCS) do rozpoznawania stanów nienormalnych i awaryjnych służy system alarmowy (SA). Stanowi on najprostsze i bardzo niedoskonałe rozwiązanie systemu diagnostycznego Metodą detekcji stosowaną w SA jest kontrola ograniczeń. Uszkodzenia i ataki powodują zmiany w funkcjonowaniu systemu sterowania i procesu odbiegające od jego normalnego stanu. Wynikowe zmiany są obserwowane przez operatora jako sekwencja alarmów informujących o przekroczeniu limitów alarmowych przez poszczególne zmienne procesowe.

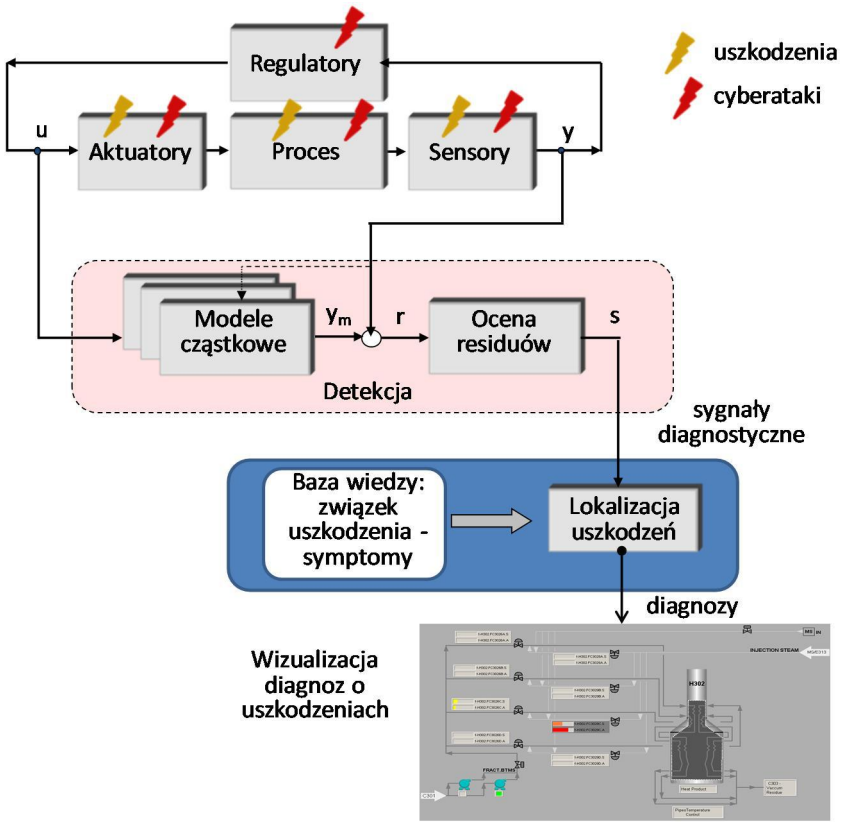
Wnioskowanie o przyczynach alarmów w SA nie jest prowadzone. To trudne zadanie spoczywa na operatorach procesu, którzy mają do dyspozycji chronologiczny wykaz alarmów i inne narzędzia udostępniane w systemach zarządzania alarmami. Podstawową wadą tego rozwiązania jest występowanie w krótkim czasie bardzo dużej liczby alarmów (flood alarms) w stanach z groźnymi uszkodzeniami lub atakami. W okresie kilku minut wystąpić może kilkaset alarmów. Nadmiar sygnalizowanych alarmów jest wadą współczesnych systemów sterowania procesami. Z danych EEMUA (The Engineering Equipment and Materials Users' Association) wynika, że średnia dobowa liczba alarmów w przemyśle petrochemicznym wynosi ok. 1500, w energetycznym 2000, natomiast według zaleceń nie powinna przekraczać 144.

Interpretacja dużej liczby alarmów powstających w krótkim okresie stanowi dla operatorów poważny problem. Występuje tutaj zjawisko przeciążenia informacyjnego, a w jego następstwie stres. W tych warunkach operatorzy nie są w stanie sformułować prawidłowej diagnozy, tj. rozpoznać zaistniałych zagrożeń. Zwiększa to prawdopodobieństwo niewłaściwych reakcji zabezpieczających, których skutki kumulując się z wcześniej zaistniałymi uszkodzeniami powodują poważne awarie. Mechanizm takiego niekorzystnego (dodatniego) sprzężenia zwrotnego był przyczyną wielu groźnych awarii w elektrowniach jądrowych i konwencjonalnych oraz zakładach chemicznych (m.in. eksplozji w rafinerii

Texaco's Milford Haven w 1994r). Ponadto ingerencja cyberataku w system sterowania może polegać na modyfikacji działania systemu alarmowego, w taki sposób, aby ukryć przed operatorem objawy ataku.

Efektywne rozpoznawanie anomalii (uszkodzeń, ataków, błędów operatorow) w systemach sterowania wymaga zastosowania metod automatycznej diagnostyki procesów przemysłowych obejmującej dwa podstawowe zadania: detekcję i lokalizację (izolację) zagrożęń (rys.2). Uszkodzenia jak też cyberataki (o ile przedostaną się przez informatyczne warstwy zabezpieczeń) powodują zakłócenia funkcjonowania systemu sterowania i przebiegu procesu [9]. Detekcja uszkodzeń/ataków polega w tym przypadku na wczesnym wykrywaniu rozbieżności między funkcjonowaniem bieżącym a referencyjnym, reprezentowanym przez modele ilościowe lub jakościowe charakteryzujące stan normalny obiektu.

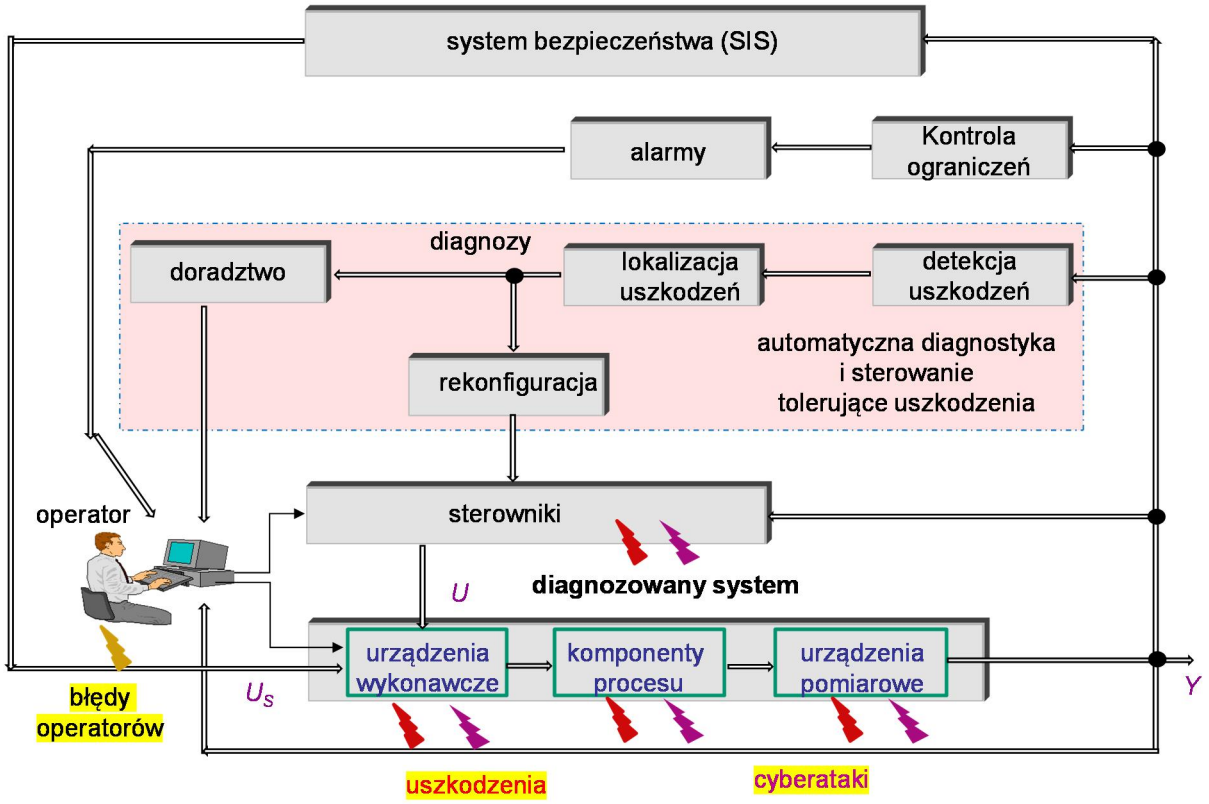
Do detekcji stosowane są zarówno modele analityczne, określone na podstawie równań fizycznych opisujących obiekt z parametrami zidentyfikowanymi eksperymentalnie, a także modele budowane na podstawie danych pomiarowych dla stanu normalnego obiektu (data driven), w tym modele neuronowe, rozmyte, kombinacje tych dwóch podejść oraz modele statystyczne. Sygnały mierzone porównywane są z sygnałami wyliczanymi na podstawie modeli (rys.2). Różnica między nimi nazywana residuum podlega ocenie (ostrej lub rozmytej) w celu wygenerowania sygnału diagnostycznego. W przypadku braku anomalii wartość residuum jest bliska zera i sygnał diagnostyczny ma wartość zero. Uszkodzenia lub ataki objawiają się jako odbiegające od zera wartości residuów i inne niż zero wartości sygnałów diagnostycznych.



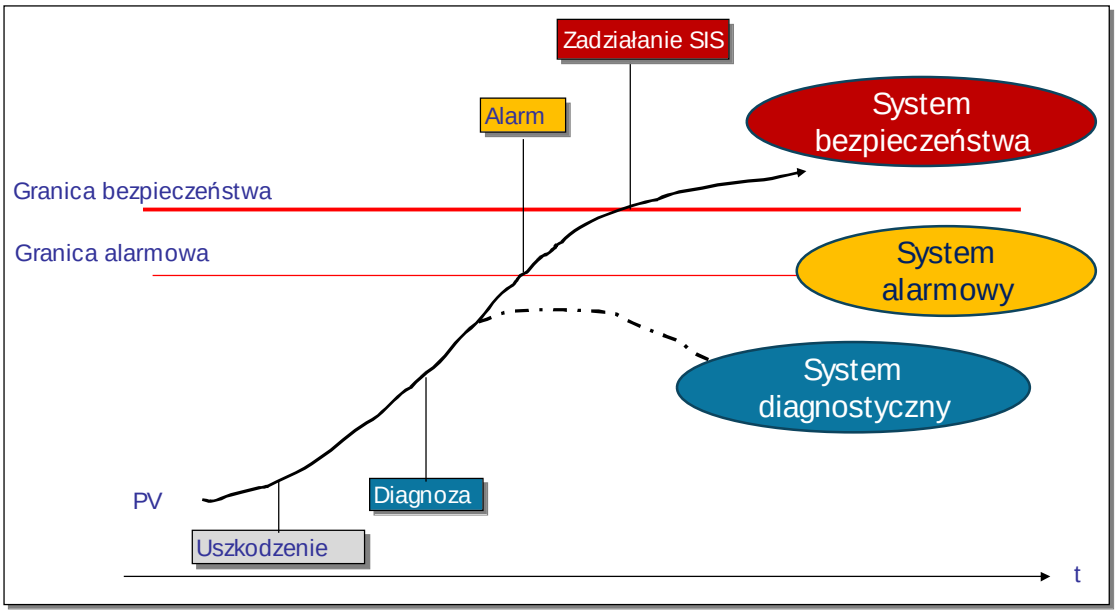
Rys.2. Schemat automatycznej detekcji i lokalizacji uszkodzeń/ataków.

Wśród metod lokalizacji uszkodzeń wyróżnić można metody klasyfikacji i metody wnioskowania automatycznego. W procesach przemysłowych praktycznie brak jest danych pomiarowych dla stanów z uszkodzeniami/atakami. To ogranicza możliwość zastosowania metod klasyfikacji, wymagających danych uczących dla poszczególnych stanów procesu. Lokalizacja uszkodzeń jest prowadzona zwykle na podstawie wnioskowania automatycznego, do czego niezbędna jest wiedza ekspercka o związku uszkodzenia – symptomy.

Wynikiem automatycznego wnioskowania jest diagnoza. Wskazuje ona uszkodzenia lub ataki możliwe przy zaobserwowanych symptomach. Diagnoza przekazywana jest operatorom w postaci tekstowej lub graficznej (rys.2). Na podstawie diagnoz system diagnostyczny może dodatkowo doradzać obsłudze, przekazując instrukcje postępowania w stanach awaryjnych. Dzięki temu mogą oni podejmować szybkie i skuteczne działania zabezpieczające. Powinny one sprowadzać proces do stanu normalnego. W rezultacie nie dochodzi do zadziałania systemu bezpieczeństwa SIS (rys.3), a tym samym do zatrzymania przebiegu części lub całości procesu technologicznego. Unika się w ten sposób znacznych strat ekonomicznych.



Rys.3. System automatycznej detekcji i diagnostyki uszkodzeń w strukturze starowania i zabezpieczenia procesu

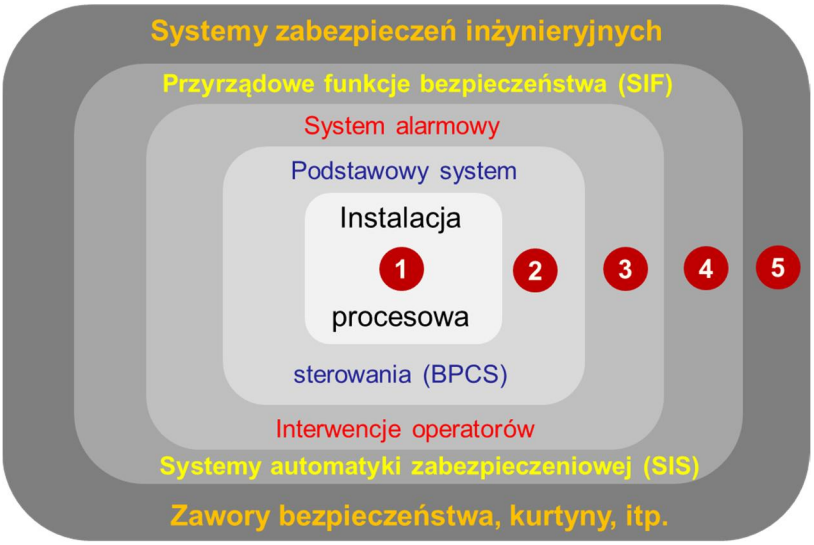


Rys.4. Porównanie reakcji systemu diagnostycznego, alarmowego i SIS na zagrożenia.

Porównanie reakcji systemu diagnostycznego, alarmowego i SIS na zagrożenia przedstawiono na rys.4.

3. System diagnostyczny jako dodatkowa warstwa zabezpieczeniowo-ochronna

Struktura systemów zabezpieczeń zarówno dla zagrożeń typu hazards (uszkodzenia) jak też threats (ataki) jest warstwowa. W normie EN 61511 bezpieczeństwa funkcjonalnego dla przemysłu procesowego określone zostały warstwy zabezpieczeniowo-ochronne (Layer of Protection – LoP) (rys.5). W przypadku ochrony przed atakami warstwy zabezpieczeń określane są jako 'Ring of Protection - RoP.



Rys.5. Warstwy zabezpieczeń (PN-EN 61511)

Pierwszą warstwę stanowi instalacja procesowa, która powinna być odporna na zakłócenia wewnętrzne i zewnętrzne. Warstwę drugą stanowi podstawowy system automatyki procesu (BPCS - Basic Process Control System). Może nim być rozproszony system DCS (Distributed Control Systems), lub system złożony ze SCADA (Supervisory Control and Data Acquisition) i sterowników programowalnych PLC/PAC (Programmable Logic Controller / Programmable Automation Controller). Warstwa trzecia to system alarmów krytycznych i interwencje operatorów procesu. System automatyki zabezpieczeniowej SIS (Safety Instrumented Systems) stanowi warstwę czwartą. Te cztery wymienione powyżej warstwy mają na celu zapobieganie występowaniu awarii. Warstwy wyższe to systemy zabezpieczeń inżynieryjnych (zawory bezpieczeństwa, kurtyny, bariery ochronne, obudowy itp.), które mają jedynie ograniczać skutki powstałych awarii.

Powszechnie stosowane systemy bezpieczeństwa SIS realizują algorytmy blokad i zabezpieczeń automatycznych, których zadaniem jest doprowadzenie procesu do stanu bezpiecznego. Zwykle działania SIS wiążą się z zatrzymaniem całego lub części procesu, co prowadzi do strat ekonomicznych. Dlatego w warstwach niższych celowe jest stosowanie rozwiązań, które mogą zagwarantować eliminację zagrożeń we wczesnym ich stadium i tym samym nie dopuścić do zadziałania SIS i odstawienia procesu. Metodą redukcji ryzyka, która nie powoduje zatrzymania procesu jest automatyczna detekcja i diagnostyka uszkodzeń, cyberataków i błędów operatorów. W strukturze warstwowej zabezpieczeń system diagnostyczny stanowi warstwę ulokowaną pomiędzy warstwą drugą a trzecią.

W podejściu warstwowym obowiązuje zasada: im więcej warstw zabezpieczeniowych tym wyższy poziom redukcji ryzyka. Dlatego wprowadzenie warstwy automatycznej diagnostyki do struktury zabezpieczeń i ochrony redukuje ryzyko w sensie safety, a także security.

Dotychczas zagadnienia bezpieczeństwa i ochrony rozpatrywane są odrębnie. Obowiązują odrębne normy, stosowane były odrębne systemy diagnostyki uszkodzeń i detekcji intruzów IDS, a w organizacji przedsiębiorstw problemy te wchodzą w zakres kompetencji odrębnych działów. Nie jest to właściwe. Potrzebna jest całościowa strategia bezpieczeństwa. Zintegrowany system detekcji i diagnostyki uszkodzeń, cyberataków i błędów operatorów jest przyszłościowym rozwiązaniem w aspekcie redukcji ryzyka.

4. Cele i ograniczenia systemów automatycznej diagnostyki

Zastosowanie systemu automatycznej detekcji i diagnostyki prowadzi do następujących korzyści:

- redukcji ryzyka zarówno w sensie *safety* jak też *security*,
- wspomagania operatorów w sytuacjach nadmiaru alarmów,
- podwyższenia niezawodności systemu,
- redukcji strat w stanach z uszkodzeniami
- możliwości prowadzenie nowoczesnej strategii utrzymania ruchu.

Osiągnięcie powyższych korzyści związane jest ze znacznymi kosztami wdrożenia i eksploatacji systemu diagnostycznego. Wymaga on odpowiednio przeszkolonej obsługi. Każdy remont lub modyfikacja instalacji wiąże się z koniecznością ponownego strojenia modeli. Te trudności, a także brak dostatecznej liczby specjalistów są prawdopodobnie

przyczyną małego rozpowszechnienia aplikacji systemów diagnostycznych. Brak jest także komercyjnych systemów automatycznej diagnostyki. Istniejące rozwiązania są opracowaniami ośrodków naukowych, np. system DiaSter [10]. Należy jednak sądzić, że systemy realizujące funkcje automatycznej detekcji i diagnostyki zagrożeń są rozwiązaniami perspektywicznymi i po osiągnięciu wymaganej jakości funkcjonowania będą wspomagały operatorów procesów przemysłowych, a docelowo zastąpią systemy alarmowe.

5. Uwagi końcowe

a) Bezpieczeństwo systemów sterowania procesami w sensie safety i security powinno być traktowane całościowo.
b) Diagnostyka uszkodzeń, cyberataków i błędów operatorów powinna być realizowana w jednym systemie diagnostycznym. Mimo różnych przyczyn, skutki uszkodzeń i cyberataków, a także ich symptomy mogą być takie same.
c) System automatycznej diagnostyki zagrożeń w powiązaniu z interwencjami operatorów tworzy dodatkową warstwę zabezpieczeniowo-ochronną w sensie *safety*. Dodatkowo system diagnostyczny stanowi ostatnią warstwę umożliwiającą wykrycie cyberataków (a także działań sabotażowych) jeśli przedostaną się do systemu sterowania przez wszystkie inne warstwy ochrony.

Wykaz literatury

1. Kościelny J.M., Sztyber-Betley A. (2025). Definitions and comprehensive assessment of fault isolability in expert-based diagnostic systems. Mechanical Systems and Signal Processing, Volume 236, 2025, 112979, ISSN 0888-3270, https://doi.org/10.1016/j.ymssp.2025.112979
2. Kościelny J.M., Bartyś M. (2023). A New Method of Diagnostic Row Reasoning Based on Trivalent Residuals. Expert Systems with Applications, Vol. 214 (2023) 119116, ISSN: 0957-4174, doi:10.1016/j.eswa.2022.119116
3. Kościelny J.M., Bartyś M., Sztyber A. (2021). Diagnosing with a hybrid fuzzy-Bayesian inference approach. Engineering Applications of Artificial Intelligence, 104(2021)104345, pp. 1-11, Elsevier, DOI:10.1016/j.engappai.2021.104345, ISSN:0952-1976.
4. Qiusheng Song, Peng Jiang, A multi-scale convolutional neural network based fault diagnosis model for complex chemical processes, Process Safety and Environmental Protection, Volume 159, 2022, Pages 575-584, ISSN 0957-5820.
5. Xiaotian Bi, Ruoshi Qin, Deyang Wu, Shaodong Zheng, Jinsong Zhao, One step forward for smart chemical process fault detection and diagnosis, Computers & Chemical Engineering, Volume 164, 2022, 107884, ISSN 0098-1354.
6. Weijun Li, Hui Li, Sai Gu, Tao Chen, Process fault diagnosis with model- and knowledge-based approaches: Advances and opportunities, Control Engineering Practice, Volume 105, 2020, 104637, ISSN 0967-0661.
7. Yuncheng Du, Dongping Du, Fault detection and diagnosis using empirical mode decomposition based principal component analysis, Computers & Chemical Engineering, Volume 115, 2018, Pages 1-21, ISSN 0098-1354.

8. Lamiaa M. Elshenawy, Mohamed A. Halawa, Tarek A. Mahmoud, Hamdi. A. Awad, Mohamed I. Abdo, Unsupervised machine learning techniques for fault detection and diagnosis in nuclear power plants, Progress in Nuclear Energy, Volume 142, 2021, 103990, ISSN 0149-1970.
9. Syfert M., Ordys A., Kościelny J.M., Wnuk P., Możaryn J., Kukiełka K. (2022). Integrated Approach to Diagnostics of Failures and Cyber-Attacks in Industrial Control Systems. Energies 2022, 15, 6212. https://doi.org/10.3390/en15176212
10. Korbicz J., Kościelny J.M. (red). Modelowanie, diagnostyka i sterowanie nadrzędne procesami. Implementacja w systemie DiaSter. WNT, Warszawa, 2009.