

Wpłynęło dnia 25. 02. 2025

Zarejestrowano pod nr 310-16-5/k Rzeszów, 20.02.2025 r.

Podpis 

Prof. Leszek Trybus
Katedra Informatyki i Automatyki
Politechnika Rzeszowska

Recenzja
rozprawy doktorskiej mgr. inż. Pawła Łydka
pt. *System wspomagania decyzji w projektowaniu i wdrażaniu*
przemysłowych systemów bezpieczeństwa wykorzystujących
techniki sztucznej inteligencji

Niniejsza recenzja została sporządzona na prośbę Pana dr. hab. inż. Ryszarda Sroki, prof. AGH, Przewodniczącego Rady Dyscypliny Automatyka, Elektronika, Elektrotechnika i Technologie Kosmiczne AGH w Krakowie.

1. Zakres, cel i tezy

Świadomość potrzeby korzystania z wieloaspektowych systemów zarządzania ryzykiem i bezpieczeństwem przemysłowym stopniowo się upowszechnia, nie tylko dzięki regulacjom prawnym (PN-ISO/IEC) i wewnętrznym przepisom przedsiębiorstw (np. Tauron). Tymczasem istniejące obecnie rozwiązania zorientowane są na wycinkowe aspekty ryzyka rzadko osadzając je w szerszym kontekście. Natomiast faktyczne zapotrzebowanie przemysłu wymaga znacznie szerszego podejścia biorącego pod uwagę wszystkie aspekty istotne dla danego przedsiębiorstwa. Dlatego cel badawczy rozprawy doktorskiej mgr. inż. Pawła Łydka jakim jest opracowanie metod wspomagania decyzji w systemach zarządzania bezpieczeństwem przemysłowym uważam za jak najbardziej właściwy.

Kierunek tych badań jest nakreślony w tezie rozprawy, która (nieco skrócona) stwierdza, że budowa odporności oraz skuteczne reagowanie na występujące zagrożenia mogą być osiągnięte za pomocą systemu wspomagania decyzji opartego na narzędziach informatycznych wykorzystujących metody sztucznej inteligencji do modelowania ryzyk przemysłowych oraz analizę wielokryterialną do generowania rekomendacji decyzyjnych. W tej sytuacji celem aplikacyjnym staje się opracowanie architektury specjalistycznego systemu informatycznego oznaczonego jako IRM DSS (*Industrial Risk Management Decision Support System*), którego działanie opiera się na metodach wymienionych w tezie.

Prawidłowość zaproponowanych rozwiązań mgr P. Łydek zweryfikował na przykładzie swego macierzystego zakładu, tzn. odkrywkowej kilkupoziomowej Kopalni Wapienia Czatkowice (KWC) koło Krzeszowic. Zagrożeniami, które tam występują są pęknięcia krawędzi ścian, osuwiska, prace na kilku poziomach, zalania, mgła. Do ich rozpoznania służy monitoring wizyjny, czujniki w działach przeróbczych oraz informacje pracowników. W razie wystąpienia konkretnego zagrożenia podstawowe decyzje dotyczą tras ewakuacji sprzętu (koparki, wozidła). Zapleczem informatycznym w KWC są systemy ERP, SCADA i AWIA. Działania w zakresie bezpieczeństwa koordynowane są z Tauronem.

2. Przegląd treści

Rozprawa doktorska składa się z 14. rozdziałów, przy czym we Wprowadzeniu (r. 1) podano schemat ich zależności wraz z podstawowymi osiągnięciami. Dwa następne rozdziały (2, 3) dotyczą zakładu KWC z charakterystyką zagrożeń procesów technologicznych oraz metod oceny ryzyka ich wystąpienia. Na podstawie prawdopodobieństwa materializacji ryzyk (20 do 80%) wskazano na potrzeby KWC w zakresie zapewnienia bezpieczeństwa. Ze

względu na rozległość obszaru górniczego perspektywicznym rozwiązaniem dla identyfikacji istotnych ryzyk byłyby drony i roboty inspekcyjne.

Przegląd literatury w rozdz. 4 dotyczy: 1) fuzji danych w sytuacji wystąpienia zagrożeń naturalnych (osuwiska, podtopienia), 2) algorytmów ewakuacji ludzi i sprzętu, 3) informatycznych systemów bezpieczeństwa. Przegląd prowadzono systematyczną metodą PRISM korzystając z baz SCOPUS i IEEE Xplore. Zapytania do baz zawierały słowa kluczowe przedzielone koniunkcją AND. Dzięki filtrom zawężającym udało się ograniczyć liczbę cytowań w rozprawie do 214. Uzyskane wyniki pozwoliły dostrzec kształtujące się trendy, w tym:

- wieloaspektowe podejście uwzględniające oprócz samych zagrożeń również inne aspekty funkcjonowania przedsiębiorstwa,
- połączenie analizy jakościowej problemów decyzyjnych z wiedzą ekspercką,
- agregacja danych z uwzględnieniem wartości historycznych.

Spośród algorytmów ewakuacji optymalizowanych ze względu na czas lub drogę zwrócono uwagę na tzw. zbiory odniesienia. W przypadku systemów informatycznych wskazano na unijny projekt THEMIS (*Distributed Holistic Emergency Management System*), w ramach którego powstał system wspomagania decyzji w razie katastrof oparty na sztucznej inteligencji.

Metody analizy wielokryterialnej przedstawione w rozdz. 5 są bezpośrednią konsekwencją holistycznego (wieloaspektowego) podejścia preferowanego w przeglądzie literatury. Oceny E (?) zachowania obiektów U ze względu na kryteria F tworzą stożek, którego wierzchołek reprezentuje decyzję kompromisową. Spośród kilku metod wyboru takiej decyzji wybrano metodą zbiorów odniesienia, w której na podstawie funkcji skoringowych ocenia się przejście między punktem *status-quo* a punktem docelowym. Przedstawiono również metodę znajdowania ścieżki wielokryterialnej w grafie, w którym na wagi krawędzi składają się wszystkie kryteria a nie tylko odległość. W sieciach (grafach) antycypacyjnych, oprócz węzłów reprezentujących stan obecny, występują również węzły dotyczące stanów przyszłych, zdolne do podejmowania racjonalnych decyzji.

W rozdz. 6 dokonano krótkiego przeglądu systemów bezpieczeństwa stosowanych obecnie w przemyśle, głównie w energetyce (PGE, Tauron, Energa). Służą one do zarządzania sieciami energetycznymi, monitorowania stabilności oraz optymalizacji dystrybucji energii. Ponieważ systemy te dedykowane są do konkretnych zastosowań nie można ich jeszcze uważać za holistyczne. Podobnie jest w przemyśle naftowym i chemicznym. Wspomniano o systemie DART do zarządzania bezpieczeństwem publicznym w miastach.

Analizy ryzyka przemysłowego rozumianego jako ilościowe przedstawienie potencjalnych skutków zagrożeń (strata finansowa) dotyczy rozdz. 7. Do analizy zastosowano metodę Bow-Tie ze względu na jej czytelność, wykorzystanie wiedzy eksperckiej, identyfikację zagrożeń wraz ze wskazaniem środków zapobiegawczych oraz oceną ich adekwatności. Analiza przeprowadzona w odniesieniu do KW Czatkowice korzysta z pojęcia „najgorszego scenariusza”. Probabilistycznych ocen ryzyka dostarczają sieci bayesowskie. Do przedstawienia całej wiedzy o systemie produkcyjnym służą grafy reprezentacji wiedzy, gdzie węzły oznaczają elementy systemu, a krawędzie relacje między nimi. Atrybuty dodawane do węzłów i krawędzi uzupełniają całość wiedzy. Grafy wiedzy są wykorzystywane przez sieci antycypacyjne do tworzenia modeli stanów przyszłych w razie wystąpienia zagrożenia. Na ilościową miarę ryzyka ciągu technologicznego składa się suma miar ryzyk w jego elementach. Miarę ryzyka w pojedynczym elemencie stanowi iloczyn prawdopodobieństwa zagrożenia, skutku materialnego i wyrażenia $(1+w \cdot T)$, gdzie w określa oddziaływanie międzywęzłowe, a T tłumienie/wzmocnienie propagacji ryzyka. Na podstawie schematów

linii produkcyjnych w KWC (kruszywa, przeróbka, przemiałowania, pakowanie) sformułowano wzory na ich skumulowane ryzyka.

Modelowanie ryzyka dla implementacji w proponowanym systemie IRM DSS jest omówione w rozdz. 8. Bazuje ono na grafach wiedzy, które uzupełnione zbiorem systematycznych zasad stają się tzw. mapami zagrożenia-ryzyka-reakcji TRRM (*Threat Risk Response Map*). Mapy TRRM, o ile nie zawierają luk, stanowią kompletną specyfikację funkcjonalności systemu IRM DSS. Podano algorytm weryfikacji kompletności tych map. Drugim rozważanym problemem jest ewakuacja maszyn i ludzi w KWC biorąc pod uwagę czas, bezpieczeństwo i straty. Z tego względu ewakuacja stanowi problem wielokryterialny, do rozwiązania którego zastosowano genetyczny algorytm NSGA II (*Non-deterministic Sorting Genetic Algorithm II*). Wynikiem jest zespół strategii optymalnych w sensie Pareto, z których decydent może wybrać odpowiedni plan ewakuacji zależnie od preferencji. Wskazano ponadto na możliwość wykorzystania wcześniejszych decyzji do tworzenia następnych jako mechanizmu uczenia maszynowego ML.

Zadania warunkujące implementację systemu IRM DSS w KWC są przedyskutowane w rozdz. 9. Ma on być jednym z komponentów architektury informatycznej złożonej z systemów ERP, SCADA, AWIA Machines (wozidła) wspieranej przez centralną bazę danych. Ponieważ obecnie do wymiany danych służą pliki, konieczne jest opracowanie interfejsów API warunkujących współpracę w czasie rzeczywistym. System ERP powinien zostać uzupełniony o moduł zarządzający zarówno majątkiem jak i bezpieczeństwem wsparty sztuczną inteligencją. Podano wyniki analizy SWOTC implementacji IRM DSS wskazując na silne i słabe strony, szanse, zagrożenia i wyzwania. Podano także zasady szacowania zagrożeń w KWC do poziomów od 0 do 3, z ostatnim w razie fatalnych skutków.

W rozdz. 10 przedstawiono proponowaną architekturę funkcjonalną systemu IRM DSS bazującą na strukturze bazy wiedzy (graf) zakładając rozszerzenie technik pomiarowych (drony, radar, roboty inspekcyjne) wraz z ich fuzją. Podstawę funkcjonowania stanowi macierz decyzyjna wskazująca ciągi przyczynowo-skutkowe prowadzące do działań zapobiegawczych. Na proponowaną architekturę składa się 6 warstw: interfejs użytkownika, analityka z logiką, integracja, baza danych, cyberbezpieczeństwo i dopasowanie do aktualnych warunków zewnętrznych. Zwrócono uwagę, że dopasowanie technologii AI w IRM DSS powinno zapewnić poziom przynajmniej równy poziomowi AI zagrażających czynników zewnętrznych. Do zarządzania ryzykiem służą modele przyczynowości i antycypacyjne. Podano ogólny schemat sieci antycypacyjnej, na który składają się decydenci (agenci), jednostki wykonawcze (np. ratownicze), relacje przyczynowe, kryteria oraz antycypacyjne sprzężenia zwrotne. Korzystając z narzędzi pobranych ze strony www.anticipatingnetworks.net przedstawiono dwa przykłady ze strukturą grafów, macierzami decyzyjnymi, sprzężeniami antycypacyjnymi, strefami antycypacyjnymi poszczególnych węzłów oraz sekwencją decyzji prowadzących do poprawnego rozwiązania. W pierwszym przykładzie chodzi o osiągnięcie wyników zgodnych z oczekiwaniami decydenta, a w drugim o maksimum efektywności działania jednostek wykonawczych.

Omówienie możliwych sytuacji w KWC na podstawie symulacji w zaprojektowanym interfejsie dla środowiska Matlab zawiera rozdz. 11. Interfejs ten umożliwi pracę na kilku podkładach graficznych (tło, drogi, pojazdy, przeszkody, zagrożenie, miejsca bezpieczne), przy czym drogi i pojazdy mają określone parametry (np. nachylenie, promień skrętu). Symulacje dotyczą materializacji ryzyka w postaci osunięcia się mas skalnych z koniecznością ewakuacji wozideł i koparki. Danymi wejściowymi są ich aktualne pozycje, miejsca bezpieczne oraz możliwe trasy ewakuacyjne w ewentualnych przeszkodach. Przedstawiono dwa warianty ewakuacji, pierwszy z dwoma trasami zawierającymi punkt wspólny, drugi z jedną trasą, ale mającą kilka odgałęzień. Wyniki zawierają czas trwania ewakuacji, długość trasy oraz procentowe uszkodzenia pojazdów. W drugiej części rozdziału

przedstawiono scenariusze zastosowania IRM DSS wynikające z dynamicznych zmian w środowisku (osunięcia), konieczność zapewnienia bezpieczeństwa maszyn, funkcjonowania samej platformy informatycznej oraz kwestii ochrony fizycznej. Pokazano co mają wtedy czynić jednostki decyzyjne i wykonawcze. Wskazano, że integracja systemu zarządzania ryzykiem z systemem ERP wymaga ciągłej komunikacji.

Na część końcową rozprawy składają się trzy ostatnie rozdziały. Proponowany szczegółowy harmonogram wdrożenia systemu IRM DSS w KWC podzielony na 4 etapy przedstawiono w rozdz. 12. Są nimi: planowanie, przygotowanie infrastruktury, wdrożenie i szkolenia. Na wdrożenie przewidziano 5...7 miesięcy. Każdy z etapów uwzględnia aspekty bezpieczeństwa technicznego, fizycznego i informatycznego. Po wdrożeniu system IRM DSS wymaga naturalnie utrzymania. Podkreślono, że w pierwszej kolejności system powinien zapobiegać skutkom osuwisk, zalań i zagrożeniom infrastruktury.

Kierunki dalszego rozwoju systemu bezpieczeństwa w KWC (rozdz. 13) wynikają z postępu technicznego i dostępności nowych rozwiązań. Skrótowo określają je hasła AI, ML, IoT, cyberbezpieczeństwo, rozwiązania chmurowe, a w odniesieniu do rozszerzenia funkcjonalności – zarządzanie danymi w kierunku analizy predykcyjnej oraz zwiększenie autonomii systemów decyzyjnych.

W podsumowaniu zawierającym Wnioski końcowe (rozdz. 14) podkreślono, że rozprawa przedstawia założenia, funkcjonalności oraz możliwości systemu klasy IRM DSS wspierającego procesy decyzyjne w zarządzaniu ryzykiem przemysłowym, zwłaszcza w sektorze górnictwa odkrywkowego. Wyniki badań wskazują na znaczenie analizy wielokryterialnej, technologii AI oraz holistycznego podejścia do zagadnień bezpieczeństwa. Podano, co rozprawa wnosi do podstaw nauki o bezpieczeństwie, jakie są nowe metodologie zastosowane w projektowaniu oraz w jaki sposób je zastosowano w proponowanym systemie IRM DSS.

3. Ocena ogólna

Zasadniczym rezultatem rozprawy doktorskiej mgr P. Łydka jest zbiór metod i algorytmów przeznaczonych do wspierania decyzji w systemach zarządzania bezpieczeństwem przemysłowym, wspartych technologiami informacyjno-komunikacyjnymi i elementami sztucznej inteligencji. Metody te odnoszone są do problemów bezpieczeństwa występujących w macierzystym zakładzie Autora, tj. Kopalni Wapienia Czatkowice, w której istnieje możliwość wdrożenia systemu IRM DSS zarządzającego bezpieczeństwem.

Solidnie przeprowadzony przegląd literatury wskazał na potrzebę wielokryterialnego (holistycznego) podejścia do zarządzania bezpieczeństwem, w którym kluczowymi metodami są sieci antycypacyjne, grafy reprezentacji wiedzy i analiza wielokryterialna. Sieci antycypacyjne umożliwiają symulację i predykcję potencjalnych zagrożeń pomagając w ich zapobieganiu. W odniesieniu do KWC przedstawiono dwuwariantową symulację ich wykorzystania dla ewakuacji. Grafy reprezentacji wiedzy są strukturą danych łączącą proces produkcyjny, infrastrukturę techniczną oraz czynniki ryzyka wraz z ich wzajemnymi relacjami. Sieci antycypacyjne korzystają z tych grafów w celu prognozowania.

Analiza wielokryterialna bazująca na sieciach i grafach umożliwia podejmowanie kompromisowych decyzji w warunkach złożoności i niepewności, w oparciu o kryteria dotyczące bezpieczeństwa pracowników i maszyn, strat finansowych, cyberbezpieczeństwa itp. Przedstawiono algorytm genetyczny rozwiązujący problem optymalizacji wielokryterialnej. Mapy TRRM, czyli zagrożenia-ryzyka-reakcje, będące instancjami grafów wiedzy, z których zaproponowany algorytm usuwa ewentualne luki, stają się kompletną specyfikacją systemu IRM DSS zarządzającego bezpieczeństwem. Warunkiem jego faktycznego zastosowania jest fuzja danych pochodzących z różnych źródeł, którymi w KWC są systemy ERP, SCADA i AWIA oraz centralna baza danych.

Przedstawiony kilkietapowy harmonogram wdrożenia systemu IRM DSS uwzględnia bezpieczeństwo fizyczne, techniczne i informatyczne. Można go uważać za realny pod warunkiem dostępności środków technicznych i wykwalifikowanej kadry. Rokuje to także perspektywę zastosowania w innych sektorach przemysłu.

Podsumowując, rozprawa doktorska mgr P. Łydka, której pracowitość wyraźnie przekracza typowe doktoraty, poprzez zaproponowanie holistycznego podejścia do zarządzania ryzykiem w zakładach przemysłowych, łączącego modele ryzyka, zapobieganie im oraz minimalizację skutków zagrożeń w jednym systemie, zrealizowała postawione cele wykazując zarazem prawdziwość tezy. Holistyczne podejście odróżnia ją od dotychczasowych rozwiązań zorientowanych na pojedyncze aspekty ryzyka. Postępując rzetelną przemyślaną drogą Autor przedstawił zbiór metod i algorytmów przeznaczonych do wspomagania decyzji w zarządzaniu ryzykiem przemysłowym wspartych architekturą systemu przeznaczonego do ich implementacji.

Spis literatury liczy 214 pozycji ściśle związanych z tematyką rozprawy, wśród których znajdują się 4 prace Autora napisane wraz z promotorem.

4. Uwagi

Podane niżej uwagi krytyczne mają znaczenie drugorzędne i nie umniejszają wartości rozprawy.

- 1) Za system informatyczny uważa się oprogramowanie i sprzęt zdolne do przetwarzania danych. System IRM DSS nie osiągnął jednak jeszcze takiego poziomu, bo w rozprawie przedstawiono przede wszystkim metody i algorytmy, na których ma on bazować. Lepiej byłoby więc nazywać go tymczasowo systemem informacyjnym.
- 2) Czy zapis $FP(U) := F(P(U, F))$ na str. 91 należy rozumieć jako rozwiązanie iteracyjne? Co oznaczają E i \emptyset we wzorze (5.1)?
- 3) System ERP wraz z bazą danych ma być głównym elementem docelowego systemu informatycznego w KWC (str. 167). Czy obecny system ERP firmy BILANS JR uzupełniony interfejsami online byłby w stanie pełnić tę rolę?
- 4) Kto jest producentem systemu SCADA, którego *dashboard* pokazano na str. 170? Jakimi protokołami komunikuje się stacja operatorska ze sterownikami PLC?
- 5) Na str. 215 napisano, że aplikacja informuje operatora o procentowych uszkodzeniach pojazdów. Czy w praktyce informacja ta pochodziłaby automatycznie z systemu AWIA Machines, czy od kierowców pojazdów?
- 6) Wdrożenie systemu IRM DSS w ciągu 5...7 miesięcy wymaga środków technicznych i kadry. Ile osób miałyby okresowo w tym uczestniczyć?

Rozprawa jest nadzwyczaj obszerna (254 strony) i pod względem formalnym nie budzi żadnych zastrzeżeń. Język opisów tekstowych (nieco emfaticzny), tabele, rysunki i zrzuty z ekranu są bez zarzutu. Usterki redakcyjno-edytorskie występują sporadycznie.

5. Wniosek końcowy

Uważam, że cele postawione w rozprawie zostały osiągnięte. Autor opracował metody i algorytmy wspomagania decyzji w przemysłowych systemach bezpieczeństwa wykorzystujących grafy wiedzy, sieci antycypacyjne i analizę wielokryterialną, wsparte sztuczną inteligencją. Przedstawił wariantową symulację ewakuacji maszyn w odkrywkowej Kopalni Wapienia Czatkowice w razie osuwisk skał.

Wobec tego uważam, że rozprawa doktorska mgr inż. Pawła Łydka pt. *System wspomagania decyzji w projektowaniu i wdrażaniu przemysłowych systemów bezpieczeństwa wykorzystujących techniki sztucznej inteligencji*, której tematyka mieści się w dyscyplinie *automatyka, elektronika, elektrotechnika i technologie kosmiczne*, w pełni spełnia wymagania stawiane w Ustawie *Prawo o Szkolnictwie Wyższym i Nauce* z dn. 20.07.2018 r. i wnoszę o dopuszczenie jej do publicznej obrony.

Leszek Tybura