AKADEMIA GÓRNICZO-HUTNICZA IM. STANISŁAWA STASZICA W KRAKOWIE

DZIEDZINA NAUK INŻYNIERYJNO-TECHNICZNYCH

DYSCYPLINA: AUTOMATYKA, ELEKTRONIKA, ELEKTROTECHNIKA

I TECHNOLOGIE KOSMICZNE

AUTOREFERAT ROZPRAWY DOKTORSKIEJ

System wspomagania decyzji w projektowaniu i wdrażaniu przemysłowych systemów bezpieczeństwa wykorzystujących techniki sztucznej inteligencji

Autor: mgr inż. Paweł Łydek

Promotor rozprawy: Prof. dr hab. inż. Andrzej M. Skulimowski

Praca wykonana: Akademia Górniczo Hutnicza,
Wydział Elektrotechniki, Automatyki, Informatyki i Inżynierii Biomedycznej

Kraków, 2025

STRESZCZENIE

Potrzeba ciągłego rozwoju i doskonalenia systemów bezpieczeństwa w zakładach przemysłowych nabrała priorytetowego charakteru w obliczu rosnących obecnie wyzwań związanych z zapewnieniem bezpiecznych warunków pracy, ochroną środowiska oraz skutecznością i ciągłością działania systemów produkcyjnych. Postęp technologiczny oraz rosnąca dostępność nowoczesnych rozwiązań otwierają możliwości w obszarze integracji nowych narzędzi i technologii z istniejącymi już systemami wspomagającymi procesy zarządzania bezpieczeństwem.

W rozprawie przedstawiono motywacje i cel badań, opisano problemy związane z bezpieczeństwem w odkrywkowym zakładzie górniczym oraz szczegółowo przeanalizowano specyficzne potrzeby związane z ochroną pracowników, zasobów i infrastruktury przed zagrożeniami, które mogą wystąpić podczas prowadzenia eksploatacji zasobów i realizacji procesów przemysłowych. Uwzględniono możliwości wykorzystania nowoczesnych technologii, takich jak monitoring wizyjny, drony oraz czujniki rozmieszczone na obszarze górniczym, które mogą być wykorzystane do monitorowania ryzyka i zapobiegania potencjalnym zagrożeniom.

Wspomniane wyżej technologie pełnią istotną rolę w koncepcji funkcjonowania opracowanego w ramach badań i przedstawionego w rozprawie innowacyjnego systemu IRM DSS (*Industrial Risk Management Decision Support System, system wspomagania decyzji w zarządzaniu ryzykiem*). Poprzez śledzenie zmian w środowisku produkcyjnym, algorytmy oparte o metody sztucznej inteligencji analizują dane z czujników, dając możliwość wczesnego wykrywania niepokojących sygnałów w trybie pracy ciągłej. Podejście takie pozwala na identyfikację nieprawidłowości w czasie rzeczywistym oraz na wdrożenie działań zapobiegawczych, co z kolei minimalizuje ryzyko zdarzeń niebezpiecznych. Szczegółowa analiza technik identyfikacji, pomiaru i zarządzania ryzykiem, które stanowią podstawę działania IRM DSS, pozwoliła na zaproponowanie architektury oprogramowania systemu wspomagania decyzji opartego na sztucznej inteligencji (AI), wykorzystującego m.in. modele sieci antycypacyjnych, metody analizy wielokryterialnej, fuzji informacji eksperckich, uczenia maszynowego i innych technik przetwarzania wiedzy.

Nowe podejście do projektowania inteligentnych systemów wspomagania decyzji w zarządzaniu ryzykiem przemysłowym i implementacja IRM DSS omówione są w kontekście integracji tego systemu z istniejącymi już w przedsiębiorstwie systemami informatycznymi, takimi jak systemy ERP i SCADA. Szczegółowa analiza środowiska IT/OT pozwoliła wskazać luki funkcjonalne w obecnie stosowanych rozwiązaniach oraz potencjalne korzyści z interoperacyjności IRM DSS z pozostałymi systemami, które pozwalają na holistyczne zarządzanie bezpieczeństwem. Szczególną uwagę zwrócono na specyficzne wymagania w zakresie dopasowania technologicznego, które mają zapewnić, że nowe metody wdrażania AI są nie tylko zgodne z potrzebami przedsiębiorstwa, ale także zoptymalizowane pod kątem efektywności i gotowości do użycia. Szczególną uwagę poświęcono modelom przyczynowości oraz zastosowaniu algorytmów optymalizacyjnych, co pozwala na lepsze planowanie działań awaryjnych. Naturalną konsekwencją projektu IRM DSS jest jego wdrożenie w warunkach przemysłowych. W tym celu zaproponowano praktyczne scenariusze zastosowania systemu w różnych sektorach przemysłowych oraz omówiono prognozowane dalsze kierunki rozwoju technologii bezpieczeństwa w przemyśle.

Wnioski końcowe z przeprowadzonych badań podkreślają znaczenie AI w nowoczesnym zarządzaniu ryzykiem przemysłowym, wskazując na potencjalne możliwości dalszej integracji tych rozwiązań z innymi obszarami zarządzania przedsiębiorstwem, takimi jak planowanie inwestycji i analiza ryzyka finansowego.

Spis treści

1 Wprowadzenie: cel i zakres prac badawczych

1.1 Cel i teza rozprawy

Głównym celem prac badawczych przedstawionych rozprawie było opracowanie metod wspomagania decyzji w systemach zarządzania bezpieczeństwem przemysłowym, w pierwszej kolejności ukierunkowanych na zapewnienie optymalnej ewakuacji maszyn górniczych z wyrobiska w sytuacji zagrożenia. Projektowane metody zostały zastosowane w interfejsie systemu wspomagania decyzji dotyczących minimalizacji ryzyk i zapewnienia bezpieczeństwa przemysłowego (*Industrial Risk Management Decision Support System* – IRM DSS) w zakładzie górnictwa odkrywkowego. Wskazany zakres badań wynika wprost z potrzeb przedsiębiorstwa, zidentyfikowanych w trakcie pracy zawodowej autora. Implementacja systemu klasy IRM DSS dopasowanego do tych potrzeb i wykorzystującego wyniki badawcze programu doktoratu wdrożeniowego jest finalnym celem opracowanych podstaw teoretycznych, metod pozyskiwania i przetwarzania danych, algorytmów i architektury informatycznej IRM DSS.

Efektem końcowym badań jest opracowanie architektury informatycznej specjalistycznego systemu wspomagania decyzji oraz zestaw algorytmów wspomagania decyzji, w szczególności:

- algorytmy weryfikujące poziom zabezpieczenia chronionego terenu i pozwalające na optymalny dobór dodatkowych sensorów i elementów zabezpieczających,

- algorytmy wyznaczania w czasie rzeczywistym optymalnej drogi ewakuacji zagrożonego sprzętu do obszarów zidentyfikowanych jako bezpieczne na podstawie odrębnych strumieni informacji pochodzących z systemu sensorów oraz od służb zapewnienia bezpieczeństwa przedsiębiorstwa w sytuacjach kryzysowych.

Algorytmy te zostały zaimplementowane i zweryfikowane symulacyjnie. Algorytmy grupy drugiej wskazują alternatywne drogi ewakuacji, stosując kryteria oczekiwanej wartości zagregowanego wskaźnika zagrożeń, oczekiwanej wartości strat materialnych oraz czasu ewakuacji. W oparciu o informacje dotyczące preferencji dysponenta systemu oraz wcześniej podjęte decyzje i ocenę ich skutków, system rekomenduje kompromisową drogę ewakuacji w oparciu o mechanizm adaptacyjny, który dla każdej maszyny wskazuje kolejne odcinki ścieżki, na podstawie aktualizowanych na bieżąco informacji o przebiegu akcji ewakuacyjnej, ewolucji zagrożeń oraz modyfikacji preferencji decydentów odpowiedzialnych za zapewnienie bezpieczeństwa zakładu i nadzorujących pracę systemu. W celu rekomendacji decyzji kompromisowych wybrana została metoda analizy wielokryterialnej oparta o zbiory odniesienia, która w optymalny sposób zapewnia reprezentację wcześniejszych wyborów dróg ewakuacji w podobnych sytuacjach (także symulowanych), ograniczeń związanych z przepisami prawnymi i procedurami zapewnienia bezpieczeństwa oraz celów akcji ewakuacyjnej opisanych przez docelowe wartości kryteriów optymalności. Z kolei priorytetyzacja akcji ratowniczych oparta jest o inną metodę sztucznej inteligencji (ang.: *Artificial Intelligence*, AI), a mianowicie o sieci antycypacyjne, łączące analizę predykcyjną dynamiki zagrożeń z preskrypcyjną analizą danych i decyzji (ang.: *prescriptive analytics*). Metody te są szczególnie pomocne w sytuacji zakłóceń lub braku komunikacji z ekipami ratowniczymi.

Mając na uwadze przedstawione wyżej cele oraz uwzględniając potrzeby przedsiębiorstwa, uzasadnione jest poszukiwanie i wdrażanie rozwiązań informatyczno-organizacyjnych opartych o podejścia holistyczne, uwzględniające wieloaspektowy charakter zarządzania ryzykiem przemysłowym. Przesłanka ta prowadzi do sformułowania następującej tezy badawczej:

TEZA ROZPRAWY

Efektywność rozwiązania problemów związanych z budowaniem i utrzymaniem odporności na różnorodne zagrożenia w zakładzie produkcyjnym przemysłu górnictwa odkrywkowego wymaga systematycznego wdrażania i stosowania najnowszych metod i technologii. W celu planowania budowy odporności oraz umożliwienia szybkiego i skutecznego reagowania na wystąpienia zagrożeń przemysłowych konieczny jest dobór odpowiednich narzędzi informatycznych. Cel ten może zostać efektywnie osiągnięty poprzez projekt i implementację Systemu Wspomagania Decyzji wykorzystującego metody sztucznej inteligencji do modelowania ryzyk przemysłowych oraz algorytmy analizy wielokryterialnej do generowania rekomendacji decyzyjnych wspierających kadrę zarządzającą odpowiedzialną za podejmowania decyzji w sytuacji zagrożenia.

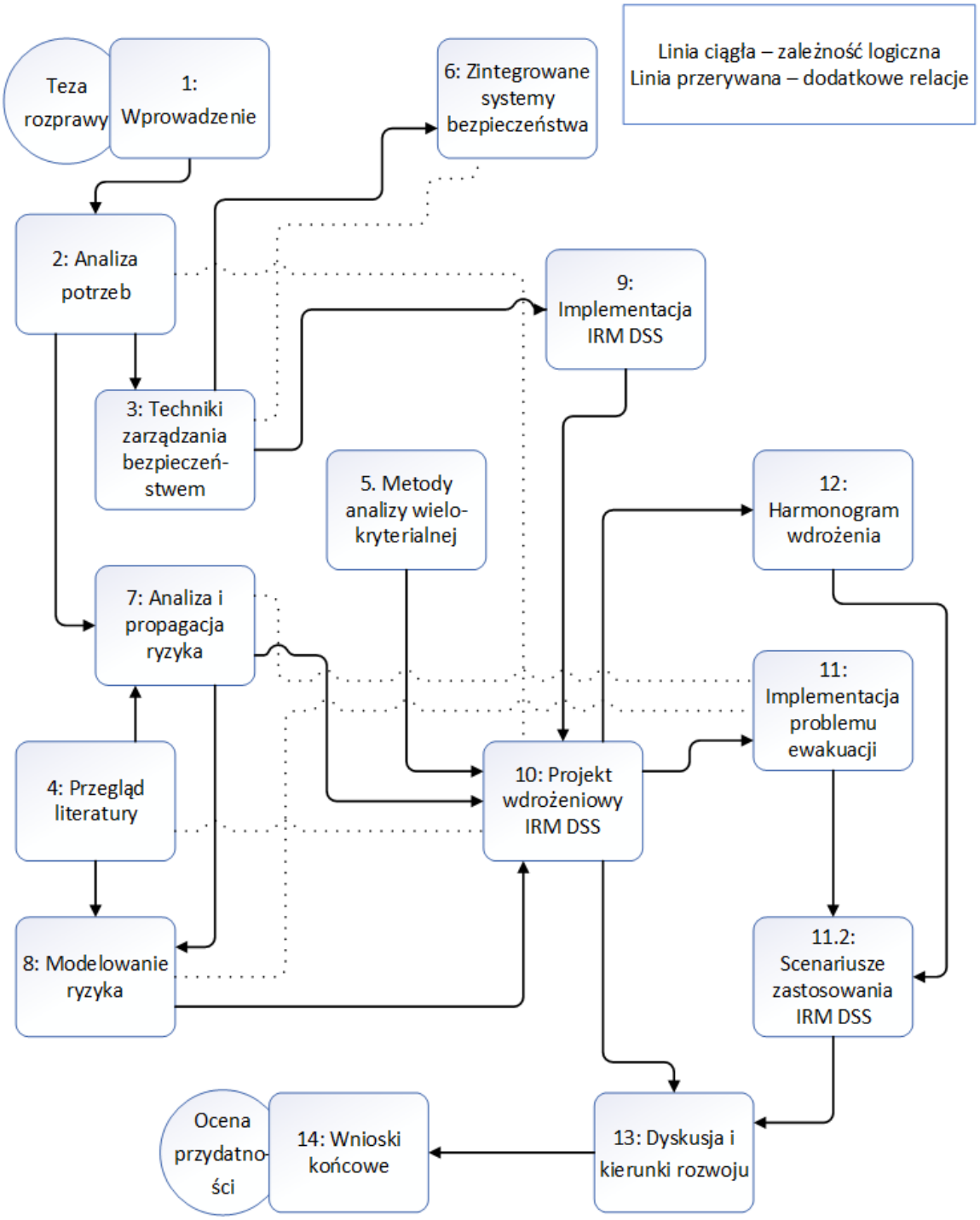
Zgodnie z wstępnym studium wykonalności, IRM DSS jest implementowany zgodnie z paradygmatem DevOps [De Nicola i in., 2022], a doświadczenie zdobyte podczas jego działania jest dodatkowo wzmacniane przez powiązania z zewnętrznymi modułami AI-foresight i AI-alignment [Rönnbäck, Holmström, 2008]. W rozważanych w pracy problemach bezpieczeństwa przemysłowego ryzyko przypisuje się m.in.:

- zagrożeniom zewnętrznym, zarówno naturalnym, jak i antropogenicznym,
- procedurom przetwarzania informacji, które mogą zniekształcać dane za pomocą zakłóceń i błędów systematycznych,
- ludzkim błędom operacyjnym i powtarzalnym błędom decyzyjnym, które mogą być podejmowane podczas procesu zarządzania ryzykiem.

Rozprawa opracowana została w sposób pozwalający płynnie przejść od zidentyfikowanych potrzeb przedsiębiorcy, poprzez badania bibliograficzne i analizy, do omówienia i podsumowania przeprowadzonych badań z uwzględnieniem specyfiki analizowanego problemu badawczego oraz propozycją systemu informatycznego, który spełni stawiane oczekiwania. W strukturze rozprawy wyróżnić można następujące, kolejno omówione, elementy logiczne:

A) Wstęp, gdzie naszkicowane zostało w sposób ogólny tło badań, oraz zaprezentowano przedsiębiorstwo, którego środowisko pracy i funkcjonowania, stanowi obszar zarówno badawczy jak i wdrożeniowy dla proponowanego systemu.
B) Sformułowanie problemu, ze szczególnym uwzględnieniem opisu zagrożeń zidentyfikowanych w KWC, ich omówieniem, identyfikacją oraz propozycją rozwiązania przy wsparciu systemu IRM DSS. Dodatkowo w tej części zaprezentowano strukturę przedsiębiorstwa z analizą ukierunkowaną na identyfikacje ryzyk i zagrożeń na kolejnych etapach ciągów produkcyjnych i uwzględniającą specyfikę środowiskową oraz branżową.
C) Omówienie obecnych sposobów zarządzania zagrożeniami i prowadzonych analiz w obszarze zarządzania bezpieczeństwem.
D) Analiza bibliograficzna w zakresie stanu badań DSS dla bezpieczeństwa przemysłowego, z uwzględnieniem zagadnień dotyczących fuzji informacji.
E) Podstawy teoretyczne dla zagadnień związanych z modelami ryzyka, sieciami antycypacyjnymi, grafami wiedzy.
F) Omówienie metodyk modelowania, pomiaru, zarządzania i propagacji ryzyka.
G) Podstawy teoretyczne i możliwości zastosowanie metody wielokryterialnej analizy danych.
H) Omówienie proponowanej architektury IRM DSS w oparciu o założenia przygotowane dla systemu TRRM oraz z uwzględnieniem architektury opartej o strukturę baz wiedzy.
I) Omówienie rzeczywistych problemów ewakuacji w oparciu o zaprojektowany interfejs dla środowiska Matlab, szczegółowe symulacje przeprowadzone w oparciu o sieci antycypacyjne przeprowadzone w dedykowanej aplikacji.
J) Propozycja implementacji zawierająca poruszone wcześniej zagadnienia i uwzględniająca potrzeby przedsiębiorcy, w tym możliwości integracji z funkcjonującymi już systemami informatycznymi oraz systemami automatyki przemysłowej (OT).
K) Podsumowanie oraz wnioski końcowe.

Schemat zależności logicznej rozdziałów rozprawy doktorskiej przedstawiony jest na Rys. 1.



Rys. 1. Schemat zależności logicznej rozdziałów z zaznaczonymi najważniejszymi osiągnięciami.

1.2 Charakterystyka przedsiębiorstwa i zagadnień związanych z bezpieczeństwem przemysłowym

Kopalnia Wapienia Czatkowice jest odkrywkowym zakładem górniczym, eksploatującym złoża wapieni karbońskich na terenie Garbu Tenczyńskiego, stanowiącego południowy fragment Wyżyny Krakowsko-Częstochowskiej, w odległości ok 28 km na zachód od Krakowa, w gminie Krzeszowice.

Działalność górnicza, a w mniejszym stopniu także pozostała działalność KWC związana jest z występowaniem szeregu ryzyk. Są to przede wszystkim:

- naturalne zjawiska geologiczne i atmosferyczne,
- intruzje połączone z włamaniem, kradzieżą lub sabotażem,
- awarie sprzętu i infrastruktury,
- wypadki z udziałem ludzi lub sprzętu.

Z kolei bezpieczeństwo zakładu przemysłowego jakim jest KWC, definiowane jest jako stan, w którym zapewnione są:

1. nieprzerwane dostawy surowca,
2. ciągłość pracy maszyn i urządzeń,
3. minimalizacja ryzyk i zagrożeń wskazanych wyżej,

oraz

4. poczucie bezpieczeństwa i komfortu psychicznego pracowników, w tym również osób dozoru odpowiedzialnych za utrzymanie bezpieczeństwa.

2 Modelowanie ryzyka dla celów implementacji IRM DSS

2.1 Zastosowanie grafów wiedzy w modelach zarządzania ryzykiem

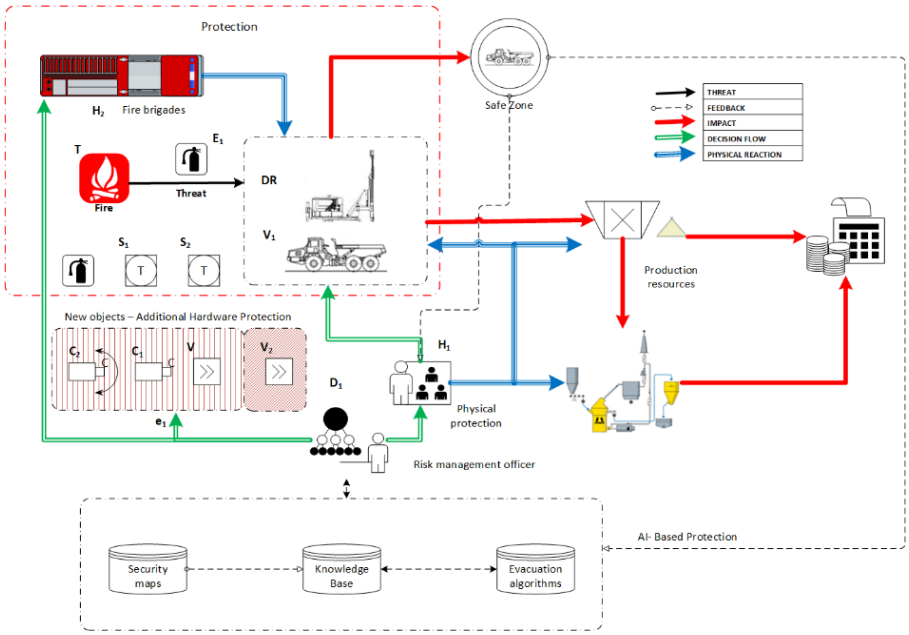
Jako narzędzia wspierającego proces zarządzania ryzykiem w systemie klasy IRM DSS wykorzystane zostały grafy wiedzy [Skulimowski, Łydek, 2022]. W celu usystematyzowania informacji przyjmujemy, że w modelu zarządzania zagrożeniami i ryzykiem występują następujące obiekty:

- Zagrożenia, naturalne lub antropogeniczne, oznaczane jako $T_1, T_2, \ldots, T_{n1}$.
- Dwa rodzaje węzłów fuzji informacji: integratory zdolne do fuzji informacji tego samego rodzaju z różnych sensorów (fuzja prosta: oznaczane jako $(\varphi_1, \ldots, \varphi_{n2})$ oraz węzły złożone zdolne do fuzji informacji heterogenicznych, oznaczane jako $\Phi_1, \ldots, \Phi_{n3}$.
- Zagrożone osoby i zespoły ludzkie, przy czym zagrożenia dotyczą ich zdrowia lub życia.
- Zagrożone artefakty, takie jak maszyny (M_i), pojazdy (V_j), budynki (B_k) itp. lub jednostki złożone odpowiedzialne za całe podprocesy produkcyjne.
- Hierarchiczna (niższy, średni i najwyższy poziom) struktura jednostek decyzyjnych D, będąca częścią systemu bezpieczeństwa przedsiębiorstwa.
- Wewnętrzne zespoły ratownicze, roboty ratownicze, urządzenia wykonawcze (np. automatyczne gaśnice), które realizują decyzje związane z zarządzaniem kryzysowym (R_j).
- Zewnętrzne służby ratownicze (ER_i), które w razie potrzeby mogą być zaangażowane w działania ratownicze oraz dodatkowe zasoby (AR_k), które w razie potrzeby mogą być zmobilizowane przez zarządzanie kryzysowe.

Powyższe obiekty są wynikiem długofalowego przydziału zasobów i działań organizacyjno-inwestycyjnych. Są to m.in. portfel technologii, które mogą być zastosowane w celu zapobiegania lub ograniczania zagrożeń, zespoły ratownicze i inne zasoby ludzkie przeszkolone w zakresie nowych technologii, regulaminy i instrukcje postępowania w przypadku wystąpienia zagrożeń, aktywa finansowe, które mogą być podstawą do długoterminowego planowania ograniczania zagrożeń i zarządzania ryzykiem.

Wskazane obiekty można przedstawić w postaci diagramu, którego węzły odpowiadają wszystkim istotnym podmiotom w zagrożonym przedsiębiorstwie, a krawędzie modelują

relacje między nimi. Jeśli dodatkowo uwzględnimy adaptacyjny charakter zarządzania zagrożeniami, diagram ten staje się dynamicznym multigrafem skierowanym z trzema rodzajami krawędzi. Oznaczają one przepływ informacji, propagację i wpływ zagrożeń oraz przekazywanie i wpływ decyzji, przy czym te ostatnie w ramach deontycznej struktury zaleceń, poleceń i granic [Rys.2].



Rys. 2. Mapa zagrożenie-ryzyko-reakcja, która odpowiada sytuacji przedstawionej w Problemie 2.1.

2.2 Problem projektowania TRRM i jego rozwiązanie

TRRM można traktować jako instancje grafów wiedzy [De Nicola i in., 2022] poświęconych zarządzaniu zagrożeniami i ryzykiem [Steinberg, 2005]. Multigraf ten [Rys.2] może być rozszerzony o kolejne obiekty, relacje i struktury, takie jak schematy linii produkcyjnych, gdzie zagrożenie nałożone na poprzednika w sekwencji propagacji zagrożeń powoduje przerwy w produkcji lub kolejne zagrożenie w kolejnym węźle. Topologia TRRM może zmieniać się w czasie w zależności od aktualnej fazy zapobiegania zagrożeniom i zarządzania ryzykiem. Zbiór obiektów włączonych do modelu jako węzły również może się zmieniać. Różne wystąpienia zagrożenia lub różnych zagrożeń będą również skutkować różnymi TRRM, nawet jeśli fizyczne obiekty objęte mapą pozostają takie same. Z punktu widzenia środowiska pracy węzły będą rozmieszczone w trzech warstwach: funkcjonalnej, operacyjnej i zarządzającej. Aby to odnieść do realiów KWC, można przyjąć, że warstwa funkcjonalna obejmuje urobek, transport i przetwarzanie surowca, warstwa zarządzająca obejmuje systemy monitorujące pracę maszyn oraz bezpieczeństwo ogólne, a warstwa operacyjna obejmuje decydentów na wszystkich poziomach decyzyjnych [Keenan, Jankowski, 2019]. Pomiędzy węzłami w trzech warstwach funkcjonalnych istnieją skomplikowane relacje dotyczące przepływu i połączeń, obejmujące przepływ materiału, przepływ informacji i przepływ energii, patrząc z punktu widzenia procesu technologicznego [Feng i in., 2024]. Celem projektanta IRM DSS jest wypełnienie wszystkich luk w TRRM, aby dostarczyć kompletną specyfikację IRM DSS. Pierwszym problemem przy projektowaniu struktury ograniczającej zagrożenie jest weryfikacja kompletności TRRM, a w przypadku odpowiedzi negatywnej rozwiązanie następujących problemów:

Problem 2.1. Biorąc pod uwagę TRRM Θ, być może niekompletny, minimalny dopuszczalny próg wiarygodności informacji $\alpha>0$, stałe τ, zbiór $Q=\{q_1,...,q_p\}$ obiektów, które można dodać do Θ jako jego węzły, potencjalne nowe połączenia $E=\{e_1,...,e_r\}$ pomiędzy węzłami oraz koszt dodania węzła q lub krawędzi $e(q,q')$ odpowiednio do Θ, $c(q)$ lub $c(e)$, znajdź kompletny TRRM Θ' taki że:

(i) $\Theta \subset \Theta'$ i Θ' ma wartość minimalną, tzn. jeżeli $\Theta \subset \Delta \subset \Theta'$ i Δ jest kompletny, to $\Delta=\Theta'$,
(ii) wiarygodność informacji wychodzącej wszystkich węzłów fuzji informacji w Θ' jest równa lub większa od α,
(iii) dla każdego zagrożenia T I obiektu Z, zdolność $h_R(T,Z,\tau)$ do łagodzenia T w kompletnym TRRM nie powinna być mniejsza niż h_R w Θ,

przy minimalnym całkowitym koszcie nowych obiektów i połączeń. ■

Problem 2.1 jest zadaniem optymalizacji kombinatorycznej, gdzie podzbiory Q i E są rozwiązaniami tentatywnymi, które mogą być poprawiane za pomocą heurystyk, takich jak algorytmy genetyczne [Katoch i in., 2021] lub symulowanego wyżarzania [Niyomubueyi i in., 2020]. Metodyka postępowania oparta jest o algorytm NSGA II, natomiast sam proces rozwiązywania składa się z dwóch etapów:

- weryfikacja kompletności Θ przy progu β

oraz – jeżeli wynik weryfikacji jest negatywny,

- rozwiązywanie problemu minimalnego kosztu modernizacji urządzeń.

Przykład kompletnej struktury TRRM który odnosi się do rzeczywistej sytuacji fizycznej w kopalni wapienia dla ustalonego czasu t przedstawiono na [Rys. 2] poniżej. Algorytm weryfikacji bada graf TRRM, oblicza i łączy zdolność usuwania skutków zagrożenia β dla każdego potencjalnego zagrożenia T. Jego pierwszym krokiem jest analogiczny algorytm, który znajduje próg

Algorytm 2.1 (weryfikacja kompletności TRRM dla τ).

Dane wejściowe: lista węzłów Θ i ich atrybutów, $X:=I\cup\psi\cup\Psi$.
Rozszerzona macierz sąsiedztwa Θ zawierająca właściwości krawędzi, zdolności łagodzącej i reguły łączenia wiarygodności informacji.
Inicjuj $\alpha:=0$, $\beta:=1$

1. Oblicz α dla podmacierzy sąsiedztwa z węzłami $I\cup\psi\cup\Psi$
2. **for** dla wszystkich węzłów Z z Θ
3. **if** Z jest obiektem aktywnym **then**
4. **for** wszystkich uczestników R_i połączonych z Z
5. Oblicz $h(R_1,T,Z,\tau)$
6. **end for**
7. Oblicz wspólną.zdolność.łagodzenia.skutków $h(R_1,...,R_m,T,Z,\tau)$
8. $\beta:=\min(\beta,h(R_1,...,R_m,T,Z,\tau))$
9. **end if**
10. **end for**
11. **if** $\beta=1$ **then** Θ jest kompletny **else** Θ jest β-kompletny **end if**
12. **end** ■

Poniżej zaproponowano zastosowanie heurystyki polegającej na dekompozycji optymalnej konstrukcji struktury TRRM na serię działań powiększających zbiór węzłów Θ o jeden element w każdym kroku.

Algorytm 2.2 (heurystyczne rozwiązanie Problemu 2.1)

Dane wejściowe: Zweryfikowany $\Theta:=(Y,\Xi)$, dostępny sprzęt i inne obiekty TRRM Q, powiązania funkcjonalne E w Θ, zbiór potencjalnych zagrożeń $\boldsymbol{T}$, koszty $c(w)$ i zdolności łagodzące $h(T,w,\tau)$ dla wszystkich $w\in Q$.
Współczynnik kompromisu $0<\lambda<1$ pomiędzy kosztem i $h(T,w,\tau)$.

1. Podziel zbiór krawędzi E na E_c – nowe połączenia do istniejących węzłów Y z Θ i E_q –połączenia pomiędzy $q\in Q$. Ustal $W:=Q\cup E_c$, $P:=\varnothing$
2. **for** wszystkich $w\in Q$
3. Oblicz niezdominowany podzbiór $X(w)$ *zbioru* $P\cup P(w)$, gdzie $P(w)$ wszystkich par $(c_e(w), h(T,w,e(w),\tau))$, gdzie $c_e(w)$ to koszty dopuszczalnych połączeń $e(w)$ pomiędzy i Y, $h(T,w,e(w),\tau)$ to ich zdolności łagodzące.
4. Ustaw: $P:=P\cup X(w)$
5. **end for**
6. **for** $x=(x_1(w),x_2(w))\in P$
   oblicz $y(w):=\lambda x_1(w)+x_2(w)$
7. **end for**
8. **while** Q jest niepuste **and** $cost\le c_{max}$ **do**
9. Sortuj $w\in W$ według $y(w)$ w porządku rosnącym
10. Wybierz pierwsze $w\in Q\cup E_c$, ustaw $\Theta:=\Theta\cup\{w\}$, oblicz β dla Θ
11. **if** Θ jest kompletny **break**
12. **elsif** $w\in Q$ set $E_c:=E_c\cup S$,
    gdzie $S:=\{s\in E_q$ które łaczą w z innymi węzłami w $\Theta\}$,
13. ustaw $Q:=Q\setminus\{w\}$, $W:=W\cup Y\setminus\{w\}$. $cost:=cost+x_1(w)$
14. **end if**
15. **end while**
16. **return** α, β, $cost$, Y, Ξ
17. **end** ■

Więcej kryteriów i wymagań można analizować jako rozszerzenie Problemu 2.1, na przykład: problem zapewnienia ograniczenia zagrożeń przy minimalnym wykorzystaniu zasobów, w tym jednostek reagujących przydzielanych dynamicznie w razie zagrożenia. Inny wariant Problemu 2.1 pojawia się w sytuacji, gdy niektóre obiekty aktualnej infrastruktury mogą być relokowane do ochrony przed nowymi zagrożeniami.

Projektowanie procesów biznesowych obejmujących zarządzanie zagrożeniami w oparciu o istniejące DSS i infrastrukturę bezpieczeństwa może być dodatkowo wspierane przez modele oparte na BPMN dostosowane do zagadnień bezpieczeństwa [Rodriguez i in., 2007]. Kolejną kwestią jest wprowadzenie najnowocześniejszych metod i narzędzi AI, a następnie ich regularne stosowanie i aktualizowanie w podatnych na zagrożenia częściach IRM DSS.

3 Ewakuacja maszyn i zespołów roboczych w KWC

Metody AI mogą być podstawą do projektowania odpowiedzi zarządczej DSS. Aby poradzić sobie ze złożonymi problemami zarządzania informacją i wiedzą, wykorzystać można przyczynowy model zagrożeń, ryzyka, decyzji zarządzania kryzysowego i ich konsekwencji. Model ten powinien ostatecznie prowadzić do optymalnego rozwiązania problemów

zarządzania ryzykiem i minimalizacji związanych z tym strat. Inteligentny i adaptacyjny DSS zawierający taki model przyczynowy jest w stanie rekomendować zależne od sytuacji działania ograniczające ryzyko, operacje i strategie w celu zapewnienia wysokiego poziomu bezpieczeństwa przemysłowego. Zakłada się, że proponowana implementacja IRM DSS będzie mogła wspierać decyzje na wszystkich istotnych poziomach, od natychmiastowych środków zaradczych do planowania złożonych operacji i długoterminowych strategicznych środków budowania odporności.

Ewakuacja w odkrywkowych zakładach górniczych jakim jest KWC jest kluczowa w obliczu zagrożeń takich jak osuwiska skalne, zalania czy pożary ze względu na specyficzne warunki panujące w tych miejscach oraz ryzyko dla zdrowia i życia pracowników. W sytuacjach awaryjnych, szybka i skuteczna ewakuacja może decydować o minimalizowaniu strat ludzkich i materialnych. Zagrożenia dla życia ludzkiego są szczególnie krytyczne i to te kwestie powinny być eliminowane w pierwszej kolejności. Równie ważne są straty materialne (przekształcające się w finansowe) oraz środowiskowe. Mając to na uwadze, zagadnienie ewakuacji rozpatrywać należy w następujących kategoriach:

1. Ochrona życia i zdrowia pracowników, narażonych na różnorodne zagrożenia, które mogą rozwijać się szybko i niespodziewanie. Ewakuacja pozwala na szybkie opuszczenie strefy zagrożenia i minimalizowanie ryzyka utraty życia lub zdrowia.
2. Szybkość rozwoju zagrożeń wynikająca ze specyfiki prowadzonej działalności.
3. Skomplikowany teren i duża skala z jaką mamy do czynienia w przypadku zakładu górniczego, złożona topografia.
4. Bezpieczeństwo sprzętu i infrastruktury w tym sprzętu ciężkiego, takiego jak koparki, ładowarki czy wozidła technologiczne, które mogą być trudne do szybkiego przemieszczania się w razie nagłego zagrożenia. Ewakuacja sprzętu i pojazdów musi obejmować bezpieczne wyłączenie maszyn z pracy i organizację ruchu na drogach dojazdowych do miejsc bezpiecznych.
5. Zminimalizowanie strat materialnych, na które kluczowy wpływ ma sprawna ewakuacja. Szybka reakcja na zagrożenie poprzez wyłączenie maszyny z prac i skierowanie w miejsca bezpieczne, ewakuacja personelu oraz sprawna koordynacja działań zmniejszają ryzyko uszkodzenia sprzętu i infrastruktury.

Zastosowanie algorytmu NSGA-II w problemie ewakuacji w sytuacji kryzysowej pozwala na znalezienie zestawu rozwiązań, które uwzględniają różne, często sprzeczne kryteria, takie jak czas ewakuacji, bezpieczeństwo trasy i wielkość strat. Algorytm ten daje możliwość wygenerowania wielu planów ewakuacyjnych, a ostateczna decyzja co do wyboru planu pozostaje w gestii decydenta.

Inteligentne systemy wspomagania decyzji w zarządzaniu awariami przemysłowymi mogą być sekwencyjnie stosowane w ramach procedury częściowo nadzorowanego uczenia maszynowego, gdzie wyniki wcześniejszych decyzji służą do informowania o parametrach procedury ograniczania ryzyka i preferencjach kierownictwa. Proces projektowania takiego systemu dla kopalni odkrywkowej pokazuje, że zastosowanie metod AI, takich jak fuzja informacji, uczenie częściowo nadzorowane i wzmacniające oraz techniki rozumienia obrazów, znacznie zwiększa możliwości i efektywność systemu. W rezultacie, zaproponowane tutaj podejście do projektowania DSS może zapewnić realne wdrożenia przemysłowe zdolne do rozwiązywania problemów zarządzania zagrożeniami naturalnymi, jak i antropogenicznymi w czasie rzeczywistym. W ten sposób holistyczny proces analizy wymagań, projektowania i implementacji, wzbogacony o ciągłe włączanie najnowszych metod AI, zapewnia przewagę

nad wcześniejszymi podejściami zajmującymi się tylko pewnym etapem drogi do efektywnych systemów bezpieczeństwa przemysłowego.

4 Projekt architektury informatycznej systemu do zarządzania ryzykiem przemysłowym (IRM DSS)

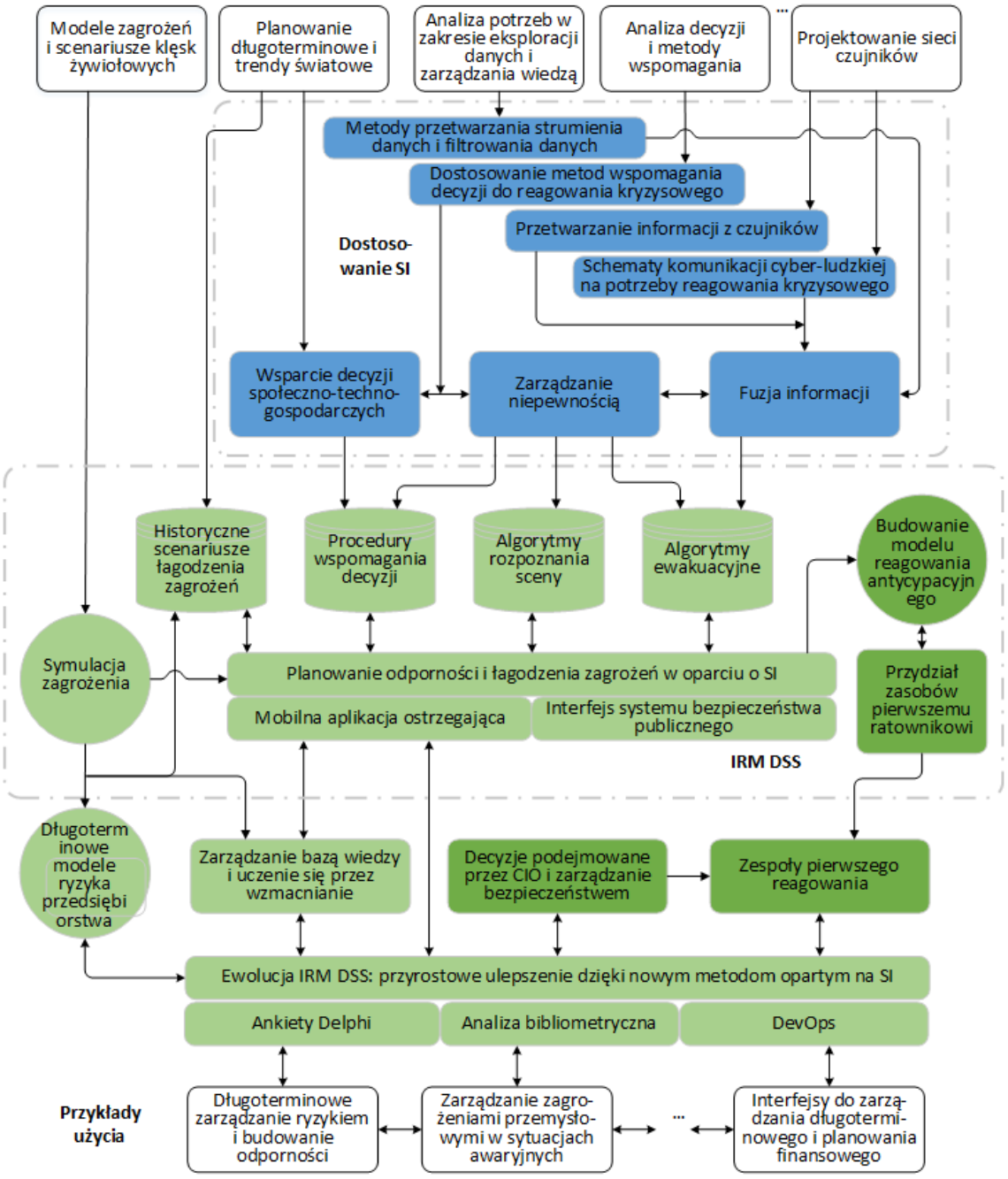
Projekt zakłada połączenie wykorzystywanych obecnie w KWC technik monitoringu wizyjnego oraz nowych rozwiązań, takich jak systemy radarowe wsparte autonomicznymi bezzałogowymi jednostkami latającymi (drony), a w razie potrzeby także naziemnymi robotami inspekcyjnymi. Dodatkowe możliwości, jakie dają nowoczesne systemy radarowe, pozwolą zbudować siatkę wzajemnie wspomagających się punktów radarowych, które pokryją swoim zasięgiem rozległy i trudny do patrolowania teren. Koncepcja uwzględnia możliwość integracji systemu radarowego z system identyfikacji zagrożenia.

Biorąc pod uwagę fakt, że zagrożenia antropogeniczne, np. związane z intruzją występować mogą z różną częstotliwością, jednak w trakcie normalnej pracy zakładu górniczego prawdopodobieństwo ich wystąpienia jest znacznie mniejsze, zasadnym wydaje się szukanie możliwości wykorzystania UAV oraz algorytmów obliczeniowych również do innych zadań, w celu optymalnego i maksymalnego ich wykorzystania. Sposób prowadzonej eksploatacji złoża oraz rodzaj złoża, jakie eksploatuje KWC, generuje ryzyko powstania niebezpiecznych dla bezpieczeństwa ludzi i maszyn zjawisk, jakimi są osunięcia się mas skalnych. Projekt zakłada możliwość wykorzystania dronów do cyklicznej analizy stanu wyrobiska górniczego w celu identyfikacji potencjalnych zagrożeń. Z zadaną częstotliwością lub bezpośrednio na polecenie osoby nadzorującej, dron patrolował będzie linie skrajne poziomów eksploatacyjnych.

Tego typu podejście pozwala stworzyć macierz, w oparciu o którą system informatyczny analizował będzie ciągi przyczynowo skutkowe wskazując w następstwie tego procesu obszary, które należy zabezpieczyć poprzez podjęcie działań prewencyjnych w celu zbudowania stosownej odporności.

4.1 Zagadnienie dopasowania technologicznego metod sztucznej inteligencji stosowanych w IRM DSS

Projekt architektury systemu IRM DSS dla KWC i jego implementacja powinny być dostosowane do najnowocześniejszych rozwiązań SI z uwzględnieniem ich dostępności. W szczególności rozwiązany musi być problem dopasowania AI do ewoluującej Architektury informatycznej IRM DSS przeznaczonej do implementacji. Schemat IRM DSS opartego o powyższe założenia pokazano na diagramie [Rys. 3]. Przykład jednoczesnego zastosowania metod fuzji informacji w postaci map zagrożeń związanych z osuwiskami, zalaniami i obrywaniem się skał oraz przetwarzania informacji wizyjnej i algorytmów decyzyjnych wskazujących optymalne ścieżki ewakuacji (kolejne warstwy diagramu).



Rys. 3. Schemat systemu klasy IRM DSS proponowanego do implementacji i wykorzystania w KWC [wg Skulimowski i Łydek, 2022a].

4.2 Zastosowanie modeli przyczynowych i antycypacyjnych w IRM DSS

Na podstawie przeprowadzonych badań bibliograficznych można stwierdzić, że systemy zarządzania ryzykiem przemysłowym ewoluują w kierunku bardziej zintegrowanych rozwiązań, odchodząc od koncepcji samodzielnych aplikacji. Obserwowane trendy rozwojowe wskazują na istotne zmiany, które zaczynają się już na etapie planowania i projektowania systemów. Kluczowym globalnym kierunkiem jest przejście od systemów dostarczających jedynie dane i wizualizacje na rzecz inteligentnych systemów wspomagania decyzji (DSS) oraz integracja procesów w trybie DevOps.

Potwierdzone w ramach badania Delphi, skoncentrowanego na DSS i IRM DSS, trendy obejmują następujące podejścia:

- Zastosowanie zasad dopasowania AI w połączeniu z DevOps, wdrażanych stopniowo zgodnie z ustalonymi schematami procesowymi.
- Uczenie modeli zagrożeń oraz reguł decyzyjnych do reagowania w sytuacjach kryzysowych za pomocą częściowo nadzorowanego uczenia maszynowego (ML).
- Projektowanie DSS wspieranych przez AI umożliwia tworzenie systemów zdolnych do rozwiązywania różnorodnych problemów związanych z zarządzaniem ryzykiem przemysłowym w czasie rzeczywistym.
- Wdrożenie sieci antycypacyjnych w IRM DSS, co zapewni elastyczne i efektywne zarządzanie działaniami minimalizującymi zagrożenia.

Proponowane rozwiązania wskazują na znaczący potencjał systemów IRM DSS opartych na AI w dostarczaniu narzędzi umożliwiających precyzyjne zarządzanie ryzykiem i szybkie reagowanie na nieprzewidywalne zdarzenia w środowisku przemysłowym.

W zakładach przemysłowych, gdzie istnieje potrzeba zarządzania zagrożeniami naturalnymi, w pierwszej kolejności przy wykorzystaniu możliwości i zasobów zakładu, konieczne jest zapewnienie zarówno odpowiedniego oprzyrządowania sprzętowego, jak i inteligentnych procedur decyzyjnych. Specyfika zagrożeń i ryzyka, które mogą wystąpić w przedsiębiorstwie wdrażającym IRM DSS, wymaga bardziej wnikliwego modelowania ryzyka i reagowania na ryzyko z zastosowaniem odpowiednich działań zapobiegawczych i łagodzących.

Rozwiązanie uwzględniające powyższe założenia, dodatkowo zapewniające decydentom odpowiedzialnym za zarządzanie sytuacjami kryzysowymi, zintegrowanie technologii nadzoru, przetwarzania sygnałów i wspomagania decyzji w całościowy system bezpieczeństwa przemysłowego oparte jest o model sieci antycypacyjnej (AN).

Problem 4.1. Załóżmy, że N wielokryterialnych problemów decyzyjnych O_1 ,…, O_N jest osadzonych w hierarchicznej strukturze raportowania, która tworzy acykliczny połączony digraf z jednym punktem początkowym. Każde O_i, i=1,…,N jest rozwiązywane przez decydenta D_i. Zgodnie z ogólnymi instrukcjami zarządzania kryzysowego D_i wybiera decyzje z zadanego zbioru U_i tak, aby kryteria F_i :=(F_{i1} ,…, $F_{ik(i)}$) zostały zoptymalizowane na U_i oraz dodatkowa informacja o preferencjach P_i dotycząca wyboru decyzji niezdominowanej z U_i była brana pod uwagę. Dodatkowo, wybierając decyzję u_i, decydent Di, który poprzedza D_j w kolejności raportowania, może nałożyć dodatkowe ograniczenia $\psi_{ij}(u_i)$ na decyzje Dj . Gdy przekazanie bezpośredniego polecenia od decydenta D_i do D_j jest niemożliwe, D_i wymaga, by D_j wybrał element zbioru V_{ji} , który – według wiedzy Di – zawiera decyzje korzystne do przebiegu działań nadzwyczajnych. Warunek deontyczny „u_j powinien należeć do V_{ji}" nazywany jest antycypacyjnym sprzężeniem zwrotnym f_{ji} (AF). Należy znaleźć strategię dla wszystkich decydentów D_i, która zaspokoi maksymalną liczbę AF w sieci lub zoptymalizuje inny cel, który zależy od wszystkich AF.

Aby zoptymalizować ilościowe kryteria zarządzania kryzysowego F_i w powyższym Problemie 4.1 zastosowano algorytmy wyprzedzającego podejmowania decyzji wbudowane w AN. Zgodnie z definicją przedstawioną w [Skulimowski, 2014] AN jest skierowanym multigrafem złożonym z acyklicznych podgrafów przyczynowych określonych przez relację przyczynową ψ_{ij} oraz wyprzedzające informacje zwrotne f_{ji} . Ponadto zakłada się, że każda para węzłów (A,B) połączonych AF spełnia implikację:

$$A\, f_{ji}\, B \Rightarrow B\ \Psi\ A, \tag{4.1}$$

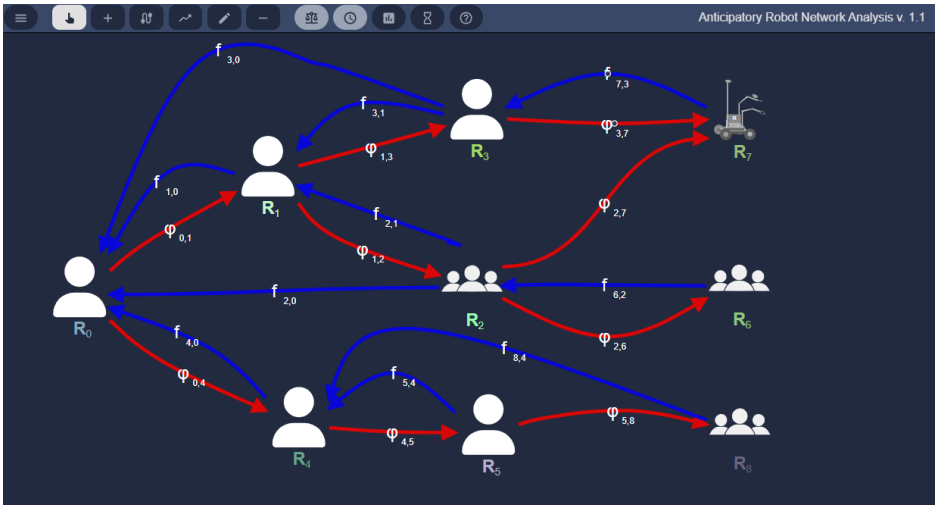
gdzie Ψ jest przechodnim domknięciem relacji ψ_{ja} , tj. $A\ \Psi B$ jeżeli w grafie ψ_{ij} istnieje droga z A do B.

Przykład 4.2. Rysunek [Rys. 4] poniżej przedstawia realistyczną AN odnoszącą się do rozwiązania Problemu 4.1 za pomocą IRM DSS. Ten przypadek problemu wyprzedzającego podejmowanie decyzji z 9 węzłami i 7 AF został rozwiązany za pomocą dedykowanego oprogramowania AN dostępnego na stronie www.anticipatorynetworks.net. Węzły D_i, i=0,1,…,8 odpowiadają decydentom, w tym koordynatorowi zarządzania kryzysowego (menadżer kryzysowy) D_0 oraz zespołom reagowania D_6 , D_7 (oba wewnętrzne) i D_8 (zespół ratowniczy zewnętrzny). Pozostałe węzły w modelu sieci stanowią pośredni poziom zarządzania kryzysowego (D_1 i D_4) oraz zespoły uzupełniające lub rezerwowe (D_2, D_3 i D_5). Wykres przyczynowy (czerwone krawędzie z adnotacją ψ_{ij}) modeluje relację raportowania i polecenia wydawane przez decydentów. Oznaczenie $D_i \psi_{ij} D_j$, jako krawędź od D_i do D_j, jest równoważne z definicją przez D_i dodatkowych ograniczeń dotyczących decyzji, które D_j może podjąć później. Jest to oznaczone jako:

$$\psi_{ij}(u_{j,,k})=\{u_{j,p1},\ldots,u_{j,p(k)}\}\subset U_j, \tag{4.2}$$

gdzie $u_{i,k}$ jest decyzją wybraną przez D_i ze zbioru U_i , a U_j jest zbiorem wszystkich dopuszczalnych decyzji D_j. Dla ekip ratowniczych elementy U_i odpowiadają rzeczywistym działaniom łagodzącym zagrożenie na zagrożonych obiektach $Z_1,\ldots Z_m$, np. „idź do Z_k", „idź do połowy drogi do Z_k ", przez pewien $1\le k\le m$, „kontynuuj akcję do zakończenia ewakuacji", „wycofaj się" itp. Relacja ψ definiuje zatem hierarchię problemów decyzyjnych, w której decyzje $u_{i,k}$ podjęte na wyższym szczeblu wpływają na decydentów D_{j1} ,…, D_{jm} na niższym szczeblu, pod warunkiem, że D_i jest połączone przez ψ_{ijk} z D_{jk}. Jednoznacznym poleceniom odpowiada $p(k)$=1, ale jest to sytuacja wyjątkowa, gdyż główną ideą stojącą za strukturą podejmowania decyzji wyprzedzających jest zapewnienie podległym decydentom pewnego poziomu swobody w nieoczekiwanych okolicznościach. Swoboda ta przekazywana jest jednostkom niższego szczebla, zespołom ratowniczym a nawet autonomicznym robotom wykonawczym.

Drugi podgraf (niebieskie krawędzie z adnotacją f_{ji}) modeluje AF, w szczególności każde f_{ji} definiuje zbiór $V_{ji}\subset U_j$ zawierający decyzje, o które zabiegał (które preferował) D_i. Zestawy V_{ji} zawierają zazwyczaj działania, które nie są obowiązkowe dla D_j, niemniej jednak mogą być korzystne dla całości działań ratowniczych, np. V_{ji} można zdefiniować jako {„*kontynuuj gaszenie pożaru"*, „*powstrzymaj się od wycofania, nawet jeśli jest to dozwolone"*}. V_{ji} rzadko pokrywa się z którymkolwiek z ograniczeń ψ_{ij} ($u_{i,k}$), więc D_i stara się wybrać taką decyzję, która uczyni D_j wybór elementu V_{ji} najbardziej prawdopodobnym.



Rys. 4. Sieć antycypacyjna stosowana do projektowania procedur decyzyjnych w IRM DSS, utworzona za pomocą narzędzi www.anticipatorynetworks.net.

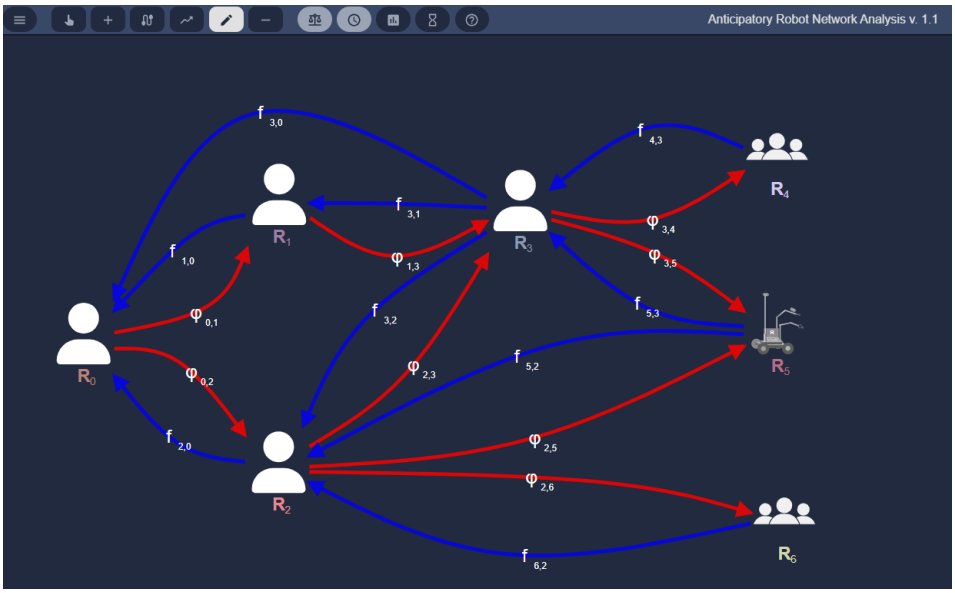
Zakładając, że D_j działa w sposób racjonalny, czyli wybiera decyzje niezdominowane maksymalizujące funkcję użyteczności ξ_j, aby znaleźć najlepszą decyzję w U_i wystarczy, że decydent D_i będzie w stanie przewidzieć funkcję użyteczności D_j. Mianowicie D_i powinien maksymalizować prawdopodobieństwo warunkowe, że D_j wybierze decyzję ze zbioru V_{ji} . Jest to równoznaczne z maksymalizacją w U_i funkcji ilorazu (4.3):

$$q(u_{i,k}):=\mu(V_{ji} \cap \text{argmax}\{\xi_{jot}(v):v\in \psi_{ij}(u_{i,k})\})/\mu(\psi_{ij}(u_{i,k})\}, \tag{4.3}$$

gdzie $\mu(Y)$ jest probabilistyczną miarą zbioru $Y\subset U_j$, a $\text{argmax}\{\xi(v):v\in X\}$ oznacza podzbiór X, w którym wartości funkcji ξ są maksymalne w X. Zgodnie z założeniem racjonalności, jeśli zbiór U_j jest skończony, można przyjąć, że $\mu(Y)$ jest licznością Y podzieloną przez liczność U_j.

Problem 4.1 jest w istocie wielopoziomowym zadaniem optymalizacji wielokryterialnej [Pfetsch, Schmitt, 2023; Zewde, Kassa, 2021], w którym dodatkowe ograniczenia w zadaniu $(U_j,F_j)\rightarrow$min są nałożone przez D_i poprzedzające D_j w porządku przyczynowym ψ. Zasada projektowania IRM DSS leżąca u podstaw modelowania antycypacyjnego polega na zaprojektowaniu struktury poleceń $\psi_{i,j}$ tak, aby AF f_{ji} zostały zaspokojone w maksymalnym możliwym stopniu, na przykład przez jak największą ich liczbę lub jako sumę dodatnich wag dla każdego zaspokojonego AF i kar ujemnych dla wszystkich niezaspokojonych AF. Dzięki wybranej metodzie rozwiązania można wtedy znaleźć optymalną sekwencję decyzji na każdym poziomie.

Zaprezentowana na Rys. 4 i omówiona symulacja dała rozwiązanie w postaci wskazania najlepszych ścieżek decyzyjnych realizowanych przez kolejnych agentów, można jednak założyć, że sam problem nie został rozwiązany w sposób satysfakcjonujący i konieczna jest eskalacja problemu. W praktyce można to sprowadzić do sytuacji, że pomimo podjęcia szeregu akcji z wykorzystaniem dostępnych zasobów ludzkich i sprzętowych, pożar który był przyczyną podjęcia działań ratowniczych, nie został opanowany przez robota gaśniczego (agent R_7) i niezbędne jest zaangażowanie dodatkowych sił w drodze eskalacji działań. Do rozwiązania drugiego etapu problemu przygotowany został zmodyfikowany schemat sieci antycypacyjnej, w którym główny nacisk położony jest na maksymalizację efektywności działań jednostek wykonawczych (agentów) D_5 i D_6 oraz zwiększenie udziału w koordynacji działań i decyzyjności agenta D_2 [Rys. 5].



Rys. 5. Drugi etap symulacji wykorzystania sieci antycypacyjnej.

5 Implementacja systemu zarządzania ewakuacją

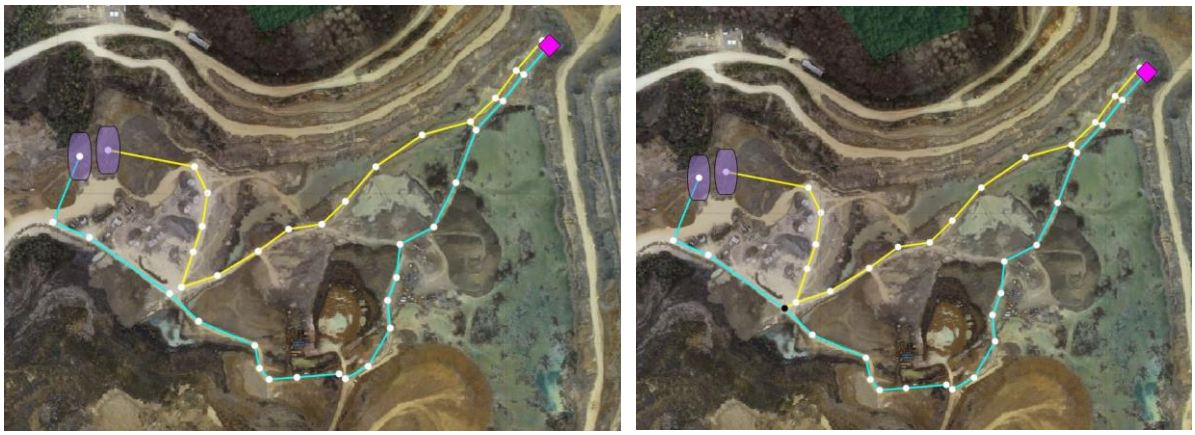
5.1 Symulacja ewakuacji

Interfejs przygotowany dedykowany do rozwiązania problemu ewakuacji omówionego wcześniej powstał przy użyciu środowiska Matlab. W celu lepszego zrozumienia omawianych zagadnień przygotowany został scenariusz bazujący na danych rzeczywistych i sytuacji prawdopodobnej do zaistnienia w odkrywkowym zakładzie górniczym. Scenariusz zakłada materializację ryzyka osunięcia mas skalnych i konieczność ewakuacji wozideł technologicznych i koparki, do wyznaczonych stref bezpiecznych. Dodatkowo część dróg technologicznych zostaje wyłączona z użytkowania z powodu osuwisk, komplikując tym samym cały proces ewakuacji. Aby przeprowadzić ewakuację należy wyznaczyć trasy dla każdego z pojazdów, uwzględniając odległości do miejsc bezpiecznych, przepustowość dróg, prędkości przemieszczania się, występujące na drogach przeszkody.

Poprawnie przygotowana mapa, jest materiałem wyjściowym do rozpoczęcia procesu symulacji ewakuacji pojazdów z miejsc zagrożonych do miejsc zdefiniowanych jako miejsca bezpieczne. Warunki minimalne, jakie muszą zostać spełnione, aby symulacja mogła zostać rozpoczęta to:

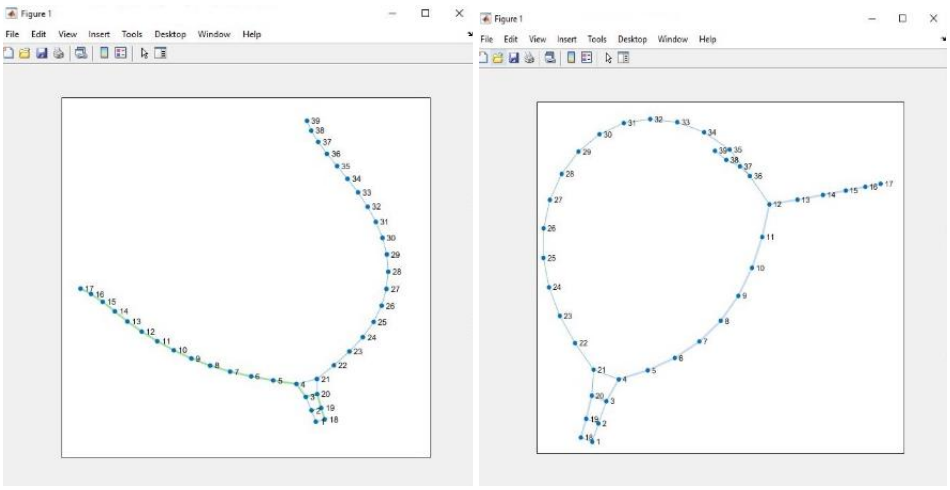
- wskazanie na mapie miejsc bezpiecznych,
- naniesienie możliwych do wyboru tras ewakuacji,
- wskazanie ewakuowanych pojazdów połączonych z przynajmniej jedną trasą.

Przykład symulacji ewakuacji do miejsca bezpiecznego pokazano na kolejnych rysunkach [Rys. 6] (różne punkty wspólne tras).



Rys. 6. Symulacja ewakuacji, warianty: jeden punkt wspólny trasy i dwa punkty wspólne.

Graficzne odwzorowanie wyników symulacji przedstawia Rys. 7.



Rys. 7. Wyniki symulacji dla wariantu pierwszego (rysunek z lewej strony) i drugiego (rysunek z prawej strony).

Po ustawieniu parametrów inicjujących rozpocząć można procedurę symulacyjną, w trakcie której aplikacja informuje operatora o:

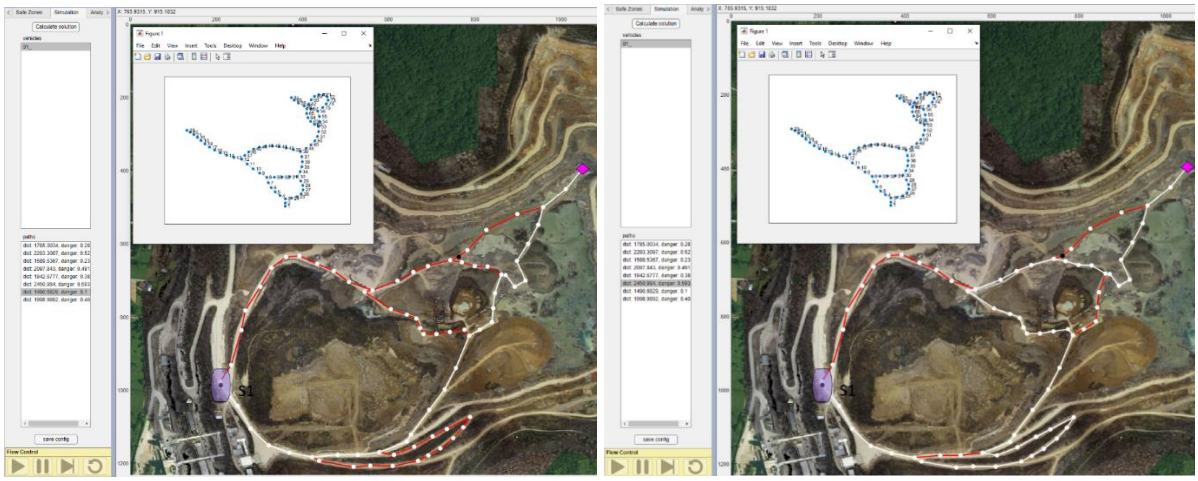
- całkowitym czasie trwania procesu ewakuacji,
- procentowe uszkodzenia poszczególnych pojazdów,
- oczekiwanym czasie dotarcia do miejsca bezpiecznego oraz o czasie faktycznym po dotarciu do tego miejsca,
- przejechanej długości trasy, dla każdego pojazdu.

Alternatywny sposób prowadzenia symulacji (Wariant 2) opiera się na założeniu, że operator tworzy jedną trasę, z kilkom rozgałęzieniami (alternatywnymi drogami), prowadzącymi do wskazanego miejsca bezpiecznego. Model ten został zaprezentowany na rysunkach [Rys. 8, Rys. 9]. Jak widać na rysunku [Rys. 10] pojazd znajdujący się w fazie początkowej bezpośrednio przy ścianie wyrobiska, na najniższym poziomie eksploatacyjnym (poziom 310) musi zostać ewakuowany do miejsca bezpiecznego (poziom 330). Po wyznaczeniu dostępnych odcinków tras możliwy jest wybór 8 wariantów drogi ewakuacji, o różnych długościach i z różnymi współczynnikami zagrożenia. Do celów symulacyjnych wybrane odcinki trasy oznaczone zostały współczynnikami uszkodzeń. Obliczone możliwe trasy mają różne długości, od 1490 metrów trasa najkrótsza, do 2450 metrów trasa najdłuższa i różne współczynniki zagrożenia, od 10% do 59% [Tab. 1].

Tab. 1. Wyniki symulacji dla Wariantu 2

Trasa	Dystans [m]	Zagrożenie [%]
T1	1785,00	28
T2	2293,31	52
T3	1589,54	23
T4	2097,84	49
T5	1942,68	38
T6	2450,98	59
T7	1490,69	10
T8	1998,99	40

Proponowana najkrótsza trasa, oznaczona kolorem białym, wraz z grafem punktów kontrolnych trasy zaprezentowana została na Rys. 8, natomiast na Rys. 9, w analogiczny sposób zaprezentowana została trasa najdłuższa.



Rys. 8. Najkrótsza trasa ewakuacji (1490 metrów). Rys. 9. Najdłuższa trasa ewakuacji (2450 metrów).

Aplikacja posiada również funkcjonalność umożliwiającą śledzenie ruchu pojazdu w trakcie symulowanego procesu ewakuacji, z opcją zatrzymania pojazdu w dowolnym momencie i wznowienia symulacji. Rys. 10 przedstawia interfejs aplikacji w trakcie symulowanego ruchu pojazdu po wybranej przez operatora trasie. Pojazd oznaczony rombem znajduje się już za połową trasy i kieruje się po wybranym wariancie trasy do miejsca ewakuacji (miejsca bezpiecznego S_1.

Rys. 10. Widok interfejsu aplikacji w trakcie symulacji ruchu ewakuowanego pojazdu.

Tab. 2. Wyniki symulacji ewakuacji 3 pojazdów.

	Czas przejazdu [s]	Długość trasy [m]	Poziom zagrożeń [%]	Minimalny czas ewakuacji [s]	Maksymalny czas ewakuacji [s]	Średni czas ewakuacji [s]
Maszyna_1 Trasa_1	73,98	1 379,01	15,30	73,98	86,86	79,16
Maszyna_1 Trasa_2	76,65	1 428,79	43,81			
Maszyna_1 Trasa_3	86,86	1 619,03	63,28			
Maszyna_2 Trasa_1	46,25	862,18	5,98	46,12	66,35	52,91
Maszyna_2 Trasa_2	46,12	859,76	15,86			
Maszyna_2 Trasa_3	66,35	1 236,70	61,54			

Maszyna_3 Trasa_1	67,62	1 260,36	12,78	50,46	67,62	56,71
Maszyna_3 Trasa_2	50,46	940,59	18,99			
Maszyna_3 Trasa_3	52,04	970,08	53,01			

Symulacja ewakuacji 3 maszyn (wodzideł technologicznych: M1, M2 i M3) z obszarów zagrożonych, do jednego, wyznaczonego miejsca bezpiecznego (S1) przedstawiono na [Rys. 11]. Wyniki symulacji prezentuje [Tab. 2]. Na czas ewakuacji i poziom zagrożeń wpływają łączne długości odcinków tras oraz przypisane poszczególnym odcinkom wartości zagrożeń wynikające z sytuacji zagrożenia, która jest bezpośrednim powodem ewakuacji.

Rys. 11. Widok rozmieszczenia ewakuowanych pojazdów i miejsca bezpiecznego.

6 Scenariusze zastosowania IRM DSS w KWC

Bezpieczeństwo w odkrywkowym zakładzie górniczym, jakim jest KWC, jest jednym z kluczowych aspektów, które muszą być uwzględniane na każdym etapie działalności. W obliczu rosnących wymagań związanych z bezpieczeństwem, ochroną zdrowia i środowiska, a także dynamicznego rozwoju technologii, wprowadzenie zaawansowanego, holistycznego systemu zarządzania bezpieczeństwem staje się koniecznością i naturalnym kierunkiem rozwoju przedsiębiorstwa. Głównym założeniem funkcjonowania takiego systemu jest integracja nowoczesnych technologii, takich jak sztuczna inteligencja (AI), Internet Rzeczy (IoT), analiza danych w czasie rzeczywistym oraz zaawansowane systemy monitorowania i alarmowania, aby zapewnić możliwie skuteczne i szybkie reagowanie na zagrożenia. Poniżej przedstawione zostały przykładowe scenariusze zastosowania systemu, uwzględniając konkretne technologie oraz ich zastosowanie:

- Jednym z najważniejszych zagrożeń w obrębie część czynnej odkrywkowego zakładu górniczego są dynamiczne zmiany w środowisku pracy, takie jak osuwiska skalne,

podtopienia oraz niekontrolowane przemieszczanie się mas skalnych (Scenariusz 1). IRM DSS powinien zapewniać sprawne alarmowanie w sytuacjach zakwalifikowanych do kategorii stanowiących zagrożenie i umożliwiać zarządzanie ewakuacją.

- Kolejnym aspektem, który powinien być analizowany i wspierany przez IRM DSS jest zapewnienie bezpieczeństwa technicznego maszyn i infrastruktury pomocniczej w przypadku wystąpienia zagrożeń (Scenariusz 2). Zadziałanie systemów automatycznych może szybko zneutralizować zagrożenie bez konieczności interwencji człowieka i dalszej eskalacji działań. W przypadku eskalacji zagrożenia kolejnym elementem jest uruchomienie maszyn autonomicznych lub półautonomicznych, które w przypadku wykrycia zagrożenia automatycznie podejmują zdefiniowane dla nich czynności.
- Jednym z kluczowych elementów zaawansowanego systemu bezpieczeństwa jest centralna platforma do zarządzania ryzykiem (Scenariusz 3). Taki system powinien integrować wszystkie dane z różnych źródeł (sensory, kamery, systemy monitorowania maszyn, informacje pogodowe, zgłoszenia osób odpowiedzialnych za dozór), na ich podstawie oceniać poziom ryzyka w różnych obszarach zakładu i proponować podjęcie działań optymalnych dla konkretnej sytuacji. Dzięki wykorzystaniu analiz historycznych, w tym w szczególności danych dotyczących wypadków i zdarzeń niebezpiecznych, a także posiadanych prognoz możliwych eskalacji ryzyka, w korelacji z aktualnymi warunkami środowiskowymi, system sugeruje działania prewencyjne.
- Równie istotne co omawiane scenariusze bazujące się na działaniu systemów i zabezpieczeń technicznych (sensory itp.) są kwestie związane z ochroną fizyczną (Scenariusz 4). Zapewnienie ochrony fizycznej, zarówno infrastruktury jak i pracowników rzutuje również na wcześniejsze scenariusze, biorąc pod uwagę fakt, że intruzja może być połączona z dodatkowymi działaniami, np. o charakterze sabotażowym.

Analizując zaproponowane scenariusze możliwości zaawansowanego systemu zarządzania bezpieczeństwem technicznym i fizycznym znacząco zwiększa poziom ochrony zarówno pracowników, jak i infrastruktury. Integracja nowoczesnych technologii, takich jak AI, IoT, automatyzacja maszyn oraz systemy monitorowania i analizy danych w czasie rzeczywistym, pozwoli na szybsze wykrywanie zagrożeń, skuteczniejsze reagowanie w sytuacjach kryzysowych oraz minimalizowanie ryzyka wypadków. Dzięki temu zakład produkcyjny może funkcjonować nie tylko efektywnie, ale przede wszystkim bezpiecznie.

6.1 Dalsze kierunki rozwoju systemów bezpieczeństwa w KWC

Ciągły rozwój i doskonalenia systemów bezpieczeństwa w zakładach przemysłowych jest niezbędny w obliczu rosnących wyzwań związanych z bezpieczeństwem, ochroną środowiska oraz skutecznością i ciągłością działania systemów produkcyjnych. Prognozowane kierunki rozwoju zaawansowanych systemów zarządzania bezpieczeństwem i wsparcia podejmowania decyzji w zakładach przemysłowych będą konsekwencją:

1. Rozwoju sztucznej inteligencji i uczenia maszynowego (ML).

Jednym z najbardziej pożądanych kierunków rozwoju jest coraz większa integracja systemów zarządzania bezpieczeństwem z zaawansowanymi algorytmami sztucznej inteligencji oraz uczenia maszynowego. Dzięki wsparciu działania systemów klasy IRM DSS przez AI coraz bardziej efektywne będzie:

- prognozowanie zagrożeń, dzięki wykorzystaniu analizy danych historycznych i bieżących, systemy zdolne będą do predykcji potencjalnych zagrożeń z większą dokładnością.

- autonomiczne podejmowanie decyzji, które w sytuacjach kryzysowych umożliwi AI przejąć funkcję decyzyjną, minimalizując czas reakcji na zagrożenia poprzez wyeliminowanie czynnika ludzkiego.
- adaptacyjność systemu bezpieczeństwa, wspartego przez algorytmy uczenia maszynowego do zmieniających się warunków pracy w zakładzie przemysłowym, co pozwoli na dynamiczne i predykcyjne zarządzanie ryzykiem.

Wprowadzenie AI do zarządzania bezpieczeństwem pozwoli na jeszcze skuteczniejsze zarządzanie ryzykiem i szybsze reagowanie na pojawiające się zagrożenia, co w rezultacie zmniejszy liczbę wypadków w zakładach górniczych.

2. Rozwoju systemów Internetu Rzeczy (IoT).

Internet Rzeczy (IoT) to technologia, która obecnie rozwija się bardzo dynamicznie i zyskuje na popularności w wielu branżach, w tym w górnictwie. W najbliższych latach rozwój systemów IoT w kontekście zarządzania bezpieczeństwem wpłynie na:

- ciągłą rozbudowę sieci czujników, w możemy spodziewać się większej liczby czujników IoT monitorujących różnorodne parametry związane z bezpieczeństwem, takie jak wibracje, wilgotność, temperatura, stężenie gazów oraz wielu innych parametrów pracy maszyn i urządzeń.
- integracji urządzeń osobistych, w które wyposażeni będą pracownicy również w zakresie inteligentnych ubrań lub innych urządzeń noszone (wearables), które będą monitorować warunki środowiskowe oraz parametry życiowe.
- zintegrowane zarządzanie produkcją i zużyciem energii przyczyni się do optymalizacji działania maszyn na podstawie bieżących potrzeb, a poprzez zabudowane na maszynach panele fotowoltaiczne poprawi efektywność operacyjną, co przełoży się pośrednio na zwiększenie bezpieczeństwa.

Systemy IoT dzięki możliwości ich olbrzymiego rozproszenia umożliwią stałe monitorowanie i kontrolę nad przedsiębiorstwem, co będzie jednym z kluczowych elementów dla zapobiegania katastrofom oraz minimalizowania ryzyka związanego z nieprzewidywalnymi warunkami pracy.

3. Upowszechnienia autonomicznych systemów robotycznych.

Kolejnym ważnym kierunkiem rozwoju jest automatyzacja i robotyzacja operacji wykonywanych obecnie przez personel ludzki. Autonomiczne systemy robotyczne odegrają kluczową rolę w przyszłości zakładów, w których wykonywane są prace niebezpieczne lub o podwyższonym ryzyku, co w sposób istotny wpłynie na zagadnienia związane z bezpieczeństwem i zarządzaniem w sytuacjach kryzysowych:

- naziemne roboty inspekcyjne oraz autonomiczne drony monitorować będą obszary trudno dostępne lub niebezpieczne dla pracowników.
- autonomiczne maszyny górnicze, takie jak koparki, ładowarki, wiertnice czy nawet wozidła, które pracować będą autonomicznie, eliminując potrzebę obecności człowieka w niebezpiecznych strefach.
- systemy autonomicznej ewakuacji w postaci autonomicznych pojazdów ewakuacyjnych, które będą transportować pracowników w bezpieczne miejsce w przypadku wykrycia zagrożenia.

Automatyzacja i robotyzacja procesów przemysłowych zwiększy zarówno wydajność pracy, jak i poziom bezpieczeństwa pracowników, eliminując ryzyko związane z obecnością

człowieka w niebezpiecznych strefach zakładu oraz podatność człowieka na wpływ czynników zewnętrznych.

4. Zwiększenia poziomu cyberbezpieczeństwa w systemach zarządzania.

Wraz z rosnącym poziomem cyfryzacji zakładów przemysłowych wzrasta nowy rodzaj zagrożeń – zagrożenia cybernetyczne. Systemy zarządzania bezpieczeństwem technicznym i fizycznym będą uwzględniać ochronę przed atakami cybernetycznymi z wielu środowisk. Kierunki rozwoju w tym obszarze obejmą:

- zabezpieczanie infrastruktury IT i OT, poprzez skuteczną ochronę przed atakami hakerskimi, które mogłyby zakłócić działanie krytycznych systemów monitorujących i decyzyjnych. Wykorzystanie technologii blockchain mogłoby zapewnić integralność danych oraz zabezpieczy sieci przed nieautoryzowanym dostępem.
- autonomiczne podsystemy obrony, będące integralnym elementem systemów bezpieczeństwa będą autonomicznie reagować na zagrożenia cybernetyczne.

Cyberbezpieczeństwo stanie się integralną częścią holistycznych systemów zarządzania bezpieczeństwem technicznym i fizycznym, co pozwoli na minimalizowanie ryzyka związanego z cyfryzacją i automatyzacją procesów w zakładach przemysłowych.

5. Inteligentnego zarządzania danymi i analizą predykcyjną.

Wraz ze wzrostem ilości danych generowanych przez systemy bezpieczeństwa kluczową rolę odegra rozwój technologii analitycznych oraz systemów big data, konsekwencją tego będzie:

- rozwój zaawansowanych narzędzi analitycznych, które będą w stanie przetwarzać ogromne ilości informacji generowanych przez czujniki IoT i inne systemy.
- rozwój systemów rekomendacyjnych, które na podstawie zebranych danych i analiz predykcyjnych będą proponować najlepsze decyzje oraz zalecać konkretne działania, w tym działania prewencyjne, takie jak optymalizacja tras transportu, niezbędne przerwy w pracy maszyn itp.

6. Integracja zarządzania bezpieczeństwem i współpraca w oparciu o rozwiązania chmurowe.

Wzrost roli i istotności rozwiązań opartych na technologii chmury obliczeniowej (*cloud computing*) umożliwi efektywniejszą współpracę i zarządzanie danymi w czasie rzeczywistym. Chmura zapewni nieograniczony dostęp do zasobów (również obliczeniowych) i pozwali na przechowywanie oraz analizę dużych ilości danych. W kontekście systemów bezpieczeństwa w zakładach przemysłowych obejmie to:

- zintegrowane platformy bezpieczeństwa pracujące w jednym ekosystemie opartym na chmurze, umożliwiają centralny dostęp do danych z wielu różnych źródeł, takich jak sensory, kamery, czy systemy zarządzania maszynami co będzie kluczowe w koordynacji działań, zwłaszcza w sytuacjach awaryjnych.
- możliwość współpracy w zakresie wymiany dozwolonych danych pomiędzy zakładami przedsiębiorstwami o podobnym profilu działalności w skali globalnej. Wdrożenie nowych, innowacyjnych technik zarządzania ryzykiem w jednym z przedsiębiorstw pozwoli wykorzystać informacje i doświadczenie innym zakładom dzięki wymianie informacji.

7. Zwiększenie autonomii systemów decyzyjnych.

Naturalnym kierunkiem rozwoju systemów klasy IRM DSS będzie wzrost autonomii tych systemów. Obecnie wiele procesów wymaga interwencji człowieka, należy jednak oczekiwać, że algorytmy będą coraz bardziej niezależne, co pozwoli na:

- automatyczne podejmowanie decyzji w sytuacjach kryzysowych, w szczególności dotyczących ewakuacji, zatrzymania i wycofania z ruchy maszyn czy zabezpieczenia terenu w przypadku wykrycia zagrożenia.
- optymalizację procedur i algorytmów odpowiedzialnych za bezpieczeństwo w celu ich dynamicznego dostosowywania się do zmieniających się procedur bezpieczeństwa, które z kolei zmieniać się będą wraz ze zmianą warunków pracy.
- decentralizację procesów zarządzania w przypadku rozproszonej infrastruktury, lokalne systemy będą mogły podejmować decyzje natychmiastowo, bez potrzeby komunikacji z centralnym serwerem, co jest szczególnie ważne w przypadku awarii sieci czy problemów technicznych.

8. Zapewnienie zrównoważony rozwoju i ochrony środowiska.

Rosnąca świadomość ekologiczna oraz zaostrzenie regulacji dotyczących ochrony środowiska w przemyśle wymusi rozwój systemów zarządzania bezpieczeństwem w kierunku zrównoważonego rozwoju. Wymusi to stosowanie rozwiań integrujących technologie, które:

- minimalizują wpływ prowadzonej działalności na środowisko, poprzez ciągłe monitorowanie otoczenia, aby wykrywać nie tylko zagrożenia dla pracowników, ale także negatywne skutki działalności zakładu dla ekosystemu, takie jak zanieczyszczenie wód, emisja gazów czy erozja gleby.
- optymalizują zużycie zasobów naturalnych poprzez automatyczne usprawnienie procesów produkcyjnych i operacyjnych. Inteligentne zarządzanie energią, zużyciem wody oraz emisją spalin stanie się jednym z kluczowych elementów rozwoju i doskonalenia tych systemów. Ważny elementem będzie również gospodarka obiegu zamkniętego połączona z zaawansowanym recyklingiem.

Zaawansowane systemy zarządzania bezpieczeństwem będą rozwijać się w kilku kluczowych, wskazanych powyżej kierunkach. Integracja AI i ML, rozwój Internetu Rzeczy (IoT), autonomicznych systemów robotycznych, a także zwiększenie autonomii decyzyjnej i ochrona przed zagrożeniami cybernetycznymi będą stanowić podstawę przyszłych holistycznych systemów bezpieczeństwa. Wraz z postępem technologicznym, systemy te staną się coraz bardziej zaawansowane i skuteczne, co pozwoli na minimalizację ryzyka, ochronę pracowników i środowiska, a także optymalizację nadzorowanych przez nie procesów operacyjnych.

7 Wnioski końcowe

Zakładając, że w najbliższych latach podstawowe technologie produkcji nie ulegną większym zmianom, najważniejszym celem strategii technologicznej KWC jest poprawa stanu bezpieczeństwa w zakładzie poprzez zastosowanie technologii informacyjno-komunikacyjnych, w tym zwłaszcza wspomaganych przez algorytmy sztucznej inteligencji. Rozprawa *„System wspomagania decyzji w projektowaniu i wdrażaniu przemysłowych systemów bezpieczeństwa wykorzystujących techniki sztucznej inteligencji”* przedstawia założenia oraz potencjalne możliwości wdrożenia systemu klasy IRM DSS. System stanowi innowacyjne narzędzie wspierające procesy decyzyjne w zakresie zarządzania ryzykiem przemysłowym, szczególnie w sektorze górnictwa odkrywkowego. Postawiona teza badawcza, która zakłada, że odporność zakładów przemysłowych na różnorodne zagrożenia można zwiększyć dzięki zastosowaniu nowoczesnych metod analizy ryzyka wspieranych sztuczną inteligencją, została potwierdzona. Wyniki przeprowadzonych badań podkreślają

znaczenie integracji technologii AI, analizy wielokryterialnej oraz holistycznego podejścia dla skutecznego zarządzania bezpieczeństwem w przedsiębiorstwach przemysłowych.

Sztuczna inteligencja (AI) odgrywa centralną rolę w konstrukcji i funkcjonowaniu proponowanego systemu, dostarczając zaawansowane narzędzia analityczne i predykcyjne. System zapewnia kompleksowe wsparcie decyzyjne w czasie rzeczywistym. Jednym z jego kluczowych elementów są sieci antycypacyjne, które umożliwiają modelowanie i predykcję potencjalnych zdarzeń zagrażających lub zakłócających stan określony jako stan bezpieczny. W oparciu o sieci AN prowadzona jest analiza dostępnych scenariuszy materializacji ryzyka, uwzględniając wzajemne zależności oraz możliwą propagację skutków w rozbudowanych systemach produkcyjnych. Na podstawie danych historycznych, bieżących oraz symulacji możliwych zdarzeń, sieci antycypacyjne generują prognozy, które pomagają zapobieganiu sytuacjom kryzysowym poprzez proponowanie decyzji racjonalnych z punktu widzenia uczestników procesu (decydentów).

Drugim kluczowym elementem systemu są grafy reprezentacji wiedzy, które strukturalizują dane dotyczące procesów przemysłowych, infrastruktury oraz czynników ryzyka. Grafy pozwalają na precyzyjne mapowanie relacji między różnymi elementami systemu, co jest szczególnie istotne w środowiskach o wysokim poziomie złożoności, takich jak zakłady górnicze. Dzięki takiemu połączeniu grafy wiedzy wspierają organizację dostarczając informacji o systemie (procesie), natomiast sieć antycypacyjna używa tej wiedzy w celu przeprowadzenia symulacji i przewidywania, jak zmiany poszczególnych węzłach wpływają na pozostałe elementy i wynik końcowy symulacji.

Integralnym elementem IRM DSS jest zastosowanie analizy wielokryterialnej, która umożliwia podejmowanie decyzji w warunkach złożoności i niepewności. Analiza ta wykorzystuje sieci antycypacyjne i grafy wiedzy do oceny ryzyk w wielu wymiarach, takich jak bezpieczeństwo pracowników, ochrona środowiska, ciągłość procesów technologicznych czy aspekty finansowe. Dzięki temu system dostarcza wieloaspektowych rekomendacji, które pozwalają na optymalizację działań prewencyjnych i reaktywnych. Sam proces analizy wielokryterialnej obejmuje zbieranie danych z różnych źródeł, w tym systemów ERP, SCADA oraz różnego rodzaju sensorów, również środowiskowych, a następnie ich integrację i analizę za pomocą algorytmów sztucznej inteligencji. Algorytmy te uwzględniają zależności między kryteriami, priorytety strategiczne organizacji oraz potencjalne kompromisy między różnymi celami. Dzięki temu system może wskazać optymalne (kompromisowe) działania w sytuacji, gdy zachodzi konflikt między kosztami operacyjnymi a wymaganiami bezpieczeństwa.

Jednym z najważniejszych wniosków wynikających z prowadzonych analiz i badań jest znaczenie holistycznego podejścia do zarządzania bezpieczeństwem w zakładach przemysłowych. Proponowany system klasy IRM DSS integruje dane, procesy oraz technologie, tworząc jednolity ekosystem, który umożliwia kompleksowe monitorowanie, analizę i reagowanie na zagrożenia. Holistyczny charakter systemu pozwala na efektywne wykorzystanie zasobów przedsiębiorstwa, eliminację redundancji w procesach zarządzania ryzykiem oraz zwiększenie odporności organizacji na zagrożenia zewnętrzne i wewnętrzne. W kontekście górnictwa odkrywkowego, holistyczne podejście oznacza uwzględnienie specyfiki procesów wydobywczych i technologicznych, takich jak urabianie, transport czy magazynowanie surowców, a także specyficznych ryzyk związanych z bezpieczeństwem pracowników, ochroną środowiska oraz infrastrukturą technologiczną. Integracja danych z różnych dostępnych w przedsiębiorstwie systemów informatycznych umożliwia pełne zrozumienie sytuacji w czasie rzeczywistym i podejmowanie decyzji opartych na wszechstronnej analizie danych.

Wdrożenie w przedsiębiorstwie systemu opartego o omówione założenia przyniesie w praktyce korzyści poprzez zwiększenie poziomu bezpieczeństwa dzięki zdolności do

wczesnego wykrywania zagrożeń i przewidywania ich skutków system oraz zredukuje ryzyko wypadków, przestojów a także strat finansowych. Poprawa efektywności operacyjnej zrealizowana poprzez holistyczne podejście do zarządzania ryzykiem umożliwi lepsze wykorzystanie dostępnych zasobów organizacji oraz optymalizację procesów produkcyjnych, co wpłynie wprost na redukcję kosztów. Podejście holistyczne zapewnia również integrację i automatyzację działań systemu oraz minimalizuje koszty związane z reakcją na zagrożenia. Należy też zwrócić uwagę na aspekt ludzki, realizowany poprzez podniesienie świadomości ryzyka, na drodze dostarczania kadrze zarządzającej kompleksowych informacji, które pozwalają na lepsze zrozumienie i zarządzanie procesami i ryzykiem na wszystkich poziomach organizacji.

W wymiarze teoretycznym rozprawa wnosi wkład w rozwój nauki o metodach wspomagania decyzji w sytuacji zagrożenia oraz zarządzaniu ryzykiem, wskazując na możliwości zastosowania sztucznej inteligencji w kontekście złożonych procesów przemysłowych. Przedstawiona koncepcja IRM DSS może być z powodzeniem adaptowana do innych sektorów przemysłowych, takich jak energetyka, logistyka czy chemia, co otwiera nowe perspektywy dla badań i wdrożeń.

Rozprawa zawiera istotne innowacje i osiągnięcia, które dotyczą zarówno teoretycznych, jak i praktycznych aspektów projektowania systemów klasy IRM DSS. Przyczyniając się do bardziej efektywnego zastosowania tych systemów w zarządzaniu ryzykiem w środowiskach przemysłowych. Syntetyczne podsumowanie zaprezentowanych i omówionych w pracy zagadnień podzielić można na trzy główne kategorie:

A. Wpływ na rozwój podstaw nauki o ryzyku przemysłowym.

W Rozprawie zdefiniowano nowe standardy w zarządzaniu ryzykiem przemysłowym polegające na wykorzystaniu zaawansowanych technologii informatycznych, w tym zwłaszcza sztucznej inteligencji na wszystkich etapach zarządzania ryzykiem. Podejście takie pozwala na lepsze modelowanie i klasyfikację ryzyk w systemach przemysłowych umożliwiając bardziej niezawodne działanie zautomatyzowanych systemów ratunkowych (takich jak automatyczne gaśnice) i alarmowych (zwłaszcza eliminacja fałszywych alarmów).

B. Osiągnięcia naukowe związane z projektowaniem systemów klasy IRM DSS.

Rozprawa proponuje holistyczne podejście do zarządzania ryzykiem w dużym zakładzie przemysłowym, proponując modele ryzyka, zapobiegania mu i minimalizacji skutków zagrożeń integrujące różne aspekty zarządzania ryzykiem w jednym systemie. Modele te łączą analizę ryzyka, monitorowanie procesów oraz wspomaganie decyzji i umożliwiając ich implementację w jednym systemie. Podejście to rozszerza dotychczasowe realizacje DSS do zarządzania ryzykiem, które były skoncentrowane na pojedynczych aspektach ryzyka, a bardziej wszechstronne spojrzenie na te zagadnienia odpowiada rzeczywistemu zapotrzebowaniu przemysłu. Wprowadzenie wspomnianych w p. A zaawansowanych technik AI, umożliwia dokładniejsze prognozowanie i analizę ryzyka w czasie rzeczywistym, a wsparcie jakie daje wykorzystanie uczenia maszynowego w wielokryterialnej analizie decyzji w akcjach ratunkowych i działaniach zapobiegawczych pozwala na dynamiczne dopasowanie modelu preferencji zastosowanego w IRM DSS do zmieniających się warunków bezpieczeństwa w środowisku przemysłowym.

C. Innowacje zastosowane w IRM DSS.

Wprowadzenie częściowo nadzorowanych algorytmów uczenia maszynowego, które na bieżąco uczą się z danych historycznych, stanowi nowy kierunek w automatyzacji decyzji w systemach IRM DSS. Z kolei dynamiczne wykorzystanie sieci antycypacyjnych wprowadza możliwość przewidywania przyszłych stanów otoczenia, decyzji ekip

ratunkowych i uwzględniania ich w procesie koordynacji decyzji w sytuacji zagrożenia. Dzięki temu system może nie tylko reagować na zdarzenia, lecz także aktywnie je przewidywać i podejmować działania prewencyjne poprzez optymalny przydział zasobów do akcji ratunkowych i odpowiednie rozlokowanie ekip i ewakuację zagrożonych pracowników i sprzętu). Włączenie do zaimplementowanego systemu modeli przyczynowości pozwala na lepsze zrozumienie zależności między obserwowanymi i przewidywanymi zdarzeniami, umożliwiając bardziej precyzyjne planowanie działań zapobiegawczych i awaryjnych.

Powyższe osiągniecia wskazują, że sformułowana w rozdziale 1 teza rozprawy została wykazana, a wszystkie cele osiągnięte. W szczególności, zaprojektowany system spełnia warunki implementacji i wdrożenia w celu zarządzania ryzykiem i systemem bezpieczeństwa w KWC.

Lista Akronimów

- AF - Anticipatory Feedback
- AI - Artificial Intelligence
- AN - Anticipatory Network
- BPMN - Business Process Model and Notation
- DevOps - Development and Operations
- ERP - Enterprise Resource Planning
- IoT - Internet of Things
- IRM DSS - Industrial Risk Management Decision Support System
- IT - Information Technology
- KWC - Kopalnia Wapienia Czatkowice Spółka z o.o.
- ML - Machine Learning
- NSGA - Non-dominated Sorting Genetic Algorithm
- OT - Operational Technology
- SCADA - Supervisory Control and Data Acquisition
- TRRM - Threat Risk Response Map
- UAV - Unmanned Aerial Vehicle

Wybrana bibliografia

[1] De Nicola A, Villani ML, Costantino F, Di Gravio G, Falegnami A, Patriarca R (2022) A Knowledge Graph to Digitalise Functional Resonance Analyses in the Safety Area. In: F. Matos, P.M. Selig, E. Henriqson (eds), Resilience in a Digital Age. Contributions to Management Science, Springer, Cham, pp. 259-269. doi:10.1007/978-3-030-85954-1_15

[2] Feng JR, Zhao MK, Lu SX (2024) Accident spread and risk propagation mechanism in complex industrial system network. Reliability Engineering and System Safety, 244, art. no. 109940, p.1-14. doi:10.1016/j.ress.2024.109940

[3] Katoch S, Chauhan SS, Kumar V (2021) A review on genetic algorithm: past, present, and future. Multimed. Tools Appl., vol. 80:8091–8126. doi:10.1007/s11042-020-10139-6

[4] Keenan PB, Jankowski P (2019) Spatial Decision Support Systems: Three decades on.) Decision Support Systems, 116:64-76. doi:10.1016/j.dss.2018.10.010

[5] Niyomubyeyi O, Sicuaio TE, González JID, Pilesjö P, Mansourian A (2020) A comparative study of

four metaheuristic algorithms, AMOSA, MOABC, MSPSO, and NSGA-II for evacuation planning. Algorithms 13(1):16, p.1-21. doi:10.3390/a13010016

[6] Pfetsch ME, Schmitt A (2023) A generic optimization framework for resilient systems. Optimization Methods and Software, 38(2):356-385

[7] Rodriguez A, Fernandez-Medina E, Piattini M, (2007) A BPMN Extension for the Modeling of Security Requirements in Business Processes. IEICE Trans. Inf. & Syst E90-D(4):745-752. doi:10.1093/ietisy/e90–d.4.745

[8] Rönnbäck L, Holmström J (2008) Running to stand still: Examining the role of information technology in industrial risk management. 16th European Conference on Information Systems (ECIS), 12, p.1-13

[9] Skulimowski AMJ (2014) Anticipatory Network Models of Multicriteria Decision-Making Processes. Int. J. Systems Sci. 45(1):39-59. doi:10.1080/00207721.2012.670308

[10] Skulimowski AMJ, Łydek P (2022) Adaptive Design of a Cyber-Physical System for Industrial Risk Management Decision Support. In Proceedings of the 2022 IEEE 17th International Conference on Control, Automation, Robotics and Vision (ICARCV), Singapur, IEEE CPC Press, p.90–97. doi: 10.1109/ICARCV57592.2022.10004251

[11] Skulimowski AMJ, Łydek P (2022b) Applications of AI Alignment and Anticipatory Networks to Designing Industrial Risk Management Decision Support Systems. In Buchmann R.A. et al. (eds.), Proceedings of the 30th International Conference on Information Systems Development (ISD2022), Cluj-Napoca, Rumunia, p.1-6. https://aisel.aisnet.org/ isd2014/proceedings2022/ai/2/

[12] Skulimowski AMJ, Łydek P (2024) Anticipatory model of intelligent decision support in industrial risk management systems. In: PP-RAI'2024: Progress in Polish Artificial Intelligence Research 5, Warsaw University of Technology, p. 419-427

[13] Steinberg AN (2005) Threat Assessment Technology Development. In: A. Dey, B. Kokinov, D. Leake, R. Turner (eds), Modeling and Using Context. CONTEXT 2005. Lect. Notes in Comp. Sci., vol. 3554, Springer, Berlin, Heidelberg, pp. 490-500

[14] Zewde AB, Kassa SM (2021) Hierarchical multilevel optimization with multiple-leaders multiple-followers setting and nonseparable objectives. RAIRO - Operations Research, 55(5):2915 – 2939. doi:10.1051/ro/2021146