AKADEMIA GÓRNICZO-HUTNICZA IM. STANISŁAWA STASZICA W KRAKOWIE

DZIEDZINA NAUK INŻYNIERYJNO-TECHNICZNYCH

DYSCYPLINA: AUTOMATYKA, ELEKTRONIKA, ELEKTROTECHNIKA

I TECHNOLOGIE KOSMICZNE

ROZPRAWA DOKTORSKA

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, 2024

AGH UNIVERSITY OF KRAKOW

FIELD OF SCIENCE ENGINEERING AND TECHNOLOGY

SCIENTIFIC DISCIPLINE: AUTOMATION, ELECTRONICS, ELECTRICAL ENGINEERING AND SPACE TECHNOLOGIES

DOCTORAL DISSERTATION

Decision support system for designing and implementing industrial security systems using artificial intelligence techniques

Author: Paweł Łydek

Supervisor: Prof. dr hab. inż. Andrzej M. Skulimowski

Completed at: AGH University of Krakow, Faculty of Electrical Engineering, Automatics, Computer Science and Biomedical Engineering

Kraków, 2024

STRESZCZENIE

Potrzeba ciągłego rozwoju i doskonalenia systemów bezpieczeństwa w zakładach przemysłowych nabrała priorytetowego charakteru w obliczu rosnących obecnie wyzwań związanych z bezpieczeństwem, ochroną środowiska oraz skutecznością i ciągłością działania systemów produkcyjnych. Postęp technologiczny oraz rosnąca dostępność nowoczesnych rozwiązań otwierają nowe możliwości w obszarze integracji nowych narzędzi i technologii z istniejącymi już systemami wspomagającymi procesy zarządzania bezpieczeństwem. Świadomość konieczności wdrażania innowacji w tym obszarze w Kopalni Wapienia Czatkowice zaowocowało podjęciem decyzji o stworzeniu podstaw organizacyjnych i technologicznych budowy holistycznego systemu zarządzania ryzykiem i bezpieczeństwem przemysłowym oraz wsparcia procesów decyzyjnych w sytuacji materializacji ryzyk.

W rozprawie przedstawiono tło i cel badań, opisano kontekst związany 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 i realizacji procesów przemysłowych. Zidentyfikowano rodzaje ryzyk, przedstawiono metody ich oceny i klasyfikacji, a także sposoby analizy procesów technologicznych pod kątem ich bezpieczeństwa. 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 w trybie pracy ciągłej niepokojących sygnałów. 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, pozwoliło na zaproponowanie architektury oprogramowania systemu wspomagania decyzji opartego na sztucznej inteligencji (AI), wykorzystującego m.in. modele sieci bayesowskich, przyczynowych i 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. Analiza metod zarządzania ryzykiem przemysłowym oraz najlepszych praktyk w tym zakresie wskazuje metody, które mogą być przydatne w projektowaniu systemów wspomagających decyzje, w tym fuzję informacji, taksonomię zagrożeń oraz algorytmy ewakuacji, które stanowią istotną część systemu IRM DSS. Szczególną uwagę poświęcono modelom przyczynowości oraz zastosowaniu algorytmów optymalizacyjnych, co pozwala na lepsze planowanie działań awaryjnych.

Naturalną konsekwencją projektu systemu 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. Rozprawa zawiera całościowe omówienie zagadnień związanych z tworzeniem i wdrażaniem systemów wspierających bezpieczeństwo przemysłowe, przedstawiając konkretne techniki oraz zalecenia, które mogą służyć jako wytyczne dla praktyków i badaczy zajmujących się tą tematyką. Podejście takie ma na celu budowanie odporności przedsiębiorstwa równolegle z projektowaniem systemu i powinno być połączone z paradygmatem DevOps.

Słowa kluczowe: systemy wspomagania decyzji, zarządzanie ryzykiem przemysłowym, sztuczna inteligencja, analiza ryzyka, propagacja zagrożeń, optymalizacja procesów, analiza wielokryterialna, fuzja informacji, sieci antycypacyjne, górnictwo odkrywkowe.

ABSTRACT

The need for continuous development and improvement of safety systems in industrial plants is essential in the face of currently growing challenges related to safety, environmental protection and the effectiveness and continuity of production systems. Technological advances and the increasing availability of modern solutions are opening up new opportunities in the area of integrating new tools and technologies into existing systems supporting safety management processes and safety itself. Such an approach resulted in the decision at the Czatkowice Limestone Mine to lay the foundations for the construction of a holistic industrial risk and safety management system and to support decision-making processes in risk materialisation situations.

The dissertation presents the background and purpose of the research, describes the context related to safety in an open-pit mining facility and analyses in detail the specific needs related to the protection of employees, resources and infrastructure from hazards that may occur during mining and the implementation of industrial processes. Types of hazards were also identified, methods for their assessment and classification were presented, as well as ways to analyse technological processes in terms of their safety. Opportunities for the use of modern technologies such as video surveillance, drones and sensors that can be used to monitor risks and prevent potential hazards are included.

The technologies in question play an important role in the IRM DSS (Industrial Risk Management Decision Support System) concept of operation, tracking changes in the production environment and analysing sensor data, providing the ability to detect early signals of disruption in continuous operation. This approach allows anomalies to be identified in real time and preventive actions to be implemented, which in turn minimises the risk of hazardous events. A detailed discussion of the risk analysis techniques that form the basis of the IRM DSS allowed the software architecture of an AI-based decision support system to be proposed, including Bayesian, causal and anticipatory networks, multi-criteria analysis, expert information fusion, knowledge processing techniques and others.

The approach to designing intelligent decision support systems for industrial risk management and IRM DSS implementation is discussed in the context of integration with a company's existing IT systems, such as ERP and SCADA systems. A detailed analysis of the IT/OT environment identified functional gaps in current solutions and the potential benefits of IRM DSS interoperability with other systems to enable holistic safety management.

Particular attention has been paid to the specific requirements for technology alignment to ensure that new methods for implementing artificial intelligence are not only tailored to the needs of the business, but also optimised for performance and readiness for use. Contracting industrial risk management methods and best practices in the field identifies methods that can be useful in the design of decision support systems, including information fusion, hazard

taxonomy and evacuation algorithms, which form an important part of IRM DSS. Particular attention is given to causality models and the use of optimisation algorithms, which allows for better planning of emergency operations. A natural consequence of the design of the IRM DSS is its implementation in an industrial setting, so practical scenarios for the application of the system in different industrial sectors are proposed and the anticipated further development of industrial safety technology is discussed.

The conclusion highlights the importance of artificial intelligence in modern industrial risk management, pointing to potential opportunities for further integration of these solutions with other areas of business management, such as financial risk analysis. The article provides a comprehensive discussion of the issues involved in developing and implementing systems to support industrial security, presenting specific techniques and recommendations that can serve as guidelines for practitioners and researchers working in this area. The approach aims to build enterprise resilience in parallel with system design and should be combined with the DevOps paradigm.

Keywords: decision support systems, industrial risk management, artificial intelligence, risk analysis, threat propagation, process optimisation, multi-criteria analysis, information fusion, anticipatory networks, open-pit mining.

Spis treści

1 Wprowadzenie: cel i zakres prac badawczych

1.1 Cel i teza rozprawy

Głównym celem prac badawczych przedstawionych w niniejszej 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 wyżej 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.

Analiza zagrożeń i przeprowadzona została w oparciu o zastosowanie metod fuzji informacji w postaci map najczęściej występujących zagrożeń na terenie kopalni odkrywkowej, związanych przede wszystkim z osuwiskami, zalaniami i obrywaniem się skał. Na podstawie analizy informacji o zagrożeniach dokonano przeglądu możliwych do zastosowania strategii zarzadzania kryzysowego, a następnie sformułowano wielokryterialny problem decyzyjny, który będzie rozwiązywany z pomocą IRM DSS jako specjalistycznego Systemu Wspomagania Decyzji (dalej: SWD). Informacja o zagrożeniach pozyskiwana będzie jednocześnie z systemu monitoringu wizyjnego, zespołu czujników tworzących sygnalizację alarmową oraz od osób zatrudnionych w kopalni. Występujące jednocześnie heterogeniczne i rozłożone na rozległym terenie zagrożenia wymagają zastosowania złożonych wielokryterialnych algorytmów decyzyjnych dotyczących m.in. przydziału zasobów do akcji ratunkowych, priorytetyzacji tych akcji w czasie i ich rozkładu przestrzennego.

Przeprowadzona na wstępnym etapie badań analiza potrzeb, potwierdzona następnie w eksperckim badaniu delfickim wskazała, że spośród wielu potencjalnie ważnych problemów rozwiązywanych przy pomocy IRM DSS, najlepszą wartość stosunku nakładów i czasu na przeprowadzenie badań i wdrożenie ich wyników do spodziewanych korzyści w postaci zmniejszenia ryzyka mierzonego wartością narażoną na stratę (VaR – *Value-at-Risk*) daje opracowanie zasad i algorytmów wspomagania decyzji w zagadnieniu ewakuacji sprzętu z zagrożonego terenu. W związku z tym opracowane zostały podstawy teoretyczne SWD w postaci hierarchicznego schematu zależności ryzyk, wywołanych nimi zagrożeń, sposobów ich detekcji i reakcji mających na celu przeciwdziałanie ryzykom lub minimalizację skutków zinwentaryzowanych zagrożeń. Na tej podstawie w sytuacji

zagrożenia nastąpi wybór kompromisowego planu ewakuacji wskazującego optymalne ścieżki i harmonogram ewakuacji poszczególnych maszyn znajdujących się w zagrożonych obszarach wyrobiska. Dodatkowo, zaproponowany został mechanizm uczenia maszynowego (ang.: *Machine Learning*, ML), pozwalający na określenie strategii zwiększenia odporności zakładu na przyszłe zagrożenia w oparciu o analizę podjętych wcześniej decyzji i ich skutków.

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 zdrowia i/lub życia pracowników, 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 (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.

Wykazaniu powyższej tezy poświęcona jest dalsza część niniejszej rozprawy. Oprócz oryginalnych badań własnych, w tym zwłaszcza związanych z zastosowaniem grafów wiedzy, sieci antycypacyjnych i metod wielokryterialnego wspomagania decyzji opartych o zbiory odniesienia, dokonany został przegląd istniejących metod i systemów informatycznych poświęconych zwłaszcza budowie odporności na zagrożenia (ang. *resilience*) w zakładach przemysłowych. Pozwoliło to na identyfikację najlepszych praktyk i ich zastosowanie w opracowanej i przedstawionej w rozprawie autorskiej koncepcji IRM DSS.

1.2 Struktura i zakres badań przedstawionych w rozprawie

Zgodnie z wstępnym studium wykonalności, IRM DSS jest rozwijany 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 [rozdz. 10.3.1, Rönnbäck, Holmström, 2008]. Prognozy te wspierają zorientowany na przyszłość technologii AI rozwój kolejnych wersji IRM DSS. Techniki AI są stosowane przede wszystkim do przetwarzania i łączenia informacji z czujników, projektowania inteligentnych wielokryterialnych metod wspomagania decyzji oraz procedur uczenia maszynowego. Optymalne decyzje podejmowane są za pomocą głównego silnika wspomagania decyzji, który przetwarza wszystkie dostępne informacje o zagrożeniach, takie jak dane z czujników, fakty historyczne dotyczące przeszłych zagrożeń oraz metody i wyniki ich eliminowania. Ograniczenia dotyczące reguł decyzyjnych są narzucane przez prawo, ograniczenia techniczne lub wewnętrzne regulacje obowiązujące w zakładzie przemysłowym. W tym przypadku przetworzone informacje są przechowywane w bazie wiedzy, która jest sprzężona z silnikiem wspomagania decyzji. Decyzje wynikające z przetwarzania wyłącznie

informacji z czujników i zespołu ratowniczego będą określane jako decyzje ad hoc. Długoterminowe decyzje dotyczące zarządzania ryzykiem, które koncentrują się na działaniach prewencyjnych, będą również uwzględniały wyniki dotychczasowych działań jako dane wejściowe do uczenia parametrów działań i preferencji menedżerskich. W rozważanych w niniejszej 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.

Dla przykładu, pomiar temperatury w czujnikach pożarowych może być obarczony błędem wynikającym z niedokładności czujników pomiarowych. Ta niedokładność może być z góry oceniona jako błąd pomiaru *ex-ante*. W ogólnym przypadku propagacja zagrożeń może być modelowana jako sieć, w której straty informacji i przypadkowe błędy operacyjne i decyzyjne są źródłami dodatkowego ryzyka. Implementacja systemu analizowanego i opartego na domenowej ontologii DSS do zarządzania ryzykiem przetwarza pierwsze informacje o zagrożeniach dostarczane przez czujniki i łączy je. Skondensowana informacja trafia do jednostek decyzyjnych, które wraz z wymienionymi obiektami są również węzłami sieci modelowej. Uzupełnieniem tej sieci jest model zarządzania ryzykiem i optymalizacji, w którym występują algorytmy decyzyjne, akcje oraz elementy wykonawcze do ich realizacji. Oba komponenty modelu są sprzężone poprzez informacje zwrotne otrzymywane przez czujniki i dostarczane bezpośrednio decydentom. Silnik DSS wykorzystuje powyższe komponenty modelu w sposób sekwencyjny i łączy je z procedurą częściowo nadzorowanego uczenia maszynowego, w której wyniki poprzednich decyzji są wykorzystywane do uczenia się charakterystyk systemu czujników, parametrów procedury ograniczania ryzyka oraz preferencji menedżera.

Przedstawione tu badania uwzględniają fakt, że górnictwo odkrywkowe wiąże się ze specyficznym ryzykiem spowodowanym występowaniem zagrożeń naturalnych, takich jak osuwiska czy obrywy skalne rozmieszczone na dużym obszarze w kopalni, bezpośrednio w miejscu, gdzie prowadzona jest eksploatacja, jak i w jej sąsiedztwie. Zagrożenia te związane są z przemieszczeniami struktur geologicznych, gdzie może dojść do usunięcia się górotworu [van Engelen, Hoos, 2020; Chen i in., 2013]. Przemieszczenia mogą występować samoistnie, w wyniku długotrwałych procesów lub mogą być spowodowane intensywnymi opadami atmosferycznymi. Powodowane są również przez ruch ciężkich pojazdów lub roboty strzałowe w kopalni. Dlatego też system zarządzania bezpieczeństwem powinien zapewnić okresowe skanowanie terenu [por. podrozdział 3.2] kopalni odkrywkowej w celu identyfikacji potencjalnych zagrożeń. Potrzeba zastosowania najnowocześniejszych narzędzi przetwarzania informacji i prewencji opartych o metody AI wynika z faktu, że wyzwania związane

z zarządzaniem zagrożeniami powinny być realizowane z coraz większą jakością i autonomią. Technologie prewencyjne oparte na AI obejmują rozumienie obrazu z kamer monitoringu wizualnego, podczerwieni i innych czujników. W połączeniu z autonomicznymi robotami inspekcyjnymi, które zapewniają automatyczną analizę próbek skał, wskazują one miejsca zagrożone w kopalni.

Chociaż metody AI są często stosowane do wspierania decyzji w finansach, gdzie ryzyko jest modelowane zazwyczaj jako wariancja lub wartość zagrożona, wykorzystanie tych metod w zarządzaniu ryzykiem przemysłowym napotkało na problemy ze znalezieniem wspólnej podstawy do kwantyfikacji heterogenicznych czynników ryzyka [Vernez i in., 2004]. W odróżnieniu od systemów zarządzania ryzykiem finansowym, gdzie ryzyko może być wyrażone w jednostkach pieniężnych, zagrożenia przemysłowe dotyczą zarówno zdrowia i życia ludzkiego, jak i dóbr materialnych [Seppanen, Virrantaus, 2015], co implikuje konieczność stosowania wielokryterialnych miar ryzyka. Przedstawiona architektura oprogramowania IRM DSS została zaprojektowana w oparciu o najlepsze praktyki zarządzania kryzysowego zaproponowane w [Barthelemy, 1998; Katoch i in., 2021], biorąc pod uwagę również architekturę DSS stosowanych do zarządzania ryzykiem w finansach. Ogólne zasady projektowania IRM DSS omówiono w [Chen i in., 2013], natomiast ontologiczne podejście do strukturalnego modelowania zagrożeń, zapobiegania i łagodzenia ich skutków przedstawiono w [Rönnbäck, Holmström, 2008; Kerr, Phaal, 2020]. Rosnąca liczba heterogenicznych źródeł informacji wykorzystywanych w zarządzaniu kryzysowym, takich jak informacje przekazywane za pośrednictwem mediów społecznościowych, wskazuje na potrzebę stosowania analizy zaufania [Lessin i in., 2019], filtrowania i fuzji informacji. Rozwiązanie problemu ewakuacji personelu, odwiedzających i pojazdów z zagrożonego obszaru w kopalni wymaga adaptacyjnych algorytmów opartych na ML badanych w [Domdouzis, 2018]. Hierarchiczny charakter podejmowania decyzji w sytuacjach kryzysowych i długoterminowego planowania prewencyjnego spowodował przyjęcie metodologii roadmappingu do zaprojektowania komponentu długoterminowego zarządzania ryzykiem i planowania strategicznego DSS [Erdeli i in., 2017; Purohit i in., 2019].

Ponadto techniki oparte na AI pozwolą na adaptacyjne wyznaczanie przez IRM DSS optymalnych ścieżek ewakuacji z zagrożonej części kopalni w przypadku wystąpienia awarii. Algorytmy AI/ML umożliwiają dostosowanie przebiegu ewakuacji do zmiennych warunków geologicznych w sytuacjach awaryjnych w kopalni spowodowanych czynnikami naturalnymi lub ludzkimi. System zasilany jest kombinacją informacji z monitoringu wizualnego stosowanego już obecnie oraz nowych sensorów, takich jak radar, lidar, obrazowanie w podczerwieni, wspieranych przez UAV [Chen i in., 2013] i autonomiczne roboty inspekcji naziemnej. Siatka wzajemnie wspierających się sensorów jest tak zaprojektowana, aby zapewnić optymalne pokrycie chronionego obszaru. System obserwacji powinien być zintegrowany z najnowocześniejszymi algorytmami analizy sygnału, fuzji informacji,

rozpoznawania wzorców i rozumienia obrazu, co pozwala na identyfikację zagrożeń. Po uruchomieniu procedury reagowania kryzysowego DSS proponuje odpowiednie działania ochronne i łagodzące, odpowiednie do danej sytuacji. DSS jest uzupełniony o autonomiczny moduł decyzyjny zdolny do inicjowania automatycznych działań łagodzących i przeciwdziałających zagrożeniom, takich jak aktywacja gaśnic w obszarze zagrożonym pożarem. Po fazie uczenia, metody klasyfikacji w systemie bezpieczeństwa zastosowane do heterogenicznych sygnałów wejściowych mogą rozróżnić potencjalne zagrożenie, takie jak wtargnięcie człowieka, od nieszkodliwego lub neutralnego dla bezpieczeństwa zakładu obiektu, takiego jak np. małe zwierzę leśne. Obiekt zdiagnozowany jako zagrożenie lub podejrzewany o nie, np. nieuprawnione osoby pojawiające się w monitorowanym obszarze, uruchamia automatyczne śledzenie przez czujniki.

Kluczową rolę w całym procesie odgrywa budowanie odporności, a jako element pomocniczy w tym procesie wykorzystać można zintegrowany system informatyczny klasy ERP wyposażony o moduł DSS Specjalistyczny moduł DSS powinien zapewniać możliwość planowania i wspierania gotowości na wypadek zaistnienia sytuacji kryzysowej w obszarze zarządzania bezpieczeństwem.

Z formalnego punktu widzenia, projektowanie i eksploatacja całego systemu bezpieczeństwa przedsiębiorstwa, w tym DSS, może być traktowana jako dwupoziomowy problem optymalizacyjny [Skulimowski, Łydek, 2022], w którym wybór infrastruktury bezpieczeństwa i procedur decyzyjnych na poziomie wyższym definiuje ograniczenia obserwowane podczas działań ograniczających zagrożenie w sytuacji kryzysowej. Natomiast optymalizacja tych działań w sytuacji wystąpienia zagrożenia jest problemem do rozwiązania na niższym, podrzędnym poziomie. Przykładowo, liczba, jakość i odpowiednie usytuowanie czujników odgrywa kluczową rolę w identyfikacji zagrożenia, odpowiednim planowaniu reakcji oraz jej terminowości [Jabbari i in., 2016]. DSS jest osadzony w strukturze cyber-fizycznej, która jest modelowana przez mapę zagrożeń, zwaną w skrócie TRRM (por. następny rozdział). TRRM stanowią klasę grafów wiedzy [Alves i in., 2021], które zostały już wcześniej zastosowane jako modele systemów bezpieczeństwa [Liu, 2013]. Podejście zaprezentowane w niniejszej rozprawie zapewnia holistyczne połączenie wszystkich etapów modelowania, planowania i implementacji przemysłowego systemu bezpieczeństwa.

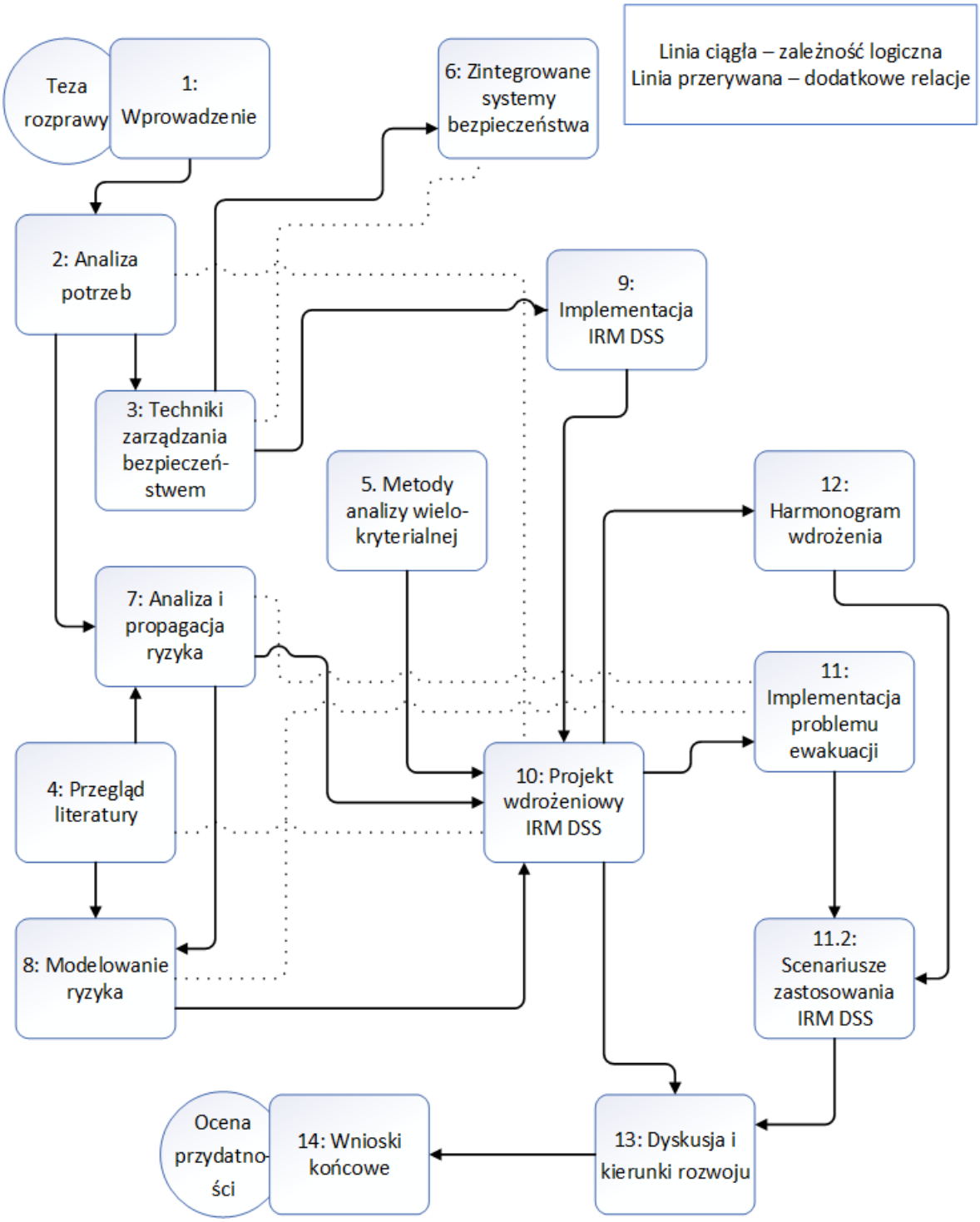
W projektowanym systemie zastosowanie znajdą również ontologie, które dzięki swym właściwościom znajdują coraz szersze zastosowanie w systemach zarządzania wiedzą, umożliwiając dynamiczne organizowanie wiedzy oraz jej łatwe wyszukiwanie i analizowanie. Ontologie umożliwiają precyzyjny opis skomplikowanych procesów i zależności, co jest niezbędne do skutecznego zarządzania zagrożeniami w złożonych systemach. Dzięki formalnym modelom wiedzy możliwe jest automatyczne podejmowanie decyzji w czasie rzeczywistym, a same systemy mogą być rozbudowywane o nowe obszary bezpieczeństwa bez potrzeby redefiniowania całej struktury wiedzy. Wprowadzenie ontologii do systemów

zarządzania bezpieczeństwem pozwala na lepsze zarządzanie procesami, automatyzację wielu działań oraz precyzyjniejszą analizę zagrożeń. Ontologie pomagają też w zintegrowaniu i unifikacji informacji, co jest kluczowe w nowoczesnych systemach bezpieczeństwa opartych na zaawansowanych technologiach, AI.

Praca 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, który spełni stawiane oczekiwania. W strukturze pracy wyróżnić można następujące, kolejno omówione, elementy logiczne:

A) Wstęp (niniejszy rozdział), 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 wielokryterialne 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 przedstawiony jest na diagramie niżej [Rys. 1].



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

1.3 Terminologia stosowana w rozprawie

Poniżej zebrane zostały, w postaci krótkiego słownika, definicje najważniejszych terminów użytych w opracowaniu. Pełen wykaz skrótów znajduje się w dodatku [Lista Akronimów].

Budowa odporności – podejmowanie działań mających podnieść poziom bezpieczeństwa poprzez zorganizowane przeciwdziałanie możliwości wystąpienia lub materializacji czynników ryzyka.

Czynnik ryzyka – zinwentaryzowane (udokumentowane) zagrożenia z możliwymi do określenia prawdopodobieństwem wystąpienia i konsekwencjami dla konkretnych aspektów bezpieczeństwa, inaczej zagrożenie bezpośrednie.

Działania prewencyjne – działania mające na celu wyeliminowanie lub zminimalizowanie możliwości materializacji zagrożenia poprzez ograniczenie możliwości zaistnienia jego przyczyny.

Miara ryzyka – jest wynikiem nakładania się wielu czynników; kwantyfikuje ryzyko odzwierciedlający rzeczywisty potencjalny wpływ na otoczenie, możliwość materializacji i wartość narażoną na stratę, zarówno materialną, jak i w postaci mierzalnego zagrożenia dla zdrowia lub życia, a także reputacji przedsiębiorcy.

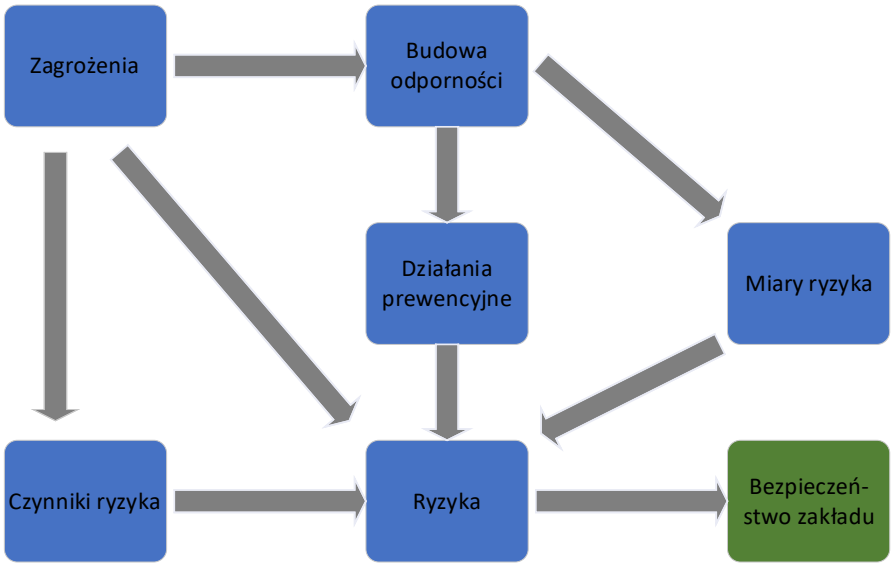
Ryzyko – mierzalna szkoda, którą może wywołać zagrożenie, określone przez prawdopodobieństwo wystąpienia i intensywność.

Właściciel ryzyka – osoba fizyczna lub prawna odpowiedzialna za zarządzanie ryzykiem oraz opracowanie mechanizmów mających doprowadzić do jego minimalizacji (lub eliminacji).

Wpływ na bezpieczeństwo – oszacowanie potencjalnych skutków zagrożeń na integralność, ciągłość oraz stabilność procesów i systemów, uwzględniające zarówno prawdopodobieństwo materializacji zdarzenia, jak i wielkość potencjalnych strat wynikających z tego zdarzenia.

Zagrożenie – potencjalne źródło zaistnienia (materializacji) szkody w obszarze majątku, zdrowia ludzkiego, wartości niematerialnych lub środowiska naturalnego (np. powódź, kradzież, trzęsienie ziemi, atak terrorystyczny, pożar).

Wzajemne relacje pomiędzy wymienionymi powyżej pojęciami, które można potraktować jako podstawę ontologii mereologicznej IRM DSS przedstawia Rys. 2.



Rys. 2. Czynniki wpływające na bezpieczeństwo i ich wzajemne relacje.

Użyte w powyższym słowniku definicje sformułowane zostały w oparciu o terminologię zgodną z obowiązującymi normami ISO [P.3][P.4], definicje zgodne z funkcjonującym w Grupie TAURON słownikiem [P.8], a podejściem indywidualnym do zagadnienia opracowanym w trakcie tworzenia podstaw teoretycznych niniejszej rozprawy. Wybór takiego rozwiązania podyktowany jest chęcią uchwycenia indywidualnych, typowych dla przedsiębiorstwa, cech opisywanych zjawisk, ich skutków, ich wpływu na przedsiębiorstwo i w dalszej konsekwencji bezpieczeństwo ocenianych i omawianych procesów.

Często można spotkać się z innymi definicjami podanych wyżej pojęć. Dla przykładu, Norma PN-ISO 31000:2012 [P.3] definiuje „Ryzyko" jako:

- niepewność związaną ze zdarzeniem lub działaniem, które wpłynie na zdolność realizacji celów działania firmy;
- szansę zajścia wydarzenia, które będzie miało wpływ na cele, wyrażoną w wielkościach prawdopodobieństwa i skutków,
- kombinację prawdopodobieństwa wystąpienia wydarzenia i jego skutków.

Definicja ryzyka dostosowana do potrzeb tego opracowania zawęża zakres rozumienia definicji zgodnej z Normą ISO do możliwości wystąpienia szkody (materialnej bądź nie) będącej następstwem omawianych zagrożeń i ich kumulacji. W myśl tej definicji, ryzyko może zostać powiązane z możliwą do oszacowania stratą, wyrażoną jako wektor wzajemnie nieporównywalnych strat oraz odpowiadający im wektor prawdopodobieństw wystąpienia każdego rodzaju ryzyk. Dodatkowo, wszystkie te wartości są traktowane jako funkcje czasu ich występowania. Zestawienie podstawowych pojęć używanych w różnych obszarach aktywności biznesowej zebrano w tabeli [Tab. 1].

Tab. 1 Zestawienie definicji z obszaru ryzyka

Ryzyko	
Terminologia stosowana w rozprawie	Mierzalna szkoda, którą może wywołać zagrożenie, określone przez prawdopodobieństwo wystąpienia i intensywność.
Norma ISO 31000	Efekt niepewności na cele. Ryzyko w tym kontekście odnosi się do odchylenia od oczekiwanych wyników, które może być zarówno pozytywne, jak i negatywne.
Project Management Body of Knowledge Guide	Niepewne zdarzenie lub warunek, którego wystąpienie może mieć pozytywny lub negatywny wpływ na cele projektu.
Ekonomia i finanse	Ryzyko odnosi się do sytuacji, w których możliwe są znane prawdopodobieństwa różnych wyników, natomiast niepewność dotyczy sytuacji, w których takie prawdopodobieństwa są nieznane.
Inżynieria i technika	Iloczyn prawdopodobieństwa wystąpienia zdarzenia i jego konsekwencji.
Czynnik ryzyka	
Terminologia stosowana w rozprawie	Zinwentaryzowane (udokumentowane) zagrożenia z możliwymi do określenia prawdopodobieństwem wystąpienia i konsekwencjami dla konkretnych aspektów bezpieczeństwa, inaczej zagrożenie bezpośrednie.
Norma ISO 31000	Okoliczności lub zjawiska, które mogą wpłynąć na pojawienie się niepewności, a w konsekwencji ryzyka, i są analizowane w kontekście oceny ryzyka.
Project Management Body of Knowledge Guide	Okoliczność lub warunek, który może wpłynąć na realizację projektu w sposób negatywny lub pozytywny
Ekonomia i finanse	Zmienne lub okoliczności, które mogą wpływać na rentowność inwestycji lub przedsiębiorstwa.
Inżynieria i technika	Zdarzenie, okoliczność lub właściwość systemu technicznego, które mogą prowadzić do wystąpienia niepożądanych konsekwencji w trakcie realizacji projektu, eksploatacji systemu lub funkcjonowania urządzenia technicznego.
Zagrożenie	
Terminologia stosowana w rozprawie	Potencjalne źródło zaistnienia (materializacji) szkody w obszarze majątku, zdrowia ludzkiego, wartości niematerialnych lub środowiska naturalnego (np. powódź, kradzież, trzęsienie ziemi, atak terrorystyczny, pożar)
Norma ISO 31000	Źródło potencjalnego szkody.
Project Management Body of Knowledge Guide	Niepewne zdarzenie lub warunek, którego wystąpienie może mieć negatywny wpływ na cele projektu.
Ekonomia i finanse	Potencjalne zdarzenie lub zjawisko, które może negatywnie wpłynąć na stan finansów przedsiębiorstwa, rynków finansowych, gospodarki narodowej lub globalnej.
Inżynieria i technika	Potencjalne źródło awarii systemu, która może prowadzić do strat materialnych, środowiskowych lub zdrowotnych

Miara ryzyka	
Terminologia stosowana w rozprawie	Jest wynikiem nakładania się wielu czynników; kwantyfikuje ryzyko odzwierciedlający rzeczywisty potencjalny wpływ na otoczenie, możliwość materializacji i wartość narażoną na stratę, zarówno materialną, jak i w postaci mierzalnego zagrożenia dla zdrowia lub życia, a także reputacji przedsiębiorcy.
Norma ISO 31000	Sposób kwantyfikacji wpływu i prawdopodobieństwa wystąpienia zagrożeń
Project Management Body of Knowledge Guide	Narzędzie służące do porównywania różnych rodzajów ryzyka, bazujące na prawdopodobieństwie wystąpienia zagrożenia oraz jego potencjalnych konsekwencjach.
Ekonomia i finanse	Definiowane przez: Value at Risk (VaR) – miara określająca maksymalną stratę portfela w określonym horyzoncie czasowym przy danym poziomie ufności.
Inżynieria i technika	Iloczyn prawdopodobieństwa wystąpienia zagrożenia i jego skutków.
Działania prewencyjne	
Terminologia stosowana w rozprawie	Działania mające na celu wyeliminowanie, lub zminimalizowanie możliwości materializacji zagrożenia poprzez ograniczenie możliwości zaistnienia jego przyczyny.
Norma ISO 31000	Kluczowy element zarządzania ryzykiem i obejmujący identyfikację ryzyka, jego analizę oraz podjęcie działań mających na celu uniknięcie ryzyka lub zmniejszenie jego prawdopodobieństwa.
Project Management Body of Knowledge Guide	Działania prewencyjne mają na celu minimalizację potencjalnych ryzyk projektowych przed ich wystąpieniem.
Ekonomia i finanse	Strategiczne środki i procesy podejmowane w celu zminimalizowania potencjalnych ryzyk finansowych lub ekonomicznych, zanim dojdzie do ich wystąpienia. Celem
Inżynieria i technika	Działania prewencyjne odnoszą się do strategii i środków, które mają na celu zapobieganie wystąpieniu sytuacji kryzysowych.

Wykaz najważniejszych pojęć i ich skrótów stosowanych w rozprawie podany jest w Tabeli 2 niżej.

Tab. 2 Zestawienie najważniejszych pojęć i ich skrótów stosowanych w rozprawie

AI	Artificial Intelligence
DevOps	Development and Operations
DSS	Decision Support System
EIS	Enterprise Information System
ERP	Enterprise Resource Planning
ICT	Information and Communications Technology
IDSS	Intelligent Decision Support System
IRM DSS	Industrial Risk Management Decision Support System

KWC	Kopalnia Wapienia Czatkowice Spółka z o.o.
MCDA	Multiple Criteria Decision Analysis
SRR	Search & Rescue Robotics
SWD	System Wspomagania Decyzji
SWOTC	Strengths Weaknesses Opportunities Threats & Challenges
TRRM	Threat Risk Response Map
UAV	Unmanned Aerial Vehicle
VaR	Value at Risk

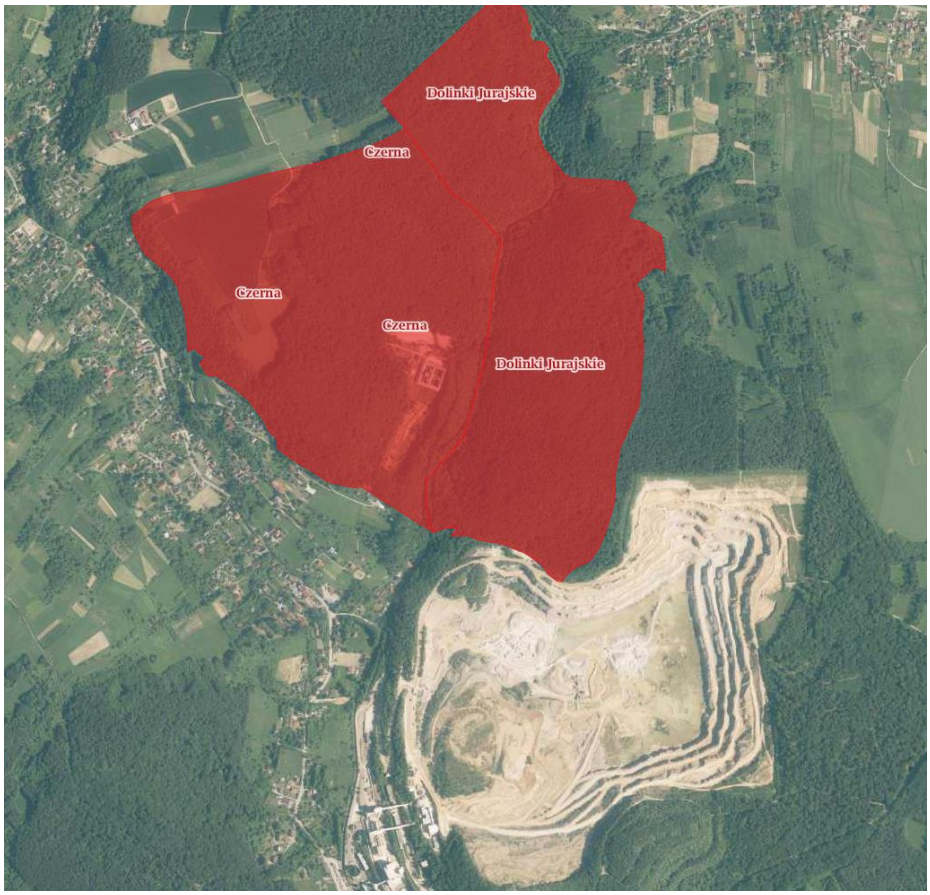
2 Analiza potrzeb przedsiębiorstwa w zakresie zapewnienia bezpieczeństwa przemysłowego

Zgodnie z przedstawionym wyżej celem rozprawy, w niniejszym rozdziale przedstawiamy motywację i zakres badań zagrożeń występujących w Kopalni Wapienia Czatkowice Spółka z o.o. (dalej Kopalnia Wapienia Czatkowice lub KWC) oraz analizę potrzeb związanych z budową odporności i zapewnieniem bezpieczeństwa zakładu.

2.1 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 [por. Rys. 3].

Rys. 3. Lokalizacja Kopalni. Źródło: zasoby własne KWC.



Rys. 4. Obszar Natura 2000 (kolor czerwony) w sąsiedztwie KWC.
Źródło: geoserwis.gdos.gov.pl, domena publiczna

Obszar, na którym prowadzona jest eksploatacja, jest rozległy, z tendencją do powiększania się o ok. 2 ha/rok. Obecnie (listopad 2024) powierzchnia obszaru eksploatacji wynosi ok. 134 ha, Kopalnia graniczy z terenami leśnymi oraz bezpośrednio przylega do obszaru Natura 2000 [Rys. 4]. Pod względem strukturalnym złoże jest zróżnicowane i trudne w eksploatacji. Wynika to z faktu, że ławice wapieni dolnego karbonu ułożone są stromo, kąt opadania wynosi od 60-70º w części środkowej, do 40-45º w części wschodniej. Złoże przecinają spękania ciosowe o różnych kierunkach i nachyleniach. Dodatkowym czynnikiem utrudniającym eksploatację są licznie występujące formy krasowe w postaci kominów i lejów krasowych [P.1].

Rys. 5. Teren prowadzenia aktywności przemysłowej. Źródło: KWC

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,

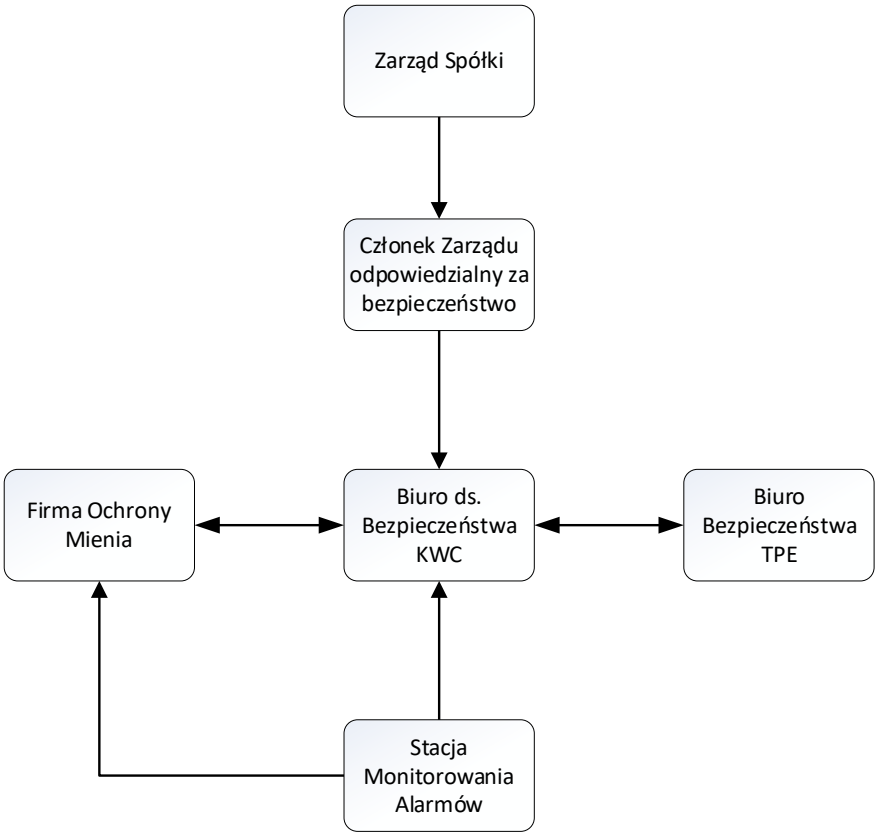
oraz

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

Warunek 4 dotyczy przede wszystkim pracowników wydobycia, pełniących obowiązki na terenie Obszaru Górniczego (OG) KWC. Osiągnięcie i trwałe zapewnienie stanu bezpieczeństwa jest zatem warunkiem koniecznym prowadzenia podstawowej działalności firmy. W tym celu w KWC powołano Biuro ds. Bezpieczeństwa, które odpowiedzialne jest w szczególności za:

- zapewnienie optymalnie dostosowanego do występujących zagrożeń poziomu bezpieczeństwa,
- realizację zadań w zakresie identyfikacji i zarządzania ryzykami,
- ciągłe monitorowanie poziomu bezpieczeństwa,
- obsługę incydentów bezpieczeństwa oraz zapewnienie reakcji minimalizującej ich skutki oraz eliminującej ich wystąpienie,
- wsparcie i promocję postaw zapewniających bezpieczeństwo,
- realizację przeglądów, kontroli oraz audytów bezpieczeństwa,
- planowanie środków technicznych, organizacyjnych i finansowych w zakresie zapewnienia bezpieczeństwa,
- koordynację działań w obszarze bezpieczeństw pomiędzy KWC a komórką bezpieczeństwa w Tauron Polska Energia SA (TPE).

Miejsce Biura ds. Bezpieczeństwa w strukturze organizacyjnej firmy pokazane jest na Rys. 6 niżej.



Rys. 6. Uproszczony schemat organizacyjny KWC ze wskazaniem funkcji Biura ds. Bezpieczeństwa

Analizy ryzyk prowadzone przez KWC ([rozdział 2.3], [P.1]) mają na celu zdefiniowanie działań zapewniających trwałe osiąganie wskazanych wyżej celów polityki bezpieczeństwa. Analizy te prowadzone są okresowo, zgodnie z obowiązującymi w Spółce regulacjami, przy czym w pierwszej kolejności analizowane są nowe ryzyka oraz zmiany poziomów zagrożeń będące wynikiem monitoringu w okresie od poprzedniej oceny ryzyk.

Mając na uwadze wyniki analizy przeprowadzonej w roku 2019, które zostały wykorzystane w niniejszej rozprawie, można stwierdzić, że ryzykiem o najwyższym potencjalnie wpływie na bezpieczeństwo jest ryzyko intruzji, a działaniem o najwyższym priorytecie jest zabezpieczenie granic terenu Spółki przed możliwością wejścia osób niepożądanych. Ryzyko to może mieć także negatywny wpływ na utrzymanie ciągłości procesów technologicznych, należy zatem dążyć do jego minimalizacji.

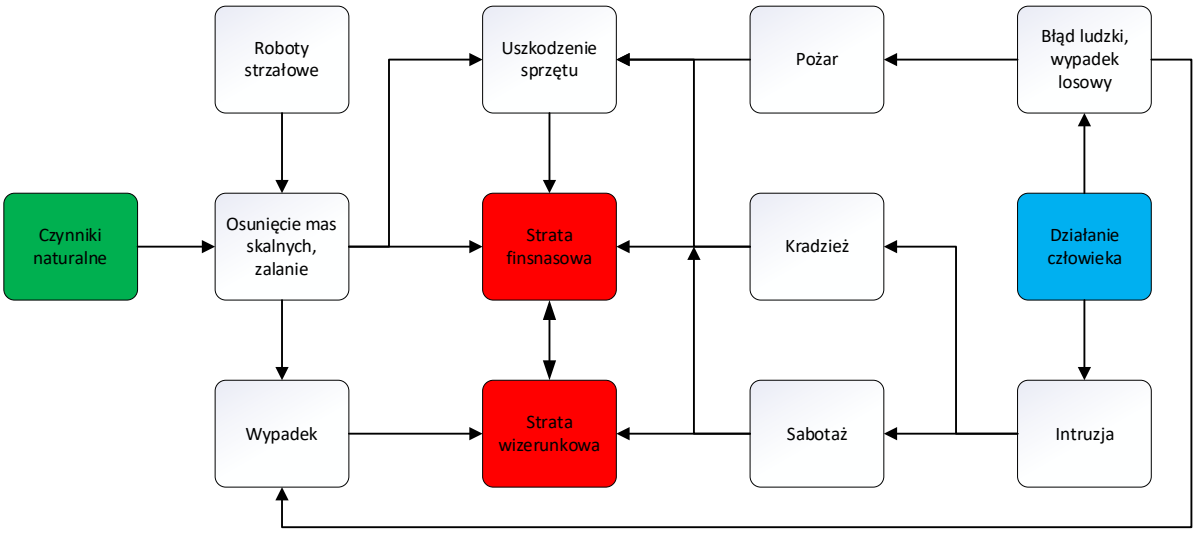
Dodatkowym aspektem, na który należy zwrócić uwagę przy kompleksowej analizie bezpieczeństwa przemysłowego KWC, jest fakt, że obszar eksploatacji górniczej może być atrakcyjny dla miłośników sportów ekstremalnych, zwłaszcza takich, jak paralotniarstwo czy sporty motocrossowe. Zwiększa to prawdopodobieństwo wypadków z udziałem ludzi o potencjalnie nieoczekiwanej lokalizacji i przebiegu.

Ze względu na charakter prowadzonej działalności, tj. praca na rozległym, trudnym, a miejscami niemożliwym do ogrodzenia terenie oraz ciągłe poszerzanie terenu eksploatacji, zapewnienie wymaganego poziomu bezpieczeństwa wiąże się z szeregiem wyzwań,

w sprostaniu którym pomóc mogą nowoczesne technologie monitoringu i prewencji wsparte wykorzystaniem technik uczenia maszynowego i sztucznej inteligencji (AI) oraz fuzja danych pozyskiwanych z wielu źródeł. Tego typu podejście do zagadnienia wpisuje się w definicję podejścia holistycznego, obejmującego przedsiębiorstwo nadzorem całościowo i dającego decydentom szeroki wachlarz możliwości do wykorzystania.

2.2 Klasyfikacja ryzyk i zagrożeń

Zagrożenia dzielimy na **zagrożenia pierwotne** i **zagrożenia wtórne** lub **bezpośrednie**. Zagrożenia pierwotne mogą być połączone w łańcuchy przyczynowo-skutkowe. Dla przykładu, zagrożeniem pierwotnym mogą być intensywne opady deszczu, które mogą spowodować oberwania skał (zagrożenie wtórne). Ryzykiem jest możliwość uszkodzenia sprzętu znajdującego się w zasięgu obrywów skalnych, a jego materializacją – zajście takiego uszkodzenia. Na podstawie prognozy opadowej i dotychczasowego przebiegu opadów można określić prawdopodobieństwo obrywania się skał w monitorowanym obszarze. Jako ryzyko pierwotne można też analizować zmiany klimatu. Wtedy intensywne opady będą ryzykiem pierwotnym pośrednim. Podobną analizę zastosować można do intruzji, której następstwem mogą być zarówno kradzieże czy uszkodzenia mienia, jak również zdarzenia prowadzące np. do pożaru lub wypadku z ofiarami ludzkimi. Odpowiedniość pomiędzy ryzykami i zagrożeniami nie jest jednoznaczna, tj. jedno ryzyko może wynikać z wielu zagrożeń, a każde zagrożenie może być przyczyną wielu ryzyk. Jednym z pierwszych etapów kompleksowej analizy ryzyka jest konstrukcja grafu kauzalnego pokazującego powiązania pomiędzy zagrożeniami, ryzykami i miarami ryzyka. Przykład takiego grafu, odwzorowującego realia analizowanego środowiska przemysłowego zaprezentowany jest na Rys. 7 poniżej.



Rys. 7. Sieć powiązań zagrożeń i ryzyk występujących w KWC

2.3 Metody oceny ryzyk i zagrożeń przemysłowych

W metodologii oceny i zarządzania zagrożeniami wyróżnia się zagrożenia trzech podstawowych typów [Di Vaio i in., 2020]:

- zagrożenia typu *safety*
- zagrożenia typu *security*
- zagrożenia dostępności.

W celu uporządkowania i usystematyzowania omawianych zagadnień związanych z występowaniem ryzyk, na potrzeby niniejszej pracy wprowadza się dwie 7-mio stopniowe skale Likerta [Skulimowski, Banuls, 2021], prawdopodobieństw materializacji oraz intensywności oddziaływania zagrożenia (wielkości potencjalnych strat) i zdefiniowane w [Skulimowski, Banuls, 2021].

Tab. 3. Skale Likerta dla oceny poziomów ryzyka, prawdopodobieństw materializacji ryzyka oraz poziomów intensywności oddziaływania zagrożeń.

Poziom ryzyka, prawdopo-dobieństwo materializacji ryzyka	wyklu-czone	bardzo niskie	niskie	średnie	wysokie	bardzo wysokie	pewność zajścia
Kwantyfikacja poziomu ryzyka dla obliczeń ilościowych	0	10%	30%	50%	70%	90%	100%
Poziom intensywności oddziaływania zagrożenia	zerowy	Możli-wość użytko-wania bez przerwy	Możli-wość użytko-wania, drobna naprawa	Znisz-czenie wyłącza-jące z ruchu, naprawa bieżąca	Znisz-czenie wyłącza-jące z ruchu, drobna naprawa	Zniszcze-nie wyłą-czające z ruchu, kwalifi-ka-cja: remont generalny	Całkowi-te znisz-czenie
Kwantyfikacja poziomu intensywności oddziaływania zagrożenia	0	0,1	0,3	0,5	0,7	0,9	1

Analiza ryzyk [P.1] uwzględniająca zakres obserwacji i ochronę fizyczną jako aspekty wpływające wprost na wskazane powyżej zagrożenia, prowadzona była w KWC do tej pory w oparciu o weryfikację warunków bezpieczeństwa poprzez odpowiedzi na zestaw pytań, których celem było uwzględnienie w sposób obiektywny uwarunkowań środowiskowych,

technicznych, organizacyjnych i proceduralnych. Przykład takiego kwestionariusza zaprezentowany jest poniżej [Rys. 8].

GRUPA TAURON WSPARCIE	**Pełna ocena stanu bezpieczeństwa obiektu** Kwestionariusz wer.01		
Nazwa obiektu:	Ochrona Fizyczna , Perymetr obiektu		
Spółka:	Kopalnia Wapienia "Czatkowice" Sp. z o.o.		
Adres:	Krzeszowice ul. Czatkowice Dolne 75		
Lokalizacja GPS geog.	50° 9'17.38"N , 19°37'51.84"E		
Wykonał:	Cezary Jarmuszkiewicz	Data:	25.11.2019r.
Sprawdził:	Mariusz Kwarciak	Data:	25.11.2019r.

Lp.	Pytanie	Odpowiedź
1. Region, miejscowość, sąsiedztwo		
1.1.	Czy wskaźnik bezrobocia w regionie jest mniejszy niż średnia ogólnopolska?	1
1.2.	Czy wskaźnik przestępczości w regionie jest niższy niż średnia ogólnopolska?	1
1.3.	Czy wskaźnik wykrywalności przestępstw w regionie jest wyższy niż średnia ogólnopolska?	1
1.4.	Czy wskaźnik bezrobocia w mieście jest mniejszy niż średnia w regionie?	1
1.5.	Czy wskaźnik przestępczości w mieście jest niższy niż średnia w regionie?	1
1.6.	Czy wskaźnik wykrywalności przestępstw w miescie jest wyższy niż średnia w regionie?	1
1.7.	Czy obiekt jest położony w tzw. dobrej dzielnicy?	0
1.8.	Czy obiekt jest dobrze widoczny ze wszystkich stron ?	0
1.9.	Czy obiekt sąsiaduje z innymi chronionymi obiektami ?	0
1.10.	Czy czas dojazdu policji jest krótszy niż 10 min?	1
1.11.	Czy są alternatywne drogi dojazdu do obiektu?	1
1.12.	Czy sąsiadujący teren jest dobrze oświetlony?	0
1.13.	Czy sąsiedztwo obiektu jest dobrze widoczne dla obsługi?	0
	Razem	8
2. Ogrodzenie zewnętrzne i wygrodzenia wewnętrzne		
	Ogrodzenie zewnętrzne	
2.1.	Czy teren jest ogrodzony?	1
2.2.	Czy wysokość ogrodzenia jest większa niż 1,80m?	1
2.3.	Czy ogrodzenie jest kompletne?	0
2.4	Czy ogrodzenie jest niezniszczone?	0
2.5	Czy ogrodzenie podwyższone jest drutem kolczastym?	0
2.6	Czy możliwość pokonania ogrodzenia z przyległych zabudowań / konstrukcji jest zabezpieczona?	0
	Bramy	
2.7	Czy w obiekcie są zamykane lub kontrolowane przez obsługę bramy zewnętrzne?	1
2.8	Czy bramy są sprawne?	1
2.9	Czy bramy są niezniszczone?	1
2.10	Czy wysokość bramy jest większa niż 1,80m?	1
2.11	Czy brama jest podwyższona? (drutem kolczastym , kolcami)	0
2.12	Czy brama zabezpieczona jest elektronicznie?	0
2.13	Czy brama jest zamykana automatycznie ?	1
2.14	Czy jest zainstalowany zamek (jeśli brama nie jest automatyczna)?	N/D
2.15	Czy zamek jest atestowany?	N/D
2.16	Czy brama jest zamykana na kłódkę (jeśli brama nie jest automatyczna)?	N/D
2.17	Czy kłódka jest atestowana?	N/D
2.18	Czy zastosowany jest system Master Key?	N/D

Rys. 8. Fragment kwestionariusza oceny ryzyka [P.1]

Ten typ podejścia wydaje się być właściwy dla rozległych obiektów o charakterze przemysłowym, ponieważ uwzględnia szereg aspektów indywidualnych dla badanego podmiotu, a kolejne kroki i pytania doprecyzowują oceniany (badany) obszar. Jako przykład powyższej argumentacji można omówić potencjalny wpływ lokalizacji zakładu na wynik analizy. I tak, począwszy od pytań o charakterze bardzo ogólnym i właściwym dla otoczenia badanego obiektu tj. np. wskaźnik bezrobocia, wskaźnik przestępczości, sąsiedztwo czy czas dojazdu służb interwencyjnych, przechodzimy do analizy sposobu zabezpieczenia obiektu:

ogrodzenia, bramy, sposoby ich zamykania (w tym takie istotne szczegóły jak automatyzacja czy używanie systemu MasterKey), by wreszcie określić możliwości dostępu do konkretnego budynku czy też jego oświetlenia. W dalszej kolejności analizowane są zabezpieczenia mechaniczne i techniczne (w szerokim spektrum szczegółowości), a na zakończenie możliwość reakcji (w tym jej szybkość i skuteczność) oraz podejście formalne, czyli posiadanie stosownych procedur i scenariuszy działania. Tego typu podejście pozawala przenalizować całą ścieżkę potencjalnego materializowania się zagrożenia, analizę jego przebiegu i rozwoju oraz wskazuje potencjalne możliwości jego rozwiązania lub punkty przerwania łańcucha następujących po sobie zdarzeń.

Analiza odpowiedzi polega na obliczeniu procentowego udziału odpowiedzi „nie" (p_i) lub „tak" ($1-p_i$) w każdym z analizowanych działów. Tym samym analiza odpowiedzi na przygotowane wg tego scenariusza pytania ankietowe pozwala w prosty sposób określić poziom ryzyka, poprzez wartość p_i. Wektor $(p_1,\ldots p_n)^T$ nazywać będziemy *wektorem ryzyka*. Istotność statystyczna udziału odpowiedzi negatywnych we wszystkich zadanych pytaniach zależy od łącznej ilości wszystkich pytań w każdym z działów. Na potrzeby dotychczasowych analiz przyjęto minimalny poziom referencyjny liczby pytań w dziale 9, przy liczbie działów 8, przy czym najbardziej rozbudowana grupa pytań liczy ich aż 49 w jednym dziale. Opisany wyżej sposób ilościowej charakterystyki ryzyk przemysłowych przedstawiony jest jako Algorytm 2.1 niżej. Sprawdzał się on w przypadku tradycyjnego, kwestionariuszowego zbierania informacji, na ogół nie częściej niż dwa razy w roku.

Algorytm 2.1 - oszacowanie ryzyka na podstawie badań kwestionariuszowych.

Krok 1. Przygotowanie formularza z uwzględnieniem: obszaru objętego badaniem, zakresu, celu, a także ewentualnych informacji dodatkowych wynikających ze specyfiki i unikalności badanego obszaru.

Krok 2. Wybór respondentów badania zgodnie z zasadą, że każdy obszar reprezentowany jest przez osobę/osoby będące ekspertami dziedzinowymi w danym obszarze oraz co najmniej jedna osoba sprawuje nadzór całościowy nad wszystkimi obszarami objętymi badaniem.

Krok 3. Przeprowadzanie badania na drodze wypełnienia formularzy przez wybrane do udziału osoby.

Krok 4. Zebranie i analiza wyników, obliczenie wskaźników procentowych zgodnie z przygotowanym w kroku 1 formularzem.

Krok 5. Ocena zebranych danych i ich analizy przez eksperta dziedzinowego.

Jeżeli wynikiem oceny jest konieczność uzupełnienia danych **Przejście do Kroku** 2

Jeżeli wynikiem oceny jest konieczność uzupełnienia analizy danych **Przejście do Kroku** 4

Krok 6. Ustalenie priorytetów ryzyk zgodnie z wynikami. ■

W przypadku oceny ryzyka online opartego na analizie dużej ilości danych, np. na potrzeby projektowanego IRM DSS, konieczne jest zastosowanie metod ilościowej oceny ryzyk bardziej zawansowanych teoretycznie i obliczeniowo. Poniżej podajemy przegląd dotychczasowych metod oraz własną propozycję metody dostosowanej do uwarunkowań działalności KWC.

Istnieje wiele różnego rodzaju modeli matematycznych formalizujących intuicyjne pojęcie ryzyka finansowego. Zdecydowana większość z nich oparta jest na wykorzystaniu rozkładu prawdopodobieństwa zysku (straty) rozważanego jako funkcja jednego lub wielu tzw. czynników ryzyka, przy czym ryzyko odnoszone jest do odchylenia pomiędzy wartością oczekiwaną zysku (lub straty) a możliwą wartością rzeczywistą. W praktyce jako miarę ryzyka rozważa się najczęściej pewną charakterystykę powyższego rozkładu, np. kilka początkowych momentów, zwłaszcza odchylenie standardowe i skośność. Powszechnie znane są modele ryzyka związane z ryzykiem kursu papierów wartościowych, czy cen surowców, gdzie ryzyko utożsamiane jest z odchyleniem standardowym kursów obliczanym na pewnym przedziale czasowym, jak np. w modelu ryzyka portfelowego Markowitza.

Ryzyko związane ze zmianami kursów finansowych jest najpowszechniej uświadamianym w codziennej działalności przedsiębiorstw, zwłaszcza zajmujących się eksportem [Vince, 1992]. Jest rodzajem ryzyka jednocześnie najgłębiej zbadanym od strony teoretycznej oraz jednym z najtrudniejszym do oszacowania w praktyce. W działalności gospodarczej przedsiębiorstw występują także inne rodzaje ryzyk finansowych, których modele teoretyczne są wciąż niedoskonałe, natomiast w zamian stosowane są rozbudowane heurystyczne procedury monitoringu tych ryzyk. Empiryczne miary ryzyka finansowego stosowane w miejsce charakterystyk rozkładów prawdopodobieństw związane są raczej z pomiarem czynników ryzyka niż z właściwym zarządzaniem ryzykiem, czego przykładem są metody oszacowania niedopasowania aktywów i pasywów, np. metodą luki. Metoda ta i wiele innych metod empirycznych opiera się na założeniu, że nieznana funkcja estymująca ryzyko globalne jest monotoniczna ze względu na miarę każdego z pojedynczych czynników ryzyka. Pozwala to na zastąpienie zadania (minimalizacji) ryzyka przez optymalizację jego mierzalnych czynników. Analiza wieloczynnikowego modelu ryzyka, szczególnie gdy poszczególne czynniki mają zupełnie odmienny charakter, wymaga oszacowania ryzyka globalnego w wybranej chwili t_0, z horyzontem czasowym τ, które może być przedstawione wzorem (2.1):

$$R_G(t_0, \tau) := sup\{\mathrm{E}(S(1),...,S(n)), t_0, t), 0 \le t \le \tau\} \quad (2.1)$$

gdzie $\mathrm{E}(S(1),...,S(n), t_0, t)$ oznacza wartość oczekiwaną straty v w chwili $t_0 + t$ generowanej przez czynniki ryzyka $S(1),...,S(n)$. Tego typu formalizacja ryzyka będzie pomocna dla całościowej oceny kondycji finansowej przedsiębiorstwa.

Połączenie w ramach jednego systemu zarządzania ryzykiem zarówno ryzyk finansowych, jak i przemysłowych nie jest działaniem standardowym i stanowi wyzwanie natury metodologicznej ze względu na odmienne dotychczas metody pomiaru, analizy i zarządzania tymi ryzykami. Z drugiej strony, objęcie jednym zintegrowanym systemem zarządzania wszystkich, lub prawie wszystkich rodzajów ryzyk występujących w przedsiębiorstwie, może w znaczący sposób zwiększyć atrakcyjność systemu zarządzania ryzykiem klasy ERMS.

2.4 Identyfikacja zagrożeń

Jak wspomnieliśmy, intruzje były do tej pory najczęściej odnotowywanymi incydentami bezpieczeństwa w KWC, lecz oprócz tego oczywistego i powszechnego zagrożenia istnieją jeszcze inne istotne czynniki ryzyka wynikające z zagrożeń zarówno o charakterze antropogenicznymi, jak i naturalnym, a także będące wynikiem synergii pomiędzy działalnością człowieka, a naturalnymi procesami w otoczeniu fizycznym. Przesłanki te wskazują na konieczność wdrożenia w KWC nowoczesnego i holistycznego systemu zarządzania bezpieczeństwem wykorzystującego nowoczesne technologie informacyjne oraz metody i techniki wspierane przez algorytmy sztucznej inteligencji. Systemy informatyczne o takich właściwościach określane są ogólnie jako systemy wspomagania decyzji zarządzania bezpieczeństwem przemysłowym. Systemy tej klasy posiadać mogą również funkcjonalności systemów zarządzania ryzykiem korporacyjnym (Enterprise Risk Management Systems [Shin i in., 2019]) – ukierunkowanych głownie na ryzyka finansowe oraz zagrożenia katastrofami naturalnymi (*Disaster Resilience Management Support Systems*, - DReMSS [Skulimowski, Banuls, 2021; Dahal i in., 2020; Comes i in., 2010; Hasan i in., 2019]). DReMSS stanowią odrębną klasę specjalistycznych systemów wspomagania decyzji zapewniających - wespół z zarządzaną infrastrukturą - maksymalną odporność na zagrożenia naturalne, która implementowana jest na poziomie jednostek administracyjnych, w tym obszarów i instytucji tworzonych pod kątem potrzeb związanych z zarządzaniem kryzysowym w sytuacji wybranych (np. RZGW) lub ogólnych ryzyk i zagrożeń (np. wojewódzkie Wydziały Bezpieczeństwa i Zarządzania Kryzysowego). W zakładach przemysłowych, gdzie występuje potrzeba zarządzania zagrożeniami naturalnymi we własnym zakresie, a nie tylko przy pomocy służb publicznych, należy przewidzieć zarówno odpowiednie instrumenty, jak i procedury decyzyjne, które będą zaimplementowane w IRM DSS. W KWC system wspomagania decyzji dla utrzymania bezpieczeństwa przemysłowego docelowo powinien umożliwiać zarządzanie wszystkimi zidentyfikowanych dotąd grupami zagrożeń, w tym także związanych z katastrofami naturalnymi.

Rys. 9. Schemat zależności ryzyk, wywołanych nimi zagrożeń, sposobów detekcji i systemów przeciwdziałania tym ryzykom w KWC.

W tym miejscu należy zwrócić uwagę, że przedstawione wcześniej [Rys. 2] i [Rys. 9] chociaż różnią się zakresem i celem, są wzajemnie uzupełniające. Pierwszy z nich [Rys. 2], który przedstawia wzajemne relacje w formie grafu przyczynowo-skutkowego, dostarcza podstaw teoretycznych i analitycznych dla zrozumienia, co wpływa na bezpieczeństwo w organizacji. Pozwala on na identyfikację źródeł ryzyka, ocenę ich znaczenia oraz zaplanowanie działań prewencyjnych. Z kolei drugi rysunek [Rys. 9] ma charakter bardziej praktyczny, skupia się bardziej na operacyjnych aspektach bezpieczeństwa, zwracając uwagę na konkretne typy ryzyk, zagrożeń i metod ich identyfikacji. Wskazuje też konkretne mechanizmy detekcji i reakcji na zagrożenia z uwzględnieniem specyfiki przedsiębiorstwa, czy innych unikalnych uwarunkowań właściwych dla analizowanego przypadku. Schemat ten ma strukturę hierarchiczną, gdzie zagrożenia prowadzą do określonych ryzyk, a te są powiązane z odpowiednimi metodami detekcji.

Połączenie obu podejść pomaga w zrozumienie analizowanych zagadnień i stworzeniu modelu zintegrowanego systemu bezpieczeństwa, który uwzględnia zarówno strategiczne planowanie, jak i praktyczne narzędzia do monitorowania i zarządzania zagrożeniami.

W tabeli 4 zestawiono kluczowe aspekty, które należy brać pod uwagę, projektując model systemu klasy IRM DSS z odniesieniem ich relacji i wzajemnych odniesień.

Tab. 4. Relacje pomiędzy czynnikami wpływającymi na bezpieczeństwo a rzeczywistymi zależnościami ryzyk.

Aspekt	**Czynniki wpływające na bezpieczeństwo**	**Zależności ryzyk, zagrożeń i detekcji**
Cel	Identyfikacja i analiza fundamentalnych elementów wpływających na bezpieczeństwo	Operacyjne monitorowanie i zarządzanie zagrożeniami oraz ryzykami
Zakres	Ogólne podejście uwzględniające procesy i strategie prewencyjne	Konkretne zagrożenia, ryzyka i technologie detekcji
Relacje	Przyczynowo-skutkowe między elementami	Powiązania między zagrożeniami a ryzykami i metodami detekcji
Struktura	Graf systemowy z relacjami wielokierunkowymi	Diagram hierarchiczny lub sieć zależności
Zastosowanie	Strategiczne planowanie działań prewencyjnych	Operacyjne zarządzanie ryzykiem i reakcją na zagrożenia

Rodzaje zagrożeń zidentyfikowanych do tej pory można podzielić grupy i zastosować gradację ich wpływu na sposób postępowania w przypadku ich zaistnienia, por. Tab. 5. Wskazane rodzaje zagrożeń obrazują potencjalny ich wpływ na bezpieczeństwo:

- osób, w szczególności pracowników, ale również klientów i osób odwiedzających,
- majątku trwałego oraz ruchomego, w tym w szczególności maszyn górniczych,
- systemów i urządzeń elektronicznych oraz danych przetwarzanych w tych systemach (szeroko rozumiane cyberbezpieczeństwo),
- utrzymania pozytywnego wizerunku przedsiębiorstwa w otoczeniu lokalnym oraz szerszym.

Tab. 5. Zidentyfikowane rodzaje zagrożeń występujących w KWC

Rodzaje zagrożeń	Zagrożenia i czynniki ryzyka występujące w KWC	Znaczenie dla KWC	Sposób monitorowania	Zarządzanie przez IRM DSS
I. Zagrożenia typu ***safety***	(i) Zagrożenia osuwiskowe [P.1]: - spękania i nachylenia zagrażające odspajaniem mas skalnych, - przewarstwienia, - uskoki, - zjawiska krasowe, - strefy drgań będących, następstwem robót strzałowych oraz ruchu maszyn ciężkich.	Bardzo duże	Kamery na pojazdach górniczych i dronach, rejestracja drgań	TAK, mapa ryzyka z obiektami charakterystycznymi (szczeliny, obszary o mniejszej wytrzymałości na obciążenia)

Rodzaje zagrożeń	Zagrożenia i czynniki ryzyka występujące w KWC	Znaczenie dla KWC	Sposób monitorowania	Zarządzanie przez IRM DSS
	(ii) Obrywanie się skał wynikające z budowy geologicznej złoża i robót strzałowych.	Duże	Badania naprężeń górotworu. Badania fotogrametryczne przy pomocy dronów, badania reakcji na obciążenia przy pomocy robotów inspekcyjnych	TAK, mapa ryzyka
	(iii) Zalania terenu Kopalni przez ulewne deszcze.	Średnie do dużego	Prognozy opadowe, kamery stacjonarne, rejestracja poziomu wody w wybranych lokalizacjach	TAK, odrębny moduł (przydział zasobów)
	(iv) Zagrożenia wodne spowodowane drenażem kanałów krasowych.	Średnie	Kamery na pojazdach górniczych i dronach, rejestracja poziomu wody w wybranych lokalizacjach	TAK
	(v) Pożary budynków lub maszyn Kopalni (niespowodowane działaniami umyślnymi).	Średnie	Czujniki dymu i temperatury zintegrowane w System Sygnalizacji Pożaru (SSP)	TAK, odrębny moduł (przydział zasobów w przypadku wielu jednoczesnych zagrożeń
II. Zagrożenia typu ***security***	(i) Świadome uszkodzenie mienia poprzedzone intruzją, w tym działania sabotażowe i akty wandalizmu. (ii) Przypadkowe uszkodzenie mienia, w tym na skutek wypadków przy pracy. (iii) Przypadki kradzieży (np. paliwa, złomu, kabli) poprzedzone intruzją. (iv) Wypadki przy pracy.	Duże	System monitoringu, pracownicy ochrony zakładu	Tylko rejestracja w bazie zdarzeń
III. Zagrożenia systemów informatycznych **(*cybersecurity*)**	(i) Próby ataków informatycznych z systemów zewnętrznych. (ii) Nieautoryzowany dostęp do danych przez nieuprawnionych pracowników. (iii) Narażanie danych na utratę. (iv) Instalacja potencjalnie niebezpiecznego	Średnie	Audyty bezpieczeństwa systemów informatycznych	NIE, (w KWC stosowane są odrębne systemy dedykowane do zarządzania cyberbezpieczeństwem)

Rodzaje zagrożeń	Zagrożenia i czynniki ryzyka występujące w KWC	Znaczenie dla KWC	Sposób monitorowania	Zarządzanie przez IRM DSS
	oprogramowania przez pracowników i kontrahentów.			
IV. Zagrożenia mające wpływ na wizerunek przedsiębiorstwa	(i) Działania radykalnych grup ekologicznych. (ii) Wypadki z udziałem osób. (iii) Zdarzenia zagrażające środowisku naturalnemu. (iv) Brak dostępności produktów handlowych z oferty KWC.	Małe	Okresowe analizy	NIE, CZĘŚCIOWO (rejestracja zdarzeń w bazie wiedzy) CZĘŚCIOWO (rejestracja zdarzeń w bazie wiedzy), NIE
V. Zagrożenia biznesowe i finansowe	(i) Utrata płynności. (ii) Utrata wartości posiadanych papierów wartościowych. (iii) Niewypłacalność kontrahentów. (iv) Brak kandydatów do pracy itp.	Średnie	Controlling, sprawozdawczość finansowa	Nie są rozważane w technicznej wersji DSS, ich znaczenie praktyczne było do tej pory znikome ze względu na zarządzanie finansami na poziomie holdingu w Grupie Tauron SA

2.5 Przykłady zagrożeń występujących w KWC

Na fotografiach niżej przedstawiono dokumentację procesu powstawania i ujawniania najczęściej spotykanych zagrożeń w KWC.

Rys. 10. Oderwanie się fragmentu ściany w rezultacie pęknięcia. Źródło: materiały własne KWC.

Rys. 11. Osuwisko. Źródło: materiały własne KWC.

Rys. 12. Prace na kliku kolejnych poziomach eksploatacyjnych. Źródło: materiały własne KWC.

Rys. 13. Osiadająca na dolnych poziomach eksploatacyjnych mgła zwiększająca ryzyko kolizji i wypadków przy pracy. Źródło: materiały własne KWC.

Rys. 14. Najniższy poziom Kopalni po okresie silnych opadów.
Źródło: fotografie wykonane dla KWC.

Rys. 15. Rozlewiska w trakcie roztopów. *Źródło*: materiały własne KWC.

Każde ze wskazanych zagrożeń ma źródło w innym rodzaju ryzyk oraz niesie z sobą inne prawdopodobieństwo materializacji. Określenie poziomu zagrożeń mających bezpośredni wpływ na poszczególne grupy aktywów narażonych na stratę jest przyczyną wykorzystania systemów wspomagania decyzji opartych o metody analizy wielokryterialnej [McCallum i in., 2016], [Sepulveda, Bull, 2019], co zostanie szczegółowo omówione dalej. Szacunkowa częstotliwość występowania pokazanych powyżej zagrożeń zaprezentowana została w [Tab. 6].

Tab. 6. Zestawienie zagrożeń, częstotliwości ich występowania i zakresu obszarowego.

Zagrożenie	Szacunkowa częstotliwość występowania (w roku)	Względna wielkość zagrożonego terenu [%]
Pęknięcie na krawędzi ściany	1	5
Osuwisko	4	5
Prace na kliku kolejnych poziomach eksploatacyjnych	24	10
Osiadająca na dolnych poziomach eksploatacyjnych mgła	12	40
Zalanie na skutek intensywnych opadów atmosferycznych	2	70
Zalanie najniższych poziomów eksploatacyjnych (roztopy)	2	50

W trakcie przeprowadzonej w roku 2019 oceny stanu bezpieczeństwa obiektu [P.1], która wciąż zachowuje aktualność, analizie poddano grupy czynników wpływających bezpośrednio

na ochronę fizyczną (*security*) oraz perymetr obiektu. Ocenę tę wykonano wg standaryzowanego schematu (formularz audytu bezpieczeństwa zawierającego 227 szczegółowych pytań dotyczących poziomu bezpieczeństwa najważniejszych obszarów zagrożeń oraz ich uwarunkowań zewnętrznych). Podsumowanie oceny określa całościowy poziom bezpieczeństwa jako wynik badania wpływu czynników, wśród których są zarówno zagrożenia, jak i zabezpieczenia. Ocena stanu bezpieczeństwa obiektu zawarta w opracowaniu [P.1] przygotowana została w oparciu o obwiązujące w Grupie Kapitałowej Tauron (GKT) wytyczne i regulacje. Pierwotna metodyka analizy powstała w spółce Wsparcie Grupa Tauron (WGT), niemniej jednak została dostosowana do specyfiki KWC. Metodyka ta bazuje na ocenie zagrożeń wynikających z otoczenia obiektu, specyfiki funkcjonowania (np. zmianowość i tryb pracy), rodzaju wykorzystywanego sprzętu i jego podatności na zagrożenia zewnętrzne oraz sposobu i rodzaju wykorzystania środków technicznych podnoszących poziom bezpieczeństwa obiektu. Co ważne, analiza przeprowadzona została z udziałem właścicieli poszczególnych ryzyk, a wachlarz pytań i badanych aspektów pozwalał na wieloaspektowe rozeznanie badanego zagadnienia.

Tab. 7. Zestawienie zagrożeń i wpływ wpływających na nie czynników wg badania [P.1], opracowanie własne.

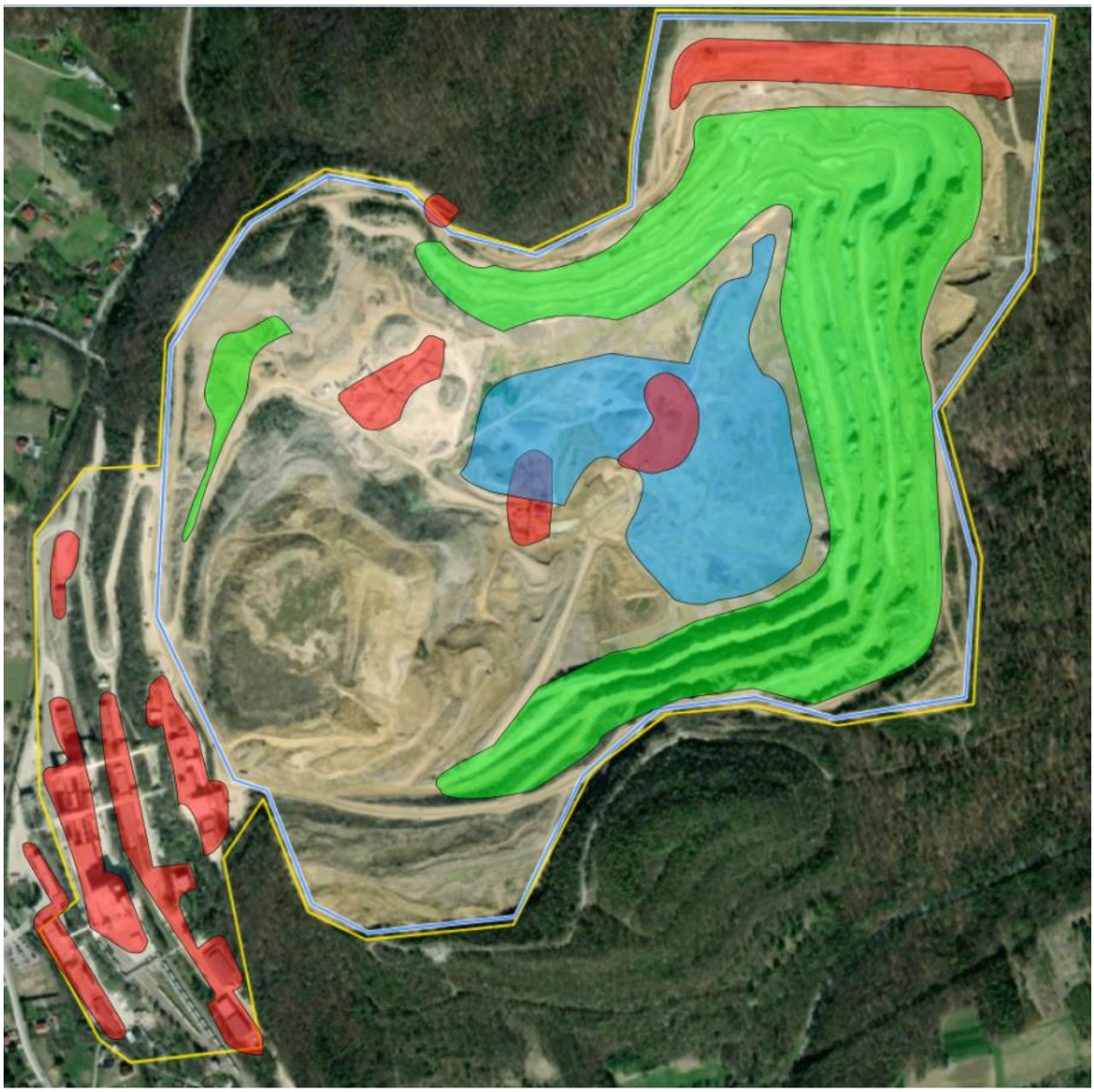
Lp.	Zidentyfikowane czynniki zagrożeń	Wybrane elementy uwzględnione w analizie	Wartość p_i (%)	Korelacja z Tabela 2 w zakresie klasyfikacji rodzaju zagrożenia
1	Region, miejscowość, sąsiedztwo	Przestępczość w regionie, wskaźnik bezrobocia, widoczność i położenie obiektu, sąsiedztwo, czas dojazdu.	38 %	II. Zagrożenia typu *security* IV. Zagrożenia mające wpływ na wizerunek przedsiębiorstwa
2	Procesy geologiczne na obszarze eksploatacji i w jego otoczeniu	Przewarstwienia, uskoki, zjawiska krasowe, spękania i nachylenia.	Nie dotyczy	I. Zagrożenia typu safety II. Zagrożenia typu security IV. Zagrożenia mające wpływ na wizerunek przedsiębiorstwa
3	Czynniki atmosferyczne	Ulewne deszcze, osuwiska.	Nie dotyczy	I. Zagrożenia typu safety II. Zagrożenia typu security IV. Zagrożenia mające wpływ na wizerunek przedsiębiorstwa
4	Ogrodzenie zewnętrzne i wygrodzenia wewnętrzne,	Ogrodzenie, kompletność (ciągłość) ogrodzenia, bramy ich stan i sposoby zabezpieczenia, oświetlenie.	44 %	II. Zagrożenia typu *security* IV. Zagrożenia mające wpływ na wizerunek przedsiębiorstwa
5	Zabezpieczenia elektroniczne	Systemy monitoringu wizyjnego, systemy sygnalizacji włamania i napadu, systemy sygnalizacji pożarowej zintegrowane w System Sygnalizacji Pożaru (SSP)	71 %	II. Zagrożenia typu *security* III. Zagrożenia systemów informatycznych (*cybersecurity*) IV. Zagrożenia mające wpływ na wizerunek przedsiębiorstwa

Lp.	Zidentyfikowane czynniki zagrożeń	Wybrane elementy uwzględnione w analizie	Wartość p_i (%)	Korelacja z Tabela 2 w zakresie klasyfikacji rodzaju zagrożenia
6	Monitoring zagrożeń	Integracja systemów zabezpieczeń elektronicznych, sposób obsługi i sygnalizacji stanów alarmowych.	Nie dotyczy	I. Zagrożenia typu safety II. Zagrożenia typu security
7	Ochrona fizyczna (OF)	Organizacja pracy, dostępność patroli, informacja dla osób postronnych	4 %	I. Zagrożenia typu safety II. Zagrożenia typu security
8	Procedury bezpieczeństwa	Posiadanie formalnych procedur i regulacji, znajomość procedur przez pracowników OF	14 %	I. Zagrożenia typu safety II. Zagrożenia typu security III. Zagrożenia systemów informatycznych (*cybersecurity*) IV. Zagrożenia mające wpływ na wizerunek przedsiębiorstwa
9	Organizacyjne aspekty bezpieczeństwa, w tym procedury wspomagania i podejmowania decyzji	Budowa poczucia odpowiedzialności pracowników za bezpieczeństwo, prowadzenie analiz i szkoleń	29 %	I. Zagrożenia typu safety II. Zagrożenia typu security III. Zagrożenia systemów informatycznych (*cybersecurity*) IV. Zagrożenia mające wpływ na wizerunek przedsiębiorstwa

Dla przykładu, własna analiza przeprowadzona ostatnio w ramach programu badań doktorskich jako podstawa dla analizy potrzeb dotyczących planowanego IRM DSS, wykazała pozytywne wskaźniki dla 3 grup czynników zagrożeń, a 2 z nich znalazły się poniżej poziomu akceptowalnego. Ocena bezpieczeństwa obiektu całościowo otrzymała poziom tolerowalny ok. 69 % [P.1], a ryzyko na poziomie 31%.

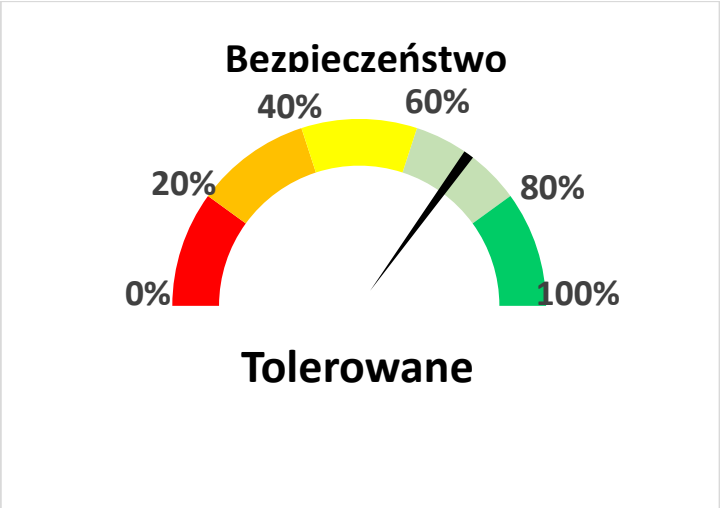
2.6 Specyficzne rodzaje zagrożeń dla Obszaru Górniczego w KWC

Widok Obszaru Górniczego KWC z częścią produkcyjną przedstawiony i oznaczony kolorem żółtym (obwód około 5,4 km) na [Rys. 16], natomiast sam Obszar Górniczy oznaczono kolorem niebieskim (obwód około 4,3 km).



Rys. 16. Zdjęcie lotnicze KWC z oznaczonymi mapami ryzyk. *Źródło* fotografie wykonane dla KWC.

Ogólna analiza zagrożeń [P.1], obejmująca zagrożenia naturalne i antropogeniczne, przeprowadzona dla poszczególnych grup ryzyk szczegółowo wskazanych w tabelach w dalszej części niniejszego rozdziału, przedstawiona jest na [Rys. 16]. Kolorami oznaczono odpowiednio ryzyka naturalne: niebieski (zalania) i zielony (osunięcia), ryzyka antropogeniczne: czerwony (intruzje – kradzież i sabotaż).



Rys. 17. Wykres obrazujący całościowy poziom ryzyka KWC bez Obszaru Górniczego – stan na koniec roku 2019. *Źródło*: [P.1].

W przedstawionej na powyższym rysunku analizie zagrożeń i oceny stanu bezpieczeństwa obiektu nie został uwzględniony Obszar Górniczy (OG) część przedsiębiorstwa, gdzie prowadzona jest eksploatacja i wstępny przerób surowca potencjalnie obszar o największym znaczeniu dla analizy zagrożeń. Wynika to z faktu, że OG aż do chwili obecnej został w niewielkim stopniu objęty procedurami bezpieczeństwa, głównie ze względów technologicznych i na skutek tego wynik oceny poziomu ryzyka całego przedsiębiorstwa byłby niemiarodajny. Ponadto Obszar Górniczy charakteryzuje się dużymi różnicami względnymi wysokości terenu, niezabezpieczonymi uskokami oraz zagrożeniami osuwiskami. Ze względu na specyfikę i nasilenie zagrożeń, a także konieczność znalezienia odpowiedniego rozwiązania technologicznego dla kompleksowego zarządzania zagrożeniami w KWC, OG wyłączony został do odrębnego uwzględnienia w IRM DSS. Badanie potrzeb w kontekście projektu IRM DSS dla KWC jest jednym z kluczowych aspektów poruszonych w pracy, a uzyskanie jego pełnej funkcjonalności dla całego obszaru, na którym prowadzona jest aktywność przemysłowa Spółki, jest również kluczowa z perspektywy funkcjonowania przedsiębiorstwa.

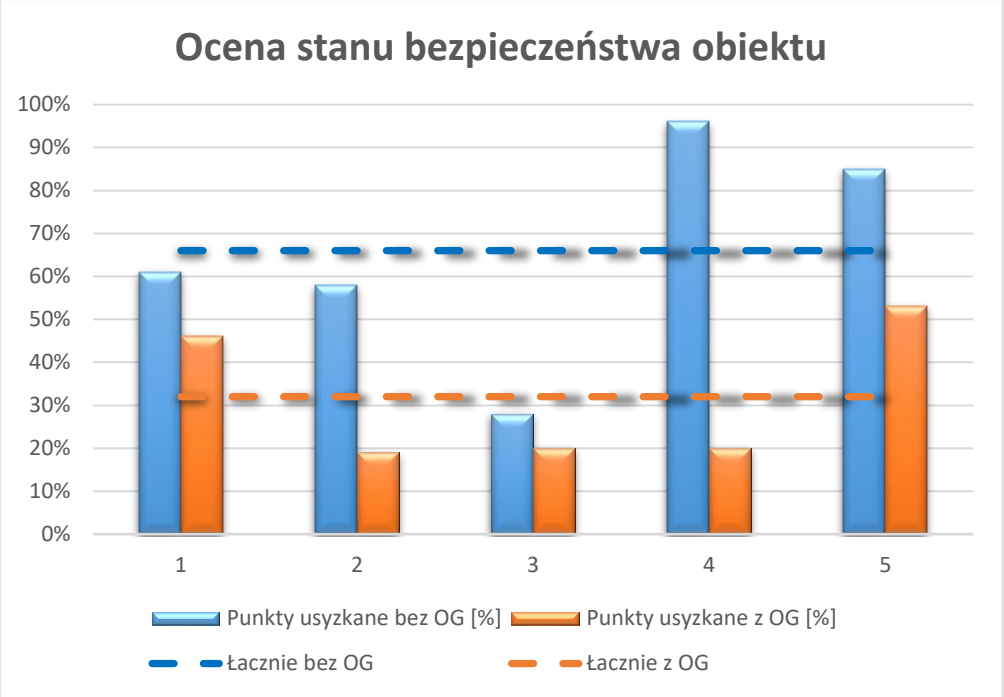
Wybrane obszary analizy ryzyk w KWC przedstawiono w Tab. 8, natomiast czynniki ryzyka związane z tymi obszarami, ich wpływ na wynik ogólny oceny ryzyka w KWC oraz zmiany poziomu ryzyka w zależności od sposobu podejścia do badanego zagadnienia przedstawia Tab. 9 i Rys. 18.

Tab. 8. Porównanie analizy ryzyk w KWC z pominięciem OG oraz symulacji uwzględniającej wpływ OG na ocenę ryzyka.

Lp.	**Obszar analizy ryzyk**	**Poziom bezpieczeństwa**		
		Ocena uzyskana bez OG [%]	**Ocena uzyskana wraz z OG [%]**	**Różnica [%]**
1	Region, miejscowość, sąsiedztwo	61%	46%	15%
2	Ogrodzenie zewnętrzne i wygrodzenia wewnętrzne	58%	19%	39%
3	Zabezpieczenia elektroniczne	28%	20%	8%
4	Ochrona fizyczna	96%	20%	76%
5	Aspekty organizacyjne	85%	53%	32%
	Wynik średni dla punktów 1-5	66%	32%	34%

Tab. 9. Czynniki wpływające na poziom badanego ryzyka w KWC.

Lp.	Czynnik mające wpływ na poziom ryzyka	Obszar analizy zgodnie z **Tabela 1**	Ocena wpływu na ryzyko KWC
1	Środowisko społeczne i otoczenie KWC	1	Niski
2	Dostępność służb interwencyjnych	1	Średni
3	Ogrodzenie zewnętrzne	2	wysoki
4	Bramy, furtki	2	wysoki
5	Oświetlenie i oznakowanie terenu	2	średni
6	Wykorzystanie Systemu Dozoru Wizyjnego (SDW)	3	średni
7	Kontrola dostępu	3	średni
8	Wykorzystanie Systemu Sygnalizacji Włamani i napadu (SSWiN)	3	średni
9	Dostępność ochrony fizycznej	4	wysoki
10	Stosowane procedury bezpieczeństwa	5	wysoki
11	Dostępność służb interwencyjnych	5	średni



Rys. 18. Ocena stanu bezpieczeństwa obiektu i symulacja uwzględniająca wpływ OG na wynik.

[Rys. 18] przedstawia w sposób zbiorczy porównanie ocen ryzyka uwzględniających czynniki z [Tab. 9] i pokazuje, jak na wynik końcowy poszczególnych obszarów analizy wpływa uwzględnienie Obszaru Górniczego.

Analizując powyższe dane, można wyciągnąć wniosek, że krytyczny z punktu widzenia bezpieczeństwa całego obiektu jest fakt rozległości terenu, na którym KWC prowadzi działalność, specyfika ukształtowania terenu i wynikający z niej ości ogrodzenia i poddania ciągłemu dozorowi. Obrazują to wartości punktów uzyskane dla obszarów analizy 2 i 4, zgodnie z [Tab. 9], gdzie odpowiednio spadek uzyskanych punktów jest z 58% na 19% i aż z 96% do 19% [Rys. 18]. Daje to mocne przesłanki ku temuby sądzić, że to właśnie te aspekty oraz brak możliwości objęcia Ochroną Fizyczną (OF) znacznej części chronionego obszaru w sposób znaczący wpłyną na globalny wskaźnik bezpieczeństwa dla KWC.

Metodyka i zakres przeprowadzanych dotychczas analiz nie obejmują szczegółowych aspektów działań związanych z Bezpieczeństwem i Higieną Pracy (BHP) oraz wybranych zagrożeń typu *safety*, które są one w mniejszym stopniu zależne od implementacji IRM DSS.

2.7 Analiza bezpieczeństwa procesów produkcyjnych KWC

Proces eksploatacji i przerobu pozyskanego surowca jest złożony, a zachowanie jego ciągłości jest uwarunkowane zapewnieniem bezpieczeństwa poszczególnym jego ogniwom (podprocesom, liniom technologicznym i maszynom). Poprzez bezpieczeństwo należy tu rozumieć w pierwszej kolejności głównie brak dostępu osób postronnych, które swym

działaniem celowym lub przypadkowym spowodować mogą uszkodzenia unieruchamiające maszyny. W skrajnym przypadku pod uwagę należy brać również działania sabotażowe np. aktywistów ekologicznych lub wybryki chuligańskie, które mogą skutkować zarówno przerwami w pracy ciągów technologicznych, a w dalszej konsekwencji również przerwaniem łańcucha dostaw sorbentu na potrzeby spółek energetycznych oraz stratami wizerunkowymi KWC, jako przedsiębiorstwa przyjaznego dla środowiska i otoczenia. Należy podkreślić, że wydobywany wapień jest surowcem całkowicie bezpiecznym ekologicznie, niestwarzającym zagrożeń dla zdrowia pracowników. W drugiej kolejności zapewnienie bezpieczeństwa dotyczyć będzie także innych czynników wpływających na zwiększenie awaryjności maszyn i niezawodności procesów technologicznych. Należy tu zaliczyć m.in.:

- części i materiały eksploatacyjne o parametrach niespełniających norm wymaganych dla poszczególnych maszyn,
- ryzyka operacyjne związane z zapewnieniem dostępności:
  - części zamiennych,
  - serwisów specjalistycznych,
  - wykwalifikowanego personelu technicznego,
  - właściwego zarządzania dostępnym parkiem maszynowym,
- utrzymanie zbilansowanego reżimu pracy zgodnego zarówno z harmonogramem dostaw (a dalej odbiorów) surowca, jak i harmonogramem okresowych przeglądów, i remontów.

Złożoność problemu zapewnienia bezpieczeństwa zakładu produkcyjnego o profilu górniczym może być zobrazowana poprzez analizę sposobu funkcjonowania KWC, który przedstawiony jest w dalszej części pracy.

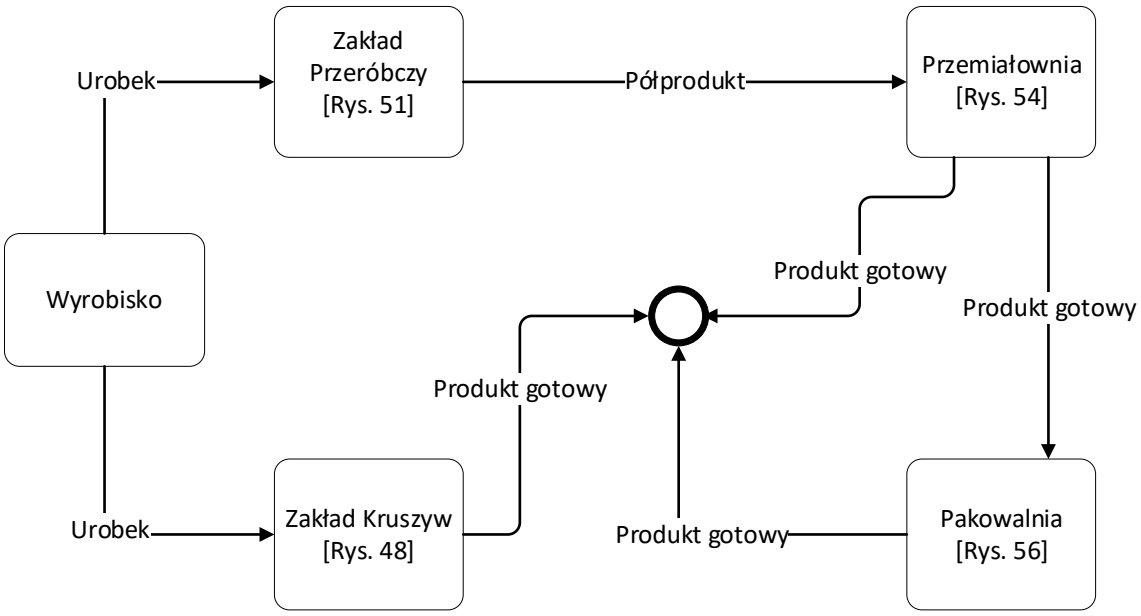
2.7.1 Analiza bezpieczeństwa procesów technologicznych

Układ technologiczny KWC składa się z procesów i podprocesów technologicznych. Są one podane w następującej tabeli:

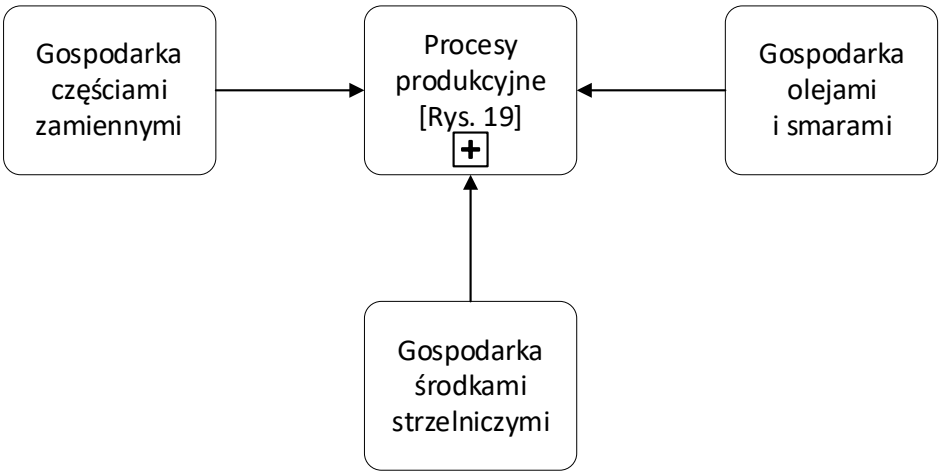
Tab. 10. Procesy i podprocesy technologiczne w KWC wraz ze stopniem zastosowania w nich ICT.

Lp.	Nazwa procesu	Maszyny i urządzenia	Technologie informacyjne, telekomunikacyjne i automatyka w procesie	Ocena obecnego stanu bezpieczeństwa procesu, Kwantyfikacja ryzyka zgodnie z [Tab. 3]
1.	Urabianie, załadunek i transport surowca	1. Koparka górnicza przedsiębierna 2. Koparka podsiębierna 3. Spycharka 4. Młot hydrauliczny na podwoziu koparki 5. Wozidło technologiczne 6. Ładowarka kołowa	- system wizyjnego monitoringu technologicznego, - system klasy ERP do zarządzania harmonogramem pracy, przeglądów, remontów itp. - system kontroli czasu pracy maszyny i bieżącego zużycia paliwa	Brak integracji pomiędzy wykorzystywanymi technologiami, zarządzanie decyzyjne odrębnie dla poszczególnych czynności. Materializacja ryzyka na poziomie 70%.
2.	Zakład Kruszyw	1. Ładowarka kołowa 2. Ciąg technologiczny, składający się kaskadowo połączonych maszyn i urządzeń pod nadzorem systemu automatyki przemysłowej.	- system wizyjnego monitoringu technologicznego, - system klasy ERP do zarządzania harmonogramem pracy, przeglądów, remontów itp. - system SCADA do nadzoru procesu produkcyjnego	Brak integracji pomiędzy wykorzystywanymi technologiami, mniejszy wpływ rozproszenia decyzyjnego. Materializacja ryzyka na poziomie 60%.
3.	Zakład Przeróbczy	Ciąg technologiczny, składający się kaskadowo połączonych maszyn i urządzeń pod nadzorem systemu automatyki przemysłowej. Ciąg posiada dwie niezależne nitki bazujące jednak na wspólnym buforze początkowym.	- system wizyjnego monitoringu technologicznego, - system klasy ERP do zarządzania, harmonogramem pracy, przeglądów, remontów itp. - system klasy SCADA do nadzoru procesu produkcyjnego	Brak integracji pomiędzy wykorzystywanymi technologiami, ciągły nadzór operatora. Materializacja ryzyka na poziomie 40%.
4.	Przemiało wnia	Ciąg technologiczny, składający się kaskadowo połączonych maszyn i urządzeń pod nadzorem systemu automatyki	- system klasy ERP do zarządzania harmonogramem pracy, przeglądów, remontów itp. - system klasy SCADA	Brak integracji pomiędzy wykorzystywanymi technologiami, ciągły nadzór operatora. Materializacja ryzyka na poziomie 30%.

Lp.	Nazwa procesu	Maszyny i urządzenia	Technologie informacyjne, telekomunikacyjne i automatyka w procesie	Ocena obecnego stanu bezpieczeństwa procesu, Kwantyfikacja ryzyka zgodnie z [Tab. 3]
		przemysłowej. Ciąg posiada 2 niezależne nitki, mogące pracować równocześnie lub zamiennie.	do nadzoru procesu produkcyjnego	
5.	Pakowalnia	Ciąg technologiczny, składający się kaskadowo połączonych maszyn i urządzeń.	- system klasy ERP do zarządzania harmonogramem pracy, przeglądów, remontów itp.	Proces niepowiązany wprost z pozostałymi, dopuszczalne przestoje, brak konieczności pełnej integracji. Materializacja ryzyka na poziomie 20%.



Rys. 19. Schemat zależności procesów produkcyjnych w KWC. Ryzyka kumulują się wzdłuż podprocesów sekwencyjnych.



Rys. 20. Procesy pomocnicze wpływające na zidentyfikowane ryzyka. Symbol „+" wskazuje odwołanie do rozwinięcia procesów produkcyjnych. Źródło: badania własne.

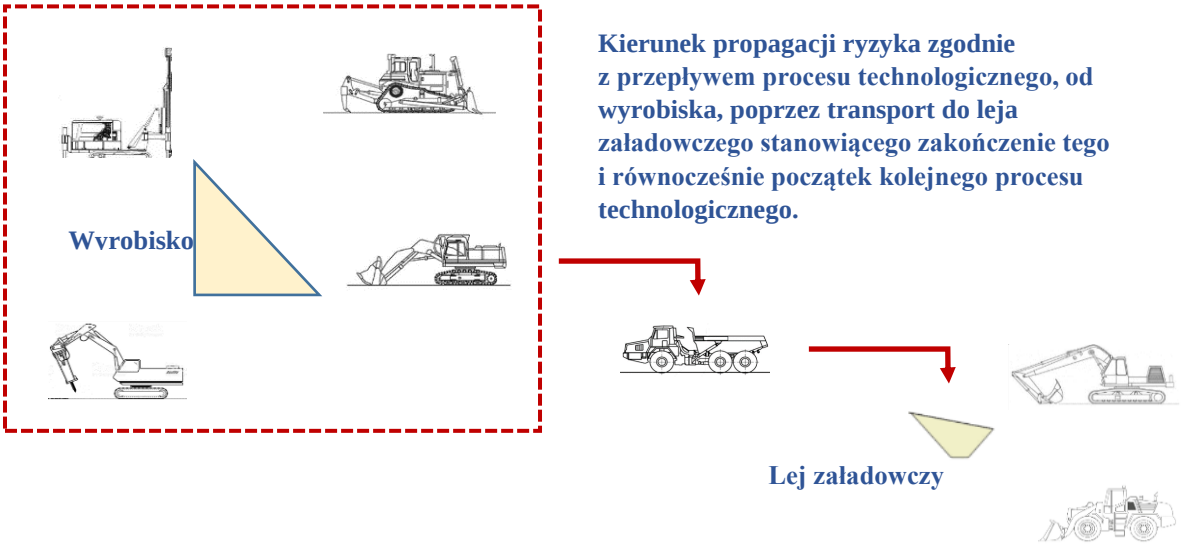
Procesy te opisane są szczegółowo niżej, a w [Tab. 11] podajemy rodzaje ryzyk dla poszczególnych komponentów procesów technologicznych w KWC.

Tab. 11. Komponenty procesów technologicznych przerobu, urabiania, załadunku i transportu surowca w KWC.

Typ maszyny	Ryzyka związane z danym typem maszyny	Dotychczasowy sposób zarządzania tym ryzykiem
Ciężkie maszyny górnicze	1. Przypadkowe uszkodzenie maszyny przez czynniki naturalne. 2. Przypadkowe awarie i wypadki, bądź działania świadome osób trzecich. 3. Akty wandalizmu. 4. Przypadki kradzieży części i podzespołów. 5. Niewłaściwy sposób zarządzania czasem pracy i dostępnością maszyny.	1. Monitoring technologiczny. 2. System ERP. 3. System kontroli czasu pracy i zużycia paliwa. 4. Systematyczne kontrole osób dozoru.
Pojazdy ogólnego przeznaczenia	1. Przypadkowe uszkodzenie maszyny przez czynniki naturalne na skutek awarii, wypadku, bądź działania świadome osób trzecich. 2. Akty wandalizmu. 3. Przypadki kradzieży. 4. Niewłaściwy sposób zarządzania czasem pracy i dostępności maszyny.	1. Monitoring technologiczny. 2. System ERP. 3. System kontroli czasu pracy i zużycia paliwa. 4. Systematyczne kontrole osób dozoru.
Dalsze komponenty, np. systemy pomiarowe, obiekty, budynki itp.	1. Uszkodzenia przez czynniki naturalne na skutek awarii, wypadku, bądź działania świadome osób trzecich. 2. Akty wandalizmu. 3. Przypadki kradzieży. 4. Niewłaściwy sposób zarządzania czasem pracy i dostępności maszyny.	1. Monitoring technologiczny. 2. System ERP. 3. Systemy SSWiN i SSP.

Ryzyka wskazane w [Tab. 11], są bezpośrednio związane z przykładami zagrożeń występujących na terenie KWC, które zostały ujęte w [Tab. 5].

2.7.2 Urabianie, załadunek i transport surowca



Rys. 21. Schemat procesu produkcyjnego w KWC. Ryzyka kumulują się wzdłuż podprocesów sekwencyjnych. Źródło: badania własne.

Od strony technologicznej, układ produkcyjny KWC, w skład którego wchodzą urabianie, załadunek i transport surowca, wykorzystuje urządzenia techniczne wskazane w [Tab. 10]. Kumulacja ryzyk wzdłuż procesów produkcyjnych może być opisana jako suma ryzyk na poszczególnych etapach, uwzględniająca ich wzajemne oddziaływania, propagację oraz wpływ zabezpieczeń i działań obniżających zagrożenie.

$$R_{total} = \sum_{i=1}^{N} (P_i * S_i * \prod_j (1 + w_{ij} * T_i)), \quad (2.2)$$

gdzie R_{total} to ryzyko całkowite awarii ciągu technologicznego, N to liczba etapów/składników ciągu, P_i prawdopodobieństwo materializacji ryzyka na *i-tym* elemencie (np. awaria, błąd ludzki, sabotaż), S_i to skutek materializacji (np. koszt, czas, liczba uszkodzonych maszyn), w_{ij} to waga oddziaływania pomiędzy węzłami ij (odzwierciedla zakres powiązań), a T_{ij} to tłumienie (lub wzmocnienie) propagacji ryzyka. Przy czym, dla T_i<1 efektywne tłumienie ryzyka, dla T_i=1 brak wpływu na tłumienie ryzyka, T_i>1 mamy do czynienia z wzmocnienie ryzyka przez brak zabezpieczeń lub kumulację problemów.

Z punktu widzenia analizy ryzyka istotny jest fakt, że w tak przedstawionym procesie, w którym kolejne elementy występują w układzie szeregowym, również ryzyka występujące dla poszczególnych elementów mają wpływ na kolejne elementy i kumulują się. Ryzyka

z obszaru wyrobiska (naturalne i antropogeniczne) oddziałują na kolejne ogniwo ciągu tj. transport, a ten z kolei wpływa na cykl przeróbczy. Liczba maszyn i obszar, na którym prowadzą one swą działalność w sposób proporcjonalny wpływa na wzrost ryzyka sumarycznego wpływającego na analizowany proces produkcyjny.

Dodatkowe informacje o stosowanych w rozprawie miarach ryzyka zamieszczono w [rozdziale 7.4].

W analizowanym tu przykładzie można wyróżnić trzy rodzaje propagacji ryzyka (szerzej o propagacji ryzyka w [rozdziale 7.2]):

1. Ryzyka powiązane z kolejnymi etapami procesu produkcji.

W tym wypadku ryzyka z obszaru wyrobiska (naturalne i antropogeniczne) oddziałują na kolejne ogniwo ciągu tj. transport, a ten z kolei wpływa na cykl przeróbczy. Liczba maszyn i obszar, na którym prowadzą one swą działalność wpływa na kumulację ryzyka sumarycznego występującego w analizowanym procesie produkcyjnym. Przykładem tego typu ryzyka jest nadgabaryt, który spowodować może zatrzymanie i/lub uszkodzenie kruszarek wstępnych, co bezpośrednio przenosi się na kolejne elementy ciągu technologicznego, powodując jego wyłączeni z produkcji na czas zależny od rodzaju uszkodzeń. Ryzyko pojawienia się w kruszarce wstępnej nadgabarytu jest konsekwencją np. nieprawidłowego odstrzału ściany lub niewychwycenia go w masie skalnej przez operatora koparki, lub niewychwycenia go przez operatora nadzorującego proces wyładunku i transportu urobku do kruszarki wstępnej. Propagację tego ryzyka w sposób graficzny prezentuje [Rys. 21].

2. Ryzyko przenoszone niezależnie od etapów procesu produkcyjnego.

Przykładem tego rodzaju ryzyka jest np. pożar, który może objąć budynki lub maszyny pozostające w sąsiedztwie z ogniskiem pożaru, niezależnie od tego, czy istnieją pomiędzy nimi powiązania produkcyjne.

W określonych sytuacjach, niewystępujących raczej w KWC, możliwe jest także występowanie przerw z zasilaniu, co w skrajnej sytuacji może prowadzić do zatrzymania pracy maszyn w stanie, w którym ponowny rozruch wymaga prac przygotowawczych. Aby tego uniknąć i zminimalizować ten rodzaj ryzyka stosuje się zasilanie rezerwowe, w postaci odrębnej linii zasilającej (w przypadku KWC 15kV) prowadzonej niezależną trasą, zasilająca dodatkowe pola transformatorowe. Analizując tego typu zdarzenie, w kontekście wsparcia jego obsługi przy wykorzystanie systemu klasy IRM DSS, rozważyć należy możliwości rozbudowy infrastruktury, zarówno techniczne, jak i ekonomiczne. W skrajnych sytuacjach okazać się może, że budowa systemu odpornego na tego typu zagrożenia nie będzie kontynuowana przez decydenta, właśnie ze względu na aspekty techniczno-ekonomiczne.

3. Mieszane rodzaje propagacji ryzyk, w których ryzyko przenosi się zarówno wraz z kolejnymi etapami procesu produkcji, jak i niezależnie od nich.

Przykładem takiego procesu może być produkcja elementów z łatwopalnych materiałów w sytuacji, gdy materiały o niebezpiecznie podwyższonej temperaturze przenoszą zagrożenie do kolejnych maszyn lub budynków, a oprócz tego ogień obejmuje kolejne obiekty niezwiązane z cyklem produkcyjnym.

3 Techniki stosowane w zarządzaniu bezpieczeństwem w KWC

Stosowane obecnie w KWC techniki zapewnienia bezpieczeństwa od strony technicznej można podzielić na 4 główne podgrupy, opisane w kolejnych podrozdziałach. Natomiast klasyfikacja funkcjonalna tych systemów z punktu widzenia prewencji, detekcji, przeciwdziałania i budowy długoterminowej odporności na zagrożenia podana jest w [Tab. 12].

Tab. 12. Zależności pomiędzy zagrożeniami i metodami detekcji, przeciwdziałania i budowy odporności w KWC.

Rodzaj zagrożenia	**Sposób detekcji**	**Powiadomienia (komunikaty)**	**Budowa odporności na zagrożenia (prewencja)**
Nieuprawniony dostęp	Monitoring wizyjny z analityką obrazu	Zalecania dla zespołów i komórek odpowiedzialnych za bezpieczeństwo	Dźwiękowe i świetlne systemy ostrzegawcze, optymalne rozmieszczenie ogrodzeń, rozwój OF (Ochrony Fizycznej)
Oderwanie mas skalnych	Czujniki naziemne i drony, rozpoznawanie wzorców	Automatyczne ostrzeżenia dla dyżurującego personelu	Fotogrametria, regularnie aktualizowana analiza dynamiki skał, siatki i ogrodzenia ochronne
Osuwiska	Fotogrametria z użyciem dronów, mapy ryzyk, roboty inspekcyjne	Adaptacyjne wyznaczanie obszarów schronienia i ścieżek ewakuacyjnych	Mapy ryzyka i analiza dynamiki górotworu, systemy ostrzegania o trzęsieniach ziemi
Przypadkowe wycieki gazu lub cieczy technicznej	Roboty inspekcyjne, czujniki gazu i oparów	Działania robotów i zespołów człowiek-robot zdefiniowane na podstawie oceny zagrożeń	Optymalne pokrycie chronionego obszaru przez roboty inspekcyjne, rozwój OF
Podtopienia	Czujniki naziemne, kamery w zakresie spektrum widzialnego i podczerwieni na dronach, inne czujniki	Automatyczne ostrzeżenia dla dyżurującego personelu generowane na podstawie zautomatyzowanego rozpoznawania obrazów	Fotogrametria w korelacji z czujnikami naziemnymi, analiza przyboru wody z prognozowaniem
Pożary	Czujniki dymu, kamery w zakresie spektrum widzialnego i podczerwieni zintegrowane w System Sygnalizacji Pożaru (SSP)	Alarm pożarowy ze wskazaniem zagrożonego obiektu generowany przez SSP	Rozbudowa systemu czujników przeciwpożarowych, zakazy palenia poza wyznaczonymi miejscami, szkolenia personelu

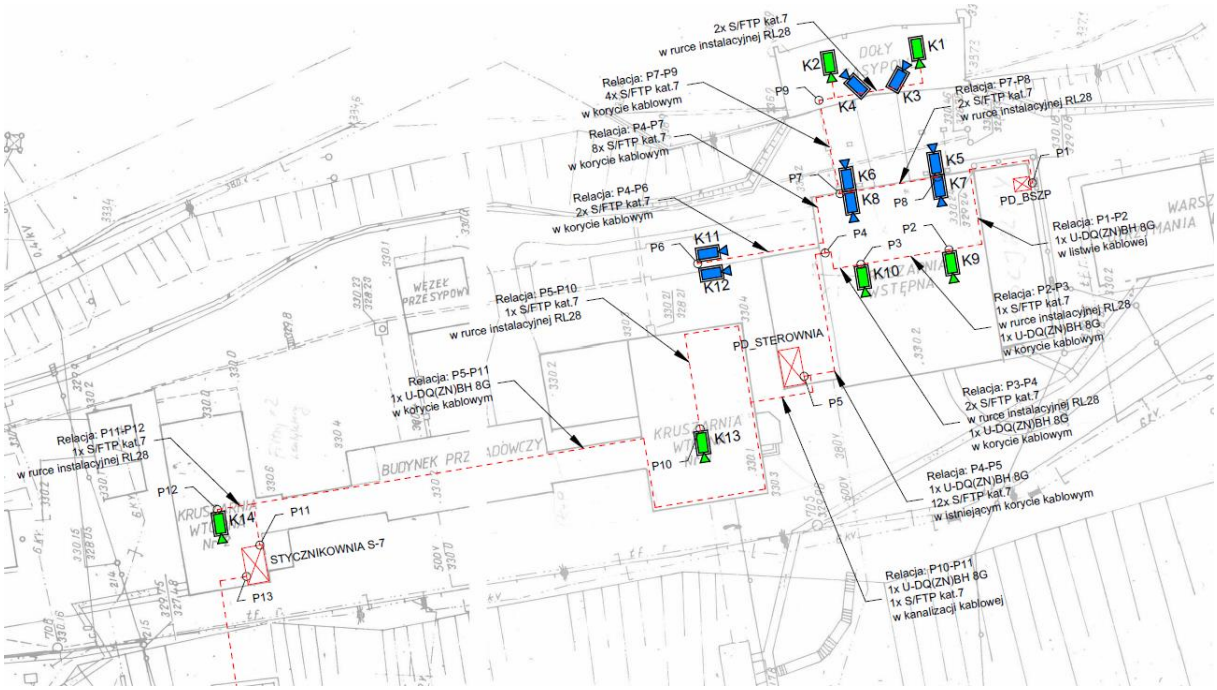
3.1 Systemy monitoringu wizyjnego

Aktualnie wykorzystywane systemy bezpieczeństwa bazują na rozwiązaniach konwencjonalnych, tj. rejestracji obrazu i analizie w czasie rzeczywistym pewnej liczby parametrów kontrolnych. Rozwiązanie takie zapewnia stosunkowo niski koszt i szybkość działania, jednak jego skuteczność, dokładność, jak też częstotliwość przekłamań, są obecnie niezadowalające. Poza tym - biorąc pod uwagę ciągłą rozbudowę samego systemu - efektywność monitoringu opartego jedynie na transmisji obrazu okazuje się być coraz mniejsza, ponieważ zwiększanie ilości danych wejściowych nie przekłada się na poprawę wyniku.

Systemy monitoringu bezpieczeństwa i technologicznego są sukcesywnie rozbudowywane i podlegają modernizacji. Aktualnie system monitoringu w obrębie wyrobiska górniczego opiera się na 5 kamerach obrotowych AXIS, 2 kamery model Q6215-LE oraz 3 kamery model Q6135-LE, wszystkie o rozdzielczości FullHD (1080p) z 30'to krotnym zoomem optycznym [Rys. 22].

Rys. 22. Kamery AXIS: Q6215-LE (z lewej i środek), Q6215-LE (z prawej).
Źródło: katalog producenta.

Umiejscowienie kamer na 30-metrowych wieżach oświetleniowych w połączeniu z dużym zoomem optycznym zapewnia widoczność około 90% eksploatowanej części wyrobiska, natomiast w obrębie Zakładu przeróbczego stosowane są kamery stacjonarne, dobrane zgodnie ze specyfiką środowiska pracy. Przykład rozmieszczenia kamer w obrębie części wstępnej Zakładu Przeróbczego przedstawia [Rys. 23].



Rys. 23. Umiejscowienie kamer w obrębie Zakładu Przeróbczego, Część 1: przeróbka wstępna. Źródło: materiały własne KWC.

Przykład istniejącej konfiguracji hardware'owej systemu monitoringu wizyjnego, w obszarze przeróbki wstępnej urobku, podany jest w Dodatku A.

Właściwie zaprojektowany i skonfigurowany system monitoringu posiada następujące właściwości:

- pełni funkcję ochrony obwodowej, zapewniając detekcję intruza oraz identyfikację obiektów,
- monitoruje główne ciągi komunikacyjne,
- monitoruje obszary wielkopowierzchniowe,
- zapewnia analitykę rejestrowanego obrazu,
- zapewnia archiwizację nagrań.

Obecnie użytkowany system monitoringu wizyjnego zrealizowany jest w całości w oparciu o rozwiązania monitoringu wizyjnego firmy Axis[1], wsparte rozwiązaniami sieciowymi Hirschmann[2] oraz Cisco[3].

[1] https://axis.com/ [dostęp: 11.2024]
[2] https://hirschmann.pl/ [dostęp: 11.2024]
[3] https://www.cisco.com/ [dostęp: 12.2024]

W przypadku pojawienia się nowego rozwiązania technicznego powyższa konfiguracja może ulec zmianie. Tej procedurze poświęcony jest rozdział dotyczący analizy problemu ewakuacji [rozdział 10.3], gdzie przedstawiamy sposób skanowania rynku rozwiązań AI i reguły podejmowania decyzji dotyczącej aktualizacji systemu monitoringu. Podobne procedury stosowane będą w ramach IRM DSS również dla pozostałych elementów systemu bezpieczeństwa KWC. Zaprezentowany w [podrozdziale 10.3] diagram [Rys. 69] należy traktować jako narzędzie uniwersalne, będące kompendium wiedzy, wraz z podzespołami do jej pozyskiwania. Takie podejście stwarza możliwości budowania otwartej i uniwersalnej platformy, a tym samym nie zamyka jej w sztywnych ramach dedykowanych np. dla konkretnego rozwiązania w przemyśle wydobywczym.

3.2 Wykorzystanie dronów dla celów fotogrametrii i monitoringu ruchów górotworu

Rozwój nowoczesnych technologii oraz postęp z zakresie miniaturyzacji odtworzył przed przedsiębiorstwami górniczymi nowe możliwości w zakresie prowadzenie geodezji wyrobiska. Wykorzystanie dronów (bezzałogowych statków powietrznych, *Unmanned Aerial Vehicle*, UAV) pozwala na dostarczenie dużej ilości danych w trójwymiarowych formatach wymiany danych (chmury punktów, modele 3D), oraz stworzenie z nich wyjściowych formatów 3D, takich jak ortofotomapy, rzuty, czy profile podłużne oraz różnego rodzaju mapy tematyczne będące wynikiem analizy tych danych. KWC z tego typu rozwiązań korzysta z powodzeniem od roku 2019, jednak w drodze zdobywania kolejnych doświadczeń zauważono możliwość wykorzystania tej technologii również do innych zastosowań, ważnych z punktu widzenia analiz bezpieczeństwa. Spółka podjęła kroki w celu wdrożenia i rozwoju technologii UAV do:

- jakościowej oceny złoża w czasie rzeczywistym,
- detekcji i oceny zagrożeń w czasie rzeczywistym,
- bezkontaktowej oceny stanu wyrobiska.

Szczególnie ważne jest wykorzystanie UAV jak automatycznego narzędzia umożliwiającego decydentowi przeprowadzenie szybkiej i bezinwazyjnej analizy ścian wyrobiska górniczego pod kątem możliwości wystąpienia takich groźnych z punktu widzenia bezpieczeństwa zjawisk, jak:

- pęknięcia i odspajanie się ściany,
- osuwiska,
- odrywanie się bloków skalnych.

Podejście holistyczne do zagadnień związanych z zapewnieniem odpowiedniego poziomu bezpieczeństwa zakłada automatyczną detekcję (bądź na polecenie decydenta) niebezpiecznych zjawisk, obróbkę danych przez algorytmy rozpoznawania obrazów oparte o głębokie sieci neuronowe i inne metody AI i podjęcie reakcji adekwatnej do zidentyfikowanego zagrożenia w celu minimalizacji materializacji ryzyka uszkodzenia maszyny górniczej lub wypadku. Kolejnym naturalnym wykorzystaniem UAV jest możliwość automatycznego patrolowania zdefiniowanego obszaru w celu poszukiwania śladów intruzji. Również to zadanie powinno być realizowane w pełni samodzielnie, a zebrane dane będą analizowane przez algorytmy AI/ML. Wszystkie te działania powinny mieć celu optymalne wykorzystanie jednostek UAV, należy jednak pamiętać, że czynnikiem mocno determinującym samą możliwość ich stosowania jest pogoda. Deszcz czy silny wiatr w zasadzie wyłączają jednostki UAV z ruchu.

3.3 Czujniki dymu, temperatury i pyłu

Czujniki zadymienia i temperatury jako standardowe elementy Systemów Sygnalizacji Pożaru (SSP) zainstalowane są w obiektach wymagających tego typu ochrony. Ich integracja z Systemem Sygnalizacji Włamania i Napadu (SSWiN) i możliwość powiadamiania pracowników ochrony zabezpiecza obiekty, których funkcjonowanie jest kluczowe w z punktu widzenia zabezpieczenia infrastruktury istotnej dla zapewnienia ciągłości działania procesów technologicznych. Wykorzystanie nowoczesnych platform zintegrowanego zarządzania (w przypadku KWC jest to platforma Gemos) pozwala poprzez integrację systemów SSWiN, SSP i sytemu monitoringu wizyjnego ograniczyć ilość fałszywych alarmów, zabezpieczyć obiekty w sposób kompleksowy oraz podnieść jakość pracy personelu odpowiedzialnego za nadzór nad zabezpieczonymi obiektami, dodatkowo zapewniając wysoki poziom synergii.

3.4 Sensory detekcji zagrożeń instalowane na robotach inspekcyjnych

Dobrym uzupełnieniem technologii radarowej mogą być czujniki drgań - stacjonarne bądź mobilne, zamontowane na robotach inspekcyjnych. Ten typ sensora badał będzie drgania generowane w górotworze w trakcie prac strzałowych oraz normalnej eksploatacji (ruchy maszyn ciężkich). Do tej pory czujniki drgań sejsmicznych wykorzystywane były w KWC jedynie w celu badania ewentualnych wstrząsów, będących następstwem robót strzałowych, a prowadzących w swojej konsekwencji do szkód górniczych. Tego typu czujniki zamontowane były dotąd na obiektach budowlanych w sąsiedztwie kopalni i ze względu na odległość od źródła drgań w OG wykrywały jedynie wstrząsy o większej amplitudzie. Przeniesienie czujników bezpośrednio na poziomy eksploatacyjne otworzy możliwość

wykorzystania ich jako elementy systemu bezpieczeństwa wspierające procesy predykcyjne dotyczące zagrożeń ze strony ruchów i pęknięć górotworu. Roboty mobilne można również wyposażyć w georadar, który dzięki wykorzystaniu fal elektromagnetycznych emitowanych bezpośrednio do gruntu pozwoli zbadać i stworzyć obraz struktury skał i mas ziemnych, dając dodatkowe informacje o potencjalnych zagrożeniach wynikających z nieciągłości czy zakłóceń w strukturze górotworu.

Robot taki składa się z kilku głównych modułów, które współpracują ze sobą, tworząc platformę do efektywnego badania struktur skalnych za pomocą georadaru. Poza modułem napędowym (napęd typu gąsienicowego, hybrydowy lub kołowy, dostosowany do trudnego terenu kopalni) głównym wyposażeniem jest sam moduł georadaru, umieszczony na stabilnym uchwycie. Urządzenie wysyła fale elektromagnetyczne w głąb podłoża, analizuje odbicia od warstw geologicznych i przeszkód. Uzyskane w ten sposób dane przetwarzane są przez moduł obliczeniowy, wykorzystywane do analizy danych z georadaru w czasie rzeczywistym. Komunikacja realizowana poprzez transmisje Wi-Fi lub GSM zapewnia przesyłanie danych do systemu nadrzędnego, gdzie algorytmy AI przetwarzają i wizualizują dane w celu identyfikacji struktur podłoża. Ważną funkcjonalnością jest możliwość zmiany kąta i głębokości penetracji w zależności od wymagań prowadzonych badań. Opcjonalnie tego typu robota wyposażyć można w moduł czujników pomocniczych dedykowany do zbierania danych o warunkach pracy, identyfikacji przeszkód, zapewnienia stabilnej pracy georadaru. Mogą to być czujniki typu inklinometr (do pomiaru nachylenia podłoża), LIDAR (do mapowania powierzchni terenu), GPS (do precyzyjnego określania pozycji robota).

3.5 Systemy robotyki dla zarządzania bezpieczeństwem

Wielkim wyzwaniem, na które przynajmniej częściowo muszą odpowiedzieć badania realizowane we współpracy z wybraną jednostką naukową, jest integracja zespołów ratowniczych ludzi i robotów w ramach jednego systemu zarządzania bezpieczeństwem przemysłowym. Szczególne znaczenie ma wsparcie koordynacji zespołów autonomicznych robotów mobilnych wykorzystywanych jako roboty inspekcyjne lub ratownicze. Problematyka Search & Rescue Robotics (SRR) jest jednym z motywów przewodnich i motorów rozwoju automatycznej robotyki mobilnej. Badania obejmują połączenie zaawansowanych metod sztucznej inteligencji wykorzystywanych głównie do planowania poszukiwań, identyfikacji otoczenia z rozpoznawaniem wzorców i podejść do zrozumienia miejsca, oceny sytuacji awaryjnej i ustalania priorytetów działań.

Już w jednym z pierwszych przeglądów potencjalnego zastosowania mobilnych mikrosystemów robotów w miejskich poszukiwaniach i ratownictwie [Blitch, 1996] omówiono zastosowanie systemu eksperckiego KNOBSAR w celu udzielania porad dotyczących przydzielania mikrorobotów do określonych punktów w miejscu kryzysu. Jednak

idea ta nie doprowadziła wówczas do odpowiednich wdrożeń praktycznych, prawdopodobnie z powodu niewystarczających jeszcze powiązań między zespołami zarządzania kryzysowego a zespołami programistów systemów robotów. Obecnie zwraca się wiele uwagi na ogromne znaczenie cyberfizycznych aspektów zastosowań SRR, w tym na sposób udzielania pomocy ofiarom, współpracę z zespołami ratownictwa OF. Ważnym aspektem jest też komunikacja z zespołem zarządzającym, który kontroluje lub nadzoruje działania zmierzające do likwidacji skutków zagrożeń przemysłowych i katastrof naturalnych. [Zadorozhny i in., 2015] przedstawiają wspólne działania przekazu informacji dla SRR z wieloma robotami. Optymalizacji harmonogramów wykorzystywania pojazdów ratowniczych i ekip naprawczych poświęcony jest artykuł [Shin, i. in., 2019]. Optymalny model planowania akcji SRR oparty jest o algorytmy mieszanego programowania liniowego i całkowitoliczbowego (MILP) i stygmergii (tzw. algorytmy mrówkowe). Autorzy [Bakhshipour i in., 2017] przedstawiają rozwiązanie nieliniowego problemu optymalizacji typu SRSR (Swarm Robotics Search & Rescue). W artykule [Sreedharan i in., 2019] omówiono problem objaśniania działania algorytmów sztucznej inteligencji w kontekście wyjaśniania planów działania robotów podczas działań robotów typu SRR w KWC, kontroli nadzorczej tych działań oraz efektywności interakcji człowiek - robot, która musi zapewniać szybką interpretowalność działań robotów autonomicznych. [Skulimowski, Ćwik, 2017] wdrożyli środowisko symulacyjne, w którym roboty ratownictwa górniczego poszukiwały optymalnych strategii przewidywania w celu wykrywania wycieków wody i gazu w kopalni soli. Ta koncepcja może być zastosowana również w KWC. Projekt IRM-MSS zaproponowany w tym opracowaniu ma również na celu włączenie do systemu zarządzania bezpieczeństwem KWC systemów robotyki typu SRR, skupiając się na wydajności akcji ratunkowych i minimalizacji ryzyka dla personelu ratowniczego. Podsumowując, optymalne wykorzystanie zespołów robotów w ogólnych działaniach SRR koordynowanych z poziomu systemu IRM DSS pozostaje wciąż ważnym problemem badawczym, który należy rozwiązać podczas prac projektowych IRM DSS.

3.6 Pozostałe sensory wykorzystywane do detekcji zagrożeń

Biorąc pod uwagę wskazane w powyżej ograniczenia systemów UAV, tj. silną zależność od panujących w danej chwili warunków atmosferycznych, mniejszą, lecz nadal istotną w przypadku GUAV, konieczne wydaje się poszukiwanie dodatkowych rozwiązań pozbawionych tej wady. Z pomocą przychodzą tutaj rozwiązania dedykowane do ochrony obwodowej zbudowane w oparciu o technologie radarową. Zaletami tych systemów są: możliwość pracy ciągłej (7 dni w tygodniu, 24 godziny na dobę), pokrycie zasięgiem widzenia znacznej powierzchni, szeroki kąt widzenia i brak części ruchomych. Dodatkowo tego typu systemy można zintegrować z monitoringiem wizyjnym, co przy jednoczesnym

wykorzystaniu metod analityki danych opartych o AI znacznie wyeliminowałoby błędy i fałszywe alarmy. Pokrycie siatką radarów terenu pozbawionego ogrodzenia oraz z łatwym dostępem dla osób postronnych, a tym samym wysokim prawdopodobieństwem intruzji pozwoli w sposób satysfakcjonujący zabezpieczyć teren przed wtargnięciem osób niepożądanych.

4 Przegląd literatury w zakresie metod analizy i implementacji systemów zarządzania ryzykiem przemysłowym

Prowadzone dotychczas badania w zakresie oceny zagrożeń w warunkach prowadzenia eksploatacji odkrywkowej złóż ukierunkowane były na analizę metod wspomagania decyzji, architekturę systemów wspomagania decyzji (*Decision Support Systems*, DSS) oraz elementy modelowania ryzyka, które w konsekwencji jego materializacji wymusza podjęcie określonych działań, a na etapie analizy służy do oceny potencjalnych zagrożeń. W zakładach przemysłowych, gdzie występuje potrzeba zarządzania zagrożeniami naturalnymi we własnym zakresie, a nie tylko przy pomocy służb publicznych, należy przewidzieć zarówno odpowiednie instrumenty, jak i procedury decyzyjne, które będą zaimplementowane w DSS. W KWC system wspomagania decyzji dla utrzymania bezpieczeństwa przemysłowego docelowo powinien umożliwiać zarządzanie wszystkimi zidentyfikowanych dotąd grupami zagrożeń, w tym także związanych z katastrofami naturalnymi. Podejście takie determinuje konieczność analizy i w dalszej kolejności opracowania metodologii przetwarzania danych pochodzących z wielu źródeł (analiza wielokryterialna połączona z fuzją danych) i koncepcyjne przygotowanie podstaw do stworzenia algorytmów postepowania w sytuacji materializacji możliwych do przewidzenia oraz nieznanych dotychczas zagrożeń.

Mając na uwadze powyższe, konieczne stało się przeprowadzenie badań bibliograficznych dostępnej literatury w zakresie niezbędnym do przygotowania opracowania, obejmującego swym zakresem tematykę związaną z fuzją danych, w pierwszej kolejności w sytuacji materializacji zagrożeń naturalnych takich, jak obsunięcia gruntu i podtopienia.

W dalszej kolejności badania prowadzone były w kierunku opracowania algorytmów ewakuacji, dających się wykorzystać w warunkach zakładów przemysłowych, w sytuacji zaistnienia zagrożenia. Naturalnym uzupełnieniem tych dwóch obszarów było wprowadzenie do analizy problematyki związanej z ryzykami, ich szacowaniem i zapobieganiem ich materializacji.

4.1 Metodyka analizy bibliograficznej

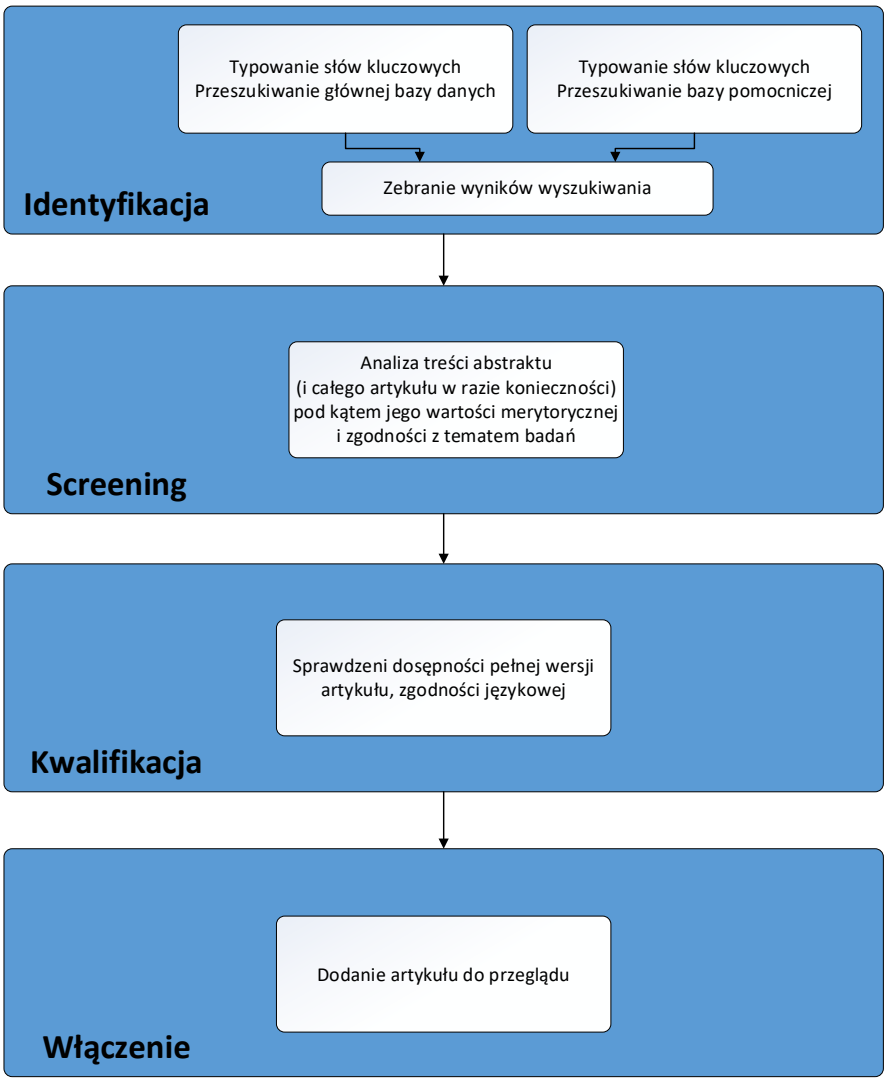
Badacze [Bueno i in., 2021] zidentyfikowali osiem możliwych metod przeprowadzania przeglądu literatury. Są to kolejno metoda systematyczna, state of the art, narracyjna, realistyczna, szybka, konceptualna, ekspercka i krytyczny przegląd literatury. Te osiem podejść autorzy pogrupowali w trzy kategorie: przegląd systematyczny, przegląd półsystematyczny i przegląd integracyjny. Przeglądowi systematycznemu przypisuje się cztery zasady: (1) wyznaczony punkt ciężkości, (2) plan znalezienia całej istotnej literatury,

(3) ocena znalezionych artykułów oraz (4) synteza podstaw wiedzy. W swej publikacji autorzy [Bueno i in., 2021] przeprowadzili przegląd systematyczny w oparty na metodzie Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA). Celem tej metody jest stworzenie ram przeglądu literatury podzielonych na cztery kluczowe kroki: (1) identyfikacja, (2) screening, (3) kwalifikacja i (4) włączenie.

Przedstawione w dalszej części pracy badania przeprowadzono w oparciu wytyczne ogólne metody PRISMA oraz wskazówki zawarte w publikacji [Bueno i in., 2021]. Aktualizacja przeglądu przeprowadzona została w styczniu oraz listopadzie 2024 w oparciu o bazy danych SCOPUS i IEEE Xplore. Bazy te wybrane zostały ze względu na to, że są reprezentatywne dla dziedziny rozprawy, a IEEE Xplore zawiera ponadto pełne teksty artykułów, w materiałach konferencyjnych czy czasopismach.

Dla każdego z wymienionych obszarów badawczych wstępnie wytypowane zostały słowa kluczowe, które wykorzystane zostały w pierwszym etapie poszukiwań. Szczegóły dotyczące słów kluczowych, ich wariantów i kombinacji omówione zostaną w olejnych rozdziałach pracy, właściwych dla kolejno omawianych zagadnień. Synonimy i warianty językowe użyte zostały w kilku kombinacjach. W trakcie pracy korzystano również z kryteriów wykluczenia, eliminując teksty w językach innych niż angielski, brak dostępu do pełnego tekstu artykułu oraz ewentualne duplikaty. Podobną metodologię pracy zastosowali autorzy przeglądów [Vieira i in., 2022] oraz [Qiu i.in., 2021].

W pierwszej kolejności [Rys. 24] wykorzystano repozytorium bibliograficzne SCOPUS, traktując go jako punkt wyjścia i bazę główną, będącą odniesieniem dla ewentualnych dalszych poszukiwań uzupełniających. Główny nacisk położony został na analizę artykułów publikowanych w czasopismach naukowych. Podejście takie sprawdziło się i potwierdziło swoją wartość w przeglądzie przeprowadzonym przez [Reyes-Riveros i.in., 2021]. Po wstępnej selekcji w oparciu o silnik wyszukiwarki analizowana była treść abstraktów wybranych artykułów, a w przypadku, gdy abstrakt nie dawał pełnej informacji o treści artykułu, analizowana była również cała praca. Na tej podstawie odrzucane były artykuły zawierające jedynie podejścia koncepcyjne, a w szczególności artykuły niezwiązane w żaden sposób z dziedziną będącą w głównym obszarze zainteresowania.



Rys. 24. Schemat blokowy wykorzystanej metodyki prowadzonych badań [Bueno i in., 2021].

W celu wizualizacji relacji zachodzących pomiędzy zbiorami pozyskanymi w trakcie procesu przeglądu literatury wykorzystać można diagramy Venna [Lam i in., 2016]. Umożliwiają one graficzne przedstawienie zbiorów, każdy zbiór jest przedstawiony jako koło, a ich wspólne części reprezentują elementy wspólne dla tych zbiorów. Diagramy te są często używane do:

- wizualizacji relacji między zbiorami – pokazują, które elementy są wspólne, a które różne dla porównywanych zbiorów,
- analizy logicznej – używane są głównie w matematyce, logice i statystyce do zobrazowania zależności między grupami danych,
- porównywania grup danych – pomagają w zrozumieniu wspólnych i odrębnych cech danych grup.

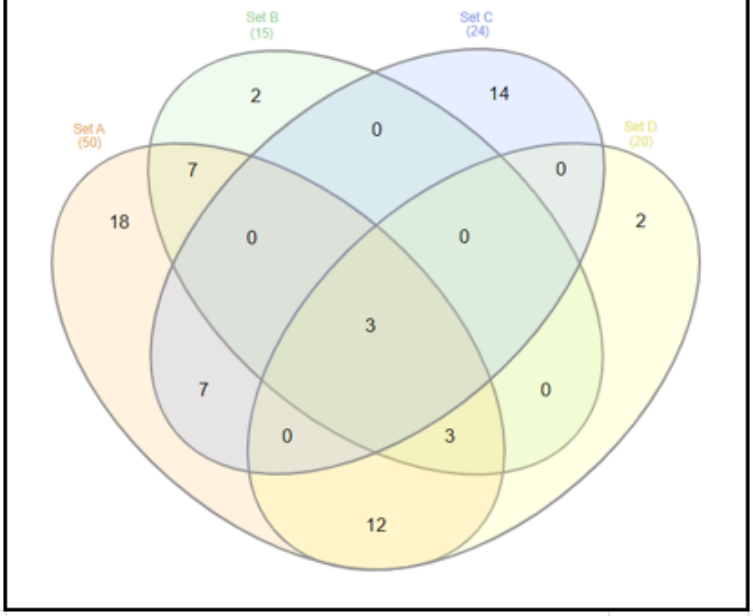
Typowy diagram Venna dla dwóch zbiorów to dwa przecinające się koła, gdzie część wspólna reprezentuje elementy obecne w obu zbiorach. Diagram może mieć więcej kół, aby reprezentować więcej zbiorów i bardziej złożone relacje.

Diagramy Venna pomagają w identyfikacji elementów, które są wspólne dla różnych zbiorów, a także tych, które są unikalne dla poszczególnych grup. Dzięki temu łatwo zobaczyć, które cechy są współdzielone przez wszystkie analizowane grupy, a które występują tylko w jednej z nich. Analiza wspólnych i różniących się elementów może wskazać wybory najbardziej efektywne lub korzystne.

Z punku widzenia omawianego tu procesu dotyczącego badań bibliograficznych diagramy Venna pozwalają, przy wykorzystaniu dostępnych, darmowych narzędzi na analizę duży zbiorów wyszukując wzajemne relacje występujące pomiędzy nimi, dzięki czemu łatwiej znaleźć cechy wspólne i unikalne dla wybranych obszarów badawczych.

Poniżej zaprezentowano analizę danych pozyskanych z repozytorium https://www.scopus.com/, przeprowadzoną przy wykorzystaniu narzędzi dostępnego pod adresem https://www.interactivenn.net/. Analiza przeprowadzona została dla słów kluczowych „evacuation", „algorithm", „disaster".

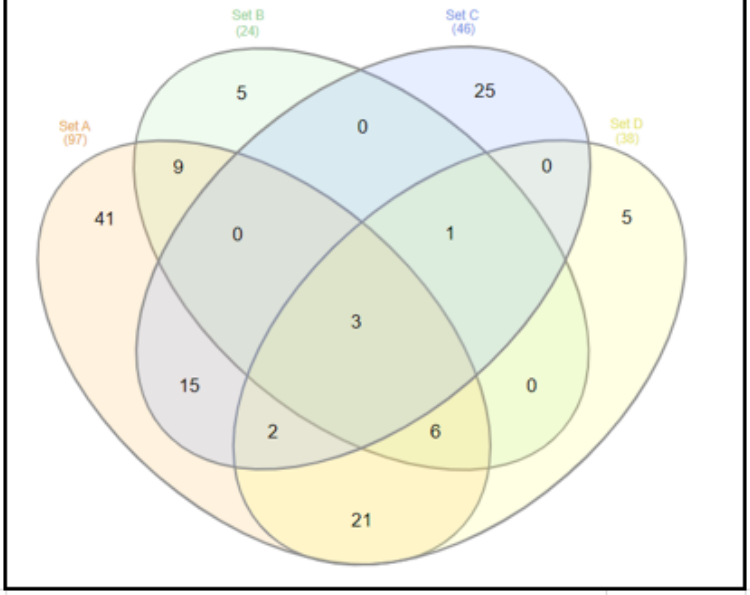
Składnia zapytania	Wynik
(evacuation W/1 algorithm*) AND (disaster*)	50
(evacuation W/1 algorithm*) AND (threat*)	15
(evacuation W/1 algorithm*) AND (decision*)	24
(evacuation W/1 algorithm*) AND (natural*)	20



Rys. 25. Zapytanie i wyniki wyszukiwarki Scopus, 12.03.2024 (parametr W/1).

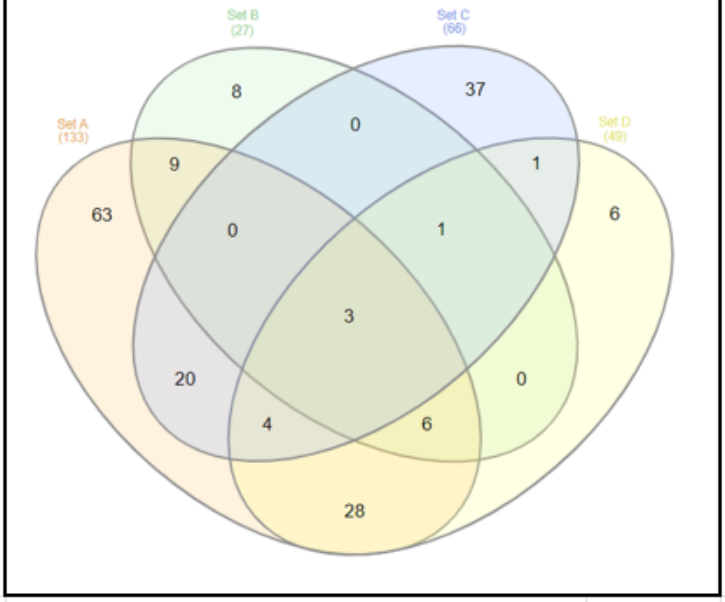
,

Składnia zapytania	Wynik
(evacuation W/2 algorithm*) AND (disaster*)	97
(evacuation W/2 algorithm*) AND (threat*)	24
(evacuation W/2 algorithm*) AND (decision*)	46
(evacuation W/2 algorithm*) AND (natural*)	38



Rys. 26. Zapytanie i wyniki wyszukiwarki Scopus, 12.03.2024 (parametr W/2).

Składnia zapytania	Wynik
(evacuation W/3 algorithm*) AND (disaster*)	133
(evacuation W/3 algorithm*) AND (threat*)	27
(evacuation W/3 algorithm*) AND (decision*)	66
(evacuation W/3 algorithm*) AND (natural*)	49



Rys. 27. Zapytanie i wyniki wyszukiwarki Scopus, 12.03.2024 (parametr W/3).

Dzięki wizualizacji wyników przy użyciu diagramów Venna zaprezentowanych na Rys. 25, Rys. 26, i Rys. 27 widać, że pomimo zwiększania zakresu przeszukiwania poprzez zwiększanie „odległości" pomiędzy słowami kluczowymi, część wyników pozostaje niezmienna, co pozwala wyciągnąć wniosek, że dalsze przeszukiwanie w tym kierunku nie przyniesie dodatkowych, wartościowych wyników.

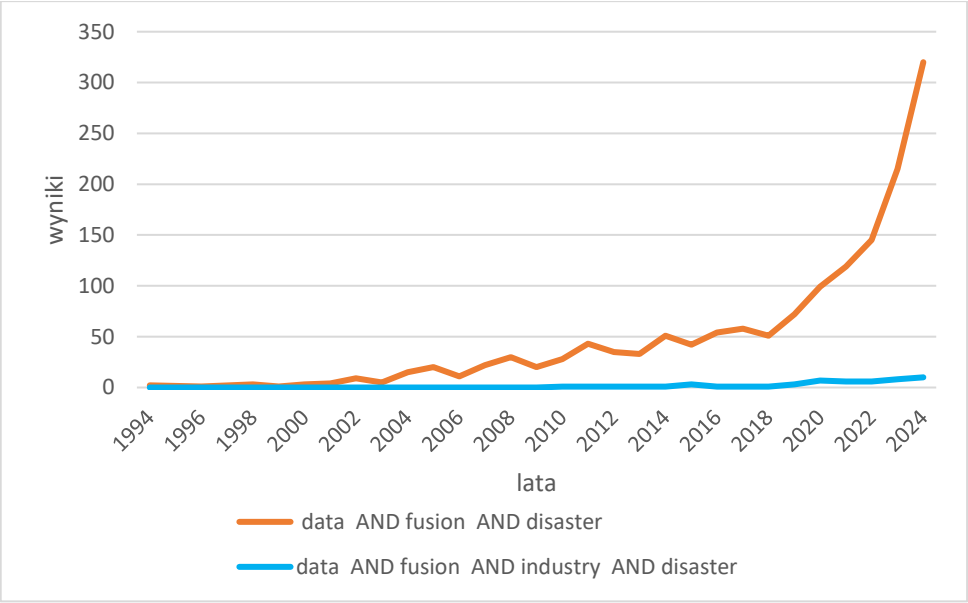
4.2 Fuzja informacji

Fuzja informacji o zagrożeniach, jest punktem wyjścia do dalszych prac mających doprowadzić do wypracowania metodyki zarządzania sytuacją kryzysową i stanowić fundament dla budowy szkieletu algorytmu ewakuacji z obszarów objętych zagrożeniem.

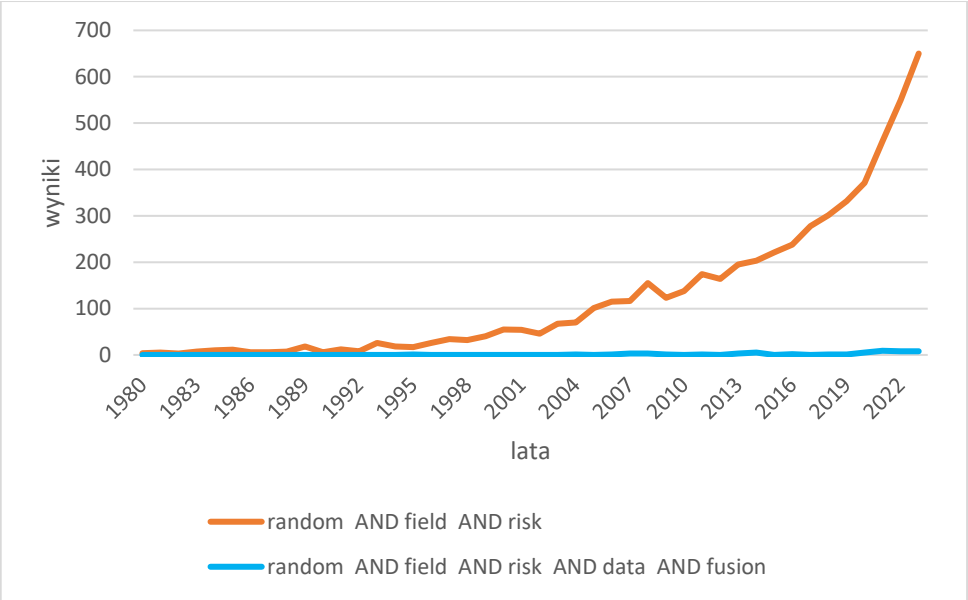
Fuzja danych jako rozwiązanie uniwersalne wykorzystywane jest jako narzędzie podstawowe w wielu dziedzinach wiedzy, co skutkuje tym, że pojęcie to jest bardzo popularne w wynikach wyszukiwania, jednak kolejne zawężenia obszarów przeszukiwania pozwalały dotrzeć do prac ściśle związanych z tematem badawczym, a tym samym najbardziej wartościowych. Kluczowa była tu wstępna, a w dalszej kolejności szczegółowa analiza treści wytypowanych do tego artykułów. Podobna metodologia pracy wykorzystywana jest często w pracach o charakterze „*bibliographic review*" (np. [Reyes-Riveros i in., 2021]).

Słowa kluczowe użyte w kolejnych iteracjach przeszukiwania bazy SCOPUS (na dzień 26.11.2024):

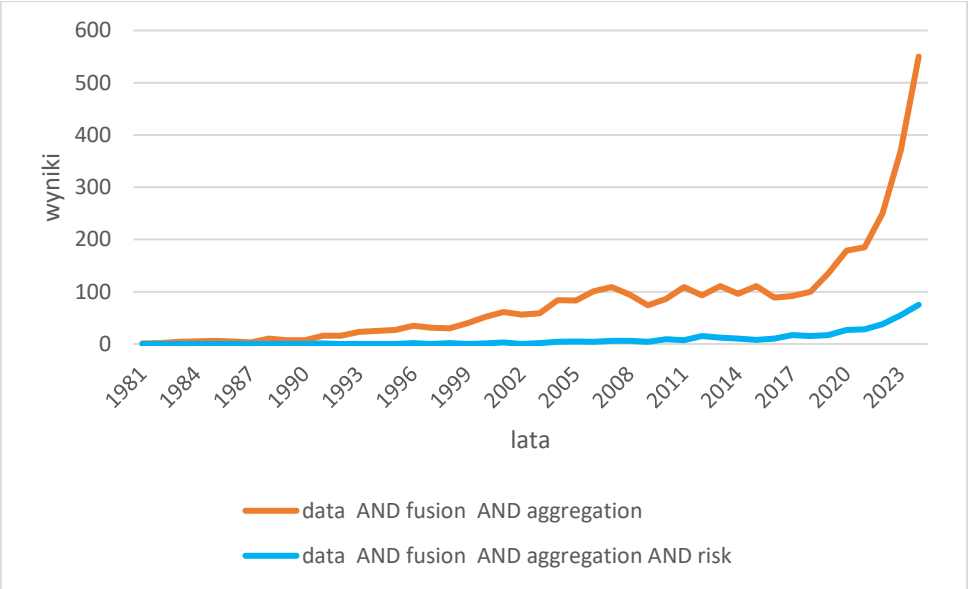
1. data AND fusion AND disaster – 1525 rezultatów
2. data AND fusion AND industry AND disaster – 49 rezultatów
3. random AND field AND risk – 6378 rezultatów
4. random AND field AND risk AND data AND fusion – 58 rezultatów
5. data AND fusion AND aggregation – 3673 rezultatów
6. data AND fusion AND aggregation AND risk – 382 rezultatów



Rys. 28. Wyniki wyszukiwania w bazie SCOPUS wskazujące na wyraźne przyspieszenie trendu rosnącego dla punktów 1 i 2, 26.11.2024.



Rys. 29. Wyniki wyszukiwania w bazie SCOPUS wskazujące na wyraźne przyspieszenie trendu rosnącego dla punktów 3 i 4, 26.11.2024.

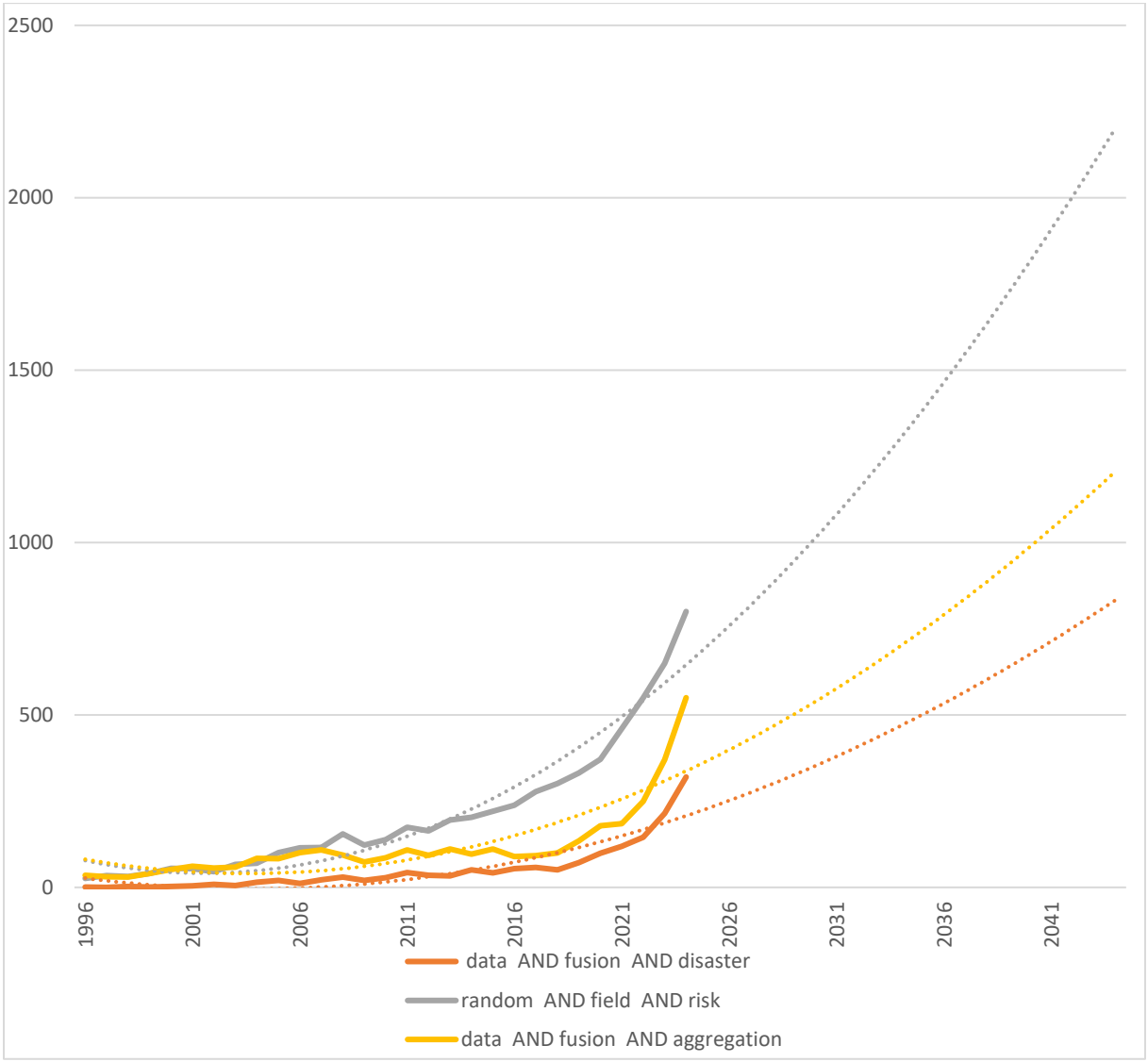


Rys. 30. Wyniki wyszukiwania w bazie SCOPUS wskazujące na wyraźne przyspieszenie trendu rosnącego dla punktów 5 i 6, 26.11.2024.

Tabelaryczne zestawienie rezultatów z podaniem ilości odwołań *accurate* i wyznaczeniem współczynnika *precision* zamieszczono poniżej w [Tab. 13]. Wyniki określone jako *accurate* są konsekwencją zawężenia puli wyników ogólnych do wyników najbardziej odpowiadających intencji prowadzonych badań, innymi słowy są najbardziej trafne względem pytania badawczego, minimalizując liczbę nieistotnych lub błędnych wyników. *Precision* wskazuje jaka część otrzymanych w wyniku zapytania wyników odpowiada kryteriom i oczekiwaniom prowadzonych badań.

Tab. 13 Wyniki wyszukiwania w bazie Scopus.

SCOPUS			
Inquiry	**Results**	**Accurate results**	**Precision**
data AND fusion AND disaster	1525	6	3,57E-03
data AND fusion AND disaster AND industry	49	6	1,07E-01
random AND field AND risk	6378	14	1,62E-03
random AND field AND risk AND data AND fusion	58	15	1,84E-01
data AND fusion AND aggregation	3673	10	2,03E-03
data AND fusion AND aggregation AND risk	382	10	2,33E-02



Rys. 31. Prognozy wzrostu liczby publikacji indeksowanych w SCOPUS w kolejnych latach.

Prognoza wzrostu wyników wyszukiwania zaprezentowana na [Rys. 31] obliczona została w oparciu o linie trendu adaptacyjnego wielomianowego 2 stopnia.

Analogiczne przeszukiwania prowadzone były również w bazie IEEE Xplore (na dzień 27.11.2024):

1. data AND fusion AND disaster – 792 rezultatów
2. data AND fusion AND industry AND disaster – 38 rezultatów
3. random AND field AND risk – 1794 rezultatów
4. random AND field AND risk AND data AND fusion – 34 rezultataty
5. data AND fusion AND aggregation – 1700 rezultatów
6. data AND fusion AND aggregation AND risk – 28 rezultatów

Zestawienie omawianych metod fuzji danych i informacji ze wskazaniem możliwości implementacji w środowisku przemysłowym przedstawiono w [Tab. 14].

Tab. 14 Metody przetwarzania danych wraz z obszarami potencjalnego zastosowania.

Autorzy	Rok wydania	Omawiane metody przetwarzania danych	Możliwości wykorzystania
De Vita, F., Bruneo, et al.	2020	Analiza warstw danych Ekstrakcja danych	Wykrywanie anomalii Drzewa decyzyjne
Diez-Olivan, A., Del Ser, et al.	2019	Ekstrakcja i analiza cech Eksploracja danych	Optymalizacja produkcji Wykrywanie anomalii
Guo, J., Wu, X., et al.	2020	Mapowanie danych Agregacja/eksploracja danych	Architektura procesowa
Martínez-Frutos, J., Herrero-Pérez, D., et al.	2018	Analiza wielokryterialna	Optymalizacja topologii i ryzyka
Lo, M.K., Leung, Y.F., et al.	2021	Analiza różnic i elementów	Analiza niezawodności
Li, X., Zhang, L., Xiao, T., et al.	2019	Ekstrakcja i analiza danych	Analiza niezawodności
Huang, J., Lyamin, A.V., et al.	2013	Szacowanie prawdopobieństw Analiza probalistyczna	Szacowanie ryzyk
Christou, V., Bocchini, P., et al.	2016	Aproksymacja danych Analiza probalistyczna	Analiza ryzyk Zagrożenia zmienne
J. Bao, X. Liu, et al.	2020	Analiza wielokryterialna Agregacja danych	Preferencje decydentów Analiza obrazu Wykrywanie anomalii
Chen, C., Fragonara, L.Z., et al.	2021	Mapowanie danych Agregacja danych	Analiza obrazu Chmury punktów
Fu, C., Dong, C., et al.	2021	Ekstrakcja i analiza danych	Predykcja zachowań
Islam, M.A., Anderson, D.T., et al.	2020	Agregacja danych	Analiza obrazu
Zhang, Y., Jiang, et al.	2019	Agregacja danych Analiza statystyczna	Analiza ilościowa i jakościowa, Szacowanie ryzyk
Bécue, A., Praça, I., et al.	2021	Ekstrakcja i analiza danych	Optymalizacja i analiza ryzyk Wykrywanie anomalii

4.2.1 Podsumowanie wyników badań

Badania w zakresie metod fuzji danych prowadzone były z ukierunkowaniem na środowiska przemysłowe, zwłaszcza przemysł ciężki, ze względu na znaczną specyfikę funkcjonowania tego typu obszarów działalności człowieka oraz wymagania stawiane w sytuacjach, z jakimi zmierzyć musi się decydent w trakcie procesu decyzyjnego. Znaczna część analizowanych publikacji nie skupia się jedynie na zagrożeniach i przetwarzaniu danych dotyczących zagrożeń naturalnych (takich jak będące głównym przedmiotem pracy osunięcia gruntu czy zalania) ale podchodzi do tematu kompleksowo uwzględniając w swych algorytmach również zmienne związane z innymi aspektami funkcjonowania przedsiębiorstwa. Podejście takie

wydaje się jak najbardziej zasadne, bo podejmowane decyzje powinny uwzględniać wszystkie czynniki i prezentować je w sposób maksymalnie uniwersalny.

Modele przetwarzania analizy danych eksploatowane w warunkach przemysłowych tworzone są w oparciu o metodologię Cross Industry Standard Process for Data Mining [Diez-Olivam i in., 2019]. Metodologia ta pozwala prowadzić proces analizy i przetwarzania danych wzdłuż kierunku przepływu pracy w rozumieniu procesu traktowanego jako proces biznesowy. Podejście takie jest niejako naturalnym rozwinięciem modelu funkcjonującego już w wielu przedsiębiorstwach na płaszczyźnie biznesowej, która w trakcie rozwoju firmy była tworzona w pierwszej kolejności. Ułatwia to zrozumienie metodyki, zwłaszcza w początkowej fazie wdrożenia i pracy systemu produkcyjnego.

Kluczowym elementem w projektowaniu, wdrażaniu i eksploatacji systemów wspomagających procesy decyzyjne jest baza danych zasilana danymi z różnych źródeł, o możliwie szerokim spektrum, w którym nie może zabraknąć informacji o pogodzie, ostrzeżeń meteorologicznych o zjawiskach gwałtownych i trudno prognozowanych w korelacji z danymi historycznymi i przebiegiem zdarzeń dla konkretnych przypadków. Do tego dodać należy informacje uzupełniające, czyli kroki i środki zaradcze dla zdarzeń archiwalnych. Wsparciem dla decydenta coraz częściej staje się sztuczna inteligencja (AI), która analizując posiadane informacje, pomaga podejmować decyzje, a w szczególnych sytuacjach podejmuje je autonomicznie. Decyzje te mogą obejmować swym zakresem obszary makro jak i mikro z punktu widzenia każdego podmiotu.

Klasyczne podejście do analizy wielokryterialnej [Bao i in., 2020] zmierza do zaproponowania rozwiązań optymalnych (często wielu rozwiązań optymalnych), co w trudnym położeniu stawia decydenta, zmuszając go do dokonania ostatecznego wyboru (podjęcia decyzji ostatecznej), ale równocześnie komplikuje sam algorytm decyzyjny. Połączenie analizy jakościowej problemów decyzyjnych z wiedzą ekspercką wykorzystywane jest również w teorii grafów czy też teorii systemów eksperckich wspieranych symulacjami jakościowymi prowadzonymi w czasie rzeczywistym. To rozwiązanie jednak również może doprowadzić do silnego wzrostu skomplikowania modelu dla złożonych zagadnień decyzyjnych [Islam i in., 2020]. Należy też zaznaczyć, że systemy eksperckie bazują na zbiorze reguł i scenariuszy, stworzonych i pozyskanych w oparciu o wiedzę i doświadczenie osób uznanych za ekspertów w danym obszarze, a więc, co łatwo zauważyć, każde odchylenie czy zdarzenie wcześniej niezarejestrowany (nieznane) interpretowane jest jako błąd.

Optymalna z punktu widzenia wszechstronności wykorzystania różnych i pochodzących z różnych źródeł danych jest metoda oparta na agregacji danych z uwzględnieniem ich wartości historycznych, co jest pewnego rodzaju predykcją. Dodatkowo, tego typu podejście pozwala tworzyć trendy, w prosty sposób eliminując dane przypadkowe (ewidentnie błędne)

unikając w ten sposób wyników chwilowych ekstremalnych, zwiększając stabilność i odporność samej metody [Islam i in., 2020]. Agregacja, analiza i przetworzenie (fuzja) danych opiera się na:

1. Pozyskaniu danych z dostępnych dla systemu czujników, detektorów i innych elementów całego systemu wykorzystywanych jako źródło danych.
2. Wygenerowaniu rozkładu gaussowskiego dla zagregowanych danych.
3. Wygenerowaniu BPA (Basic Probability Assignment) dla poszczególnych zagrożeń.
4. Fuzji danych i podjęciu decyzji z uwzględnieniem BPA wyliczonych w punkcie 3.
5. Punktem dodatkowym, podnoszącym sprawność decyzyjną (adekwatność podjętych decyzji), ale nie wymaganym, jest dodanie kroku łączącego przeprowadzoną analizę z wiedzą ekspercką. Daje to decydentowi dodatkowy argument poparty często unikalną wiedzą i doświadczeniem.

Podobne podejście zaproponować można dla analiz punktowych, np. miejscowych osunięć gruntu, bez analizy dalszych konsekwencji jakie to może za sobą pociągnąć [Li i in., 2019], czyli kroki: zebranie danych z czujników, wygenerowanie rozkładu Gaussa, fuzja i porównanie z metodami eksperckimi. W tym konkretnym przykładzie beyessowska metoda identyfikacji może zostać użyta do wykorzystania danych z monitoringu, a jej wydajność będzie wzrastać wraz z liczba punktów obserwacyjnych [Li i in., 2019].

Tak prowadzona analiza danych powinna być oparta o podejście stochastyczne, które w przeciwieństwie do podejścia deterministycznego prowadzi do kompleksowego opisu zdarzania i proponowanego rozwiązania problemu decyzyjnego, co z kolei przekłada się wprost na zwiększenie jego niezawodności [Vadlamani, 2019]. Problemem może być wzrost wymagań obliczeniowych, ale wydaje się, że dzisiejsza technika przetwarzania danych sprosta tym wymaganiom. Jest to zgodne z trendem, jakim jest wykorzystanie wielowymiarowych pól losowych. Tutaj właściwa do wykorzystania wydaje się metoda SROM (Stochastic Reduced-Order Models) wykorzystywana do rozwiązywania problemów inżynierskich.

Ogólna architektura systemu, z punktu widzenia fuzji danych powinna zawierać [Guo i in., 2020]:

1. Warstwę danych, stanowiącą fundament systemu analizy.
2. Warstwę usług, gromadzącą informacje spływające z wielu różnych źródeł wspomnianych we wcześniejszej części podsumowania.
3. Warstwę aplikacji, czyli system zarządzający relacyjną bazą danych z interfejsem dla użytkownika końcowego w postaci GUI.

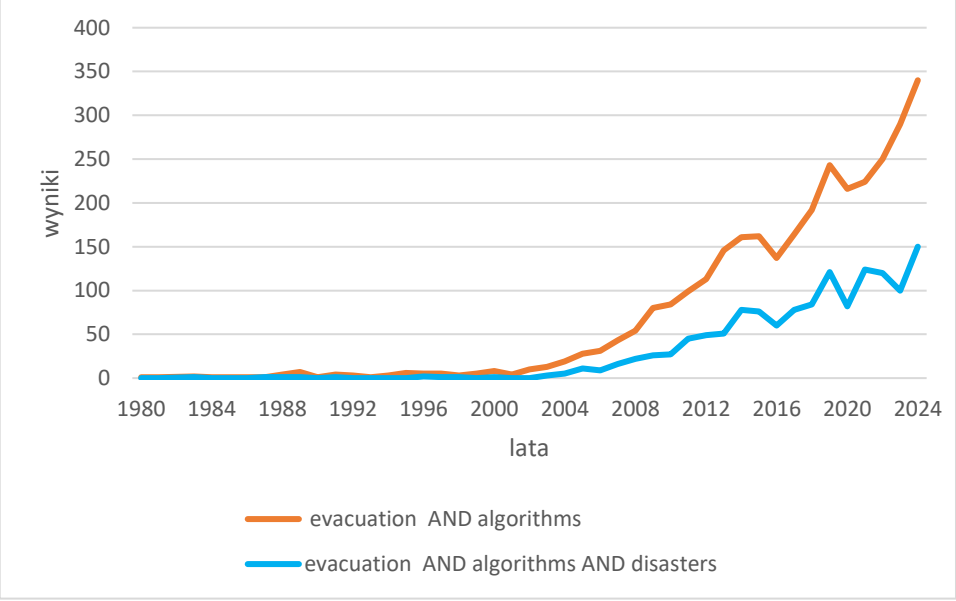
4.3 Taksonomia i algorytmy ewakuacji

Tematyka badana w tym rozdziale związana jest bezpośrednio z zagadnieniami ewakuacji osób i mienia z obszarów zagrożonych katastrofami lub klęskami żywiołowymi, co w przypadku Zakładu Górniczego jakim jest KWC, w efekcie końcowym prowadzi do tego problemu stawianego decydentom, tj. wybór właściwego algorytmu ewakuacji.

Badania skupiły się na analizie opisanych w literaturze ścieżek postępowania oraz w efekcie końcowym - wyborze rozwiązania lub rozwiązań optymalnych dla zdanego przypadku. Trudność polegała głównie na tym, że zdecydowana większość opracowań skupia się na problemach ewakuacyjnych dużych skupisk ludzkich, zwłaszcza z obiektów budowlanych oraz miejsc zgromadzeń. Jest to sprzeczne z założeniami stawianymi w temacie pracy, niemniej jednak pewna grupa artykułów spełnia wymagane kryteria, a ich analiza zaprezentowana jest w dalszej części pracy.

Słowa kluczowe użyte w kolejnych iteracjach przeszukiwania bazy SCOPUS (na dzień 26.11.2024):

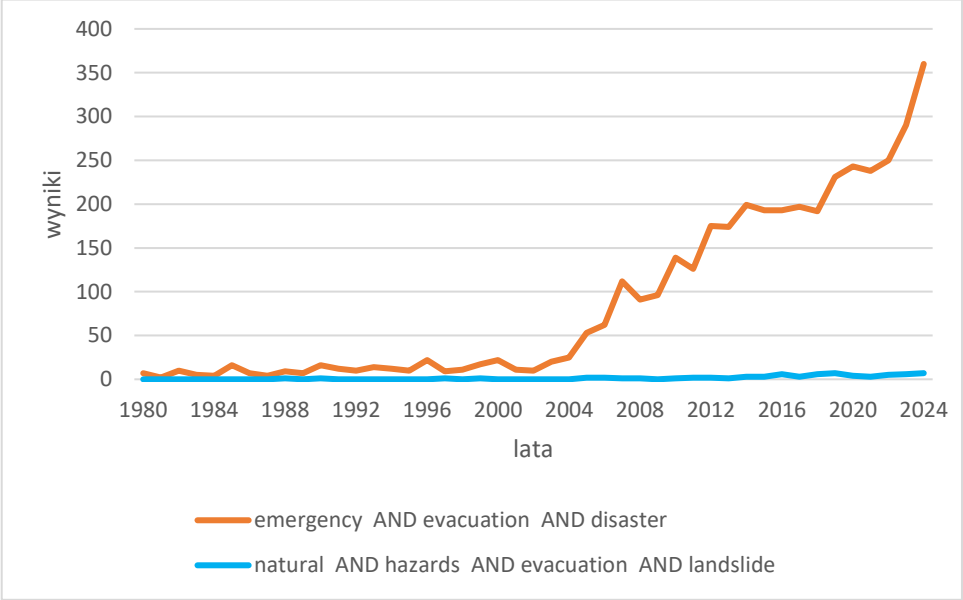
1. evacuation AND algorithms – 3145 rezultatów
2. evacuation AND algorithms AND disasters – 1312 rezultatów
3. emergency AND evacuation AND disaster – 3941 rezultatów
4. natural AND hazards AND evacuation AND landslide – 70 rezultaty



Rys. 32. Prezentacja wyników wskazujących na wyraźny wzrost trendu dla zapytań 1 i 2, 26.11.2024.

Wyniki zaprezentowane odpowiednio na rysunkach [Rys. 32] i [Rys. 33] obrazują jak znacząco wzrasta zainteresowanie problematyką wykorzystującą algorytmy, czyli metody wspomagające podejmowanie decyzji. Tematyka dotycząca tego obszaru zaczęła być

analizowana i opisywana począwszy od roku około 2002 i jej istotność systematycznie wzrasta w latach kolejnych. Należy zakładać, że trend ten utrzyma się potwierdzając rosnącą rolę AI w procesach zarządzania sytuacjami kryzysowymi.

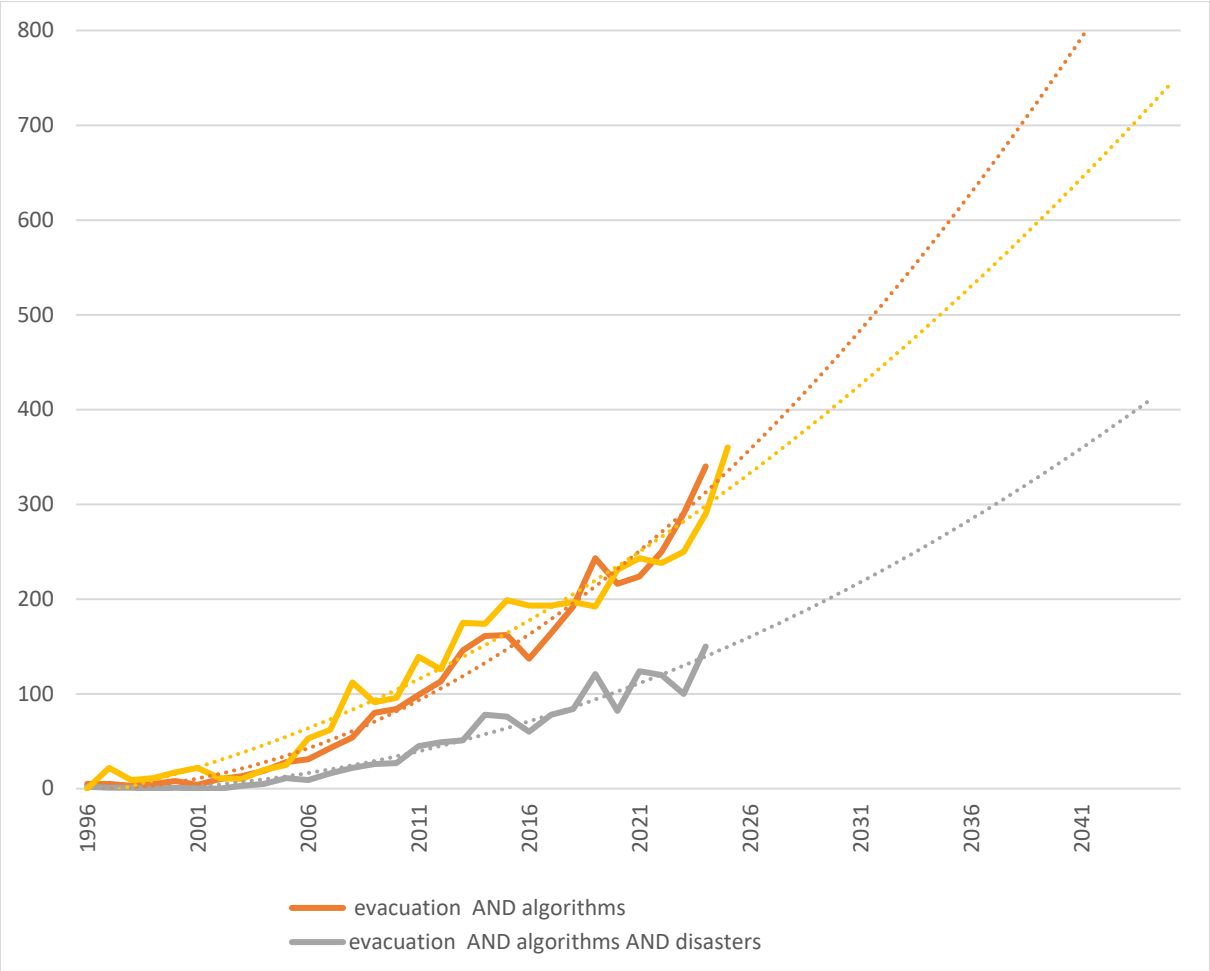


Rys. 33. Prezentacja trendu wzrostowego dla zapytań 3 i 4, 26.11.2024.

Tabelaryczne zestawienie rezultatów z podaniem ilości odwołań *accurate* i wyznaczeniem współczynnika precision zamieszczono poniżej [Tab. 15]. Znaczenie pojęć *accurat* i *precision* omówiono przy analizie danych zawartych w [Tab. 13].

Tab. 15. Wyniki wyszukiwania w bazie Scopus , 26.11.2024.

SCOPUS			
Inquiry	**Results**	**Accurate results**	**Precision**
evacuation AND algorithms	3145	14	3,05E-03
evacuation AND algorithms AND disasters	1312	14	7,16E-03
emergency AND evacuation AND disaster	3941	6	9,88E-04
natural AND hazards AND evacuation AND landslide	70	10	9,43E-02



Rys. 34. Prognoza wzrostu wyników indeksowanych w SCOPUS w kolejnych latach.

Prognoza wzrostu wyników wyszukiwania zaprezentowana na [

Rys**. 49**] obliczona została w oparciu o linie trendu adaptacyjnego wielomianowego 2 stopnia.

W związku z częściową i często opóźnioną indeksacją artykułów IEEE w bazie SCOPUS, analogiczne przeszukiwania prowadzone były również w bazie IEEE Xplore (stan na dzień 27.11.2024):

1. evacuation AND algorithms – 814 rezultatów
2. evacuation AND algorithms AND disasters – 281 rezultatów
3. emergency AND evacuation AND disaster – 653 rezultatów
4. natural AND hazards AND evacuation AND landslide – 3 rezultaty

W dalszej kolejności wyniki zawężane były do obszarów tematycznie zbliżonych do przedmiotu badania poprzez filtry zawężające [Vieira i in., 2022], [Shi i in., 2023].:

- Engineering,
- Decision Making,
- Language – English,

Wybór ostateczny związany był z koniecznością analizy treści wytypowanych wstępnie artykułów pod kątem ich adekwatności dla zadanego obszaru badawczego[Reyes-Riveros i in., 2021]. Pozwoliło to wybrać materiały najbardziej tematycznie związane z obszarem poszukiwań, a tym samym wyeliminować te, które pomimo zgodności słów kluczowych dotyczyły innego obszaru lub środowiska.

W ten sposób przeprowadzona analiza doprowadziła do wyboru najbardziej pożądanych wyników, które zaprezentowane zostały poniżej wraz z wypunktowaniem najważniejszych treści, zawartych w poszczególnych pracach i mających potencjalny wpływ na ostateczny wybór metod zaprezentowanych przez[Guo i in., 2020].

Zestawienie wykorzystanych w literaturze algorytmów oraz wskazanie najczęstszych kierunków prowadzonej analizy przedstawiono w [Tab. 16].

Tab. 16. Analiza wykorzystanych modeli i algorytmów.

lp.	Algorytm/algorytmy	Kryteria ewakuacji	Prezentowane podejście / sposób wykorzystania algorytmu	Rok wydania, autorzy publikacji	Przydatność dla IRM DSS w KWC
1	Algorithm for the Search of Potentially Suitable Evacuation Points	Rozwiązaniem problemu jest wyznaczenie najkrótszej drogi (ewakuacja) do bezpiecznego punktu. Dopuszcza się korektę punktu ewakuacyjnego.	Łączenie map ryzyk. Łączenie map zagrożeń. Analiza przestrzenna.	2021 [Korolov i in.]	duża
2	Algorithm DRTCCR (Dynamic Real-Time Capacity Constrained Routing)	Dobór miejsc bezpiecznych optymalnych pod względem chwilowej dostępności. Dobór z uwzględnieniem minimalnego czasu oczekiwania	Dynamiczny routing z ograniczona przepustowością dróg (uwzględnianą dynamicznie w trakcie ewakuacji).	2020 [Korolov i in.]	duża
3	Particle Swarm Optimisation (PSO) algorithm	Dobór miejsc bezpiecznych z uwzględnieniem zmiany parametrów w trakcie (zmian dostępności, zmiana ilości ewakuowanych obiektów, zmian obszaru	Modele lokalizacji/przydziału. Utworzenie modelu statycznego dla każdego etapu ewakuacji, weryfikacja pod względem dostępności, korekta odległości, uwzględnienie zmiennych dynamicznych.	2020 [Quin i in.]	średnia

lp.	Algorytm/algorytmy	Kryteria ewakuacji	Prezentowane podejście / sposób wykorzystania algorytmu	Rok wydania, autorzy publikacji	Przydatność dla IRM DSS w KWC
		zagrożenia).			
4	Particle Swarm Optimisation (PSO) algorithm SA-PSO Algorithm	Alokacja jednostek ewakuowanych w miejscach bezpiecznych, z uwzględnieniem indywidualnych priorytetów.	Algorytm ewolucyjny o dużej wydajności.	2020 [Wang i in.]	duża
5	Simulated Annealing (SA) algorithm	Alokacja jednostek ewakuowanych w miejscach bezpiecznych, z uwzględnieniem indywidualnych priorytetów.	Rozwinięcie algorytmu wyszukiwania lokalnego, przyjmuje gorsze rozwiązania z mniejszym prawdopodobieństwem, w celu uniknięcia minimum lokalnego.	2020 [Wang i in.]	średnia
6	Non-dominated Sorted Genetic Algorithm II (NSGA-II)	Znalezienie optymalnego czasu ewakuacji i odpowiedniego przydziału miejsc bezpiecznych (schronów).	Algorytmy ewolucyjne, strojenie parametrów.	2020 [Niyomubyeyi i in.]	średnia
7	Archive Multi-objective Simulated Annealing (AMOSA)	Znalezienie optymalnego czasu ewakuacji i odpowiedniego przydziału miejsc bezpiecznych (schronów).	Reprezentuje algorytmy oparte na fizyce/chemii.	2020 [Niyomubyeyi i in.]	średnia
8	Multi-objective Arificial Bee Colony (MOABC)	Znalezienie optymalnego czasu ewakuacji i odpowiedniego przydziału miejsc bezpiecznych (schronów).	Reprezentują algorytmy oparte na inteligencji roju.	2020 [Niyomubyeyi i in.]	średnia
9	RefSet	Optymalizacja w zależności od analizowanych kryteriów.	Punkty odniesienia, rozwiązania kompromisowe.	1997 [Skulimowski]	niezbędny
10	Algorytm Dijkstra	Ewakuacja do miejsca bezpiecznego (wyznaczenie trasy minimalnej) uwzględniająca wariant: jeden do	Model maksymalnego przepływu. Uwzględnienie założeń: 1 start i docelowo 1 stop. Wymagana znana liczba pojazdów ewakuowanych, znane	2014 [Li i in.]	mała

lp.	Algorytm/algorytmy	Kryteria ewakuacji	Prezentowane podejście / sposób wykorzystania algorytmu	Rok wydania, autorzy publikacji	Przydatność dla IRM DSS w KWC
		wielu i optymalizacja w planowaniu.	parametry rasy, iteracja uwzględnia kolejne skrzyżowania.		
11	Weighted Linear Combination (WLC)	Ocena i optymalizacja wydajności sieci transportowej.	Analiza hierarchiczna. Ocena ryzyka. Integracja z metodami wielokryterialnymi w celu analizy wskaźników i dopasowania optymalnych modeli wyboru tras ewakuacji.	2019 [Ghavami]	niezbędny
12	Algorytm Analytic Hierarchy Process (AHP)	Minimalizacja wskaźników ilościowych i jakościowych dotyczących procesu ewakuacji w celu wyznaczenia optymalych tras ewakuacji.	Analiza hierarchiczna. Analizy ryzyka. Metoda bazująca na wiedzy eksperckiej.	2021 [Ganiehi i in.]	średnia
13	Cross-Impact Analysis Interpretatice Structural Modeling (CIA-ISM)	Nauka w oparciu o scenariusze, optymalizacja scenariuszy, tworzenie planów awaryjnych, rekomendowanie działań.	Wykonanie pomiaru efektu wzmacniającego lub kaskadowego zakłócenia w przebiegu zdarzenia.	2021 [Banuls i in.]	duża
14	Branch-and-price matheuristic algorithm	Wyznaczenie dróg ewakuacji z punktami pośrednimi niezbędnymi do uwzględnienia, optymalizacja tras z uwzględnieniem specyfiki wymagań konkretnego pojazdu.	Budowa i analiza drzewa ewakuacyjnego, wszyscy ewakuowani są kierowani jedną ścieżką do węzła/schronu. Algorytm ma na celu znalezienie najlepszego drzewa ewakuacji, w którym każda ścieżka minimalizuje czas ewakuacji i spełnia ograniczenia kolejnych ruchów.	2022 [Purba i in.]	duża
15	Pythagorean Theorem (PT) and Dijkstras Algorithm (DA)	Wyznaczenie najkrótszej trasy ewakuacji z uwzględnieniem istniejących oraz pojawiających się przeszkód.	PT - znalezienie najkrótszej drogi pomiędzy kolejnymi węzłami na trasie ewakuacji DA - znajdowanie/obliczanie odległości pomiędzy węzłami.	2022 [Ibrahim i in.]	średnia

lp.	Algorytm/algorytmy	Kryteria ewakuacji	Prezentowane podejście / sposób wykorzystania algorytmu	Rok wydania, autorzy publikacji	Przydatność dla IRM DSS w KWC
16	Crowd Density-based Reciprocal Velocity Obstacle (CD-RVO)	Ewakuacja, sterowanie przepływem jednostek ewakuowanych w celu uniknięcia zatorów, uwzględnia zmienną prędkość ruchu ewakuowanych jednostek.	Zbadanie związku pomiędzy zagęszczeniem jednostek ewakuowanych a średnią prędkością pojedynczej jednostki. Gęstość wpływa na zmianę prędkości.	2022 [Zhang i in.]	niepewna
17	Salp Swarm Algorithm / Hybrid Salp Swarm Algorithm	Optymalizacja czasu ewakuacji w drodze optymalizacji trasy (uwzględniając jej długość, przejezdność, obciążenie ruchem).	Poprzez grupowanie optymalizuje schematy ewakuacji wybiera optymalne ścieżki/trasy pojazdów.	2022 [Duan i in.]	niepewna
18	Quadrant Shirnking Method (QSM) Quadrant Shrinking Heuristic (QSH)	Dynamiczny i statyczny routing tras ewakuacji oraz przydział służb ratunkowych (personelu ratunkowego), wspomagane przez algorytm heurystyczny	Podejście dynamiczne uwzględnia zmiany parametrów rozwiązywanego problemu w trakcie trwania zdarzenia, uwzględnia zmienność popytu na usługi w zależności od przebiegu zdarzenia w różnych lokalizacjach, wagi sprawiedliwości podziału środków uwzględniają zmianę zapotrzebowania w trakcie trwania zdarzenia.	2023 [Tarhan i in.]	duża
19	Algorytm oparty na rozmytym grupowaniu hierarchicznym	Lokalizacja miejsc bezpiecznych i rozdział ewakuowanych jednostek, minimalizacja ofiar.	Opracowano wielocelowy model optymalizacyjny w celu rozwiązania problemu przydzielania ewakuowanych jednostek do optymalnych dla nich miejsc bezpiecznych. Wyniki wykorzystywane są w kolejnej iteracji do ustalenia priorytetów zaopatrzeniowych. Grupowanie	2023 [Geng i in.]	niepewna

lp.	Algorytm/algorytmy	Kryteria ewakuacji	Prezentowane podejście / sposób wykorzystania algorytmu	Rok wydania, autorzy publikacji	Przydatność dla IRM DSS w KWC
			hierarchiczne w celu optymalnego doboru schronu zgodnie z potrzebami/wymaganiami ewakuowanej jednostki.		
20	Algorytm A*	Definiowane cechy tras ewakuacji; szerokość, długość, otoczenie (np. przeszkody i inne utrudnienia) warstwa dróg, przeszkód, miejsc bezpiecznych, mapa fizyczna.	Wielościeżkowe planowanie tras, które uwzględnia trasy od jednego punktu początkowego do kilku schronów i uwzględnia liczbę ewakuowanych oraz liczbę ewakuowanych, których może przyjąć każdy schron, w zależności od skali katastrofy.	2008 [Likhachev i in.]	duża
21	Cuckoo Search Algorithm CSA	Wyszukiwanie najlepszej trasy ewakuacji, pomiędzy kolejnymi miejscami bezpiecznymi, uwzględniając czasoprzestrzenne warunki każdej lokalizacji w odniesieniu dla zagrożenia całościowo i odnosząc się do jego eskalacji.	Podejście uwzględnia wiele czynników, w tym położenie, ilość przeszkód, warunki zmienne. Oceniając te parametry, każdemu obszarowi przypisujemy wagę czynnika ryzyka, mając na celu zminimalizowanie potencjalnego zagrożenia.	2023 [Spyrou i in.]	mała
22	Chain Flow Algorithm	Minimalizacja kosztu i maksymalizacja przepływu.	Przepływ łańcuchowy definiowany jako przepływ wzdłuż ukierunkowanej trasy.	2023 [Takahashi i in.]	niepewna
23	Lagrangian Relaxation (LR)	Optymalizacja punktów odbioru i tras pojazdów ratowniczych.	Uwzględniane problemu zakłócenia w punktach zbiórki, wstępnych i zapasowych punktów ewakuacji, planowania tras pod kątem ich niezawodności.	2023 [Jiang i in.]	średnia

lp.	Algorytm/algorytmy	Kryteria ewakuacji	Prezentowane podejście / sposób wykorzystania algorytmu	Rok wydania, autorzy publikacji	Przydatność dla IRM DSS w KWC
24	Mixed Integer Programs - Large Neighborhood Search (MIP-LNS)	Optymalizacja funkcji celu, w tym przypadku głównie optymalizacja tras i harmonogra-mów.	Planowanie tras ewakuacji ludzi z terenów objętych zagrożeniem, biorąc pod uwagę ich rozproszone rozmieszczenie w terenie. Cele do minimalizacji: średni czas ewakuacji i czas zakończenia całej ewakuacji.	2023 [Islam i in.]	średnia

4.4 Przegląd literatury na temat informatycznych systemów zarządzania bezpieczeństwem

Informatyczne systemy zarządzania bezpieczeństwem mają swoje korzenie w rozwoju technologii informacyjnych i potrzebie zwiększenia kontroli oraz monitorowania bezpieczeństwa w różnych obszarach funkcjonowania człowieka. Pierwsze tego typu systemy pojawiły się w latach 60. i 70. XX wieku, kiedy przedsiębiorstwa zaczęły wykorzystywać komputery do automatyzacji procesów administracyjnych oraz produkcyjnych. W tym czasie bezpieczeństwo było postrzegane głównie w kontekście fizycznym (ochrona obiektów, nadzór nad pracownikami) oraz technicznym (bezpieczeństwo maszyn, zarządzanie awariami).

W latach 80. wraz z rozwojem technologii cyfrowych i wzrostem dostępności komputerów, firmy zaczęły wdrażać bardziej złożone systemy do zarządzania bezpieczeństwem w zakładach pracy. Początkowo systemy koncentrowały się na ochronie fizycznej budynków i infrastruktury. Tworzone były złożone sieci systemów monitoringu, alarmów oraz kontroli dostępu, aby chronić zakłady pracy przed zagrożeniami takimi, jak włamania, pożary czy wypadki. W kolejnych latach zaczęły się pojawiać pierwsze systemy służące do ochrony informacji cyfrowych oraz systemy do zarządzanie bezpieczeństwem technicznym i przemysłowym. Coraz częściej pojawiały się potrzeby łączenia różnych systemów zarządzania bezpieczeństwem w jedną, spójną platformę. Powstawały zintegrowane systemy, które łączyły zarządzanie bezpieczeństwem fizycznym, technicznym i informacyjnym, które ze względu na złożoność wyposażone musiały być w moduły odpowiedzialne za wsparcie w realizacji procesów decyzyjnych.

Wstępne badania rozważań projektowych systemu dla wspomagania decyzji zarządzania kryzysowego zostały przedstawione przez [Belardo i in., 1984], natomiast zasady ogólnego zarządzania kryzysowego DSS zostały omówione w artykule [Marovac, Stähly, 2001].

Ewolucja informatycznych systemów zarządzania bezpieczeństwem związana była z rozwojem technologii oraz coraz większą potrzebą integracji różnych obszarów bezpieczeństwa, opis badań w dziedzinie systemów informacyjnych do reagowania i zarządzania kryzysowego do końca ubiegłego stulecia oraz ich perspektywy rozwojowe, w dużej mierze trafne, można znaleźć w systemie informacji o zarządzaniu kryzysowym i indeksie referencyjnym (EMISARI) w Biurze Przygotowania na Kryzysy (OEP) w USA [Turoff, 2002]. System EMISARI w sposób nowatorski umożliwił użytkownikom rozsianym po całych Stanach Zjednoczonych skoordynowane reagowanie na sytuacje kryzysowe już w latach 70. Funkcjonowanie tego systemu zostało poprawione i rozszerzone, efektem czego był Dynamiczny System Informacji Zarządzania Reagowaniem Kryzysowym (DERMIS), który zawierał zestaw ogólnych zasad projektowych zapewniających ramy i kierunki dla rozwoju elastycznych i dynamicznych systemów informacyjnych reagowania kryzysowego [Campbell i in., 2004]. Wytyczne dotyczące systemów wspomagania decyzji związanych z katastrofami obejmują zakładają wykorzystanie DSS do tworzenia strategii ewakuacji np. w przypadku powodzi [Windhouwer i in., 2004] lub do planowania lokalizacji wyznaczenia stref bezpiecznych na obszarach katastrof z wykorzystaniem metod wielokryterialnych [Degener i in., 2013]. Nowoczesne systemy zarządzania bezpieczeństwem coraz częściej korzystają z automatyzacji oraz sztucznej inteligencji (AI) do monitorowania procesów w czasie rzeczywistym, przewidywania zagrożeń oraz szybkiej reakcji na incydenty. Inteligentne DSS do wsparcia podejmowania decyzji w warunkach niepewności z elementami wnioskowania rozproszonego przedstawiono w [Comes i in., 2014]. Należy również wspomnieć o badaniach dotyczących modelowania scenariuszy współpracy dla ochrony infrastruktury krytycznej [Bañuls i in., 2010; Bañuls i in., 2013; Lopez-Silva i in., 2015; de la Huerga i in., 2015; Turoff, 2014; Turoff i in., 2017], które są fundamentalne dla projektu IRM DSS dla KWC.

W ostatnich latach w ramach projektów realizowanych w ramach m.in. Programów Ramowych UE powstało kilka prototypowych systemów klasy IRM DSS. Badacze [Simões-Marques i in., 2019] przedstawiają pierwsze testy użytkowników systemu wspomagania decyzji zarządzania kryzysowego opracowanego w ramach projektu THEMIS (DisTributed Holistic Emergency Management Intelligent System [Simões-Marques i in., 2019]. Prototyp systemu THEMIS wykorzystuje oparty na sztucznej inteligencji system wspomagania decyzji dla osób zarządzających (decydentów) odpowiedzialnych za koordynowanie procesów zarządzania akcją ratowniczą w przypadku katastrof oraz ratowników, czyli osób bezpośrednio zaangażowanych w akcję ratunkową. Architektury systemu klasy DSS, dostosowane systemu do optymalizacji dystrybucji pomocy podczas klęsk żywiołowych, w tym zapewnienie łańcuchów dostaw i zagadnienia związane z wyznaczaniem optymalnych tras pojazdów, omówione zostały przez [Sepulveda, Bull, 2020]. Nowoczesne systemy koncentrują się nie tylko na zapobieganiu zagrożeniom, ale także na zapewnieniu ciągłości

działania w sytuacjach kryzysowych, kwestia to poruszona została przez [Turoff i in., 2016]. Przeprowadzona analiza omawia problem systemowego powiązania między 16 komponentami infrastruktury krytycznej. Zaprezentowane w niej zależności mogą służyć jako tło do badania optymalnych struktur oprogramowania i wzajemnego dopasowania takich struktur w zaawansowanym systemie wspomagania decyzji. Idee te były kontynuowane w specjalnym wydaniu czasopisma TFSC poświęconym predykcji i zwiększaniu odporności na przyszłe katastrofy [Hernantes i in., 2017]. Kluczowe znaczenie, a zarazem aspekt praktyczny prezentowanego podejścia do zapewnienia interoperacyjności systemów klasy DSS w sytuacjach kryzysowych zostały zbadane i potwierdzone w ramach zrealizowanego projektu badawczego ISYCRI (Interoperability of Systems in CRIsis [Daclin, Chapurlat, 2009]).

Współczesne systemy oparte na AI, automatyzacji oraz zaawansowanych technologiach monitorowania stają się kluczowe w sektorach takich, jak energetyka, finanse, przemysł czy administracja publiczna. Więcej informacji na temat relacji między AI a zarządzaniem odpornością na katastrofy można znaleźć w ankiecie przeprowadzonej przez [Saleha, Allaert, 2011], którzy zbadali zachodzące relacje pomiędzy wyzwaniami technologicznymi, takimi jak systemy wczesnego ostrzegania, nawigacja, GIS a możliwości ich analizy z wykorzystaniem optymalizacji wielokryterialnej. Próbę taksonomii metod wsparcia zarządzania katastrofami z wykorzystaniem technik opartych o AI przedstawiono w [Abu Bakar i in., 2016]. Praca ta wykazała, że około 60% narzędzi do zarządzania katastrofami już wtedy wykorzystywało metody opierające się o AI. Udział sztucznej inteligencji (AI) w systemach zarządzania bezpieczeństwem stopniowo zwiększał się od lat 2000, a obecnie jest kluczowym elementem w rozwijających się technologiach monitorowania i zarządzania zagrożeniami. W ostatnich latach AI znalazła szerokie zastosowanie w analizie behawioralnej i zintegrowanych systemach bezpieczeństwa. Dzięki zastosowaniu głębokiego uczenia (deep learning) AI nie tylko analizuje dane, ale też uczy się wzorców zachowań użytkowników, co pozwala na wykrywanie subtelnych i ukrytych zagrożeń. AI ewoluowała od podstawowej analizy danych do zaawansowanych systemów, które autonomicznie monitorują, analizują i reagują na zagrożenia. Integracja AI z IoT oraz rozwój metod głębokiego uczenia pozwala na tworzenie coraz bardziej złożonych i samodzielnych systemów bezpieczeństwa, które są zdolne do szybkiego wykrywania i eliminowania zagrożeń w wielu branżach.

4.5 Wnioski z badań bibliograficznych

Badania literatury w zakresie przeglądu, analizy i wreszcie wyboru optymalnego algorytmu wspomagającego procesy decyzyjne w sytuacji wystąpienia zagrożenia w zakładzie przemysłowym poprzedzone zostały analizą potrzeb mającą na celu zdefiniowanie i sparametryzowanie systemu informacyjnego klasy Systemów Wspomagania Decyzji

(Decision Support Systems, DSS) i określenie priorytetowych funkcjonalności takiego systemu. Zgodnie z definicją zaprezentowaną przez [Ghavami, 2019], DSS jest systemem informatycznym zaprojektowanym i wdrożonym w celu wspierania procesów biznesowych, organizacyjnych i działań decyzyjnych. Rozwinięcie tej definicji, uzupełnione o uproszczony model zaprezentowane zostało przez [Baloian i in. 2019]. Autor ten określa DSS jako interaktywne systemy komputerowe, które pomagają decydentom w wykorzystaniu danych i modeli rozwiązywani wielkokryterialnych problemów. Uproszczony model zbudowany w oparciu o te założenia zakłada następujące etapy: (1) identyfikacja problemu, (2) identyfikacja celu decyzji, (3) fuzja danych, (4) ocena zgodności ze zdefiniowanymi uprzedni celami, (5) wybór optymalnej decyzji połączony z analizą wpływu na środowisko pracy. Model ten zakłada pracę w trybie *anytime computing* [Zilberstein, 1996], w przypadku, gdy ilość posiadanej informacji nie jest wystarczająca do podjęcia decyzji ostatecznej następuje powrót do etapu 2 lub 3. W podejściu tym decyzje nie są podejmowane autonomicznie, a decydent odgrywa kluczowa rolę w procesie podejmowania ostatecznej decyzji, co jest zgodne z zasadami odpowiedzialności za prowadzenie działań zapobiegawczych i ratunkowych w przypadku zagrożenia zakładu.

Na podstawie analizy potrzeb oraz wyników badania delfickiego, planowanie ewakuacji z zagrożonego terenu zostało uznane za priorytetowy problem w zakresie budowy strategii zarządzania ryzykiem [Abusalama i in., 2020], która będzie implementowana w IRM DSS dla KWC. Wdrożenie systemu wspomagającego decyzje w tym obszarze zmierza do zminimalizowania potencjalnych strat ludzkich i majątkowych. Wybór ten potwierdzają także przeprowadzone badania literaturowe, które wskazują, że problematyka analizy ryzyk i tworzenia map ryzyk dla potrzeb ewakuacji jest nieodzownym elementem koncepcji DSS [Tab. 16].

W związku z tym celem badań literaturowych było również wskazanie optymalnego algorytmu wyszukiwania punktów ewakuacji dla K maszyn rozmieszczonych w zagrożonym terenie wraz z wyborem trasy ewakuacji. Algorytm powinien uwzględniać szereg zmiennych decyzyjnych, w tym również informację o ukształtowaniu terenu. Problem decyzyjny posiadający tak zdefiniowane założenia zmierza do znalezienia (obliczenia) najbliższego docelowego miejsca ewakuacji i wyznaczenia najlepszej trasy, którą ma przebiegać ewakuacja z uwzględnieniem przejezdności rozumianej jako drożność trasy oraz przepustowości, czyli ograniczenia liczby ewakuowanych maszyn na wyznaczonej ścieżce. Zarówno przy niespełnieniu warunku przepustowości, jak i drożności konieczna jest korekta i ponowne wyznaczenie trasy.

W przypadku, z jakim mamy do czynienia dla analizowanego zakładu przemysłowego (KWC), należy założyć, że punkty docelowe (punkty ewakuacji), są znane i zdefiniowane, skutkiem czego z przeglądu literatury można wyeliminować pozycje, które zakładały w pierwszej kolejności znalezienie punktów ewakuacji. Tego typu metodyka rozpatrywana

jest głównie dla katastrof o charakterze klęsk żywiołowych, na obszarze rozległym i nie zbadanym na etapie szacowania ryzyk [Bécue i in., 2021]. Metodyki te są wprawdzie uniwersalne, jednak znaczny nakład pracy niezbędny do znalezienia punktów ewakuacji wydaje się w sposób oczywisty eliminować je dla badanego zagadnienia.

W celu tworzenia optymalnego dynamicznego planu ewakuacji stworzony został algorytm *Dynamic Real-Time Capacity Constrained Routing* (DRTCCR) [Abusalama i in., 2020]. Jego celem jest znalezienie najlepszej drogi ewakuacji, poprzez przetwarzanie danych w sposób iteracyjny, dodatkowo jego użycie pozwala skrócić czas ewakuacji oraz koszt obliczeń. Jednak jego użycie ze względów wskazanych wcześniej wydaje się mało zasadne. Podobnie sytuacja wygląda z algorytmem typu PSO (*Particle Swarm Optimisation*) [Qin i in., 2020]. Może on zostać wykorzystany do rozwiązywania złożonych problemów, przy zachowaniu szybkości, odporności na zakłócenia i skuteczności, jednak jego wadą jest możliwość wpadnięcia w pułapkę lokalnego minimum.

Zaproponowany do implementacji algorytm wymaga zdefiniowania założeń wstępnych będących punktem wyjścia do budowy diagramu działania. Są one następujące:

(1) dla danego pojazdu definiujemy jeden punkt docelowy ewakuacji,

(2) dozwolony maksymalny czas ewakuacji jest zdefiniowany,

(3) znana jest przepustowość każdego odcinka trasy pomiędzy kolejnymi węzłami,

(4) dążymy do maksymalizacji liczby ewakuowanych pojazdów i minimalizacji czasu ewakuacji uwzględniając przepustowość [Likhachev i in., 2008].

Po takim zdefiniowaniu kryteriów ewakuacji przystępujemy do gromadzenia danych i nałożenia ich na mapy zagrożonego terenu w korelacji z priorytetami i preferencjami decydentów. Do podjęcia ostatecznej decyzji pomocne będzie wyznaczenie wag kryteriów, które może być dokonane metodami badania współczynników przetargowych pomiędzy poszczególnymi kryteriami i zaimplementowane w systemie przed rozpoczęciem ewakuacji. Stosowane są w tym celu także metody porównań kryteriów parami, wśród których najbardziej popularna jest metoda AHP (Analytic Hierarchy Process, [Ganiehi, 2019]) obarczona jednak istotnymi wadami wynikającymi z przyjętej heurystyki. W związku z tym w celu wyboru rozwiązania kompromisowego i weryfikacji logicznej spójności proponowanego procesu rozwiązania proponowana jest metoda zbiorów odniesienia (RefSet) [Skulimowski, 2023]. Metodologia oparta na zbiorach odniesienia składa się z następujących etapów: (1) budowa modelu uporządkowanej struktury kilku (3-4) klas odniesienia, następnie (2) rozwiązanie poszukiwane jest wśród niezdominowanych alternatyw decyzyjnych z uwzględnieniem priorytetów wynikających ze zdefiniowanych wcześniej klas odniesienia. Ostatnim etapem (3) jest analiza postoptymalizacyjna i ocena spójności tak znalezionego rozwiązania z regułami decyzyjnymi i innymi rodzajami dostępnej informacji o preferencjach. Co ważne, metoda zbiorów odniesienia pozwala decydentom na ilościowe określenie wagi

czynników nieobiektywnych. Więcej informacji dotyczących zastosowania tej metody w IRM DSS znajduje się w [podrozdziale 5.3].

Uzupełnieniem omówionej metody RefSet jest analiza scenariuszy, która w swym założeniu jest procesem oceny przyszłych zdarzeń i ich konsekwencji na drodze rozważenia możliwych alternatywnych przebiegów zdarzeń [Baloian i in., 2019]. Jest to metoda analizująca niepewność przyszłego przebiegu zagrożenia, przygotowująca decydenta do wyboru rozwiązania po uwzględnieniu szeregu możliwych wyników pośrednich. Często scenariusz złożony składa się z szeregu prostych scenariuszy analizowanych przez ekspertów w danej dziedzinie [Baloian i in., 2019]. Z punktu widzenia algorytmu, scenariusz może być zdefiniowany matematycznie jako zbiór *n* zdarzeń w określonej kolejności. Dla tego zbioru zdarzeń możemy znaleźć n! permutacji, co nam daje n! scenariuszy [Banuls i in., 2021]. Analiza scenariuszy oraz analiza hierarchiczna połączone np. z algorytmem Dijkstry pojawiają się jako główne modele w wytypowanych i przeanalizowanych pozycja bibliograficznych [Li i in., 2014].

Platforma informatyczna zbudowana w oparciu o przedstawione założenia powinna zapewniać [Dahal i in., 2020]:

- wsparcie przy reagowaniu na katastrofy,
- dopasowanie systemu do rzeczywistych warunków lokalnych implementacji systemu,
- ujednolicenie zarządzania informacjami,
- zrozumiały i czytelny dla użytkownika interfejs,
- redundantną konstrukcję systemu,
- wsparcie i przetwarzanie danych z wielu źródeł.

4.6 Podsumowanie: najlepsze praktyki w zakresie analityki decyzyjnej stosowane w specjalistycznych SWD do zarządzania ryzykiem przemysłowym

Inteligentne systemy wspomagania decyzji (DSS) są nowoczesnymi systemami informatycznymi, najczęściej interaktywnymi, których zadaniem jest wsparcie decydenta (osoby decyzyjnej) w procesie podejmowania decyzji. DSS wymagają implementacji wielu modeli analitycznych, w tym metod rozwiązywania problemów wielokryterialnych. DSS mogą funkcjonować jako systemy niezależne (dedykowane) lub być częścią systemu – podsystemem, dedykowanym do przetwarzania danych i zadań związanych z podejmowaniem decyzji.

Sytuacja awaryjna, którą możemy w uproszczeniu zdefiniować jako odstępstwo od stanu normalnego (warunków eksploatacyjnych), która w konsekwencji może doprowadzić do

straty lub szkody (dla ludzi lub majątku), stawia przed decydentem konieczność podjęcia decyzji, często złożonej i o krytycznym znaczeniu. Wiedza dostępna dla decydenta (zbiór danych wejściowych) jest zwykle niepełna, wymaga bieżącego uzupełniania z wielu źródeł oraz łączenia w ciągi przyczynowo skutkowe. Dodatkowo powinien on uwzględnić konsekwencje podejmowanych działań i ich implikację na kolejne kroki postępowania, ale również wziąć pod uwagę indywidualne preferencje i ścieżki alternatywne. Co ważne, podjęcie właściwej/dobrej decyzji musi uwzględniać również tło działań, czynniki środowiskowe czy społeczne oraz być spójne/zgodne z obowiązującymi regulacjami (zarówno wewnętrznymi jak i ogólnymi). Z punktu widzenia przedsiębiorstwa istotne są również aspekty gospodarcze, czyli optymalizacja działania w kierunku zapewnienia zysku (minimalizacji straty), maksymalizacji wydajności i wreszcie, co bardzo ważne, zabezpieczenia reputacji/wizerunku.

Aby spełnić te wszystkie oczekiwania DSS muszą wspomagać podejmowanie decyzji w czasie rzeczywistym prowadząc równoległą analizę złożonych scenariuszy, czyli symulację możliwych przebiegów zdarzeń w korelacji z obowiązującymi procedurami, ale również w sposób aktywny integrować się z otoczeniem poprzez interfejs komunikacji (np. GUI). Jednak co nie mniej istotne tego typu systemy muszą być elastyczne i dawać wsparcie również w sytuacji, gdy obsługujący je operator nie jest ekspertem w dziedzinie IT (być „*user friendly*") poprzez odpowiedni stopień interaktywności.

Wsparcie systemów DSS przez mechanizm uczenia maszynowego (ML) daje możliwość właściwego rozwiązywania problemów między innymi dzięki:

- nabyciu umiejętności weryfikowania i oznaczania poszczególnych zdarzeń jako mniej lub bardziej istotne,
- właściwemu i optymalnemu zarządzaniu przepływem informacji i rozdziałem dostępnych w danej sytuacji zasobów,
- analizie problemów o niejasnej strukturze i przebiegu poprzez indeksacje poszczególnych etapów, łączeniu ich we właściwe scenariusze i przypisywanie do konkretnych jednostek,
- równoległej obsłudze kilku decydentów na różnych szczeblach (hierarchiach) prowadzonej akcji zapewniając indywidualne podejście do każdego uczestnika procesu decyzyjnego.

Sam proces podejmowania decyzji jest procesem złożonym i może składać się z następujących kroków [Baloian i in., 2019]:

- identyfikacji problemu,
- identyfikacji celu,
- gromadzenia i przetwarzania danych,
- oceny wariantów (scenariuszy) rozwoju zdarzeń,

- wyboru opcji i analizy wpływu.

W celu realizacji powyżej zaproponowanych kroków właściwa wydaje się trójpoziomowa architektura systemu, składająca się z warstw [Ben Othman i in., 2017]:

- modelowania matematycznego analizowanego problemu, będąca niejako warstwą wiedzy niezbędnej do rozwiązania problemu,
- komunikacji z agentami rozproszonymi w terenie, w czasie rzeczywistym,
- odwzorowującej rzeczywiste, unikalne dla danej sytuacji, środowisko fizyczne oraz wyposażonej w mechanizm interaktywnej komunikacji z użytkownikiem (GUI).

Tak realizowany proces powinien zapewniać możliwość bezpośredniego wykorzystania przez decydenta danych wyjściowych, dostarczanych przez system w postaci jasnych i jednoznacznych komunikatów dających możliwość podjęcia decyzji ostatecznej lub przeprowadzenia kolejnej iteracji badanego (rozwiązywanego) problemu. Otrzymane w ten sposób wsparcie decyzyjne ułatwia podejmowanie decyzji pod presją czasu, w sposób znaczący skraca procesy decyzyjne i jest mniej wrażliwe na luki informacyjne, które potrafi zapełnić danymi historycznymi lub predykcyjnymi.

Poprawnie zaprojektowany i działający system DSS dodatkowo powinien służyć jako narzędzie w realizacji scenariuszy testowych oraz szkoleniowych, co może być wykorzystane zarówno do jego optymalizacji poprzez gromadzenie wniosków z realizowanych scenariuszy testowych jak oraz wnosić aspekt predykcyjny i mitygujący poprzez eliminację potencjalnych zagrożeń zidentyfikowanych w trakcie realizacji scenariuszy testowych. Ta właściwość systemu może w realnym środowisku znacząco skracać przebieg/rozwój zdarzenia i w ten sposób minimalizować prawdopodobieństwo materializacji zdarzeń o charakterze krytycznym. Możliwość szczegółowej analizy przebiegu konkretnej procedury (post factum) jest dodatkowym wsparciem dla decydenta i stanowi przyczynek do budowy mechanizmów samooceny i samodoskonalenia.

Powyższe założenia zgodne są z przytaczanymi w literaturze etapami zarządzania klęskami żywiołowymi w skład których wchodzą etapy [Baloian i in., 2019]:

- gotowości,
- łagodzenia skutków,
- reagowania,
- usuwania skutków.

Biorąc pod uwagę proponowane wykorzystanie mechanizmów ML, można uzupełnić je o etap piąty, będący niejako sprzężeniem zwrotnym:

- wdrażanie wniosków w celu minimalizacji powtórnej materializacji ryzyka.

Oczekiwania stawiane projektowanym i wdrażanym systemom DSS są indywidualne dla konkretnych środowisk pracy i warunków wdrożeniowych, można jednak wyodrębnić kilka cech wspólnych (uniwersalnych), które stanowią fundament działania każdego systemu klasy DSS [Zhu i in., 2021]:

- analizuje i dostarcza informacje o ryzykach adekwatnych dla konkretnych sytuacji i decyzji podejmowanych w ich następstwie,
- dostarczone informacje wspierają strategie prowadzonej akcji, dążąc do optymalnego rozwiązania problemu, maksymalizując skuteczność i minimalizując ryzyka,
- generuje ostrzeżenia o potencjalnie błędnych decyzjach, ślepych zaułkach, pomagając decydentowi wybrać ścieżkę/scenariusz minimalizującą ryzyko niepowodzenia,
- sygnalizuje braki/niedopasowania w obszarze prowadzonej analizy w korelacji z posiadanym zasobem danych bądź dostępem do danych/informacji/scenariuszy,
- w sposób aktywny (proaktywny) dostarcza informacje dla decydenta, na bieżąco uwzględniając podejmowane przez niego decyzje,
- analizuje w sposób ciągły zmieniające się ryzyka, dopasowując scenariusze zgodnie z wagą problemu, alokując zasoby adekwatnie do potrzeb i przebiegu zdarzeń,
- gromadzi informacje o podjętych działaniach, wybranych scenariuszach (ścieżkach) postępowania, które potrafi wykorzystać w kolejnych iteracjach lub nowych problemach.

Wskazane powyżej zadania mogą być realizowane przez system DSS dzięki informacjom gromadzonym i przetwarzanych w bazie/bazach danych, w których można wydzielić obszary dziedzinowe, związane ze specyfiką prowadzonej w danej chwili operacji. Ogólny podział może wyglądać następująco [Palestini, 2021]:

- baza danych podstawowych zawierająca podstawowe informacje o przedsiębiorstwie, w tym w szczególności, mapy, zdjęcia, dokumentację regulacyjną,
- baza modeli zawierająca procedury, modele matematyczne,
- baza reguł z relacjami logicznymi i scenariuszami możliwymi do realizacji.

Tak zaprojektowany system dodatkowo posiada podsystem zarządzania zbiorem przetwarzanych informacji, podsystem modelowania danych oraz podsystem mechanizmów ML/AI. Integralnym i niezbędnym uzupełnieniem całości są elementy GUI, czyli interfejs prezentacji danych i komunikacji z użytkownikiem (decydentem).

Integralną częścią algorytmu przetwarzania danych są procedury oceny ryzyka bazujące na identyfikacji zagrożeń i klasyfikacji ich na grupy. Dodatkowo procedury identyfikacji powinny być wspierane przez mechanizmy weryfikacji dostarczanych danych (danych źródłowych) przy wykorzystaniu algorytmów porównujących i oceniających wiarygodność

w oparciu o dane historyczne i rozkłady probabilistyczne (algorytm głosowania) [Palestini, 2021]. Po weryfikacji dane powinny zostać sprawdzone pod względem przydatności i dalej przypisane prawdopodobieństwa do tak zidentyfikowanych ryzyk/zagrożeń [Rest, Hirsch, 2022].

Prezentowany model będzie przydatny w rozwiązywaniu dużej klasy problemów budowania odporności dla zakładów przemysłowych. Podsystemy detekcji zagrożeń, pomiaru czynników zagrożenia i fuzji sygnałów z czujników są połączone z jednostkami zarządzania ryzykiem siecią przetwarzania informacji obejmującą chroniony obszar. Sieć ta uzupełniona jest o bazę wiedzy oraz silnik wspomagania decyzji podzielony na trzy podmoduły.

Pierwszy podmoduł odpowiada za zarządzanie bezpieczeństwem i optymalizację. Zawiera on algorytmy decyzyjne, planowanie działań łagodzących skutki zagrożenia oraz sterowanie aktuatorami w celu ich realizacji. Sygnały otrzymywane z czujników są przekazywane bezpośrednio do silnika decyzyjnego; system podejmuje autonomiczne decyzje dotyczące natychmiastowych działań, podczas gdy decydenci zatwierdzają złożone plany działań i modyfikują parametry systemów bezpieczeństwa, stosując oceny ograniczania zagrożeń jako informacje zwrotne. Drugi podmoduł zarządza ogólnym ryzykiem, na które narażony jest zakład. Rozwiązuje problemy kompromisowe dotyczące środków ochrony zakładu i ich kosztów oraz określa długoterminowe strategie ograniczania ryzyka. Trzeci podmoduł to baza wiedzy, w której przechowywane są historyczne informacje na temat wcześniejszych działań związanych z zarządzaniem zagrożeniami, czujników i innych parametrów instalacji ochronnych oraz naturalnych cech zagrożeń, takich jak historyczne dane o opadach. Baza wiedzy jest wzbogacona o metody eksploracji danych i ML. Moduł ten oblicza parametry algorytmów wspomagania decyzji i zarządzania ryzykiem za pomocą regresji nieliniowej i optymalizacji bayesowskiej.

Decydent będący zarówno ogniwem, kontrolerem jak i beneficjentem systemu DSS oczekuje dostarczenia mu informacji o możliwych działaniach/akcjach, korzyściach i/lub stratach będących wynikiem prowadzonych operacji, ale również wskazania zagrożeń i/lub luk pośrednich lub będących implikacją podejmowanych w trakcie procesu decyzji. Komunikacja systemu z decydentem realizowana np. dzięki wykorzystaniu języka modelowania procesów BPMN w proponowanym tu rozszerzeniu do notacji IRM-BPMN daje możliwość podejmowania decyzji racjonalnych, w oparciu o zdefiniowane reguły/wzorce postepowania oraz w oparciu pakiet zgromadzonych informacji.

5 Metody analizy wielokryterialnej

Analiza wielokryterialna należy do najważniejszych metod analityki decyzyjnej stosowanej w IRM DSS. Geneza analizy wielokryterialnej (MCDA - Multiple Criteria Decision Analysis) wywodzi się z potrzeby rozwiązywania złożonych problemów decyzyjnych, które nie mogą być opisane za pomocą pojedynczego kryterium [Kulkarni, 2022]. Pojawienie się MCDA jest związane z dynamicznym rozwojem teorii decyzji, ekonomii oraz nauk zarządzania w XX wieku. Rozwój systemów informatycznych i oprogramowania umożliwił implementację skomplikowanych algorytmów, co znacznie przyspieszyło rozwój narzędzi wspomagających proces decyzyjny. Kamieniem milowym w tym obszarze wiedzy był rozwój technologii Big Data, który spowodował, że analiza wielokryterialna ewoluowała, umożliwiając złożone analizy w czasie rzeczywistym. Nowoczesne narzędzia pozwalają na integrację z systemami baz danych, co czyni je bardziej efektywnymi w podejmowaniu decyzji. Coraz częściej MCDA jest stosowana w połączeniu z metodami sztucznej inteligencji, takimi jak algorytmy genetyczne, co pozwala na automatyzację procesu podejmowania decyzji, natomiast badania koncentrują się na rozwijaniu metod MCDA poprzez integrację z nowymi technologiami oraz wprowadzenie narzędzi umożliwiających lepsze reprezentowanie preferencji decydentów, co pozwala na uzyskanie bardziej trafnych decyzji. Obecnie analiza wielokryterialna odgrywa kluczową rolę w rozwiązywaniu problemów decyzyjnych o złożonej naturze, gdzie w procesie decyzyjny uwzględniane być muszą kryteria zarówno ilościowe, jak i jakościowe. Zagadnienie ogólnie nazywane jako analiza wielokryterialna obejmuje optymalizację wielokryterialną, której celem jest eliminacja decyzji nieracjonalnych (zdominowanych) oraz wiele technik wyboru rozwiązania kompromisowego, które różnią się sposobem podejścia do problemu i sposobem oceny alternatyw decyzyjnych.

5.1 Sformułowanie problemu optymalizacji wielokryterialnej

Celem tego podrozdziału jest przedstawienie i porównanie możliwości praktycznego zastosowania podstawowych metod wyboru rozwiązań kompromisowych ze zbioru punktów i ocen niezdominowanych (odpowiednio P(U,F) i FP(U), przy czym FP(U):=F(P(U,F)) w problemach optymalizacji wielokryterialnej rozwiązywanych przez autonomiczne moduły DSS generujące rekomendacje decyzyjne lub przez operatora DSS. Rozwiązywany może być ogólny problem typu:

$$[F:U\rightarrow E]\rightarrow \min(\theta), \tag{5.1}$$

gdzie dla uproszczenia prezentacji problemu jako stożek θ można przyjąć $\mathbf{R}^N_+$ (tj. „naturalny" porządek częściowy w $\mathbf{R}^N$), co jest równoważne z minimalizacją wszystkich kryteriów $F=(F_1,\ldots,F_N)$ [Skulimowski, 1996].

W rozwiązywanym w IRM DSS przypadku dyskretnym problemu (5.1) znany jest *m*-elementowy zbiór obiektów $U=\{u_1,\ldots,u_m\}$ oceniany na podstawie wartości *N* kryteriów $F_1,\ldots,F_N$. Oceny elementów zbioru *U* (zbioru decyzji) ze względu na kryteria $F:=(F_1,\ldots,F_N)$ są zapisane jako współczynniki macierzy decyzyjnej $D[m\ x\ N]$. Zakładamy przy tym, że wszystkie oceny są kompletne i znane. Poszukiwane jest wówczas rozwiązanie problemu optymalizacji wielokryterialnej dyskretnej postaci:

$$[(F_1,\ldots,F_N):U \rightarrow IR^N] \rightarrow \min(\theta) \qquad (5.2)$$

gdzie $\theta=R_{s1}\times\ldots\times R_{sN}$, a R_{si} oznacza albo R_+ albo R_-, co odpowiada albo minimalizacji, albo maksymalizacji kryterium F_i.

Problem (5.2) można rozwiązać stosując następujący algorytm, zaimplementowany w IRM DSS:

Algorytm 5.1 Algorytm z filtracją punktów zdominowanych

Input: X – zbiór decyzji
Output: P(X) - zbiór decyzji niezdominowanych

```
1: P-lista pusta;
2: for i= 1,…n
3: Y:=X(i); fl{=0
4:     for j=i+1,…n
5:             if Y≤X(j) usuń X(j) z przeglądanej listy
6:             else if X(j)≤Y
7:                     {usuń Y z przeglądanej listy X; Y:=X(j); fl:=1}
8:             end if
9:     end for
10:            dodaj Y do listy punktów niezdominowanych P(X)
11:            usuń z X wszystkie elementy X(k) takie, że Y≤X(k) //filtracja
12:            usuń Y z przeglądanej listy X
13:            if X={X(p)} dodaj X(p) do listy punktów niezdominowanych P end if
                              // gdy w X został tylko jeden element
14:            break
15: end for
16: end
```

Uwaga: gdy fl=0 na koniec pętli zewnętrznej algorytmu, wtedy Y=X(i), gdyż w trakcie wykonywania pętli wewnętrznej nie nastąpiła żadna zmiana porównywalnego punktu aktywnego.

Algorytmy filtracji skończonych zbiorów decyzji w celu wyodrębnienia punktów niezdominowanych stosowane są zarówno w technologii interfejsów opartych o metody wielokryterialne i punkty odniesienia, jak i w innych modułach IRM DSS. Analiza dyskretnych problemów decyzyjnych z wieloma punktami odniesienia, które występują przy wyborze strategii kompromisowej, wymaga:

a) znalezienia podzbiorów niezdominowanych decyzji rekomendowanych przez SWD (przypadek dyskretny)

oraz

b) eliminacji nadmiarowych elementów z klas punktów odniesienia wskazywanych przez decydenta lub ekspertów jako dodatkowa informacja o preferencjach.

Wybór decyzji kompromisowych z wyodrębnionych wcześniej zbiorów decyzji niezdominowanych odbywa się zgodnie z jednym z następujących scenariuszy:

A) Decydent wybiera niezdominowane decyzje w oparciu o kryteria *H* (wyższego poziomu) i przekazuje do DSS komendy maksymalizujące prawdopodobne następstwo wyboru takich decyzji.

B) Decydent może także wybierać niezdominowane decyzje w oparciu o kryteria niższego poziomu niż analizowane w sposób formalny przez DSS. Taki proces decyzyjny realizowany może być również w aplikacji do analizy sieci antycypacyjnych (front-end – edycja zbiorów, back-end – filtracja punktów niezdominowanych i przekazywanie niezdominowanego podzbioru do front-endu), por. [podrozdz. 5.5].

Algorytmy dyskretnej optymalizacji wielokryterialnej mogą być również wykorzystane przy rozwiązywaniu innych praktycznych problemów, takich jak

- Aproksymacja P(U,X) dla problemów zdyskretyzowanych,
- Wieloetapowa aproksymacja P(U,X) w problemach uczenia z wymuszeniem (*reinforcement learning*),
- Sortowanie, rankingowanie oraz ewaluacja decyzji ex-post.

Zakładamy, że w IRM DSS dla KWC zbiory P(U,F) i FP(U) wyznaczane będą jedynie dla przypadku dyskretnego), co dotyczy większości zastosowań w DSS, przy pomocy algorytmów z filtracją dla liczby potencjalnych rozwiązań do 1000. W przypadku ciągłego zbioru U, a także zbioru U z bardzo dużą liczbą alternatyw (powyżej 10000), P(U,F) i FP(U) wyznaczane mogą być metodami skalaryzacji [Skulimowski, 1996].

5.2 Metody wyboru decyzji kompromisowych

Niniejszy podrozdział zawiera opisy wybranych metod modelowania preferencji w interfejsach systemów wspomagania decyzji IRM DSS, zwłaszcza opartych o punkty odniesienia i modele kauzalne. W celu rekomendacji lub wyboru kompromisowych decyzji metody te korzystają z reguły z implementacji algorytmów wielokryterialnej optymalizacji dyskretnej. Przedstawimy te metody wielokryterialne, które mogą być użyteczne dla celów modelowania preferencji w projektowanej aplikacji IRM DSS.

Zagadnienie ogólnie nazywane jako analiza wielokryterialna obejmuje wiele technik wyboru decyzji kompromisowych, które różnią się sposobem podejścia do problemu, rodzajem dodatkowej informacji o preferencjach i sposobem jej wykorzystania. Do najbardziej rozpowszechnionych metod należą:

1. Metoda AHP (Analytic Hierarchy Process), [Kulkarni, 2022] polega na budowaniu hierarchii kryteriów i ocenianiu ich względem siebie. Jest szczególnie przydatna w sytuacjach, gdzie decydenci muszą uporządkować złożone problemy, redukując je do serii prostszych decyzji. Kluczową ideą metody jest dekompozycja problemu decyzyjnego na mniejsze, łatwiejsze do analizy elementy, które można porównać ze sobą w sposób systematyczny, uwzględniając znane kryteria odniesienia. Analiza problemu wielokryterialnego zgodnie z metodą AHP rozpoczyna się od stworzenie hierarchii problemu, co oznacza sprecyzowanie celu głównego, wyznaczenie kryteriów oceny oraz wskazanie dostępnych alternatyw dla kolejnych etapów oceny. Oceny pary alternatyw dokonuje się na każdym poziomie hierarchii, celem jest określenie, które z kryteriów lub alternatyw są ważniejsze i o ile bardziej. Kolejnym krokiem jest wyznaczanie wag kryteriów i stworzenie macierzy porównań, z której wylicza się wagi (priorytety) dla każdego z kryteriów. Wagi te reprezentują względną ważność każdego kryterium w procesie podejmowania decyzji. Tak przygotowane dane podlegają procesowi ocena alternatyw i priorytetyzacji, a następnie agregowane wyniki są sumowane, aby uzyskać ostateczną rangę alternatyw. Ostatnim etapem procesu jest ocena spójności, która ma potwierdzić, że decyzje dokonywane przez decydenta są logiczne.

AHP znajduje zastosowanie w wielu dziedzinach, takich jak planowanie strategiczne, zarządzanie projektami czy procesy inwestycyjne. Metoda jest bardzo intuicyjna, łatwa do zrozumienia i wdrożenia, jednak decyzje są oparte na subiektywnych ocenach, co może prowadzić do błędów, a w przypadku złożonych problemów obliczenia mogą być czasochłonne, co niewątpliwie stanowi wadę tej metody.

2. Metoda PROMETHEE (Preference Ranking Organization Method for Enrichment Evaluation) [Kulkarni, 2022] to metoda umożliwiająca porównywanie i ocenę alternatyw na podstawie preferencji decydentów. W tej metodzie każda alternatywa jest oceniana względem innych na podstawie zdefiniowanych kryteriów. Dzięki temu możliwe jest uszeregowanie

wszystkich opcji od najlepszej do najgorszej. Analiza problemu wielokryterialnego przy użyciu tej metody rozpoczyna się od zdefiniowania problemu decyzyjnego, uwzględniając alternatywy decyzyjne oraz kryteria, według których będą oceniane. Co istotne kryteria mogą być zarówno ilościowe, jak i jakościowe. Kluczowym elementem PROMETHEE jest określenie funkcji preferencji dla każdego kryterium. Funkcje te określają, jak duża różnica między dwiema alternatywami wpływa na preferencję decydenta względem jednej z nich. Tak przygotowane dane są materiałem wejściowym do obliczanie preferencji par alternatyw w oparciu o funkcje preferencji dla każdego z kryteriów. Wynik ten jest następnie agregowany, co pozwala na ustalenie, która z alternatyw jest preferowana. Uporządkowanie alternatyw generuje częściowy ich ranking, w którym nie wszystkie alternatywy są jednoznacznie uporządkowane. Metoda PROMETHEE wprowadza tzw. indeksy przepływu preferencji, które oceniają "poziom przewagi" danej alternatywy nad innymi.

Metoda PROMETHEE jest szeroko wykorzystywana w planowaniu inwestycji, logistyce i ocenie ryzyka w projektach i przedsięwzięciach. Jest to konsekwencją jej elastyczności, która wpływa na możliwość dostosowanie funkcji preferencji do różnych typów kryteriów i problemów decyzyjnych. Fakt, że metoda jest stosunkowo prosta do zrozumienia ułatwia jej implementację w różnych dziedzinach. Na niekorzyść stosowanie tej metody przemawia fakt, że opiera się ona na subiektywnej ocenie decydenta i jego preferencjach.

3. Metoda TOPSIS (*Technique for Order Preference by Similarity to Ideal Solution*) [Kulkarni, 2022] to jedna z najpopularniejszych metod analizy wielokryterialnej, służy do wybierania najlepszej alternatywy spośród wielu opcji na podstawie ich podobieństwa do rozwiązania idealnego. Celem metody jest wybór takiej alternatywy, która jest najbliższa rozwiązaniu idealnemu i jednocześnie najdalsza od rozwiązania anty-idealnego. Aby zrozumieć idę tej metody, należy wyjaśnić, czym są rozwiązania idealne i anty-idealne. Rozwiązanie idealne, jest to hipotetyczna sytuacja, która maksymalizuje wszystkie kryteria korzystne i minimalizuje wszystkie kryteria niekorzystne, stanowi ona punkt odniesienia, do którego porównywane są inne alternatywy. Natomiast rozwiązanie anty-idealne jest to odwrotność rozwiązania idealnego, tzn. maksymalizuje niekorzystne kryteria i minimalizuje korzystne. Analiza problemu wielokryterialnego przy użyciu tej metody rozpoczyna się od stworzenia macierzy decyzyjnej, która zawiera dane na temat alternatyw i wartości każdego kryterium dla każdej alternatywy. Następnie, w oparciu o preferencje decydenta kryteriom przypisuje się odpowiednie wagi. W oparciu o tak przygotowane dane następuje obliczenie idealnego i anty-idealnego rozwiązania. Idealne rozwiązanie składa się z najlepszych możliwych wartości dla każdego kryterium, natomiast anty-idealne rozwiązanie składa się z najgorszych możliwych wartości dla każdego kryterium. W oparciu o odległości euklidesowe wyznaczane są odległości alternatyw od rozwiązań idealnych i anty-idealnych, w efekcie czego otrzymujemy wskaźnik podobieństwa do rozwiązania idealnego, który wyraża się jako stosunek odległości od anty-idealnego rozwiązania do sumy odległości od

rozwiązania idealnego i anty-idealnego. Alternatywy klasyfikowane są na podstawie wartości wskaźnika podobieństwa, przy czym alternatywa z najwyższym wskaźnikiem jest uznawana za najlepszą.

TOPSIS znajduje szerokie zastosowanie w różnych dziedzinach, takich jak zarządzanie zasobami ludzkimi, logistyka i zarządzanie łańcuchem dostaw, inżynieria i projektowanie. Jest metodą prostą i intuicyjną, daje możliwość uwzględniania różnych kryteriów, jednak skale kryteriów wymagają normalizacji, co może wprowadzać pewne zniekształcenia w ocenie końcowej.

4. Metoda ELECTRE (*Elimination Et Choice Translating Reality*) [Kulkarni, 2022] to metoda eliminacyjna, której głównym celem jest stopniowe odrzucanie słabszych alternatyw. Proces obejmuje tworzenie relacji preferencji pomiędzy alternatywami, co prowadzi do wyeliminowania opcji, które są znacznie gorsze od pozostałych. ELECTRE jest szczególnie użyteczna w podejmowaniu decyzji w warunkach niepewności. Metoda to posiada kilka wariantów: ELECTRE I (najprostsza wersja, stosowana głównie do problemów wyboru jednej najlepszej alternatywy), ELECTRE II, III, IV (rozszerzone wersje, które umożliwiają bardziej złożone analizy, takie jak częściowe porządkowanie alternatyw lub wielokrotne eliminacje), ELECTRE TRI (stosowana do klasyfikacji, gdzie alternatywy są przypisywane do różnych klas), niemniej jednak podstawowe założenia są wspólne dla każdej z nich. W metodzie ELECTRE, alternatywy są porównywane parami na podstawie każdego z kryteriów. Każda alternatywa jest oceniana pod kątem jej przewagi lub dominacji nad innymi, dzięki temu zamiast tworzyć pełny ranking alternatyw, metoda ta eliminuje te, które są w sposób istotny gorsze. Dla każdej pary alternatyw stosuje się dwa rodzaje progów: próg zgodności (pokazuje w jakim stopniu jedna alternatywa jest lepsza lub równa innej w odniesieniu do każdego z kryteriów) i próg niezgodności (pokazuje w jakim stopniu jedna alternatywa jest wyraźnie gorsza od drugiej). Po obliczeniu wskaźników zgodności i niezgodności dla każdej pary alternatyw, tworzy się tzw. relację przewagi, która pokazuje, która alternatywa jest preferowana i w jakim stopniu. W końcowym etapie, metoda eliminuje alternatywy, które są słabsze od innych, pozostawiając te, które spełniają kryteria preferencyjne. Wynik jest prezentowany w formie uporządkowanego zestawu alternatyw, które mogą być wybrane i prezentowane w zależności od specyfiki problemu.

Metoda ELECTRE znalazła głównie szerokie zastosowanie w dziedzinach inżynieryjnych, dzięki możliwości szybkiej eliminacji „złych" alternatyw oraz możliwości obsługi konfliktowych kryteriów i możliwości uwzględniania współczynnika niepewności. Zalety te przekształcają się w wadę w przypadku z niektórych problemów, ponieważ metoda staje się dość złożona i wymaga zaawansowanych obliczeń, a decydent musi określić progi zgodności i niezgodności, co może wprowadzać subiektywność do procesu decyzyjnego.

5.3 Podstawy metody zbiorów odniesienia

Jak już wspomnieliśmy w poprzednim rozdziale, w metodzie zbiorów odniesienia (RefSet) zdefiniowane zostają klasy punktów odniesienia A_1, …, A_k, przy czym najczęściej k=4 [Skulimowski, 1996, 1997, 2023]

Metoda RefSet może służyć do poszukiwania decyzji kompromisowej zarówno dla problemów ciągłych, jak i dyskretnych. Dla skończonych zbiorów decyzji U metoda zbiorów odniesienia może też być w prosty sposób zastosowana do wygenerowania rankingów sekwencyjnych, tj. w drodze M kolejnych procesów wyboru rozwiązania kompromisowego $u_{opt,k}$ ze zbioru $U_k := U_{k-1} \setminus \{u_{opt,\ k-1}\}$. Wymagać to może jednak przeprowadzania k kolejnych procedur dialogowych, co najczęściej przekracza zasoby czasowe decydenta i nie jest możliwe w przypadku decyzji podejmowanych przez autonomiczne SWD. W związku z tym bardziej obiecujące są metody równoległego poszukiwania kilku lub wszystkich elementów zbioru $\{u_1, \ldots u_m\}$. W najprostszy sposób można tego dokonać znając wartości funkcji v i traktując ją jako kryterium skoringowe. Wymaga to jednak znajomości globalnego oszacowania v.

Inny sposób polega na równoczesnej dekompozycji zbioru alternatyw i zbioru punktów odniesienia (i być może także zbioru kryteriów) w taki sposób, by każda alternatywa decyzyjna była porównywalna z każdym punktem odniesienia w zredukowanym problemie. Skutkuje to sformułowaniem m nowych połączonych problemów wielokryterialnych, każdy z mniejszą ilością punktów odniesienia, które mogą być rozwiązywane równolegle. Jeśli w jednym z nowych problemów istnieje potrzeba wyboru więcej niż jednego elementu zbioru szeregowanych elementów, wówczas dla każdego takiego problemu zastosować można niezależnie podejście sekwencyjne. Jednak w dalszym ciągu otrzymujemy m nieporównywalnych rozwiązań kompromisowych.

W przypadku, gdy w jednym ze zdekomponowanych problemów co najmniej jeden punkt odniesienia jest porównywalny z alternatywą decyzyjną przyporządkowaną do innego problemu powstałego w wyniku dekompozycji, wskazana wyżej dekompozycja może prowadzić do utraty informacji dotyczącej preferencji. Sposobem rozwiązania nie posiadającym tej wady może być przyjęcie jednolitej funkcji aproksymującej użyteczność decydenta pomiędzy punktami odniesienia poszczególnych klas. Jeśli porządkowane punkty dyskretnego zbioru U leżą pomiędzy – w sensie częściowego porządku – jednym poziomem aspiracji i jednym poziomem status-quo, wówczas do uprządkowania tego podzbioru punktów można zastosować np. rozszerzenia metody TOPSIS [Kulkarni, 2022] (należy co najmniej zamienić punkt antyidealny na punkt nadir i uzgodnić wagi ze współczynnikami skali lub w ogóle zrezygnować z ich stosowania).

Problem komplikuje się, gdy punktów odniesienia jest więcej, a zastosowanie metody TOPSIS do każdej pary złożonej z punktu aspiracji i punktu status-quo daje odmienne wyniki.

Jest to regułą w złożonych problemach rankingowania, z którymi mamy do czynienia w przypadku analizy wieloetapowych strategii decyzyjnych.

W takiej sytuacji proponowaliśmy następującą procedurę:

Algorytm 5.2.

Wejście:

a) Definiujemy dane wejściowe zbiór punktów odniesienia A podzielony na podklasy A_1, …,A_k (konieczne jest do tego odpowiednie GUI).

b) Przy pomocy algorytmu podanego w [Skulimowski, 2023] sprawdzamy, czy spełnione są warunki dobrego zdefiniowania (niesprzeczności) klas, w razie potrzeby dokonujemy korekty klas.

c) Wizualizowany jest zbiór potencjalnych rozwiązań F(U), które będą szeregowane.

Wyjście: ranking U i F(U)

1. Dla każdej pary punktów $a_{i,j} < a_{i-1,k}$, gdzie $a_{i,j}$ jest punktem docelowym, a $a_{i-1,k}$, - punktem *status-quo* [Skulimowski, 1997] konstruujemy funkcję skoringową $f(a_{i,j},a_{i-1,k},u)$, która porządkuje punkty u ze zbioru $F(U)$ leżące pomiędzy $a_{i,j}$ a $a_{i-1,k}$,.
2. Dla każdego punktu $u \in U$ znajdujemy kolejno wszystkie punkty aspiracji i *status-quo*, takie że $a_{i,j} \leq F(u) \leq a_{i-1,k}$,.
3. Jeśli nierówność z kroku 2 jest spełniona tylko jednostronnie (przez element $a_{i,j}$ lub $a_{i-1,k}$,), wówczas funkcję skoringową budujemy jedynie w oparciu o informacje o jednej klasie punktów odniesienia, np. jako sumę odległości od takich punktów ważoną objętościami wielościanów o punktach narożnych w u oraz w elementach tej klasy.
4. Gdy *u* nie jest porównywalne z żadnym elementem analizowanych klas odniesienia (i-tej i *(i-1)*-szej), lecz jest porównywalne z elementami innej klasy o wskaźniku *p* najbliższym do *i* lub *(i-1)*, wówczas do utworzenia funkcji skoringowej można zastosować te klasy (lub jedną z nich) w podobny sposób, jak klasy *i*–ta i *(i-1)-sza*, a następnie otrzymaną wartość *f* należy przeskalować do zakresu [i:p] lub [p:i-1].
5. Gdy *u* nie jest porównywalne z elementami żadnej z klas, wówczas stosujemy procedurę opisaną w [podrozdziale 5.2].
6. Tworzymy nową funkcję skoringową równą sumie ważonej wszystkich funkcji powiązanych z parami ($a_{i,j}$, $a_{i-1,k}$,) i porządkujemy według niej punkty zbioru *U*.

Lub alternatywnie

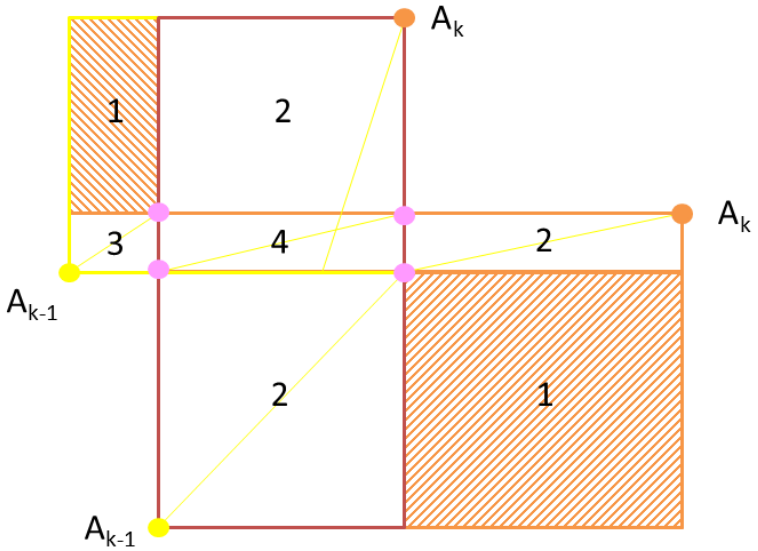
6’. W każdym podzbiorze typu

$$A_{jkpq} := A_{jk} \cap A_{pq},$$

gdzie

$$A_{jk} := \{x: a_{i,j} \leq x \leq a_{i-1,k}\},$$

funkcję skoringowe f_{jkpq} budujemy odrębnie, skalując je jednak nie do przedziału wartości [0, 1], lecz do wartości $[r_m, r_{m+1}]$, $m=0,\ldots,m_{jkpq}$ i zakładając wartości zerowe f_{jkpq} poza zbiorami $A_{jk} \cap A_{pq}$. Następnie tak dobieramy wartości r_m, by $\Sigma_{0\leq m\leq m_{jkpq}} r_m = 1$ oraz by wartości $f_{j1,k1,p1,q1}$ i $f_{j2,k2,p2,q2}$ były zgodne na częściach wspólnych obszarów $A_{j1,k1,p1,q1}$ i $A_{j2,k2,p2,q2}$. Funkcje postaci f_{jkpq} dodajemy, a poza obszarem porównywalnym z punktami klas A_i i A_{i-1} wartości określamy podobnie, jak w algorytmie podanym w podrozdz. [5.1]. ■



Rys. 35. Przykład dekompozycji obszaru porównywalnego z punktami odniesienia na podobszary, w których dokonywana jest interpolacja wartości funkcji skoringowych [wg Skulimowski, 2023]

Podobnie postępujemy dla każdej pary sąsiadujących ze sobą klas odniesienia. Ze względu na fakt, że w prawidłowo sformułowanym problemie brak rankingowanych punktów lepszych od punktów aspiracji (klasa A_1), z reguły nie jest konieczna budowa funkcji skoringowej dla pary klas A_1, A_2.

5.4 Metody znajdowania najkrótszej ścieżki wielokryterialnej

Jako uzupełnienie opisu podstawowych metod analizy wielokryterialnej zaprezentowana zostanie metodyka znajdowania najkrótszej ścieżki przy założeniu konieczności rozwiązania problemu jako typowego problemu wielokryterialnego. Metoda ta zastosowana została w [rozdz. 11] w celu wyboru najlepszych ścieżek ewakuacji sprzętu z zagrożonego terenu.

Problem znajdowania najkrótszej ścieżki wielokryterialnej jest rozwinięciem podstawowego problemu najkrótszej ścieżki w grafie. W klasycznym problemie celem jest znalezienie ścieżki pomiędzy węzłami grafu, która minimalizuje sumę wag przypisanych do krawędzi. W wersji wielokryterialnej optymalizacja nie dotyczy jednej miary (np. odległości), lecz wielu kryteriów, które mogą być ze sobą sprzeczne lub niezależne. Podobnie jak

w klasycznym grafie węzły reprezentują punkty decyzyjne, lokalizacje lub zdarzenia, natomiast krawędzie łączą wierzchołki mają przypisane wagi, gdzie każda składowa reprezentuje inne kryterium. Wielokryterialna funkcja celu dąży do optymalizacji wielu kryteriów, np. minimalizacja czasu i kosztu jednocześnie. Główne wyzwania, z jakimi mamy tu do czynienia to sprzeczne kryteria, złożoność obliczeniowa i interpretacja wyników. Zbiór rozwiązań Pareto-optymalnych może być duży, co wymaga dodatkowych kroków lub narzędzi decyzyjnych.

Notacja i założenia będące podstawą rozwiązania problemu:

($G:=(V,E)$ – multigraf skierowany spójny, $f:E\rightarrow R_+^M$ - etykiety krawędzi grafu G,

V_1 – punkt (węzeł) startowy, V_2 – punkt (węzeł) docelowy, $W(e):=(W_1(e), W_2(e))$ - węzły krawędzi *e*, początkowy i końcowy,

Λ- zbiór wszystkich ścieżek z V_1 do V_2, tj. $p\in\Lambda\Leftrightarrow p=(e_{p1},\ldots,e_{p,n(p)})$, gdzie $e_{pi}\in E$, $W(e_{p1})=(V_1, V_{p1},)$, $W(e_{p,n(p)})=(V_{p,n(p)-1},V_2)$ oraz $\forall i$, $1\leq i\leq n(p)-1$: $W(e_i)=(V_{p,i}, V_{p,i+1})$

Ewaluacja ścieżek w grafie G polega na określeniu wartości funkcji F dla każdej ścieżki w oparciu o etykiety f, tj. określenia wartości

$$F: \Lambda\rightarrow R_+^N$$

np. gdy M=N jako

$$F(p):=\Sigma_{1\leq i\leq n(p)}f(e_i), \qquad (5.3)$$

gdzie n(p) jest liczbą krawędzi w p [lub inna agregacja f], przy czym $\forall$c-cyklu w G: $F(c)\geq 0$

Problem 5.3. Należy znaleźć wszystkie niezdominowane ścieżki z V_1 do V_2 względem kryterium $F=(F_1,\ldots,F_N)$ [np. najkrótszą i jednocześnie najszybszą trasę z V_1 do V_2].

Przykład 5.1. Rozwiązania Problemu 5.3 algorytmem WOD (np. naiwnym z filtracją):

Algorytm WOD (Weighted Ordered Distance) jest kolejną metodą stosowaną w analizie danych i wielokryterialnym podejmowaniu decyzji. Jego głównym celem jest określenie odległości między analizowanymi obiektami lub rozwiązaniami na podstawie ważonych różnic między kryteriami, uwzględniając ich uporządkowanie. Wersja naiwna algorytmu WOD charakteryzuje się prostotą implementacji i minimalnym przetwarzaniem dodatkowym.

Na grafie $G:=(V,E)$ wyżej należy znaleźć wszystkie ścieżki wielokryterialne pomiędzy węzłami $V_1 = (1)$ i $V_2 = (4)$. Etykiety krawędzi grafu $f:E\rightarrow R_+^2$ podane są w nawiasach przy każdej krawędzi. Λ- zbiór wszystkich ścieżek z V_1 do V_2, można zapisać jako

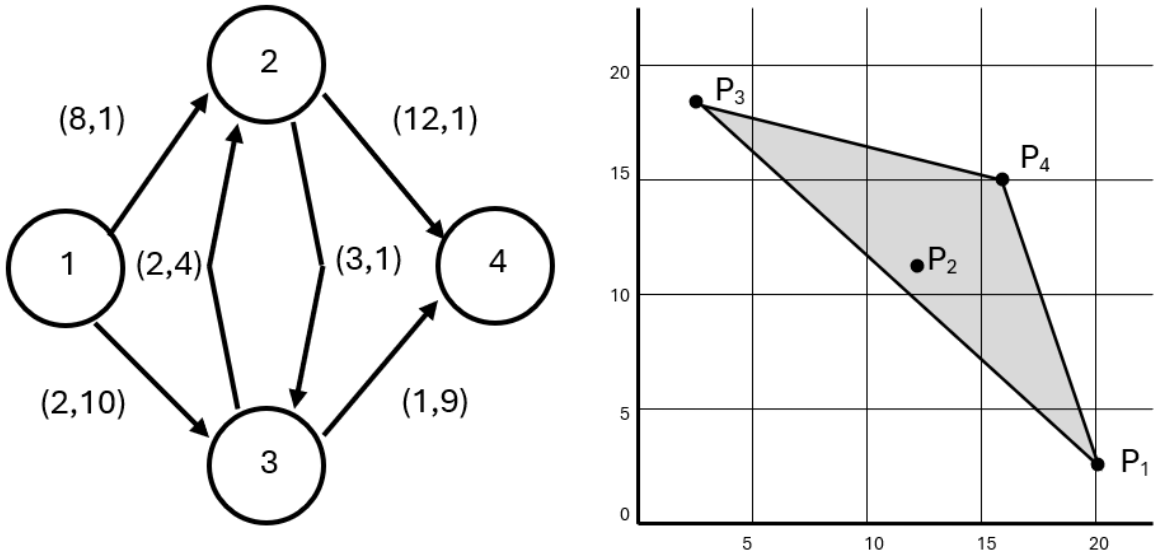
p1:=(1)-(2)-(4), **F(p1)=(20,2)**

p2:=(1)-(3)-(4) **F(p2)=(3,19)**

p3:=(1)-(2)-(3)-(4) **F(p3)=(12,11)**

p4:=(1)-(3)-(2)-(4) F(p4)=(16,15)

Ścieżki niezdominowane w powyższej analizie oznaczono pogrubioną czcionką.



Rys. 36. Ilustracja Przykładu 5.1.

Sformułowanie problemu K-kryterialnej najkrótszej ścieżki dla algorytmu Martinsa.

Podobnie jak w Problemie 5.3, sieć, w której poszukujemy ścieżek jest zdefiniowana jako skierowany graf spójny G=(V,A), gdzie V={V_1,..,V_n} jest zbiorem wierzchołków o liczności |V| = *n* i A = {(i_1,j_1), ..,(i_m, j_m)} jest zbiorem krawędzi o liczności |A| = *m*. Skierowana krawędź łącząca wierzchołki *i* oraz *j* jest oznaczona jako (*i*,*j*), a wektor (c^1(*i*,*j*), .., c^K(*i*,*j*)) reprezentuje wartości kosztów przypisanych do krawędzi (*i, j*). $C_{m,K}$ jest macierzą kosztów dla wszystkich krawędzi grafu G. W zbiorze V wskazujemy wierzchołek początkowy *s* i wierzchołek końcowy *t*. Ścieżka *r* z *s* do *t* w G jest sekwencją wierzchołków i krawędzi z *s* do *t*, gdzie koniec krawędzi danego wierzchołka zbiega się z początkiem krawędzi wierzchołka kolejnego na ścieżce. $R_{s,t}$ oznacza zbiór wszystkich ścieżek z *s* do *t* i $R_{s,}$. zbiór wszystkich ścieżek z *s* do wszystkich pozostałych wierzchołków V\{s} w G. Niech $z^p(r)$ oznacza wartość ścieżki *r* z uwzględnieniem kryterium *p*, dla *p* = 1, ..,K, gdzie K=σ+μ, ilość kryteriów. Stąd wektor *z*(*r*) = (z^1(r), .., z^K(r)) jest wektorem oceny dla ścieżki *r* ϵ $R_{s,t}$. Kryteria mają postać opisaną wzorem (5.4):

$$z^p(r) = \Sigma_{(i,j)\epsilon r}\, c^p(i, j) \tag{5.4}$$

dla funkcji liniowej oraz

$$z^p(r) = \min\{(i, j)\in r : c^p(i, j)\} \tag{5.5}$$

dla funkcji max-min (czyli kryterium typu „wąskie gardło” - *bottleneck*). Kiedy minimalizujemy wszystkie kryteria, ścieżka r_e jest niezdominowana wtedy i tylko wtedy, gdy nie istnieje ścieżka *r* w $R_{s,t}$, taka, że $z^p(r) \le z^p(r_e)$, dla wszystkich *p* = 1, ...,K, z przynajmniej

jedną ostrą nierównością. Wtedy $z(r_e)$ jest punktem niezdominowanym w przestrzeni kryteriów.

Ścieżka r_{we} jest słabo niezdominowana wtedy i tylko wtedy gdy nie istnieje ścieżka r w $R_{s,t}$, taka że $z(r) < z(r_{we})$. $z(r_{we})$ jest punktem lub wektorem słabo niezdominowanym.

Rozwiązanie problemu najkrótszych ścieżek wielokryterialnych przy pomocy algorytmu Martinsa.

Problem wyżej można rozwiązać przy pomocy algorytmu ustawiania etykiet Martinsa (*Martins label setting algorithm*) [Martins, 1984]. Algorytm Martinsa to jedno z podejść do rozwiązania problemu najkrótszej ścieżki wielokryterialnej. Rozwija klasyczne metody, takie jak algorytm Dijkstry, w celu obsługi wielu kryteriów przy zachowaniu efektywności obliczeniowej. Główną ideą algorytmu jest iteracyjne wyszukiwanie ścieżek, które są Pareto-optymalne, tzn. niezdominowane przez inne ścieżki w kontekście wielu kryteriów. Podstawowa wersja tego algorytmu nie uwzględnia jednak dynamiki (zmiennej struktury) sieci, która może wystąpić np. w DES. W takich sytuacjach można użyć algorytmu zmodyfikowanego [Gandibleux i in. 2004]. Pozwala on na optymalizację dwóch typów kryteriów: liniowe – S i *bottleneck* – M. Zapis problemu ma postać (σ-S| μ-M), gdzie σ i μ oznaczają odpowiednio liczbę problemów pierwszego i drugiego typu. Algorytm pozwala na optymalizację (σ-S|1-M), gdzie σ > 0 i wylicza kompletny zbiór niezdominowanych ścieżek.

Algorytm Martinsa (wg [Gandibleux i in., 2006]):

Wymagania: G = (V,A) i C
Oczekiwania: odnalezienie wszystkich efektywnych ścieżek z *s* do pozostałych wierzchołków.

- l_i – etykieta wierzchołka *i*
- lt_i – lista tymczasowych etykiet wierzchołka *i*
- lp_i – lista stałych etykiet wierzchołka *i*
- $z^p_{q,h}$ – jest wynikiem p-tej stałej etykiety wierzchołka *q* w pozycji *h*
- Δ – jest relacją dominacji (jeśli zΔz' to z jest zdominowany przez z')

Inicjalizacja

- $lt_i, lp_i \leftarrow Ø$ dla każdego $i \in V$
- $lt_s \leftarrow \{[0, .., 0, \perp, \perp]\}$

Iteracja, dopóki dla każdego $i \epsilon V$ $lt_i \neq Ø$ wykonuj:

1. Znajdź najmniejszą leksykograficznie etykietę w lt_i.
2. Przenieś wybraną etykietę z listy tymczasowych do listy stałych.

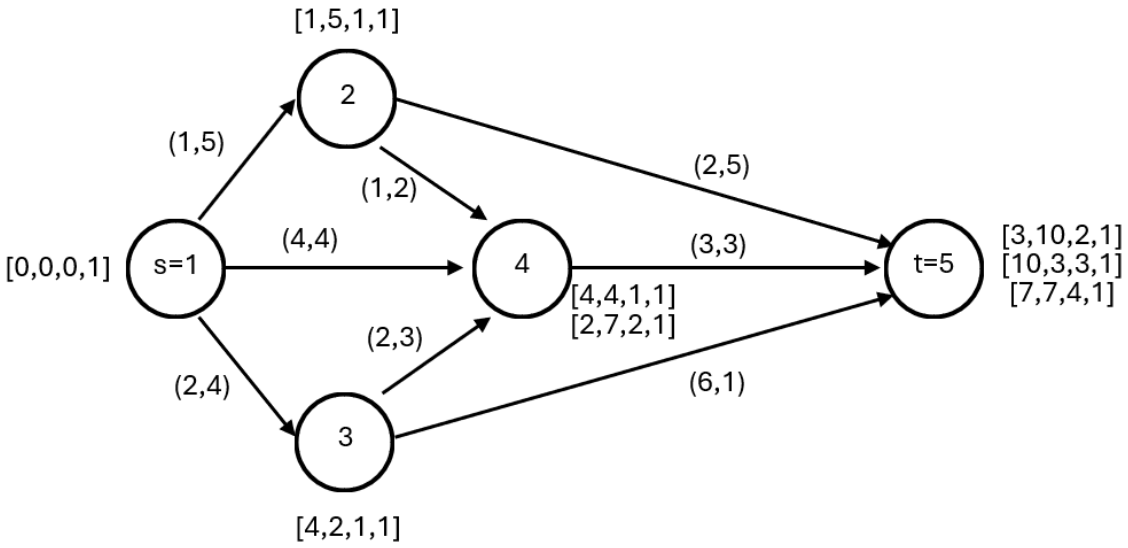
3. Zapisz pozycję etykiety l_q z listy lp_q.
4. Oznacz etykietą wszystkich następców *q*.
5. Dla każdego $j \in V|(q,j) \in A$ wykonaj.
6. Wylicz l_j (aktualną etykietę wierzchołka *j)*.
7. Upewnij się, że nie istnieją wartości etykiet dla wierzchołka *j* dominujące wartość aktualnej etykiety.
8. Jeśli nie istnieją, zapisz etykietę l_j jako tymczasową i usuń wszystkie tymczasowe etykiety wierzchołka j, które są zdominowane przez etykietę l_j.

Zaprezentowany powyżej algorytm Martinsa można modyfikować, w celu podniesienia jego efektywności. Założenia:

- Nie usuwamy żadnej etykiety, gdy dwie etykiety są nieporównywalne lub jeśli dwie etykiety są równe.
- Etykieta 2 jest usuwana, jeśli jest zdominowana przez etykietę 1.
- Etykieta 2 jest słabo niezdominowana przez etykietę 1 z przynajmniej jedną ostrą nierównością. Jeżeli istnieje przynajmniej jeden $p' \in \{1, ..,\sigma\}$, taki że $z^{p}_{q,1} < z^{p}_{q,2}$, wtedy etykieta 2 jest usuwana, ponieważ te dwie etykiety nie mogą stać się jednoznaczne w następnej iteracji (zakładając nieujemne koszty). W przeciwnym wypadku $z^{p}_{q,1} = z^{p}_{q,2}$, i wtedy żadna etykieta nie jest usuwana, ponieważ te dwie etykiety mogą stać się równoważne dla wierzchołka *j*.

Dalsze modyfikacje tego algorytmu można znaleźć np. w [Demeyer i in., 2013], [Janssens i in., 2011] i [Cass i in., 2021].

Przykład 5.2. Analiza możliwości zastosowania algorytmu Martinsa [Rys. 37].



Rys. 37. Ilustracja Przykładu 5.2.

W celu znalezienia niezdominowanych rozwiązań, kolejno wykonujemy:

1. Przypisujemy tymczasową etykietę [0,0,0,1] do wierzchołka s=1. Wybieramy tą etykietę i ustawiamy jako stałą. Przypisujemy tymczasowe etykiety do następców wierzchołka 1 czyli: [1,5,1,1] dla wierzchołka 2, [4,2,1,1] dla wierzchołka 3 i [4,4,1,1] dla wierzchołka 4.
2. Z etykiet tymczasowych wybieramy najmniejszą leksykograficznie [1,5,1,1] i ustawiamy ją jako stałą. Przypisujemy tymczasowe etykiety dla następców 2, czyli: [2,7,2,1] dla 4 i [3,10,2,1] dla 5.
3. Z etykiet tymczasowych wybieramy najmniejszą leksykograficznie [4,2,1,1] i ustawiamy jako stałą. Przypisujemy tymczasowe etykiety dla następców 3, czyli: [10,3,3,1] dla 5. Nie ustawiamy etykiety [6,5,3,1] ponieważ jest zdominowana przez [4,4,1,1].
4. Z etykiet tymczasowych wybieramy najmniejszą leksykograficznie [4,4,1,1] i ustawiamy jako stałą. Przypisujemy tymczasowe etykiety dla następców 4, czyli: [7,7,4,1] dla 5.
5. Z etykiet tymczasowych wybieramy najmniejszą leksykograficznie [3,10,2,1] i ustawiamy jako stałą. Wierzchołek 5 nie ma następców, więc nie przypisujemy etykiet tymczasowych.
6. Wybieramy etykietę [10,3,3,1] i ustawiamy jako stałą.
7. Wybieramy etykietę [7,7,4,1] i ustawiamy jako stałą.

Z powyższego algorytmu wyliczyliśmy 3 niezdominowane ścieżki:

1 -> 2 -> 5.

1 -> 3 -> 5.

1 -> 4 -> 5.

Dla problemów poszukiwania najlepszej ścieżki, z wieloma kryteriamilstosowany jest również algorytm A*. Opis wielokryterialnej wersji tego algorytmu zaprezentowany został przez [Likhachev i in., 2008]. Algorytm A* jest jedną z najpopularniejszych metod znajdowania optymalnych ścieżek robotów, szczególnie gdy mamy do czynienia z kryteriami wielowymiarowymi. Jest to algorytm oparty na heurystyce, dzięki czemu jest bardziej wydajny od innych metod, takich jak algorytm Dijkstry. Znajduje zastosowanie w logistyce, planowaniu tras, zarządzaniu ryzykiem i innych dziedzinach, jednak wymaga odpowiedniego zaprojektowania funkcji celu i heurystyki, aby osiągnąć maksymalną efektywność.

5.5 Sieci antycypacyjne

Sieci antycypacyjne stanowią model łączący analitykę predykcyjną z analityką preskrypcyjną, oparte o prognozowanie decyzji podejmowanych w powiązanych z problemem rozwiązywanym obecnie oraz ze sobą wzajemnie przyszłych problemach decyzyjnych. W trakcie analizy problemu opartej o model sieci antycypacyjnej, obecne i prognozowane otoczenie problemu modelowane jest jako sieć wzajemnie zależnych obiektów, z których część zdolna jest do autonomicznego, inteligentnego i racjonalnego podejmowania decyzji. W procesie analizy wyodrębnić można zbiór optymalizatorów, czyli obiektów podejmujących decyzje w sposób racjonalny z punktu widzenia uczestników procesu (decydentów). Racjonalność decydenta modelowanego w sieci antycypacyjnej zdefiniowana jest jako zdolność do optymalizacji pewnego zbioru kryteriów i wybór decyzji wg zdefiniowanej struktury preferencji. Zbiór takich optymalizatorów tworzy antycypacyjny system decyzyjny, przez który rozumieć będziemy układ analityki predykcyjnej ze sprzężeniem zwrotnym opartym o prognozy otoczenia i antycypacje decyzji przyszłych decydentów, nazywanym *sprzężeniem antycypacyjnym* [Skulimowski, 2014].

Dzięki wskazanym powyżej właściwościom, sieci antycypacyjne mogą być stosowane do modelowania i prognozowania konsekwencji w wielokryterialnych systemach decyzyjnych. Wykorzystanie multigrafu skierowanego jako modelu kauzalnego w teorii sieci antycypacyjnych (AN) można rozpatrywać zarówno jako metodykę wspierającą i opisującą proces decyzyjny oraz jako narzędzie podstawowe w razie zaistnienia sytuacji kryzysowej. Ten drugi przypadek zasługuje na odrębną analizę i powinien być traktowany jako równie istotny w sytuacjach materializacji ryzyk skutkujących np. całkowitą utratą komunikacji, brakiem decydenta (bądź decydentów) czy też koniecznością automatycznej (inteligentnej – wymuszonej przez algorytm AI, w oparciu o scenariusz przebiegu zdarzeń) eskalacji problemu.

Analiza przebiegu procesu decyzyjnego w sytuacji zdarzenia o charakterze katastrofy krytycznej, w wyniku której wyłączony z łańcucha decyzyjnego zostaje decydent (np. w wyniku utraty łączności, jedno- lub dwukierunkowej) zakłada, że oczekiwania stawiane jednostkom wykonawczym nie mogą ulec zmianie, zwiększa się jednak niepewność co do akcji podejmowanych przez kolejnych decydentów (będących niżej w strukturze decyzyjnej). Dotyczy to również oczekiwań co do kierunku prowadzenia akcji ratowniczej oraz jej efektów końcowych. Niezmienna pozostaje konieczność minimalizacji strat oraz łagodzenia wpływu zaistniałego (zmaterializowanego) zdarzenia na pozostałą infrastrukturę, nieobjętą pierwotnym zdarzeniem.

Przy tak postawionych wymaganiach przebieg procesu decyzyjnego powinien uwzględniać braki w zakresie monitoringu działań wyeliminowanych z łańcucha decyzyjnego węzłów, a ciężar decyzji przenosić zarówno na obecne w łańcuchu ogniwa, jak i dawać możliwość

wykorzystania potencjału swobody podejmowania decyzji przez jednostki niższego szczebla, takie jak np. zespoły ratownicze czy wspomagające.

W przypadku braku wpływu decydenta, pozostałe dostępne węzły decyzyjne kontynuują swoje działania, zakładając w sposób autonomiczny i zgodny z kierunkiem przepływu decyzji, że decydent niedostępny w łańcuchu wpływu nadal podejmuje akcje zgodnie z ustalonym algorytmem decyzyjnym. Tym samym decyzje te są antycypowane przez decydentów pozostających w łańcuchu. Kluczowe w tej sytuacji staje się przekierowanie informacji z sensorów (o ile to możliwe) oraz przewidywanie wyników optymalizacji problemów, co do których decyzje powinny zostać podjęte w węźle niedostępnym (wyłączonym z łańcucha decyzyjnego).

Zgodnie z tymi założeniami prognozowanie potencjalnych decyzji decydenta, który nie uczestniczy w procesie, opierać się powinno na znajomości zbioru decyzji dopuszczalnych, kryteriów i algorytmu podejmowania decyzji konkretnego węzła i/lub jednostki wykonawczej. Wybór decyzji przez jednostki pozostające w łańcuchu dokonywany jest następnie w oparciu o założenie, że niedostępny węzeł podejmuje decyzje, które prowadzą do rozwiązania optymalnego i tożsamego lub maksymalnie zbliżonego do tożsamego w stosunku do rozwiązania przez siec kompletną.

W analogiczny sposób modelowane są ewentualne braki dostępności kolejnych węzłów decyzyjnych, natomiast „istotność decyzyjna” jest zależna od umiejscowienia konkretnego węzła decyzyjnego w grafie, a tym samym zależna od wpływu jednostki decyzyjnej na podległe jej węzły oraz ilości decyzji dostępnych w tym punkcie decyzyjnym.

Szczegółowe omówienie modelu, wraz z symulacjami zaprezentowane zostało w podrozdziale 10.4.1.

6 Zintegrowane systemy bezpieczeństwa stosowane w przemyśle

Holistyczne systemy zarządzania bezpieczeństwem, mimo swojego potencjału, nie zyskały jeszcze szerokiej popularności głównie ze względu na ich złożoność i koszt ich wdrożenia, będący konsekwencją konieczności zaangażowania w proces wdrożeniowy specjalistów z wielu branż. Systemy ego typu wymagają integrowania różnych technologii, danych oraz procesów w sposób zapewniający spójność działań w zakresie bezpieczeństwa technicznego, operacyjnego i fizycznego. Są one często bardziej skomplikowane niż tradycyjne systemy zarządzania, ponieważ uwzględniają wszystkie aspekty działalności, a nie jedynie pojedyncze zagrożenia, a systemy zarządzania klasy ERP mogą zasilać je dodatkowymi danymi.

W praktyce holistyczne systemy bezpieczeństwa są obecnie wykorzystywane głównie w sektorach wysokiego ryzyka, takich jak przemysł energetyczny, naftowy, gazowy, chemiczny oraz górnictwo. W tych branżach stosowanie holistycznych systemów pozwala na monitorowanie i zarządzanie ryzykiem w czasie rzeczywistym oraz na optymalizację procesów produkcyjnych, co wpływa na zmniejszenie liczby incydentów i strat. Warto też zaznaczyć, że możliwości predykcyjne oraz w zakresie wsparcia decyzyjnego są jeszcze mało zaawansowane w istniejących systemach.

W sektorze energetycznym działają już zintegrowane systemy zarządzania bezpieczeństwem, choć ich pełne wdrożenie nadal nie jest tak powszechne jak w innych branżach. Polskie przedsiębiorstwa energetyczne, takie jak PGE, Tauron czy Energa, stosują różne systemy wspomagające zarządzanie bezpieczeństwem technicznym i operacyjnym, jednak nie można ich nazwać systemami holistycznymi, a raczej dedykowanymi do konkretnych zastosowań.

Ze względu na tajemnice przedsiębiorstwa nie są dostępne szczegółowe informacje dotyczące wdrażanych i użytkowanych systemów, natomiast przegląd dostępnych w Internecie informacji pozwala to podsumować w następujący sposób:

1. PGE (Polska Grupa Energetyczna) – wdraża rozwiązania w ramach szeroko pojętego zarządzania ryzykiem operacyjnym i technicznym. Firma stosuje systemy nadzoru nad sieciami energetycznymi, które monitorują stabilność przesyłu energii oraz bezpieczeństwo infrastruktury. Zintegrowane systemy wykorzystywane przez PGE mają na celu nie tylko minimalizację ryzyka awarii, ale także optymalizację działania infrastruktury energetycznej.
2. Tauron – wdrożył zaawansowane systemy monitoringu sieci i zarządzania bezpieczeństwem energetycznym, w szczególności w ramach tzw. Smart Grid (inteligentnych sieci energetycznych). Takie rozwiązania umożliwiają stałe

monitorowanie i optymalizację dostaw energii, a także szybkie reagowanie na potencjalne awarie czy zakłócenia.

3. Energa – wdraża systemy zintegrowane w zakresie zarządzania bezpieczeństwem sieci i infrastrukturą przesyłową. Systemy te pomagają w zarządzaniu ryzykiem, monitorując stan sieci w czasie rzeczywistym i umożliwiając szybkie reagowanie na zagrożenia, takie jak przeciążenia sieci czy incydenty związane z warunkami atmosferycznymi.

W polskim sektorze energetycznym systemy te są wykorzystywane głównie w ramach zarządzania sieciami przesyłowymi, monitorowania stabilności infrastruktury oraz optymalizacji dystrybucji energii. Chociaż te rozwiązania są wprowadzane, ich pełna integracja w całym sektorze wymaga dalszych inwestycji i rozwoju, szczególnie w kontekście modernizacji infrastruktury oraz wdrożenia bardziej zaawansowanych technologii, takich jak sztuczna inteligencja czy Internet Rzeczy (IoT).

Przemysł naftowy stosuje zintegrowane systemy zarządzania bezpieczeństwem, które obejmują monitorowanie operacji wiertniczych, zarządzanie integralnością rurociągów oraz nadzór nad procesami technologicznymi w czasie rzeczywistym. Podobnie sytuacja wygląda w sektorze chemicznym, gdzie systemy pozwalają na zarządzanie bezpieczeństwem procesów produkcyjnych, które są narażone na ryzyko awarii technicznych lub wycieków niebezpiecznych substancji.

Pierwsze systemy tego typu pojawiają się również w administracji publicznej. System DART to polskie rozwiązanie do zarządzania bezpieczeństwem publicznym, które ma na celu poprawę koordynacji służb ratunkowych, takich jak straż miejska, straż pożarna i policja. System DART umożliwia monitorowanie wydarzeń w czasie rzeczywistym, zarządzanie zasobami oraz pozycjonowanie pojazdów służb ratunkowych za pomocą GPS. System jest modułowy, elastyczny i skalowalny, co pozwala na dostosowanie go do potrzeb różnej wielkości miast czy aglomeracji. Integruje się on z istniejącą infrastrukturą, taką jak centrale telefoniczne i systemy alarmowe, a także obsługuje funkcje, takie jak komunikacja VoIP (*Voice over IP*), wideokonferencje i systemy płatności mobilnych. Te technologie pomagają obniżyć koszty operacyjne i skrócić czas reakcji służb ratunkowych. System ten jest szeroko stosowany w polskich miastach, w tym w Olsztynie, Poznaniu, Gdańsku i Lublinie. DART jest szczególnie przydatny podczas dużych wydarzeń publicznych i w miastach, gdzie wymagana jest skuteczna koordynacja wielu służb bezpieczeństwa.

7 Analiza propagacji ryzyka

7.1 Metody i modele analizy ryzyka

Najlepiej dobrana dla analizowanych zagadnień wydaje się być definicja ryzyka zaproponowana w [Kaplan, Garrick, 1981], gdzie ryzyko jest zdefiniowane poprzez odpowiedzi na pytania: co może się wydarzyć, jak prawdopodobne jest, że to się stanie i wreszcie, jeżeli tak się stanie, jakie będą tego konsekwencje. Ten elementarny ciąg przyczynowo skutkowy wykorzystywany będzie w dalszych rozważaniach.

Analiza i zarządzanie ryzykiem są kluczowe dla zapewnienia bezpieczeństwa oraz ciągłości procesów technologicznych, a sam proces analizy i ocena ryzyka idą ze sobą w parze. Istnieją dwa rodzaje technik analizy ryzyka: analiza jakościowa i analiza ilościowa. Ilościową metodę oceny ryzyka wykorzystuje algorytm przewidywania zagrożeń oparty na sieciach Bayesa [Zhang i in., 2024]. Wykorzystanie do analizy przebiegu zdarzeń sieci Bayesa, oprócz wymagania danych dotyczących prawdopodobieństwa i strat dla każdego węzła, narzuca również potrzebę przygotowania tabel prawdopodobieństwa warunkowego dla odpowiednich węzłów. Może to stanowić wyzwanie w przypadku złożonych systemów przemysłowych z dużą liczbą węzłów [Feng i in., 2024]. Zastosowanie tradycyjnych metod analizy procesu wypadkowego i analizy ryzyka wykorzystujących głównie liniowe zależności przyczynowe do zobrazowania statycznych zależności między zmiennymi logicznymi, takie jak analiza drzewa błędów, analiza drzewa zdarzeń, analiza muchy, analiza scenariuszy, analiza procesu wypadkowego w oparciu o diagram logiczny obarczone są ryzykiem wystąpienia uproszczeń, czy skrótów, które mogą w sposób znaczący wpłynąć na wynik końcowy prowadzonego procesu [Feng i in., 2024].

Tradycyjne metody oceny ryzyka, oparte na rachunku prawdopodobieństwa (probabilistyczna ocena ryzyka, Probabilistic Risk Assessment PRA), korelują deterministyczne zależności pomiędzy podstawowymi zdarzeniami, tworząc w wyniku tego działania różne scenariusze zagrożeń. PRA dobrze łączą procesy zachodzące w złożonych organizacjach przemysłowych, a tym samym nadają się dla potrzeb skomplikowanych i rozbudowanych systemów inżynieryjnych dzięki umiejętności radzenia sobie z niepewnością, podejmowaniu decyzji kompromisowych i przede wszystkim bazowaniu na podejściu opartym na ryzyku [Rolland i in., 2010].

Kroki jakie należy uwzględnić przy analizie opartej na PRA to:

1. Gromadzenie informacji, ich segregowanie i przygotowanie do dalszej analizy, np. poprzez właściwe oznaczenie.
2. Rozpoznanie i klasyfikacja zdarzeń inicjujących, czyli pierwotnych przyczyn zaistnienia zjawiska.

3. Tworzenie scenariuszy możliwych przebiegów zidentyfikowanego i sklasyfikowanego wstępnie zdarzenia.
4. Opracowanie modelu logicznego przebiegu zdarzenia.

Rozwinięciem tej metodyki jest dynamiczna probabilistyczna ocena ryzyka (DPRA) [Vience, 1992]. To podejście umożliwia uwzględnienie w tworzonych scenariuszach również zmiennych dynamicznych, będących następstwem zmian niezamierzonych, zależnych od czasu i pozostających w interakcji z innymi czynnikami czy elementami analizowanego systemu. Dzięki uwzględnieniu nieliniowości i cech stochastycznych zapewniają możliwość dokładniejszego przewidywania kierunków rozwoju analizowanej sytuacji.

W celu monitorowania ryzyka w systemach złożonych, w oparciu o metody probabilistyczne stworzona została również metoda Hybrid Causal logic (HCL). Zbudowana jest ona w oparciu o trójwarstwowy model hybrydowy, składający się z diagramu/drzewa zdarzeń, diagramu/drzewa błędów oraz sieci bayesowskich. Jest to struktura zbudowana o model PRA pozwalający na włączenie do analizy czynników miękkich wprowadzanych przez czynnik ludzki i organizacyjny [Rodriguez i in., 2011].

Uzupełnieniem powyżej opisanych metod, jest analiza pozwalającą zidentyfikować opóźnienia pomiędzy materializacją poszczególnych ryzyk, zależności pomiędzy ryzykami, i co ważniejsze pomiędzy poszczególnymi elementami infrastruktury przemysłowej. *Design Structure Matrix* (DSM), to stworzenie zależności typu urządzenie – urządzenie pozwalające przewidzieć wpływ na produkt końcowy, jakość, opóźnienie i dalej koszty, jakie mogą być wynikiem materializacji zaistniałego ryzyka [Moradi, Growth, 2020].

W tym miejscu należy zwrócić uwagę na fakt, że systemy zarządzania ryzykiem w przedsiębiorstwie (enterprise risk management, ERM) zazwyczaj skupiają się na ryzyku finansowym, natomiast zarządzanie ryzykiem w przemyśle (IRM) jest szerszym tematem, skupiającym się na kontroli systemów cyber-fizycznych za pomocą nadzoru wideo i innych czujników. Systemy ERM jak i IRM różnią się również ramami czasowymi wdrożenia ERM jest wykorzystywany do długoterminowego planowania finansowego bez wcześniej ustalonej konkretnej czynności wdrożenia. Natomiast znaczenie IRM jest szczególnie widoczne w sytuacjach kryzysowych, kiedy to system IRM zarządza krótkoterminową reakcją na sytuację kryzysową i średnioterminowymi działaniami naprawczymi. Obecnie dzięki dostępności nowych metod sztucznej inteligencji (AI) możliwe jest zintegrowanie zarządzania ryzykiem z wielopoziomowym inteligentnym systemem wspomagania decyzji (intelligent DSS, lub IDSS), obejmującym planowanie strategiczne i operacyjne, jak również doraźne reagowanie w sytuacjach kryzysowych. W szczególności, inteligentne modele decyzyjne będą wspierane przez techniki uczenia maszynowego (ML), umożliwiając autonomiczne budowanie modeli zagrożeń na podstawie pobranych strumieni danych i wcześniejszych zapisów działań w sytuacjach kryzysowych.

Analiza problemów bezpieczeństwa przemysłowego opiera się na określeniu ryzyk, które przypisuje się zagrożeniom zewnętrznym, procedurom przetwarzania informacji, które mogą zafałszować obserwacje zagrożeń, błędom operacyjnym człowieka oraz systematycznym błędnym decyzjom, które można podjąć podczas zarządzania ryzykiem. Transfer danych o zagrożeniach można modelować jako sieć, w której utrata informacji oraz przypadkowe błędy operacyjne i decyzyjne są źródłem dodatkowych zagrożeń. Uzupełnieniem tej sieci jest model zarządzania ryzykiem i optymalizacji, obejmujący algorytmy decyzyjne, działania i aktorów je realizujących. Obydwa elementy modelu powiązane są informacją zwrotną otrzymaną przez czujniki, porównaną z wartościami dostarczonymi przez model i przedstawionymi modułowi ML nadzorowanemu przez decydentów.

Analiza ryzyka przemysłowego określa ilościowo potencjalne skutki zagrożeń, dostrzega zależności między nimi i zaleca optymalne środki zapobiegania ryzyku i jego łagodzenia. Dostępność informacji przechowywanych i przetwarzanych w innych systemach informatycznych przedsiębiorstwa oraz efektywność komunikacji są kluczowymi czynnikami wdrażania IRM DSS [Skulimowski, Łydek 2022a; Skulimowski, Łydek, 2022b].

7.1.1 Modele dyfuzyjne

Zaproponowana w ostatnim czasie metoda osłabienia propagacji ryzyka w sieci poprzez kontrolowanie wag węzłów i obciążenie początkowe wydaje się być rozwiązaniem, dzięki któremu można lepiej kontrolować (a nawet hamować) propagację ryzyka. Tego typu model propagacji ryzyka oparty jest teorii perkolacji [Guo i in., 2021], czyli matematycznej metodzie opisu układów nieuporządkowanych. Modelowanie propagacji jest zbliżone do procesu dyfuzji płynu w teorii perkolacji, z uwzględnieniem następujących aspektów [Guo i in., 2021]:

- propagacja ryzyka zależy od przepływu ładunku (surowca),
- propagacja ryzyka może przebiegać jedynie do sąsiednich węzłów i krawędzi, i nie zachodzi proces propagacji krzyżowej,
- kierunek propagacji może przebiegać w dowolnym kierunku.

Poza modelami bazującymi na sieciach Bayesa główne metody badawcze propagacji ryzyka obejmują modele epidemiczne (typu SIR– - Susceptible Infected Recovered) [Shan i in., 2024], [Shan i in., 2023], które jednak nie są istotne w przypadku zagrożeń *stricte* przemysłowych. Modele te dają jednak to nową perspektywę w badaniu propagacji ryzyka wskazując możliwość, że wypadki związane z bezpieczeństwem nie są zdarzeniami losowymi, ale raczej wynikiem silnej korelacji pomiędzy różnymi czynnikami ryzyka, w obszarze bezpieczeństwa [Han i in., 2024]. Modele te zakładają, że przeniesienie ryzyka

wzdłuż krawędzi z węzła do węzła powoduje zmianę wagi krawędzi przenoszącej, a tym samym wzrasta poziom ryzyka w sposób, który opisuje równanie (7.1) [Shan i in., 2024]:

$$f(j) = \frac{e_{ij*}\,\alpha_{i*}\,x_j^{\varepsilon}}{\sum_{q=1}^{n} e_{yj}};\ \alpha_j = f(j) \tag{7.1}$$

gdzie α oznacza prawdopodobieństwo propagacji ryzyka, e_{ij} jest wagą krawędzi węzłów i oraz j, a $\mathcal{E}$ jest parametrem regulowanym.

Należy mieć na uwadze, że modele te opisują jedynie reakcję łańcuchową stanu węzła wywołaną ryzykiem, nie biorąc pod uwagę, że konsekwencje ryzyka (tj. obciążenie ryzykiem) mogą być kumulowane w coraz większym stopniu, aż przekroczą zdolność graniczną węzłów do zapobiegania ryzyku [Zhang, Yang, 2018]. Gdy obciążenie węzła przekroczy jego zdolność do kumulacji ryzyka, nastąpi przeciążenia ryzykiem. W konsekwencji ryzyko przeniesie się na kolejne węzły i/lub sieci. W celu badania zdolności kumulacji ryzyka na poziomie pojedynczego węzła wprowadzono parametr tolerancji β na podatność. Gdy wartość β jest wystarczająco duża dla większości węzłów sieci, zdolność do podejmowania ryzyka jest wystarczająco duża, aby pomieścić dodatkowy ładunek ryzyka ze strony bardziej obciążonych węzłów [Zhang, Yang, 2018].

Nowe modele badania mechanizmu rozprzestrzeniania się awarii i ryzyka w złożonych sieciach systemów przemysłowych oparte o teorię sieci złożonych stanowią podstawę do ustalenia heterogenicznego modelu dynamicznego propagacji ryzyka, wskazanego już wcześniej - SIRS. Wydaje się on być lepiej dostosowany do złożonych sieci systemów przemysłowych i pozwala na metodyczne konstruowanie procesów rozprzestrzeniania się wypadków w sieciach oraz zapewnia platformę do systematycznego badania różnych mechanizmów mających wpływ na propagację ryzyka. Teoria kaskadowego modelowania rozprzestrzeniania się ryzyk definiuje całkowite obciążenie $L_i(t)$ ryzykiem jako sumę konsekwencji ryzyk (7.2), które wystąpiły w przedsiębiorstwie i o n węzłach w czasie t [Feng i in., 2024]:

$$L_i(t) = \sum_{j=1}^{n} w_j * n_j^i(t) \tag{7.2}$$

gdzie w_j jest konsekwencją ryzyka R_j, $n_j^i(t)$ wskazuje czy ryzyko R_j *wystąpiło do czasu t*.

Modele propagacji ryzyka bazujące na automatach komórkowych traktowane są jako narzędzie wykorzystywane w analizie katastrof naturalnych o charakterze środowiskowym. Badają one ewolucję podejmowanych decyzji i wskazują, że charakterystyka przestrzenna analizowanego środowiska ma kluczowy wpływ na przebieg zdarzenia. Również dynamika zmian oraz wzajemne relacje, w tym sprzężenia zwrotne pomiędzy poszczególnymi węzłami sieci, uwzględniane są w analizie propagacji ryzyka opartej na modelach automatów komórkowych. Modele te nie są jednak właściwe do prowadzenia analizy w przypadku, gdy pewną niepewnością obciążone są dane dotyczące badanego otoczenia, natomiast mogą one

uwzględniać wiele czynników wpływających na przebieg zdarzenia i skomplikowane interakcje pomiędzy nimi [Shan i in., 2024].

7.1.2 Zastosowanie modeli łańcuchów dostaw w analizie ryzyka

Zdecydowana większość prowadzonych w dostępnej literaturze analiz propagacji ryzyka dotyczy przypadków związanych bezpośrednio z łańcuchem dostaw (*supply chains*). Wydaje się jednak, że możliwe jest przeniesienie tego typu analiz do innych środowisk, w tym produkcyjnych z uwzględnieniem niezbędnych niewielkich zmian w samym procesie analizy [Ghadge i in., 2022]. Wynika to z faktu, że modele stosowane w analizie propagacji ryzyka w łańcuchach dostaw opierają się na prawdopodobieństwie materializacji pięciu podstawowych zagrożeń, w różnej ich konfiguracji [Yan i in., 2024]:

- prawdopodobieństwo wystąpienia ryzyka,
- ryzyko straty,
- nieprzewidywalność ryzyka,
- brak kontroli ryzyka,
- możliwość przeniesienia ryzyka.

Łańcuchowy model propagacji ryzyka opisuje sposób, w jaki jedno zdarzenie wywołuje kolejne, prowadząc do kaskadowych skutków w systemie. Wykorzystanie tego modelu propagacji ryzyka w kopalni odkrywkowej uwidacznia, jak jedno zdarzenie początkowe (np. intensywne opady deszczu) może wywołać serię powiązanych ryzyk, prowadząc do poważnych konsekwencji finansowych, środowiskowych i operacyjnych. Wykorzystanie takich modeli w praktyce umożliwia identyfikację kluczowych punktów interwencji i skuteczne ograniczanie ryzyka na różnych poziomach propagacji. Zdarzenie początkowe (intensywne opady deszczu) powoduje osunięcie ziemi (zwiększone uwilgotnienie gruntu prowadzi do zmniejszenia spójności skał i gleby), to prowadzi do zatrzymanie operacji wydobywczych (zablokowanie dróg transportowych, uszkodzenie infrastruktury), czego skutkiem są straty finansowe i środowiskowe (straty związane z przestojami i naprawami, zanieczyszczenie wód gruntowych).

7.1.3 Metoda Bow-Tie

Ukazanie zależności pomiędzy zidentyfikowanymi ryzykami, a skutkami ich materializacji (analiza ryzyka) możliwe jest na kilka sposobów. Metodą wykorzystywaną w KWC jest metoda Bow-Tie (inaczej metoda Muchy, [Feng i in., 2024]). Zgodnie z [P.5] jest ona kombinacją metod *Fault Tree Analysis* i *Event Tree Analysis* i umożliwia między innymi:

- zaprezentowanie uporządkowanej i czytelnej struktury analizy,

- wykorzystanie wiedzy eksperckiej osób prowadzących analizę,
- identyfikację zagrożeń oraz wskazanie właściwych działań prewencyjnych,
- ocenę adekwatności istniejących działań prewencyjnych.

Zależności zgodne z tą metodologią wykazane w tabeli [Tab. 5] w sposób uproszczony prezentuje poniższy diagram [

Rys. ***38***]. Wybór metody jest konsekwencją wzajemnych powiązań i zależności występujących pomiędzy poszczególnymi Spółkami Grupy Tauron oraz łańcucha decyzyjnego zgodnie z [Rys. 6]. Metoda została rekomendowana przez Biuro Bezpieczeństwa TPE.

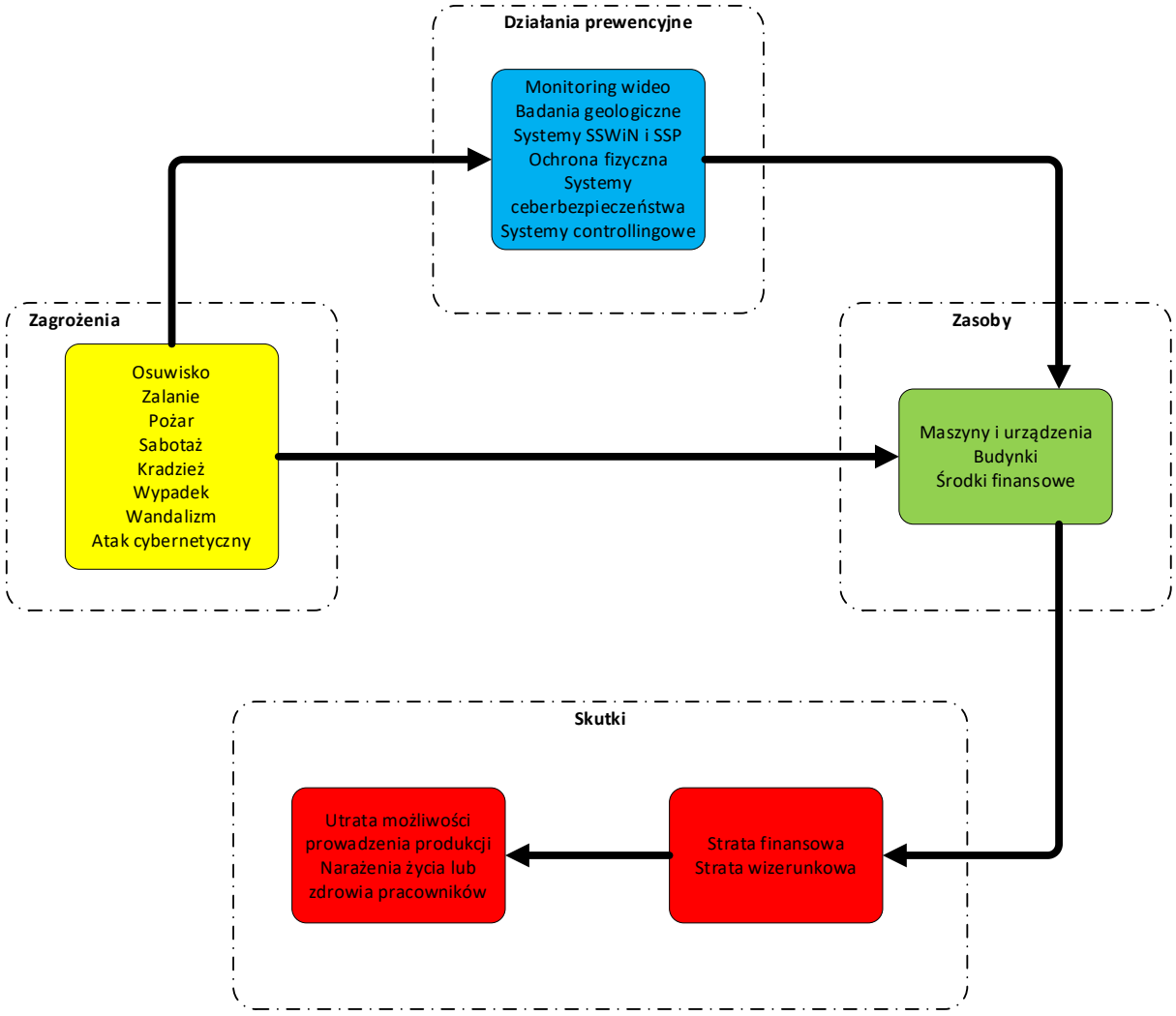
Metoda analizy ryzyka Bow-Tie, dzięki połączeniu wspomnianych wcześniej dwóch metod (FTA i ETA) daje możliwość oceny ryzyka na podstawie posiadanego doświadczenia i dobrych praktyk, uwzględniając tym samym subiektywne oceny i miary poszczególnych jej czynników [Yang, Haugen, 2015]. Proces analizy dostosowany zgodnie z tą metodyką do warunków KWC korzysta z pojęcia „najgorszego scenariusza", przez który należy rozumieć najbardziej niepożądane zdarzenie związane z brakiem możliwości realizacji podstawowego, zidentyfikowanego wcześniej, procesu. Procedura przebiega w następujących krokach:

Procedura 7.1

1. Identyfikacja kluczowych procesów i zasobów niezbędnych do ich realizacji.
2. Wybór „najgorszego scenariusza" (o charakterystyce deterministycznej): „najgorszy scenariusz" oznacza największe koszty potencjalnych strat, poza kosztami wyliczonymi metodami finansowo-ekonomicznymi, uwzględniając również koszty społeczne i środowiskowe. Wybór opiera się o wiedzę ekspercką, czyli reprezentatywną dla konkretnego środowiska przemysłowego.
3. Identyfikacja i analiza, kolejno przyczyn i zdarzeń pośrednich prowadzących do materializacji „najgorszego scenariusza".
4. Identyfikacja skutków i konsekwencji materializacji „najgorszego scenariusza".
5. Wskazanie istniejących, a następnie nowych, możliwych do wdrożenia, działań prewencyjnych. Krok ten wymagana znacznej znajomości środowiska pracy, w którym prowadzona jest analiza, opiera się więc na doświadczeniu i wiedzy osób bezpośrednio zaangażowanych w proces, przy wsparciu ekspertów i/lub firm doradczych, specjalizujących się w rozwiązywaniach dedykowanych.
6. Wskazanie podatności, czyli czynników narażających działania prewencyjne na niepowodzenie.
7. Wskazanie działań prewencyjnych eliminujących zidentyfikowane podatności. Również w tym kroku kluczową rolę odgrywają eksperci dziedzinowi, których wiedza pozwala przygotować zestaw możliwych akcji.

8. Przedstawienie do akceptacji decydentom zestawu możliwych akcji wraz ze wskaźnikami finansowo-ekonomicznymi. W przypadku braku akceptacji uzupełnienie analizy – przejście do Kroku 3
9. Opracowanie wyników i wniosków. ■

Kluczowym elementem procesu analizy jest identyfikacja „najgorszego scenariusza" – z opisanej powyżej definicji wynika, że powinien to być ciąg zdarzeń wysokopoziomowych z punktu widzenia procesów biznesowych, którego materializacja może mieć największy wpływ na przerwanie ciągłości tych procesów. Zefiniowanie „najgorszego scenariusza" jest zatem próbą wychwycenia i opisania potencjalnego zdarzenia o możliwie szerokim zasięgu i wpływie na całe spektrum procesów biznesowych i produkcyjnych przedsiębiorstwa oraz jego przyczyn, które mogą być zarówno pojedynczym zdarzeniem, jak i ciągiem takich zdarzeń [Yang, Haugen, 2015]. Z kolei wskazanie skutków materializacji „najgorszego scenariusza" powinno obejmować cały zakres możliwych konsekwencji wliczając zdrowie i życie pracowników, straty materialne, finansowe i wizerunkowe. Wyniki będące efektem poprawnie przeprowadzonej analizy powinny w sposób wyraźny wskazywać konieczności podjęcia działań prewencyjnych dla poszczególnych, zidentyfikowanych w procesie analizy przyczyn, wraz z uzasadnieniem tej konieczności i ukierunkowaniem na działania korekcyjne adekwatne dla danego „najgorszego scenariusza".



Rys. 38. *Diagram ukazujący zależności pomiędzy ryzykami występującymi w KWC i ich konsekwencjami, a działaniami prewencyjnymi.*

7.1.4 Zastosowanie sieci bayesowskich w IRM DSS

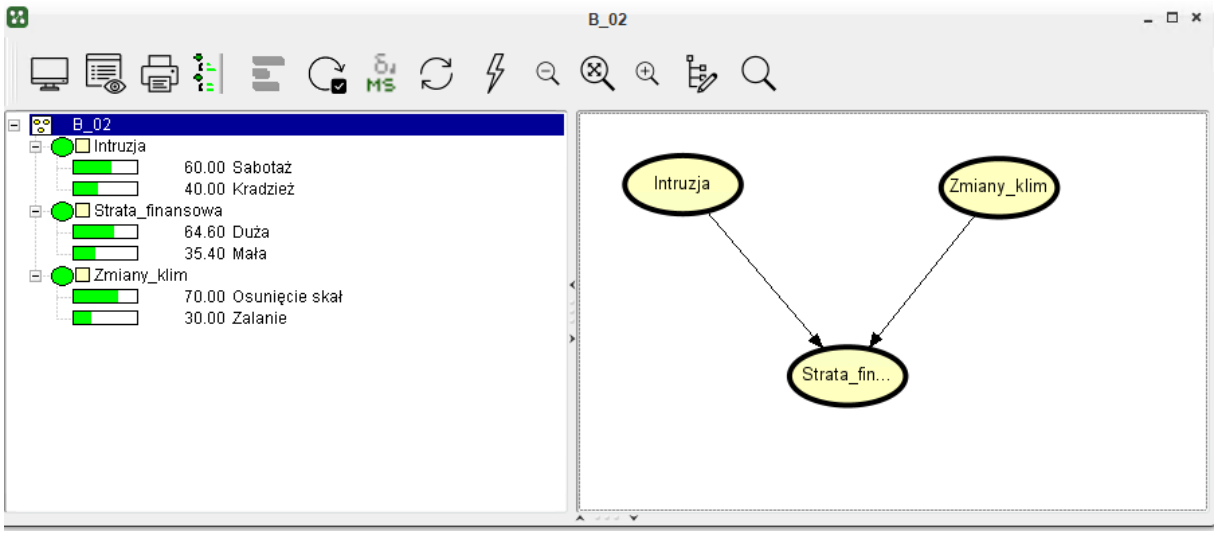
Dobrym i praktycznym sposobem modelowania relacji pomiędzy zdarzeniami i zmiennymi losowymi są tzw. sieci bayesowskie [Pearl, 1988]. Wierzchołkami takiej sieci są zmienne losowe, opisujące losowe zdarzenia i procesy, a krawędziami pomiędzy nimi są związki przyczynowe pomiędzy następującymi po sobie zmiennymi. Związki pomiędzy zdarzeniami mogą być opisywane przez zmienne losowe binarne. Zgodnie z [Monge i in., 2022] sformułujemy następującą definicję:

Definicja 7.1. Sieć bayesowska jest grafem acyklicznym skierowanym $G=(V,E)$, w którym V jest pewnym zbiorem zmiennych losowych, a $E=\{E_{i,j}\}$, gdzie $E_{i,j}:=P(V_i|V_{i,j1},\ldots,V_{i,jk(i)})$ opisuje probabilistyczne relacje kauzalne zachodzące pomiędzy węzłami sieci. ■

Analiza sieci tego typu korzysta wprost z teorii statystyki Bayesa, gdyż [Monge i in., 2022] sieci bayesowskie stanowią graficzną reprezentację rozkładu prawdopodobieństwa wielu zmiennych w postaci rozkładów warunkowych każdej z nich.

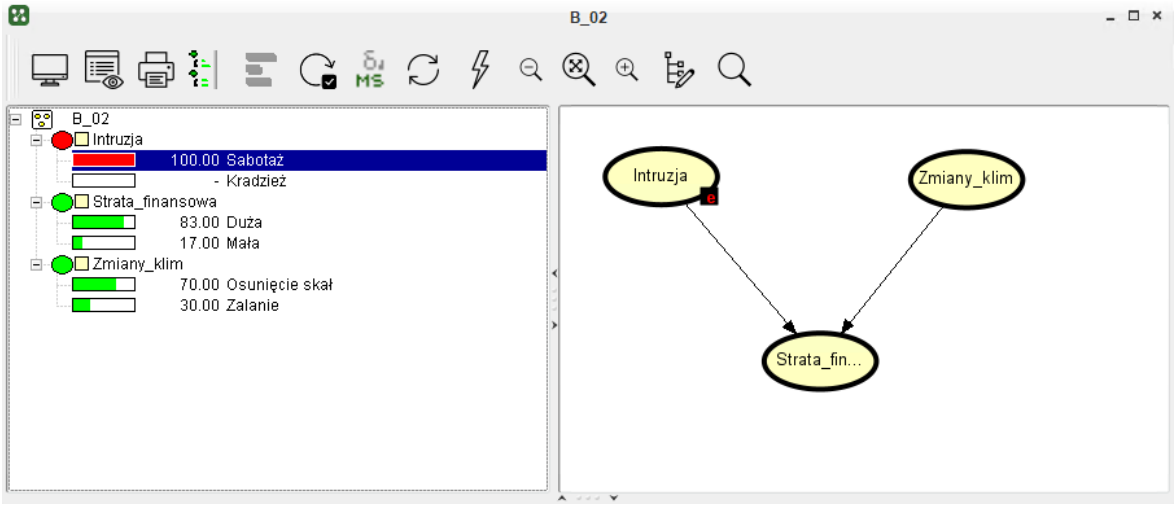
Prostą symulację możliwości wykorzystania sieci bayesowskiej do oceny wpływu zagrożeń zewnętrznych [

Rys. ***38***] na potencjalną stratę finansową przeprowadzono przy pomocy oprogramowania Hugin Lite 9.5. W symulacji uwzględniono zarówno czynniki o charakterze naturalnym, jak i antropogenicznym, natomiast rozkłady prawdopodobieństw dla poszczególnych zdarzeń określone zostały w oparciu o wiedzę ekspercką. Zadany rozkład prawdopodobieństw dla poszczególnych węzłów sieci bayesowskiej przygotowanej do oceny wpływu zjawisk związanych ze zmianami klimatycznymi oraz następstw intruzji na stratę finansową przedsiębiorstwa prezentuje rysunek [Rys. 39].

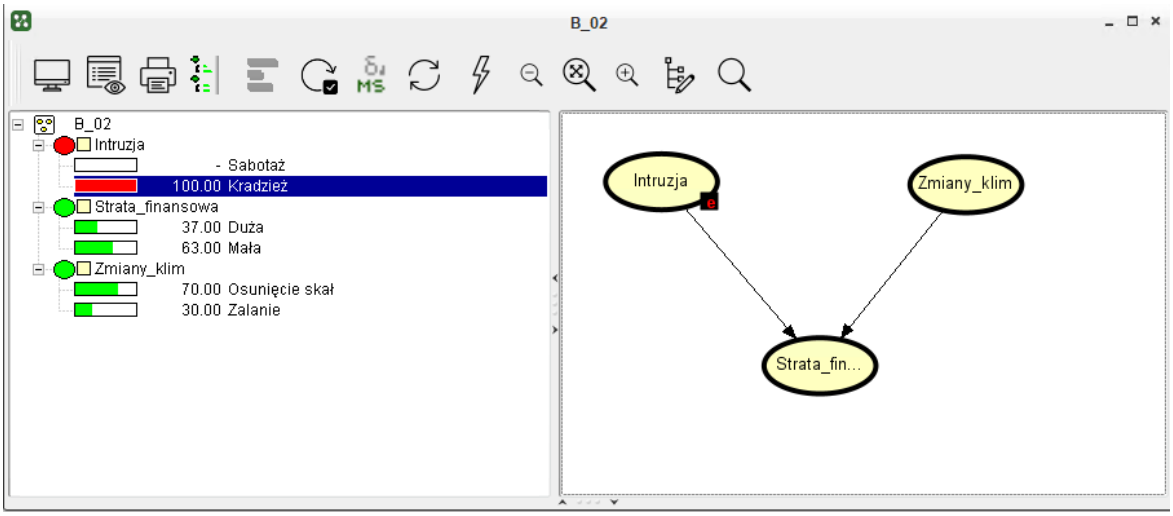


Rys. 39. Zadany rozkład prawdopodobieństw w sieci bayesowskiej.

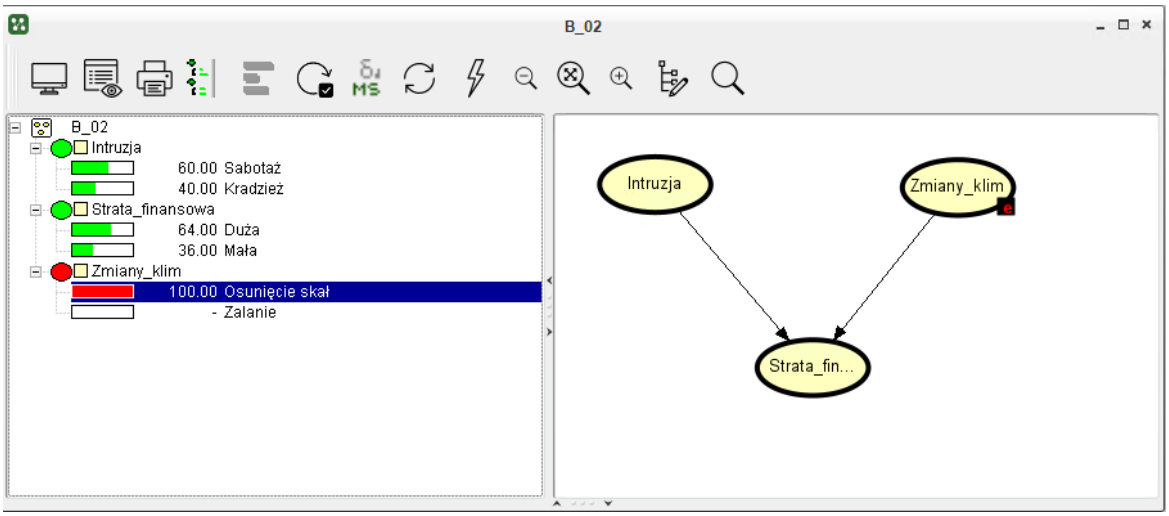
Kolejne rysunki przedstawiają symulacje zmian rozkładu prawdopodobieństwa w przypadku materializacji (prawdopodobieństwo 100%) poszczególnych ryzyk, kolejno: sabotaż [Rys. 40], kradzież [Rys. 41], osunięcie mas skalnych [Rys. 42], zalanie [Rys. 43].



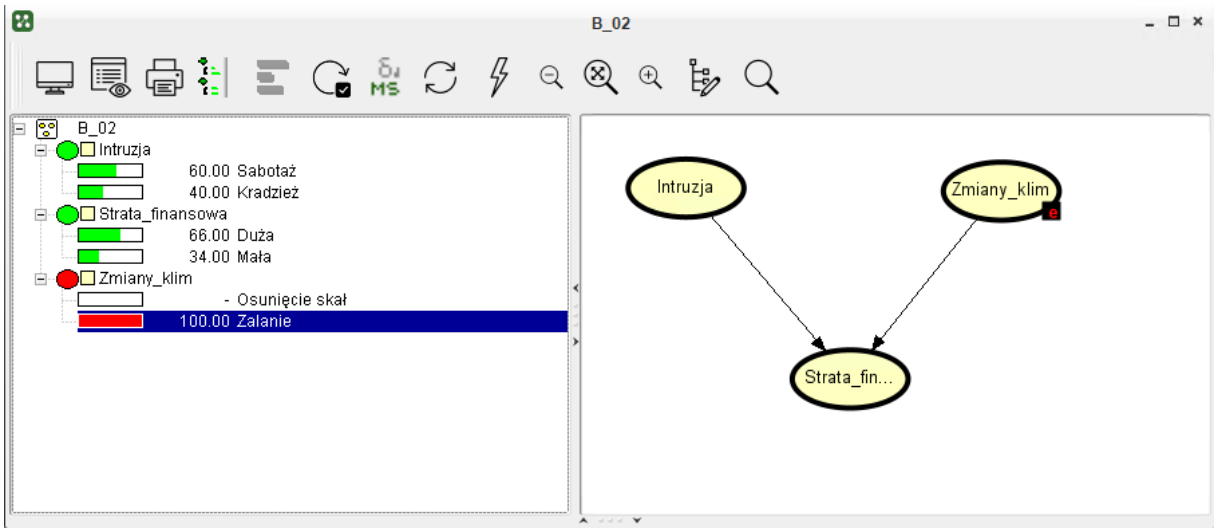
Rys. 40. Przykład obliczeń rozkładu prawdopodobieństwa w przypadku materializacji ryzyka sabotażu.



Rys. 41. Przykład obliczeń rozkładu prawdopodobieństwa materializacji ryzyka kradzieży.



Rys. 42. Przykład obliczeń rozkładu prawdopodobieństwa w przypadku materializacji ryzyka osunięcia mas skalnych.



Rys. 43. Przykład obliczeń rozkładu prawdopodobieństwa w przypadku materializacji ryzyka zalania maszyn i budynków.

Analiza powyższych przykładów pozwala potwierdzić możliwość i skuteczność wykorzystania modeli opartych na sieciach bayesowskich do oceny ryzyka w stanach niepewności oraz prowadzić symulację wpływu kolejnych elementów na wynik końcowy. Poziom szczegółowości można zwiększać, tym samym uwzględniając w symulacjach kolejne czynnik, ale nawet prowadząc proste analizy, uwzględniające tylko cztery rodzaje ryzyka (sabotaż, kradzież, osuniecie i zalanie) i zakładając materializację w każdym przypadku tylko jednego z czynników, widać, że wpływ na wynik ostateczny analizy (stratę finansową) zależy po pierwsze bezpośrednio od ryzyka, którego materializację badamy, a po drugie od zakładanego prawdopodobieństwa. Należy tu dodać, że w przypadku analiz dotyczących obszarów o charakterze przemysłowym i w przypadku braku danych historycznych, pozwalających precyzyjnie określić prawdopodobieństwo, bazować należy na wiedzy eksperckiej i doświadczaniu/intuicji osób prowadzących analizę w celu zarządzania ryzykiem

Sieci bayesowskie można rozbudowywać [Monge i in., 2022] w bardziej złożone struktury, takie jak diagramy decyzyjne, poprzez włączenie w ich strukturę węzłów decyzyjnych, jak w przypadku tzw. diagramów wpływu (Influence diagrams, Howard & Matheson). Analiza sieci bayesowskich i diagramów wpływu może korzystać także z metod ukrytych procesów Markowa, systemów zdarzeń dyskretnych, a po uwzględnieniu sprzężeń informacyjnych z wynikami przyszłych procesów - również sieci antycypacyjnych.

W niniejszej pracy sieci baayesowskie służyć będą głównie do opisu propagacji ryzyk w procesach produkcyjnych i logistycznych KWC. Etapy likwidacji zagrożeń opisywane będą innymi metodami z wykorzystaniem optymalizacji procesów.

Zaprezentowana na [Rys. 45] sieć składa się z:

1. Ryzyk o charakterze pierwotnym (kolor zielony):
   - zmiany klimatyczne,

- struktura geologiczna złoża,
- intruzja,
- roboty strzałowe,
- brak dostępności zasobów.

2. Ryzyk o charakterze wtórnym (kolor niebieski):
   - osunięcia skał,
   - zalanie,
   - sabotaż,
   - kradzież,
   - przypadkowe uszkodzenie,
   - świadome uszkodzenie,
   - pożar,
   - błąd ludzki,
   - cyberprzestępczość,
   - błąd operacyjny,
3. Zmiennych losowych, na które wpływ mają wskazane w punktach 1 i 2 ryzyka (kolor czerwony):
   - strata finansowa,
   - strata wizerunkowa,
   - szkody dla środowiska.

Dzięki takiemu podejściu możliwe jest utworzenie modelu rozkładów prawdopodobieństw zaistnienia pewnych zdarzeń poprzez połączenie w ciąg relacyjny zdarzeń o różnym charakterze oraz różnym źródle pochodzenia. Fakty wynikające wprost z otaczającej procesy rzeczywistości można w sposób logiczny połączyć z wiedzą ekspercką, parametryzując atrybuty związane z rozkładami prawdopodobieństwa zmiennych będących węzłami sieci bayesowskiej.

Zakłada się, że krawędzie sieci opisują relacje kauzalne pomiędzy węzłami. Nie zawsze jednak możliwe jest wskazanie bezpośredniego związku przyczynowego, gdyż nie zawsze znany jest przyszły skutek. Z tego względu parametry zmiennych i relacji w sieciach bayesowskich są estymowane adaptacyjnie w procesach uczenia maszynowego na podstawie danych obserwacyjnych. Istotną właściwością tych sieci jest funkcjonalność *anytime*, która oznacza, że sieci bayesowskie mogą generować przybliżone wyniki na dowolnym etapie obliczeń, nawet jeśli proces nie został jeszcze zakończony. Zamiast czekać na pełen zestaw danych lub zakończenie wszystkich iteracji, sieci bayesowskie są w stanie zaproponować najlepszą możliwą odpowiedź na podstawie aktualnie dostępnych informacji. W praktyce oznacza to, że wyniki mogą być użyteczne nawet w sytuacjach, gdy czas na analizę jest ograniczony, a dane przychodzą stopniowo. Drugim istotnym parametrem jest *incremental computing*, który odnosi się do zdolności sieci bayesowskich do aktualizacji swojego modelu w czasie rzeczywistym, w miarę jak nowe dane stają się dostępne. Sieci te nie wymagają przetwarzania wszystkich danych od początku przy każdej aktualizacji. Zamiast tego ich

struktura pozwala na dostosowanie się do nowych informacji bez utraty poprzednich wyników. Dzięki temu w środowiskach dynamicznych generują najlepsze wyniki na podstawie dostępnych w danej iteracji informacji.

Zbudowana w oparciu o opisane założenia sieć odwzorowuje procesy rzeczywiste, które wykazują ciągłość przy przechodzeniu z jednego stanu w kolejny, po nim następujący z punktu widzenia przebiegu samego procesu w czasie. Łańcuch zdarzeń, z jakim mamy do czynienia zachowuje powiązania kauzalne pomiędzy stanami, a przejścia do kolejnych stanów opisane są przez prawdopodobieństwo materializacji zdarzenia, czyli de facto prawdopodobieństwo przejścia ze stanu s_i do stanu s_j z prawdopodobieństwem $p_{ij} > 0$. W przypadku niektórych zdarzeń możliwe jest jednak przejście do kolejnych stanów procesu w sposób skokowy (podobnie jak w łańcuchach Markowa). Ten typ zjawisk wymaga analizy powiązań pomiędzy ryzykami, które analizowane są w rozdziale 2.5 i rozdziale 2.6, w wielu sytuacjach przy pomocy sieci bayesowskich lub antycypacyjnych.

7.1.5 Grafy reprezentacji wiedzy

Grafy wiedzy definiuje się jako strukturę matematyczną służącą do przedstawiania i badania wzajemnych relacji pomiędzy obiektami. Z matematycznego punktu widzenia graf jest zbiorem wierzchołków, które są połączone krawędziami w taki sposób, że każda krawędź kończy się i zaczyna w jednym z wierzchołków. W związku z tym, że graf wiedzy formalnie opisuje jednostki i ich relacje, naturalnym wydaje się wykorzystanie tej struktury jako schematu umożliwiającego logiczne wnioskowanie w celu pobierania informacji predykcyjnych [Skulimowski, Łydek, 2022b].

Grafy wiedzy są obecnie szeroko wykorzystywane w obszarach związanych z przetwarzaniem danych, w szczególności przy wsparciu przez algorytmy AI, funkcjonując jako rozbudowane struktury danych. Rozpatrując graf wiedzy jako zbiór danych, składających się z wierzchołków (reprezentujących obiekty, miejsca, zdarzenia) i krawędzi (odwzorowujących relacje zachodzące pomiędzy węzłami) wspomnieć należy również o atrybutach (etykietach), czyli informacjach dodatkowych, które przypisane mogą być zarówno do węzłów, jak i krawędzi. Atrybuty wzbogacają graf, dodając kontekst i dane szczegółowe, dzięki którym łatwiej jest zrozumieć relacje zachodzące pomiędzy poszczególnymi elementami w strukturze grafu. Dodatkowo atrybuty przypisane do krawędzi mogą być wykorzystane do popisania cech, które wpływają na proces decyzyjny, takich jak np. siła oddziaływania, czas trwania czy kierunek relacji [Purohit i in., 2019].

Modelowanie rzeczywistych sytuacji przy wykorzystaniu grafy wiedzy odbywa się na drodze dodawania i usuwania wierzchołków oraz krawędzi odwzorowujących relacje pomiędzy nimi. Natomiast matematyczna analiza zgromadzonych w ten sposób danych prowadzona jest

w oparciu o dwuwymiarowy rachunek macierzowy (macierz incydencji). Macierz zawiera zestaw wierzchołków i krawędzi, oraz odwzorowuje występujące pomiędzy nimi powiązania.

Dzięki opisanej powyżej funkcjonalności grafy wiedzy mogą być wykorzystywane przez sieci antycypacyjne jako jedna z technik budowania złożonych modeli predykcyjnych [Skulimowski, Łydek, 2022b]. Realizowane jest to na drodze budowania struktur wiedzy o systemie (procesie), który podlega modelowaniu. Tak skonstruowany model wykorzystywany jest przez sieci antycypacyjne do tworzenia prognoz co do dalszych stanów systemu (procesu). Analiza wzajemnych zależności realizowana w grafach umożliwia symulację przyszłych stanów systemu (procesu). Można powiedzieć, że grafy wiedzy wspierają organizację 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.

Podsumowując, można powiedzieć, że grafy wiedzy i sieci antycypacyjne mogą się wzajemnie uzupełniać, organizując posiadane informacje (wiedzę) i używając ich w celu podejmowania bardziej świadomych i adekwatnych do sytuacji decyzji.

7.2 Ontologie i notacja stosowane w IRM DSS

Ontologia w kontekście przetwarzania danych to struktura formalna, która opisuje zbiór pojęć i relacji między nimi w danym obszarze wiedzy. Jest to rodzaj wiedzy o tym, jak różne elementy i pojęcia w danej dziedzinie są zdefiniowane, powiązane i organizowane. Ontologie są kluczowe dla umożliwienia efektywnego zarządzania, przetwarzania i wymiany informacji w różnych systemach oaz pomiędzy różnymi systemami. Do kluczowych elementów ontologii zaliczyć można:

- pojęcia (klasy) – są to abstrakcyjne reprezentacje obiektów lub zjawisk z danej dziedziny,
- relacje – opisujące związki między pojęciami,
- atrybuty (własności) – czyli cechy, które można przypisać pojęciom,
- instancje – konkretne obiekty, które należą do danej klasy,
- reguły i aksjomaty – czyli zbiory zasad, które określają ograniczenia lub wytyczne w ramach konkretnej, wybranej ontologii.

7.2.1 Zastosowanie ontologii do reprezentacji i przetwarzania wiedzy

Przetwarzanie wiedzy w IRM DSS opiera się o ontologię domenową zarządzania ryzykiem przedstawioną wstępnie w [rozdział 1.2] baza wiedzy wchodząca w skład IRM DSS zawiera

także inne informacje i procesy opisane w [10.2], do obsługi których wykorzystywane są dodatkowe ontologie, przede wszystkim ontologia metod analitycznych i sztucznej inteligencji oraz ontologia nadrzędna związana z opisem procesów wspomagania decyzji. Struktura ontologii IRM DSS odpowiada strukturze opisanej poniżej.

W celu opisu ontologii wykorzystuje się język OWL (Web Ontology Language), który umożliwia reprezentowanie złożonych struktur wiedzy w sposób zrozumiały zarówno dla algorytmów, jak i ludzi. Ontologie w OWL składają się z klas, relacji (własności), indywidualnych obiektów (instancji) i reguł. OWL pozwala na definiowanie hierarchii pojęć, relacji między nimi oraz tworzenie logicznych ograniczeń. Aby stworzyć bazę danych odpowiadającą ontologii przedstawionej w OWL, musimy przekształcić elementy składające się na klasy, relacje (własności) oraz instancje w tabele relacyjne. Każda klasa w ontologii staje się tabelą, a relacje między klasami są odwzorowywane jako tabele łączące.

Przykładowa struktura bazy danych dla środowiska zagrożeń przemysłowych:

1. **Tabela Maszyny** – przechowuje dane dostępnych maszynach.
2. **Tabela Zagrożenia** – przechowuje dane o zidentyfikowanych zagrożeniach.
3. **Tabela Wozidło** – dedykowana tabela zagrożeń dla wozideł (podklasa Zagrożenia).
4. **Tabela Personel** – dedykowana tabela zagrożeń dla personelu (podklasa Zagrożenia).
5. **Tabela MasZag** – odwzorowuje relacje pomiędzy Maszynami i Zagrożeniami, jest to tabela łącząca.

Ta struktura pozwala na odwzorowanie koncepcji ontologicznych, takich jak klasy, podklasy oraz relacje, w typowej relacyjnej bazie danych. Możliwe jest rozszerzanie tego modelu o dodatkowe informacje, a także bardziej złożone relacje.

7.2.2 Notacja BPMN w IRM DSS

Notacja BPMN (Business Process Model and Notation) jest standardem służącym do modelowania procesów biznesowych. Umożliwia graficzne przedstawienie przebiegu procesów w przedsiębiorstwie, co ułatwia ich zrozumienie, analizę oraz optymalizację. BPMN, szczególnie w swojej wersji BPMN 2.0, pozwala modelować szeroki wachlarz procesów i otwiera możliwość ich automatycznej weryfikacji oraz dalszego przeniesienia na język zrozumiały dla komputera, umożliwiając prowadzenie symulacji. Istnieją również specjalistyczne rozwinięcia BPMN, takie jak DMN (Decision Model and Notation), które ukierunkowane są na modelowanie procesów decyzyjnych. Proces obrazujący schemat funkcjonowania systemu IRM DSS zaprezentowany został na rysunku [Rys. 99].

Pomimo szerokich możliwości i wszechstronności notacji BPMN, nie jest ona idealna do modelowania procesów czysto przemysłowych, takich jak procesy produkcyjne czy

techniczne. Wynika to z jej skupienia na przepływie informacji i zadań między uczestnikami procesu, podczas gdy kluczowe aspekty w procesach przemysłowych obejmują przepływ surowców, półproduktów i produktów gotowych. Brakuje jej również szczegółowych reprezentacji maszyn, urządzeń i zmiennych fizycznych, które są istotne w technicznych procesach produkcyjnych. Co więcej, procesy produkcyjne często charakteryzują się dużą liczbą równoległych operacji wymagających synchronizacji i harmonogramowania, co stanowi wyzwanie dla precyzji BPMN.

W kontekście projektowania IRM DSS dla Kopalni Wapienia Czatkowice (KWC), BPMN stosowano jako narzędzie do specyfikacji procesów na poziomie ogólnym, odpowiadające modułowej architekturze systemu. Procedury związane z oceną, analizą i zapewnieniem bezpieczeństwa można zdefiniować jako działania realizowane w określonej kolejności, które mogą także odwoływać się do wcześniej wykonanych zadań. Taki sposób opisu pozwala na przejrzystą prezentację złożonych procesów, co ma znaczenie dla zarządzania bezpieczeństwem w środowisku przemysłowym.

Dotychczas notacja BPMN nie była szeroko wykorzystywana do szczegółowego modelowania procesów związanych z zarządzaniem bezpieczeństwem. Dlatego w ramach dalszych prac nad IRM DSS rekomenduje się opracowanie wariantu BPMN dedykowanego właśnie takim celom (IRM-BPMN). Wariant ten uwzględniłby specyfikę zarządzania bezpieczeństwem, w tym integrację działań prewencyjnych i ratunkowych, co otworzy nowe możliwości w zastosowaniu BPMN w środowiskach przemysłowych. Jest to szczególnie istotne w kontekście rosnącej popularności tej notacji i jej zdolności do adaptacji w nowych, dotąd nieeksplorowanych obszarach. Podsumowując, BPMN pozostaje standardem o dużym potencjale, szczególnie w zakresie modelowania procesów biznesowych. Jednak jej ograniczenia w obszarze procesów technicznych i przemysłowych wskazują na potrzebę rozwijania wariantów dedykowanych, takich jak IRM-BPMN, które lepiej odpowiadałyby specyficznym wymaganiom środowiska przemysłowego.

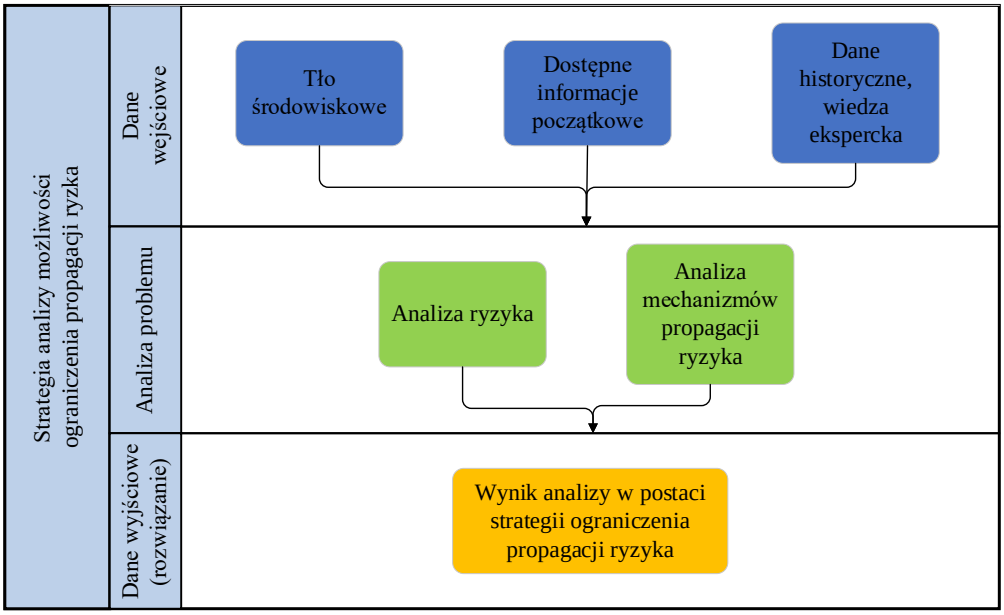
Pośrednim krokiem pomocniczym, wykorzystywanym w formułowaniu odpowiedzi decyzyjnej (rozwiązania badanego problemu) jest opracowanie macierzy konsekwencji oraz macierzy decyzji i dopiero w oparciu o to zaproponowanie decyzji optymalnej [Cremen, Galasso, 2021]. Natomiast w oparciu o dane historyczne i eksperckie system pełni funkcje pewnego rodzaju symulatora, który wykorzystując posiadane dane i reguły, wskazuje możliwość materializacja ryzyk, tworzy symulacje katastrof i wyciąga wnioski zapobiegające wystąpieniu zdarzenia objętego procesem symulacji. Pomagać w tym powinno ciągłe zasilanie systemu danymi technicznymi, środowiskowymi i ekonomicznymi. Zapewnić to może integracja systemu DSS np. z system klasy ERP wykorzystywanym w przedsiębiorstwie oraz podsystemami dziedzinowymi dedykowanymi dla specyficznych obszarów funkcjonowania przedsiębiorstwa produkcyjnego. W takim globalnym ujęciu proces podejmowania decyzji rozpoczyna się od gromadzenia informacji na długo przed

hipotetycznym jeszcze zdarzeniem [Wilson i in., 2014] i obejmuje etapy tworzenia reguł, modeli, omawianych powyżej scenariuszy oraz modelowania danych w procesie analizy wielokryterialnej pod kątem stopnia ich użyteczności i priorytetu. Tak przygotowane dane (decyzje) są zwłaszcza przydatne w pierwszej fazie działania, kiedy ilość danych rzeczywistych (tj. pozyskanych do obsługi konkretnego zdarzenia) może być skąpa i/lub niepełna.

7.3 Propagacja ryzyka

Współczesne systemy przemysłowe są zwykle bardzo złożone, składają się z wielu współzależnych elementów, a ich opisanie i poddanie szczegółowej analizie jest trudne i wymagające często wykorzystania hybrydowych modeli nieliniowych, zarówno dyskretnych, jak i modeli procesów ciągłych oraz wsparcia wiedzą ekspercką. Z tego względu, analiza złożonych modeli wymaga również zrozumienie mechanizmu propagacji ryzyka w sieciach systemów przemysłowych, które jest istotne z punktu widzenia skutecznego ograniczania ryzyka w celu zapewnienia bezpieczeństwa systemów przemysłowych [Feng i in., 2024]. W systemach tych występują złożone interakcje i mechanizmy sprzężenia zwrotnego. Dla celów wspomagania decyzji w niniejszej rozprawie przyjęliśmy metody modelowania rzeczywistych układów przemysłowych w postaci grafów wiedzy (por [rozdz. 7.1.5]), gdzie węzły reprezentują główne elementy procesów (np. technologicznych), natomiast krawędzie odwzorowują połączenia i wzajemne relacje pomiędzy tymi elementami [Feng i in., 2024].

Zakłócenia spowodowane bezpośrednio lub pośrednio różnymi zagrożeniami powstającymi w systemach przemysłowych powodują przestoje operacyjne. Jest to konsekwencją faktu, że zakłócenia w działaniu dowolnego węzła sieci, odwzorowującej rzeczywiste środowisko przemysłowe, mogą wpływać na inne węzły poprzez propagację, powodując straty ekonomiczne [Xue i in., 2024]. Multigrafy typu TRRM odwzorowujące rzeczywiste systemem będące głównym przedmiotem badania w pracy, również podlegają procesowi propagacji ryzyka, co wynika wprost ze zmienności (dynamiki) procesu będącego źródłem i konsekwencją zagrożenia, w czasie. W przypadku modelowania propagacji ryzyka w sieci charakteryzującej się dynamiką zmian, każdy z węzłów można traktować jako element generujący ryzyko. Budowa modelu takich procesów oparta jest o wybór metody identyfikacji elementów ryzyka, ocenę zasad przenoszenia ryzyka i formułowanie strategii zapobiegania propagacji ryzyk [Rys. 44].



Rys. 44. Formułowanie strategii zapobiegania propagacji ryzyk.

W oparciu o przeprowadzone badania bibliograficzne i analizy własne postawić można dwie główne hipotezy, w oparciu o które prowadzona będzie analiza możliwości budowy modelu ryzyka w systemie przemysłowym KWC, a w przypadku pozytywnym - dalsza analiza propagacji ryzyka

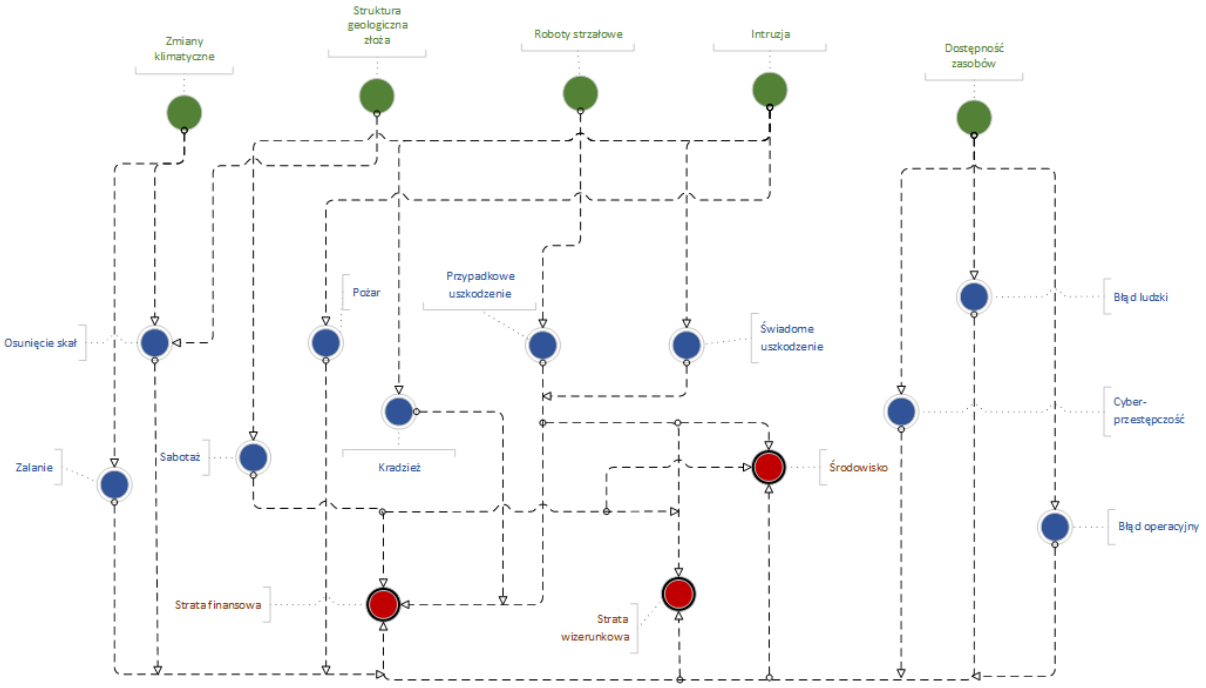
Założenie 1. W złożonym systemie przemysłowym propagacja ryzyka jest dynamicznym procesem jednokierunkowym lub dwukierunkowym i wymaga wskazania źródeł ryzyka, dlatego sieć opisująca propagację ryzyka w systemie przemysłowym jest multigrafem skierowanym [Feng i in., 2024].

Założenie 2. W sieciach opisujących złożone systemy przemysłowe możliwość propagacji ryzyka modelowana jest przez krawędzie sieci. Krawędź taka otrzymuje atrybut „aktywny", gdy na podsystem będący jednym z węzłów tej krawędzi oddziałuje ryzyko pochodzące z podsystemów modelowanego przez drugi węzeł [Feng i in., 2024]. Gdy model ryzyka nie jest związany z konkretnym przebiegiem procesu propagacji, wówczas krawędź oznaczana jest jako „nieaktywna".

Przebiegi procesu propagacji nie są jednorodne, w szczególności prędkość propagacji zagrożeń (będących konsekwencją materializacji ryzyk) może się istotnie zmieniać. Różne występujące w tych procesach czynniki, wpływają na rozprzestrzenianie się zagrożeń i propagację ryzyka, zarówno przyspieszając, jak i spowalniając ten proces. W przypadku wystąpienia awarii, *post factum* analizujemy czynniki, które mogą mieć wpływ na dalszą prędkość rozprzestrzeniania się ryzyka, uwzględniając całe środowisko, w którym funkcjonuje dany proces przemysłowy (czynnik ludzki, maszyny, środowisko naturalne, procesy zarządcze) [Rys. 44]. Oczywistym jest również, że struktura i wzajemna odległość obiektów przemysłowych modelowanych w takiej sieci odgrywa kluczową rolę

w rozprzestrzenianiu się ryzyka. Dodatni stopień węzła, tj. liczba krawędzi wchodzących modelujących proces propagacji ryzyka określa możliwość nakładania się ryzyka w tym węźle.

Powiązane ze sobą zagrożenia i ryzyka mogą być modelowane przy wykorzystaniu sieci bayesowskich. Dla przykładu, na [Rys. 45] można wskazać stany, których pojawienie się (materializacja) możliwe będzie dopiero po ustaniu stanu poprzedniego. Mając na uwadze realia zakładu przemysłowego, z rozległym i trudnym do zabezpieczenia terenem, procesami o charakterze skokowym będą przede wszystkim zjawiska o charakterze antropogenicznym, czyli kradzież czy świadome uszkodzenie na skutek aktu wandalizmu.



Rys. 45. Propagacja ryzyk w procesach produkcyjnych w kopalni odkrywkowej.

7.3.1 Dynamiczne modele propagacji ryzyka

Z punktu widzenia analizy procesu rozprzestrzeniania się awarii i propagacji ryzyka zarówno stany węzłów, jak i struktura złożonej sieci systemów przemysłowych ulegają zmianom w czasie, czyniąc zbiór węzłów złożonej sieci systemów przemysłowych częścią nieliniowego układu dynamicznego. Rozprzestrzenianie się ryzyka awarii w sieci można modelować za pomocą wzoru (7.3) uwzględniającego propagację ryzyka między węzłami na podstawie ich wzajemnych zależności:

$$Np. \quad R_i(t+1)=R_i(t)+\sum_{j\in N(i)}(R_j(t)*w_{ij}*T_{ij}) \tag{7.3}$$

gdzie: $R_i(t)$ to ryzyko awarii w węźle i w czasie t, $N(i)$ to zbiór węzłów j, które oddziałują na i, w_{ij} to waga krawędzi ij a T_{ij} to tłumienie (lub wzmocnienie) propagacji ryzyka.

Dynamika propagacji ryzyka opisuje sytuacje, gdy w miarę rozprzestrzeniania się awarii, mogą być tworzone nowe połączenia i węzły (w określonych sytuacjach), co spowoduje szybszą propagację. Można to rozumieć jako powstawanie nowych połączeń, co prowadzi do ciągłych zmian w strukturze sieci. Z tego wynika konieczność dogłębnego zbadania mechanizmu rozprzestrzeniania się awarii i propagacji ryzyka, a także obliczenie progu propagacji ryzyka, rozprzestrzeniania się awarii i zasięgu propagacji ryzyka. Kontrolowanie procesu rozprzestrzeniania się ryzyka ma z założenia zapobiec jego niekontrolowanej eskalacji, przy czym ukierunkowana strategia ochrony wydaje się być bardziej skuteczna niż strategia losowej ochrony ryzyka ze względu na możliwość podejmowania działań zapobiegawczych w trakcie trwania procesu. Należy jednak zaznaczyć, że obie strategie ochrony są skuteczniejsze niż scenariusz bez wdrożonej strategii ochrony. Wynika to wprost z faktu, że strategia właściwa (ukierunkowana) dostosowana będzie po pierwsze do specyfiki środowiskowej analizowanego problemu oraz szybkości przebiegu zdarzań, z uwzględnieniem struktury przepływu zagrożenia, a po drugie pozwoli uwzględnić posiadaną wiedzę, zarówno ekspercką, jak i nabytą w wyniku badań i analiz prowadzonych w ramach profilaktyki przeciwwypadkowej.

Istotnym wyjątkiem, na który w przypadku analizy prowadzanej w niniejszej pracy trzeba zwrócić uwagę, jest fakt, że pomiędzy węzłami warstwy urządzeń inteligentnych nie ma bezpośredniego połączenia fizycznego, a ich komunikacja zależy od sieci komunikacyjnej warstwy wyższej (np. IoT). Mając na uwadze powyższe, należy uwzględnić, że propagacja ryzyka w warstwie inteligentnych urządzeń wymaga zamodelowanie interakcji związanych z cyberbezpieczeństwem oraz zakłóceniami transmisji, a z pomocą przychodzi model propagacji ryzyka, którego rdzeniem jest prawdopodobieństwo, opisujące proces propagacji ryzyka w warstwie urządzeń inteligentnych [Ju i in., 2024]. Ryzyko zostanie tutaj przeniesione pomiędzy dwoma węzłami połączonymi krawędzią, a wraz ze wzrostem ilości danych możliwa będzie identyfikacja rozkładu prawdopodobieństwa charakteryzująca transfer ryzyka pomiędzy dwoma powiązanymi węzłami. Wówczas na podstawie stanu początkowego węzła i prawdopodobieństw jego wpływów na stan węzłów sąsiednich, można symulować stan całej sieci [Ju i in., 2024].

Głęboka integracja systemów o charakterze czysto produkcyjnym z systemami informatycznymi, z jaką mamy do czynienia w ostatnich latach (Przemysł 4.0, technologia IoT) spowodowała, że możemy mówić o systemach cyberfizycznych. Niesie to jednak ze sobą konsekwencję w postaci braku jednolitych metod modelowania tego typu relacji. Podobną do TRRM metodę analizy zaproponowano w [Li i in., 2022].

Propagacja ryzyka jest zwykle procesem dynamicznym i począwszy od pierwszego zdarzenia, pierwszej materializacji ryzyka, prawdopodobieństwo w każdym kolejnym węźle wzrasta. Kluczowe staje się więc określenie końcowego zasięgu oddziaływania w korelacji z mechanizmem rozprzestrzeniania się zagrożenia. Zaproponowane rozwiązanie tego typu

problemu opiera się o model smugi Gaussa. Uzupełnieniem tego modelu może być wykorzystanie parametru kontrolnego znanego jako próg zakłócenia. Parametr ten zapewnia większą elastyczność w zakresie łagodzenia skutków zakłóceń. Przyjąć można, że im wyższy próg zakłóceń posiada sieć, tym mniejsze prawdopodobieństwo propagacji zakłóceń w sieci. Ponieważ różne zdarzenia, będące konsekwencją różnych ryzyk, mają różny wpływ na stabilność całej sieci, parametr ten jest narzędziem, dzięki któremu decydent może prowadzić analizę wyników poprzez symulację różnych źródeł zakłóceń [Habibi i in., 2023].

Zestawienie omówionych modeli propagacji ryzyka, z uwzględnieniem głównych obszarów ich wykorzystania oraz oceną przydatności zastosowywania do analizy zagadnień propagacji ryzyka w środowisku przemysłowym przedstawiono w [Tab. 17].

Tab. 17. Główne modele propagacji ryzyka.

Modele propagacji ryzyka	**Główne obszary zastosowania**	**Przydatność w problematyce przemysłowej**
TRRM	Systemy przemysłowe, katastrofy naturalne, zdarzenia wielkoskalowe	Duża
Modele dyfuzyjne	Logistyka transportu	Średnia
Automaty komórkowe	Logistyka transportu, katastrofy naturalne o przewidywalnym zasięgu	Średnia
Modele łańcuchowe	Logistyka transportu	Mała
Modele epidemiczne	Logistyka transportu	Mała

Ostatnim aspektem, na który należy zwrócić uwagę w procesie analizy odporności i propagacji ryzyka jest konieczność znalezienia kompromisu między ograniczaniem propagacji ryzyka a odbudową systemu w przypadku braku możliwości zapobieżenia propagacji. Analizując przyczyny materializacji ryzyka znaleźć i wskazać należy czynniki, które wpływać będą na przenoszenia ryzyka, tworząc mapę propagacji, w postaci łańcucha zdarzeń przyczynowo skutkowych. Kluczowa jest w tym przypadku jest dynamika zmian w sieci, której to wartość rzutować będzie na sam proces propagacji. Przy dużej dynamice zmian, przekraczającej tempo, w jakim można poznać charakterystyczne zachowanie systemu, jego reakcję i ewentualną odbudowę lub nawet dynamice wykraczającej poza możliwości percepcyjne decydenta, propagacja jest zjawiskiem nieuniknionym i szukanie

kompromisu przechodzi na dalszy plan, a kluczowe staje się doraźne usuwanie skutków zagrożenia i ograniczanie strat.

7.4 Miary ryzyka

Miary ryzyka to narzędzia umożliwiające ocenę, analizę i zarządzanie różnymi rodzajami ryzyka w różnych dziedzinach, takich jak inżynieria, zarządzanie projektami, logistyka, bezpieczeństwo i inne, w których problematyka związana z oceną ryzyka jest analizowana. Służą do ilościowego wyrażenia zagrożeń, z którymi może się zetknąć organizacja lub system. W zależności od specyfiki ryzyka, stosowane są różne metody mierzenia jego skali i prawdopodobieństwa. Najbardziej rozpowszechnione są miary ryzyka używane w ekonomii finansach. Stosuje się w tych obszarach wiele różnych miar ryzyka w celu oceny zagrożeń i potencjalnych strat. Są one kluczowymi narzędziami, które pozwalają na ocenę i zarządzanie różnorodnymi zagrożeniami w finansach. Wybór odpowiedniej miary zależy od charakterystyki aktywów, strategii inwestycyjnej oraz warunków rynkowych. Efektywne zarządzanie ryzykiem opiera się na kombinacji tych narzędzi w celu zminimalizowania potencjalnych strat. Do najbardziej znanych miar ryzyka w obszarze finansów należą:

- Wartość zagrożona (Value at Risk, VaR) - mierzy maksymalną oczekiwaną stratę portfela przy danym poziomie ufności w określonym horyzoncie czasowym.
- Odchylenie standardowe (Standard Deviation) - mierzy zmienność wartości aktywów lub portfela wokół ich średniej.
- Wartość oczekiwana (Expected Shortfall) - jest rozszerzeniem VaR i mierzy średnią stratę, której można się spodziewać w najgorszych przypadkach, przekraczających VaR.
- Współczynnik Sharpe'a (Sharpe Ratio) - mierzy stosunek zwrotu z inwestycji do jej ryzyka (mierzonego jako odchylenie standardowe).
- Ryzyko kredytowe (Credit Risk) - mierzy prawdopodobieństwo niewypłacalności kontrahenta, który nie jest w stanie spłacić swojego długu lub zobowiązań.

Miary ryzyka są również stosowane w innych dziedzinach aktywności, aby zidentyfikować, ocenić i zminimalizować zagrożenia, które mogą wpływać na operacje, zasoby czy procesy decyzyjne. Poniżej znajdują się kluczowe miary ryzyka stosowane w sektorach, takich jak zarządzanie projektami, bezpieczeństwo, logistyka czy środowisko.

- Ryzyko operacyjne - odnosi się do strat wynikających z niedoskonałości procesów wewnętrznych, błędów ludzkich, awarii systemów lub czynników zewnętrznych. W sektorze przemysłowym może obejmować awarie sprzętu, przestoje, a także błędy związane z procesami produkcyjnymi.

- Ryzyko technologiczne związane jest głównie z niewłaściwym użytkowaniem czy wdrażaniem nowych technologii, ale również z awarią systemów informatycznych lub cyberatakami.
- Ryzyko środowiskowe dotyczy zagrożeń wynikających z oddziaływania na środowisko lub zmian klimatycznych.
- Ryzyko projektowe odnosi się do możliwości wystąpienia problemów lub niepowodzeń w realizacji projektów w określonym czasie, budżecie i zakresie. Ryzyko projektowe jest kluczowe w zarządzaniu projektami i obejmuje zarówno ryzyka wewnętrzne, jak i zewnętrzne.
- Ryzyko związane z bezpieczeństwem obejmuje zagrożenia, które mogą prowadzić do uszczerbku na zdrowiu lub życiu ludzi, uszkodzenia mienia lub środowiska, np. pożary, wybuchy, wypadki pracy.
- Ryzyko logistyczne obejmuje zagrożenia związane z przerwaniami w łańcuchu dostaw, opóźnieniami w dostawach, czy niedoborem zasobów. Jest to istotne ryzyko w zarządzaniu operacyjnym i logistyką, szczególnie w globalnych łańcuchach dostaw.
- Ryzyko regulacyjne dotyczy zmian w regulacjach prawnych lub politykach rządowych na również na szczeblu lokalnym (samorządowym), które mogą wpłynąć na działalność firmy lub całego sektora gospodarczego.

Tak opisane miary ryzyk spełniają swoją rolę jako narzędzia, których rola jest zapobieganie negatywnym skutkom ryzyk poprzez ich wczesną identyfikację, ocenę i wdrożenie działań prewencyjnych. Skuteczne zarządzanie ryzykiem pozwala firmom i organizacjom minimalizować straty, zwiększać efektywność operacyjną oraz spełniać wymagania prawne i regulacyjne.

Zagadnienie miar ryzyka można również rozpatrywać z punktu widzenia systemu zarządzającego bezpieczeństwem, czy nawet bezpośrednio decydenta odpowiedzialnego za podejmowanie kluczowych decyzji w oparciu o dostarczane przez wspomagający go system (DSS) informacje. W takiej sytuacji kluczowe stają się informacje dotyczące:

- Prawdopodobieństwa wystąpienia, które wyraża jak duże jest prawdopodobieństwo, że dane ryzyko się zmaterializuje. Jest szeroko stosowana w zarządzaniu bezpieczeństwem i projektami. Wykorzystuje się ją do określenia, jak często zagrożenie może wystąpić na podstawie danych historycznych, symulacji lub ocen ekspertów.
- Wpływu zdarzenia, jeśli do niego dojdzie, na funkcjonowanie całego systemu, a w szczególności uszkodzenie mienia, zagrożenie zdrowia, środowiska czy przestój w produkcji.
- Oczekiwanej straty, obliczanej jako średnia strata związana z wystąpieniem określonego zagrożenia, uwzględniając zarówno prawdopodobieństwo, jak i wpływ

tego ryzyka. Jest to często stosowane w branżach takich jak energetyka, gdzie krytyczne awarie mogą prowadzić do dużych strat.

- Wskaźnika awaryjności stosowanego w przypadku złożonych systemów przemysłowych, który mierzy, jak często określony system lub urządzenie zawodzi w określonym czasie lub w warunkach użytkowania. Jest stosowany głównie w branżach inżynieryjnych, gdzie niezawodność maszyn i urządzeń ma kluczowe znaczenie.
- Wskaźnika niezawodności, który mierzy zdolność systemu do pracy bez awarii przez określony czas, podobnie jak wskaźnik awaryjności stosowany głównie w branżach inżynieryjnych.

W oparciu o powyżej przedstawione parametry zbudować można macierz ryzyka, która klasyfikuje ryzyka w dwóch wymiarach: prawdopodobieństwa i wpływu. Dzięki temu możliwe jest stworzenie priorytetów dla różnych zagrożeń, a ryzyka klasyfikowane mogą być np. w kategoriach: niskie, średnie, wysokie i krytyczne. Priorytetyzacja taka umożliwia podjęcie właściwych działań zapobiegawczych oraz określenie, które ryzyka należy traktować jako najpilniejsze do rozwiązania. Dzięki temu organizacja może podjąć działania zmierzające do minimalizowania ryzyka i zwiększanie niezawodności procesów oraz systemów, co ma bezpośredni wpływ na efektywność operacyjną i bezpieczeństwo.

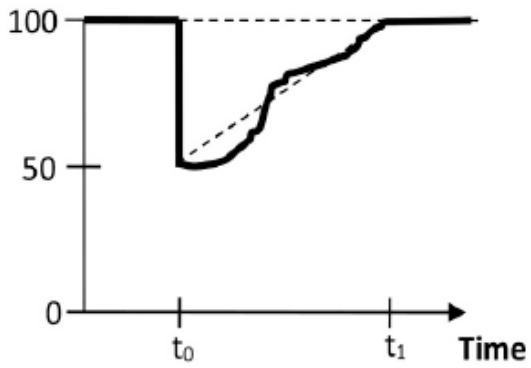
7.5 Specjalistyczne metody analizy ryzyka stosowane w IRM DSS

W systemie klasy IRM DSS działającym w czasie rzeczywistym i uwzględniającym bez zwłoki każdorazowe zmiany w zakresie materializacji zdefiniowanych ryzyk, istnieje możliwość wyznaczenia hipotetycznego ryzyka sumarycznego przed podjęciem decyzji o wdrożeniu działań mitygujących, o ile wyznaczone tak ryzyko *ex post* wzrosłoby przekraczając ustalony wcześniej dopuszczalny poziom.

Właściwe zarządzanie ryzykiem narzuca konieczność ciągłego gromadzenie danych dotyczących czynników ryzyka i zarządzanie tą informacją. Gromadzone i aktualizowane powinny być także metody analizy danych, optymalizacji ryzyka i wspomagania decyzji. Szczególną role odgrywają tu metody sztucznej inteligencji [Skulimowski, Bañuls, 2021]. Bazy danych i bazy wiedzy będące częścią systemu muszą zawierać również informacje historyczne. Zadaniem systemu zarządzania ryzykiem realizującego powyższą zasadę jest także generowanie wszystkich standardowych raportów stosowanych w analizie ryzyka finansowego, w tym wymaganych przez prawo. Implementacja systemu powinna zapewniać pełną zgodność zakresu i metod pomiaru ryzyka z obowiązującym w przedsiębiorstwie regulacjami i dobrymi praktykami wypracowanymi w tym obszarze.

7.5.1 Przegląd metody ilościowej oceny ryzyk przemysłowych

Ciekawą i wielowymiarową analizę metod oceny zagrożeń przedstawił [Zobel, 2010]. Artykuł powstał w oparciu o rzeczywiste zdarzenie, które dotknęło miasto Nowy Jork, a był nim huragan Sandy, który zaatakował wschodnie wybrzeże Stanów Zjednoczonych w roku 2012. Autor zastosował metodykę opartą o podejście inżynierskie, tj. przeprowadził ocenę odporności na klęskę żywiołową analizując fizyczne cechy systemu i zmieniającą się w czasie ewolucję zagrożeń od momentu uderzenia huraganu aż do odzyskania normalnej funkcjonalności systemów uszkodzonych w trakcje zdarzenia. Teoretyczne rozważania wsparte zostały ilościowym pomiarem odporności na zmaterializowaną katastrofę dzięki wykorzystaniu układów odniesienia i w dalszej kolejności porównaniu wyników. Badania prowadzone były w obszarze odporności społecznej (odporności na zagrożenia), łańcucha dostaw (surowców i mediów) i dalej odporności przedsiębiorstw na przerwy w dostawach (zerwania łańcucha dostaw). Autor w drodze rozważań zdefiniował i omówił koncepcję trójkąta odporności na katastrofy.



Rys. 46. Procentowa wydajność systemu w funkcji czasu [Zobel, 2010] .

Wykres pokazuje gwałtowny spadek wydajności systemu w chwili materializacji zagrożenia i późniejsze skutki będące reakcją systemu na czynnik wzbudzający. Obszar powyżej krzywej odpowiedzi (przeciwprostokątna trójkąta) zdefiniowany został jako miara utraty odporności [Rys. 46]. Zobel definiuje oczekiwaną odporność na awarie i katastrofy jako względną ilość pierwotnych funkcji systemu zachowywaną przez system w miarę upływu czasu (7.4). Jest ona obliczana w następujący sposób [Zobel, 2010]:

$$R\,(X,T) = \frac{T^* - \frac{XT}{2}}{T^*} = 1 - \frac{XT}{2T^*}, \quad X \in [0,1],\ T \in [0,T^*], \tag{7.4}$$

gdzie X to początkowa utrata wydajności systemu, a T to czas niezbędny do powrotu systemu do założonych parametrów początkowych. Kluczowym założeniem umożliwiającym porównanie różnych katastrof jest utrzymanie parametru T na stałym poziomie.

Należy zwrócić uwagę na fakt, że analiza przeprowadzona przez autora [Zobel, 2010] zrealizowana została *post factum*, gdy możliwe było wykorzystanie znacznej ilość rzeczywistych danych wejściowych. Prezentowane rozważania opierają się w znacznej mierze o wiedzę ekspercką użytkowników systemu i właścicieli ryzyk. Niemniej jednak, pomimo tej różnicy i bazowaniu na założeniach niepotwierdzonych empirycznie, zaproponowana metodyka uwzględnia aspekty rzeczywiste o różnych prawdopodobieństwach materializacji. Dodatkowo zalecane jest w takich sytuacjach używanie parametru *T* o wartości wskazanej przez decydenta tak, aby jak najlepiej odzwierciedlić jego ocenę sytuacji i interpretacje wyników.

7.6 Model propagacji i kumulacji ryzyk w KWC

Ryzyka w procesach przemysłowych kumulują się zgodnie z przebiegiem ciągu technologicznego, należy jednak zwrócić uwagę, że na kolejnych etapach po pierwsze mogą osiągać różne wartości, a po drugie zależeć będą od innych czynników, właściwych dla konkretnego umiejscowienia w ciągu produkcyjnym (np. wydobywanie urobku, załadunek, transportu, procesy przeróbcze i pomocnicze)

$$R = \Sigma_{1\le i\le n}\, S_i * E_i * P_i, \tag{7.5}$$

gdzie indeksy i=1, 2 ... *n* oznaczają kolejne elementy składowe ciągu technologicznego, które rozpatrywane są odrębnie. Dla procesu urabiania, załadunku i transportu surowca *n* ma wartość *n=4*, uwzględniając kolejno: prace przygotowawcze, urobek i załadunek surowca, transport, załadunek wtórny jako punkt styku z kolejnym ciągiem technologicznym. Propagację ryzyka opisujemy w postaci grafu skierowanego G, w którym węzłami są zagrożone obiekty, a krawędzie oznaczają wpływ ryzyka w obiekcie początkowym krawędzi A na obiekt w węźle końcowym B tej krawędzi. W najczęściej stosowanym modelu wpływ ten opisywany jest przez warunkowy rozkład prawdopodobieństwa wystąpienia ryzyka w węźle B pod warunkiem uprzedniego wystąpienia (materializacji) tego ryzyka w węźle A.

W ogólnym przypadku graf G jest multigrafem, w którym krawędzie jednego rodzaju odpowiadają propagacji określonego rodzaju ryzyka. Gdy występowanie czynników ryzyka jest wzajemnie niezależne, wówczas również niezależnie analizować można każdy z grafów poszczególnych ryzyk, po czym dokonać należy analizy skumulowanego ryzyka i wartości narażonej na stratę (VaR).

Gdy na prawdopodobieństwo wystąpienia ryzyka R w węźle B wpływają ryzyka w węzłach $A_1,\ldots,A_n$ oraz rozkłady prawdopodobieństw $\xi(B|A_1),\ldots, \xi(B|A_n)$ są warunkowo niezależne, wówczas prawdopodobieństwo materializacji przeniesionego ryzyka w węźle B grafu G można w tym przypadku wyrazić wzorem

$$\xi_R(B|A_1,\ldots,A_n)=1-\prod_{1\le i\le n}(1-\xi(B|A_i)) \tag{7.6}$$

Jeśli ryzyko R może wystąpić także w węźle B z rozkładem $\xi_{R,0}(B)$ niezależnie od propagacji R z węzłów $A_1,\ldots,A_n$, wówczas całkowity rozkład prawdopodobieństwa wystąpienia ryzyka R w B można opisać jako

$$\xi_R(B|A_1,\ldots,A_n)=1-\prod_{1\le i\le n}(1-\xi(B|A_i))(1-\xi_{R,0}(B)) \quad (7.7)$$

Poniżej podajemy przykład liczbowy wystąpienia ryzyka uszkodzenia obiektów produkcyjnych dla kolejnych elementów ciągu, tj. urobku i załadunku, transportu, maszyn pomocniczych.

Przykład 7.1.

W celu określenia liczbowych wartości prawdopodobieństwa materializacji tych ryzyk należy wziąć pod uwagę wynikające z doświadczenia zakładu oszacowanie bezpośredniej ekspozycji na zagrożenia opisane powyżej z uwzględnieniem kwantyfikacji zgodnej ze skalą Likerta [Tab. 3] oraz parametrem wskazującym czas pracy maszyny (dostępność maszyny) w warunkach, w których narażona jest na zagrożenia. Bezpośrednią ekspozycję na zagrożenia (naturalne i antropogeniczne) wyznaczamy w oparciu o wiedze ekspercką uczestników i/lub decydentów procesu, natomiast dostępność maszyny określamy przyjmując pewne uproszczenie, tzn. zakładając czas pracy zgodny z normami pracy dla poszczególnych ogniw uczestników procesu (praca na jedną, dwie lub trzy zmiany).

Przykład zakłada dwa węzły biorące udział w procesie:

A – urabianie i załadunek,

B – transport wraz z maszynami i urządzeniami pomocniczymi.

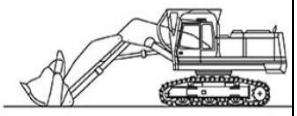
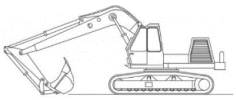
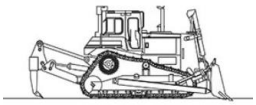
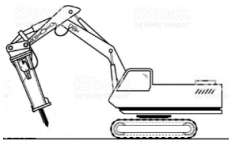
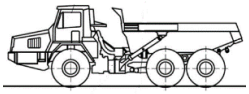
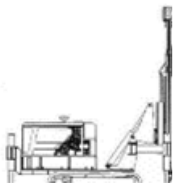
Podczas załadunku może się zdarzyć, np. uszkodzenie koła lub zawieszenia, które spowoduje zatrzymanie się samochodu po przejechaniu pewnego odcinka. W trasie mogą też zdarzyć się awarie niezwiązane z procesem załadunku.

Korzystając z omówionego powyżej wzoru:

$$\xi_R(B|A_1,\ldots,A_n)=1-\prod_{1\le i\le n}(1-\xi(B|A_i)) \quad (7.8)$$

przy czym każdorazowo węzły A i B zgodnie z powyższym wyjaśnieniem uwzględniają odmienne warunki pracy, w szczególności dostępność maszyny (można ją zdefiniować jako miarę efektywnego czasu, w którym maszyna jest gotowa i zdolna do realizacji wyznaczonych zadań, gotowość do pracy) i ekspozycję na zagrożenie (definiowaną jako miara prawdopodobieństwa oraz potencjalnych skutków, na jakie maszyna jest narażona w wyniku różnych czynników ryzyka w czasie przebywania w miejscach objętych badanym ryzykiem).

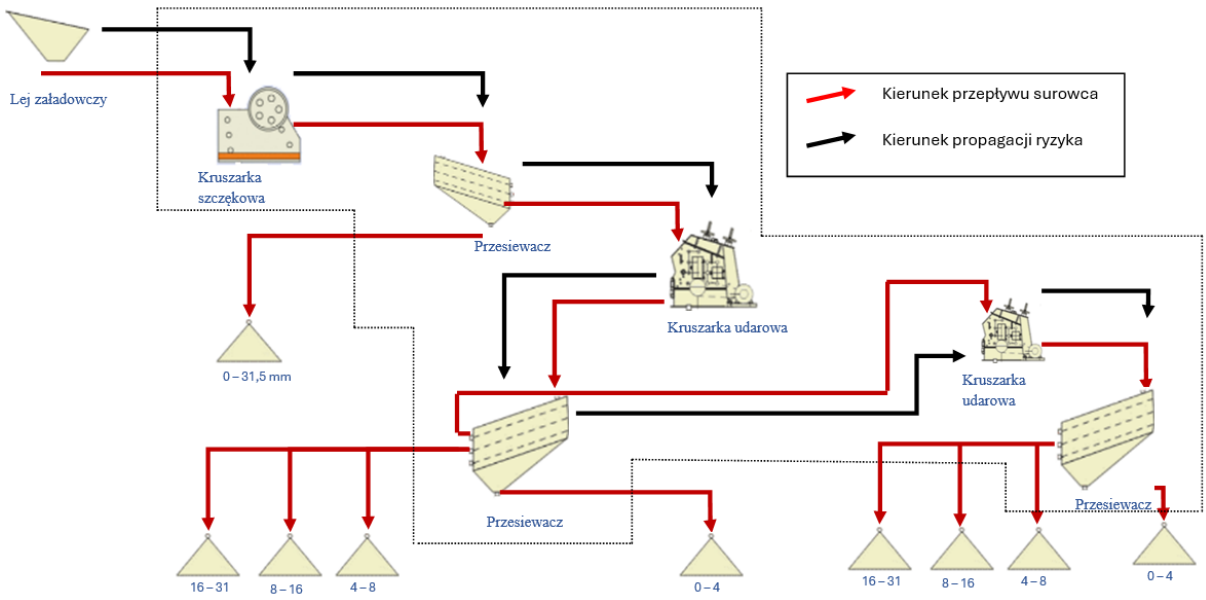
Tab. 18. Sposoby zarządzania ryzykami w procesie technologicznym urabiania, załadunku i transportu surowca (w kol. 4-7 7-stopniowa skala Likerta wg [Tab. 3]).

Rodzaj maszyny	Nazwa	Liczba maszyn	Ryzyko uszkodzenia maszyny na skutek awarii, wypadku, bądź świadomego zniszczenia	Pozostałe akty wandalizmu, przypadki kradzieży	Niewłaściwy sposób zarządzania czasem pracy i dostępności maszyny	Roczna wartość strat
1	2	3	4	5	6	7
	Koparka górnicza przedsiębierna	3	bardzo wysokie	wysokie	średnie	wysoka
	Koparka podsiębierna	2	średnie	średnie	średnie	bardzo niska
	Spycharka	2	średnie	średnie	średnie	niska
	Młot hydrauliczny na podwoziu koparki	1	średnie	średnie	średnie	bardzo niska
	Wozidło technologiczne	13	bardzo wysokie	wysokie	wysokie	wysoka
	Ładowarka kołowa	7	wysokie	wysokie	wysokie	wysoka
	Wiertnica	2	bardzo wysokie	wysokie	niskie	wysoka

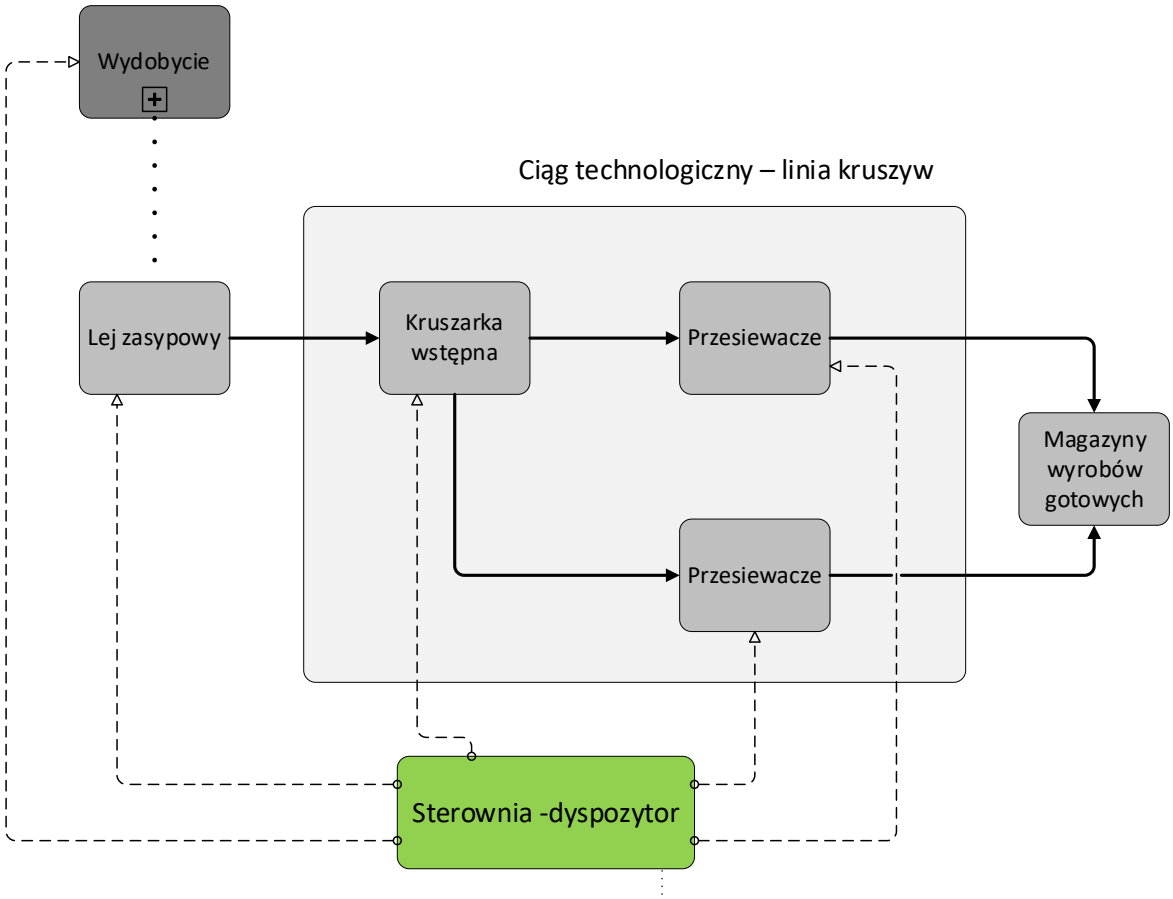
Rys. 47. Mapa obszaru górniczego KWC. Kolorem czerwonym oznaczono zabezpieczone przed dostępem osób nieuprawnionych miejsca postoju maszyn w nocy i w dni wolne od pracy. Źródło: fotografie wykonane dla KWC.

7.6.1 Zakład Kruszyw

Wydobywany surowiec, zgodnie z ze schematem na [Rys. 19] trafia bezpośrednio na linię produkcyjną Zakładu Kruszyw [Rys. 48].



Rys. 48. Schemat procesu produkcyjnego w KWC. Ryzyka kumulują się wzdłuż podprocesów sekwencyjnych. Źródło: badania własne.



Rys. 49. Schemat blokowy procesu technologicznego zakładu kruszyw z uwzględnieniem wzajemnych zależności.

Linie ciągłe na [Rys. 49] odwzorowują przepływ materiału, natomiast linie przerywane oznaczają przepływ informacji i decyzji.

Specyfika pracy ciągu technologicznego, narzuca też w pewien sposób metodykę analizy ryzyk dla maszyn zależnych od siebie w sposób kaskadowy. Awaria lub brak dyspozycyjności (dostępności) np. kruszarki szczękowej (wstępnej) pokazanej na [Rys. 48] wyłączy z produkcji cały ciąg technologiczny. Dlatego też sposób prowadzonej analizy musi być odmienny, niż w przypadku procesów urabiania, załadunku i transportu surowca prezentowanych na [Rys. 45]. Proponowany wzór (7.9) uwzględnia możliwość kumulacji się ryzyk na poszczególnych etapach procesu technologicznego:

$$R=\sum_{i=1}^{N}(P_i * S_i * \prod_j(1 + w_{ij} * T_{ij})) \tag{7.9}$$

gdzie: R to ryzyko całkowite awarii ciągu technologicznego, N to liczba etapów/składników ciągu, P_i prawdopodobieństwo materializacji ryzyka na *i-tym* elemencie, S_i to skutek materializacji, w_{ij} to waga oddziaływania pomiędzy węzłami ij a T_{ij} to tłumienie (lub wzmocnienie) propagacji ryzyka.

Tab. 19. Ryzyka zidentyfikowane dla Zakładu Kruszyw.

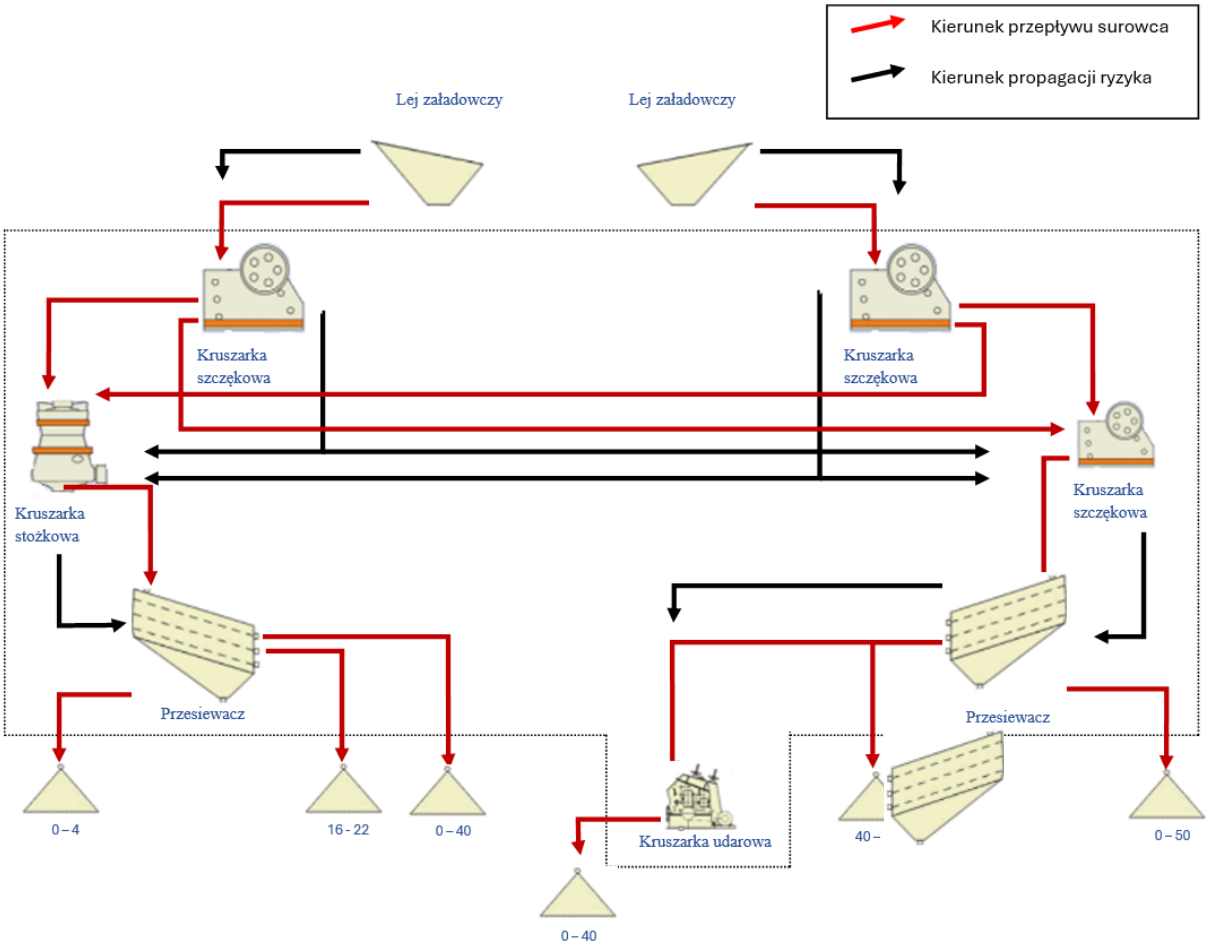
Główne urządzenia	Maksymalna kaskadowa ilość urządzeń	Ryzyka związane ciągiem technologicznym Zakładu Kruszyw	Dotychczasowy sposób zarządzania tym ryzykiem
Kruszarka szczękowa. Kruszarki udarowe. Przesiewacze. Przenośniki taśmowe.	15	1. Przypadkowe uszkodzenie maszyn przez czynniki naturalne na skutek awarii, wypadku bądź działania świadome osób trzecich. 2. Akty wandalizmu. 3. Przypadki kradzieży. 4. Niewłaściwy sposób zarządzania czasem pracy i dostępności maszyny. 5. Brak dostępności systemu informatycznego.	1. Monitoring technologiczny. 2. System ERP. 3. System klasy SCADA. 4. Monitoring sieci komputerowej.
Możliwość kumulacji ryzyk w procesie technologicznym			
Rodzaje zagrożeń			Prawdopodobieństwo wystąpienia
1. Wejście układu – brak dostaw surowca. 2. Awaria mechaniczna. 3. Zdarzenie losowe – wypadek. 4. Brak dostępności elementu ciągu na skutek konieczności postoju.			Niskie Wysokie Średnie Średnie

5. Brak możliwości sterownia. 6. Brak materiałów eksploatacyjnych.	Średnie Niskie

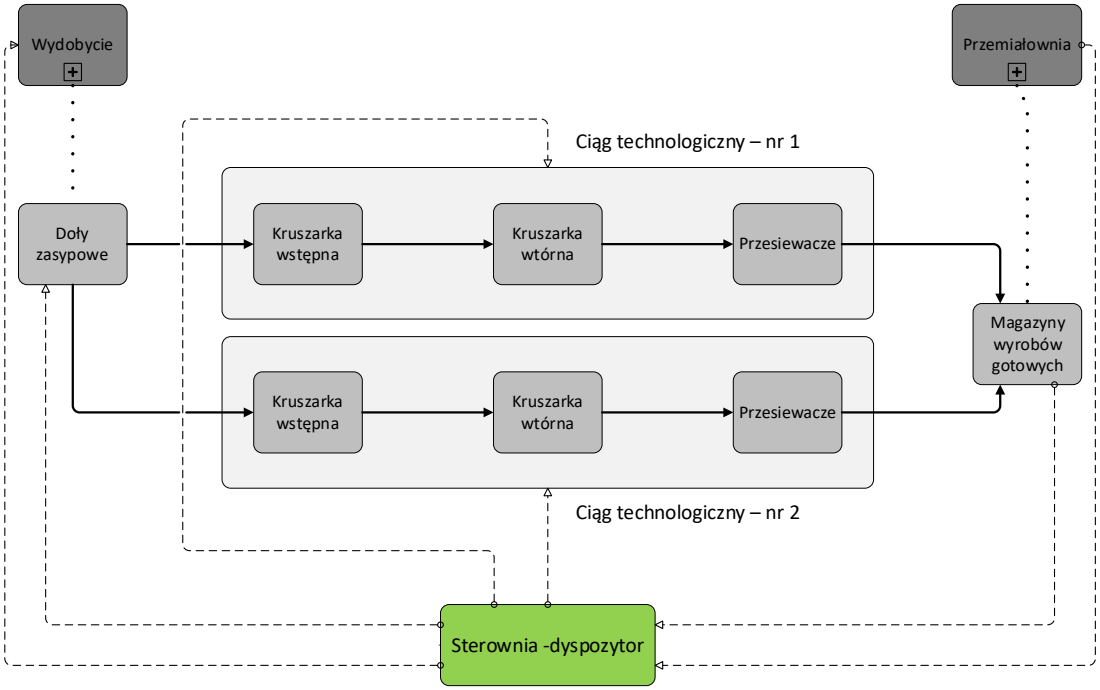
Rys. 50. Umiejscowienie Zakładu Kruszyw. Źródło: KWC.

7.6.2 Zakład Przeróbczy

W przypadku Zakładu Przeróbczego [Rys. 51] można wyróżnić dwa ciągi technologiczne, mogące pracować równocześnie, dostarczając niezależnie od siebie surowiec dla Przemiałowni, z różną wydajnością, zależną od złożoności linii produkcyjnej i granulacji produkowanego asortymentu. Każdy z nich składa się jednak z kaskadowo pracujących maszyn, dlatego sposób analizy prowadzony jest w sposób analogiczny jak w przypadku Zakładu Kruszyw.



Rys. 51. Schemat procesu produkcyjnego w KWC. Ryzyka kumulują się wzdłuż podprocesów sekwencyjnych.



Rys. 52. Schemat blokowy procesu technologicznego zakładu przeróbczego z uwzględnieniem wzajemnych zależności.

Linie ciągłe na [Rys. 52] odwzorowują przepływ materiału, natomiast linie przerywane oznaczają przepływ informacji i decyzji.

W przypadku dwóch równoległych ciągów technologicznych, jak na [Rys. 52], rozpoczynających się od wspólnego węzła początkowego W_0 (doły zasypowe), całkowite ryzyko R można opisać jako sumę ryzyk z obu ciągów, z uwzględnieniem ich współzależności i interakcji (7.10):

$$R=R_{W_0}+\sum_{i=1}^{N_1}(P_{1i} * S_{1i} * \prod_j(1+w_{ij} * T_{ij}))+\sum_{k=1}^{N_2}(P_{2k} * S_{2k} * \prod_l(1+w_{kl} * T_{kl})) \quad (7.10)$$

gdzie: *1* i *2* to dwa ciągi technologiczne, R to ryzyko całkowite awarii ciągów technologicznych, N_1 i N_2 to liczba etapów/składników odpowiedniego ciągu, P_{1i} i P_{1k} prawdopodobieństwo materializacji ryzyka na *i-tym* lub *k-tym* elemencie, S_{1i} i S_{1k} to skutek materializacji, w_{ij} i w_{kl} to waga oddziaływania pomiędzy węzłami *ij* lub *kl* a T_{ij} i T_{kl} to tłumienie (lub wzmocnienie) propagacji ryzyka odpowiedniego ciągu.

Tab. 20. Ryzyka zidentyfikowane dla Zakładu Przeróbczego.

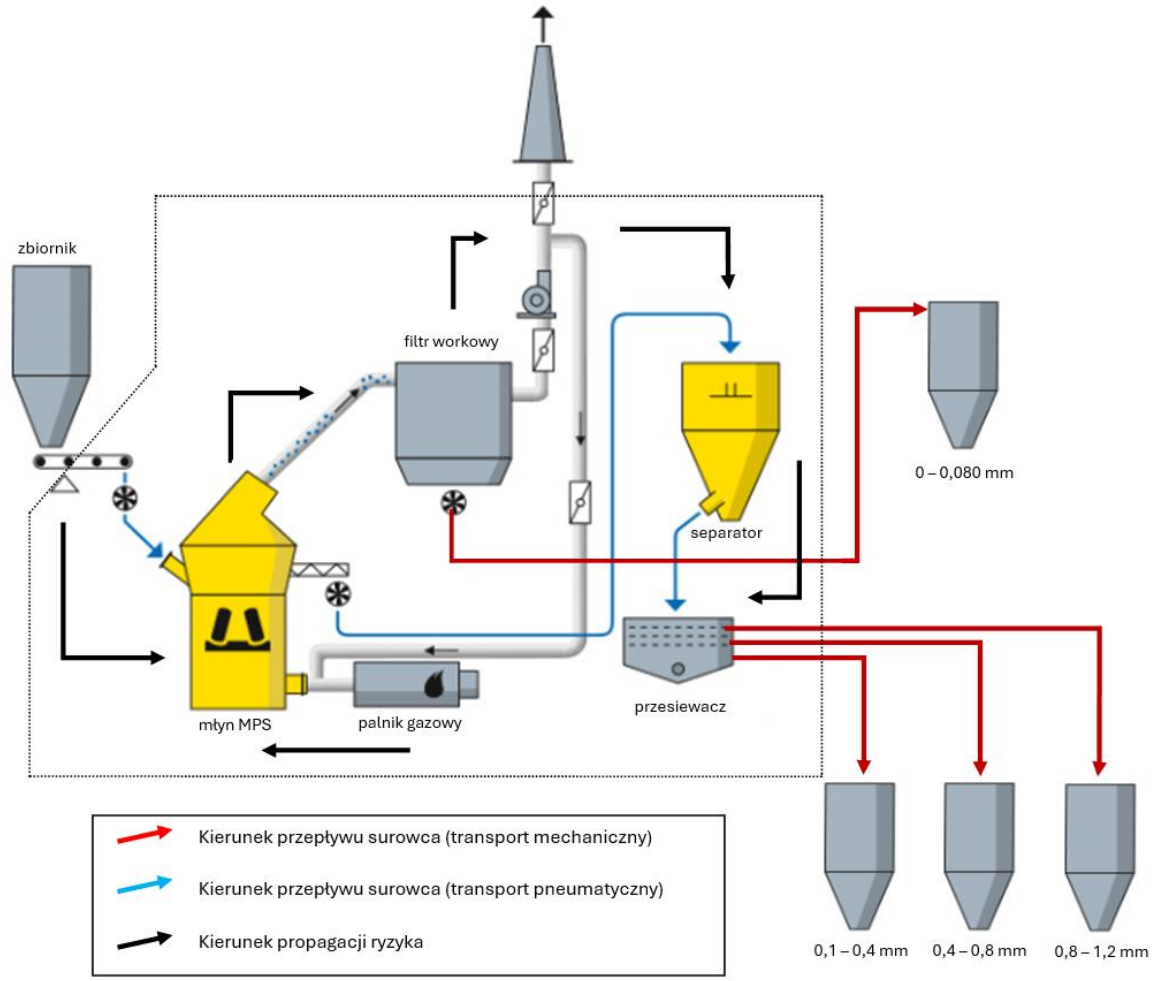
Główne urządzenia	Maksymalna kaskadowa ilość urządzeń	Ryzyka związane ciągiem technologicznym Zakładu Przeróbczego	Dotychczasowy sposób zarządzania tym ryzykiem
Kruszarki szczękowe. Kruszarka stożkowa. Kruszarka udarowa. Przesiewacze. Przenośniki stalowo-członowe. Przenośniki taśmowe.	Ciąg 1 – 27 urządzeń. Ciąg 2 – 25 urządzeń.	1. Przypadkowe uszkodzenie maszyn przez czynniki naturalne na skutek awarii, wypadku bądź działania świadome osób trzecich. 2. Akty wandalizmu. 3. Przypadki kradzieży. 4. Niewłaściwy sposób zarządzania czasem pracy i dostępności maszyny. 5. Brak dostępności systemu informatycznego.	1. Monitoring technologiczny. 2. System ERP. 3. System klasy SCADA. 4. Monitoring sieci komputerowej.
Możliwość kumulacji ryzyk w procesie technologicznym.			Prawdopodobieństwo wystąpienia
1. Wejście układu – brak dostaw surowca. 2. Awaria mechaniczna. 3. Zdarzenie losowe – wypadek. 4. Brak dostępności elementu ciągu na skutek konieczności postoju. 5. Brak możliwości sterownia. 6. Brak materiałów eksploatacyjnych.			Niskie Wysokie Średnie Średnie Średnie Niskie

Rys. 53. Doły zasypowe, początek ciągu technologicznego „Zakład Przeróbczy”.
*Źródł*o: materiały własne KWC.

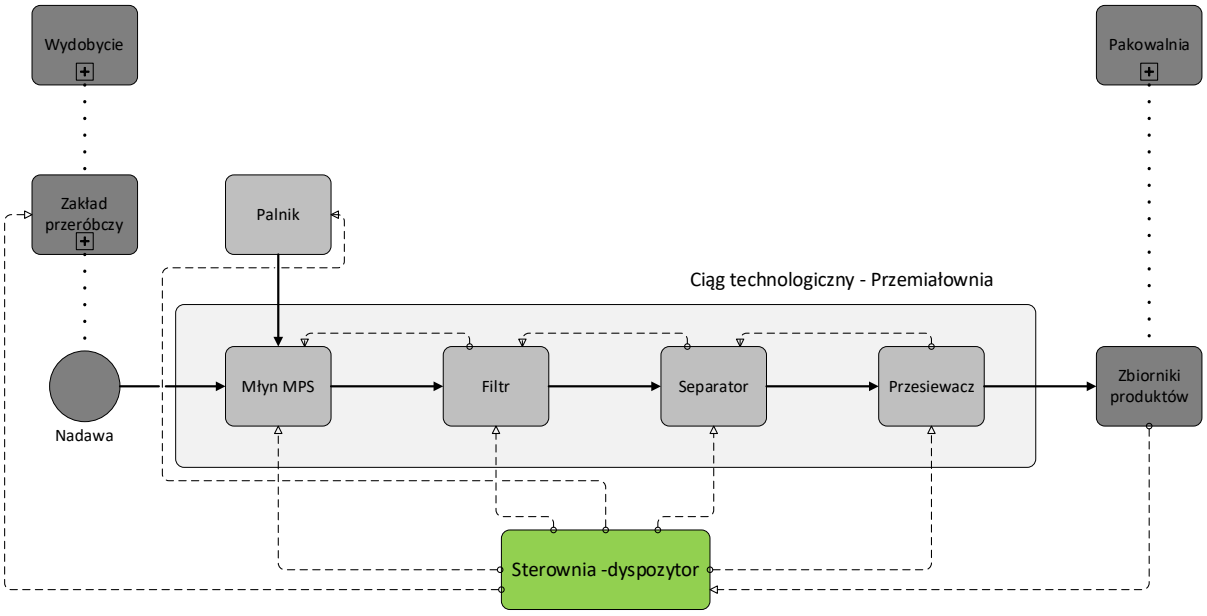
7.6.3 Przemiałownia

Przedstawiona na [Rys. 54] linia technologiczna przemiału kamienia wapiennego składa się z dwóch równolegle pracujących linii technologicznych o wysokim stopniu skomplikowania i zaawansowania technologicznego. W związku z lokalizacją w zamkniętej hali produkcyjnej, linie technologiczne zabezpieczone są przed nieuprawnionym dostępem oraz działaniem czynników atmosferycznych. Główne ryzyka związane z koniecznością utrzymania ciągłości produkcji związane są z koniecznością utrzymania w ruchu ciągłym urządzeń pracujących kaskadowo. Sytuacja taka narzuca konieczność utrzymania ścisłego reżimu okresowych przeglądów i remontów oraz zapewnienia dostępności materiałów eksploatacyjnych i części zamiennych. Procesy te realizowane są przy wsparciu systemu klasy ERP (*Enterprise Resource Planning*). Dodatkowo zabezpieczenie strefy obwodowej obiektu, dzięki wykorzystaniu kamer monitoringu wizyjnego wyposażonego w system analityki obrazu w połączniu z patrolami firmy ochrony, zapewnia minimalizację ryzyk związanych z intruzją.

Podsumowując, bieżący monitoring ryzyk wsparty technologicznie systemem IRM DSS pozwoli w sposób optymalny z biznesowego punktu widzenia zarządzać pracą ciągu technologicznego, przynosząc zakładany zysk dzięki optymalizacji czasu pracy oraz czasu przerw remontowych i przeglądowych.



Rys. 54. Uproszczony schemat procesu produkcyjnego w KWC. Ryzyka kumulują się wzdłuż podprocesów sekwencyjnych.



Rys. 55. Schemat blokowy procesu technologicznego przemiałowni z uwzględnieniem wzajemnych zależności.

Linie ciągłe na [Rys. 55] odwzorowują przepływ materiału, natomiast linie przerywane oznaczają przepływ informacji i decyzji.

Charakterystyka pracy i budowa tej linii produkcyjnej zbliżona jest do Zakładu przeróbczego, w związku z czym ryzyka również można opisać takim samym wzorem, tj.: (7.9).

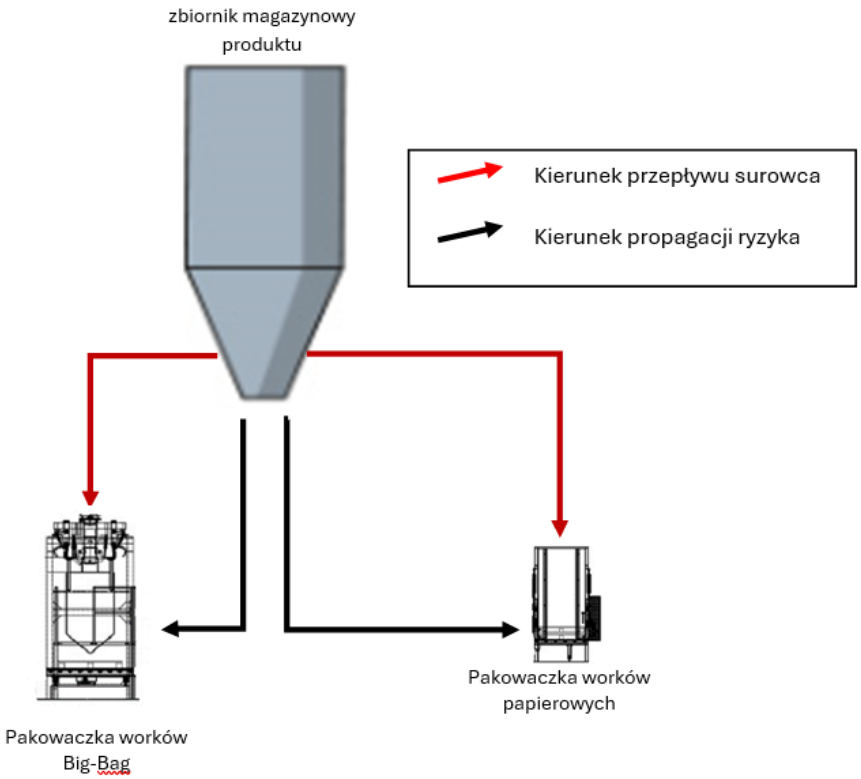
Tab. 21. Ryzyka zidentyfikowane dla Przemiałowni.

Ryzyka związane ciągiem technologicznym Przemiałowni	Dotychczasowy sposób zarządzania tym ryzykiem
1. Przypadkowe uszkodzenie maszyn przez czynniki naturalne na skutek awarii, wypadku bądź działania świadome osób trzecich. 2. Niewłaściwy sposób zarządzania czasem pracy i dostępności maszyny. 3. Brak dostępności systemu informatycznego.	1. Monitoring technologiczny. 2. System ERP. 3. System klasy SCADA. 4. Monitoring sieci komputerowej.

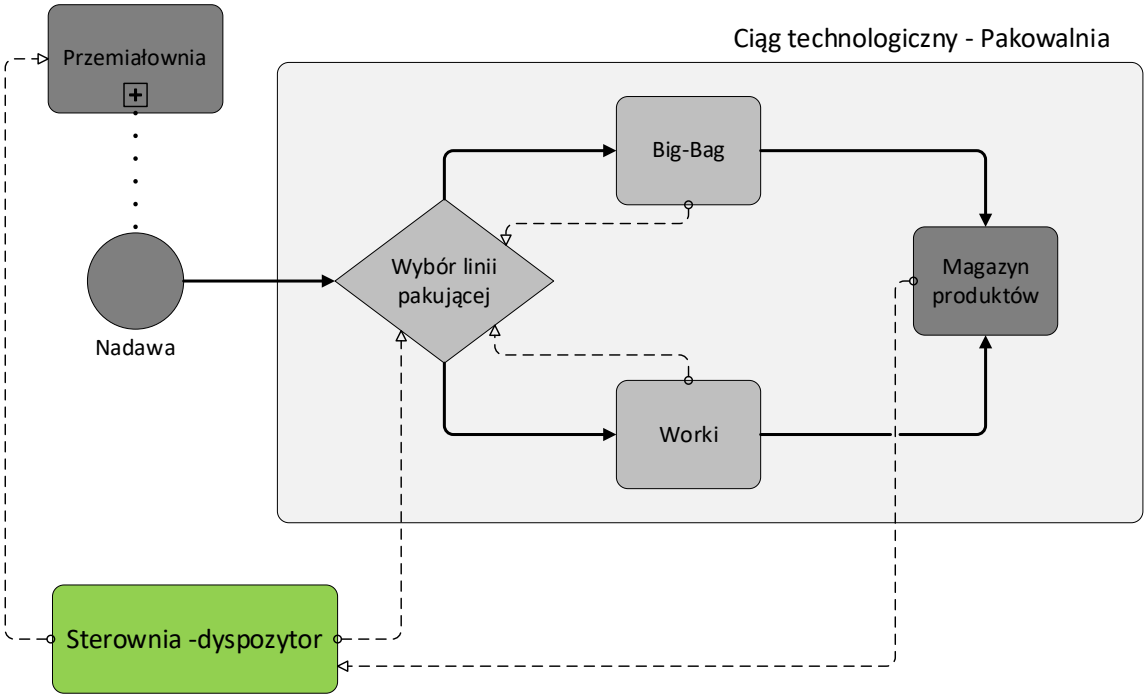
Możliwość kumulacji ryzyk w procesie technologicznym.	Prawdopodobieństwo wystąpienia
1. Awaria mechaniczna.	Niskie
2. Zdarzenie losowe – wypadek.	Średnie
3. Brak dostępności elementu ciągu na skutek konieczności postoju.	Średnie
4. Brak możliwości sterowania.	Średnie
5. Brak materiałów eksploatacyjnych.	Niskie

7.6.4 Pakowalnia

W porównaniu do procesów produkcyjnych przedstawionych w podrozdziałach poprzednich schemat przetwarzania produktu w Pakowalni jest stosunkowo prosty. Głównym obszarem narażonym na zagrożenia jest zbiornik magazynowy produktu [Rys. 56]. Wynika to ze specyfiki konstrukcji całej linii technologicznej, która poza zbiornikiem z zapasem surowca zamknięta jest w hali produkcyjnej, zabezpieczającej ją przed nieuprawnionym dostępem oraz czynnikami atmosferycznymi. Sam zbiornik surowca jest odrębną konstrukcją umiejscowioną w bezpośrednim sąsiedztwie, jednak jego rozmiar sprawia, że może być podatny na działanie czynników atmosferycznych, w tym w szczególności wyładowań atmosferycznych. Ryzyka związane z koniecznością utrzymania działania całej linii, biorąc pod uwagę jej niską krytyczność na funkcjonowanie przedsiębiorstwa, wydają się być zabezpieczone przy użyciu wykorzystywanych obecnie technologii. Jest to głownie system ERP, w którym prowadzona jest gospodarka remontowa, magazynowa i zakupowa.



Rys. 56. Schemat procesu produkcyjnego w KWC. Ryzyka kumulują się wzdłuż podprocesów sekwencyjnych.



Rys. 57. Schemat blokowy procesu technologicznego pakowalni z uwzględnieniem wzajemnych zależności.

Linie ciągłe na [Rys. 57] odwzorowują przepływ materiału, natomiast linie przerywane oznaczają przepływ informacji i decyzji.

Układ wzajemnych relacji linii Pakowalni jest stosunkowo prosty, przy czym maszyny pakujące mogą pracować niezależnie od siebie, a relacja występuje jedynie pomiędzy nimi i węzłem początkowym, z czego wynika, że awaria w tym węźle bezpośrednio wpływa na ryzyko układu, a także na ryzyko maszyn dodatkowych (pakujących). Można to pisać wzorem (7.11):

$$R=R_{G+}\sum_{i=1}^{2}(P_i * S_i * (1 + w_{Gi} * T_{Gi})) \quad (7.11)$$

gdzie: R to ryzyko całkowite awarii ciągu technologicznego, R_G to ryzyko awarii maszyny głównej (węzeł początkowy), P_i prawdopodobieństwo materializacji ryzyka na *i-tym* elemencie, S_i to skutek materializacji, w_{Gi} to waga oddziaływania pomiędzy węzłami maszyną główną a kolejną a T_{Gi} to tłumienie (lub wzmocnienie) propagacji ryzyka.

Wykaz charakterystycznych ryzyk dla obszaru Pakowalni podany jest w tabeli niżej.

Tab. 22. Ryzyka zidentyfikowane dla Pakowalni.

Ryzyka związane ciągiem technologicznym Pakowalni	Dotychczasowy sposób zarządzania tym ryzykiem
1. Przypadkowe uszkodzenie maszyn przez czynniki naturalne na skutek awarii, wypadku bądź działania świadome osób trzecich. 2. Niewłaściwy sposób zarządzania czasem pracy i dostępności maszyny.	1. Monitoring technologiczny. 2. System ERP.
Możliwość kumulacji ryzyk w procesie technologicznym	Prawdopodobieństwo wystąpienia
1. Awaria mechaniczna. 2. Zdarzenie losowe – wypadek. 3. Brak dostępności elementu ciągu na skutek konieczności postoju. 4. Brak materiałów eksploatacyjnych.	Niskie Niskie Niskie Niskie

8 Modelowanie ryzyka dla celów implementacji IRM DSS

8.1 Zastosowanie grafów wiedzy w modelach zarządzania ryzykiem

Grafy wiedzy wraz z prezentacją możliwości, jakie oferują w DSS, omówione zostały w rozdziale 7.1.5, tutaj zaprezentowana zostanie możliwość ich wykorzystania jako narzędzia wspierającego proces zarządzania ryzykiem w systemie klasy IRM DSS.

W celu usystematyzowania informacji przyjmujemy, że w modelu zarządzania zagrożeniami i ryzykiem występują następujące obiekty:

- Wiele zagrożeń, naturalnych lub antropogenicznych, oznaczanych jako $T_1, T_2, \ldots, T_{n1}$.
- Dwa rodzaje węzłów fuzji informacji: 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 $\Phi_1, \ldots, \Phi_{n3}$.
- Zagrożeni ludzie 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. Niektóre z nich mogą być również źródłami zagrożeń lub propagować zagrożenia, które je dotykają; propagacja zagrożeń jest przedstawiona jako podgraf ogólnego multigrafu.
- Hierarchiczna (niższy, średni i najwyższy poziom) struktura jednostek decyzyjnych D, sztuczna autonomiczna lub będąca częścią systemu bezpieczeństwa przedsiębiorstwa opartego na decyzjach człowieka.
- Wewnętrzne zespoły ratownicze, roboty ratownicze, urządzenia wykonawcze (np. gaśnice), które realizują decyzje związane z zarządzaniem kryzysowym. Dla zwięzłości będą one nazywane "jednostkami reagującymi" (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 wspierane przez inne zasoby i środki długofalowe:

- Portfel technologii, które mogą być zastosowane w celu zapobiegania lub ograniczania zagrożeń. Należą do nich technologie oparte na AI, takie jak nowe systemy czujników, przetwarzanie sygnałów, robotyka inspekcyjna, algorytmy wspomagania decyzji.
- Zespoły ratownicze i inne zasoby ludzkie przeszkolone w zakresie nowych technologii, które będą wykorzystywane w przypadku zagrożenia.
- Aktywa finansowe, które mogą być podstawą do długoterminowego planowania ograniczania zagrożeń i zarządzania ryzykiem.

Powyższe obiekty, mierniki i relacje między nimi tworzą ontologię domeny. Można je 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. Aby umożliwić zastosowanie metod ML i analizy ilościowej w zarządzaniu kryzysowym zgodnie z powyższym schematem, należy zastosować następujące zasady:

(1) Źródła informacji $I_1,\ldots, I_n \in I$ zgłaszających to samo zagrożenie T musi sąsiadować z węzłem fuzji informacji φ lub Φ, gdzie I jest zbiorem dostępnych źródeł informacji.

(2) Przepływy informacji są oznakowane współczynnikami wiarygodności informacji [Moyano i in., 2012].

(3) Każda jednostka fuzji informacji powinna być połączona z wystarczającą liczbą źródeł informacji tak aby wychodząca wiarygodność informacji c_r była wyższa od progu α zdefiniowanego wcześniej dla ψ lub Ψ. Ten sam próg może być zdefiniowany dla całej sieci.

(4) Istnieją ścieżki przepływu informacji między każdym źródłem informacji I a węzłem fuzji informacji Ψ oraz między każdą jednostką przetwarzania informacji (w tym fuzji) z jednej strony a węzłem decyzyjnym D lub z bazą wiedzy KB z drugiej.

(5) Każda jednostka reagująca R jest połączona ścieżką przychodzącego polecenia z co najmniej jednego węzła decyzyjnego D. Polecenia, takie jak przydziały zadań lub przydziały cząstkowe, stanowią drugi rodzaj krawędzi.

(6) Jeżeli jednostka reagująca R jest bezpośrednio połączona ścieżką poleceń z kilkoma jednostkami decyzyjnymi $D_1,\ldots,D_k$ na tym samym lub różnych poziomach (tzn. na ścieżce łączącej nie ma innych jednostek decyzyjnych) zakłada się, że zdefiniowane są odpowiednie reguły łączące decyzje $u_1,\ldots,u_k$ przekazywane ze wszystkich jednostek wpływających do R.

(7) Jednostki reagujące połączone są krawędziami wychodzącymi wskazującymi na działania zapobiegawcze lub łagodzące dla zagrożeń T, obiektów zagrożonych Z oraz obiektów propagujących zagrożenia Z_r. Powyższe obiekty określane są jako aktywne. Krawędzie akcji należą do podgrafu poleceń.

(8) Każda jednostka reagująca R charakteryzuje się zdolnością kompensacji $h(R,T,Z,\tau)$, która oznacza względny stopień (w %), w jakim ta jednostka może zmniejszyć wpływ zagrożenia T na aktywny obiekt Z po upływie czasu τ.

(9) Jeżeli aktywny obiekt Z jest bezpośrednio związany z kilkoma jednostkami reagującymi $R_1,\ldots,R_m$ to dla tego samego zagrożenia T (lub ich grupy wspólnie oddziałującej na Z) definiuje się odpowiednie reguły łączące zdolności kompensacji

$h(R_1,T,Z,\tau),\ldots,h(R_m,T,Z,\tau)$ we wspólną zdolność kompensacji $h(R_1,\ldots,R_m,T,Z,\tau)$. Dla stałych $R_1,\ldots,R_m$ ta ostatnia będzie oznaczana jako $h_R(T,Z,\tau)$.

Definicja 8.1. Multigrafy posiadające własności (1)-(9) będziemy nazywać mapami zagrożenia-ryzyka-reakcji (TRRM). ■

Argument T w funkcjach h i h_R będzie pomijany, jeśli zagrożenie jest stałe lub jednoznacznie powiązane z Z; Z będzie pomijane, jeśli h jest wyznaczone dla standardowego obiektu aktywnego Z_0, a wyniki wszystkich akcji reagowania na każdy Z można wyprowadzić z $h(Z_0)$. Powyższa charakterystyka obiektów aktywnych i jednostek reagujących oraz powiązań między nimi pozwala nam sformułować następujące definicję.

Definicja 8.2. TRRM taki, że dla każdego aktywnego obiektu Z i danego τ zdolność łagodzenia $h_R(Z,\tau)=1$ będziemy nazywać *kompletnym*. Jeżeli dla każdego aktywnego obiektu $1\geq h_R(Z,\tau)\geq\beta>0$, to taki TRRM będziemy nazywać *β-kompletnym*. ■

Upływ czasu, który występuje w Definicji 8.2 jest zwykle determinowany jest przez przepisy bezpieczeństwa obowiązujące w chronionej organizacji oraz przez ograniczenia fizyczne. Jeśli jest traktowany jako zmienna, może stać się dodatkowym kryterium optymalizacji. Modele zagrożenie-ryzyko-reakcja, które nie spełniają wszystkich reguł (1)-(9), ale mimo to zawierają kluczowe obiekty, takie jak zagrożenia, osoby reagujące, artefakty lub osoby zagrożone, przepływy informacji, przynajmniej jednego decydenta i być może jeszcze kilka cech TRRM, określa się mianem niepełnych map zagrożeń lub niepełnych TRRM. TRRM można traktować jako instancje grafów wiedzy [De Nicola i in., 2022] poświęconych zarządzaniu zagrożeniami i ryzykiem, patrz także [Steinberg, 2005]. Pojęcie kompletności TRRM odgrywa kluczową rolę w projektowaniu IRM DSS.

Tab. 23. Notacja stosowana dla istotnych obiektów systemu bezpieczeństwa.

Notacja	Opis	Domena modelowania
I_k, **I**	*k*-th źródło, informacji, zbiór informacji	Informacja
J	przepływ informacji	Informacja
φ or Φ	homo- lub heterogeniczne węzły fuzji informacji	Informacja
c_r	wiarygodność źródła informacji	Informacja
α	predefiniowany próg wiarygodności informacji	Informacja
R_j, R	*j*-ty pierwszy ratownik, zespół ratowników	Pierwsza reakcja
ER_i	*i*-tezewnętrzne służby ratownicze	Pierwsza reakcja

Notacja	Opis	Domena modelowania
h, h_R	funkcje łączące zdolności łagodzące	Pierwsza reakcja
β	Łagodzenie progu zdolności	Pierwsza reakcja
D_k, D	k-ta jedostka decyzyjna, system decyzyjny	Pierwsza reakcja
τ	predefiniowany okres działań ratowniczych	Pierwsza reakcja
M_i, V_j, B_k	zagrożone artefakty: maszyny (M_i), pojazdy (V_j), budynki (B_k),	Podmioty chronione
Z_k	(ogólnie) zagrożony obiekt	Podmioty chronione
Z_{pk}	obiekt rozprzestrzeniający zagrożenie ogólne	Podmioty chronione
T_i	i-te zagrożenie	Zagrożenia i ryzyka
Θ	mapa zagrozenie-ryzyko-reakcja (TRRM)	Model ogólny

8.2 Problem projektowania TRRM i jego rozwiązanie

TRRM można traktować jako instancje grafów wiedzy [De Nicola i in., 2022] poświęconych zarządzaniu zagrożeniami i ryzykiem, patrz także [Steinberg, 2005]. Zaprezentowany na [Rys. 61] multigraf 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. Należy zauważyć, że graficzna reprezentacja ryzyka i zagrożeń zawarta w TRRM dostarcza bezpośrednich wskazówek dotyczących optymalizacji wymagań związanych ze strukturą DSS. 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]. Aby system zachował wymaganą stabilność, w razie materializacji ryzyk, jego odporność i zdolność powrotu do stanu uznawanego za normalny stan pracy musi być na odpowiednim poziomie, uwzględniając każdą ze wspomnianych warstw.

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 8.1. Biorąc pod uwagę TRRM Θ, być może niekompletny, minimalny dopuszczalny próg wiarygodności informacji $\alpha>0$, stałe τ, zbiór $Q=\{q_1,\ldots,q_p\}$ obiektów, które można dodać do Θ jako jego węzły, potencjalne nowe połączenia $E=\{e_1,\ldots,e_r\}$ 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. ■

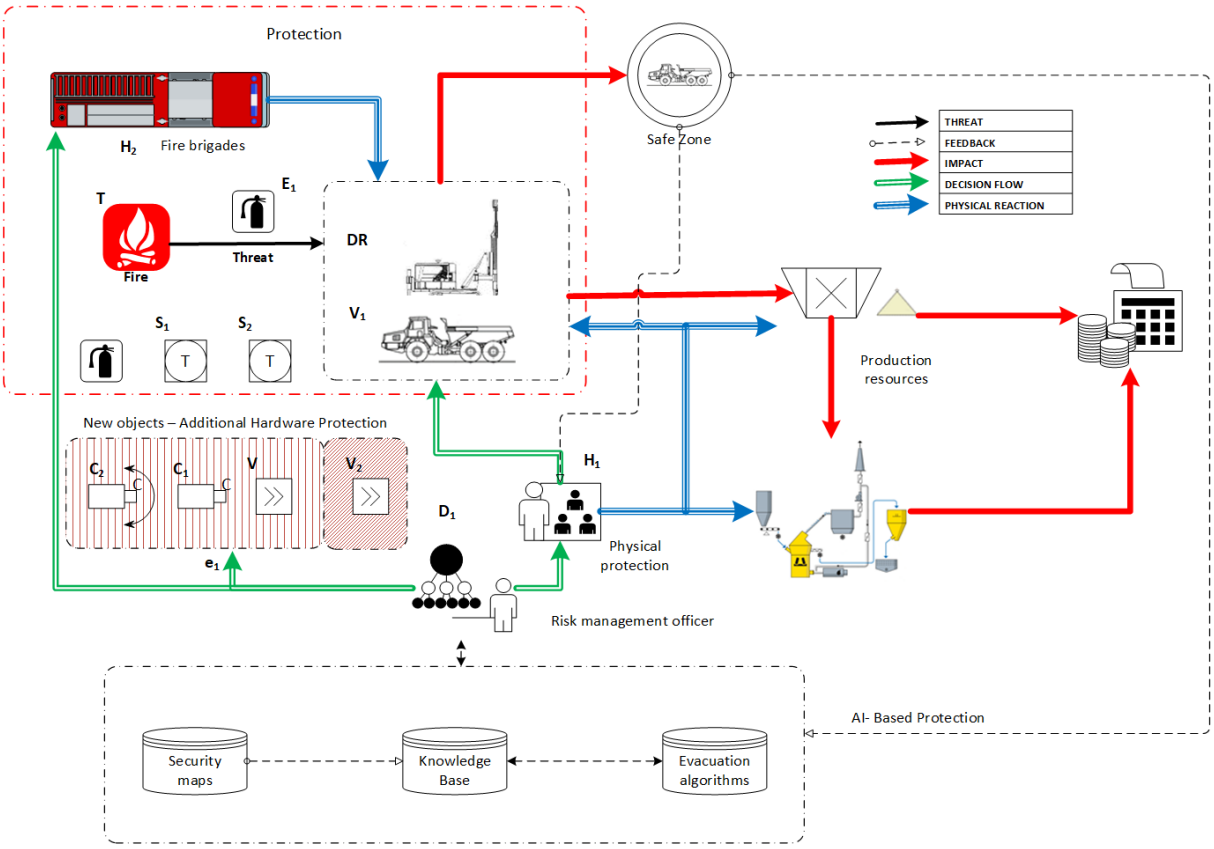
Problem 8.1 jest zadaniem optymalizacji kombinatorycznej, gdzie podzbiory Q i E są rozwiązaniami tentatywnymi, które mogą być poprawiane za pomocą heurystyk, takich jak algorytmy genetyczne [Katoch i in., 2021] lub symulowanego wyżarzania [Niyomubueyi i in., 2020]. Metodyka postępowania z wykorzystaniem algorytmu NSGA II opisana została w [rozdziale 8.3.1], 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. 58 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 wiarygodności α.



Rys. 58. Mapa zagrożenie-ryzyko-reakcja, która odpowiada sytuacji przedstawionej w przykładzie 1.

Algorytm 8.1 (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 $h(R_1,\ldots,R_m,T,Z,\tau)$
8. $\beta:=\min(\beta,h(R_1,\ldots,R_m,T,Z,\tau))$
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 8.2 (heurystyczne rozwiązanie Problemu 8.1)

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** $\alpha, \beta, cost, Y, \Xi$
17. **end** ■

Więcej kryteriów i wymagań można analizować jako rozszerzenie Problemu 8.1, na przykład: problem zapewnienia ograniczenia zagrożeń przy minimalnym wykorzystaniu zasobów, w tym jednostek reagujących przydzielanych dynamicznie w razie zagrożenia. Inny wariant Problemu 8,1 pojawia się w sytuacji, gdy niektóre obiekty aktualnej infrastruktury mogą być relokowane do ochrony przed nowymi zagrożeniami. Poniżej omówiony zostanie przykład rozwiązania Problemu 8.1.

Przykład 8.1. Załóżmy, że instalacja przemysłowa modelowana przez TRRM przedstawiona na [Rys. 58] jest zagrożona pożarem T, który może wystąpić podczas tankowania wiertnicy (DR). T może stanowić bezpośrednie zagrożenie dla DR oraz pojazdu technologicznego V_1, obu wycenianych v=2000 jednostek pieniężnych (MU). Pożar spowoduje uruchomienie ogólnej procedury awaryjnej dla zdarzeń nietypowych. W skład istniejącej warstwy ochrony technicznej tego TRRM wchodzi automatyczna gaśnica (E_1) o zdolności łagodzenia h_1=0,5, która ogranicza straty w układzie hydraulicznym DR i trakcyjnym V_1 do $c_1=v(1-h_1)$=1000 MU. Jako pierwszy reagujący na miejsce zdarzenia zostanie wezwana zakładowa straż pożarna H_1 ze zdolnością łagodzącą h_2 dla T równego 0,6. Procedura weryfikacyjna (Alg. 9.1) wskazuje, że stopień zagrożenia pożarowego, oceniany przez H_1, ogranicza wspólną zdolność łagodzenia skutków pożaru przez E_1 i H_1 do poziomu $h(E_1,H_1,T,DR,V_1,\tau)$=0,7 < $h_1+h_2(1-h_1)$=0,8, czyli E_1

i H_1 nie mogą łagodzić skutków pożaru niezależnie. Ponieważ poziom ten jest niezadowalający, konieczne będzie wezwanie wsparcia ze strony zewnętrznej jednostki służb utrzymania ruchu H_2, która wraz z H_1 opanuje pożar w czasie τ przy wspólnej zdolności łagodzenia $h_3=h(E_1,H_1,H_2,T,DR,V_1,\tau)$=0,8. Koszt ratunku zewnętrznego z H_2 wynosi c_4=100. Straty poniesione przez pożar po wyłącznej interwencji H_1 wyniosłyby c_2=600<c_1, przy czym ucierpiałaby również V_1. Dodatkowa działalność ratownicza H_2 ograniczy straty do $c_3=v(1-h_3)$=400, ponieważ uszkodzeniu może ulec tylko *DR*. Całkowite koszty związane ze zdarzeniem wyniosą c_3+c_4=500<c_2.

W drugim scenariuszu, na podstawie danych wyjściowych z Algorytmu 8.1, koordynator bezpieczeństwa D_1 odpowiedzialny za walkę z pożarami stwierdza, że zagrożenie pożarowe podczas tankowania jest niewystarczająco pokryte przez istniejące czujniki temperatury S_1 i czujniki wizualne S_2, które dostarczają wspólnej informacji wiarygodności α_0<1. W związku z tym D_1 przypisuje nowe obiekty i połączenia do istniejącego TRRM Θ, aby uzupełnić go zgodnie z Alg. 8.2 przed jakimkolwiek zdarzeniem. Nowe obiekty uwzględnione jako elementy *Q* to kamera C_1 obejmująca miejsce zdarzenia, kamera *PTZ* (pan-tilt-zoom) C_2 przekierowana na obserwację zdarzenia, o kosztach odpowiednio c_5=50 i c_6=100 *MU*. Wszystkie czujniki zapewniają obecnie doskonały monitoring ryzyka przy α_1=1. Ulepszony monitoring zwiększa zdolność łagodzenia skutków zdarzenia przez H_1 do h_4=0,7, a wspólną zdolność łagodzenia skutków zdarzenia przez E_1 i H_1 do h_5=0,85, co sprawia, że wzywanie pomocy z zewnątrz staje się zbędne. Dodatkowo, kosztem c_7=50 ustanowione jest łącze komunikacyjne $e_1 \in E_1$ z autonomicznym robotem remontowym V_2, dzięki czemu V_2 może być przemieszczany z innej lokalizacji w celu wsparcia bieżących działań łagodzących. Konkretnie, V_2 będzie obsługiwał mobilny zestaw gaśniczy *V* o koszcie c_8=270 i zdolności łagodzącej h_6=0,8 przy wspieraniu zespołu ludzkiego. Koszt eksploatacji V_2, z uwzględnieniem spodziewanego kosztu ponownej naprawy w przypadku uderzenia niewielkim uszkodzeniem, wynosi c_9=50. Po uwzględnieniu C_1, C_2, *V*, e_1, H_1 i V_2 w Θ, zdolność do zniwelowania zagrożenia *T* przez wszystkie elementy pierwszego reagowania w określonym czasie szacowana jest na poziomie

$$\beta := hR(T,DR,V_1,\tau)=1-(1-h_6)(1-h_5)=97\%. \quad (8.1)$$

Przy powyższych założeniach, charakterystyce sprzętu i reakcji, łączna wartość strat poniesionych przez pożar i koszt utworzenia z Alg. 2 a β-kompletnej struktury Θ' pokazanej na [Rys. 58]z początkowego TRRM wynosi:

$$c(\Theta',T)= v(1-\beta) +(c_5+ c_6)/f_c + c_7/f_e +c_8/f_k+c_9, \quad (8.2)$$

gdzie f_c=2, f_e=2 i f_k=3 to spodziewane częstości występowania pożaru w okresie eksploatacji odpowiednio kamer, łącza komunikacyjnego i zestawu gaśniczego. Otrzymana wartość

$c(\Theta',T)$=300 *MU* jest znacznie lepsza od całkowitego kosztu związanego ze zdarzeniem w poprzednim scenariuszu (500 *MU*). ■

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.

8.2.1 Problem zarządzania ryzykiem przemysłowym i badania pokrewne

W omawianych dotychczas zagadnieniach zapewnienia bezpieczeństwa przemysłowego, ryzyko jest przypisane do zagrożeń zewnętrznych, do procedur przetwarzania informacji, które mogą zniekształcać dane z błędami, do ludzkich błędów operacyjnych oraz do systematycznych błędnych decyzji, które mogą być podejmowane podczas zarządzania ryzykiem. Ponadto pomiary czujników (sensorów) mogą być zafałszowane ze względu na ich niedokładność. Ogólny transfer zagrożeń można modelować jako sieć, w której utrata informacji oraz przypadkowe błędy operacyjne i decyzyjne są źródłami dodatkowego ryzyka. Sieć ta jest uzupełniona przez model zarządzania ryzykiem i optymalizacji obejmujący algorytmy decyzyjne, działania i aktuatory do ich realizacji. Oba składniki modelu są sprzężone przez informacje zwrotne, otrzymywane przez czujniki, porównywane z wartościami dostarczanymi przez model i prezentowane modułowi ML oraz decydentom. Silnik DSS sekwencyjnie wykorzystuje powyższe komponenty modelu i łączy je z procedurą częściowo nadzorowanego uczenia maszynowego [van Engelen, Hoos, 2020]. Oceny poprzednich (archiwalnych) sytuacji kryzysowych służą do wprowadzania etykiet bieżących nieznakowanych danych z czujników, charakterystyk zagrożeń, parametrów procedur ograniczania ryzyka oraz decyzji menedżerskich.

Złożone procesy produkcyjne często związane są z określonymi zagrożeniami spowodowanymi potencjalnym wystąpieniem zjawisk naturalnych, takich jak powódź czy osuwiska, awarii przemysłowych lub zagrożeń antropogenicznych, takich jak włamanie czy akt sabotażu. Zagrożenia te mogą występować jednocześnie w wielu miejscach rozmieszczonych na dużym obszarze. Analiza ryzyka przemysłowego określa ilościowo potencjalne skutki zagrożeń, rozróżnia zależności między nimi i rekomenduje optymalne procedury lub środki zapobiegania i ograniczania ryzyka. Dostępność informacji przechowywanych i przetwarzanych w innych systemach informacyjnych przedsiębiorstwa (EIS) [Hevner i in., 2004] zwiększa efektywność systemu IRM. Na przykład zarządzanie zapasami w systemie planowania zasobów przedsiębiorstwa (ERP) dostarcza wskazówek, gdzie przechowywane są niebezpieczne substancje lub drogie urządzenia narażone na określone ryzyko. Systemy wspomagające utrzymanie ruchu przetwarzają informacje

z czujników połączonych z przemysłowym internetem rzeczy (IoT) [Porte i in., 2020], a moduły predykcyjnego utrzymania ruchu wskazują miejsca narażone na zagrożenia i ich zwiększoną ekspozycję na ryzyko. Dlatego systemy IRM powinny być interoperacyjne i uwzględniać strumienie danych z heterogenicznych procesów zarządzania kryzysowego.

Dostawcy systemów informacyjnych stosunkowo wcześnie zauważyli istotność i potencjał IRM [Rönnbäck, Holmström, 2008]. Podczas gdy AI jest szeroko stosowana w systemach zarządzania ryzykiem finansowym, jej zastosowanie w systemach zarządzania kryzysami naturalnymi i antropogenicznymi było do niedawna rzadkie [Domdouzis, 2018; Skulimowski, Bañuls, 2021]. Projektując IRM DSS, wzięto pod uwagę obecny rozwój systemów zarządzania kryzysowego z funkcjami wspomagania decyzji. Wyłoniły się one z systemów wczesnego ostrzegania, które ewoluowały w kierunku opartego na chmurze heterogenicznego przetwarzania sygnałów [Middleton i in., 2014]. Następnie zaproponowano różne architektury zarządzania kryzysowego i DSS [Domdouzis, 2018]. Różnorodność zagrożeń, w połączeniu z możliwymi do zastosowania środkami zapobiegania i łagodzenia, wykazała wzrost znaczenia ontologii dziedzinowych [Bayar i in., 2014] i jakości informacji [Seppanen, Virrantaus, 2015]. Najważniejszym zagadnieniem z punktu widzenia rozwiązywania problemów *„resilience”* w kopalni odkrywkowej okazała się ewakuacja pracowników i sprzętu [Domdouzis, 2018]. Wśród modeli analitycznych stosowanych do modelowania ryzyka w systemach informacyjnych znajdują się dynamika systemów [Garbolino i in., 209] i sieci Petriego [Vernez i in., 2004].

Problematyka zarządzania ryzykiem w projektach inżynieryjnych jest tematem bardzo istotnym, a efektywne zarządzanie ryzkiem jest kluczowe w wielu branżach o dużym potencjale wzrostu. Zagadnienie wzrastającej złożoności projektów w branży budowlanej poruszone zostało przez [Krechowicz, 2017], która wskazuje właśnie na złożoność projektów jako jeden z głównych czynników powodujących trudności w tworzeniu planów zapobiegania zagrożeniom dla całego przedsięwzięcia. Proces zarządzania ryzykiem w złożonych projektach podzielony został na kolejne etapy, które dzięki zaproponowanej przez autorów metodzie jakościowej i ilościowej oceny ryzyka prowadzą do opracowania strategii reagowania na zagrożenia. Cytowana praca wskazuje ryzyka dla krytycznych obszarów projektów budowlanych, gdzie potencjalne niespodziewane zdarzenia mogą szczególnie mocno wpłynąć na ciągłość prac i na efekt końcowy całego projektu.

8.3 Ewakuacja maszyn i zespołów roboczych w KWC – wprowadzenie do problemu

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. Instancje DSS dedykowane dla konkretnych zakładów przemysłowych są budowane z wykorzystaniem ontologii domenowej zarządzania zagrożeniami oraz języka wizualizacji zgodnego z założeniami ontologii. 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, takich jak wskazane, szybka i skuteczna ewakuacja może decydować o minimalizowaniu strat ludzkich i materialnych. Wszelkie opóźnienia czy nieprawidłowości, np. w zakresie poprawności podejmowanych decyzji, przepływu decyzji lub nawet ich braku, mogą doprowadzić do poważnych w skutkach konsekwencji związanych z bezpieczeństwem ludzi i sprzętu [Tab. 24].

Tab. 24. Potencjalny wpływ zagrożeń na ewakuowane jednostki.

Potencjalne wpływ na: / Przyczyna ewakuacji	Zagrożenie zdrowia i życia	Straty materialne (szacowana wartość strat)
Osuwiska skalne	krytyczne	krytyczne
Zalania	duże	krytyczne
Pożar	duże	duże

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.

Przykładowe zagrożenia:

- osuwiska skalne: mogą nagle zasypać pracowników, szczególnie tych pracujących na niższych poziomach odkrywki. Ewakuacja pozwala uniknąć zasypania i poważnych obrażeń.
- zalania: woda może szybko wypełnić wyrobisko, uniemożliwiając ucieczkę. Pracownicy muszą być ewakuowani natychmiast, aby uniknąć uwięzienia lub utonięcia.
- pożary: ogień, dym oraz toksyczne gazy mogą szybko rozprzestrzeniać się w otwartym terenie, zagrażając pracownikom. Ewakuacja jest konieczna, aby ograniczyć ekspozycję na dym i toksyny.

2. Szybkość rozwoju zagrożeń wynikająca ze specyfiki prowadzonej działalności, np.:
   - osuwiska i osiadanie gruntu: niestabilność gruntu i potencjalne osuwiska mogą wystąpić bez ostrzeżenia, a wtedy czas reakcji musi być krótki, a ewakuacja natychmiastowa, aby uniknąć ofiar.
   - zalania: nagłe ulewy będące konsekwencją postępujących zmian klimatycznych mogą doprowadzić do szybkiego zatopienia dolnych partii wyrobisk, co zagraża życiu osób pracujących na niższych poziomach.
   - pożary: pożary mogą szybko objąć duże obszary, a gwałtowny rozwój pożaru sprawia, że konieczna jest natychmiastowa reakcja.
3. Skomplikowany teren i duża skala z jaką mamy do czynienia w przypadku zakładu górniczego, złożona topografia wymuszają:
   - dokładną znajomość dróg ewakuacyjnych oraz planowania z wyprzedzeniem, ponieważ niektóre drogi mogą być zablokowane przez osuwiska, wodę lub ogień.
   - skoordynowane działania w celu sprawnego ewakuowania dużej liczby osób bez wywołania chaosu, który może zwiększyć zagrożenie.
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.

Ewakuacja w odkrywkowych zakładach górniczych jest elementem kluczowym w pierwszej fazie reagowania na zagrożenie, głównie ze względu na dynamikę rozwoju zdarzeń i opiera się w szczególności na:

- ochronie zdrowia i życia pracowników,
- szybkiej reakcji na dynamicznie rozwijające się zagrożenia,
- znajomości terenu i infrastruktury zakładu,
- dobrej organizacji wspartej dedykowanymi systemami klasy IRM DSS.

Analiza przebiegu ewakuacji w sytuacji materializacji zagrożeń występujących w obszarze prowadzenia prac górniczych omówiona zostanie w oparciu o przedstawiony na [Rys. 59] przykład.

Rys. 59. Przykład zastosowania fuzji informacji o zagrożeniach i algorytmów decyzyjnych systemu IRM DSS proponowanego do implementacji i wykorzystania w KWC. Źródło: fotografia podkładowa: KWC.

Na rysunku zaznaczono kluczowe z punktu widzenie przebiegu ewakuacji elementy oraz początkową lokalizacją maszyn, które należy ewakuować z miejsc zagrożonych do miejsc bezpiecznych. Linie ciągłe oznaczają optymalne drogi ewakuacji sprzętu do obszarów zidentyfikowanych jako bezpieczne (obramowanych czerwonymi liniami), a linie przerywane - alternatywne drogi ewakuacji, spośród których system rekomendować będzie drogę kompromisową zależną od wyniku analizy wielokryterialnej dodatkowych informacji o preferencjach decydentów KWC odpowiedzialnych za zapewnienie bezpieczeństwa OG.

8.3.1 Wykorzystanie algorytmu NSGA-II do wyznaczania niezdominowanych strategii zarzadzania ewakuacją w sytuacji kryzysowej

Algorytm NSGA-II (Non-dominated Sorting Genetic Algorithm II) to jeden z najbardziej popularnych algorytmów genetycznych stosowanych do optymalizacji wielokryterialnej. Jego celem jest znalezienie rozwiązań kompromisowych (tzw. rozwiązań Pareto-optymalnych), które równoważą różne kryteria jednocześnie, bez wyraźnej przewagi jednego nad drugim [Niyomubyeyi i in., 2020]. Algorytm działania NSGA-II opiera się o kolejne kroki:

Algorytm 8.3

1. Inicjalizacja, czyli stworzenie początkowej populacji losowych rozwiązań oraz ocena ich jakości na podstawie funkcji celu (kryteriów).
2. Sortowanie i selekcja, w trakcie których populacja jest sortowana na podstawie relacji dominacji Pareto.
3. Krzyżowanie i mutacja, w tym kroku wybrane rozwiązania są krzyżowane i mutowane, aby stworzyć nową populację, proces ten ma na celu wprowadzenie różnorodności i eksplorację przestrzeni rozwiązań.
4. Ocena nowej populacji, nowa populacja jest oceniana, a rozwiązania nie-dominujące są zachowywane.
5. Powtórzenie procesu sortowania, krzyżowania i mutacji aż do osiągnięcia określonego, zadanego kryterium zatrzymującego ten proces (np. maksymalna liczba pokoleń).
6. Zachowanie rozwiązań Pareto-optymalnych, po zakończeniu algorytmu najlepsze rozwiązania są zachowywane i tworzą tzw. zbiór (front) Pareto, który zawiera rozwiązania kompromisowe. Zbiór Pareto przedstawia zestaw takich rozwiązań, gdzie nie można poprawić jednej miary (kryterium), nie pogarszając innej. W kontekście decyzji optymalizacyjnych, mówimy o rozwiązaniach nie zdominowanych.

Aby omówić możliwość zastosowania algorytmu NSGA-II do problemu ewakuacji w sytuacji kryzysowej, naświetlić należy kontekst problemu. W przypadku sytuacji kryzysowych, takich jak pożar, osuwisko skalne czy zalanie w odkrywkowym zakładzie górniczym, szybka i bezpieczna ewakuacja ludzi i sprzętu staje się kluczowa. Problem ten można modelować jako wielokryterialny problem optymalizacji, w którym różne aspekty muszą być brane pod uwagę jednocześnie. Należą do nich:

- minimalizacja czasu ewakuacji (aby jak najszybciej ewakuować ludzi z zagrożonego obszaru),
- maksymalizacja bezpieczeństwa (wybieranie tras ewakuacyjnych minimalizujących ryzyko dodatkowych zagrożeń, np. kolizji, osuwisk),

- minimalizacja strat (priorytetowe ewakuowanie osób i sprzętu znajdujących się najbliżej zagrożenia).

Biorąc pod uwagę tak sformułowane kryteria, kolejne kroki (wskazane powyżej) zastosowania algorytmu NSGA-II przedstawiają się następująco :

Algorytm 8.4

1. Krok 1: utworzenie początkowej populacji rozwiązań
   - Populacja w tym przypadku reprezentuje różne możliwe plany ewakuacji, gdzie każdy plan to zestaw tras ewakuacyjnych dla poszczególnych jednostek.
   - Każdy plan ma przypisane wartości kryteriów, takich jak czas ewakuacji, poziom bezpieczeństwa trasy (uwzględniając ryzyko dodatkowego zagrożenia) oraz liczba ewakuowanych jednostek.
2. Krok 2: definicja funkcji celu (zgodnie z zadanymi kryteriami)
   - Czas ewakuacji: funkcja celu minimalizuje czas, w jakim możliwe jest wyprowadzenie wszystkich jednostek z zagrożonego terenu.
   - Bezpieczeństwo: funkcja celu maksymalizuje bezpieczeństwo trasy, na podstawie danych dotyczących zidentyfikowanych ryzyka.
   - Wielkość strat: minimalizowanie strat, z priorytetowym ewakuowaniem osób i sprzętu znajdujących się w bezpośrednim sąsiedztwie zagrożenia.
3. Krok 3: krzyżowanie i mutacja
   - Krzyżowanie polega na wymianie fragmentów planów ewakuacyjnych pomiędzy różnymi rozwiązaniami, aby stworzyć nowe trasy ewakuacyjne.
   - Mutacja w tym przypadku wprowadza niewielkie zmiany w planach, np. zmieniając trasę jednej jednostki, co pozwala eksplorować nowe rozwiązania.
4. Krok 4: dominacja Pareto
   - Algorytm NSGA-II sortuje wygenerowane rozwiązania na podstawie kryteriów czasu, bezpieczeństwa i wielkości strat.
   - Rozwiązania dominujące trafiają do pierwszego zbioru Pareto (zbiór rozwiązań kompromisowych), a pozostałe są przypisywane do dalszych zbiorów.
5. Krok 5: wybór najlepszych rozwiązań
   - Algorytm wybiera zestawy tras ewakuacyjnych, które znajdują się w pierwszym zbiorze Pareto (najlepsze kompromisy między czasem, bezpieczeństwem i wielkością strat).
6. Krok 6: ewaluacja wyników

- Wynik algorytmu to zestaw rozwiązań Pareto-optymalnych. Każde z nich jest potencjalnym planem ewakuacji, który uwzględnia czas ewakuacji, bezpieczeństwo i wielkość strat.
- Decydenci mogą wybrać najbardziej odpowiedni plan w zależności od priorytetów w danej sytuacji kryzysowej. ■

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, z których każdy może być dostosowany do specyficznych warunków kryzysowych, a ostateczna decyzja co do wyboru planu pozostaje w gestii decydenta.

8.4 Optymalne zarządzanie ryzykiem przemysłowym

Informacje o metodach AI dostępnych do wdrożenia w IRM DSS pochodzą z badań AI-foresight, jak również z analizy rynku oprogramowania i badań z zakresu AI stosowanej. W omawianym przykładzie architektura DSS wykorzystuje również informacje zwrotne z operacji DSS i procedury ML w ramach schematu DevOps. Węzły decyzyjne, decyzje przekazywane jednostkom niższego szczebla, poszczególnym jednostkom reagującym, zespołom ratowniczym i aktuatorom oraz informacje zwrotne o ich konsekwencjach zostały przedstawione w poprzednim podrozdziale jako komponenty modelu zarządzania zagrożeniami. Biorąc pod uwagę przepływ informacji J, który wywołał alarm w chwili t, wielokryterialny problem decyzyjny do rozwiązania i wdrożenia można sformułować podobnie jak w Rozdz. 5 jako:

$$[F:=(F_1,\ldots,F_N):\ U(J,t)\rightarrow \mathbb{R}^N]\rightarrow \min, \tag{8.3}$$

gdzie $F_1,\ldots,F_N$ to ilościowe kryteria efektywności, zarówno techniczne, jak i ekonomiczne, $U(J,t)$ to zbiór decyzji dopuszczalnych po otrzymaniu alertu $J(t)$. Zazwyczaj decyzje są ciągami zaleceń i poleceń wydawanych przez Risk managera jednostkom reagującym $R_1,\ldots,R_m$, z uwzględnieniem ich zdolności łagodzących $h(R_i,Z_j,\tau)$, oraz relacji między stopniami łagodzenia zagrożeń w zagrożonych obiektach a oczekiwanymi wartościami ogólnych kryteriów skuteczności działania F. Dodatkowe preferencje potrzebne do wyboru kompromisowego planu działania spośród niezdominowanych rozwiązań (2) są przewidziane jako następujące zbiory wartości referencyjnych [Skulimowski, 2011]:

A_1 – wartości kryteriów, które odpowiadają pożądanym wynikom działań ograniczających zagrożenie; zwykle nie można ich osiągnąć, ale można się do nich zbliżyć, stosując miarę odległości w przestrzeni kryteriów,

A_2 – wartości kryteriów, które są akceptowalne, ale powinny być poprawione, gdy tylko jest to możliwe; mogą być one ustalone jako wymagania w instrukcjach ogólnych, normach i zasadach zarządzania ryzykiem oraz w polityce bezpieczeństwa,

A_3 – wyniki poprzednich działań związanych z zarządzaniem zagrożeniami, które są uznawane za niepowodzenie.

Zamiast odwoływać się do syntetycznych kryteriów *F*, wartości referencyjne *A1, A2* i *A3* mogą być zdefiniowane dla pewnych mierzalnych kryteriów wstępnych, takich jak stopień uszkodzenia części instalacji produkcyjnych lub przewidywany czas zapewnienia bezpieczeństwa chronionych obiektów. Inną strukturą informacji, którą można zbadać przy wyborze planu łagodzenia skutków i ochrony, jest kombinacja prognoz dotyczących ewolucji obecnych zagrożeń, oczekiwań i spodziewanych wyników planowanych działań. Można również rozważyć przewidywane decyzje zespołów ratowniczych i systemów autonomicznych, które zostaną podjęte w przypadku braku odbioru poleceń w razie awarii łączności. Informacje te mogą pochodzić z TRRM z symulacją lub prognozowaniem ilościowych i jakościowych cech zagrożeń i reakcji. Problem optymalnego wykorzystania infrastruktury TRRM można teraz sformułować następująco:

Problem 8.2. Na podstawie ograniczeń *U(J,t),* informacji otrzymanych z czujników i innych źródeł J oraz przetworzonych i uzupełnionych przez fuzję i inne jednostki przetwarzające, struktury TRRM, instrukcji, norm i polityk zarządzania ryzykiem, informacji o preferencjach zawartych w zbiorach A_1, A_2, A_3, sieci antycypacyjnej Ω, a także potencjalnych kompromisów pomiędzy kryteriami *F*, dla każdego momentu t okresu ograniczania zagrożeń i ochrony, obliczyć kompromisowy plan działania *p(t)* i przedstawić go do zatwierdzenia decydentowi w ramach procedury interaktywnej. ■

Problem 8.2 jest kolejnym zadaniem optymalizacji kombinatorycznej rozwiązywanym adaptacyjnie, co oznacza, że biorąc pod uwagę plan działań *p(t)*, działania wyznaczone w chwili $t+1$ uwzględniają działania z *p(t)* i ich wyniki jako ograniczenia. Poniżej wyjaśniamy, jak powyższe struktury danych i preferencji mogą być wykorzystane do rozwiązania Problemu 2 dla struktury TRRM jak [Rys. 58].

Kryteria *F* opisujące przypisanie działań łagodzących do osób udzielających pierwszej pomocy w problemie (8.2) można zdefiniować jako:

F_1 - kryteria przeciwdziałania/zmniejszania skutków zagrożenia kradzieżą, wandalizmem,

F_2 - wynik finansowy planu działania *p(t)*: straty i koszty wszystkich działań,

Dodatkowe informacje o preferencjach są dostarczane jako zestawy:

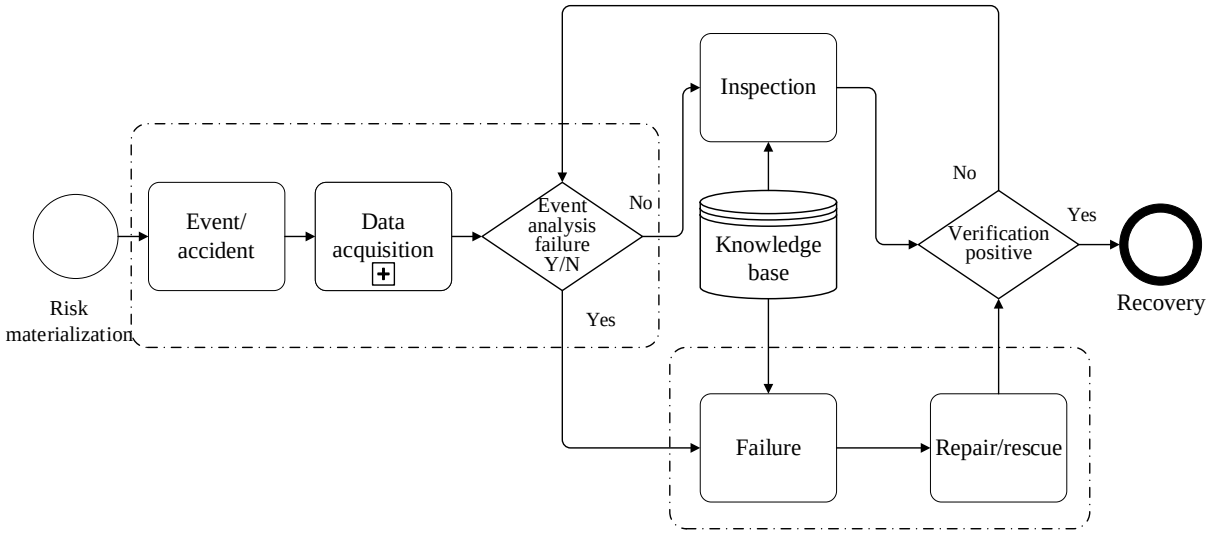
A_1 – docelowy poziom wpływu ryzyka na majątek firmy,

A_2 - parametry wynikowe możliwych do realizacji działań ratowniczych wynikające bezpośrednio z przepisów i polityki,

A_3 - dane historyczne przechowywane w bazie wiedzy dotyczące katastrofalnych zdarzeń o podobnym charakterze.

Wybór planu reakcji *p(t)* ma na celu obniżenie poziomu ryzyka do $R_0 \in A_1$ z uwzględnieniem parametrów zawartych w zbiorze danych A_2 i uniknięciem elementów A_3.

W dłuższej perspektywie ewolucja IRM DSS może być połączona z długofalowym zarządzaniem ryzykiem przedsiębiorstwa w ramach procedury roadmappingu technologicznego [Skulimowski, Pukocz, 2012]. Proces identyfikacji najnowocześniejszych metod AI i urządzeń opartych na AI, wprowadzanie ich do systemu w oparciu o zasady dostosowania AI przedstawiono w [Skulimowski, Bañuls, 2021]. Podsystem decyzyjny TRRM może być modelowany jako hybrydowa sieć antycypacyjna Ω z jednym koordynatorem [Skulimowski, 2014]. Ogólny schemat procesu zarządzania ryzykiem przedstawiono na Rys. 63.



Rys. 60. Przykład przepływu pracy związanego z zarządzaniem ryzykiem (awaria maszyny).

Podsumowując, zauważmy, że problemy 1 i 2 rozpatrywane łącznie tworzą dwupoziomowy problem optymalizacji projektowania [Barthelemy, 1998], gdzie infrastruktura modelowana w TRRM definiuje ograniczenia dla Problemu 8.2 wyrażone jako zawartość przepływu informacji J(t) oraz przez granice planowania działań p(t).

8.4.1 Podsumowanie problemu ewakuacji

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

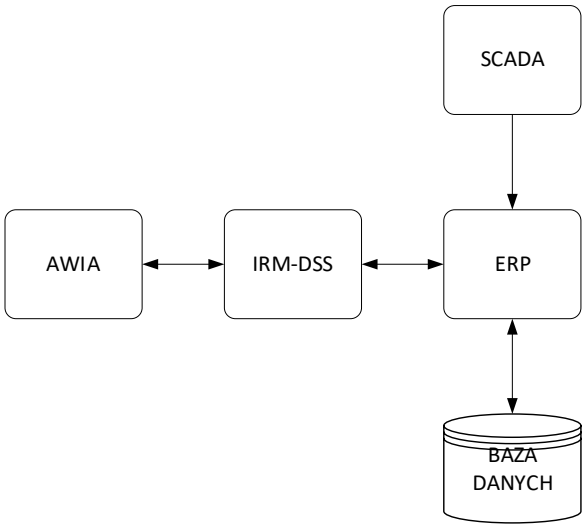
systemu dla kopalni odkrywkowej pokazuje, że zastosowanie metod AI, takich jak fuzja informacji, uczenie częściowo nadzorowane i wzmacniające oraz techniki rozumienia obrazów, znacznie zwiększa możliwości i efektywność systemu. W rezultacie, zaproponowane tutaj podejście do projektowania iDSS może zapewnić 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 ocenami zajmującymi się tylko pewnym etapem drogi do efektywnych systemów bezpieczeństwa przemysłowego.

Analiza wymagań poprzedzająca projektowanie systemu wspomagania decyzji miała na celu predykcję poprzez zapobieganie potencjalnym przyszłym zagrożeniom, usuwanie lub ograniczanie skutków obecnych zagrożeń industrialnych oraz usuwanie skutków zagrożeń przeszłych. W przypadku zastosowania do projektowania konkretnego systemu bezpieczeństwa przemysłowego, zaproponowany powyżej schemat rozwiązań musi zostać uszczegółowiony tak, aby odzwierciedlał konkretne uwarunkowania fizyczne i ekonomiczne. Realizacja IRM DSS zapewnia jednoczesną optymalizację kryteriów zarządzania bezpieczeństwem i kryteriów ekonomicznych. Pierwsza grupa kryteriów jest określona w strategii zapewnienia bezpieczeństwa organizacji, natomiast druga charakteryzuje bilans i zwykle odnosi się do rocznych wyników ekonomicznych.

Kolejność wdrażania poszczególnych modułów IRM DSS powinna być zgodna z aktualnym rankingiem wymagań określonym przez *Chief Information Officer* (CIO) lub *Chief Technology Officer* (CTO). Ważną rolę w projekcie IRM DSS odgrywają graficzne reprezentacje ryzyka, zagrożeń, zapobiegania i łagodzenia skutków, wbudowane w ogólne procesy biznesowe organizacji. Zaproponowana w analizie problemu nowa notacja odpowiada fizycznej strukturze artefaktów ryzyka i łączy je z procedurami wspomagania decyzji i podejmowania decyzji. W przeciwieństwie do innych podejść opartych na BPMN [Mehla, Jain, 2020] lub UML [Purohit, i in., 2019], koncentruje się ona na bezpieczeństwie fizycznym, a nie na zarządzaniu zagrożeniami cybernetycznymi. Tendencyjność poznawcza personelu ludzkiego [Rodriguez i in., 2011] jest kolejnym zagadnieniem, które powinno być brane pod uwagę przy projektowaniu przyszłych złożonych systemów cyber-fizycznych obejmujących interakcje człowieka z AI. W dużych zakładach przemysłowych, gdzie istnieje potrzeba zarządzania zagrożeniami naturalnymi z wykorzystaniem sił wewnętrznych, a nie tylko publicznych służb zarządzania kryzysowego, konieczne jest zapewnienie zarówno, odpowiednich instrumentów, jak i procedur decyzyjnych. Należy przyjąć, że wszystkie one powinny być realizowane jako holistyczny IRM DSS. DSS dla utrzymania bezpieczeństwa przemysłowego powinny umożliwiać zarządzanie wszystkimi rodzajami zagrożeń, w tym związanymi z katastrofami naturalnymi. Ich charakterystyka powinna być zidentyfikowana do poziomu szczegółowości wymaganego do rozwiązywania problemów optymalizacji przez DSS.

9 Implementacja IRM DSS w kontekście obecnych rozwiązań informatycznych w KWC

W chwili obecnej procesy produkcyjne i biznesowe w KWC wspierane są przez systemy informatyczne, które z założenia mają usprawnić i zoptymalizować funkcjonowanie przedsiębiorstwa, zwiększając efektywność oraz automatyzując pewne procesy biznesowe. Wymiana danych pomiędzy poszczególnymi systemami nie jest realizowana w oparciu o szynę danych, a jedynie w okrojonym zakresie poprzez pliki wymiany danych, co obniża ogólną efektywność i możliwości płynące w wykorzystani systemów w pełni zintegrowanych. Rysunek [Rys. 61] pokazuje strukturę i relacje, uwzględniając integrację dzięki wdrożeniu systemu IRM DSS.



Rys. 61. Schemat poglądowy prezentujący zależności pomiędzy użytkowanymi i planowanymi do wdrożenia systemami.

Poszczególne komponenty pokazane na rysunku [Rys. 61] omówione zostaną w kolejnych podrozdziałach, a są to kolejno systemy:

- ERP - system informatyczny służących wspomaganiu zarządzania przedsiębiorstwem,
- SCADA - system informatyczny nadzorujący przebieg procesu technologicznego i produkcyjnego,
- AWIA - system monitorowania pracy maszyn ciężkich,
- IRM DSS - Industrial Risk Management Decision Support System – system będący przedmiotem projektowania w ramach niniejszej pracy,
- BAZA DANYCH – centralna baza danych wspierająca pracę wszystkich systemów.

9.1 System ERP

KWC wykorzystuje w prowadzeniu bieżącej działalności operacyjnej system klasy ERP (Enterprise Resource Planning) pn. Zintegrowany System Zarządzania Przedsiębiorstwem Bilans (producent: Bilans JR). Jest to system pracujący w architekturze typu klient-serwer, w skład którego wchodzą między innymi moduły wskazane na [Rys. 62].

Rys. 62. Główne moduły systemu ERP (Enterprise Resource Planning) wykorzystywane w KWC.

Wskazane na [Rys. 62] elementy składają się na system oprogramowania klasy ERP, stanowiąc zestaw zintegrowanych modułów do zarządzania głównymi procesami biznesowymi firmy.

Moduł Handlowy – zapewnia pełną obsługę procesów zakupów i sprzedaży, dając możliwość obsługi wielu magazynów wewnętrznych oraz zapewniając pełny obieg dokumentów związanych z tymi procesami, łącznie z wielopoziomową ich akceptacją. Dodatkowo moduł ten zintegrowany jest z urządzaniem zewnętrznymi, typu wagi i czytniki, zapewniając automatyczną obsługę i obieg dokumentów handlowych. Moduł ten zintegrowany jest również z platformą B2B gwarantując klientom zewnętrznym dostęp zarówno do danych w zakresie zakupu jak i możliwość samodzielnej obsługi w zakresie zamawiania i awizowania odbiorów.

Moduł Magazynowy – zapewnia pełną obsługę gospodarki magazynowej zakresie przepływu towarów (i usług), automatyzując procesy magazynowe. Moduł jest w pełni zintegrowany z pozostałymi modułami, dzięki czemu wiele czynności odbywa się w pełni automatycznie, usprawniając i przyspieszając pracę osób odpowiedzialnych za poszczególne magazyny przedsiębiorstwa.

Moduł Remontowy – wspiera utrzymanie ruchu i ciągłości produkcji, gospodarkę remontową (zarządzanie remontami) oraz jej efektywne z planowanie. Dzięki funkcjonalności obsługi zleceń produkcyjnych (w tym zleceń awaryjnych) umożliwia efektywne zarządzanie parkiem maszynowym oraz infrastrukturą posiadaną przez przedsiębiorstwo. Integracja z systemami HR zapewnia dokładne rozliczanie czasu pracy niezbędnego do realizacji zadań związanych z szeroko rozumianą obsługą remontową majątku przedsiębiorstwa.

Moduł Środków Trwałych – zapewnia kompleksowe zarządzanie środkami trwałymi, wartościami niematerialnymi i prawnymi, naliczanie amortyzacji, przeprowadzanie inwentaryzacji itp. Dodatkowo dzięki wykorzystaniu funkcjonalności kilku magazynów umożliwia prowadzenie ewidencji wyposażenia nisko cennego oraz Narzędziowni, z pełną obsługą historii obrotu wewnętrznego sprzętu i narzędzi.

Moduł Analiz – stanowi rozbudowane narzędzie do wielowymiarowych analiz. Umożliwia wykonywanie analiz trendów sprzedaży lub analiz finansowych oraz wielopoziomowej analityki danych na potrzeby analiz statystycznych.

Moduł CRM – służy do planowania kontaktów z klientem, ewidencjonowania przeprowadzonych spotkań i rozmów telefonicznych oraz przydzielania zadań pracownikom.

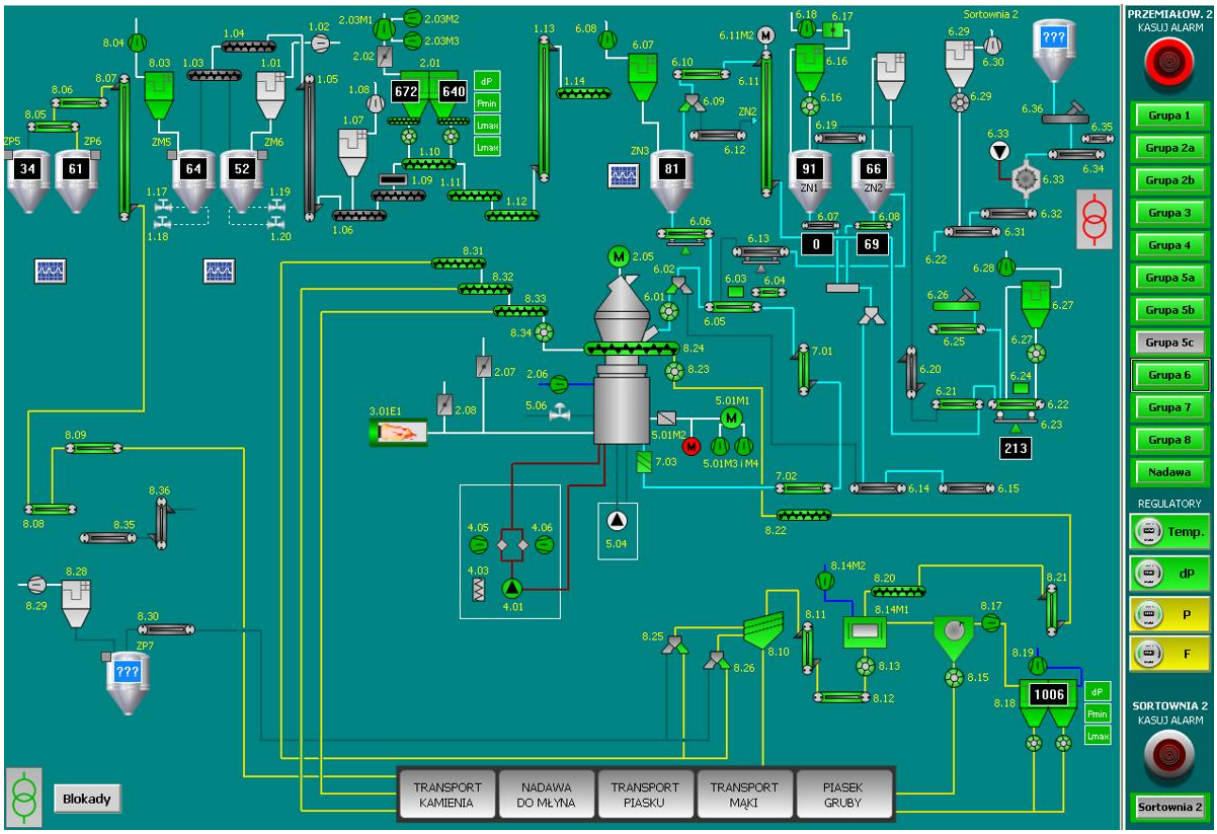
Kolorem zielonym oznaczono moduły systemu wykorzystywane w KWC uczestniczące w procesach związanych z bezpieczeństwem pracy maszyn i urządzeń.

Kluczową rolę w procesach zapewnienia ciągłości pracy maszyn i urządzeń, a tym samym bezpieczeństwie produkcji pełni Moduł Remontowy. Prawidłowe i pełne wykorzystanie wiedzy, jaką daje narzędzie informatyczne pozwala w sposób predykcyjny planować dyspozycyjność poszczególnych elementów łańcucha technologicznego oraz zapewnia jego optymalne wykorzystanie.

9.2 System SCADA

Drugim, równolegle wykorzystywanym w KWC systemem informatycznym jest system SCADA (Supervisory Control And Data Acquisition). Jest to system nadzorujący procesy technologiczne, w tym w szczególności ich pracę i funkcjonowanie. Kluczowa funkcjonalność systemu opiera się na zapewnieniu możliwości ciągłego, precyzyjnego i adekwatnego do potrzeb sterowania i zarządzania procesem produkcyjnym. Aby zapewnić powyższą funkcjonalność system musi gromadzić w sposób ciągły szereg danych, agregować je w sposób zgodny z potrzebami technologicznymi oraz zapewniać możliwość ingerencji operatora w przebieg procesu w sposób ciągły. Architektura systemu SCADA wykorzystywana w KWC opiera się o rozwiązania klasyczne [Skulimowski, 2011], bazujące na serwerach bazodanowych, aplikacyjnych, dostępowych, sterownikach PLC oraz stacjach roboczych. W calu podniesienia bezpieczeństwa i zapewnienia wymaganej dostępności

kluczowe elementy systemu są redundantne, a architektura sieciowa oparta jest o urządzenia pracujące w ringu. Przykładowy widok interfejsu dostępnego dla operatora systemu prezentuje rysunek [Rys. 63].



Rys. 63. Interfejs graficzny systemu SCADA. Źródło: materiały własne KWC.

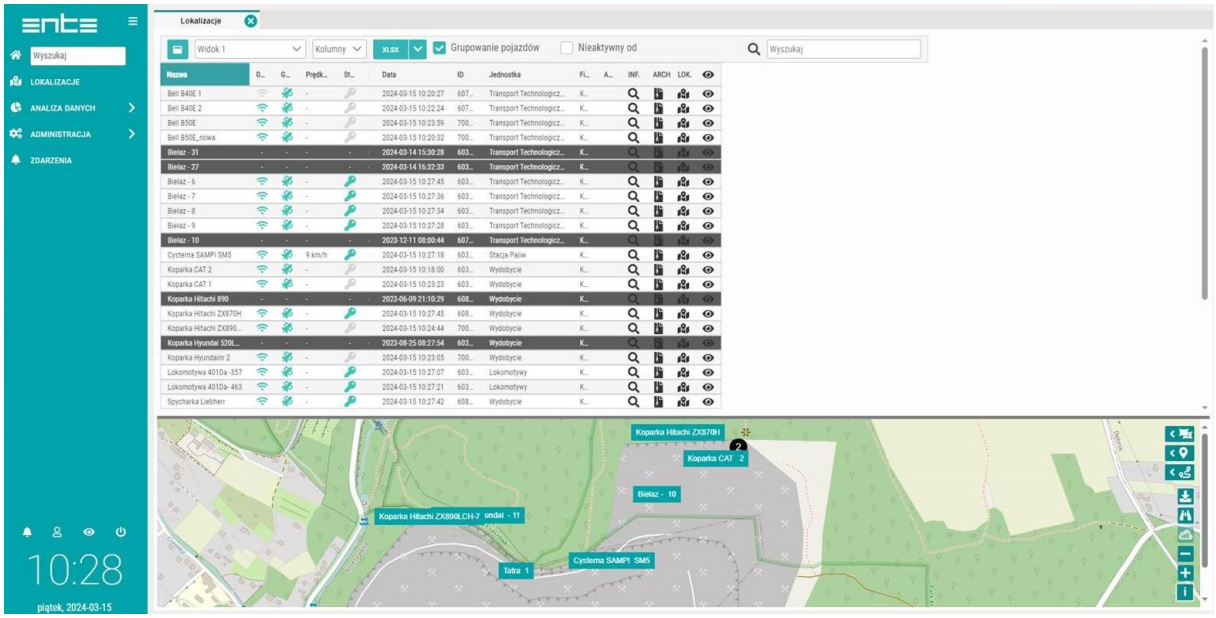
Systemy automatyki przemysłowej (OT) są kluczowe dla zapewnienia ciągłości działania ciągów technologicznych, a co za tym idzie, ich dostępność i odporność na zagrożenia jest priorytetowa. Spółka zarządza bezpieczeństwem systemu SCADA zgodnie z obowiązującymi w Grupie Tauron regulacjami (w szczególności w zakresie OT), spełniającymi najwyższe wymagania w kwestii bezpieczeństwa.

9.3 AWIA Machines

Flota maszyn spalinowych (wozidła technologiczne) nadzorowana i monitorowana jest przy wykorzystaniu systemu monitorowania maszyn ciężkich AWIA Machines. System[4] ten zapewnia kontrolę nad flotą maszyn i optymalizację kosztów związanych z ich utrzymaniem. Realizowane jest to głównie poprzez bieżącą kontrolę zużycia paliwa oraz kontrolę czasu i rodzaju pracy maszyny (sonda paliwa, czujnik obrotów silnika, czytnik kart RFID do identyfikacji operatora, interfejs magistrali CAN). Dane przesyłane są w trybie online

[4] https://ente.com.pl/

w oparciu o sieć komórkową, a do geolokalizacji system wykorzystuje technologię GPS. Dane prezentowane są operatorowi w postaci raportów, wykresów oraz z wykorzystaniem wizualizacji naniesionej na mapę wyrobiska. System pracuje samodzielnie, bez integracji z innymi systemami informatycznymi, a ilość dostarczanych danych dostosowana jest do obecnych potrzeb i oczekiwań użytkowników, jednak jego rozbudowa otwiera perspektywy w obszarze predykcyjnego utrzymania ruchu. Obecnie trwają prace wdrożeniowe dodatkowego modułu, który w swym założeniu usprawni obsługę bieżącą wodzideł technologicznych poprzez uruchomienie funkcjonalności elektronicznych kart drogowych, uzupełnianych przez operatora na tablecie. Przykładowy widok interfejsu dostępnego dla operatora systemu prezentuje rysunek [Rys. 64].



Rys. 64. Interfejs graficzny systemu AWIA Machines. Źródło: materiały własne KWC.

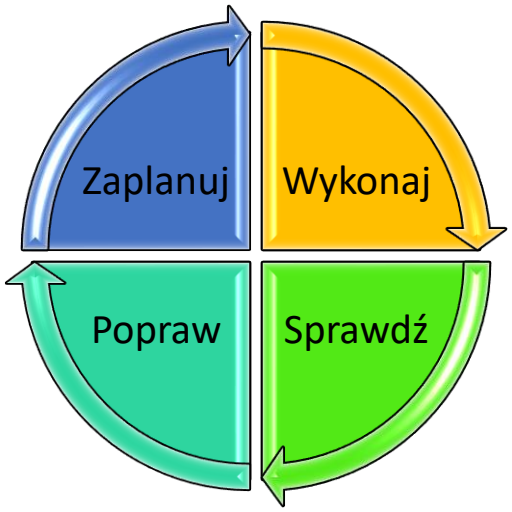
9.4 Luki funkcjonalne w użytkowanych systemach informatycznych.

Aktualny stopień wykorzystania i rozwoju używanych systemów informatycznych pozwala wyciągnąć wnioski co dalszych kierunków rozwoju systemu ERP i jego integracji z pozostałymi istniejącymi i planowanymi do implementacji w KWC rozwiązaniami (systemami).

1. Moduł pobierania i analizy danych z systemów niezależnych (np. SCADA) w zakresie czasu pracy, przerobu, zużycia mediów maszyn i ciągów technologicznych.
2. Moduł planowania wsparty przez AI, działający w oparciu o dane zebrane z różnych składników szeroko rozumianego systemu bezpieczeństwa, dający jako wynik swego działania wytyczne optymalizujące zarządzanie zarówno majątkiem, jak i holistycznym

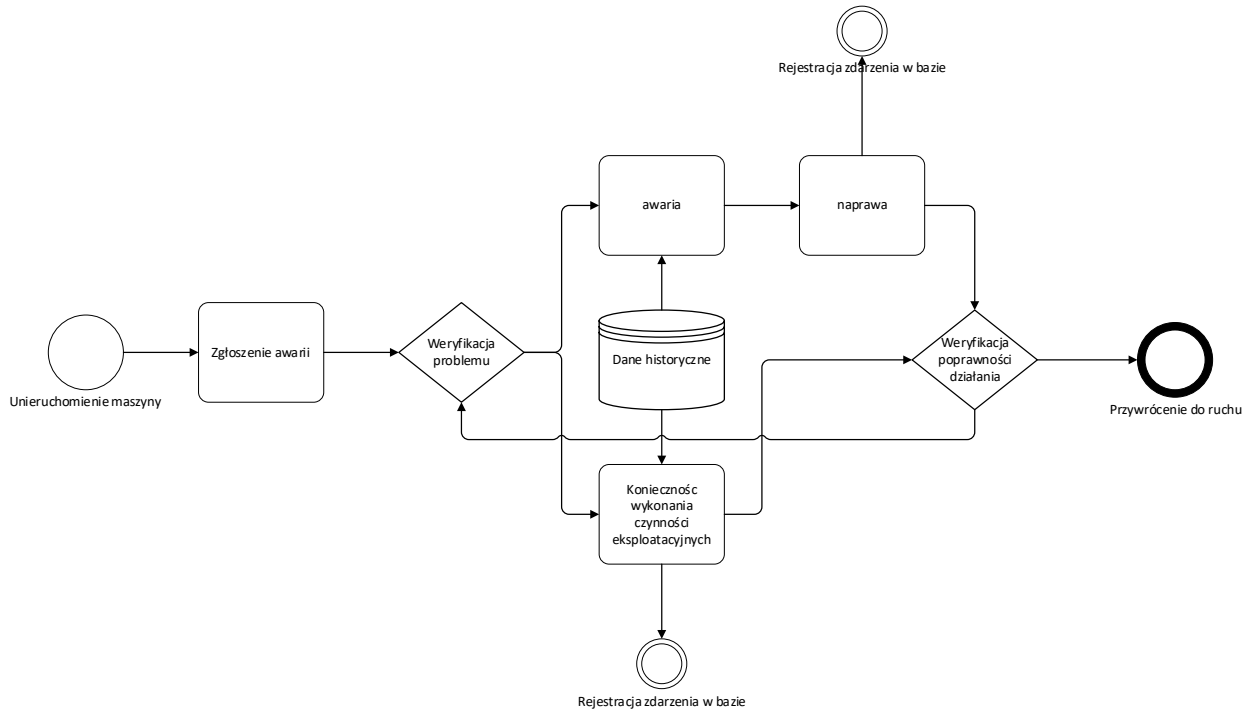
system bezpieczeństwa. Rozwiązanie takie będące swoistym sprzężeniem zwrotnym pozwoli w sposób ciągły, zgodnie z cyklem Deminga, na doskonalenie systemu.

Cykl Deminga [Rys. 65] jest koncepcją zarządzania procesem opracowaną przez Williama Edwardsa Deminga. Zgodnie z wypracowana koncepcją, poprzez cykliczne wykonywanie kolejnych kroków dążymy do ciągłego doskonalenia procesu. Odbywa się to w czterech następujących po sobie etapach: planowanie – wykonanie – sprawdzenie – poprawienie (ang. Plan – Do – Check – Act).



Rys. 65. Cykl Deminga.

Na etapie planowania określony zostaje sposób działania, który realizowany jest w kroku kolejnym - wykonaj. Następnie mamy etap sprawdzenia i badania wyników podjętych wcześniej działań, ich zgodności z założeniami z etapu planowania. W ostatni kroku cyklu, na podstawie wyników opracowanych na etapie sprawdzenia wdrażamy poprawki czy usprawnienia, których efekt oceniony zostanie w nowym cyklu rozpoczynającym się od zaplanowania nowych działań. Dzięki takiemu podejścia optymalizacja i poprawa skuteczności opracowanych metod realizowana jest w sposób kontrolowany, monitorowany, bezpieczny i zrozumiały przez uczestników procesu, jednocześnie zwiększa wydajność operacyjną analizowanego procesu.



Rys. 66. Propozycja procesu obsługi zgłoszenia awarii zapisana w notacji BPMN.

Integracja na poziomie platformy informatycznej systemu klasy ERP oraz IRM DSS pozwoli analizować procesy biznesowe z uwzględnieniem podejścia holistycznego, dając osobom odpowiedzialnym pełen zakres wiedzy niezbędny do zarządzania poszczególnymi procesami związanymi tak z bieżącą eksploatacją, jak i bezpieczeństwem poszczególnych składników majątku Spółki. Propozycję transferu informacji w trakcie obsługi awarii maszyny przedstawia [Rys. 66].

9.5 Interoperacyjność używanych systemów informatycznych

Jak pokazano na [Rys. 61], wymienione w powyższych podpunktach systemy powinny zasilać danymi IRM DSS, a przepływ informacji powinien optymalizować pracę systemu. Aby to osiągną niezbędna jest odpowiednia interoperacyjność każdego z omówionych systemów. Przez interoperacyjność należy tu rozumieć zbiór cech systemu, dzięki którym system jest w stanie współpracować z innymi systemami na drodze wymiany i wykorzystania informacji. Kluczową rolę w realizacji takich oczekiwań odgrywa interfejs programistyczny aplikacji (API - application programming interface). API definiuje się na poziomie kodu źródłowego każdej z aplikacji (np. w postaci bibliotek systemu operacyjnego) i jest zbiorem wytycznych, jak powinna przebiegać interakcja zarówno pomiędzy poszczególnymi komponentami samego systemu, a także opisuje protokoły komunikacji z zewnętrznymi systemami, co jest kluczowe na etapie integracji kilku systemów informatycznych,

pracujących na różnych platformach programistycznych. Korzyści z wykorzystania API przy integracji różnych systemów wydają się oczywiste, podstawowe z nich to:

- automatyzacja procesu wymiany danych,

- elastyczność tworzonych platform informatycznych,

- zwiększenie bezpieczeństwa (brak bezpośredniego dostępu do struktur bazy danych, a jedynie za pośrednictwem dedykowanych interfejsów).

Poniższa tabela [Tab. 25] zawiera zestawienie informacji, które dzięki odpowiedniej interoperacyjności, mogą być przekazywane z systemów dziedzinowych do systemu IRM DSS.

Tab. 25. Zakres wymiany danych pomiędzy używanymi systemami.

IRM DSS		
ERP	SCADA	AWIA
- harmonogram przeglądów, - zlecenia w zakresie eksploatacji bieżącej, - zlecenia awaryjne, - stany magazynowe.	- stan pracy poszczególnych ciągów i urządzeń, - przeroby, - przerwy i postoje, - stany magazynowe (produktów), - dane z czujników w zakresie pracy bieżącej ciągów i urządzeń.	- stan pracy poszczególnych maszyn, - czas i charakter pracy, - dane z czujników w zakresie bieżącego stanu maszyny, - dane archiwalne o zdarzeniach awaryjnych, - lokalizacja maszyny.

9.6 Uwzględnienie zagrożeń i ryzyk w analizie procesów biznesowych i technologicznych

9.6.1 Analiza ryzyka i wrażliwości implementacji IRM DSS w KWC

Analizy ryzyka przeprowadzone przez KW Czatkowice wskazują na konieczność uszczelnienia granic terenu Spółki i zabezpieczenia się przed możliwością wejścia osób niepożądanych. To ryzyko może mieć wpływ na utrzymanie ciągłości procesów technologicznych, należy zatem dążyć do jego minimalizacji. Dodatkowym aspektem, na który należy zwrócić uwagę przy kompleksowej analizie bezpieczeństwa przemysłowego

KW Czatkowice jest fakt, że sposób prowadzonej eksploatacji złoża oraz rodzaj złoża generuje ryzyko powstania zagrożeń dla bezpieczeństwa ludzi i maszyn, takich jak obsunięcia się mas skalnych. Oprócz ryzyka intruzji istnieją jeszcze inne istotne czynniki ryzyka związane z zagrożeniami antropogenicznymi i naturalnymi, a także będące wynikiem synergii pomiędzy działalnością człowieka a procesami naturalnymi. Wszystkie te procesy, czynniki zagrażające bezpieczeństwu oraz konieczność spełniania przepisów i norm o szybko rosnącej złożoności decydują o konieczności wdrożenia w KW Czatkowice systemu zarządzania bezpieczeństwem wykorzystującego nowoczesne technologie informacyjne, metody i techniki sztucznej inteligencji. Systemy informatyczne o takich właściwościach określane są ogólnie jako systemy wspomagania decyzji zarządzania bezpieczeństwem przemysłowym. Systemy tej klasy posiadać mogą również funkcjonalności systemów zarządzania ryzykiem korporacyjnym (Enterprise Risk Management Systems) – ukierunkowanych głównie na ryzyka finansowe oraz Industrial Resilience Management Decision Support Systems (IRM DSS) – specjalistycznych systemów zapewnienia maksymalnej odporności na zagrożenia naturalne i antropogeniczne. W KW Czatkowice system taki docelowo powinien umożliwiać zarządzanie wszystkimi zidentyfikowanymi dotąd grupami zagrożeń.

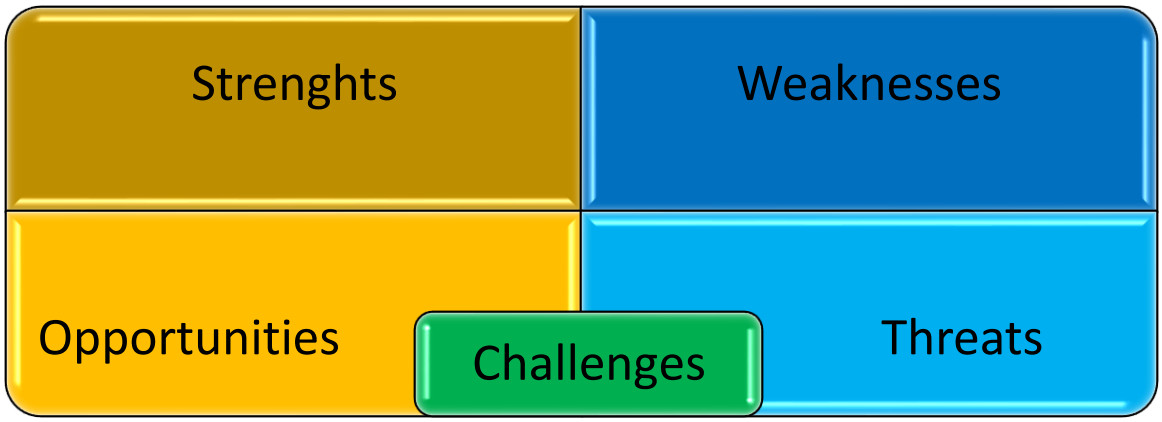
System wspomagania decyzji dla utrzymania bezpieczeństwa przemysłowego (IRM DSS) docelowo powinien umożliwiać zarządzanie wszystkimi zidentyfikowanych grupami zagrożeń, w tym także związanych z katastrofami naturalnymi. Rodzaje zagrożeń po ich zidentyfikowaniu i sklasyfikowaniu należy podzielić grupy i zastosować gradację ich wpływu na sposób postępowania w przypadku ich zaistnienia. W metodologii oceny i zarządzania zagrożeniami wyróżnia się ryzyka trzech podstawowych typów, jak wskazano już w rozdziale „Metody oceny ryzyk i zagrożeń przemysłowych” [Di Vaio i in., 2020]:

- Zagrożenia typu safety,
- Zagrożenia typu security,
- Zagrożenia dostępności.

9.6.2 Analiza SWOTC implementacji IRM DSS w KWC

Analiza SWOTC [Skulimowski, 2006] [Rys. 67] jest zorientowanym praktycznie rozszerzeniem uniwersalnej i popularnej techniki analizy biznesowej dostępnych o przedsiębiorstwie informacji, w odniesieniu zarówno do otoczenia zewnętrznego, jak i wewnętrznego. Polega na podzieleniu zebranych informacji na 4 główne kategorie (Strengths – silne strony, Weaknesses – słabe strony, Opportunities – szanse, okazje, Threats – zagrożenia i wyzwania - Challenges, przekształcające się w O lub T w zależności od podjętych decyzji i innych czynników) będące materiałem wejściowym do wnioskowania co do kierunków rozwoju i poprawy funkcjonowania przedsiębiorstwa. Poprawnie przeprowadzona analiza SWOT pozwala na systematyczne i kompleksowe spojrzenie na

przedsiębiorstwo, zarówno od strony procesów wewnętrznych, jak i otoczenia zewnętrznego. Jest narzędziem strategicznym, zarówno do diagnozowania stanu obecnego jak i planowania przyszłych działań.



Rys. 67. Analiza SWOTC.

Silne strony:

Kopalnia jest wiodącym producentem sorbentów w Polsce. Złoże w Czatkowicach charakteryzuje się bardzo dobrymi parametrami chemicznymi kamienia wapiennego. Kamień wapienny pochodzący z KW Czatkowice znajduje szerokie zastosowanie w przemyśle energetycznym, budowlanym, w drogownictwie oraz przemyśle paszowym. Zakład posiada certyfikaty normy Systemu Zarządzania Jakością ISO 9001:2000 oraz ISO 14001:1996 w zakresie wydobywania i przerobu kamienia wapiennego. KWC posiada szeroką ofertę produktów charakteryzujących się wysoką jakością.

Słabe strony:

Teren kopalni zaliczyć należy do kategorii obiektów z podwyższonym zagrożeniem, co wymusza dbanie o kontrolę przepływu osób i towarów na terenie obiektu, a przede wszystkim wszelkich aktów wkroczenia na teren w miejscach do tego nie przewidzianych. Teren kopalni nie jest obecnie wygrodzony szczelnym ogrodzeniem zewnętrznym. Teren w znacznej części graniczy z obszarami leśnymi co dodatkowo ułatwia możliwość wtargnięcia na teren kopalni.

Szanse:

Rozwój i postęp technologii otwierają obecnie nowe możliwości w wielu dziedzinach przemysłu, w tym również związanych z zapewnieniem bezpieczeństwa. Szczególne znaczenie mają techniki sztucznej inteligencji, umożliwiające zastąpienie i/lub wsparcie personelu przy analizie danych, a także np. rozpoznawania sytuacji potencjalnie niebezpiecznych, stosowane w systemach monitoringu wizyjnego.

Wdrożenie nowego systemu zarządzania bezpieczeństwem wykorzystującego nowoczesne technologie informacyjne, metody i techniki sztucznej inteligencji.

Zagrożenia:

Zagrożenia typu safety (zagrożenia geologiczne, osuwiska, obrywanie się skał wynikające z budowy geologicznej złoża, robót strzałowych i eksploatacji przy wykorzystaniu ciężkiego sprzętu, zagrożenia wodne spowodowane drenażem kanałów krasowych czy też gwałtownymi ulewami).

Zagrożenia typu security (świadome lub przypadkowe uszkodzenie mienia, w tym działania sabotażowe, akty wandalizmu, przypadki kradzieży, próby ataków informatycznych).

Zagrożenia mające wpływ na wizerunek przedsiębiorstwa (działania radykalnych grup ekologicznych, wypadki z udziałem osób, zdarzenia zagrażające środowisku naturalnemu).

Tradycyjna analiza SWOT może zostać rozszerzona o dodatkowy aspekt: Wyzwania – Challanges, w którym wskazane zostają możliwe i proponowane przez autora analizy kierunki rozwoju wynikające wprost z przeprowadzonej w sposób standardowy analizy.

Wyzwania:

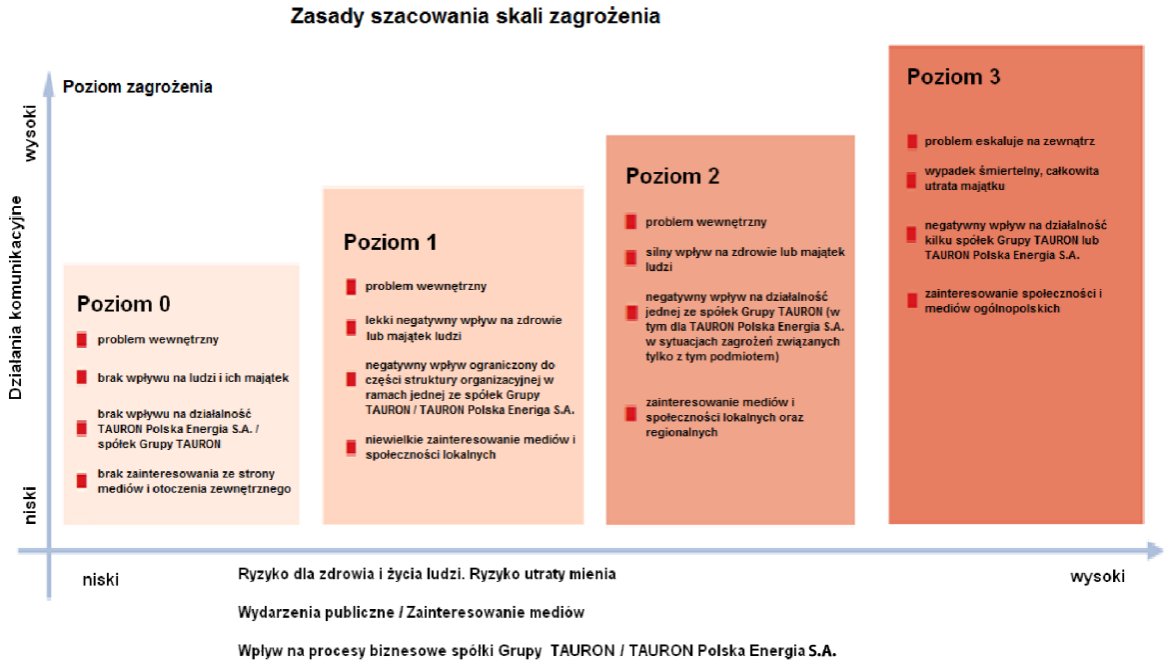
Wdrożenie nowego systemu zarządzania bezpieczeństwem, wykorzystującego nowoczesne technologie informacyjne, metody i techniki sztucznej inteligencji, pozwoli zwiększyć szanse na rozwój i redukcję kosztów, podnosząc jednocześnie poziom bezpieczeństwa oraz w sposób pozytywny wpływając na wizerunek przedsiębiorstwa.

9.6.3 Cele i problemy badawcze związane z zarządzaniem ryzykiem przemysłowym w KWC

W niniejszym rozdziale przedstawiono uszczegółowienie tezy i wynikające z niej problemy badawcze w oparciu o analizę przedstawionych wyżej rzeczywistych potrzeb zakładu w zakresie bezpieczeństwa.

Akcje ratownicze planowane i realizowane są w oparciu o obowiązujące w Spółce regulacje, w tym w szczególności Zasady komunikowania w sytuacjach kryzysowych [P.12]. Punktem wyjścia jest zrozumienie czym jest sytuacja kryzysowa. Pojęcie to ma szerokie znaczenie i odnosi się do każdego nieprzewidzianego zdarzenia,w sferze materialnej bądź niematerialnej, którego rzeczywiste lub potencjalne skutki mogą mieć negatywny wpływ na przedsiębiorstwo. W szczególności sytuacją kryzysową jest zmaterializowanie się zagrożenia.

Spółka określiła stały skład osobowy Sztabu Reagowania Kryzysowego uzupełniany każdorazowo o Właściciela Zagrożenia, który jednocześnie kieruje działaniami w obszarze funkcjonalnym zbieżnym z konkretnym zagrożeniem. Sposób reakcji zależy od skali i okoliczności związanych z zaistniałym kryzysem. Każde zdarzenie może zostać zakwalifikowane do poziomu zagrożenia 0, 1, 2 lub 3. Zwołanie Sztabu Reagowania Kryzysowego następuje zawsze w przypadku wydarzenia o poziomie zagrożenia 1, 2 lub 3.



Rys. 68. Zasady szacowania skali zagrożenia, zgodnie z [P.12].

Ocena sakali zagrożenia powinna być przeprowadzona już w trakcie zidentyfikowania (materializacji) zdarzenia i określać:

1. Jaki jest stopień zagrożenia dla bezpieczeństwa ludzi i sprzętu?
2. W jakim stopniu może pojawić się zagrożenie dla osób lub mienia w najbliższej przyszłości?
3. W jakim stopniu wydarzenie może w najbliższej przyszłości zainteresować otoczenie zewnętrzne, w tym media?
4. Jaki wpływ na proces biznesowy ma zaistniała Sytuacja kryzysowa?

Klasyfikacja poziomu zagrożenia odbywa się według kryterium „lub”. Wystarczy zaistnienie tylko jednego z kryteriów, aby sklasyfikować wydarzenie do wyższego poziomu zagrożenia. Kryterium o najwyższym wskaźniku zawsze decyduje o kwalifikacji wydarzenia do odpowiedniego poziomu zagrożenia.

Oceny i klasyfikacji zagrożenia dokonuje, bezpośrednio po powiadomieniu o zagrożeniu, właściciel zagrożenia, przypisując odpowiedni poziom. W zależności od ustalonego poziomu zagrożenia łaściciel zagrożenia podejmuje działania stosownie do zaistniałych problemów i istniejących procedur.

W przypadku zagrożenia o poziomie 0 właściciel zagrożenia podejmuje działania samodzielnie. W przypadku zagrożeń o wyższym poziomie powiadamia Sztab reagowania (na poziomie Spółki lub Grupy), przekazując informacje o wydarzeniu:

1. Co się wydarzyło?
2. Gdzie to wydarzenie nastąpiło?
3. Kto z pracowników jest związany z tym wydarzeniem?
4. Czy istnieje zagrożenie dla bezpieczeństwa zdrowia, życia, majątku ludzi lub reputacji?
5. Czy wydarzenie miało charakter publiczny (postronni obserwatorzy, telefony z zewnątrz z pytaniami do pracownika zgłaszającego problem)?
6. Czy wydarzenie zakłóca w jakimś stopniu pracę pracowników spółki Grupy TAURON?

Dalsze kroki i działania podejmowane są adekwatnie do zidentyfikowanego zdarzenia, przy czym należy pamiętać również o działaniach po zakończeniu kryzysu, mających na celu mitygację ryzyka powtórnego zdarzenia o tym samy charakterze.

Mając na uwadze powyższe wytyczne, kluczowe jest zapewnienie środków wykonawczych i organizacyjnych, które zapewnią możliwość efektywnego:

- reagowania i rozwiązywania problemów,
- budowania odporności,
- wsparcia decydentów w podejmowaniu optymalnych decyzji.

Każde ze wskazanych kryteriów może być w stosunkowo prosty sposób zrealizowane odrębnie, często nawet na drodze prostych środków organizacyjnych, jak odpowiednie regulaminy, procedury itp. Problem pojawia się jednak przy próbie podejścia holistycznego. Należy oczekiwać, że system zapewniający podejście holistyczne zapewni wsparcie dla decydentów oraz właścicieli biznesowych zarówno na etapie bezpośrednio „po" materializacji ryzyka, jak i „przed" zdarzeniem, dając możliwości predykcyjne. Prawidłowo zaprojektowany System Wspomagania Decyzji powinien również uzupełniać przedstawiony zakres możliwości o działania doradcze wyznaczają potencjalne scenariusze zdarzeń i optymalnych reakcji (odpowiedzi) w przypadku ich zaistnienia.

Jak widać oczekiwania stawiane projektowanemu systemowi są wysokie, a potencjalna ilość danych w oparciu, o które podjęte zostaną decyzje wydaje się być duża, a co więcej zgormadzona w oparciu w aktuatory często pozornie ze sobą zapełnienie niezwiązane (należące do różnych kategorii dziedzinowych). Aby temu sprostać algorytmy decyzyjne prowadzić muszą analizę danych wielokryterialnie, modelując w sposób ciągły ścieżki rozwoju zdarzeń (przebiegu zagrożeń) zarówno realnych, jak i hipotetycznych. Aby dodatkowo zbudować odpowiedni poziom zaufania decydentów do mechanizmów decyzyjnych zaimplementowanych w systemie DSS algorytmy powinny umożliwiać symulację zdarzeń możliwych do wystąpienia i, co chyba najważniejsze zapewniać ciągłość podejmowania, i właściwego przepływu procesu decyzyjnego w sytuacji pojawiających się

zakłóceń, które w skrajnym przypadku mogą doprowadzić do wykluczenia w łańcucha decyzyjnego jednego z ogniw.

Takim wysokim wymaganiom dotyczącym efektywności oferowanego przez DSS wsparcia w zakresie budowania i utrzymania odporności na zagrożenia wydają się sprostać algorytmy decyzyjne funkcjonujące w oparciu o sieci antycypacyjne.

Zaprojektowanie i przygotowanie do implementacji Systemu Wspomagania Decyzji zgodnie z omówionymi powyżej wymaganiami zapewni wymagany stopień efektywności, gwarantując użytkownikom systemu odpowiednie wsparcie w każdej sytuacji, kiedy będzie to niezbędne, dodatkowo dając czas i możliwość przygotowania się na zdarzenia hipotetyczne, na drodze wdrażania procedur, które pozwolą ich uniknąć.

Należy jednak zwrócić uwagę, że równie istotne, co systematyczna budowa odporności i efektywne rozwiązywanie problemów, jest dobór i zapewnienie dostępności właściwych narzędzi informatycznych, które w oparciu o wspólną platformę stworzą system holistyczny o oczekiwanej wydajności. Wynika to z faktu, że środowisko pracy, z którym będzie miał do czynienia system DSS, jest bardzo specyficzne, co przekłada się na konieczność stosowania narzędzi i rozwiązań odpornych, w sensie zarówno fizycznym jak i technicznym, na typowe dla tego środowiska wyzwania oraz zdolnych do adaptacji do zadanych, ale i zmieniających się warunków otoczenia.

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

10.1 Wdrażanie metod i narzędzi sztucznej inteligencji w KWC

Naturalnym krokiem w rozwoju przedsiębiorstwa w zakresie technologii informacyjno-komunikacyjnych jest zaprojektowania, implementacja i wdrożenie w ciągu najbliższych lat zintegrowanego systemu zarządzania bezpieczeństwem przemysłowym wskazanej wyżej klasy IRM DSS. Projekt wdrożenia takiego systemu bezpieczeństwa zakłada połączenie wykorzystywanych już obecnie w KW Czatkowice technik monitoringu wizyjnego oraz nowych rozwiązań, takich, jak systemy radarowe wsparte autonomicznymi bezzałogowymi jednostkami latającymi (drony), a w razie potrzeby także naziemnymi robotami inspekcyjnymi. Dodatkowo 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 zakłada integrację systemu radarowego z systemem optycznej identyfikacji zagrożenia i innymi sensorami. Sposób prowadzonej eksploatacji złoża oraz rodzaj złoża KW Czatkowice generuje ryzyko powstania zjawisk zagrażających bezpieczeństwu ludzi i maszyn, jakimi są obsunięcia się mas skalnych. W związku z tym 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, drony patrolować będą linie skrajne poziomów eksploatacyjnych. Wsparcie, jakie daje wykorzystanie procesów fuzji danych oraz sztucznej inteligencji będzie, kluczowe w procesie wielokryterialnej analizy danych spływających do systemu ze wszystkich jego elementów składowych i zapewni rozróżnienie obiektu niegroźnego i neutralnego z punktu widzenia systemu bezpieczeństwa, jak np. zwierzę leśne, od obiektu, którego identyfikacja, przejęcie i dalsze śledzenie jest wskazane z punktu widzenia zdiagnozowanych zagrożeń, tj. np. pojawienia się na monitorowanym terenie nieuprawnionych osób. Korzyści dla przedsiębiorstwa wynikające z wdrożenia systemu bezpieczeństwa wydają się zabezpieczać potrzeby podniesienia poziomu bezpieczeństwa technicznego, bezpieczeństwa fizycznego oraz otwierają perspektywy dalszego wykorzystania technologii, które w najbliższych latach odgrywać będą dużą rolę w gospodarce państw uprzemysłowionych, stawiając tym samym KW Czatkowice w grupie przedsiębiorstw nowoczesnych i zaawansowanych technologicznie, ale również zapewniających najwyższe standardy bezpieczeństwa.

10.2 Projekt funkcjonalny IRM DSS wykorzystującego metody i narzędzia sztucznej inteligencji

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. W tym miejscu wskazać należy innego rodzaju zagrożenia występujące w odkrywkowych zakładach górniczych.

Sposób prowadzonej eksploatacji złoża oraz rodzaj złoża, jakie eksploatuje KWC, generuje ryzyko powstania niebezpiecznych dla bezpieczeństwa ludzi i maszyn zjawisk, jakimi są obsunięcia 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.

Szczegółowy projekt funkcjonalny IRM DSS opierać się będzie o wyniki badania bezpieczeństwa i analizę czynników zagrożeń w KWC zgodnie z podaną niżej tabelą, która powstała w oparciu o analizę zidentyfikowanych zagrożeń, czynników i technologii przedstawionych w [Tab. 5]. Zbudowana w ten sposób macierz morfologiczna [Tab. 26] określa zależności pomiędzy poszczególnymi czynnikami ryzyka a technologiami i metodami AI.

Tab. 26. Macierz morfologiczna dla czynników ryzyka i planowanych do implementacji technologii AI w IRM DSS KWC – adekwatność technologii do minimalizacji ryzyk powiązanych z poszczególnymi czynnikami.

Czynniki ryzyka / **Technologie AI i pokrewne**	**Intruzje**	**Oberwania skał**	**Obsunięcia terenu**	**Zalania**
Monitoring wizyjny	Duża	niewielka	średnia	średnia
Okresowe obserwacje i mapowanie terenu z powietrza (drony)	niewielka	Średnia	duża	niewielka
Algorytmy automatycznego rozpoznawanie sytuacji niebezpiecznych	bardzo duża	średnia	duża	średnia
Algorytmy oceny zagrożeń na podstawie fuzji danych	mała	średnia	duża	duża
Inteligentne prognozowanie połączone z uczeniem maszynowym	mała	mała	średnia	średnia
Inteligentne wspomaganie decyzji	duża	średnia	średnia	średnia
Autonomiczne algorytmy decyzyjne	duża	średnia	średnia	duża

Architektura systemu powinna być zaprojektowana w sposób umożliwiający jego skalowalność, elastyczność oraz łatwość integracji z systemami opisanymi w rozdziale 8, a w przyszłości również z innymi systemami, którymi dysponował będzie przedsiębiorca. Propozycja architektury opiera się o następujące warstwy funkcjonalne:

1. Warstwa interfejsu użytkownika – powinna się charakteryzować dużą funkcjonalnością oraz umożliwia użytkownikom interakcję z systemem poprzez intuicyjne interfejsy. Powinna obsługiwać zarówno aplikacje webowe, jak i mobilne. Podstawowym elementem tej warstwy będą pulpity użytkownika (dashboardy) do wizualizacji stanu zdefiniowanych ryzyka w czasie rzeczywistym. Dodatkowo

warstwa ta powinna posiadać zintegrowane formularze do wprowadzania danych, ustawiania parametrów i progów ryzyka oraz moduły raportowania.

2. Warstwa logiki (analityki) – odpowiadająca za przetwarzanie danych i realizację reguł funkcjonalnych i biznesowych, takich jak analiza ryzyka, ocena kryterialna czy wnioskowanie. Warstwa ta powinna być wyposażona w podmoduły:
   - moduł analizy wielokryterialnej,
   - moduł predykcji i optymalizacji (np. z zaimplementowanym algorytmem NSGA-II do optymalizacji decyzji w oparciu o kryteria ryzyka),
   - moduł zarządzania scenariuszami: umożliwia tworzenie, symulowanie i ocenę alternatywnych strategii działania (np. w oparciu o grafy wiedzy).
3. Warstwa integracji odpowiadająca za komunikację pomiędzy różnymi modułami systemu oraz integrację z zewnętrznymi systemami w oparciu o API. Dodatkowo warstwa ta musi być wyposażona w narzędzia do zarządzania komunikacją i przepływem danych pomiędzy modułami systemu.
4. Warstwa danych odpowiadająca za przechowywanie i zarządzanie danymi przetwarzanymi w systemie. Kluczowym elementem tej warstwy są:
   - baza danych operacyjnych, która przechowuje dane o bieżących operacjach, stanach ryzyka oraz danych historycznych,
   - baza danych analitycznych, dedykowana do skomplikowanych analiz typu BI,
   - repozytorium dokumentów raportów, strategii i innej dokumentacji.
5. Warstwa bezpieczeństwa zapewniająca właściwą ochronę systemu przed atakami i zapewniająca zgodności z wymaganiami prawnymi dotyczącymi ochrony danych.
6. Warstwa dostosowania posiadająca moduły odpowiedzialne za analizę trendów zmian oraz zapewniająca właściwe i bieżące dopasowanie funkcjonalne systemu do zmieniających się warunków otoczenia.

Proponowany system zarządzania ryzykiem i wspierania decyzji opiera się na modularnej, skalowalnej architekturze, która pozwala na integrację z różnymi źródłami danych, a także automatyzację wielu procesów związanych z oceną ryzyka i podejmowaniem decyzji. Implementacja zaawansowanych technik AI/ML, takich jak analiza wielokryterialna oraz algorytmy optymalizacyjne, zapewnia skuteczność i elastyczność systemu w zmieniających się warunkach biznesowych.

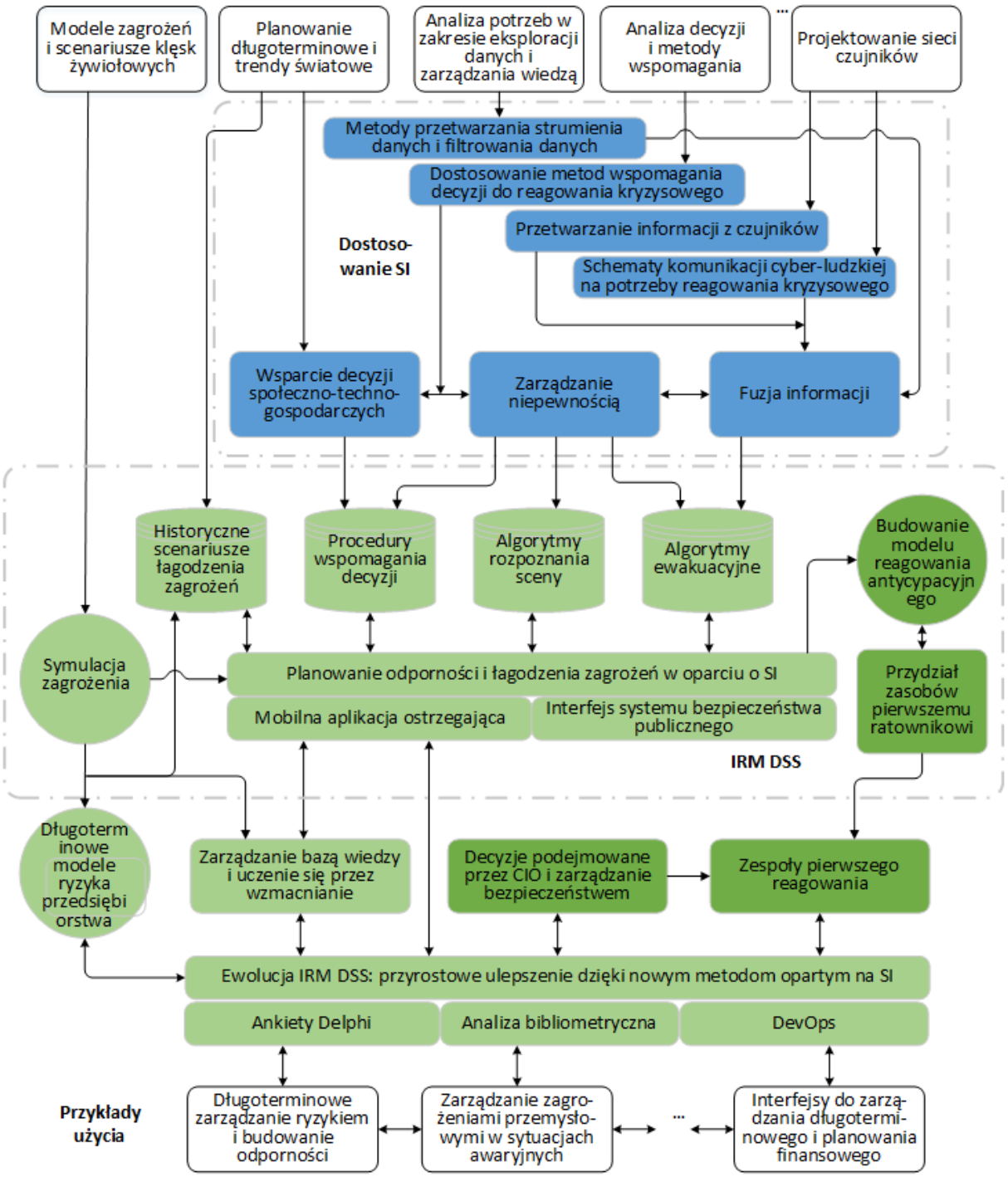
10.3 Zagadnienie dopasowania technologicznego metod sztucznej inteligencji stosowanych w IRM DSS

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. Problem ten można sformułować w następujący sposób [Skulimowski, Banuls, 2021].

Problem 10.1 (dopasowanie AI). W celu zapewnienia stałej przewagi technologicznej systemu nad potencjalnymi zagrożeniami antropogenicznymi wykorzystującymi metody AI należy dokonać analizy rynku technologii sztucznej inteligencji, aby znaleźć te, które odpowiadają potrzebom IRM DSS, na podstawie wcześniejszej analizy i kategoryzacji tych potrzeb. Techniki i metody AI należy również podzielić na kategorie i uporządkować w każdej kategorii według ceny, kompatybilności z innymi technologiami, prognozowanych parametrów pracy zaktualizowanego systemu i innych kryteriów wydajności odpowiednich dla danego zastosowania. Na tej podstawie w oparciu o analizę wielokryterialną zostanie wybrany najlepszy portfel technologii i plan ich wdrożenia uwzględniający dodatkowe informacje o preferencjach pochodzące z symulacji działania systemu i ocen ekspertów.

Ogólny schemat architektury informatycznej zapewniającej rozwiązanie powyższego problemu dopasowania SI można przedstawić w następujący sposób:

- Zostanie zbudowany model ewolucji AI jako samodzielny system wsparcia prognozowania i foresightu technologicznego, zdolny do modelowania rozwoju AI i powiązanych technologii. Ten model ewolucji technologicznej dostarczy wskazówek dotyczących rozwoju wybranych technologii sztucznej inteligencji, istotnych dla IRM DSS przez następne 10-15 lat.
- Ocena potrzeb technologicznych powinna być wykonywana przed rozpoczęciem wdrażania systemu i aktualizowana nie rzadziej niż co 2 lata. Zapewni ona aktualizację zapotrzebowanie na technologie AI, takie jak fuzja informacji lub autonomiczna robotyka, które będą wdrożone w IRM DSS.
- Potrzeby te, skonfrontowane z prognozami technologicznymi, umożliwiają wybranie najbardziej opłacalnej i użytecznej architektury oprogramowania, wdrożenie technik sztucznej inteligencji oraz ustalenie harmonogramu wdrożenia.



Rys. 69. Schemat systemu klasy IRM DSS proponowanego do implementacji i wykorzystania w KWC [wg Skulimowski i Łydek, 2022a].

Na tej podstawie plan wdrożenia IRM DSS zostanie zweryfikowany i zatwierdzony, a system wdrożony i przetestowany. Schemat IRM DSS opartego o powyższe założenia pokazano na diagramie wyżej [Rys. 69]. 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 (warstwy 4, 5, 6 diagramu) omówiony zostanie w dalszej części pracy i pokazany jest na [Rys. 59].

Sam schemat w celu zwiększenia przejrzystości podzielony został na obszary oznaczone innymi kolorami, a główne funkcjonalności zakreślone liniami przerywanymi. Górna część (bloki białe), to obszar zbierania danych ze źródeł dostępnych zarówno jako serwisy udostepniające dane online (np. serwisy pogodowe czy finansowe) jak i wewnętrznie w samej organizacji wykorzystującej system z wszelkiego rodzaju dostępnych czujników czy sensorów. Uzupełnieniem informacji zasilającej system są zewnętrzne analizy w zakresie metodyk przetwarzania danych, ich optymalizacji pod kątem konkretnego zastosowania oraz metod wspomagania tych analiz. Zebrane w początkowej fazie dane trafiają w większości do modułu odpowiedzialnego za ich dostosowanie, zgodnie z paradygmatem AI Alignment. Takie podejście powinno zagwarantować właściwe ukierunkowanie systemu na cele zamierzone, oczekiwane i zgodne z preferencjami decydentów, a sam system pozwolić uznać za system realizujący cele zgodne z potrzebami użytkowników go obsługujących. Cały ten moduł (oznaczony na niebiesko) składa się z bloków odpowiedzialnych za wstępne przetwarzanie zgromadzonych danych, obróbki danych z wykorzystaniem wbudowanych schematów postępowania właściwych dla analizowanej sytuacji oraz podmodułów fuzji informacji współpracujących z elementami zarządzania niepewnością. Przetworzone wstępnie dane trafiają do jądra systemu IRM DSS (kolor jasno zielony). Silnik systemu pracujący w oparciu o równolegle przetwarzające dane algorytmy ewakuacyjny i analizy sceny, przy wsparciu mechanizmów wspomagania decyzji oraz bazy historycznych scenariuszy reagowania przygotowuje zestaw danych, które trafiają do modelu sieci antycypacyjnych. W tym obszarze podejmowane są pierwsze decyzje wykonawcze wraz z ich przydziałem dla odpowiednich zespołów wykonawczych, w szczególności dla zespołu pierwszego reagowania. Bloki odpowiedzialne za podejmowanie decyzji w oparciu o dane przetwarzane w Sieci antycypacyjne oraz za ich realizację oznaczone zostały kolorem ciemno-zielonym. Ostatnim elementem systemu są moduły odpowiedzialne za utrzymanie systemu w zgodności z najnowszymi rozwiązanymi technicznymi i najnowszą wiedzą w zakresie opisanych wcześniej elementów. Główną rolę odgrywają tu mechanizmy wsparte badaniami bibliometrycznymi, ankietami Delphi oraz metodyką DevOps, mającą zapewnić ciągły rozwój systemu zgodnie z obowiązującymi trendami. Kluczowe bloki systemu IRM DSS omówione zostały w rozdziałach pracy, właściwych dla podejmowanych w nich tematyki.

10.3.1 Zasady dopasowania technologii SI zastosowane w projekcie IRM DSS

Ogólny model zarządzania ryzykiem przetwarza dane z sieci modułów przetwarzania informacji, w skład której wchodzą sensory, fuzja informacji, węzły wspomagania decyzji, a także węzły automatycznego podejmowania decyzji. Jako dane wejściowe służą

bezpośrednie sygnały z jednostek pomiarowych czynników zagrożenia, zarówno zautomatyzowanych, nadzorowanych, jak i obsługiwanych przez człowieka. Sieć tę uzupełnia model zarządzania ryzykiem i optymalizacji, obejmujący algorytmy decyzyjne, działania i elementy wykonawcze służące do ich realizacji. Wykonywalna informacja zwrotna jest bezpośrednio dostarczana decydentom przez ten sam system informacyjny i przetwarzany w IDSS. Model wspomagania decyzji zawiera następujące komponenty [Skulimowski, Łydek, 2022a]:

i. czujniki i inne jednostki zbierające informacje o wszystkich zagrożeniach, naturalnych lub antropogenicznych,
ii. dwa rodzaje węzłów fuzji informacji: zdolne do łączenia informacji tego samego rodzaju z różnych czujników (fuzja prosta) oraz złożone węzły fuzji zdolne do przetwarzania informacji heterogenicznych,
iii. zagrożeni ludzie, którzy mogą stanąć w obliczu zagrożenia swojego zdrowia lub życia, a także urządzenia, pojazdy, budynki i inne obiekty związane z relacją propagacji zagrożenia,
iv. jednostki decyzyjne niższego, średniego i najwyższego poziomu, sztuczne lub ludzkie, oraz moduł wspomagania decyzji stosujący przyczynowe i wyprzedzające modele decyzyjne na średnim i najwyższym poziomie,
v. zespoły pierwszego reagowania, roboty i inne urządzenia, które realizują wszystkie decyzje z zakresu zarządzania kryzysowego.

Obiekty modelu i relacje między nimi można przedstawić jako dynamiczny multigraf skierowany, z trzema rodzajami krawędzi oznaczającymi przepływ informacji, propagację i oddziaływanie zagrożeń oraz przekazywanie decyzji w postaci poleceń.

Implementacja najnowocześniejszych technik AI jest szczególnie istotna dla wsparcia komponentów (i), (ii) oraz (iv) architektury IRM DSS. Problem dostosowania AI, na podstawie wcześniejszej analizy potrzeb, został sformułowany w [Skulimowski, Bañuls, 2021] dla IRM DSS w kontekście zintegrowanego EIS poprzez następujące zasady:

1. Zidentyfikować najlepsze technologie AI do wykorzystania w EIS (w tym IRM DSS) i wdrożyć je w przedsiębiorstwie, aby zbudować odporność na zagrożenia zewnętrzne, spowodowane przez przeciwstawną AI lub nie oraz utrzymać konkurencyjność na zadowalającym poziomie.
2. Utrzymać poziom wdrożenia AI w EIS na poziomie zapewniającym co najmniej równie silną reakcję przedsiębiorstwa na wyzwania i zagrożenia tworzone przez czynniki zewnętrzne wykorzystujące również AI.

Na przykład zasada (2) wymaga, aby zdolność czujników do wykrywania włamań z inteligentnymi dronami przewyższała zdolność złośliwej/atakującej AI używanej przez intruzów do ukrywania się. Ogólna procedura projektowania IDSS obejmująca implementację

technologii in-the-loop została zaproponowana w [Skulimowski, Bañuls, 2021]. Proponowane podejście do projektowania IRM DSS dla kopalni odkrywkowej z dopasowanym do AI portfelem algorytmów ewakuacyjnych, fuzji informacji, rozumienia sceny i modeli decyzji wyprzedzających omówiona zostanie dalej. Procedura dopasowania wykorzystuje analizę badań Delphi ekspertów dziedzinowych, analizę trendów bibliometrycznych oraz skanowanie stron internetowych. Schemat funkcjonalny projektowania architektury oprogramowania w oparciu o zasady zrównywania AI zastosowany do komponentów IRM DSS (i), (ii) i (iv) dla powyższej aplikacji przedstawiono na [Rys. 69].

10.3.2 Metodyka zapewnienia gotowości IRM DSS w oparciu o najnowszy stan badań w zakresie AI

Proponowany dla KWC plan badań mający na celu zbudowanie modelu ewolucji AI i zastosowanie go w IRM DSS składa się z trzech współzależnych faz:

- Budowa wielopoziomowego modelu ewolucji sztucznej inteligencji, obejmującego pozyskiwanie i aktualizację informacji eksperckich metodą Delphi, uzupełnione badaniem trendów ilościowymi i generowaniem jakościowych scenariuszy technologicznych.
- Model potrzeb i skutków technologicznych związanych z zastosowaniem AI w IRM DSS KWC, zakładający, że charakterystyka zagrożeń przemysłowych oraz wynikająca z zagrożeń antropogenicznych (takich jak intruzje) i zjawisk naturalnych (takich jak klęski żywiołowe) jest optymalnie dopasowana do metod i narzędzi AI, które zostaną nabyte lub opracowane w celu zastosowania w IRM DSS. Modelowanie długofalowych konsekwencji implementacji IRM DSS będzie dokonywane zgodnie z zasadami sieci antycypacyjnych i przewidywanymi zmianami w otoczeniu ekonomiczno-społecznym KWC.
- Wdrożenie metod sztucznej inteligencji w IRM DSS, zdolnych do rozwiązywania rzeczywistych problemów związanych z budową odporności kopalni na zagrożenia, w szczególności tych związanych z zagrożeniami zidentyfikowanymi w rozdziale 2.5 i rozdziale 2.6, zwłaszcza z nieupoważnionymi wtargnięciami na teren KWC, włamaniami do budynków, kradzieżami, uszkodzeniami sprzętu związanymi z wyciekami paliwa lub gazu, osuwiskami i katastrofami zależnymi od pogody, takimi jak powodzie itp.

10.4 Zarządzanie ryzykiem jako element systemu IRM DSS

Koncepcja zakłada przygotowanie mechanizmu, dzięki któremu heterogeniczne zagrożenia naturalne i antropogeniczne mogą być łagodzone za pomocą kombinacji technik opartych na sztucznej inteligencji, takich jak uczenie maszynowe (ML) modeli zagrożeń, łączenie i rozumienie informacji z czujników oraz wielokryterialne procedury decyzyjne. Techniki te pozwolą uzyskać optymalne plany działania w przypadku zagrożenia, które będą przetwarzane i realizowane w czasie rzeczywistym. Działania zapobiegawcze będą podejmowane jako wyniki planowania średnio- i długoterminowego, które również wykorzystują metody sztucznej inteligencji, takie jak dynamiczne mapy zagrożeń [Seppanen, Virrantaus, 2015], prognozowanie finansowe oparte na rekurencyjnych sieciach neuronowych oraz planowanie scenariuszy katastrof naturalnych.

Inteligentny DSS, który zawiera powyższe funkcjonalności, jest w stanie rekomendować zależne od sytuacji działania, operacje i strategie ograniczania ryzyka w celu zapewnienia optymalnego poziomu bezpieczeństwa przemysłowego dla wszystkich horyzontów planowania obowiązujących w przedsiębiorstwie. Systemy takie określane jako DSS zarządzania ryzykiem przemysłowym lub DSS zarządzania odpornością na katastrofy (IRM DSS lub DRMSS [Skulimowski, Bañuls, 2021]). Projektując IRM DSS uwzględnić należy złożone problemy zarządzania informacją i wiedzą, które ostatecznie powinny doprowadzić do optymalnego rozwiązania problemów związanych z zarządzaniem ryzykiem i zminimalizowania związanych z nim strat. Aby skutecznie zintegrować zarządzanie ryzykiem na różnych poziomach, we wszystkich istotnych horyzontach planowania, od natychmiastowych środków zaradczych do planowania złożonych operacji i długoterminowych strategicznych działań budujących odporność, wykorzystać można przyczynowy model zagrożeń, ryzyka, decyzji dotyczących zarządzania kryzysowego i ich konsekwencji. Ostateczny model IRM DSS, powinien wspierać decyzje związane z zarządzaniem kryzysowym i ryzykiem na wszystkich stosownych poziomach. Optymalne decyzje wynikają ze wszystkich dostępnych informacji o zagrożeniach, takich jak dane z czujników, fakty historyczne dotyczące przeszłych zagrożeń oraz sposoby i wyniki ich obsługi. Ograniczenia dotyczące reguł decyzyjnych są narzucone przez prawo lub wewnętrzne regulacje w danym zakładzie przemysłowym. System ten powinien być rozwijany zgodnie z paradygmatem DevOps, a doświadczenie zdobyte w trakcie jego działania jest wzbogacone o połączenia z zewnętrznymi modułami AI-foresight i AI-alignment. Wspierają one zorientowany na przyszłość rozwój kolejnych wersji IRM DSS.

Kluczowe jest stworzenie architektury oprogramowania, która pozwala decydentom odpowiedzialnym za zarządzanie kryzysowe zintegrować technologie nadzoru, przetwarzania sygnałów i wspomagania decyzji w holistyczny system bezpieczeństwa przemysłowego. Kolejnym celem jest dostarczenie schematu organizacyjnego do projektowania

wyspecjalizowanych systemów informatycznych do rozwiązywania problemów odporności przemysłowej i zarządzania ryzykiem. Funkcjonalności, które wymagają intensywnego rozwoju nowych technik AI to fuzja informacji pozyskiwanych z różnych źródeł w czasie rzeczywistym oraz opracowanie optymalnych algorytmów decyzyjnych wykorzystujących te informacje. Ponadto techniki ML, w tym zarówno uczenie wzmacniające, jak i częściowo nadzorowane, mogą być stosowane w sytuacjach kryzysowych, a także do określania działań zapobiegawczych i ograniczających ryzyko.

10.4.1 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 z DevOps.

Potwierdzone w ramach badania Delphi, skoncentrowanego na DSS i IRM DSS, trendy w zakresie wykorzystania sztucznej inteligencji (AI) w projektowaniu takich systemów 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). W tym podejściu etykiety danych do szkolenia są wnioskowane na podstawie wyników wcześniejszych podobnych przypadków.
- 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 w przypadku sytuacji kryzysowych.

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).

Współczesne systemy zarządzania kryzysowego wyposażone w funkcje wspomagania decyzji wywodzą się z systemów wczesnego ostrzegania, które ewoluowały w kierunku heterogenicznego przetwarzania sygnałów w chmurze [Middleton i in., 2014]. Zaawansowane oprogramowanie do przetwarzania informacji oparte na ML pozwala programistom DSS na efektywną integrację systemów IRM z infrastrukturą teleinformatyczną przedsiębiorstwa. Dalsze najnowocześniejsze metody sztucznej inteligencji stosowane w IRM, takie jak automatyczne rozpoznawanie niebezpiecznych sytuacji w danych z monitoringu wizualnego [Foresti i in., 2002], mogą w zadowalający sposób spełniać cele bezpieczeństwa przedsiębiorstwa. Ogólny model IRM zawiera sieć modułów przetwarzania informacji, która obejmuje czujniki, fuzję informacji, wspomaganie decyzji, a także zautomatyzowane węzły decyzyjne, które tworzą graf wiedzy [Skulimowski, Łydek, 2022b], elementy te stanowią kluczową strukturę IRM DSS. Powstały model wspomagania decyzji oparty na grafach wiedzy zawiera także zespoły udzielające pierwszej pomocy, ich hierarchię wykonania działań, wiedzę o innych obiektach i wymianę tych informacji.

Te ostatnie obiekty wraz z instrukcjami bezpieczeństwa, rozkazami wykonania, oczekiwaniami i powiązaniami przyczynowymi pomiędzy nimi można przedstawić w postaci dynamicznego multigrafu skierowanego, z trzema rodzajami krawędzi oznaczającymi przepływ informacji, propagację i wpływ zagrożenia oraz przekazywanie poleceń. Taki multigraf, którego węzły odpowiadają agentom i obiektom aktywnym, jest przykładem sieci antycypacyjnej (AN) [Skulimowski, 2014], która zostanie zdefiniowana w kolejnym podrozdziale.

Problem decyzyjny, który należy rozwiązać za pomocą powyższego hybrydowego modelu sprzętu i oprogramowania, można sformułować w następujący sposób.

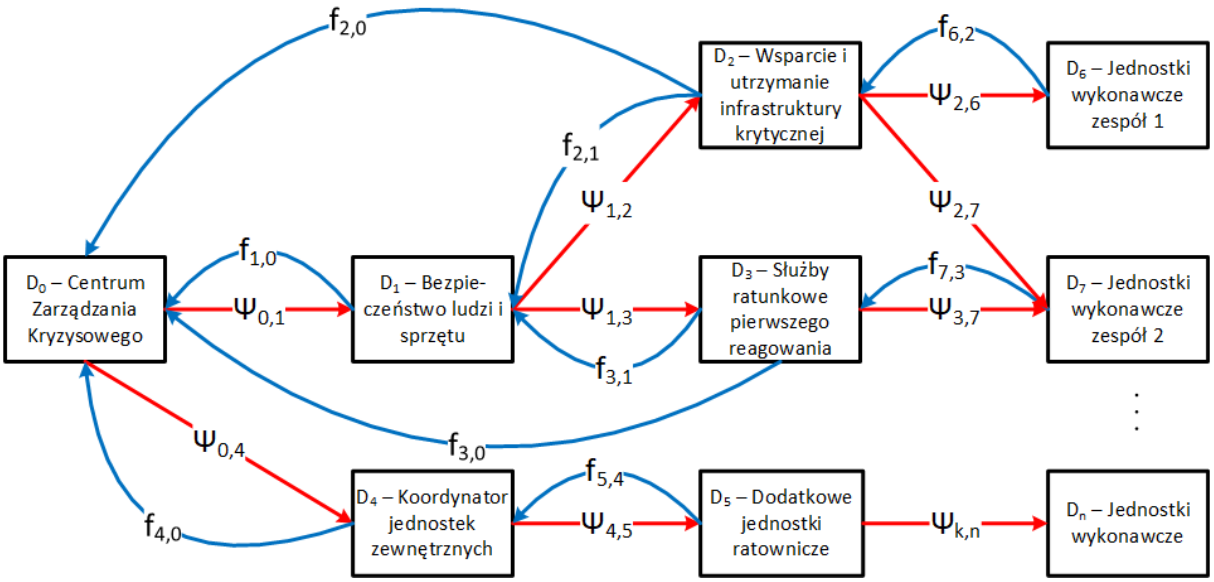
Problem 10.2. Załóżmy, że N wielokryterialnych problemów decyzyjnych O_1 ,…, O_N jest osadzonych w hierarchicznej strukturze raportowania, która tworzy acykliczny połączony digraf z jednym punktem początkowym. Każde O_i, i=1,…,N jest rozwiązywane przez

decydenta D_i. Zgodnie z ogólnymi instrukcjami zarządzania kryzysowego D_i wybiera decyzje z zadanego zbioru U_i tak, aby kryteria $F_i := (F_{i1}, \ldots, F_{ik(i)})$ 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 może chcieć, aby D_j wybrał element zbioru V_{ji} , który – według wiedzy Di – zawiera decyzje, które mogą być korzystne do przebiegu działań nadzwyczajnych. Warunek deontyczny „uj 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 10.2 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:

$$A\, f_{ji}\, B \Rightarrow B\ \Psi\ A, \tag{10.1}$$

gdzie Ψ jest przechodnie domknięcie relacji ψ_{ja} , tj. $A\ \Psi B$ jeżeli w grafie ψ_{ij} istnieje droga z A do B. Przykład sieci antycypacyjnej modelującej rzeczywistą strukturę decyzyjną w Problemie 10.2 przedstawiono poniżej [Rys. 70].



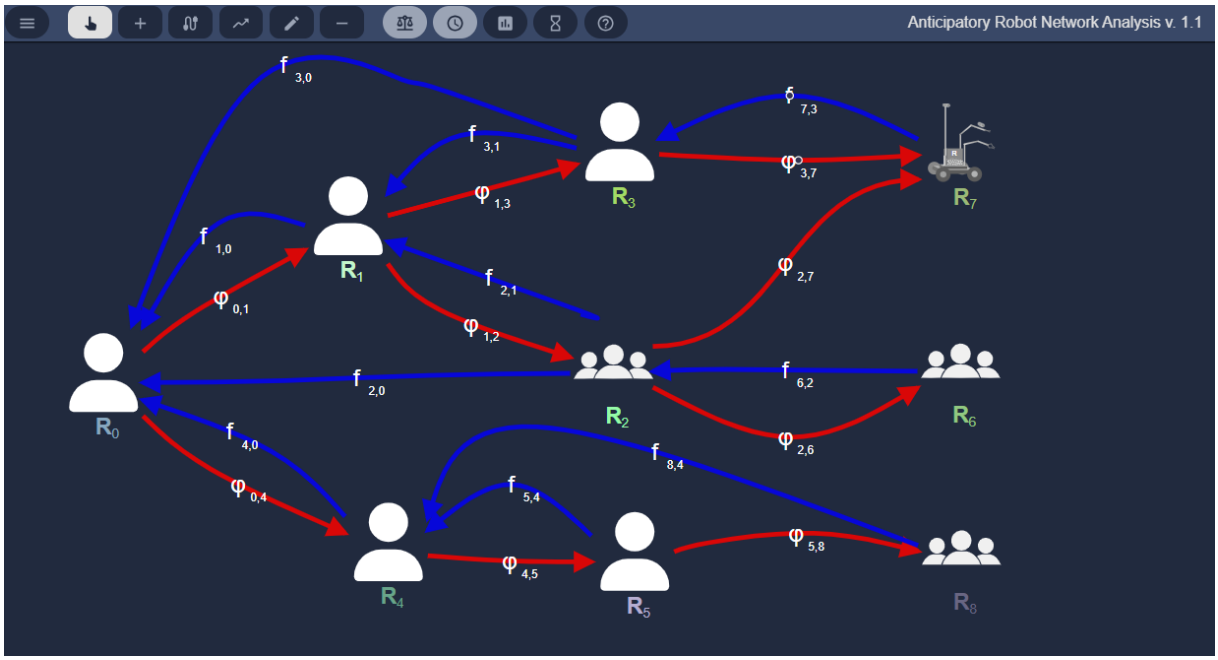
Rys. 70. Blokowy schemat sieci antycypacyjnej omawianej w Problemie 10.2.

Przykład 10.1. Rysunek [Rys. 71] poniżej przedstawia realistyczną AN odnoszącą się do rozwiązania Problemu 9.2 za pomocą IRM DSS zaprojektowanego dla kopalni wapienia w Polsce. 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 $D_i \psi_{ij} D_j$, przedstawione na [Rys. 70] 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:

$$\psi_{ij}(u_{j,,k})=\{u_{j,p1},\ldots,u_{j,p(k)}\}\subset U_j, \tag{10.2}$$

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 zgodnie do (2), 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. 71. 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 (10.3):

$$q(u_{i,k}):=\mu(V_{ji} \cap \text{argmax}\{\xi_{jot}(v):v\in \psi_{ij}(u_{i,k})\})/\mu(\psi_{ij}(u_{i,k})\}, \tag{10.3}$$

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.

Powyższe podejście do wyboru decyzji w AN nazywane jest *zasadą symulacji*. Symulacja przepływu decyzji i wynikające z niej optymalne sekwencje decyzyjne dla każdego D_i, $0 \le i \le 8$ w AN przedstawionej na [Rys. 71] pokazano w tabelach omówionych poniżej. Zasada optymalności zastosowana w algorytmie symulacji decyzji zakładała, że należy osiągnąć maksymalną liczbę zadowolonych informacji zwrotnych.

Zgodnie z wymogiem zachowania racjonalności, jeśli zbiór *Uj* jest skończony, można przyjąć, że $\mu($ Y $)$ jest krotnością *Y*. Takie podejście do wyboru decyzji w AN nazywa się *zasadą symulacji*.

Problem 10.1 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.

Symulację przepływu decyzji dla sieci antycypacyjnej wskazanej na [Rys. 71] wraz ze wskazaniem matryc decyzyjnych omówione zostaną szczegółowo poniżej.

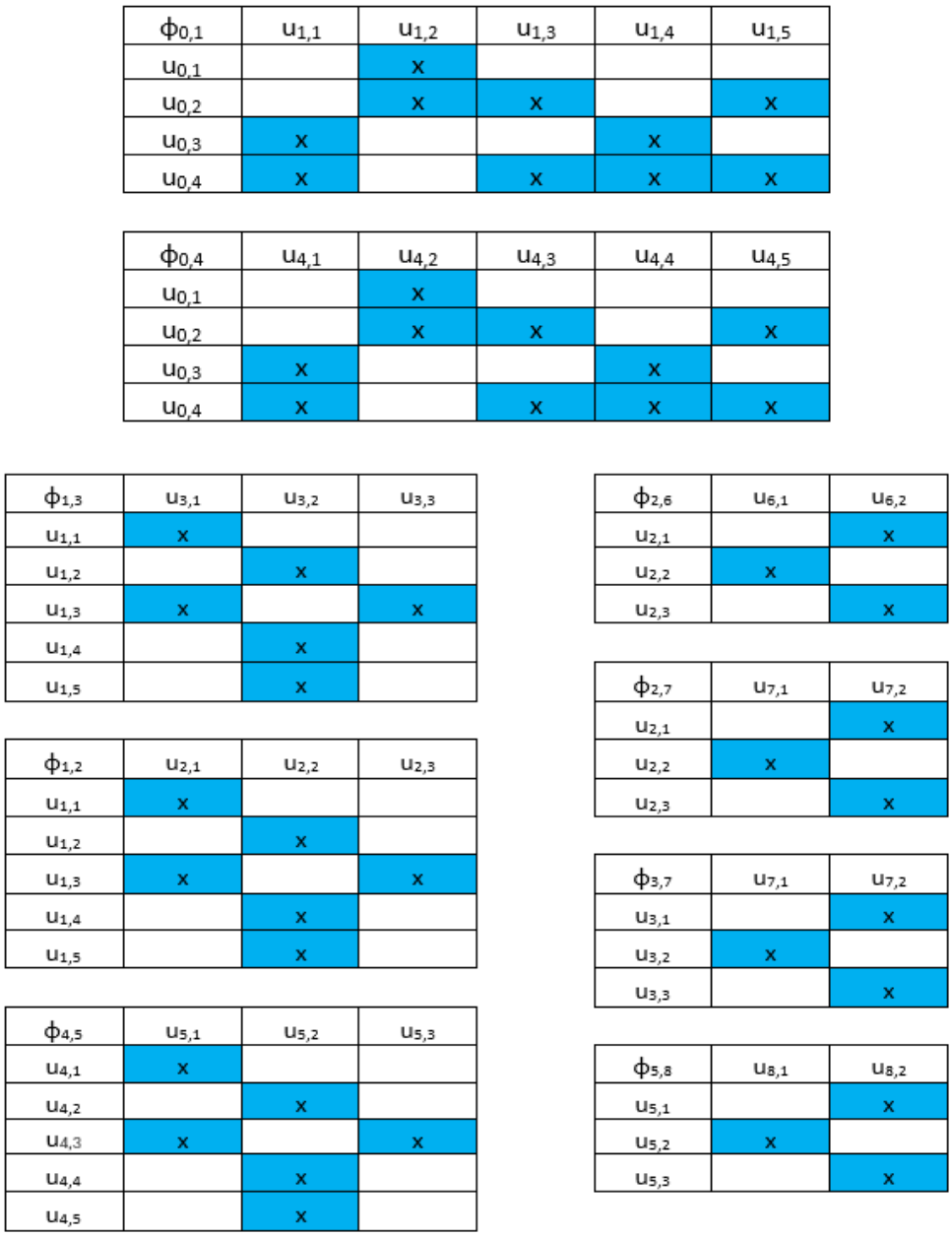
W oparciu o omówiony powyżej przykład zostały przeprowadzone symulacje działania sieci antycypacyjnej w warunkach rzeczywistych, z uwzględnieniem konkretnych decyzji i poleceń przekazywanych w łańcuchu decyzyjnym. Pierwszy etap symulacji odwzorowany w sposób graficzny na [Rys. 71] zakłada udział łącznie 8 węzłów, na które składają się jednostki wskazane w [Tab. 27].

Dodatkowo tabela zawiera liczbę i wykaz dostępnych dla jednostek $D_1 – D_8$ decyzji (akcji) do podjęcia oraz w przypadku decydenta D_0 stopień akceptacji decyzji podejmowanych na niższych poziomach.

Tab. 27. Zestawienie dostępnych decyzji dla kolejnych agentów.

Symbol	**(liczba dostępnych decyzji) Opis jednostki**	**Dostępne decyzje**
D_0	(4) Centrum Zarządzania Kryzysowego (4) Crisis Management Centre	Pożądane, Akceptowane działanie, Zbyt ryzykowne, Konieczna dodatkowa analiza **[D**esired, **A**ction **A**ccepted, **T**oo **R**isky, **A**dditional **A**nalysis **N**ecessary]
D_1	(5) Bezpieczeństwo ludzi i sprzętu (5) Human safety and health services	Stój, Idź, Czekaj, Sprawdź, Idź do połowy trasy do zagrożenia **[S**top, **G**o, **W**ait, **C**heck, **G**o **H**alfway]
D_2	(3) Wsparcie i utrzymanie infrastruktury krytycznej (3) Critical infrastructure inspection and maintenance	Stój, Idź, Czekaj **[S**top, **G**o, **W**ait]
D_3	(3) Służby ratunkowe pierwszego reagowania (3) First aid and urban rescue services	Stój, Idź, Czekaj **[S**top, **G**o, **W**ait]
D_4	(5) Koordynator jednostek zewnętrznych (5) Coordination of external units	Stój, Idź, Czekaj, Sprawdź, Idź do połowy **[S**top, **G**o, **W**ait, **C**heck, **G**o **H**alfway]
D_5	(3) Dodatkowe jednostki ratownicze (3) Supplementary emergency units	Stój, Idź, Czekaj **[S**top, **G**o, **W**ait]
D_6	(2) Jednostki wykonawcze zespół 1 (2) Response task 1 execution	Działanie, Brak działania **[A**ction, **N**o Action]
D_7	(2) Jednostki wykonawcze zespół 2 (2) Response task 2 execution (robotic)	Działanie, Brak działania **[A**ction, **N**o Action]
D_8	(2) Jednostki wykonawcze (2) Response task 3 execution	Działanie, Brak działania **[A**ction, **N**o Action]

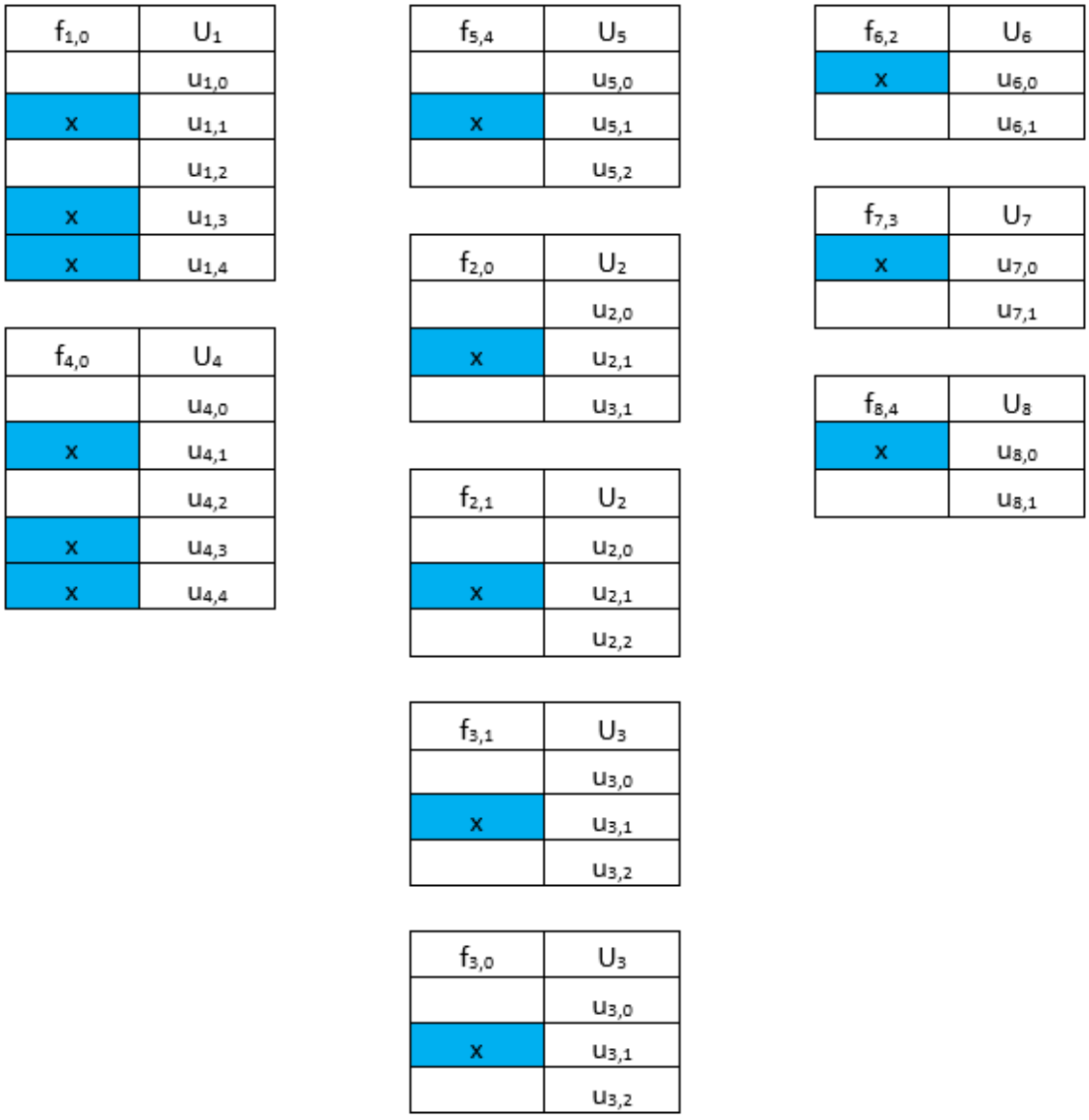
Każdy agent decyzyjny posiada przypisaną mu liczbę decyzji (realizowane na etapie budowy modelu) oraz macierz zależności budowaną w oparciu o wiedzę ekspercką i preferencje indywidulna decydentów. Macierz zależności wskazuje relacje pomiędzy decyzjami agentów pozostających we własnych strefach antycypacyjnych. Zależność jest tu następująca: wybrana decyzja agenta „B" może zostać podjęta tylko wtedy, gdy zostanie podjęta wybrana decyzja agenta „A". Jeśli więc chcemy pozwolić U_1 na podjęcie decyzji $u_{1,1}$ tylko wtedy, gdy U_0 podejmie decyzję $u_{0,1}$, musimy zaznaczyć „checkbox" przy ich skrzyżowaniu w macierzy. Szczegółowe zależności decyzyjne dla wszystkich agentów wskazane zostały na [Rys. 72].



Rys. 72. Macierze zależności decyzyjnych dla pierwszego etapu symulacji.

Poza połączeniami kauzalnymi, odwzorowującymi ciąg decyzyjny, sieć antycypacyjna składa się z połączeń stanowiących swoiste sprzężenie zwrotne, które niesie za sobą informacje

o preferencjach decydenta wyższego poziomu w stosunku do decydenta mu podległego. Krawędzie sprzężenia zwrotnego również opisane są macierzą, w której „checkbox" macierzy połączenia $f_{1,0}$ wskazuje decyzje preferowane w węźle agenta D_0 w stosunku do decyzji podejmowanych przez agenta D_1. Całość zależności sprzężeń zwrotnych dla omawianej sieci przestawia [Rys. 73].



Rys. 73. Macierz antycypacyjnych sprzężeń zwrotnych dla pierwszego etapu symulacji.

Poprawna konstrukcja i definicja zależności sieci pozwala na przejście do etapu symulacji (aplikacja weryfikuje poprawność danych). Symulacje w omawianym przypadku prowadzone były pod kątem maksymalizacji zadowolenia z informacji zwrotnej, czyli maksymalizacji osiągnięcia wyników zgodnych z oczekiwaniami decydentów (agentów) nadrzędnych. Maksymalny wynik, jaki mógł zostać osiągnięty przy prezentowanej sieci został uzyskany w czterech przypadkach. Szczegółowe dane dla najlepszy wyników prezentuje Rys. 74.

Decisions									Satisfied feedbacks										Score
U_0	U_1	U_4	U_3	U_2	U_5	U_7	U_6	U_8	$f_{1,0}$	$f_{3,1}$	$f_{3,0}$	$f_{2,0}$	$f_{6,2}$	$f_{2,1}$	$f_{5,4}$	$f_{4,0}$	$f_{8,4}$	$f_{7,3}$	
$u_{0,2}$	$u_{1,3}$	$u_{4,3}$	$u_{3,1}$	$u_{2,1}$	$u_{5,1}$	$u_{7,2}$	$u_{6,2}$	$u_{8,2}$	-	-	-	-	-	-	-	-	-	-	0.00
...	...	...	...	...	...	...	...	...											
$u_{0,1}$	$u_{1,2}$	$u_{4,2}$	$u_{3,2}$	$u_{2,2}$	$u_{5,2}$	$u_{7,1}$	$u_{6,1}$	$u_{8,1}$	$u_{1,2}$	$u_{3,2}$	$u_{3,2}$	$u_{2,2}$	$u_{6,1}$	$u_{2,2}$	$u_{5,2}$	$u_{4,2}$	$u_{8,1}$	$u_{7,1}$	10.00
$u_{0,2}$	$u_{1,2}$	$u_{4,2}$	$u_{3,2}$	$u_{2,2}$	$u_{5,2}$	$u_{7,1}$	$u_{6,1}$	$u_{8,1}$	$u_{1,2}$	$u_{3,2}$	$u_{3,2}$	$u_{2,2}$	$u_{6,1}$	$u_{2,2}$	$u_{5,2}$	$u_{4,2}$	$u_{8,1}$	$u_{7,1}$	10.00
$u_{0,3}$	$u_{1,4}$	$u_{4,4}$	$u_{3,2}$	$u_{2,2}$	$u_{5,2}$	$u_{7,1}$	$u_{6,1}$	$u_{8,1}$	$u_{1,4}$	$u_{3,2}$	$u_{3,2}$	$u_{2,2}$	$u_{6,1}$	$u_{2,2}$	$u_{5,2}$	$u_{4,2}$	$u_{8,1}$	$u_{7,1}$	10.00
$u_{0,4}$	$u_{1,4}$	$u_{4,4}$	$u_{3,2}$	$u_{2,2}$	$u_{5,2}$	$u_{7,1}$	$u_{6,1}$	$u_{8,1}$	$u_{1,4}$	$u_{3,2}$	$u_{3,2}$	$u_{2,2}$	$u_{6,1}$	$u_{2,2}$	$u_{5,2}$	$u_{4,2}$	$u_{8,1}$	$u_{7,1}$	10.00

Rys. 74. Wyniki symulacji dla pierwszego etapu (zrzut z ekranu symulacji).

W przypadku uzyskania rozwiązania dla sieci o zadanych parametrach przeprowadzić można również symulację sekwencji podejmowanych decyzji w funkcji czasu. Zestawienie takie dla jednego z wyników dających rozwiązanie, zaprezentowano na Rys. 75.

Solution method: Decision sequence simulation

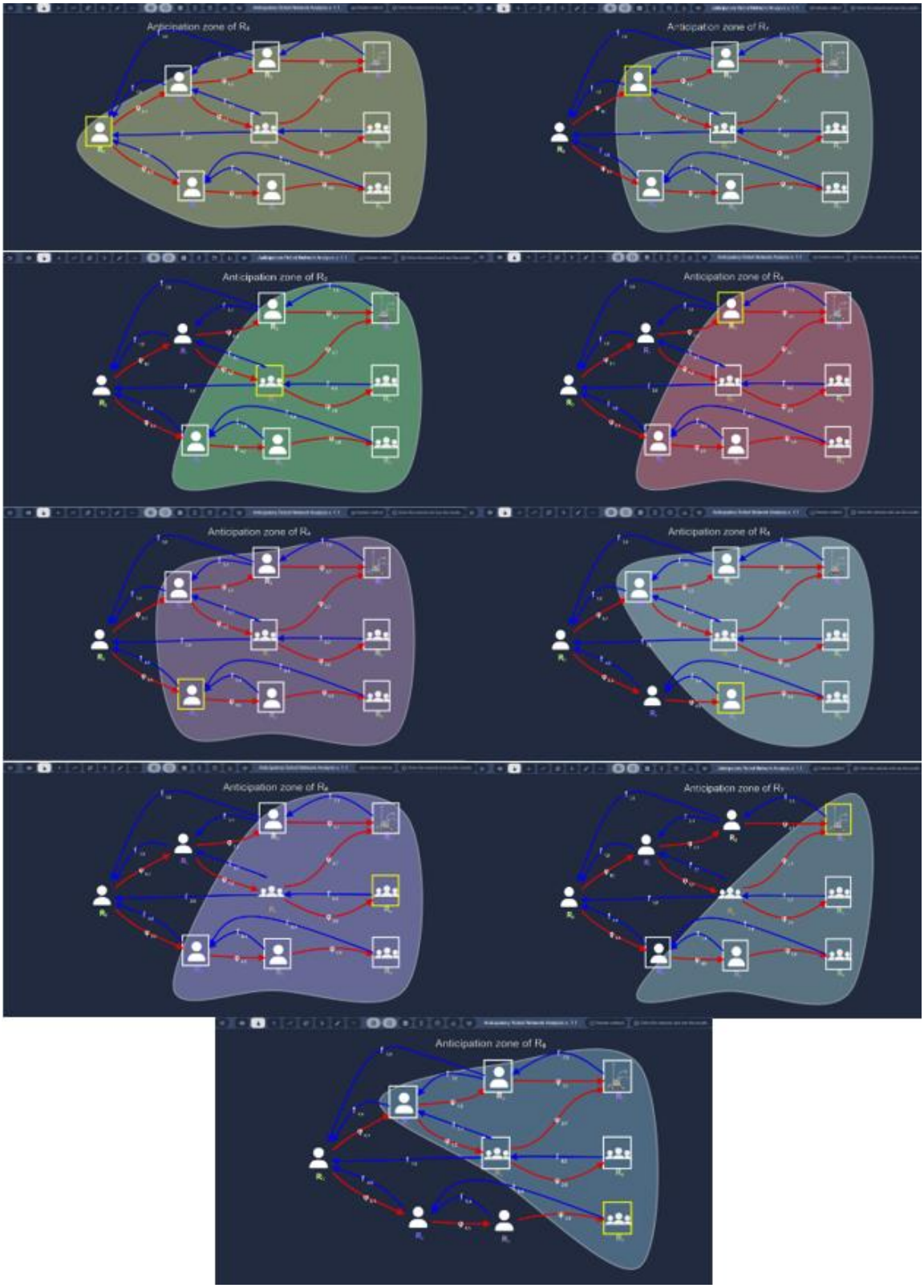
decisions

U_0	U_1	U_2	U_3	U_4	U_5	U_6	U_7	U_8
t_0=1.12	t_1=1.30	t_2=1.39	t_3=1.97	t_4=1.23	t_5=5.00	t_6=3.31	t_7=7.24	t_8=7.72
$u_{0,1}$	$u_{1,2}$	$u_{2,2}$	$u_{3,2}$	$u_{4,2}$	$u_{5,2}$	$u_{6,1}$	$u_{7,1}$	$u_{8,1}$

Rys. 75 Sekwencja decyzji dla poprawnego rozwiązania Przykładu 10.1

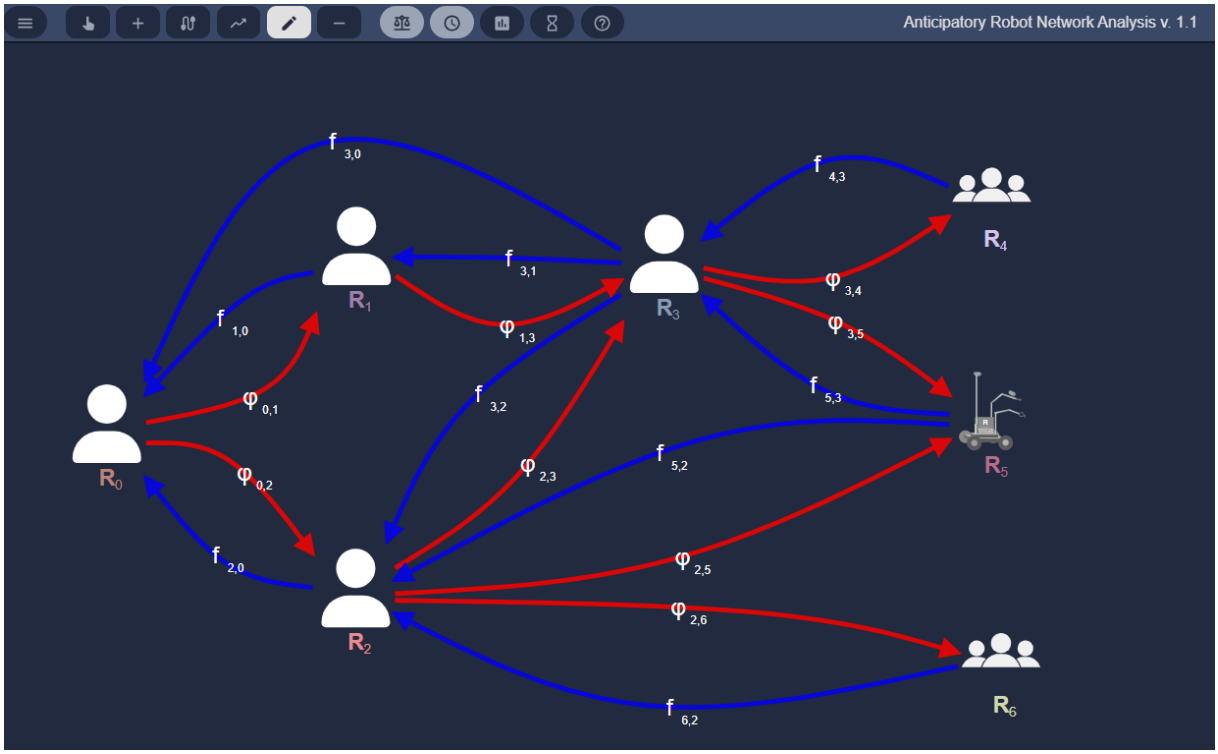
Sieci antycypacyjne odwzorowuje model, w którym uwzględniane są nie tylko aktualny stan systemu, ale również potencjalne przyszłe stany na podstawie przewidywań i symulacji. Pojęcie strefa antycypacyjna odnosi się do zakresu, w którym system antycypacyjny „wyprzedza" bieżące wydarzenia, uwzględniając potencjalne przyszłe zdarzenia i ich wpływ na decyzje lub działania w czasie rzeczywistym. Strefa antycypacyjna w sieci to inaczej przestrzeń przewidywania, czyli zakres potencjalnych przyszłych stanów sieci, które są brane pod uwagę w procesie decyzyjnym ograniczony przez horyzont prognostyczny. W symulacjach praktycznych może obejmować różne scenariusze, takie jak awarie, zmiany parametrów systemu lub działania zewnętrzne. Informacje przetwarzane w obrębie takiej strefy mają wpływ na decyzje, ponieważ są na bieżąco wykorzystywane do podejmowania decyzji w czasie rzeczywistym, uwzględniając nie tylko obecne dane, ale także przewidywane konsekwencje działań. Wykorzystywana do prowadzenia symulacji aplikacja pozwala na budowanie stref antycypacyjnych zgodnie z potrzebami użytkowania, a wynik umożliwiając dynamiczną adaptację systemu poprzez modyfikację zakresy decyzji lub działań w zależności od przewidywanych przyszłych scenariuszy. Uwzględnienie strefy antycypacyjnej pomaga zminimalizować ryzyko niepożądanych zdarzeń (np. awarii, opóźnień) poprzez wcześniejsze przygotowanie systemu. Dzięki tej funkcjonalności strefa antycypacyjna to istotny element

wspomagający procesy decyzyjne. Na Rys. 76 zaprezentowano, w sposób zbiorczy strefy antycypacyjne dla poszczególnych węzłów decyzyjnych omawianej sieci.



Rys. 76. Strefy antycypacyjne poszczególnych węzłów decyzyjnych dla Przykładu 10.1.

Zaprezentowana na Rys. 71 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. 77].



Rys. 77. Drugi etap symulacji wykorzystania sieci antycypacyjnej.

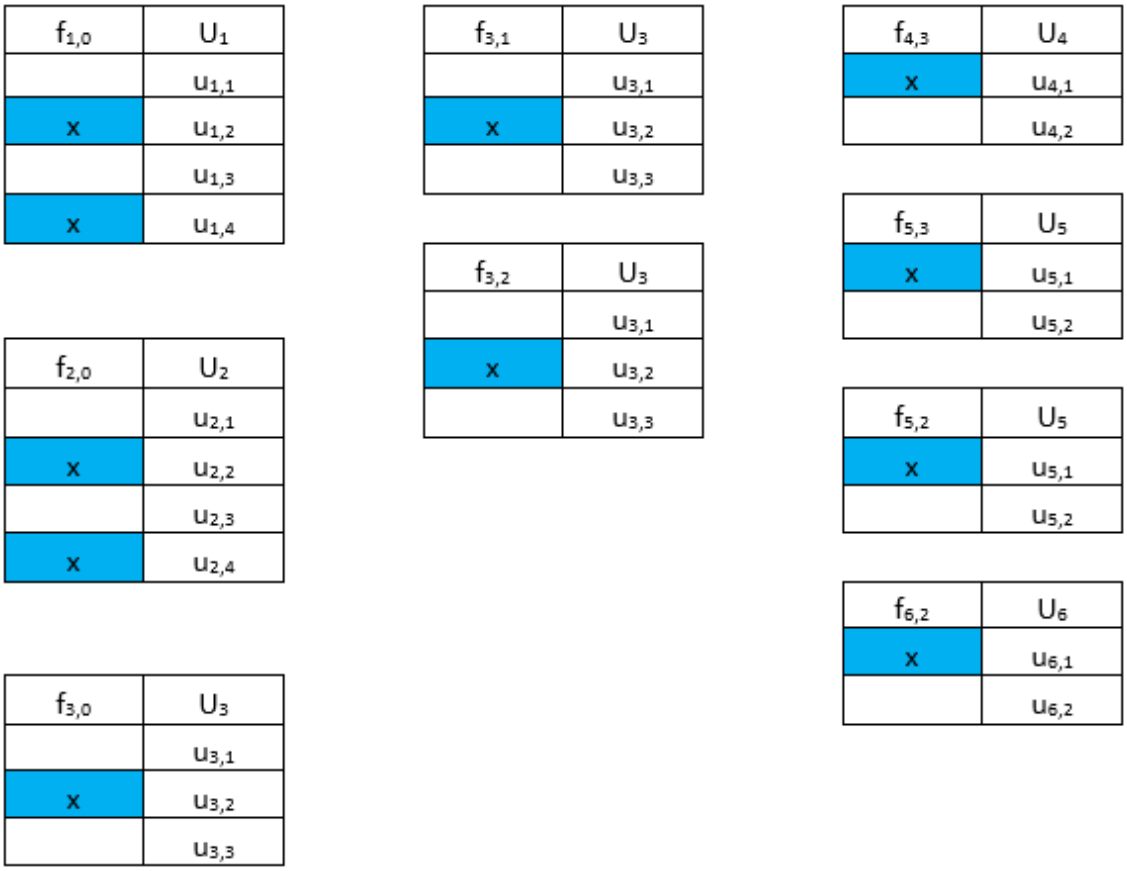
Analogicznie jak w pierwszym etapie przygotowana została tabela z wykazem decyzji oraz akceptowalnych przez agenta D_0 akcji realizowanych na niższych szczeblach decyzyjnych [Tab. 28].

Tab. 28. Zestawienie dostępnych decyzji dla kolejnych agentów.

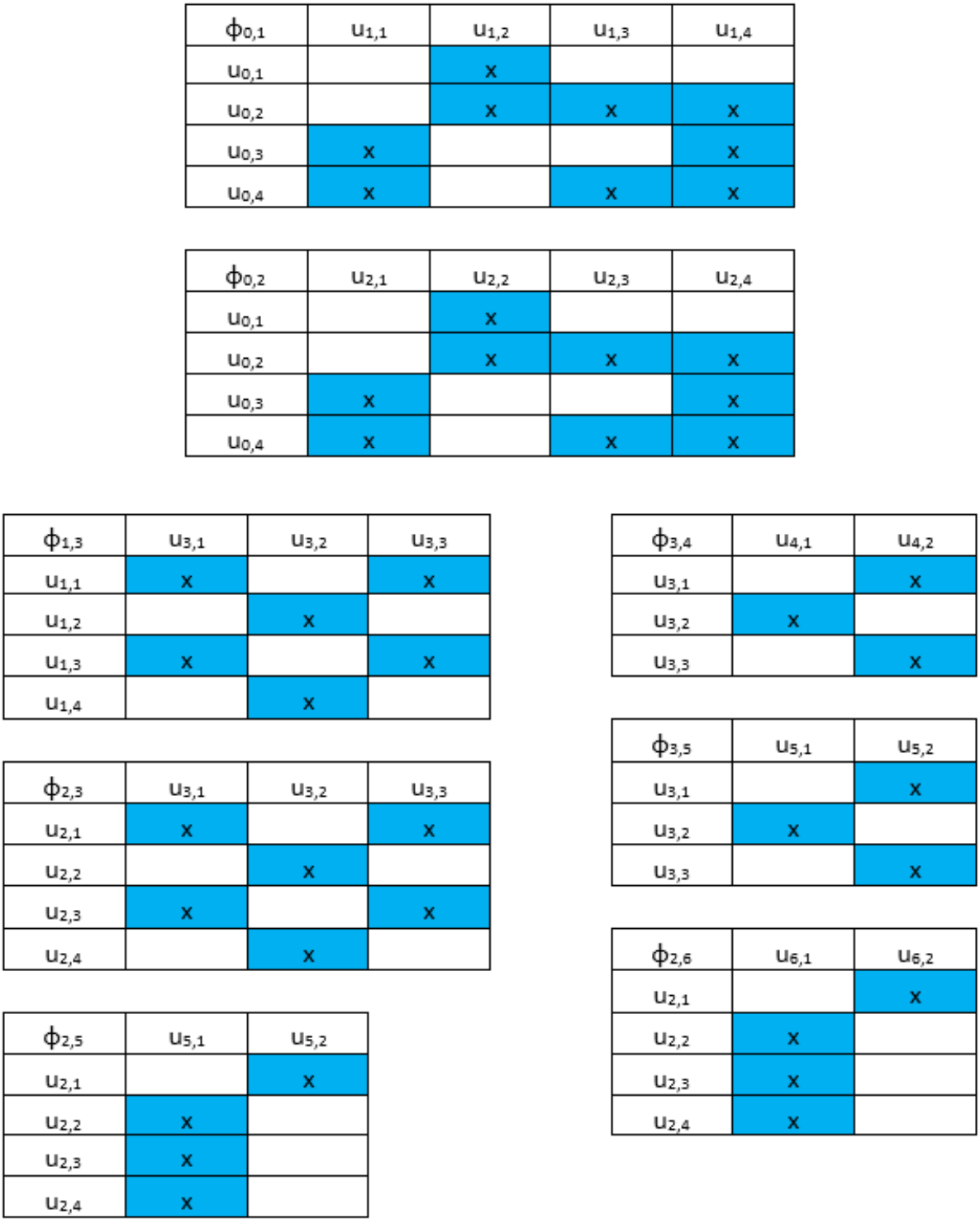
Symbol	**(liczba dostępnych decyzji) Opis jednostki**	**Dostępne decyzje**
D_0	(4) Centrum Zarządzania Kryzysowego (4) Crisis Management Centre	Pożądane, Akceptowane działanie, Zbyt ryzykowne, Konieczna dodatkowa analiza **[D**esired, **A**ction **A**ccepted, **T**oo **R**isky, **A**dditional **A**nalysis **N**ecessary]

Symbol	(liczba dostępnych decyzji) Opis jednostki	Dostępne decyzje
D_1	(4) Bezpieczeństwo ludzi i sprzętu (4) Human safety and health services	Stój, Idź, Sprawdź, Konieczna eskalacja **[S**top, **G**o, **C**heck, **N**ecessary **E**scalation]
D_2	(4) Koordynator jednostek zewnętrznych (4) Coordination of external units	Stój, Idź, Sprawdź, Konieczna eskalacja **[S**top, **G**o, **C**heck, **N**ecessary **E**scalation]
D_3	(3) Służby ratunkowe pierwszego reagowania (3) First aid and urban rescue services	Stój, Idź, Czekaj **[S**top, **G**o, **W**ait]
D_4	(2) Jednostki wykonawcze zespół 1 (2) Response task 1 execution	Działanie, Brak działania **[A**ction, **N**o **A**ction]
D_5	(2) Jednostki wykonawcze zespół 2 (robot) (2) Response task 2 execution (robotic)	Działanie, Brak działania **[A**ction, **N**o **A**ction]
D_6	(2) Jednostki wykonawcze zespół 2 (2) Response task 3 execution	Działanie, Brak działania **[A**ction, **N**o **A**ction]

Z macierzy dostępnych decyzji wyeliminowane zostały decyzje mniej stanowcze typu „Idź do połowy” („Go Halfway”) czy „Czekaj” („Wait”) i zastąpione decyzjami „Konieczna eskalacja” („Necessary Escalation”) [Rys. 78, Rys. 79]. Takie podejście ma w założeniu zwiększyć skuteczność prowadzonych działań poprzez zmniejszenie ilości decyzji nieprowadzących do bezpośredniego zaangażowania jednostek wykonawczych w akcję ratowniczą.



Rys. 78. Macierze antycypacyjnych sprzężeń zwrotnych dla drugiego etapu symulacji.



Rys. 79. Macierze zależności decyzyjnych dla drugiego etapu symulacji.

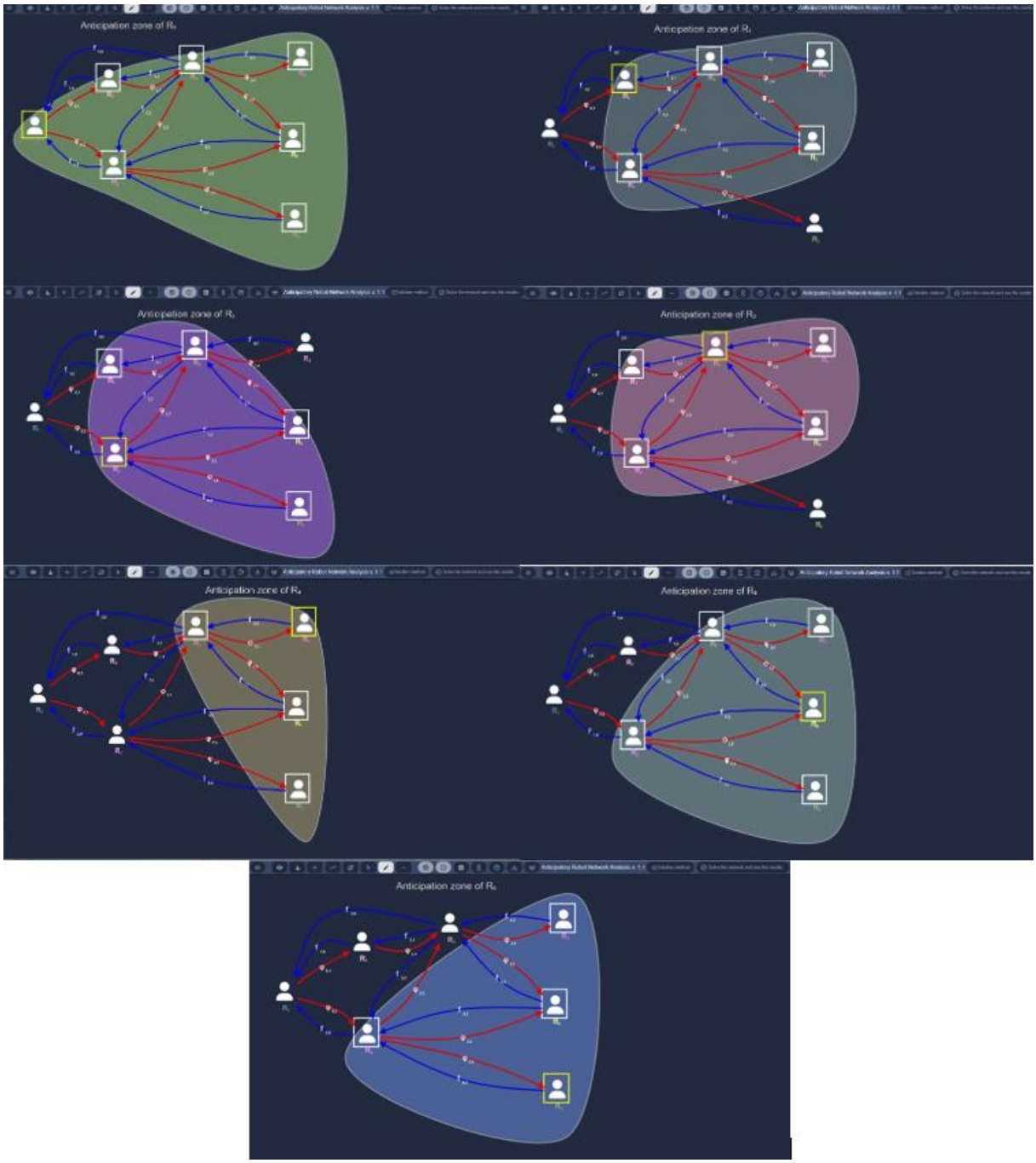
Wyniki symulacji przeprowadzonej analogicznie jak w etapie pierwszym według zasady maksymalizacji osiągnięcia wyników zgodnych z oczekiwaniami decydentów wyższych szczebli zaprezentowane zostały na Rys. 80. Dzięki zwiększeniu ilości poleceń o charakterze

kategorycznym wynik symulacji zawierają więcej satysfakcjonujących wyników, z pełną dostępną przy tej ilości agentów punktacją.

Decisions							Satisfied feedbacks									Score
U_0	U_1	U_2	U_3	U_6	U_5	U_4	$f_{1,0}$	$f_{2,0}$	$f_{3,1}$	$f_{3,2}$	$f_{6,2}$	$f_{5,3}$	$f_{5,2}$	$f_{4,3}$	$f_{3,0}$	
$u_{0,3}$	$u_{1,1}$	$u_{2,1}$	$u_{3,1}$	$u_{6,2}$	$u_{5,2}$	$u_{4,2}$	-	-	-	-	-	-	-	-	-	0.00
$u_{0,3}$	$u_{1,1}$	$u_{2,1}$	$u_{3,1}$	$u_{6,2}$	$u_{5,2}$	$u_{4,2}$	-	-	-	-	-	-	-	-	-	0.00
$u_{0,4}$	$u_{1,1}$	$u_{2,1}$	$u_{3,1}$	$u_{6,2}$	$u_{5,2}$	$u_{4,2}$	-	-	-	-	-	-	-	-	-	0.00
$u_{0,4}$	$u_{1,1}$	$u_{2,1}$	$u_{3,1}$	$u_{6,2}$	$u_{5,2}$	$u_{4,2}$	-	-	-	-	-	-	-	-	-	0.00
$u_{0,4}$	$u_{1,1}$	$u_{2,1}$	$u_{3,1}$	$u_{6,2}$	$u_{5,2}$	$u_{4,2}$	-	-	-	-	-	-	-	-	-	0.00
$u_{0,4}$	$u_{1,1}$	$u_{2,1}$	$u_{3,1}$	$u_{6,2}$	$u_{5,2}$	$u_{4,2}$	-	-	-	-	-	-	-	-	-	0.00
$u_{0,1}$	$u_{1,2}$	$u_{2,2}$	$u_{3,2}$	$u_{6,1}$	$u_{5,1}$	$u_{4,1}$	$u_{1,2}$	$u_{2,2}$	$u_{3,2}$	$u_{3,2}$	$u_{6,1}$	$u_{5,1}$	$u_{5,1}$	$u_{4,1}$	$u_{3,2}$	9.00
$u_{0,2}$	$u_{1,2}$	$u_{2,2}$	$u_{3,2}$	$u_{6,1}$	$u_{5,1}$	$u_{4,1}$	$u_{1,2}$	$u_{2,2}$	$u_{3,2}$	$u_{3,2}$	$u_{6,1}$	$u_{5,1}$	$u_{5,1}$	$u_{4,1}$	$u_{3,2}$	9.00
$u_{0,2}$	$u_{1,2}$	$u_{2,4}$	$u_{3,2}$	$u_{6,1}$	$u_{5,1}$	$u_{4,1}$	$u_{1,2}$	$u_{2,4}$	$u_{3,2}$	$u_{3,2}$	$u_{6,1}$	$u_{5,1}$	$u_{5,1}$	$u_{4,1}$	$u_{3,2}$	9.00
$u_{0,2}$	$u_{1,4}$	$u_{2,2}$	$u_{3,2}$	$u_{6,1}$	$u_{5,1}$	$u_{4,1}$	$u_{1,4}$	$u_{2,2}$	$u_{3,2}$	$u_{3,2}$	$u_{6,1}$	$u_{5,1}$	$u_{5,1}$	$u_{4,1}$	$u_{3,2}$	9.00
$u_{0,2}$	$u_{1,4}$	$u_{2,4}$	$u_{3,2}$	$u_{6,1}$	$u_{5,1}$	$u_{4,1}$	$u_{1,4}$	$u_{2,4}$	$u_{3,2}$	$u_{3,2}$	$u_{6,1}$	$u_{5,1}$	$u_{5,1}$	$u_{4,1}$	$u_{3,2}$	9.00
$u_{0,3}$	$u_{1,4}$	$u_{2,4}$	$u_{3,2}$	$u_{6,1}$	$u_{5,1}$	$u_{4,1}$	$u_{1,4}$	$u_{2,4}$	$u_{3,2}$	$u_{3,2}$	$u_{6,1}$	$u_{5,1}$	$u_{5,1}$	$u_{4,1}$	$u_{3,2}$	9.00
$u_{0,4}$	$u_{1,4}$	$u_{2,4}$	$u_{3,2}$	$u_{6,1}$	$u_{5,1}$	$u_{4,1}$	$u_{1,4}$	$u_{2,4}$	$u_{3,2}$	$u_{3,2}$	$u_{6,1}$	$u_{5,1}$	$u_{5,1}$	$u_{4,1}$	$u_{3,2}$	9.00

Rys. 80. Wyniki symulacji dla drugiego etapu (zrzut z ekranu symulacji).

Również w przypadku symulacji przeprowadzonej dla procesu eskalacji zdarzeń wyznaczone zostały strefy antycypacyjne odwzorowujące rzeczywiste relacje poszczególnych uczestników procesu decyzyjnego. Zbiorcze zestawienie zastosowanych stref antycypacyjnych przedstawia Rys. 81.



Rys. 81. Strefy antycypacyjne poszczególnych węzłów decyzyjnych dla eskalacji Przykładu 10.1

11 Implementacja problemu ewakuacji

11.1 Opis interfejsu – koncepcja

Interfejs przygotowany w oparciu o przedstawione i szczegółowo omówione w powyższych rozdziałach założenia powstał przy użyciu środowiska Matlab. Dzięki dużej funkcjonalności, Matlab może być z powodzeniem wykorzystany jako interaktywne środowisko do wykonywania obliczeń naukowych i inżynierskich, oraz do tworzenia wielowymiarowych symulacji, również realizowanych na zadanych podkładach graficznych. Taka właśnie idea przyświeca opisanemu w dalszej części interfejsowi programistycznemu: umożliwić symulację tras ewakuacji maszyn, których parametry własne, i parametr ruchu mogą być definiowane w trakcie symulacji, zaś sama symulacja prowadzona będzie w warunkach zbliżonych do rzeczywistych, między innymi dzięki możliwości wczytania aktualnej mapy terenu. Oczekiwania stawiane na etapie tworzenia wytycznych zakładają również możliwość wskazywania aktualnych pozycji maszyn przeznaczonych do ewakuacji, wskazywania miejsc docelowych, czyli tzw. punktów bezpiecznych, wyznaczania tras (i tras alternatywnych) z uwzględnieniem ich parametrów dodatkowych, jak np. nośność, przepustowość, ilość pasów ruchu czy też przeszkód, które pojawiają się na drodze i mogą wpływać na parametry drogi.

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.

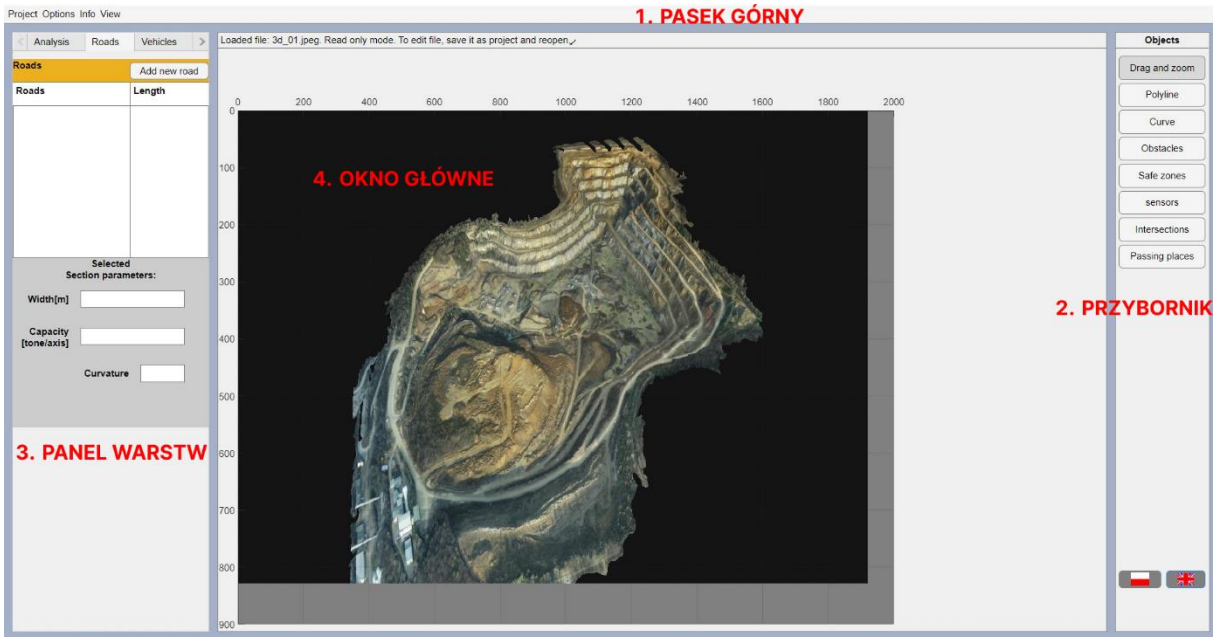
Dalsza części pracy zawiera szczegółowy opis interfejsu, wraz załączonymi zrzutami z ekranu, tworzonymi w trakcie symulacji oraz opis kolejnych etapów symulacji.

11.1.1 Ogólna struktura interfejsu:

Przedstawiona w tym rozdziale implementacja aplikacji do symulacji ewakuacji stanowi przykładowy prototyp modułu IRM DSS, wybrany na podstawie analizy potrzeb KWC przedstawionej w [rozdział 2].

Widok główny aplikacji [Rys. 82] oferuje dostęp do czterech podstawowych elementów:

1. paska górnego,
2. przybornika,
3. panelu warstw mapy terenu,
4. okna głównego.



Rys. 82. Okno główne interfejsu aplikacji symulacyjnej w środowisku Matlab.

Zastosowane podejście zakłada pracę na warstwach, mogących być edytowane i przetwarzane niezależenie od siebie, ale również współdzielących niektóre elelementy, w zależności od potrzeb i zastosowanego w danej sytuacji algorytmu. Rozwiązanie takie daje operatorowi (decydentowi, szukającemu rozwiązania rzeczywistego problemu) dużą elastyczność we wprowadzaniu danych, a tym samym zapewnia odwzorowanie sytuacji rzeczywistej. W prezentowanej wersji, program oferuje możliwość pracy na następujących warstwach:

1. warstwa podkładowa (tło), którą może być fotografia lotnicza lub statyczna mapa terenu,
2. warstwa dróg (tras),
3. warstwa pojazdów (maszyn/obiektów),
4. warstwa przeszkód,
5. warstwa zagrożeń (jedna lub więcej),
6. warstwa miejsc bezpiecznych.

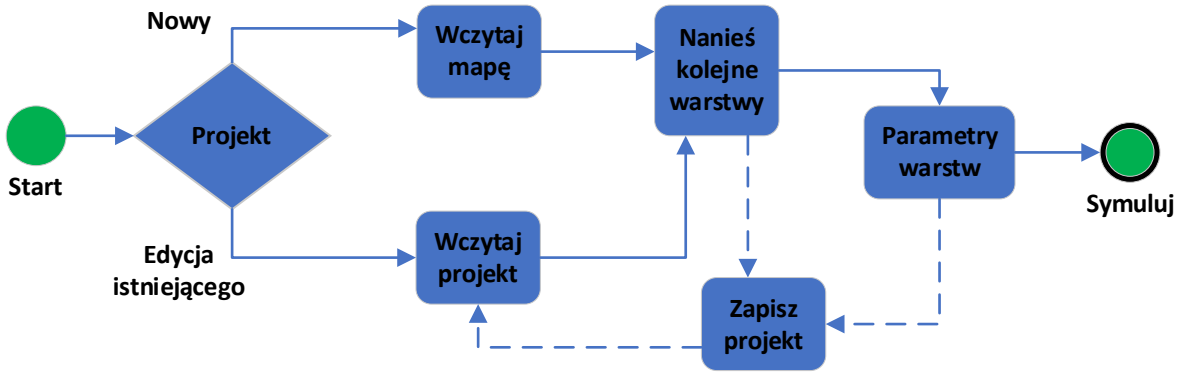
Każda z warstw tworzona jest w sposób niezależny od pozostałych, a kolejność ich nanoszenia na tło zależy od preferencji operatora budującego model.

11.1.2 Definiowanie konfiguracji modelu

Symulacja rozpoczyna się od wczytania do interfejsu mapy tła, będącej podkładem do dalszej pracy. Rozmiar i dokładność mapy w sposób oczywisty determinuje wiarygodność tworzonego modelu, ale również komfort pracy operatora nanoszącego kolejne warstwy. Jest to szczególnie widoczne, np. w sytuacji uwzględniania przeszkód na drodze z dwoma pasami ruchu, kiedy przeszkoda nie zamyka pełnej przepustowości, a jedynie zawęża drogę do jednego pasa, co w konsekwencji wymusza konieczność kolejkowania przejazdu lub wyszukiwania tras alternatywnych.

Z założenia interfejs umożliwia wczytywanie zdjęcia lub mapy podkładowej zagrożonego terenu i stworzenie na tej podstawie mapy cyfrowej 2D i 3D. Dane dotyczące współrzędnych mapy (wysokość względna i bezwzględna, współrzędne geograficzne etc.) są edytowalne w odpowiedniej zakładce paska górnego. Możliwa jest także praca na zwykłym pliku graficznym, wtedy jednostką długości jest piksel. To drugie rozwiązanie - chociaż mniej dokładne - jest bardziej praktyczne dzięki szybkości tworzenia modelu i łatwości jego obsługi. Błędy, które mogą pojawić się przy wykorzystaniu modelu 2D, tj. bez uwzględnienia różnic w wysokościach, w niektórych sytuacjach są nieistotne. O możliwości pominięcia trzeciego wymiaru mapy bez, lub z minimalną stratą dla wyniku końcowego prowadzonych obliczeń decyduje wiedza ekspercka użytkownika, .

Po wczytaniu i skonfigurowaniu pliku mapy podkładowej, użytkownik może rozpocząć nanoszenie kolejnych warstw zgodnie bieżącymi potrzebami.
W ramach podstawowych funkcjonalności interfejs pracuje w oparciu o pliki projektu o rozszerzeniu „*.czat”. Możliwe jest zapisanie i wczytanie wcześniej przygotowanych map wraz z naniesionymi już warstwami (trasy, przeszkody, etc.) w dowolnym momencie. Tak zdefiniowany schemat funkcjonalny prezentuje [Rys. 83].

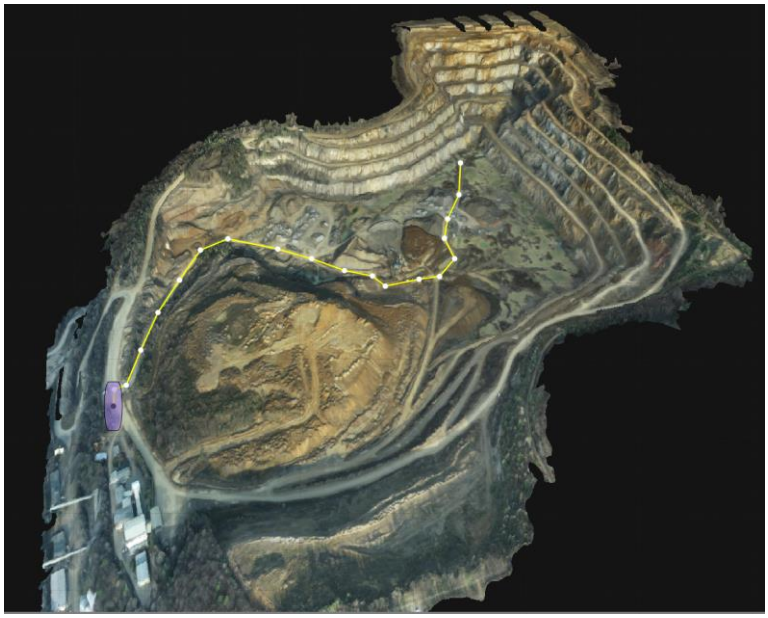


Rys. 83. Schemat blokowy konstrukcji modelu symulacji.

11.1.3 Nanoszenie kolejnych warstw modelu

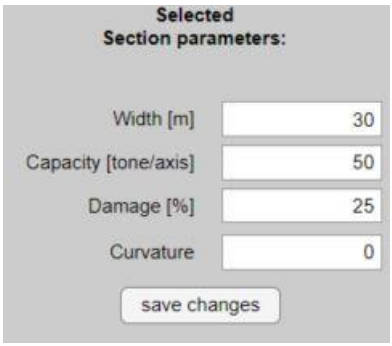
Kolejność tworzenia warstw nanoszonych na przygotowaną mapę tła nie jest narzucona. Poniższe omówienie jest zgodne z praktykowaną logiką postępowania, która zależy jednak od decyzji.

Budowa warstwy dróg (tras), odbywa się poprzez wskazywanie na mapie kolejnych punktów końcowych odcinków trasy, które aplikacja automatycznie łączy rysując trasę przemieszczania się pojazdu od punktu startowego do miejsca zdefiniowanego jako punkt końcowy. Punktem takim jest zwykle miejsce zakwalifikowane jako bezpieczne. Powstaje w ten sposób trasa aproksymowana przez łamaną [Rys. 84].



Rys. 84. Przykład tworzenia trasy ruchu pojazdu.

Dodatkową funkcjonalnością jest możliwość edycji przebiegu odcinków trasy (pomiędzy kolejnymi punktami) i parametryzowanie odcinków trasy poprzez zdefiniowanie ich szerokości, nośności, ewentualnych przeszkód czy uszkodzeń oraz krzywizny, co jest istotne w przypadku ostrych zakrętów [Rys. 85]. Ponadto odcinki trasy mogą łączyć się na skrzyżowaniach pod pewnym kątem, który można definiować w zakresie od -90 do 90 stopni. Pozostawienie wartości domyślnej 0 stopni interpoluje odcinek między punktami jako fragment linii prostej. Można też aproksymować fragment trasy jako część łuku okręgu. W tym wypadku w punktach końcowych fragmentu trasy należy zdefiniować kąty pomiędzy prostą styczną do okręgu, a osią układu współrzędnych. Aplikacja wyznaczy wtedy parametry okręgu i połączy punkty łukiem. Przeciwne wartości kąta zgięcia aproksymują ten fragment jako łuk tego samego okręgu, tyle że o promieniu zwróconym w przeciwnym kierunku.

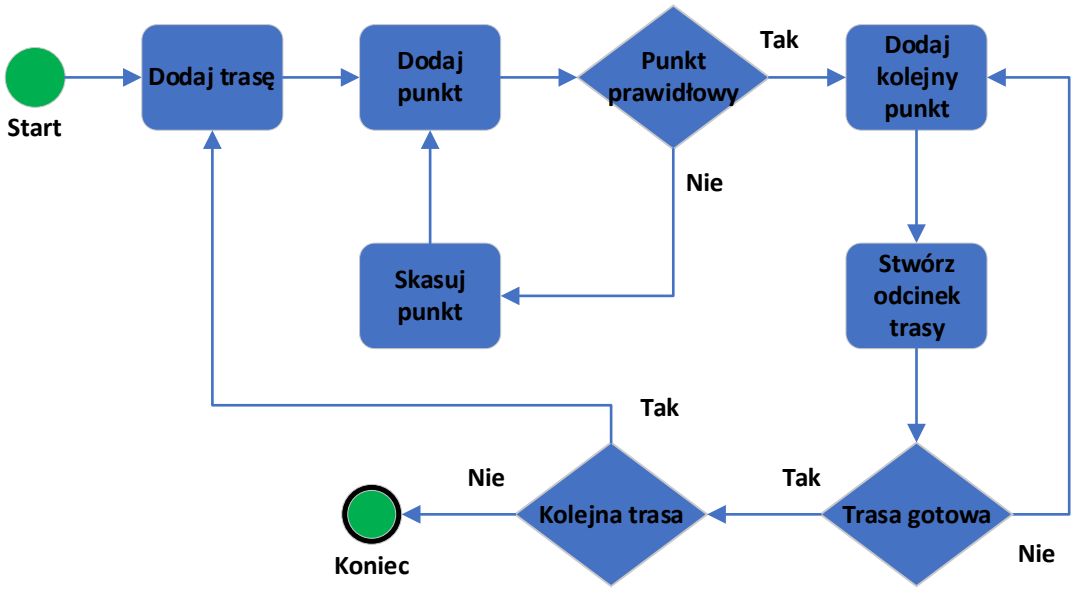


Rys. 85. Okno parametrów trasy.

Ostatnio utworzony punkt trasy można usunąć przyciskiem „cofnij” w prawym rogu paska informacji. Wtedy automatycznie usuwa się też ostatni utworzony odcinek trasy kończący się w usuniętym punkcie [Rys. 87]. Dodawanie kolejnej trasy zainicjować można w dowolnym momencie, poprzez menu boczne, w ten sam sposób można przejść do edycji trasy już istniejącej. W celu ułatwienia obsługi różne trasy można łączyć, a także wprowadzać informacje, że wybrane fragmenty różnych tras pokrywają się ze sobą.

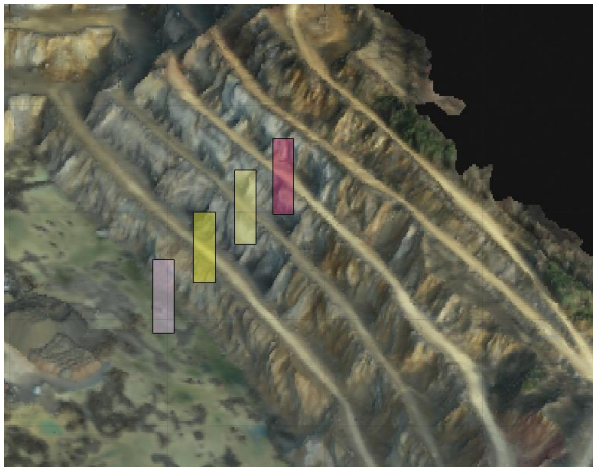
Rys. 86. Propozycja 3 tras ewakuacji, ze wskazaniem miejsc bezpiecznych oraz obliczanie długości tras.

Ewentualne dalsze wykorzystanie przygotowanych w aplikacji tras możliwe jest poprzez wyeksportowanie danych trasy do pliku w popularnym formacie *.xlsx lub poprzez zapisanie całego projektu.



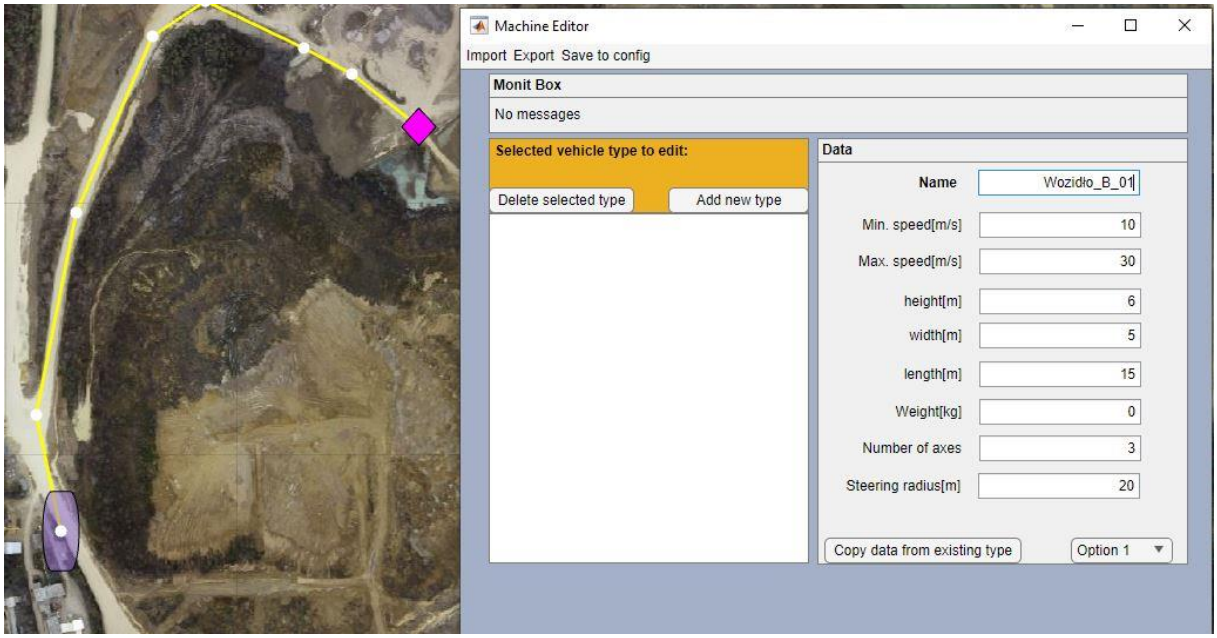
Rys. 87. Schemat tworzenia trasy pojazdu.

Tworzenie i edycja przeszkód dostępna jest poprzez zakładkę „Obstacles” w panelu warstw. Po naciśnięciu przycisku „Add new obstacle”, klikając w dwa punkty na mapie, użytkownik ustanawia dwa przeciwległe wierzchołki prostokąta symbolizujące przeszkodę [Rys. 88]. Możliwe jest usunięcie przeszkody („delete obstacle”) bądź jej wyłączenie dla danej symulacji, poprzez odznaczenie pola „active”. Liczba przeszkód możliwych do naniesienia nie jest limitowana. Poniższy rysunek przedstawia przykład oznaczenia przeszkody będącej konsekwencją osuwiska, które swoim zasięgiem objęło kilka poziomów eksploatacyjnych, wyłączając tym samym z ruchu dostępne na nich drogi technologiczne.



Rys. 88. Oznaczenia przeszkód spowodowanych przez osuwiska na drogach kilku poziomów eksploatacyjnych.

Pojazdy (maszyny) są reprezentowane w programie poprzez klasę „Vehicle”, której można przypisać parametry istotne z punktu widzenia prowadzonych symulacji [Rys. 89]. Zaznaczyć tu należy, że nie wszystkie dostępne parametry mają istotny wpływ na charakterystykę ruchu konkretnej badanej maszyny, dlatego wybór parametrów istotnych pozostaje w gestii decydenta i zależy od posiadanej wiedzy eksperckiej.



Rys. 89. Okno parametrów maszyny.

Tworzenie warstwy pojazdów polega na nanoszeniu kolejnych pojazdów na przygotowaną w poprzednich krokach mapę i przypisanie im niezbędnych parametrów technicznych. Lokalizacja maszyn na mapie realizowana jest przez wskazanie konkretnego miejsca na istniejącym już odcinku. Pojazd reprezentowany może być przypisaną mu ikoną, a w przypadku braku takiej ikony oznaczony jest rombem.

Kolejnym krokiem przygotowania symulacji jest utworzenie w warstwie dróg miejsc bezpiecznych, które odzwierciedlają miejsca schronienia dla pojazdów w sytuacjach zagrożenia. Technicznie obsługa miejsc bezpiecznych realizowana jest analogicznie jak obsługa przeszkód. Na mapie miejsca bezpieczne odwzorowane są poprzez pola o parametryzowanym rozmiarze [Rys. 90]. Parametrem opisującym miejsce bezpieczne jest jego pojemność, czyli liczba standardowych maszyn którą jest w stanie pomieścić dane miejsce. która wykorzystywana jest w procesie symulacji. Możliwość takiego uproszczenia wynika z parametrów maszyn stosowanych w KWC.

Rys. 90. Oznaczenie na mapie miejsca bezpiecznego.

Ostatnim krokiem fazy przygotowania mapy przed symulacją jest naniesienie warstwy zagrożeń. W procesie tym wykorzystana została triangulacja Delaunay'a [Kucwaj, 1996]. Operator edytuje i oznacza na mapie odcinki tras, które uznawane są za niebezpieczne, przypisując im odpowiedni współczynnik zagrożenia, który można zdefiniować jako miarę oceniającą prawdopodobieństwo i potencjalne skutki wystąpienia zagrożenia w danym miejscu, nawet jeśli jest ono sklasyfikowane jako bezpieczne. Miejsce uznane za bezpieczne nie oznacza, że ryzyko jest zerowe, lecz że ryzyko znajduje się poniżej akceptowalnego poziomu.

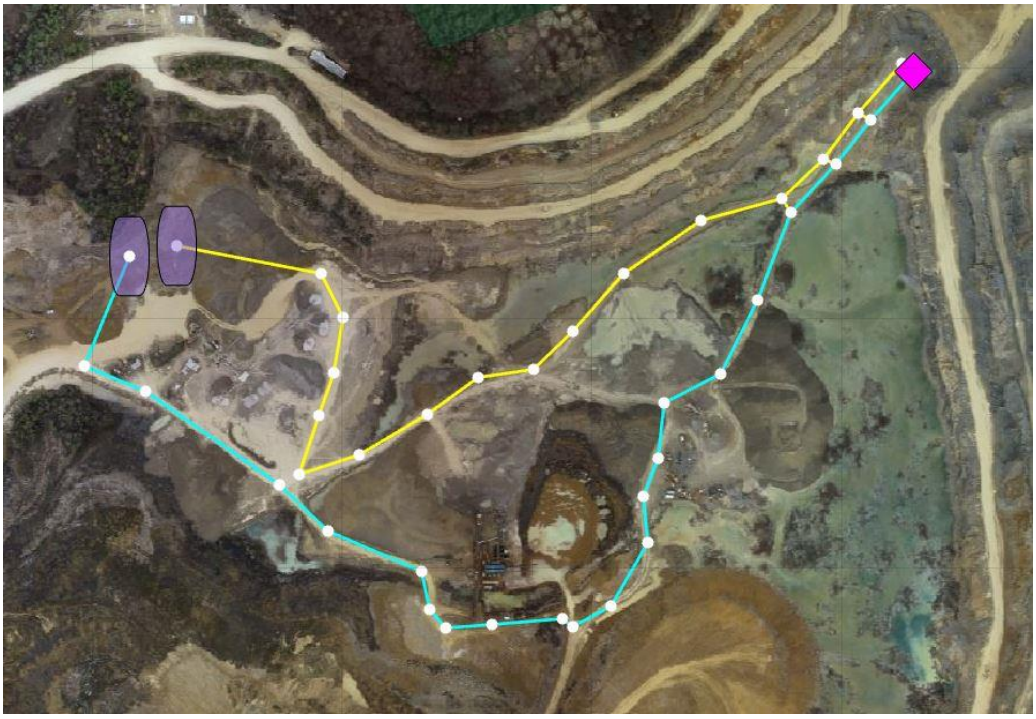
11.1.4 Symulacja ewakuacji

Poprawnie przygotowana mapa, zgodnie z opisem zaprezentowanym powyżej, 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.

Funkcje dostępne dla operatora w zakresie prowadzenie symulacji zebrane są w zakładce „Analizy". Wybrać można algorytm wg. którego odbędzie się symulacja oraz typ ewakuacji, tj. czy maszyny same na bieżąco wykrywają przeszkody, czy dostają wcześniej ostrzeżenie od operatora. Symulacja realizowana zgodnie z algorytmem przedstawionym na [Rys. 87] może być przeprowadzona w dwóch wariantach, w zależności od preferencji operatora.

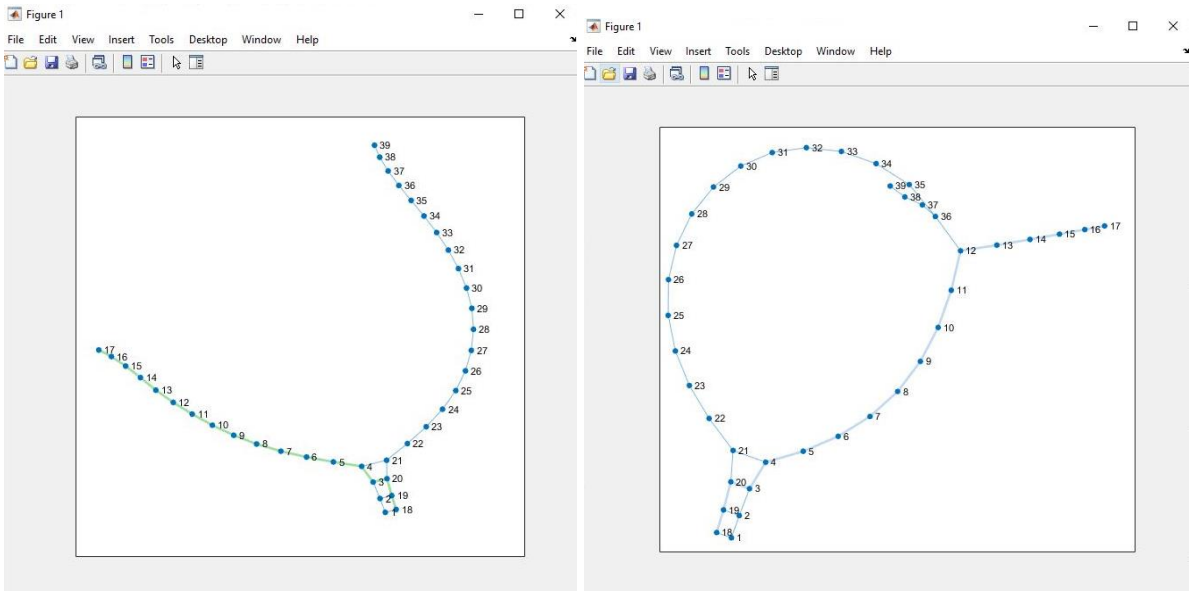
Wariant 1. Przykład symulacji ewakuacji do miejsca bezpiecznego pokazano na kolejnych rysunkach [Rys. 91, Rys. 92]. Zakładamy dwie możliwe trasy, przy czym w pierwszej symulacji tylko początkowe punkty trasy pokrywają się (punkty wspólne trasy oznaczone na czerwono), a w drugiej symulacji również w środku trasy założono możliwy punkt wspólny.



Rys. 91. Symulacja ewakuacji wariant pierwszy.

Rys. 92. Symulacja ewakuacji wariant drugi.

Graficzne odwzorowanie wyników symulacji przedstawia Rys. 93.



Rys. 93. 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:

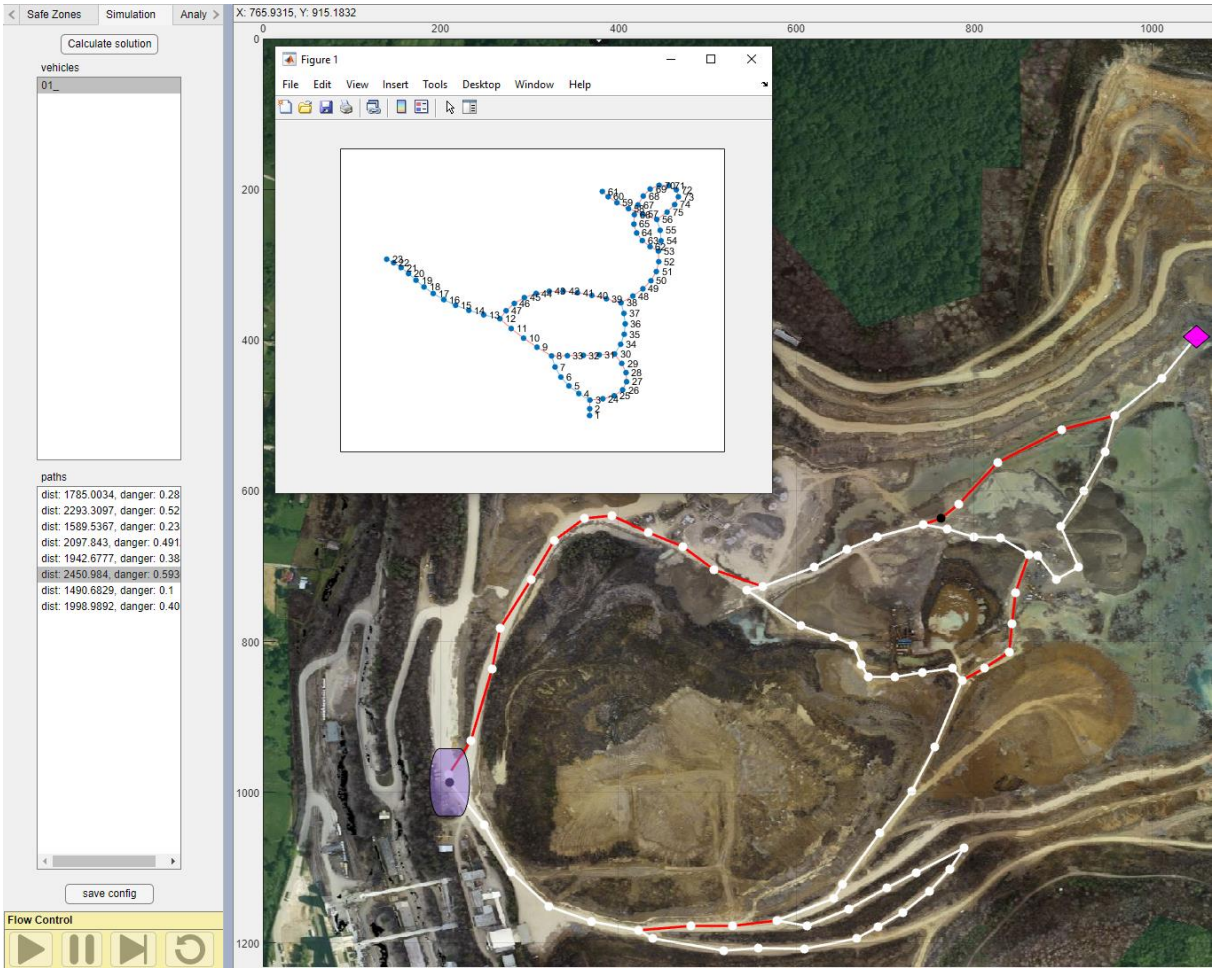
- całkowitym czasie trwania procesu ewakuacji,
- procentowe uszkodzenia poszczególnych pojazdów,
- oczekiwanym czasie dotarcia do miejsca bezpiecznego oraz o czasie faktycznym po dotarciu do tego miejsca,
- przejechanej długości trasy, dla każdego pojazdu.

Wariant 2. Ten sposób prowadzenia symulacji 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. 94, Rys. 95]. Jak widać na rysunku [rys.95] 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 (zgodnie z [Rys. 85]). 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. 29].

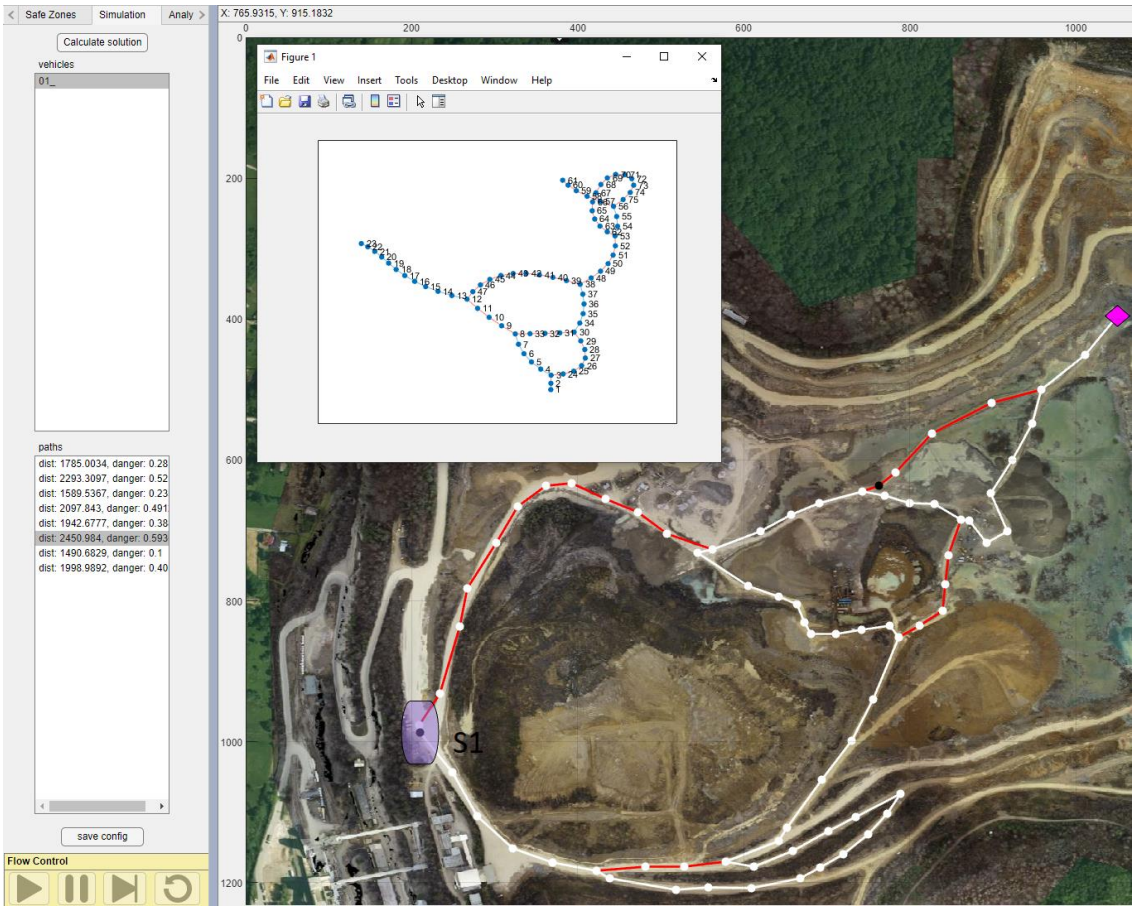
Tab. 29. Wyniki symulacji dla Wariantu 2

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. 94, natomiast na Rys. 95, w analogiczny sposób zaprezentowana została trasa najdłuższa.



Rys. 94. Najkrótsza trasa ewakuacji (1490 metrów, kolor biały).



Rys. 95. Najdłuższa trasa ewakuacji (2450 metrów, kolor biały).

Aplikacja posiada również funkcjonalność umożliwiającą śledzenie ruchu pojazdu w trakcie symulowanego procesu ewakuacji, z opcją zatrzymania pojazdu w dowolnym momencie i wznowienia symulacji. Rys. 96 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.

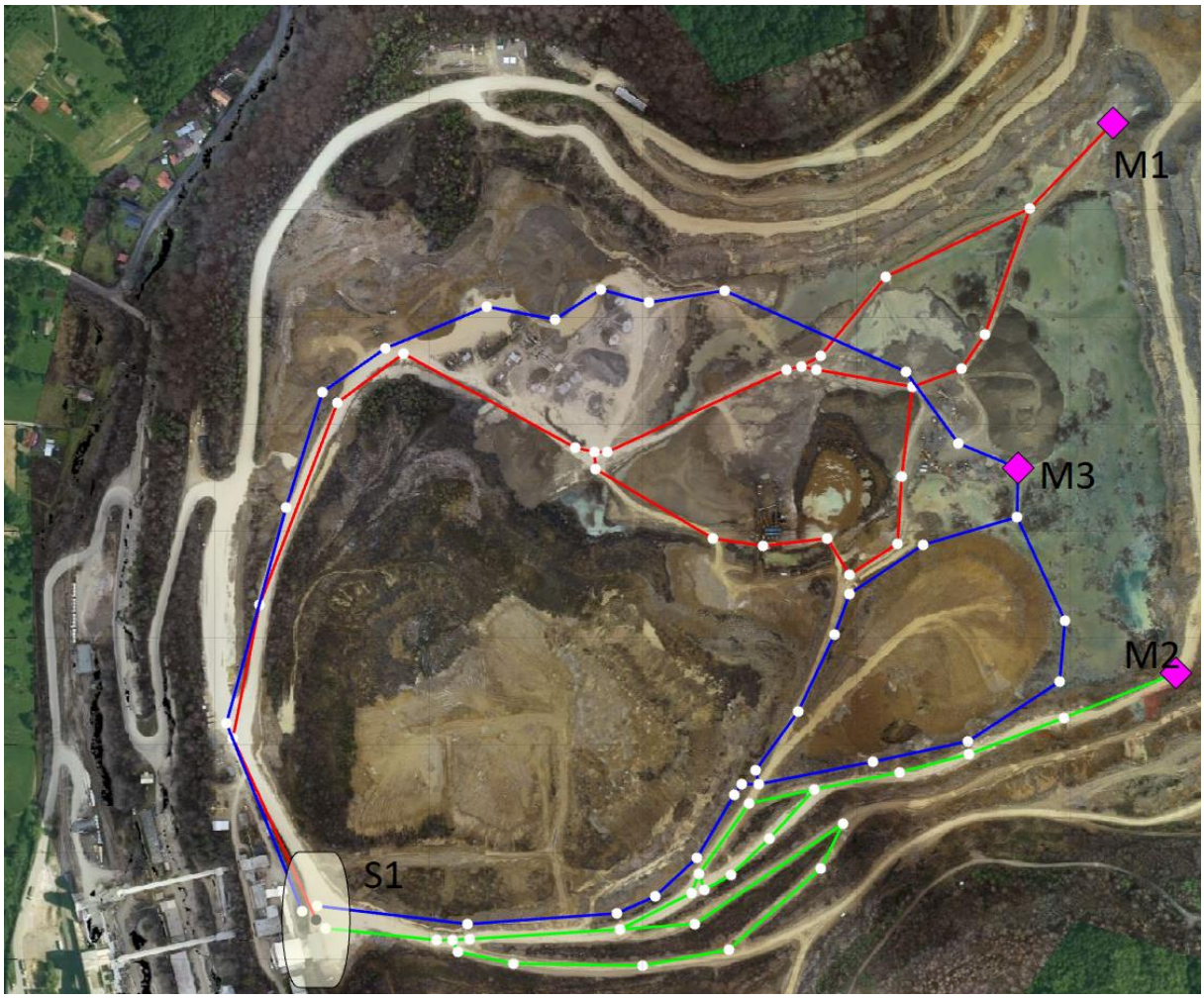
Rys. 96. Widok interfejsu aplikacji w trakcie symulacji ruchu ewakuowanego pojazdu.

Wyniki symulacji prezentowane w formie graficznej [Rys. 91, Rys. 92, Rys. 94, Rys. 95], można wyeksportować do pliku z rozszerzeniem *.xslx lub *.csv, co umożliwia przekazanie tych danych do innych modułów systemu klasy IRM DSS. Dodatkową funkcjonalnością, jaką oferuje aplikacja jest możliwość porównywania zaimplementowanych (bądź wczytanych) algorytmów. Funkcjonalność dostępna w zakładce „Comparison" w panelu warstw.

Symulacja ewakuacji 3 maszyn (wodzideł technologicznych: M1, M2 i M3) z obszarów zagrożonych, do jednego, wyznaczonego miejsca bezpiecznego (S1) przedstawiono na [Rys. 97]. Wyniki symulacji prezentuje [Tab. 30]. 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.

Tab. 30. Wyniki symulacji ewakuacji dla 3 pojazdów.

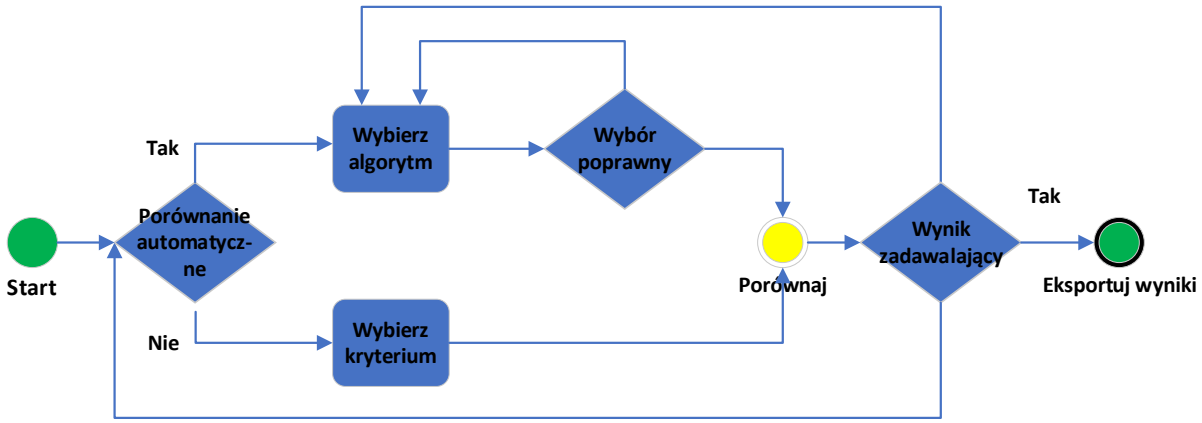
	Czas przejazdu [s]	Długość trasy [m]	Poziom zagrożeń [%]	Minimalny czas ewakuacji [s]	Maksymalny czas ewakuacji [s]	Średni czas ewakuacji [s]
Maszyna_1 Trasa_1	73,98	1 379,01	15,30	73,98	86,86	79,16
Maszyna_1 Trasa_2	76,65	1 428,79	43,81			
Maszyna_1 Trasa_3	86,86	1 619,03	63,28			
Maszyna_2 Trasa_1	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			



Rys. 97. Widok rozmieszczenia ewakuowanych pojazdów i miejsca bezpiecznego.

Porównanie wyników różnych wariantów ewakuacji realizowane może być poprzez manualny lub automatyczny wybór parametrów [Rys. 98]. W pierwszym przypadku należy wybrać algorytmy w sekcji „compared algorithms".

Porównywanie automatyczne odbywa się za pomocą zakładki „compare by" – z listy rozwijanej wybrać należy jedynie parametr, wg którego porównywane będą algorytmy, po czym należy nacisnąć przycisk „compare by" obok. Wówczas pojawi się okno wyników, takie jak przy porównywaniu manualnym, z tym że porównane zostaną wszystkie dostępne algorytmy, z czego wyświetlone najlepsze dwa wg wybranego kryterium.



Rys. 98. Funkcjonalność porównywania algorytmów.

11.2 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 przedstawiona została szczegółowa propozycja zastosowania takiego systemu, uwzględniając konkretne technologie oraz ich zastosowanie.

Biorąc pod uwagę charakter i sposób wykorzystania posiadanych przez algorytm danych, scenariusze można podzielić na eksploracyjne i przewidywania [Baloian i in., 2019]. Z kolei scenariusze eksploracyjne mogą posiadać charakter projekcyjny, czyli rozwijać się zgodnie z dotychczasowymi trendami i nie uwzględniając trendów warunkowych mających cechy predykcji możliwych zdarzeń. Scenariusze przewidywania opierają się na możliwych zdarzeniach, pożądanych lub niepożądanych, a wynikających ze zgromadzonej wiedzy ekspertów, którzy są często interesariuszami danego procesu, dlatego ich ścisła współpraca z decydentami jest nieodzowna. To właśnie ten ostatni aspekt (udział w procesie wielu interesariuszy) narzuca określony reżim pracy, zgodnie z którym istotne jest uwzględnienie wymiaru czasowego, a formułowane hipotezy powinny być analizowane pod względem prawdopodobieństwa z uwzględnieniem [Baloian i in., 2019]: wiarygodności (definiowanej

w oparci u o realność danych wejściowych), pewności (z założeniem, że dane wejściowe mieszczą się w pewnych ustalonych granicach) oraz niepewności (sytuacji, gdy dane klasyfikowane są jako nieprzydane w procesie decyzyjnym).

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). Zaawansowany system monitorowania i reagowania na zagrożenia środowiskowe powinien obejmować:

- czujniki zamontowane w kluczowych miejscach prowadzenia eksploatacji, które będą monitorować zmiany w górotworze, przemieszczenia i wibracji w czasie rzeczywistym oraz czujniki zamontowane na maszynach i urządzeniach analizujące w sposób ciągły parametry pracy maszyny,
- systemy monitoringu i analizy obrazu, pokrywające swym zasięgiem możliwie duży obszar prowadzenia działalności, które dzięki zaawansowanym algorytmom analizy obrazu będą w stanie wychwycić wszelkie anomalie w analizowanej scenie i uruchomić procedurę alarmową,
- system zbierania i analizy danych z sensorów w czasie rzeczywistym przy użyciu zaawansowanych algorytmów, wsparty algorytmami AI w celu predykcji potencjalnych zagrożeń i ryzyk, w celu wczesnego reagowania, aby zwiększyć bezpieczeństwo,
- opcjonalnie systemy radarowe i georadarowe, do monitorowania aktywności na obserwowanym terenie i stabilności górotworu, z założeniem identyfikacji potencjalnych intruzji czy osuwisk, w celu uruchomienia procedur ewakuacyjnych.

Tak zaprojektowany systemy powinien zapewniać sprawne alarmowanie w sytuacjach zakwalifikowanych do kategorii stanowiących zagrożenie i umożliwiać zarządzanie ewakuacją.

Kluczowym elementem zarządzania bezpieczeństwem w sytuacjach kryzysowych jest sprawny system ewakuacyjny. Dzięki wykorzystaniu zaawansowanych technologii można zoptymalizować proces ewakuacji, zapewniając jak najszybsze opuszczenie strefy zagrożenia przez pracowników oraz maszyny. Uruchomienie i przebieg procedury alarmowej, potwierdzone analizą i walidacją dostępnych danych zakłada:

- skuteczne przekazanie informacji o stanie zagrożenia i konieczności ewakuacji do wszystkich osób i jednostek zlokalizowanych na obszarze zagrożonym,
- wyznaczenie bezpiecznych miejsc, a następnie tras ewakuacji, ulatniając specyfikę zarówno samych tras jaki i ewakuowanych jednostek,

- bieżącą analizę rozwoju zagrożenia i przebiegu procesu ewakuacji z możliwością dynamicznego wprowadzania zmian w trwającej procedurze adekwatnie do rozwoju zdarzeń,
- ciągłą i w miarę możliwości dwukierunkową komunikację, w celu usprawnienia całego procesu, ale również zapewnienia poczucia bezpieczeństwa ewakuowanym jednostkom,
- bieżące śledzenie położenia jednostek ewakuowanych pracowników w celu skutecznego zarządzanie ewakuacją.

Kolejnym aspektem, który powinien być analizowany i wspierany przez system IRM DSS jest zapewnienie bezpieczeństwa technicznego maszyn i infrastruktury pomocniczej w przypadku wystąpienia zagrożeń (Scenariusz 2). W odkrywkowych zakładach górniczych używa się dużych, ciężkich maszyn, które mogą stanowić zagrożenie w sytuacjach kryzysowych również dla otoczenia. Uruchomienia procedury alarmowej w takim przypadku obejmuje:

- natychmiastowe uruchomienia systemów automatycznych, zabudowanych na maszynach (np. systemy gaszenia pożarów), co jest szczególnie istotne w przypadku maszyn zasilanych paliwami płynnymi. 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, które w zależności od rodzaju maszyny mogą polegać na podjęciu akcji ratunkowej lub wstrzymaniu swojej typowej aktywności i rozpoczęciu ewakuacji w bezpieczne miejsce. Systemy te mogą będąc w pełni zintegrowanymi z centralnym systemem zarządzania bezpieczeństwem, wspomagając koordynację działań w sytuacjach awaryjnych, np. poprzez udostępnienie obrazu bezpośrednio z miejsca prowadzenia akcji.
- zdalne monitorowanie przebiegu akcji ratowniczej oraz stanu technicznego maszyn umożliwia dalszą eskalację prowadzonych działań, wezwanie dodatkowych jednostek ratowniczych, wyłączenie z ruchu i dostępności zagrożonych obszarów, a w przypadku zagrożonych obiektów stałych również odcięcie dopływu mediów i przejście w stan czuwania awaryjnego.

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. Istota działania systemu w takim scenariuszu opiera się o następujące elementy:

- system klasy IRM DSS w sposób ciągły analizuje spływające dane i prognozy. 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, takie jak przeniesienie pracowników z zagrożonych obszarów, wstrzymanie prac w określonych częściach zakładu czy modyfikacje tras transportu.
- system prezentuje wizualizację dostępnych danych oraz proponowane działania zapobiegawcze na interaktywnej mapie zakładu, co ułatwia szybką identyfikację obszarów zagrożonych.
- decydenci zarządzający bezpieczeństwem na bieżąco monitorują sytuację w całym zakładzie, łącznie z obszarem zagrożonym i podejmują decyzję w oparciu o propozycje reakcji prezentowane przez system wsparcia, zatwierdzając je lub wprowadzając niezbędne korekty w oparciu o posiadaną wiedze ekspercką.
- system gromadzi wszystkie przetwarzane dane i buduje kolejne scenariusze, które posłużą jako dane wejściowe przy kolejnym zdarzeniu o podobnym charakterze.

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. W celu zagwarantowania poprawnej reakcji system powinien być właściwie wyposażony, skonfigurowany i rekomendować właściwe działania opierając się na:

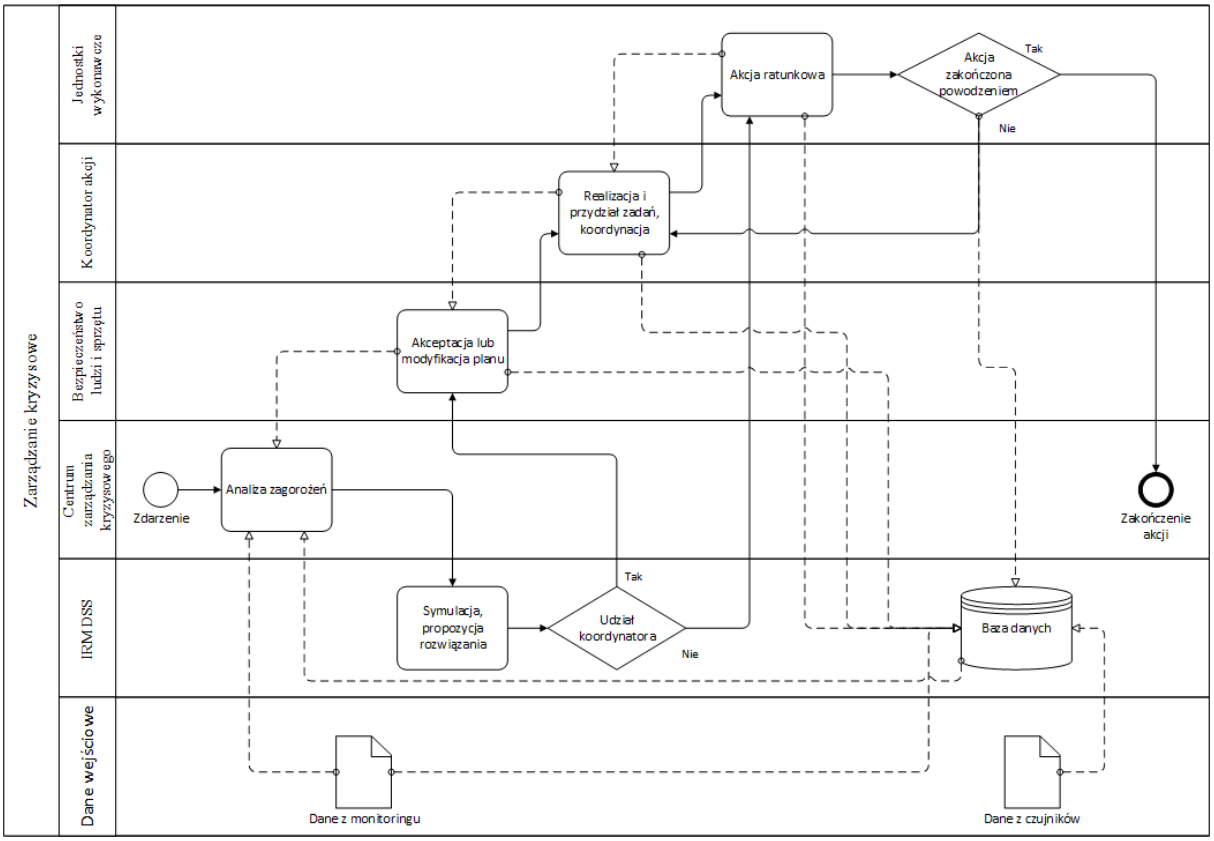
- kamerach monitoringu w zaawansowaną analityką obrazu i detekcją zagrożeń: Kamery monitorujące teren zakładu (wsparte np. systemami radarowymi) wyposażone w inteligentne systemy detekcji ruchu, automatycznie identyfikują nieautoryzowane osoby lub potencjalne zagrożenia (np. pożary, wycieki), potrafią w oparciu o bazę wiedzy odrzucić alarmy fałszywe, spowodowane np. zwierzyną leśną i zadysponować właściwe działania poprzez wysłanie patrolu w miejsce zdarzenia lub prowadząc inteligentne śledzenie obiektu w celu dalszej analizy sceny, aż do momentu jednoznacznego zakwalifikowania analizowanego przypadku.
- Właściwie rozmieszczone systemy dostępu gwarantują dostęp do stref objętych restrykcjami tylko dla uprawnionych pracowników, co daje gwarancję, że do stref niebezpiecznych nie dostaną się osoby nieuprawnione oraz pozwoli w trybie ciągły kontrolować kanały dostępowe do tak zdefiniowanych miejsc czy obiektów,

umożliwiając tym samym możliwość szybkiej i właściwej reakcji w przypadku stwierdzonych nadużyć.

Analizując zaproponowane w tym rozdziale 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 może funkcjonować nie tylko efektywnie, ale przede wszystkim bezpiecznie.

11.3 Schemat systemu z propozycjami wykorzystania w kopalni odkrywkowej

Zaprezentowany [Rys. 99] diagram przedstawia schemat BPMN IRM DSS dla odkrywkowego zakładu górniczego, opracowanego we wcześniejszych rozdziałach rozprawy. Diagram ten [Rys. 99] prezentuje głównych uczestników procesów i ich interakcje z systemem, zapewniając wizualizację funkcjonalności systemu. Natomiast propozycje możliwych przypadków użycia systemu uwzględniające analizowane scenariusze, takie jak ewakuacja, akcje ratunkowe, wykrywanie intruzji czy ochrona terenu przedstawione są w notacji UML Use Case na [Rys. 100, Rys. 101, Rys. 102, Rys. 103, Rys. 104].



Rys. 99. Diagram BPMN działania IRM DSS.

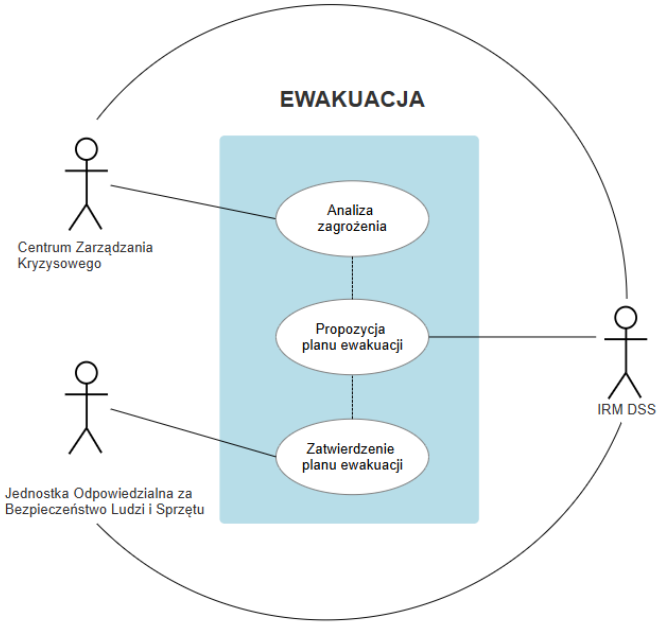
Diagram w notacji BPMN na [Rys. 99] ilustruje proponowany model funkcjonowania systemu klasy IRM DSS w KWC, uwzględniając udział w procesie uczestników:

1. Centrum Zarządzania Kryzysowego - koordynuje operacje produkcyjne, monitoruje ryzyko i podejmuje decyzje strategiczne w oparciu o dane systemowe.
2. Jednostkę odpowiedzialną za Bezpieczeństwo Ludzi i Sprzętu - odpowiada za zarządzanie sytuacjami kryzysowymi, w tym ewakuację i akcje ratunkowe.
3. Koordynatora Akcji - wykonuje operacje na maszynach, zabezpiecza ludzi i sprzęt w przypadku zagrożenia.
4. Jednostki Wykonawcze - zajmują się wykrywaniem i reagowaniem zgodnie z otrzymanymi poleceniami.
5. IRM DSS - centralny system wspomagający decyzje, gromadzi dane, przeprowadza analizy ryzyka i dostarcza rekomendacje.

Tak opisana struktura realizuje zadania zgodnie ze swoimi kompetencjami i rolami, jakie odgrywają. Sam przebieg akcji ratunkowej zależy od charakteru zidentyfikowanego zagrożenia, można wyróżnić następujące główne scenariusze działania:

1. Ewakuacja [Rys. 100].

- Uczestnicy procesu: Centrum Zarządzania Kryzysowego, Jednostka odpowiedzialna za Bezpieczeństwo Ludzi i Sprzętu, IRM DSS.
- Opis procesu:
    1. Centrum Zarządzania Kryzysowego: Rozpoczyna analizę zagrożenia na podstawie danych z IRM DSS.
    2. IRM DSS: Przeprowadza symulację i proponuje optymalną trasę ewakuacyjną oraz alokację zasobów.
    3. Jednostka odpowiedzialna za Bezpieczeństwo Ludzi i Sprzętu: Akceptuje lub modyfikuje plan ewakuacji i rozpoczyna jego realizację.

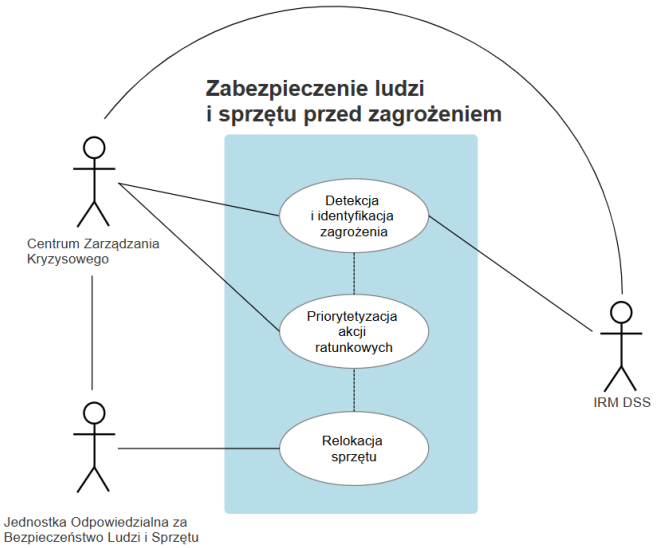


Rys. 100. Proces Ewakuacja w notacji UML (Use Case).

2. Zabezpieczenie ludzi i sprzętu przez zagrożeniem [Rys. 101].

- Uczestnicy procesu: Centrum Zarządzania Kryzysowego, Jednostka odpowiedzialna za Bezpieczeństwo Ludzi i Sprzętu, IRM DSS.
- Opis procesu:

1. IRM DSS: Wykrywa zagrożenie i powiadamia Centrum Zarządzania Kryzysowego.
2. Centrum Zarządzania Kryzysowego: Decyduje o priorytetach akcji ratunkowej (ludzie vs sprzęt).
3. Jednostka odpowiedzialną za Bezpieczeństwo Ludzi i Sprzętu: Przenosi maszyny w bezpieczne miejsca zgodnie z instrukcjami systemu.



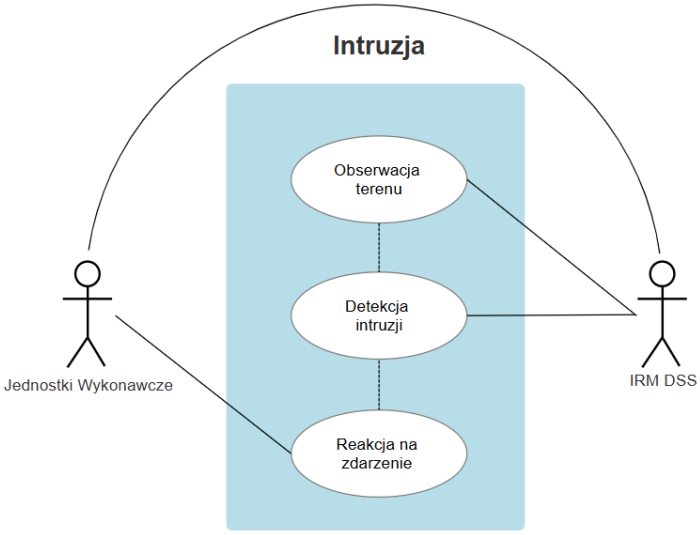
Rys. 101. Proces zabezpieczenia ludzi i sprzętu przed zagrożeniem w notacji UML Use Case.

3. Intruzja [

Rys. *102*].

Uczestnicy: Jednostki Wykonawcze, IRM DSS.

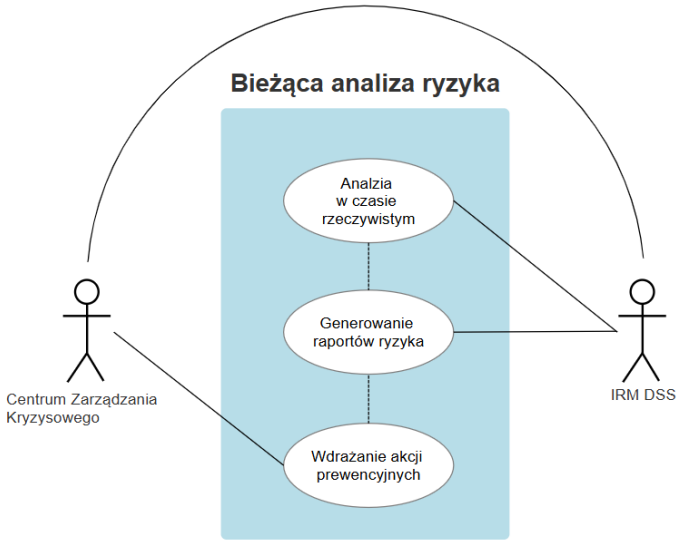
- Opis procesu:
    1. IRM DSS: Monitoruje teren kopalni za pomocą czujników i kamer.
    2. W przypadku wykrycia intruzji:
        - System powiadamia Jednostki Wykonawcze i generuje alert.
        - Jednostki Wykonawcze podejmuje rekomendowane działania.



Rys. 102. Proces Intruzji w notacji UML Use Case.

4. Bieżąca analiza ryzyka [Rys. 103].

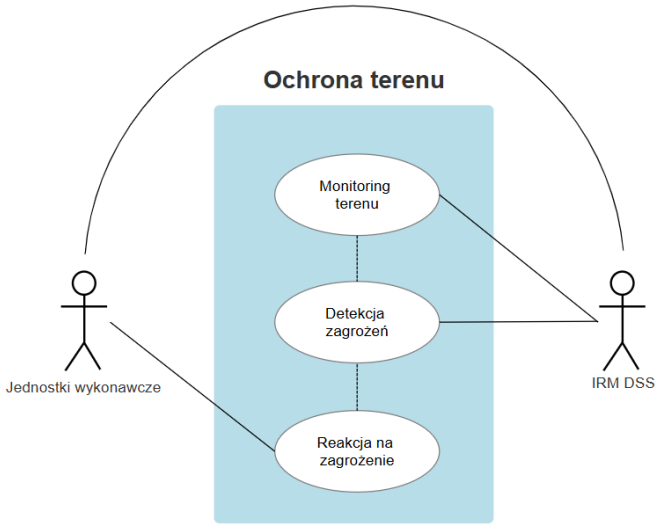
- Uczestnicy: Centrum Zarządzania Kryzysowego, IRM DSS.
- Opis procesu:
    1. IRM DSS: Analizuje dane w czasie rzeczywistym z czujników, dronów i systemów wizyjnych.
    2. Centrum Zarządzania Kryzysowego: Otrzymuje raporty ryzyka i wprowadza działania prewencyjne.



Rys. 103. Proces Bieżącej analizy ryzyka w notacji UML Use Case.

5. Ochrona terenu [Rys. 104].

- Uczestnicy: Jednostki Wykonawcze, IRM DSS.
- Opis procesu:
    1. IRM DSS: Monitoruje granice terenu i identyfikuje potencjalne zagrożenia (np. naruszenie obszaru, nielegalne działania).
    2. Jednostki Wykonawcze: Aktywnie reagują na alerty i zabezpieczają teren (np. uruchamiają blokady, wysyłają patrole).



Rys. 104. Proces Ochrony terenu w notacji UML Use Case.

Aby opisane procesy były możliwe i efektywne niezbędne jest zapewnienie właściwego przepływu informacji między uczestnikami. Kluczowe jest zwłaszcza zapewnienie przepływów pomiędzy: Centrum Zarządzania Kryzysowego (priorytetyzacja działań ratunkowych), Jednostką odpowiedzialną za Bezpieczeństwo Ludzi i Sprzętu (akceptacja lub

modyfikacja planu ewakuacji), Jednostkami Wykonawczymi (realizacja przydzielonych zadań). Podstawowe przepływy pomiędzy wskazanymi uczestnikami procesów to:

1. Dane wejściowe (np. z czujników, kamer, dronów) są przetwarzane przez IRM DSS.
2. IRM DSS generuje rekomendacje i przekazuje je odpowiednim uczestnikom procesu (np. Centrum Zarządzania Kryzysowego, Jednostka odpowiedzialna za Bezpieczeństwo Ludzi i Sprzętu).
3. Uczestnicy podejmują decyzje i wykonują działania zgodnie z rekomendacjami systemu dostarczając równocześnie informację zwrotną o przebiegu i wynikach prowadzonej akcji.

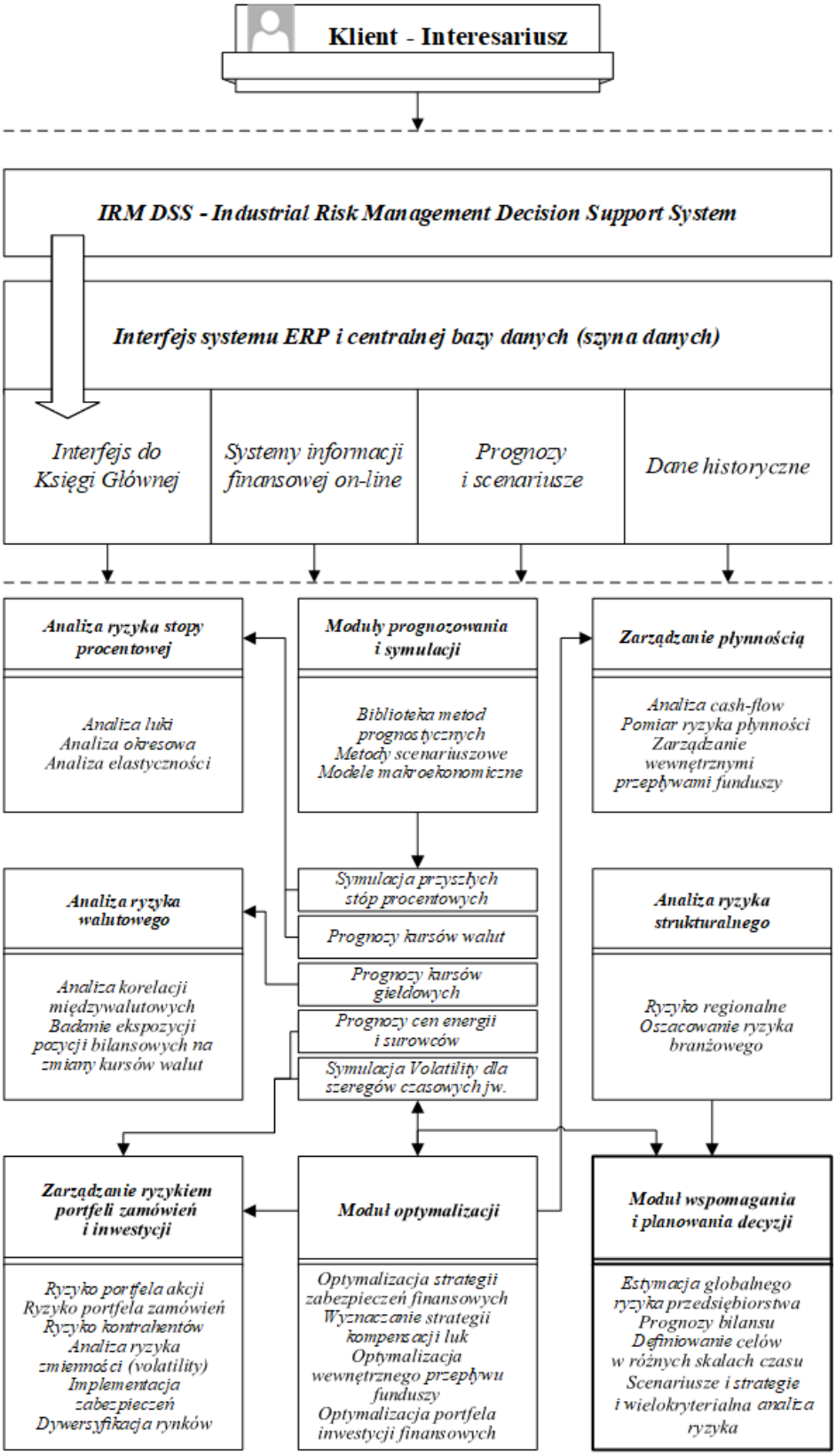
11.4 Integracja zarządzania ryzykiem przemysłowym z systemem ERP i analizą ryzyka finansowego

Schemat systemu wspomagania decyzji integrujący przedstawione wyżej zasady i szczegółowe metody zarządzania grupami ryzyk finansowych pokazany jest na [Rys. 105]. Schemat ten, oparty o idee przedstawione w [Skulimowski, 1997], stanowi zarazem propozycję implementacji specjalistycznego modułu zarządzania ryzykiem finansowym jako elementu systemu klasy ERP. Funkcjonalności tego systemu szczegółowo omówione zostały w rozdziale 9.1. Kolejnym etapem implementacji byłoby rozszerzenie tego modułu o funkcjonalności zarządzania ryzykiem przemysłowym. Podejście takie jest konsekwencją rozbudowy systemu i luk funkcjonalnych omówionych w rozdziale 9.4.

Szybki rozwój w obszarach metod badań operacyjnych, optymalizacji i analizy wielokryterialnej oraz postęp w zakresie wdrażania najnowszych technologii informatycznych w systemach ERP umożliwia obecnie, również dzięki wparciu AI, modelowanie i monitoring ryzyka przemysłowego i finansowego w czasie rzeczywistym, zapewniając równolegle dwukierunkową efektywną komunikację systemu wspomagania decyzji z osobami pełniącymi kluczowe funkcje w przedsiębiorstwie [Skulimowski, 1997]. Pomimo tak zaawansowanych rozwiązań, należy mieć na uwadze, że istniejące od wielu lat na rynku systemy zarządzania aktywami i pasywami oraz ryzykiem finansowym charakteryzują się często dużą inercją i w pewnej część wciąż opierają się na rozwiązaniach wypracowanych i wdrożonych klika lat temu. Kolejnym aspektem, na który należy zwrócić uwagę, jest fakt, że część producentów oprogramowania, głównie zagranicznych, do zarządzania ryzykiem stosuje agresywne strategie marketingowe ukierunkowane na wykorzystanie niepełnej wiedzy potencjalnych klientów w zakresie informatyki finansowej [Skulimowski, 1997]. Systemy ukierunkowane na ryzyko instytucji finansowych i oparte na doświadczeniach zaczerpniętych głównie z obszaru finansów, poświęcając nieproporcjonalnie wiele uwagi ryzyku hipotecznemu, co

wpisuje się głównie w politykę instytucji finansowych (mortgage risk). Mając na uwadze powyższe zastrzeżenia, należy podkreślić, że projektowany system pozwoli bez istotnych modyfikacji również na analizę obligacji indeksowanych inflacją, które w związku z globalną sytuacją finansową znowu stają się popularne. Stąd podjęcie inicjatywy stworzenia finansowego systemu wspomagania decyzji dostosowanego do potrzeb i problematyki polskich przedsiębiorstw i sektora finansowego, który wykorzystywać będzie najnowsze technologie informacyjne dla systemów wspomagania decyzji oraz implementować będzie aktualne osiągnięcia w zakresie informatyki finansowej, wpisuje się to w potrzeby sygnalizowane w literaturze już w roku 1997 [Skulimowski, 1997].

Proponowany tu do realizacji system zarządzania ryzykiem przemysłowym i finansowym oferuje zakres metod pomiaru i symulacji ryzyka szerszy, niż dostępne na rynku pakiety „czysto" finansowe służące głównie do zarządzania aktywami i pasywami (*asset & liability* management, ALM). Rozbudowany został o moduły wyznaczania strategii redukcji ryzyka i interakcyjnego wspomagania decyzji dotyczących wyboru strategii inwestycji rzeczowych. Z systemem zintegrowane będą bazy danych i bazy wiedzy udostępniane w trybie online przez dostawcę oprogramowania i zawierające informacje dotyczące ryzyk składowych dla poszczególnych kategorii aktywów i pasywów, miary ryzyka związanego z krajami, walutami i cenami najważniejszych surowców i in. W bazie danych przechowywane będą także historyczne dane dotyczące wskaźników makroekonomicznych i społecznych, kursy walut i papierów wartościowych, cen metali szlachetnych i ważniejszych surowców. Tak wyspecyfikowany moduł zarządzania ryzykiem powinien zwiększyć sukces rynkowy oprogramowania oraz zapewnić stałe dostosowanie do najnowszych technologii sztucznej inteligencji, analizy i eksploracji danych oraz kolektywnej inteligencji sztucznych systemów autonomicznych.



Rys. 105. Schemat systemu wspomagania decyzji w zarządzaniu ryzykiem finansowym.

11.4.1 Ryzyka finansowe

Każdą pozycję na liście aktywów i pasywów firmy można związać z pewną miarą ryzyka. Sumaryczne ryzyko bilansowe nie jest jednak zwykłą sumą ryzyka poszczególnych pozycji, lecz - ze względu na korelację pomiędzy różnymi grupami i pozycjami bilansowymi, a w szczególności występowanie korelacji ujemnych - musi być ono oszacowane przy pomocy specjalistycznych metod analizy ryzyka. Ponadto ryzyko związane z pojedynczymi pozycjami bilansowymi daje się z reguły przedstawić jako pewna funkcja ryzyk składowych, jak np. ryzyko stopy procentowej, walutowe, branżowe, czy ryzyko płynności. Dodatkową trudność w analizie ryzyka stanowi konieczność uwzględnienia zależności oszacowanego ryzyka od czasu, co pozwala na podjęcie odpowiedniej decyzji w momencie, w którym konieczna jest zmiana struktury portfela.

Zaproponowany niżej schemat systemu monitoringu globalnego ryzyka finansowego uwzględnia w jednym modelu podstawowe rodzaje ryzyka związanego z wszystkimi kategoriami aktywów i pasywów, zwłaszcza:

- ryzyko stóp procentowych,
- ryzyko zmiany kursów walutowych,
- ryzyko płynności,
- ryzyko portfelowe związane z papierami wartościowymi posiadanymi lub emitowanymi przez przedsiębiorstwo, jak np. obligacje korporacyjne.

Główna idea wykorzystania systemu zarządzania ryzykiem finansowym przedsiębiorstwa (Enterprise Risk Management System, dalej: ERMS) może być wykorzystana jako element łączący podejście do problemu finansowe i przemysłowe.

Zgodnie z przedstawionym wcześniej schematem systemu zarządzania ryzykiem finansowym w przedsiębiorstwie, wielokryterialna charakterystyka całościowego ryzyka przedsiębiorstwa wyznaczana jest w module wspomagania decyzji. Następnie dokonywane jest oszacowanie zmiany sumarycznego ryzyka i dochodu przedsiębiorstwa - użytkownika modułu w analizowanym okresie prognostycznym jako wyniku potencjalnie podjętych decyzji. Symulacja taka, prowadzona z reguły w trybie interakcyjnym, pozwala na zaplanowanie i przetestowanie skutków działań zmierzających do osiągnięcia wyznaczonego uprzednio poziomu wskaźników ryzyka i dochodu przedsiębiorstwa. Będąca częścią tego podejścia wieloetapowa analiza decyzyjna umożliwia ponadto ujawnienie działań, które nie mogłyby być przeprowadzone, gdyby ich konsekwencje rozważane były w oderwaniu od analizy całościowego ryzyka przedsiębiorstwa w dłuższym okresie. Wynika to z faktu, że skutkiem ujemnych korelacji pomiędzy efektami działań podejmowanych w różnych okresach czasu może być zmniejszenie wynikowego ryzyka globalnego, pomimo chwilowego pogorszenia wskaźników w pewnych podokresach analizowanego okresu.

Będące częścią systemu i występujące poza tym jedynie w zaawansowanych systemach pomiaru ryzyka najważniejszych banków i towarzystw ubezpieczeniowych (m.in. UBS, SKA, Citibank) zaawansowane metody wielokryterialnej analizy ryzyka umożliwi równoczesną ocenę ryzyka lub strategii obniżania ryzyka, przy pomocy dwóch lub więcej niezależnych wskaźników. Pozwala to na wyeliminowanie niepoprawnych ocen warunkowanych przez subiektywny wybór wskaźników. Użytkownik systemu może ponadto definiować własne dodatkowe miary ryzyka i integrować je z zaimplementowanymi wcześniej wskaźnikami oraz ze wskaźnikami oceny płynności, ryzyka przemysłowego oraz własnościami portfela polis ubezpieczeniowych firmy.

Wszystkie operacje matematyczne związane z pomiarem i zarządzaniem ryzykiem wykonywana powinny być przez system w sposób autonomiczny i przyjazny dla użytkownika, tj. bez konieczności ingerencji przez użytkowników systemu w struktury sterujące obliczaniem zastosowanych wskaźników ilościowych. Żądane wartości wskaźników oceny pracy przedsiębiorstwa mogą być definiowane w sposób graficzny przez wskazanie odpowiednich punktów odniesienia na wykresie planowanych wartości miar ryzyka.

Metoda punktów odniesienia stanowi jedną z najważniejszych klas procedur rozwiązywania problemów optymalizacji wielokryterialnej. Idea punktów odniesienia reprezentujących pożądane (lub idealne) wartości kryteriów została wyczerpująco zbadana m.in. przez Leitmanna, Yu, Skulimowskiego [1996], por. Rozdz. 5.3. Wadą klasycznego podejścia opartego na pojedynczym punkcie referencyjnym jest fakt, że decydent w danym czasie nie może skorzystać z rekomendacji kilku ekspertów. Powyższe uwagi mogą być uwzględnianie jako motywacja wprowadzenia metodyki zbiorów odniesienia jako uogólnienia podejścia punktów odniesienia do sytuacji, gdzie informacja preferencyjna może być wyrażona jako kilka klas punktów odniesienia, które muszą być uwzględnione równocześnie. Tak więc, podobnie jak w Rozdz. 5.3 poza docelowymi punktami odniesienia, rozważamy anty-idealne punkty odniesienia (lub poziomy porażki), których osiągnięcie może być uznane jako porażka, rozwiązania osiągalne na etapie pre-decyzyjnym (lub punkty status-quo) oraz granice optymalności. Dodatkowo, każda z tych klas punktów odniesienia może być podzielona na podklasy.

W systemach wspomagania decyzji dotyczących aktywami i pasywami jako kryteria rozważa się:

- przewidywane zyski,
- globalne ryzyko finansowe,

i

- poziom płynności,

w różnych, określonych przez użytkownika systemu pasmach czasowych. Natomiast punkty odniesienia można scharakteryzować dwoma typami informacji:

- znaczeniem dla decydenta, określanym na ogół a priori przez ekspertów zaangażowanych we wspomaganie decyzji, zwykle nie biorąc pod uwagę ograniczeń problemu optymalizacji;

oraz

- relacją do zbioru osiągalnych wartości kryteriów w problemie optymalizacji wektorowej.

Druga charakterystyka może być stosowana po uzyskaniu choćby częściowej informacji o położeniu zbioru wartości kryteriów, a jej uwzględnienie może prowadzić do zweryfikowania pierwszej klasyfikacji.

12 Harmonogram wdrożenia IRM DSS

Kolejność wdrażania poszczególnych modułów IRM DSS będzie zgodna z rankingiem potrzeb KWC, który określany jest w trakcie procesu wdrożeniowego i wynika z audytów przeprowadzonych w etapach początkowych procesu wdrożenia. Szczegółowy harmonogram wdrożenia systemu przedstawiony został poniżej, natomiast należy podkreślić, ze jest to jedynie propozycja, która musi zostać dostosowana do specyfiki funkcjonowania konkretnego zakładu przemysłowego objętego procesem wdrożenia.

Przykładowo, wdrażany system może w pierwszej kolejności koncentrować się na zapobieganiu i łagodzeniu skutków osuwisk związanych z ruchami górotworu oraz opadami oraz na zapewnieniu odporności na zagrożenia infrastruktury krytycznej KWC. Zgodnie z powyższymi priorytetami należy wybrać najbardziej odpowiednie metody i narzędzia AI przeznaczone do implementacji w IRM DSS. W szczególności, ewolucja inteligentnych technologii wspomagających podejmowanie decyzji, w tym koordynacji i wspomagania grupowego podejmowanie decyzji dedykowanych zarządzaniu operacjami zapobiegania zagrożeniom i zmniejszania ich skutków. Do priorytetów należeć też będzie opracowanie scenariuszy rozwoju autonomicznej robotyki ratowniczej, które mogą stanowić podstawę systemów zapewniających odporność na zagrożenia wskazane w tej pracy.

Analizując powyżej omówione problemy należy mieć na uwadze, że systemy zarządzania ryzykiem przemysłowym nie są już samodzielnymi aplikacjami. Są to głównie hybrydowe systemy cyberfizyczne, w których wykorzystuje się różne techniki sztucznej inteligencji i sprzęt obsługujący sztuczną inteligencję. Ponadto zasada „człowiek w pętli” jest niezbędnym paradygmatem, wyznaczającym sposoby projektowania i wdrażania systemów klasy IRM DSS. Doświadczenia zdobyte przy wyborze metod AI do wspomagania planowania działań ratowniczych w dużym przedsiębiorstwie z branży energetycznej pozwoliły wykryć kilka istotnych trendów rozwojowych. Po pierwsze, w związku z rosnącą niepewnością co do zagrożeń antropogenicznych i możliwością wystąpienia heterogenicznych zagrożeń różnego typu, wzrasta złożoność planowania działań w przypadku sytuacji awaryjnych i niemożliwym staje się uwzględnienie w sytuacji awaryjnej wszystkich przypadków potencjalnych zagrożeń i ich kombinacji w prostej instrukcji postępowania. Trwające przejście od systemów skupiających się na dostarczaniu, wizualizacji i prezentacji informacji decydentom do inteligentnych, częściowo autonomicznych systemów DSS również zostało zidentyfikowane na podstawie skanów bibliograficznych jako trendy światowe. Zostały one już uwzględnione na etapie projektowania IRM DSS.

Zaprezentowane powyżej modele podejmowania decyzji przyczynowych i wyprzedzających - okazują się szczególnie przydatnymi narzędziami wspomagania decyzji przy planowaniu - działań ratowniczych na wypadek klęsk żywiołowych. Adaptacyjne reguły decyzyjne

wbudowane w AN mogą kompensować przerwy w komunikacji i sprawić, że instrukcje awaryjne będą elastyczne, a jednocześnie zgodne z regulacjami i ogólną polityką bezpieczeństwa firmy. Dalsze kierunki wykorzystania AI, wdrożone w IRM DSS lub zastosowane w procesie projektowania, obejmują procedury wzmacniania i częściowo nadzorowanego uczenia maszynowego stosowane do uczenia się modeli zagrożeń i ich reakcji w zakresie odporności, zasad podejmowania decyzji i parametrów działań łagodzących w sytuacji awaryjnej [Foresti i in., 2002]. Konflikty pomiędzy celami w pojawiających się wielokryterialnych problemach optymalizacji można skutecznie rozwiązać za pomocą metod wspomagania decyzji opartych na wielu klasach zbiorów odniesienia [Skulimowski, Łydek, 2022b]. Zastosowane w interaktywnym projekcie procedury DSS mające na celu rozwiązywanie problemów związanych z zarządzaniem ryzykiem przemysłowym w czasie rzeczywistym oraz zestawy referencyjne mogą zapewnić intuicyjne i efektywne schematy komunikacji z menadżerami ryzyka i osobami nadzorującymi działania awaryjne.

Wdrożenie zaawansowanego systemu bezpieczeństwa przemysłowego wymaga kompleksowego podejścia, które powinno obejmować aspekty z zakresu bezpieczeństwa technicznego oraz fizycznego. Bezpieczeństwo techniczne dotyczy głównie ochrony maszyn i urządzeń, zaś bezpieczeństwo fizyczne obejmuje ochronę pracowników oraz samej infrastruktury przed zagrożeniami zewnętrznymi. Poniżej znajduje się proponowany harmonogram wdrożenia systemu bezpieczeństwa przemysłowego, który obejmuje zarówno bezpieczeństwo techniczne oraz fizyczne jak i aspekty związane z cyberbezpieczeństwem.

Procedura 12.1

Etap 1: Analiza przedwdrożeniowa i planowanie (5–7 tygodni).

1.1. Audyt bezpieczeństwa obecnych systemów (2 tygodnie).

Audyt ten powinien obejmować zarówno systemy IT i OT, jak i maszyny oraz urządzenia fizyczne a także otoczenie badanego przedsiębiorstwa. Kluczowe aspekty do uwzględnienia to:

- Ocena stanu technicznego bezpieczeństwa maszyn: sprawdzenie, czy maszyny i urządzenia są wyposażone w odpowiednie środki ochrony technicznej (np. osłony, przyciski awaryjne, systemy blokad) i czy spełniają normy bezpieczeństwa.
- Audyt bezpieczeństwa fizycznego: sprawdzenie stanu ochrony dostępu fizycznego do krytycznych stref zakładu, w tym kontroli dostępu do maszyn i obszarów o wysokim ryzyku wypadków. Weryfikacja posiadania wyznaczonych stref bezpiecznych oraz zasad i dróg ewakuacji.
- Ocena stanu cyberbezpieczeństwa: identyfikacja zagrożeń w systemach informatycznych i przemysłowych, w tym systemach SCADA. Weryfikacja istnienia zabezpieczeń na styku różnych środowisk informatycznych.

Na podstawie wyników audytu powinien powstać raport identyfikujący luki w zabezpieczeniach zarówno w zakresie IT/OT, jak i technicznych oraz fizycznych aspektów bezpieczeństwa.

1.2. Określenie wymagań systemu (1–2 tygodnie).

Na podstawie wyników audytu należy określić specyficzne wymagania w trzech kluczowych obszarach:

- Bezpieczeństwo techniczne: określenie wymagań dotyczących ochrony maszyn i urządzeń przemysłowych. Należy uwzględnić zintegrowane systemy ochrony, takie jak blokady bezpieczeństwa, osłony mechaniczne, systemy reagowania awaryjnego oraz regularne inspekcje i konserwacje.

- Bezpieczeństwo fizyczne: zdefiniowanie standardów ochrony fizycznej, takich jak kontrola dostępu do stref krytycznych, zabezpieczenia przed włamaniem oraz monitorowanie wizyjne (CCTV).

- Cyberbezpieczeństwo: wymagania dotyczące ochrony systemów IT i OT, w tym segmentacja sieci, monitorowanie ruchu, zarządzanie dostępem oraz ochrona przed atakami cybernetycznymi.

1.3. Wybór technologii i dostawców (2–3 tygodnie).

Wybór odpowiednich rozwiązań musi uwzględniać zarówno narzędzia do zarządzania cyberbezpieczeństwem, jak i systemy wspierające bezpieczeństwo techniczne oraz fizyczne. Kluczowe elementy to:

- Technologie bezpieczeństwa technicznego: wybór i instalacja systemów blokad maszyn, monitorowanie stanu maszyn, systemy kontrolne dla operatorów maszyn, systemy wspomaganie podejmowania decyzji.

- Technologie w obszarze bezpieczeństwa fizycznego: systemy kontroli dostępu do stref krytycznych, monitoring wizyjny, systemy alarmowe oraz ochrony perymetrycznej.

- Technologie IT/OT: systemy monitorowania sieci przemysłowej, systemy zarządzania incydentami, detekcja anomalii oraz zapory ogniowe, systemy wspomagania decyzji, systemy analiz trendów zmian, moduły AI Alignment.

Etap 2: Przygotowanie infrastruktury (5–7 tygodni).

2.1. Modernizacja istniejącej infrastruktury, wymiana i instalacja sprzętu (2–4 tygodnie). Prace modernizacyjne powinny obejmować w szczególności:

- Maszyny przemysłowe: wdrożenie zabezpieczeń technicznych, osłony maszyn, przyciski awaryjnego zatrzymania oraz integracja czujników bezpieczeństwa

monitorujących stan maszyn. Instalacja interfejsów systemu wspomagania decyzji i integracja z systemami pokładowymi maszyny.

- Infrastruktura fizyczna: instalacja systemów kontroli dostępu, monitoringu wizyjnego oraz systemów alarmowych w strefach o podwyższonym ryzyku. Wyznaczenie i wyposażenie stref bezpiecznych w interfejsy systemu wspomagania decyzji. Integracja systemów monitoringu z systemami wspomagania.

- Sieci IT i OT: rozbudowa infrastruktury sieciowej w celu obsługi nowych rozwiązań zabezpieczających oraz nowych punktów krytycznych z punktu widzenia funkcjonowania systemu bezpieczeństwa, zainstalowanie systemów monitorowania ruchu, firewalli, systemów detekcji intruzji.

2.2. Koncepcja segmentacji sieci i stref bezpieczeństwa.

Segmentacja dotyczy zarówno cyberbezpieczeństwa, jak i aspektów technicznych oraz fizycznych:

- Bezpieczeństwo techniczne: wydzielenie obszarów pracy maszyn, które wymagają dodatkowych zabezpieczeń fizycznych (np. blokady dostępowe), aby ograniczyć dostęp do maszyn wyłącznie dla osób upoważnionych. Opracowanie szczegółowych map stref bezpiecznych, stref ewakuacji oraz parametrów tras ewakuacyjnych.

- Bezpieczeństwo fizyczne: wydzielenie stref o podwyższonym ryzyku (np. miejsca pracy z substancjami niebezpiecznymi) i wprowadzenie odpowiednich procedur oraz technologii kontroli dostępu i monitorowania. Opracowanie procedur postępowania w przypadku zdarzeń w obszarach objętych funkcjonowaniem systemu.

- Cybersegmentacja: oddzielenie sieci IT i OT, stworzenie segmentów sieciowych o różnym poziomie ryzyka, ograniczenie dostępu do krytycznych systemów.

Etap 3: Wdrożenie systemu bezpieczeństwa (6–10 tygodni).

3.1. Instalacja i konfiguracja oprogramowania oraz systemów technicznych (4–6 tygodni). Wdrożenie systemów bezpieczeństwa obejmuje w szczególności:

- Bezpieczeństwo techniczne: instalacja systemów bezpieczeństwa maszyn, automatyczne wyłączniki awaryjne oraz czujniki monitorujące pracę maszyn. Konfiguracja systemów, które będą monitorować zużycie maszyn i informować o potencjalnych awariach. Konfiguracja systemów wsparcie podejmowania decyzji oraz systemów wykonawczych aktywowanych w sytuacji zagrożenia.

- Bezpieczeństwo fizyczne: instalacja systemów kontroli dostępu do stref krytycznych, monitoringu wizyjnego (CCTV) oraz systemów powiadamiania w obszarach o podwyższonym ryzyku.

- Cyberbezpieczeństwo: instalacja i konfiguracja systemów kontroli intruzji, firewalli, systemów do monitorowania sieci przemysłowej oraz automatyczne wykrywanie zagrożeń. Instalacja systemów przekazywania decyzji oraz systemów autonomicznego wspomagania podejmowania decyzji w przypadku problemów z komunikacją.

3.2. Integracja z istniejącymi systemami (2–3 tygodnie).

Integracja obejmuje:

- Systemy bezpieczeństwa technicznego: połączenie systemów monitorujących stan maszyn z centralnym systemem zarządzania, który pozwoli na zdalne monitorowanie ich pracy i reagowanie na awarie.

- Systemy fizyczne: integracja systemów kontroli dostępu oraz monitoringu wizyjnego z systemem zarządzania bezpieczeństwem, aby w czasie rzeczywistym śledzić, kto i kiedy przebywał w określonych strefach. Integrację z systemami wczesnego ostrzegania o zdarzeniach niebezpiecznych.

- Systemy IT i OT: synchronizacja i ujednolicenie baz danych różnych systemów, aby umożliwić centralne monitorowanie incydentów.

3.3. Testowanie i walidacja systemu (2–3 tygodnie).

Testowanie obejmuje:

- Bezpieczeństwo techniczne: testowanie systemów zainstalowanych na maszynach, przycisków awaryjnych oraz czujników bezpieczeństwa w różnych scenariuszach awaryjnych. Testowanie modułów wspomagania decyzji i komunikacji z systemami centralnymi z uwzględnieniem opracowanych scenariuszy postępowania.

- Bezpieczeństwo fizyczne: symulacje sytuacji awaryjnych i ocena skuteczności systemów monitoringu i kontroli dostępu.

- Cyberbezpieczeństwo: przeprowadzenie testów penetracyjnych i walidacja skuteczności systemów wykrywania zagrożeń oraz prawidłowości reakcji systemu w przypadku zaistnienia takich sytuacji w różnych scenariuszach.

Etap 4: Szkolenia i procedury (3–4 tygodnie).

4.1. Szkolenie personelu (2–3 tygodnie).

Szkolenia muszą obejmować trzy główne obszary:

- Bezpieczeństwo techniczne: szkolenie operatorów maszyn, inżynierów utrzymania ruchu i osób nadzorujących system bezpieczeństwa w zakresie obsługi systemów zabezpieczeń technicznych, takich jak reagowanie na sygnały awaryjne z maszyn oraz bezpieczne przeprowadzanie obsługi procesów ewakuacji czy innych

uruchomionych i prowadzonych przez system wspomagania decyzji. Dodatkowe szkolenia w identyfikowaniu potencjalnych zagrożeń wynikających z nieprawidłowej pracy maszyn, warunków środowiskowych itp. w celu budowania scenariuszy awaryjnych wspierających system.

- Bezpieczeństwo fizyczne: szkolenie pracowników w zakresie procedur ewakuacyjnych, reagowania na sytuacje awaryjne (np. pożary, wycieki substancji niebezpiecznych), a także w obsłudze systemów kontroli dostępu oraz reagowania na incydenty związane z bezpieczeństwem fizycznym. Podnoszenie świadomości w zakresie pracy w strefach niebezpiecznych oraz korzystania z odpowiednich środków łączności w sytuacjach awaryjnych.

- Cyberbezpieczeństwo: szkolenie zespołów IT i OT w zakresie obsługi systemów zintegrowanego zarządzania bezpieczeństwem, w tym monitorowania incydentów, zarządzania zagrożeniami i reagowania na naruszenia. Kluczowe jest przeszkolenie personelu w rozpoznawaniu zagrożeń oraz umiejętności doskonalenia systemu w oparciu o wdrożone procedury AI Alignment.

4.2. Opracowanie procedur operacyjnych (1 tydzień).

Po zakończeniu szkoleń należy opracować zestaw procedur operacyjnych, które będą regulować codzienne funkcjonowanie systemu bezpieczeństwa przemysłowego oraz zapewniać jego rozwój zgodnie z oczekiwaniami osób decyzyjnych. Procedury powinny obejmować:

- Procedury związane z bezpieczeństwem technicznym: instrukcje dotyczące korzystania z systemów zabezpieczeń maszyn, instrukcje postępowania w sytuacji zagrożenia w oparciu o decyzje podejmowane przez system, a także reagowania na awarie i niebezpieczne sytuacje.

- Bezpieczeństwo fizyczne: zasady dotyczące kontroli dostępu do stref o podwyższonym ryzyku, procedury ewakuacyjne oraz reagowanie na sytuacje zagrożenia fizycznego. Istotne jest również określenie harmonogramów regularnych przeglądów systemów monitorowania i alarmowych oraz kontroli ochrony fizycznej zakładu.

- Zarządzanie incydentami cyberbezpieczeństwa: jasno określone kroki, jakie należy podjąć w przypadku wykrycia naruszeń bezpieczeństwa IT/OT, w tym procesy zgłaszania incydentów, eskalacji oraz reagowania na zagrożenia.

Etap 5: Utrzymanie i monitorowanie systemu bezpieczeństwa (tryb ciągły).

Po wdrożeniu systemu bezpieczeństwa przemysłowego należy zapewnić jego regularne monitorowanie i utrzymanie, aby zagwarantować ciągłość działania i skuteczność zabezpieczeń.

5.1. Monitorowanie i audyt (tryb ciągły).

Regularne monitorowanie systemu bezpieczeństwa obejmuje:

- Bezpieczeństwo techniczne: stałe monitorowanie stanu technicznego maszyn i urządzeń, w tym regularne przeglądy i konserwacje. Istotne jest także monitorowanie systemów bezpieczeństwa i automatycznych wspomagania decyzji, aby zapewnić ich sprawne działanie.

- Bezpieczeństwo fizyczne: regularne inspekcje systemów kontroli dostępu, monitoringu wizyjnego i czujników alarmowych. Ważnym elementem jest także przeprowadzanie próbnych ewakuacji oraz testów systemów reagowania na zagrożenia zarówno techniczne, jak i fizyczne.

- Cyberbezpieczeństwo: stałe monitorowanie ruchu sieciowego, wykrywanie anomalii oraz analizowanie logów z systemów zintegrowanych w ramach systemu wspomagania decyzji. Należy także przeprowadzać regularne audyty bezpieczeństwa IT i OT, aby identyfikować nowe zagrożenia i weryfikować skuteczność stosowanych rozwiązań.

5.2. Aktualizacje i utrzymanie systemu (tryb ciągły).

W miarę pojawiania się nowych zagrożeń oraz rozwoju technologii, system bezpieczeństwa powinien być regularnie aktualizowany. Obejmuje to:

- Modernizację urządzeń technicznych: regularna wymiana i modernizacja starszych urządzeń, które mogą stanowić zagrożenie dla bezpieczeństwa pracowników lub które nie spełniają aktualnych standardów.

- Aktualizację systemów fizycznych: utrzymanie systemów kontroli dostępu, monitoringu i alarmów w pełnej sprawności, aby zagwarantować ochronę fizyczną zakładu i jego pracowników.

- Aktualizację oprogramowania: regularne aktualizowanie składników zintegrowanego systemu bezpieczeństwa, aby zabezpieczyć go przed nowymi zagrożeniami. ■

Wdrożenie kompleksowego systemu bezpieczeństwa przemysłowego obejmuje szereg złożonych działań, od analizy przedwdrożeniowej i planowania, poprzez instalację i konfigurację systemów, aż po szkolenia pracowników i opracowanie procedur operacyjnych. Uwzględnienie aspektów bezpieczeństwa technicznego, bezpieczeństwa fizycznego oraz informatycznego (cyberbezpieczeństwa) pozwala na stworzenie skutecznej ochrony zarówno przed zagrożeniami fizycznymi, jak i cyfrowymi. Kluczowe znaczenie mają regularne audyty, monitorowanie oraz utrzymanie systemu, aby zapewnić jego niezawodność i dostosowanie do zmieniających się warunków oraz zagrożeń.

13 Dyskusja - 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. Postęp technologiczny oraz rosnąca dostępność nowoczesnych rozwiązań umożliwiają integrację nowych narzędzi z istniejącymi systemami zarządzania bezpieczeństwem. Wszystko wskazuje na to, że w najbliższych latach możemy spodziewać się dalszego rozwoju tego typu systemów w kilku kluczowych, zaprezentowanych poniżej obszarach. Prognozowane kierunki rozwoju zaawansowanych systemów zarządzania bezpieczeństwem i wsparcia podejmowania decyzji w zakładach przemysłowych będą konsekwencją:

1. Rozwoju sztucznej inteligencji (AI) 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. Analiza dużych zbiorów danych z sensorów, kamer, systemów monitorowania oraz innych dostępnych źródeł zapewni możliwość przewidywania zdarzeń niebezpiecznych, awarie maszyn czy inne sytuacji, które skutkować mogą zagrożeniem.
- autonomiczne podejmowanie decyzji, które w sytuacjach kryzysowych umożliwi AI przejąć funkcję decyzyjną, minimalizując czas reakcji na zagrożenia poprzez wyeliminowanie czynnika ludzkiego. System będzie mógł w pełni autonomicznie i automatycznie uruchamiać procedury ewakuacyjne, wyłączać maszyny czy uruchamiać systemy gaśnicze.
- adaptacyjność systemu bezpieczeństwa, wspartego przez algorytmy uczenia maszynowego do zmieniających się warunków pracy w zakładzie przemysłowym, co pozwoli na dynamiczne i predykcyjne zarządzanie ryzykiem. System będzie uczyć się na podstawie wcześniejszych zdarzeń, będzie potrafił wyszukać właściwe informacje w globalnej sieci danych, optymalizując dzięki temu funkcjonujące procesy bezpieczeństwa.

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. Każdy element infrastruktury zakładu będzie monitorowany w czasie rzeczywistym, co pozwoli na szybkie i efektywne wykrywanie zagrożeń już we wczesnych fazach ich występowania.
- 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. Czujniki monitorujące puls, temperaturę ciała czy narażenie na niebezpieczne substancje mogą ostrzegać przed zagrożeniem i automatycznie zgłaszać alarmy do centralnego systemu.
- 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 w trybie ciągłym lub z zadaną częstotliwością. Dzięki zdalnej inspekcji i bieżącej analizie spływających danych

zminimalizowane będzie ryzyko wypadków związanych z osuwiskami czy innymi zdarzeniami w obrębie górotworu.

- autonomiczne maszyny górnicze, takie jak koparki, ładowarki, wiertnice czy nawet wozidła, które pracować będą autonomicznie, eliminując potrzebę obecności człowieka w niebezpiecznych strefach. Zdalne sterowanie oraz autonomiczne podejmowanie decyzji przez maszyny zmniejszy ryzyko wypadków związanych z obsługą ciężkiego sprzętu. Nie mniej istotnym elementem jest tu likwidacja przerw w pracy, które są niezbędne dla człowieka.
- systemy autonomicznej ewakuacji w postaci autonomicznych pojazdów ewakuacyjnych, które będą transportować pracowników w bezpieczne miejsce w przypadku wykrycia zagrożenia. Pojazdy te zintegrowane z centralnym systemem zarządzania bezpieczeństwem, zagwarantują szybkie i skuteczne działanie w sytuacjach kryzysowych.

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. AI w połączeniu z technologiami zabezpieczającymi automatycznie wykryje nieprawidłowości i zablokuje potencjalne ataki, zanim spowodują one zakłócenia w funkcjonowaniu przedsiębiorstwa.

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, kamery i inne systemy monitorowania. Zaawansowane algorytmy będą analizować te dane w czasie rzeczywistym, umożliwiając prognozowanie zagrożeń oraz podejmowanie bardziej precyzyjnych i zgodnych z oczekiwaniami decydentów decyzji.
- 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. Dane zebrane z jednego zakładu mogą pomóc przewidzieć potencjalne zagrożenia w innych podobnych miejscach, dzięki czemu możliwe będzie skuteczniejsze reagowanie na globalne problemy tej samej branży.

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. Dzięki autonomii systemy te będą działały znacznie szybciej i efektywniej, co skróci czas reakcji na 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. Takie podejście znacząco wpłynie na poprawę skuteczności zarządzania ryzykiem.
- 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 sztucznej inteligencji (AI) i uczenia maszynowego (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.

Z punktu widzenia odporności samego systemu czynniki mogące wpłynąć na proces decyzyjny to zagrożenia wynikające głownie z liczby decydentów i ich wiedzy dziedzinowej w obszarze analizowanych zagadnień, krytyczności problemu, zasad i norm obwiązujących w chwili i miejscu podejmowania decyzji oraz, co nie mniej ważne, ograniczeń zewnętrznych [Zhu i in., 2021]. Dodatkowym aspektem niezbędnym do uwzględnia w holistycznym procesie decyzyjnym jest niepewność, rozumiana w tym przypadku jako brak pełnej wiedzy (wiedza ograniczona), którą można minimalizować poprzez pozyskiwanie przez decydenta

dodatkowych informacji. Dlatego ważna jest, już na etapie gromadzenia i wstępnego przetwarzania informacji ich kategoryzacja i właściwe indeksowanie poprzez przypisanie cech. Można dzięki temu na wczesnym etapie wykryć luki informacyjne oraz informacje, których nie można właściwie skategoryzować. Wykorzystując przypisane cechy informacji oraz wspierając się modelami scenariuszowymi AI może przygotować model decyzyjny adekwatny dla potrzeb i będący odpowiedzią na aktualnie analizowany problem. Należy w tym miejscu pamiętać, że wybrany scenariusz zawsze posiada alternatywę oraz wpływa na przyszłe działania powodując powiększanie się możliwych ścieżek decyzyjnych dostępnych dla przyszłego decydenta. W następstwie przeprowadzonej analizy system AI proponuje zestaw scenariuszy z odpowiadającymi im prawdopodobieństwami i konsekwencjami [Xang, Haugen, 2015].

14 Wnioski końcowe

Zakładając, że w najbliższych latach podstawowe technologie produkcji kruszyw i sorbentów wapiennych 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 (Industrial Risk Management Decision Support System). System ten stanowi innowacyjne narzędzie wspierające procesy decyzyjne w zakresie zarządzania ryzykiem przemysłowym, szczególnie w sektorze górnictwa odkrywkowego. Postawiona teza badawcza, która zakładała, 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.

Uwzględniając istniejące analizy ryzyk przeprowadzone w KWC, rekomendowane jest wykorzystanie nowoczesnych technologii w zarządzaniu bezpieczeństwem przy pomocy holistycznego systemu wspomagania decyzji oraz monitoringu zapewniającego automatyczne lub półautomatyczne (częściowo nadzorowane) rozpoznawanie obserwowanych sytuacji. Ze względu na charakter prowadzonej działalności, tj. pracy na rozległym, trudnym, a miejscami niemożliwym do ogrodzenia terenie oraz ciągłe poszerzanie terenu eksploatacji, rekomendowane jest wykorzystanie technologii monitoringu i prewencji oparte o systemy zrobotyzowane, zwłaszcza UAV, wsparte wykorzystaniem technik uczenia maszynowego (ML) i sztucznej inteligencji (AI) oraz fuzja danych pozyskiwanych z wielu źródeł.

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. Wykorzystując grafy wiedzy, IRM DSS może identyfikować kluczowe punkty ryzyka, analizować ich potencjalny wpływ na inne procesy i zasoby, a także rekomendować konkretne działania zapobiegawcze. 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. Dzięki zastosowaniu wydajnych algorytmów AI analiza wielokryterialna realizowana jest w czasie rzeczywistym, jest także precyzyjna i elastyczna, co umożliwia dostosowanie decyzji do dynamicznie zmieniających się warunków już w trakcie trwania procesu decyzyjnego.

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, eliminuje redundancję w procesach zarządzania ryzykiem 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 praca wnosi wkład w rozwój nauki o 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.

Wyniki pracy wskazują na potrzebę dalszych badań i rozwijania technologii wspomagających zarządzanie ryzykiem przemysłowym. Potencjalne kierunki rozwoju obejmują głównie integrację z technologiami robotycznymi poprzez wprowadzenie zrobotyzowanych systemów monitorujących oraz autonomicznych urządzeń zapobiegawczych może znacząco zwiększyć skuteczność IRM DSS. Istotny wpływ mieć będzie również rozwój algorytmów uczenia maszynowego, dzięki zastosowaniu zaawansowanych metod uczenia maszynowego system będzie jeszcze lepiej adaptować się do zmieniających się warunków i przewidywać nietypowe zagrożenia. Rozszerzenie funkcjonalności o analizę ryzyk finansowych, połączenie analizy ryzyk przemysłowych i finansowych pozwoli na bardziej kompleksowe podejście do zarządzania przedsiębiorstwem.

Wprowadzenie na szeroką skalę systemów takich, jak IRM DSS opisany w niniejszej rozprawie może przekształcić podejście do zarządzania bezpieczeństwem w przemyśle, czyniąc je bardziej zintegrowanym, odpornym i przygotowanym na wyzwania przyszłości. Tym samym praca stanowi istotny krok w kierunku budowy nowoczesnych, inteligentnych organizacji przemysłowych.

Praca 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 rozdziale 8 Pracy zdefiniowano nowe standardy w zarządzaniu ryzykiem przemysłowym polegające na wykorzystaniu zaawansowanych technologii informatycznych, w tym zwłaszcza sztucznej inteligencji na wszystkich etapach zarządzania ryzykiem. Wyniki badań delfickich przeprowadzonych przez autora rozprawy w ramach projektu PPI/APM/2018/1/00049/U/001 NAWA, tytuł raportu: „Przeprowadzenie analizy bibliograficznej w zakresie fuzji danych dotyczących zagrożeń naturalnych, ze szczególnym uwzględnieniem zagrożeń obsunięciami gruntu i podtopieniami oraz w zakresie algorytmów ewakuacji z terenu eksploatacji przemysłowej w sytuacjach zagrożeń naturalnych, ze szczególnym uwzględnieniem zagrożeń obsunięciami gruntu i podtopieniami" [rozdział 4], a także inne prognozy, wskazują, że intensywne i holistyczne zastosowania metod AI w IRMDSS staną się standardem w przyszłości. Nastąpi rozwój systemów hybrydowych, oferując innowacyjne połączenie różnych metod AI (uczenie maszynowe, analiza wielokryterialna, grafy wiedzy, sieci antycypacyjne, bayesowskie i przyczynowe) i wnosząc nową jakość w projektowanie i rozwój systemów IRM DSS. Natomiast propozycja integracji IRM DSS z istniejącymi systemami ERP i SCADA zwiększa potencjał wdrożeniowy i adaptacyjność systemów w rzeczywistych warunkach przemysłowych.

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

Praca 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 opisane są w rozdziale 7 i rozdziale 8 łącząc 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 wyżej 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. Należy również wskazać na istotny wkład w rozwój interoperacyjności systemów informatycznych przedstawiony w rozdziale 9.5, gdzie zaproponowano płynną wymianę danych między IRM DSS, a systemami zarządzania zasobami przedsiębiorstwa (ERP) oraz systemami sterowania procesami (SCADA). Takie podejście zwiększa efektywność zarządzania ryzykiem, zapewniając spójność pomiędzy decyzjami strategicznymi i operacyjnymi. Monitorowanie, modelowanie i analiza ryzyka z wykorzystaniem nowoczesnych technologii pozwala na dokładniejsze planowanie akcji likwidujących skutki materializacji ryzyka w środowiskach przemysłowych.

Integracja zebranych danych w IRM DSS umożliwia szybsze reagowanie na zdarzenia kryzysowe, minimalizację ich skutków i planowanie działań prewencyjnych. Niemniej istotne jest włączenie paradygmatu DevOps w proces tworzenia IRM DSS [rozdział. 10.4]. To innowacyjne podejście skraca cykl rozwoju i wdrożenia systemu oraz zwiększa jego elastyczność.

C. Innowacje zastosowane w IRM DSS.

Wprowadzenie [rozdział 8.4] częściowo nadzorowanych algorytmów uczenia maszynowego, które na bieżąco uczą się z danych historycznych, stanowi nowy kierunek w automatyzacji decyzji w systemach IRM DSS. 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). Z kolei dynamiczne wykorzystanie sieci antycypacyjnych [rozdział 5.5] 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 [rozdział 8.3]). Włączenie do zaimplementowanego systemu modeli przyczynowości pozwala na lepsze zrozumienie zależności między obserwowanymi i przewidywanymi zdarzeniami, umożliwiając bardziej precyzyjne planowanie działań zapobiegawczych i awaryjnych. Scenariuszowe modelowanie ryzyka realizowane poprzez propozycję praktycznych scenariuszy zastosowania IRM DSS w różnych obszarach przemysłowych przedstawione w rozdziale 11.2 stanowi wkład w rozwój metod testowania i implementacji tych systemów, a symulacje pomagają ocenić efektywność systemu w rzeczywistych warunkach i umożliwiają jego dalszy rozwój. Na uwagę zasługuje również nowe podejścia do fuzji informacji eksperckich i technologicznych [rozdział 8.1], [rozdział 8.4.1]). Połączenie danych eksperckich i meldunków służb ochrony zakładu z informacjami generowanymi przez systemy technologiczne (czujniki, monitoring) tworzy wszechstronny model wspomagania decyzji, który może być szeroko stosowany w przemyśle oraz przyczynia się do poprawy dokładności przewidywań i minimalizacji błędów. Nową jakość stanowią także grafy wiedzy zastosowane do modelowania zagrożonych instalacji przemysłowych i akcji ratunkowych [rozdział 8.1], Algorytmy 8.1 i 8.2, Przykład 8.1.

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.

Spis Rysunków

Lista Tabel

Lista Akronimów

- AF - Anticipatory Feedback
- AHP - Analytic Hierarchy Process
- AI - Artificial Intelligence
- ALM - Asset and Liability Management
- AN - Anticipatory Network
- API - Application Programming Interface
- BHP - Bezpieczeństwo i Higiena Pracy
- BPA - Basic Probability Assignment
- BPMN - Business Process Model and Notation
- CAN - Controller Area Network
- CIO - Chief Information Officer
- CTO - Chief Technology Officer
- DERMIS - Dynamic Emergency Response Management Information System
- DevOps - Development and Operations
- DMN - Decision Model and Notation
- DPRA - Dynamic Probabilistic Risk Assessment
- DRDSS - Disaster Resilince Decision Support System
- DReMSS, DRMSS - Disaster Resilience Management Support Systems
- DRTCCR - Dynamic Real-Time Capacity Constrained Routing
- DSM - Design Structure Matrix
- DSS - Decision Support System
- EIS - Enterprise Information System
- ELECTRE - Elimination Et Choice Translating Reality
- EMISARI - Emergency Management Information System
- ERM - Enterprise Risk Managemen
- ERMS - Enterprise Risk Management System
- ERP - Enterprise Resource Planning
- ETA - Event tree analisys
- FTA - Fault tree analysis
- GKT - Grupa Kapitałowa Tauron
- GPS - Global Positioning System
- GUAV - Gliding Unmanned Aerial Vehicle
- GUI - Graphical User Interface
- HCL - Hybrid Causallogic
- ICT - Information and Communications Technology
- IDSS - Intelligent Decision Support System
- IoT - Internet of Things
- IRM - Industrial Risk Managemen
- IRM DSS - Industrial Risk Management Decision Support System
- ISO - International Organization for Standardization
- ISYCRI - Interoperability of Systems in CRIsis; Daclin, Chapurlat
- IT - Information Technology
- KWC - Kopalnia Wapienia Czatkowice Spółka z o.o.
- MCDA - Multiple Criteria Decision Analysis

- MILP - Mixed-Integer Linear Programming
- ML - Machine Learning
- OEP - Office of Emergency Prepared
- OF - Ochrona Fizyczna
- OG - Obszar Górniczy
- OT - Operational Technology
- OWL - Web Ontology Language
- PLC - Programmable Logic Controller
- PN - Polska Norma
- PRA - Probabilistic Risk Assessment
- PRISMA - Preferred Reporting Items for Systematic Reviews and Meta-Analyses
- PROMETHEE - Preference Ranking Organization Method for Enrichment Evaluation
- PSO - Particle Swarm Optimisation
- SCADA - Supervisory Control and Data Acquisition
- SIR - Susceptible Infected Recovered
- SROM - Stochastic Reduced-Order Models
- SRR - Search & Rescue Robotics
- SRSR - Swarm Robotics Search & Rescue
- SSP - System sygnalizacji pożaru
- SSWiN - System Sygnalizacji Włamania i Napadu
- SWD - System Wspomagania Decyzji
- SWOT - Strengths Weaknesses Opportunities Threats
- SWOTC - Strengths Weaknesses Opportunities Threats & Challenges
- THEMIS - DisTributed Holistic Emergency Management Intelligent System
- TOPSIS - Technique for Order Preference by Similarity to Ideal Solution
- TPE - Tauron Polska Energia SA
- TRRM - Threat Risk Response Map
- UAV - Unmanned Aerial Vehicle
- UML - Unified Modeling Language
- VaR - Value at Risk
- WOD - Weighted Ordered Distance
- WGT - Wsparcie Grupa Tauron

Bibliografia

[1]	Abu Bakar H, Mohd H, Mohd I (2016) S&T Converging Trends in Dealing with Disaster: A Review on AI Tools. In: International Nuclear Science, Technology And Engineering Conference – Inustec 2015, AIP Conference Proceedings 1704:030001, p.1-8
[2]	Abusalama J, Razali S, Choo YH, Momani L, Alkharabsheh A (2020) Dynamic real-time capacity constrained routing algorithm for evacuation planning problem. Indonesian Journal of Electrical Engineering and Computer Science 20(3):1388-1396. doi:10.11591/ijeecs.v20.i3.pp1388-1396
[3]	Alonso Vicario S, Mazzoleni M, Bhamidipati S, Gharesifard M, Ridolfi E, Pandolfo C, Alfonso L (2020) Unravelling the influence of human behaviour on reducing casualties during flood evacuation. Hydrological Sciences Journal 65(14):2359-2375. doi:10.1080/02626667.2020.1810254
[4]	Alves MJ, Antunes CH, Costa JP (2021) New concepts and an algorithm for multiobjective bilevel programming: optimistic, pessimistic and moderate solutions. Oper. Res. Int. J., vol. 21:pp. 2593–2626. doi:10.1007/s12351-019-00534-9
[5]	Bakhshipour M, Jabbari Ghadi M, Namdari F (2017) Swarm robotics search & rescue: A novel artificial intelligence-inspired optimization approach. Applied Soft Computing 57:708-726. doi:10.1016/j.asoc.2017.02.028
[6]	Baloian N, Frez J, Pino JA, Peñafiel S, Zurita G, Abarca A (2019) Technology support for collaborative preparation of emergency plans. Sensors 19(22):5040, p.1-20. doi:10.3390/s19225040
[7]	Baloian N, Frez J, Pino JA, Peñafiel S, Zurita G, Abarca A (2019) Technology support for collaborative preparation of emergency plans. Sensors (Switzerland), 19 (22), art. no. 5040, p.1-20. doi:10.3390/s19225040
[8]	Balta H, Będkowski J, Govindaraj S, Majek K, Musialik P, Serrano D, Alexis K, Siegwart R, De Cubber G (2017) Integrated Data Management for a Fleet of Search-and-Rescue Robots. J. Field Robotics 34(3):539-582. doi:10.1002/rob.2165
[9]	Banuls VA, Skulimowski AMJ, Begines JAR (2021) Disaster resilience modeling of municipal water supply infrastructures in the context of atmospheric threats. Proceedings of the International ISCRAM Conference, May 2021 pp.198-207.
[10]	Bañuls VA, Turoff M, Hiltz SR (2013) Collaborative scenario modeling in emergency management through cross-impact. Technological Forecasting and Social Change, 80 (9), pp. 1756 – 1774. doi:10.1016/j.techfore.2012.11.007
[11]	Bañuls VA, Turoff M, Lopez J (2010) Clustering scenarios using cross-impact analysis. ISCRAM 2010 - 7th International Conference on Information Systems for Crisis Response and Management: Defining Crisis Management 3.0, p.1-11
[12]	Bao J, Liu X, Xiang Z, Wei G (2020) Multi-Objective Optimization Algorithm and Preference Multi-Objective Decision-Making Based on Artificial Intelligence Biological Immune System. IEEE Access vol. 8:160221-160230. doi:10.1109/ACCESS.2020.3020054
[13]	Barthelemy JFM (1998) Improved multilevel optimization approach for the design of complex engineering systems. AIAA Journal, vol. 26(3):353-360. doi:10.2514/3.9896
[14]	Bayar N, Darmoul S, Hajri-Gabouj S, Pierreval H (2014) An immune based ontology implementation of hazard and operability analysis in production systems. Appl. Mech. Mater. 575:884-894. doi:10.4028/www.scientific.net/AMM.575.884
[15]	Bécue A, Praça I, Gama J (2021) Artificial intelligence, cyber-threats and Industry 4.0: challenges and opportunities. Artificial Intelligence Review 54:3849–3886. doi:10.1007/s10462-020-09942-2
[16]	Belardo S, Karwan KR, Wallace W (1984) An investigation of system design considerations

	for emergency management decision support. IEEE Transactions on Systems, Man, and Cybernetics SMC-14(6):795-804, November-December 1984. doi: 10.1109/TSMC.1984.6313308
[17]	Ben Othman S, Zgaya H, Dotoli M, Hammadi S (2017) An agent-based Decision Support System for resources' scheduling in Emergency Supply Chains. Control Engineering Practice, 59:27-43.doi:10.1016/j.conengprac.2016.11.014
[18]	Bevilacqua M, Ciarapica FE, Paciarotti C (2012) Business Process Reengineering of emergency management procedures: A case study. Safety Sci. 50(5):1368-1376. doi:10.1016/j.ssci.2012.01.002
[19]	Biard T, Le Mauff A, Bigand M, Bourey JP (2015) Separation of Decision Modeling from Business Process Modeling Using New "Decision Model and Notation" (DMN) for Automating Operational Decision-Making, IFIP Advances in Information and Communication Technology, v.463, p.1-8. doi:10.1007/978-3-319-24141-8_45
[20]	Blitch JG (1996) Artificial intelligence technologies for robot assisted urban search and rescue. Expert Systems with Applications 11(2):109-124
[21]	Bueno S, Banuls VA, Gallego MD (2021) Is urban resilience a phenomenon on the rise? A systematic literature review for the years 2019 and 2020 using textometry. International Journal of Disaster Risk Reduction 66:102588, p.1-14. doi:10.1016/j.ijdrr.2021.102588
[22]	Cabrera D, Rubilar R, Cubillos C (2019) Resilience in the Decision-Making of an Artificial Autonomous System on the Stock Market. IEEE Access, 7, art. no. 8856190, pp. 145246-145258. doi:10.1109/ACCESS.2019.2945471
[23]	Cai B, Liu Y, Liu Z, Chang Y, Jiang L (2019) Bayesian Networks for Reliability Engineering, pp. 1-257, doi: 10.1007/978-981-13-6516-4
[24]	Campbell CL, Turoff M, Van DeWalle B, Deek FP (2004) A Research Design for Asynchronous Negotiation of Software Requirements for an Emergency Response Information System. 10th Americas Conference on Information Systems, AMCIS 2004, pp. 3426 - 3432
[25]	Carter L, Yoon V, Liu D (2022) Analyzing e-government design science artifacts: A systematic literature review. International Journal of Information Management, 62, art. no. 102430, p.1-13. doi:10.1016/j.ijinfomgt.2021.102430
[26]	Çavdur F, Sebatlı-Sağlam A, Köse-Küçük M (2021) A scenario-based decision support system for allocating temporary-disaster-response facilities. Journal of the Faculty of Engineering and Architecture of Gazi University, 36(3):1499-1514. doi:10.17341/gazimmfd.685383
[27]	Chen C, Fragonara LZ, Tsourdos A (2021) RoIFusion: 3D Object Detection from LiDAR and Vision. IEEE Access 9:9393330:51710-51721. doi:10.1109/ACCESS.2021.3070379
[28]	Chen D, Liu Z, Wang L, Dou M, Chen J, Li H (2013) Natural disaster monitoring with wireless sensor networks: A case study of data-intensive applications upon low-cost scalable systems. Mobile Netw. Appl., vol. 18(5):651–663
[29]	Cheng ML, Matsuoka M, Liu W, Yamazaki F (2022) Near-real-time gradually expanding 3D land surface reconstruction in disaster areas by sequential drone imagery. Automation in Construction, 135, art. no. 104105, p.1-12. doi:10.1016/j.autcon.2021.104105
[30]	Christou V, Bocchini P, Miranda MJ (2016) Optimal representation of multi-dimensional random fields with a moderate number of samples: Application to stochastic mechanics. Probabilistic Engineering Mechanics 44:53-65. doi:10.1016/j.probengmech.2015.09.016
[31]	Clímaco JCN, Craveirinha JMF, Pascoal MMB (2006) An automated reference point-like approach for multicriteria shortest path problems. J. Syst. Sci. Syst. Eng. 15, 314–329, doi.org/10.1007/s11518-006-5015-5
[32]	Comes T, Conrado C, Hiete M, Kamermans M, Pavlin G, Wijngaards N (2010) An intelligent decision support system for decision making under uncertainty in distributed reasoning frameworks. In: C. Zobel, B.T.S. French (Eds.), ISCRAM 2010 – 7th International Conference on Information Systems for Crisis Response and Management: Defining Crisis Management 3.0, Proceedings, Seattle, p.1-10

[33]	Comes T, Van de Walle BA (2014) Measuring disaster resilience: The impact of hurricane sandy on critical infrastructure systems. In: P.C. Shih, L. Plotnick, S.R. Hiltz (Ed.), ISCRAM 2014 Conference Proceedings – 11th International Conference on Information Systems for Crisis Response and Management, pp. 195–204, University Park, PA, The Pennsylvania State University
[34]	Cremen G, Galasso C (2021) A decision-making methodology for risk-informed earthquake early warning. Computer-Aided Civil and Infrastructure Engineering, 36(6): 747-761. doi:10.1111/mice.12670
[35]	Daclin N, Chapurlat V (2009) An Anticipative Effects-Driven Approach for Analyzing Interoperability in Collaborative Processes. In: L.M. Camarinha-Matos et al. (Eds.): PRO-VE 2009, IFIP AICT 307:441–448
[36]	Dahal A, Sharma P, Hazarika MK (2020) Implementation of integrated geospatial platform, database, and application for disaster risk management in Uttarakhand. 40th Asian Conference on Remote Sensing, ACRS 2019: Progress of Remote Sensing Technology for Smart Future, p.1-10.
[37]	De La Huerga MR, Bañuls VA, Turoff M (2015) A scenario-based approach for analyzing complex cascading effects in Operational Risk Management. ISCRAM 2015 Conference Proceedings - 12th International Conference on Information Systems for Crisis Response and Management, 2015-January, pp. 244 - 253
[38]	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
[39]	De Vita F, Bruneo D, Das SK (2020) On the use of a full stack hardware/software infrastructure for sensor data fusion and fault prediction in industry 4.0. Pattern Recognition Letters 138:30-37. doi:10.1016/j.patrec.2020.06.028
[40]	Degener P, Gösling H, Geldermann J (2013) Decision support for the location planning in disaster areas using multi-criteria methods. In: T. Comes, F. Fiedrich, S. Fortier, J. Geldermann, and T. Müller (Eds.), ISCRAM 2013 Conference Proceedings – 10th International Conference on Information Systems for Crisis Response and Management, pp. 278–283, KIT, Baden-Baden: Karlsruher Institut fur Technologie
[41]	Demeyer S, Goedgebeur J, Audenaert P, Mario Pickavet M, Demeester P (2013) Speeding up Martins' algorithm for multiple objective shortest path problems. 4OR-Q J Oper Res 11, 323–348. https://doi.org/10.1007/s10288-013-0232-5
[42]	Di Vaio A, Palladino R, Hassan R, Escobar O (2020) Artificial intelligence and business models in the sustainable development goals perspective: A systematic literature review, Journal of Business Research 121:283-314. doi:10.1016/j.jbusres.2020.08.019
[43]	Diez-Olivan A, Del Ser J, Galar D, Sierra B (2019) Data fusion and machine learning for industrial prognosis: Trends and perspectives towards Industry 4.0. Information Fusion 50:92-111. doi:10.1016/j.inffus.2018.10.005
[44]	Domdouzis, K (2018) Artificial-intelligence-based service-oriented architectures (SOAs) for crisis management. Handbook of Research on Investigations in Artificial Life Rese¬arch and Development, pp. 79–95. IGI (2018). DOI: 10.4018/978-1-5225-5396-0.ch005
[45]	Drogosz J (2001) Safety and Security Bezpieczeństwo i Zabezpieczenia; Systemy alarmowe nr 1
[46]	Drogosz J (2001) Safety and Security Bezpieczeństwo i Zabezpieczenia; Systemy alarmowe, nr 1
[47]	Duan XH, Wu JX, Xiong YL (2022) Dynamic Emergency Vehicle Path Planning and Traffic Evacuation Based on Salp Swarm Algorithm. Journal of Advanced Transportation, art. no. 7862746, p.1-28. doi:10.1155/2022/7862746
[48]	Erdelj M, Król M, Natalizio E (2017) Wireless Sensor Networks and Multi-UAV systems for natural disaster management. Computer Networks, vol. 124:72-86. doi:

	10.1016/j.comnet.2017.05.021
[49]	Fang C, Marle F, Zio E, Bocquet JC (2012) Network theory-based analysis of risk interactions in large engineering projects. Reliability Engineering & System Safety, 106, p.1-10
[50]	Favereau M, Robledo LF, Villalobos D, Descote PY (2022) On disasters evacuation modeling: From disruptive to slow-response decisions. International Journal of Disaster Risk Reduction 67:102678, p.1-11. doi:10.1016/j.ijdrr.2021.102678
[51]	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
[52]	Foresti GL, Marcenaro L, Regazzoni CS (2002) Automatic detection and indexing of video-event shots for surveillance applications. IEEE Trans. Multimedia 4(4):459-471. doi:10.1109/TMM.2002.802024
[53]	Fu C, Dong C, Mertz C, Dolan JM (2020) Depth completion via inductive fusion of planar LIDAR and monocular camera. IEEE International Conference on Intelligent Robots and Systems 9341385:10843-10848. doi:10.1109/IROS45743.2020.9341385
[54]	Gabriel I (2020) Artificial Intelligence, Values, and Alignment, Minds and Machines 30(3):411-437. doi:10.1007/s11023-020-09539-2
[55]	Gaj P (2013) Aspekty bezpieczeństwa komputerowych systemów przemysłowych; Napędy i sterowanie nr 4, p.1-11
[56]	Gandibleux X, Beugnies F, Randriamasy S (2006) Martins' algorithm revisited for multi-objective shortest path problems with a MaxMin cost function. 4OR 4, 47–59. https://doi.org/10.1007/s10288-005-0074-x
[57]	Ganjehi S, Norouzi Khatiri K (2021) Determination of emergency roads to emergency accommodation using loss analysis results. Geoenvironmental Disasters 8,1(15), p.1-25. doi:10.1186/s40677-021-00190-2
[58]	Garbolino E, Chéry JP, Guarnieri F (2019) Systems dynamics applied to the analysis of risk at an industrial installation. Safety Dynamics, Evaluating Risk in Complex Industrial Systems, pp. 31-91. Springer, Advanced Sciences and Technologies for Security Applications. doi:10.1007/978-3-319-96259-7_2
[59]	Gębka A (2020) Projekt wykonawczy systemu dozory wizyjnego w Kopalni Wapienia Czatkowice
[60]	Geng S, Hou H, Zhou Z (2023) A dynamic multi-objective model for emergency shelter relief system design integrating the supply and demand sides, Natural Hazards, p.1-25. doi:10.1007/s11069-023-06280-8
[61]	Gerow JE, Thatcher JB, Grover V (2015) Six types of IT-business strategic alignment: An investigation of the constructs and their measurement. European Journal of Information Systems 24(5):465–491. doi:10.1057/ejis.2014.6
[62]	Ghadge A, Er M, Ivanov D, Chaudhuri A (2022) Visualisation of ripple effect in supply chains under long-term, simultaneous disruptions: a system dynamics approach. International Journal of Production Research, 60 (20), pp. 6173 – 6186. Doi:10.1080/00207543.2021.1987547
[63]	Ghavami SM (2019) Multi-criteria spatial decision support system for identifying strategic roads in disaster situations. International Journal of Critical Infrastructure Protection 24:23-36. doi:10.1016/j.ijcip.2018.10.004
[64]	Górecki H, Skulimowski AMJ (1988) Safety Principle in Multiobjective Decision Support in the Decision Space Defined by Availability of Resources. Arch. Automatyki i Telem., 32, 339-353
[65]	Groth K, Wang C, Mosleh A (2010) Hybrid causal methodology and software platform for probabilistic risk assessment and safety monitoring of socio-technical systems. Reliability Engineering & System Safety, 95, p.1-10
[66]	Guo J, Wu X, Wei G (2020) A new economic loss assessment system for urban severe rainfall

	and flooding disasters based on big data fusion. Environmental Research 188: 109822, p.1-10. doi:10.1016/j.envres.2020.109822
[67]	Guo J, Xu J, He Z, Liao W (2021) Research on risk propagation method of multimodal transport network under uncertainty. Physica A: Statistical Mechanics and its Applications, 563, art. no. 125494, p.1-21. doi:10.1016/j.physa.2020.125494
[68]	Habibi F, Chakrabortty RK, Abbasi A (2023) Evaluating supply chain network resilience considering disruption propagation. Computers and Industrial Engineering, 183, art. no. 109531, p.1-23. doi:10.1016/j.cie.2023.109531
[69]	Han Y, Shen J, Zhu X, An B, Liu F, Bao X (2024) Study on the Mechanism of Safety Risk Propagation in Subway Construction Projects. Sustainability (Switzerland), 16 (2), art. no. 796, p.1-27. doi:10.3390/su16020796
[70]	Hasan MM, Lwin K, Imani M, Shabut A, Bittencourt LF, Hossain MA (2019) Dynamic multi-objective optimisation using deep reinforcement learning: benchmark, algorithm and an application to identify vulnerable zones based on water quality. Engineering Applications of Artificial Intelligence 86:107–135
[71]	Hasani S, El-Haddadeh R, Aktas E (2014) A disaster severity assessment decision support tool for reducing the risk of failure in response operations. WIT Transactions on Information and Communication Technologies, 47:69-380. doi:10.2495/RISK140311
[72]	Hernantes J, Labaka L, Turoff M, Hiltz SR, Bañuls VA (2017) Moving forward to disaster resilience: Perspectives on increasing resilience for future disasters. Tech. Forec. Soc. Change 121:1-6. doi:10.1016/j.techfore.2017.05.011
[73]	Hevner AR, March ST, Park J, Ram S (2004) Design Science in Information Systems Research. MIS Quarterly 28(1):75-105. https://www.jstor.org/stable/25148625
[74]	Huang J, Lyamin AV, Griffiths DV, Krabbenhoft K, Sloan SW (2013) Quantitative risk assessment of landslide by limit analysis and random fields. Computers and Geotechnics 53:60-67. doi:10.1016/j.compgeo.2013.04.009
[75]	Huang JH, Sun MG, Cheng Q (2021) Congestion risk propagation model based on multi-layer time-varying network. International Journal of Simulation Modelling, 20 (4), pp. 730 – 741. doi:10.2507/IJSIMM20-4-585
[76]	Ibrahim AM, Venkat I, Subramanian KG, Khader AT, De Wilde P (2016) Intelligent Evacuation Management Systems: A Review. ACM Trans. Intell. Syst. Technol. 7, Art. 36:27, p.1-27. doi:10.1145/2842630
[77]	Ibrahim N, Hassan FH, Ab Wahab MN, Letchmunan S (2022) Emergency route planning with the shortest path methods: static and dynamic obstacles. International Journal of Simulation Modelling, 21(3):429-440. doi:10.2507/IJSIMM21-3-608
[78]	Iglesias A, del Castillo MD, Serrano JI, Oliva J (2011) A decision support system applied to emergency situations in real time [Sistema de Ayuda a la Decisión Aplicado a Situaciones de Emergencia en Tiempo Real]. RIAI - Revista Iberoamericana de Automatica e Informatica Industrial, 8(1):80-88. doi:10.4995/RIAI.2011.01.10
[79]	Islam KA, Chen DQ, Marathe M, Mortveit H, Swarup S, Vullikanti A (2023) Simulation-Assisted Optimization for Large-Scale Evacuation Planning with Congestion-Dependent Delay, IJCAI International Joint Conference on Artificial Intelligence, 2023-August, pp. 5359 – 5367
[80]	Islam MA, Anderson DT, Pinar AJ, Havens TC, Scott G, Keller JM (2020) Enabling Explainable Fusion in Deep Learning with Fuzzy Integral Neural Networks. IEEE Transactions on Fuzzy Systems 28(7):8715679:1291-1300. doi:10.1109/TFUZZ.2019.2917124
[81]	Jabbari R, bin Ali N, Petersen K, Tanveer B (2016) What is DevOps? A Systematic Mapping Study on Definitions and Practices. In: Proceedings of the Scientific Workshop of XP2016 (XP'16 Workshops), Art. #12, p. 11. Association for Computing Machinery, New York, NY, USA. doi:10.1145/2962695.2962707
[82]	Janssens GK, Pangilinan JM (2011) An Empirical Evaluation of Martins' Algorithm for the

	Multi-Objective Shortest Path Problem. ESM 2011 - European Simulation and Modelling Conference: Modelling and Simulation 2011, pp. 252–256
[83]	Jiang Z, Shen S, Ouyang Y (2023) Planning of reliable targeted evacuation under the threat of disasters, Transportation Research Part C: Emerging Technologies, 153, art. no. 104197, p.1-13. doi:10.1016/j.trc.2023.104197
[84]	Ju J, Wang Q, Wang W, Ni M (2024) Resilience enhancement strategy for cyber–physical distribution systems that considers cross-space propagation of information risk. IET Renewable Power Generation, 18 (7), pp. 1193 – 1203. doi:10.1049/rpg2.12767
[85]	Kaliszewski I (2008) Wielokryterialne podejmowanie decyzji: obliczenia miękkie dla złożonych problemów decyzyjnych. WNT, Warszawa, s.154
[86]	Kaplan S, Garrick BJ (1981) On the quantitative definition of risk, Risk anal.1, p.11-27
[87]	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
[88]	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
[89]	Kerr C, Phaal R (2020) Technology roadmapping: Industrial roots, forgotten history and unknown origins. Technological Forecasting and Social Change, vol. 155, Art. No. 119967:16. doi:10.1016/j.techfore.2020.119967
[90]	Kongsvik T, Almklov P, Haavik T, Haugen S, Vinnem JE, Schiefloe PM (2015) Decisions and decision support for major accident prevention in the process industries. Journal of Loss Prevention in the Process Industries, 35:85-94. doi:10.1016/j.jlp.2015.03.018
[91]	Korolov V, Kurowska K, Korolova O, Zaiets Y, Milkovich I, Kryszk H (2021) Methodology for determining the nearest destinations for the evacuation of people and equipment from a disaster area to a safe area. Remote Sensing 13(11):2170, p.1-18. doi:10.3390/rs13112170
[92]	Krechowicz M. (2017) Risk Management in Complex Construction Projects that Apply Renewable Energy Sources: A Case Study of the Realization Phase of the Energis Educational and Research Intelligent Building, IOP Conference Series: Materials Science and Engineering, 245 (6), art. no. 062007, doi:10.1088/1757-899X/245/6/062007
[93]	Kucwaj J (1996) Delaunay triangulation of surfaces, ZAMM Zeitschrift fur Angewandte Mathematik und Mechanik, 76 (SUPPL. 3), pp. 487 - 488
[94]	Kulkarni AJ (2022) Multiple Criteria Decision Making: Techniques, Analysis and Applications doi:10.1007/978-981-16-7414-3
[95]	Lai K, Yanushkevich SN, Shmerko VP (2021) Intelligent Stress Monitoring Assistant for First Responders. IEEE Access, 9, art. no. 9348878:25314-25329. doi:10.1109/ACCESS.2021.3057578
[96]	Lam F, Lalansingh CM, Babaran HE, Wang Z, Prokopec SD, Fox NS, Boutros PC (2016) VennDiagramWeb: A web application for the generation of highly customizable Venn and Euler diagrams, art. no. 401, p.1-8. doi:10.1186/s12859-016-1281-5
[97]	Lamnabhi-Lagarrigue F, Annaswamy A, Engell S, Isaksson A, Khargonekar P, Murray RM, Nijmeijer H, Samad T, Tilbury D, Van den Hof P (2017) Systems & Control for the future of humanity, research agenda: Current and future roles, impact and grand challenges. Annual Reviews in Control 43:1–64
[98]	Laskov LM, Marinov ML (2023. List of Pareto Optimal Solutions of a Biobjective Shortest Path Problem, 2023 18th Conference on Computer Science and Intelligence Systems (FedCSIS), Warsaw, Poland, pp. 603-613, doi: 10.15439/2023F3718.
[99]	Lessin AM, Lunday BJ, Hill RR (2019) A multi-objective, bilevel sensor relocation problem for border security. IISE Trans., vol. 51(10):1091-1109. doi:10.1080/24725854.2019.1576952
[100]	Li G, Zhang L, Wang Z (2014) Optimization and planning of emergency evacuation routes considering traffic control. Scientific World Journal 164031, p.1-15. doi:10.1155/2014/164031
[101]	Li J, Yu A, Xu B (2022) Risk propagation and evolution analysis of multi-level handlings at

automated terminals based on double-layer dynamic network model. Physica A: Statistical Mechanics and its Applications, 605, art. no. 127963, p.1-16. doi:10.1016/j.physa.2022.127963

[102] Li X, Zhang L, Xiao T, Zhang S, Chen C (2019) Learning failure modes of soil slopes using monitoring data. Probabilistic Engineering Mechanics 56:50-57. doi: 10.1016/j.probengmech.2019.04.002

[103] Likhachev M, Ferguson D, Gordon G, Stentz A, Thrun S (2008) Anytime Search in Dynamic Graphs, Artificial Intelligence, 172, 1613–1643, doi.org/10.1016/j.artint.2007.11.009

[104] Liu S, Chen J, Weiszer M (2022) Multi-objective Multigraph A* Search with Learning Heuristics based on Node Metrics and Graph Embedding, *2022 IEEE 11th International Conference on Intelligent Systems (IS)*, Warsaw, Poland, pp. 1-8, doi: 10.1109/IS57118.2022.10019653.

[105] Liu W (2013) Discussion on Enterprise Emergency Management Decision Support System. In: Du Z. (ed.) Intelligence Computation and Evolutionary Computation. Advances in Intelligent Systems and Computing, vol 180, p.73-77. Springer, Berlin, Heidelberg. doi:10.1007/978-3-642-31656-2_1

[106] Liu Y, Li Y, Huang D, Packo P (2020) A Multiobjective Optimization Model for Continuous Allocation of Emergency Rescue Materials. Mathematical Problems in Engineering, art. no. 5693182, p.1-15. doi:10.1155/2020/5693182

[107] Lo MK, Leung YF, Ku T (2021) Variability response function approach for foundation reliability. Probabilistic Engineering Mechanics 64:103129, p.1-15. doi:10.1016/j.probengmech.2021.103129

[108] López-Silva J, Bañuls VA, Turoff M (2015) Scenario based approach for risks analysis in critical infrastructures. ISCRAM 2015 Conference Proceedings - 12th International Conference on Information Systems for Crisis Response and Management, 2015-January, p.1-9

[109] Ma Y, Wang Y, Zhao Y (2015) Realization of VR Technology - based Flood Control DSS. In; Proceedings of the 5th International Yellow River Forum on Ensuring Water Right of the River's Demand and Healthy River Basin Maintenance. Zhengzhou, China, Sept. 24-28, 2012, Vol. V, pp. 45-50

[110] Marcos MP, Pitarch JL, de Prada C (2020) Decision support system for a heat-recovery section with equipment degradation. Decision Support Systems, 137, art. no. 113380, p.1-10. doi:10.1016/j.dss.2020.113380

[111] Markowitz H (1959) Portfolio Selection: Efficient Diversification of Investments, Yale Univ. Press

[112] Maristany de las Casas P, Sedeño-Noda A, Borndörfer R (2021) An Improved Multiobjective Shortest Path Algorithm, Computers & Operations Research 135, 105424, doi.org/10.1016/j.cor.2021.105424

[113] Marovac N, Stähly P (2001) CRISIS-2000: A decision support system for major disasters. International Symposium on OR, Dresden, Germany, Sept. 09-12, 2000. Operations Research Proceedings 2000, Springer Verlag AG, pp. 246-253

[114] Martínez-Frutos J, Herrero-Pérez D, Kessler M, Periago F (2018) Risk-averse structural topology optimization under random fields using stochastic expansion methods. Computer Methods in Applied Mechanics and Engineering 330:180-206. doi:10.1016/j.cma.2017.10.026

[115] Martins, E.Q.V. (1984). On a multicriteria shortest path problem. Eur J Oper Res 16, 236–245

[116] McCallum I, Liu W, See L, Mechler R, Keating A, Hochrainer-Stigler S, Mochizuki J, Fritz S, Dugar S, Arestegui M, Szoenyi M, Laso B, Burek P, French A, Moorthy I (2016) Technologies to Support Community Flood Disaster Risk Reduction. Int J Disaster Risk Sci 7:198–204. doi:10.1007/s13753-016-0086-5

[117] Mehla S, Jain S (2020) An ontology supported hybrid approach for recommendation in emergency situations. Ann. Telecommun., vol. 75:421–435. doi:10.1007/s12243-020-00786-z

[118]	Middleton SE, Middleton L, Modafferi S (2014) Real-time crisis mapping of natural disasters using social media. IEEE Intell. Syst. 29(2):9-17. doi:10.1109/MIS.2013.126
[119]	Minhas MR, Potdar V (2020) Decision support systems in construction: A bibliometric analysis. Buildings, 10 (6), art. no. 108, p.1-26. doi:10.3390/BUILDINGS10060108
[120]	Monge JJ, McDonald N, McDonald GW (2022) A review of graphical methods to map the natural hazard-to-wellbeing risk chain in a socio-ecological system, Science of the Total Environment, 803, art. no. 149947, doi: 10.1016/j.scitotenv.2021.149947, p.1-17
[121]	Moradi R, Growth K (2020) Modernizing risk assessment: A systematic integration of PRA and PHM techniques. Reliability Engineering & System Safety 204, p.1-11
[122]	Moyano F, Fernandez-Gago C, Lopez J (2012) A Conceptual Framework for Trust Models, Trust, Privacy and Security in Digital Business. Lecture Notes in Computer Science, vol. 7449, Springer-Verlag, Berlin-Heidelberg, pp. 93-104
[123]	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
[124]	Palestini L (2021) Communication and decision support systems. International Journal of Safety and Security Engineering, 11(4):397-407. doi:10.18280/ijsse.110413
[125]	Parhizkar T, Vinnem JE, Utne IB, Mosleh A (2021) Supervised Dynamic Probabilistic Risk Assessment of Complex Systems, Part 1: General Overview. Reliability Engineering & System Safety, Volume 208, p.1-12
[126]	Pearl J (1988) Probabilistic Reasoning in Intelligent Systems. Morgan-Kaufmann, San Mateo
[127]	Pfetsch ME, Schmitt A (2023) A generic optimization framework for resilient systems. Optimization Methods and Software, 38(2):356-385
[128]	PMBOK Guide - Seventh Edition (2021) A Guide to the Project Management Body of Knowledge, Project Management Institute
[129]	Porte J, Briones A, Maso JM, Pares C, Zaballos A, Pijoan JL (2020) Heterogeneous wireless IoT architecture for natural disaster monitorization. EURASIP J Wireless Com Network, art. 184:27. doi:10.1186/s13638-020-01793-3
[130]	Prońko J, Wojtasiak B (2018) Analiza wielokryterialna w badaniach nad bezpieczeństwem. Zeszyty Naukowe SGSP 2018, Nr 66 (TOM 2)/2/2018, p.1-21
[131]	Purba DSD, Kontou E, Vogiatzis C (2022) Evacuation route planning for alternative fuel vehicles. Transportation Research Part C: Emerging Technologies, 143, art. no. 103837, p.1-32. doi:10.1016/j.trc.2022.103837
[132]	Purohit H, Kanagasabai R, Deshpande N (2019) Towards Next Generation Knowledge Graphs for Disaster Management. In: 2019 IEEE 13th International Conference on Semantic Computing (ICSC), pp. 474-477. doi:10.1109/ICOSC.2019.8665638
[133]	Qin L, Xu W, Zhao X, Ma Y (2020) Typhoon track change-based emergency shelter location-allocation model: A case study of Wenchang in Hainan province. Injury Prevention 26(3):196-203. doi:10.1136/injuryprev-2018-043081
[134]	Rest KD, Hirsch P (2022) Insights and decision support for home health care services in times of disasters. Central European Journal of Operations Research, 30 (1), pp. 133-157. doi:10.1007/s10100-021-00770-5
[135]	Reyes-Riveros R, Altamirano A, De La Barrera F, Rozas-Vasquez D, Vieli L, Meli P (2021) Linking public urban green spaces and human well-being: A systematic review. Urban Forestry & Urban Greening 61:127105, p.1-15. doi:10.1016/j.ufug.2021.127105
[136]	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
[137]	Rodriguez A, Fernandez-Medina, Trujillo J, Piattini M (2011) Secure business process model specification through a UML 2.0 activity diagram profile. Decision Support Systems,

51(3):446 – 465. doi:10.1016/j.dss.2011.01.018

[138] Rolland E, Patterson RA, Ward K, Dodin B (2010) Decision support for disaster management. Operations Management Research, 3(1):68-79. doi:10.1007/s12063-010-0028-0

[139] 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

[140] Rostek K, Wiśniewski M (2014) Zarządzanie wiedzą w doskonaleniu i rozwoju systemu bezpieczeństwa Logistyka 5:1292-1303

[141] Sahebjamnia N, Torabi SA, Mansouri SA (2017) A hybrid decision support system for managing humanitarian relief chains. Decision Support Systems, 95:12-26. doi:10.1016/j.dss.2016.11.006

[142] Saleh HA, Allaert G (2011) Scientific Research Based Optimisation and Geo-information Technologies for Integrating Environmental Planning in Disaster Management. In: D. Tang (ed.), Remote Sensing of the Changing Oceans, Chapter 19, 9th Pan Ocean Remote Sensing Conference, PORSEC 2008, Guangzhou, China, Dec. 02-06, 2008, pp. 359-390, Springer-Verlag, Berlin Heidelberg. doi:10.1007/978-3-642-16541-2_19

[143] Sengupta R, Lafortune S (1992) A graph-theoretic optimal control problem for terminating discrete event processes. Discrete Event Dyn Syst 2, 139–172. doi.org/10.1007/BF01797725

[144] Seppanen H, Virrantaus K (2015) Shared situational awareness and information quality in disaster management. Safety Sci. 77:112-122. doi:10.1016/j.ssci.2015.03.018

[145] Septiana Y (2018) Design of prototype decision support system for flood detection based on ultrasonic sensor. MATEC Web of Conferences, 197, art. no. 03017, p.1-4. doi:10.1051/matecconf/201819703017

[146] Sepulveda J, Bull J (2019) A Model-Driven Decision Support System for Aid in a Natural Disaster. In: IHSED 2019: Human Systems Engineering and Design II, Advances in Intelligent Systems and Computing 1026:523-528

[147] Sepulveda J, Bull J (2020) A Model-Driven Decision Support System for Aid in a Natural Disaster, Advances in Intelligent Systems and Computing, 1026, pp. 523 – 528. doi:10.1007/978-3-030-27928-8_79

[148] Shan H, Fei J, Shi J, Zhang Q, Yan F, Qiu J (2024) Investigation of risk propagation and control in emergency response logistics networks: A cellular automata based approach. Computers and Industrial Engineering, 193, art. no. 110267, p.1-20. doi:10.1016/j.cie.2024.110267

[149] Shan H, Guo Q, Wei J (2023) The impact of disclosure of risk information on risk propagation in the industrial symbiosis network. Environmental Science and Pollution Research, 30 (16), pp. 45986 – 46003. doi:10.1007/s11356-023-25592-7

[150] Shi F, Marini JL, Audry E (2015) Towards a Psycho-Cognitive Recommender System. In: ERM4CT '15: Proceedings of the International Workshop on Emotion Representations and Modelling for Companion Technologies, November 9-13 2015, Seattle, pp. 25-31. doi:10.1145/2829966.2829968

[151] Shi Q, An P, Kang K, Hu J, Han T, Rauterberg M (2023) Investigating socially assistive systems from system design and evaluation: a systematic review. Universal Access in the Information Society, 22:609–633. doi:10.1007/s10209-021-00852-w

[152] Shin Y, Kim S, Moon I (2019) Integrated optimal scheduling of repair crew and relief vehicle after disaster. Computers and Operations Research 105:237-247

[153] Simões-Marques M, Mendonça P, Figueiredo D, Nunes IL (2019) Disaster Management Support System Prototype Design Evolution Based on UX Testing. In: Nunes I. (eds), AHFE 2019: Advances in Human Factors and Systems Interaction, Advances in Intelligent Systems and Computing 959:374-385. doi:10.1007/978-3-030-20040-4_34

[154] Siskos Y, Grigoroudis E, Matsatsinis NF (2016) UTA Methods W: Greco S, Ehrgott M, Figueira J (red.) Multiple Criteria Decision Analysis. International Series in Operations

	Research & Management Science, vol. 233, s.315-362, Springer, New York, doi.org/10.1007/978-1-4939-3094-4_9
[155]	Skulimowski AMJ (1996) Decision Support Systems Based on Reference Sets. Monografie t.40, Wyd. AGH, Kraków
[156]	Skulimowski AMJ (1997) Methods of Multicriteria Decision Support Based on Reference Sets. In: R. Caballero, F. Ruiz, R.E. Steuer (Eds.), Advances in Multiple Objective and Goal Programming, Lecture Notes in Economics and Mathematical Systems, 455, Springer-Verlag, Berlin-Heidelberg -New York, pp. 282-290. doi:10.1007/978-3-642-46854-4_31
[157]	Skulimowski AMJ (2006) Framing new member states and candidate countries information society insights. Prospects for a knowledge-based society in the new members states and candidate countries, FISTERA Foresight on Information Society Technologies in the European Research Area. — Bucharest: The Publishing House of the Romanian Academy, pp 9-58
[158]	Skulimowski AMJ (2011) Freedom of Choice and Creativity in Multicriteria Decision Making. In: T. Theeramunkong, S. Kunifuji, C. Nattee, and V. Sornlertlamvanich V. (eds.), Knowledge, Information, and Creativity Support Systems: KICSS2010 Revised Selected Papers, Lect, Notes in Artif. Intell., vol. 6746, Springer, Berlin; Heidelberg, pp. 190-203
[159]	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
[160]	Skulimowski AMJ (2019) Multicriteria Coordination of Flood Control in Water Reservoir Systems, In: 24th International Conference on Methods and Models in Automation and Robotics (MMAR), Aug. 2019, pp. 296-301. doi:10.1109/MMAR.2019.8864657
[161]	Skulimowski AMJ (2023) Reconciling Inconsistent Preference Information in Group Multicriteria Decision Support with Reference Sets. In: Fujita, H., Wang, Y., Xiao, Y., Moonis, A. (eds), Advances and Trends in Artificial Intelligence. Theory and Applications. IEA/AIE 2023. Lecture Notes in Computer Science, 13925, Springer, Cham. doi.org/10.1007/978-3-031-36819-6_18
[162]	Skulimowski AMJ, Bañuls VA (2021) AI Alignment of Disaster Resilience Management Support Systems. In: Rutkowski, L. et al. (eds) Artificial Intelligence and Soft Computing. ICAISC 2021. Lect. Notes in Artif. Intell. 12855:354-366. Springer (2021)
[163]	Skulimowski AMJ, Banuls VA (2021) Metodologia projektowania systemów zarządzania bezpieczeństwem przemysłowym wykorzystujących techniki i narzędzia sztucznej inteligencji, Raport Techniczny NAWA
[164]	Skulimowski AMJ, Ćwik A (2017) Communication Quality in Anticipatory Vehicle Swarms: A Simulation-Based Model. In: Peng SL, Lee GL, Klette R, Hsu CH (eds), Internet of Vehicles. Technologies and Services for Smart Cities. IOV 2017, Lecture Notes in Computer Science 10689:119-134. doi:10.1007/978-3-319-72329-7_11
[165]	Skulimowski AMJ, Łydek P (2022a) 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
[166]	Skulimowski AMJ, Łydek P (2022b) AI-based design of decision support systems for industrial risk management. In: PP-RAI'2022: Proceedings of the 3rd Polish Conference on Artificial intelligence, April 25–27, 2022, Gdynia, Poland. Gdynia Maritime University Press, pp. 138-142
[167]	Skulimowski AMJ, Łydek P (2022c) 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/
[168]	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

[169] Skulimowski AMJ, Pukocz P (2012) Enhancing creativity of strategic decision processes by technological roadmapping and foresight", in: V.C.S. Lee, K.L. Ong (eds.), KICSS 2012: 7th International Conference on Knowledge, Information and Creativity Support Systems: Melbourne, VIC, Australia, 8–10 Nov. 2012. IEEE Computer Society, CPS, pp. 223–230. doi:10.1109/KICSS.2012.42

[170] Šliogeriene J, Kaklauskas A, Štreimikiene D, Bianchi M (2012) Multiple criteria decision support system for the assessment of energy generation technologies considering the dimension of values. International Journal of Strategic Property Management, 16 (4):370-391. doi:10.3846/1648715X.2012.722132

[171] Spyrou ED, Anagnostopoulou A, Kappatos V (2023) Cuckoo search algorithm for the evacuation strategy of people in flash floods using a spatiotemporal conditions weight, E3S Web of Conferences, 436, art. no. 02001, p.1-5. doi:10.1051/e3sconf/202343602001

[172] Sreedharan S, Chakraborti T, Muise C, Kambhampati S (2019) A General Framework for Synthesizing and Executing Self-Explaining Plans for Human-AI Interaction, In: ICAPS 2019 Proceedings, AAAI Press, p.9

[173] 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

[174] Sung I, Buderath M, Nielsen P (2022) Unpacking the Role of Artificial Intelligence for a Multimodal Service System Design. Electronics (Switzerland), 11 (4), art. no. 549, p.1-13. doi:10.3390/electronics11040549

[175] Takahashi H, Inagawa T, Sumitani Y, Omae Y (2023) Evacuation planning model using chain flow algorithm: case of different evacuation speeds, ICIC Express Letters, 17 (5), pp. 569 - 578. doi:10.24507/icicel.17.05.569

[176] Tarhan İ, Zografos KG, Sutanto J, Kheiri A (2023) A quadrant shrinking heuristic for solving the dynamic multi-objective disaster response personnel routing and scheduling problem, European Journal of Operational Research, p.776-791. doi:10.1016/j.ejor.2023.09.002

[177] Tarka P (2015) Własności 5- i 7-stopniowej skali Likerta w kontekście normalizacji zmiennych metodą Kaufmana i Rousseeuwa; Prace Naukowe Uniwersytetu Ekonomicznego ee Wrocławiu - Research Papers of Wrocław University of Economics nr 385:286-295

[178] Teniwut WA, Hasyim CL (2020) Decision support system in supply chain: A systematic literature review. Uncertain Supply Chain Management, 8(1):131-148. doi:10.5267/j.uscm.2019.7.009

[179] Turoff M (2002) Past and Future Emergency Response Information Systems, Communications of the ACM 45(4):29-32. doi:10.1145/505248.505265

[180] Turoff M (2014) Emergency management education and ISCRAM. ISCRAM 2014 Conference Proceedings - 11th International Conference on Information Systems for Crisis Response and Management, pp. 533 – 537

[181] Turoff M, Bañuls VA, Plotnick L, Hiltz SR, Ramírez de la Huerga M (2016) A collaborative dynamic scenario model for the interaction of critical infrastructures, Futures, 84, pp. 23 – 42. doi:10.1016/j.futures.2016.09.003

[182] Turoff M, Bañuls VA, Yang L (2017) A review of qualitative comments on a proposed master's degree in emergency management. Proceedings of the Annual Hawaii International Conference on System Sciences, 2017-January, pp. 247 - 256

[183] Uno K, Kashiyama K (2008) Development of Simulation System for the Disaster Evacuation Based on Multi-Agent Model Using GIS. Tsinghua Science and Technology 13(SUPPL.1):348-353. doi:10.1016/S1007-0214(08)70173-1

[184] Vadlamani S, C.O. A (2019) A stochastic B-spline wavelet on the interval finite element method for problems in elasto-statics. Probabilistic Engineering Mechanics 58:102996, p.1-15. doi:10.1016/j.probengmech.2019.102996

[185] van Engelen JE, Hoos HH (2020) A survey on semi-supervised learning. Mach. Learn.

109:373–440. doi:10.1007/s10994-019-05855-6

[186] Vernez D, Buchs DR, Pierrehumbert GE, Besrour A (2004) MORM - A Petri net based model for assessing OH&S risks in industrial processes: Modeling qualitative aspects. Risk Analysis 24(6):1719-1735. doi:10.1111/j.0272-4332.2004.00562.x

[187] Vieira O, Ribeiro RS, Diaz de Tuesta JL, Gomes HT, Silva AMT (2022) A systematic literature review on the conversion of plastic wastes into valuable 2D graphene-based materials. Chemical Engineering Journal 428:131399, p.1-15. doi:10.1016/j.cej.2021.131399

[188] Vince R (1992) The Mathematics of Money Management. Risk Analysis Techniques for Traders, Wiley, New York, p.377

[189] von der Gracht H, Bañuls VA, Turoff M, Skulimowski AMJ, Gordon TJ (2015) Foresight support systems: The future role of ICT for foresight. Technological Forecasting and Social Change 97:1-6. doi:10.1016/j.techfore.2014.08.010

[190] Voorberg S, Eshuis R, van Jaarsveld W, van Houtum GJ (2021) Decisions for information or information for decisions? Optimizing information gathering in decision-intensive processes. Decision Support Systems, 151, art. no. 113632, p.1-15. doi:10.1016/j.dss.2021.113632

[191] Wang J, Shen D, Yu M (2020) Multiobjective Optimization on Hierarchical Refugee Evacuation and Resource Allocation for Disaster Management. Mathematical Problems in Engineering 8395714, p.1-18. doi:10.1155/2020/8395714

[192] Wex F, Schryen G, Feuerriegel S, Neumann D (2014) Emergency response in natural disaster management: Allocation and scheduling of rescue units. European Journal of Operational Research, 235(3):697-708.doi:10.1016/j.ejor.2013.10.029

[193] Wilson DT, Hawe GI, Coates G, Crouch RS (2011) A decision support framework for large scale emergency response. WIT Transactions on the Built Environment, 119:87-98. doi:10.2495/DMAN110091

[194] Wilson DT, Hawe GI, Coates G, Crouch RS (2014) Evaluation of centralised and autonomous routing strategies in major incident response. Safety Science, 70:80-88. doi:10.1016/j.ssci.2014.05.001

[195] Windhouwer CJ, Klunder GA, Sanders FM (2005) Decision support system emergency planning, creating evacuation strategies in the event of flooding. Proceedings of ISCRAM 2005 - 2nd International Conference on Information Systems for Crisis Response and Management, pp. 171 - 180

[196] Wu CL, Chau KW (2006) A flood forecasting neural network model with genetic algorithm, International Journal of Environment and Pollution 28(3-4):261-273

[197] Xue S, Li J, Yu J, Li M, Shi X (2024) Research on Supply Chain Network Resilience: Considering Risk Propagation and Node Type. Applied Sciences (Switzerland), 14 (7), art. no. 2675, p.1-21. doi:10.3390/app14072675

[198] Yadav G, Paul K (2021) Architecture and security of SCADA systems: A review. International Journal of Critical Infrastructure Protection, 34, art. no.100433, p.1-26. doi:10.1016/j.ijcip.2021.100433

[199] Yan H, Li H, Sun Q, Jiang Y (2024) Propagation and control of congestion risk in scale-free networks based on information entropy. PLoS ONE, 19 (3 March), art. no. e0300422, p.1-13. doi:10.1371/journal.pone.0300422

[200] Yang X, Haugen S (2015) Classification of risk to support decision-making in hazardous processes. Safety Science, 80:115-126. doi:10.1016/j.ssci.2015.07.011

[201] Yang Z, Drake W, Li Y, Zobel C, Cowell M (2015) Fostering Community Resilience through Adaptive Learning in a Social Media Age: Municipal Twitter Use in New Jersey following Hurricane Sandy. In: L. Palen, M. Buscher, T. Comes, A. Hughes (Eds.), ISCRAM 2015 Conference Proceedings – 12th International Conference on Information Systems for Crisis Response and Management. University of Agder (UiA), Kristiansand, Norway, p.1-9

[202] Yatsalo B, Radaev A, Haktanir E, Skulimowski AMJ, Kahraman C (2024) A family of fuzzy multi-criteria sorting models FTOPSIS-Sort: features, case study analysis, and the statistics of

	distinctions. Expert Systems with Applications, 237 pt. B, art. no. 121486, p. 18, www.sciencedirect.com/science/article/pii/S0957417423019887
[203]	Zadorozhny V, Lee PJ, Lewis M (2015) Collaborative Information Sensemaking for Multi-Robot Search and Rescue. In: L. Palen, M. Buscher, T. Comes, A. Hughes (Eds.), ISCRAM 2015 Conference Proceedings – 12th International Conference on Information Systems for Crisis Response and Management, Kristiansand, Norway, University of Agder (UiA), p.1-9
[204]	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
[205]	Zhang C, An B, Wang Y, Lu D (2022) Data-Driven Crowd Evacuation Simulation Method Based on Raspberry Pi. Advances in Transdisciplinary Engineering, 20, pp. 870-877. doi:10.3233/ATDE220090
[206]	Zhang J, Zheng J, Zhang Z, Chen T, Tan YA, Zhang Q, Li Y (2024) ATT&CK-based Advanced Persistent Threat attacks risk propagation assessment model for zero trust networks. Computer Networks, 245, art. no. 110376, p.1-15. doi:10.1016/j.comnet.2024.110376
[207]	Zhang X, Liu Q, Huang H (2019) Numerical simulation of random fields with a high-order polynomial based Ritz–Galerkin approach. Probabilistic Engineering Mechanics 55:17-27. doi:10.1016/j.probengmech.2018.08.003
[208]	Zhang Y, Jiang W, Deng X (2019) Fault diagnosis method based on time domain weighted data aggregation and information fusion. International Journal of Distributed Sensor Networks 15(9), p.1-12. doi:10.1177/1550147719875629
[209]	Zhang Y, Yang N (2018) Vulnerability analysis of interdependent R&D networks under risk cascading propagation. Physica A: Statistical Mechanics and its Applications, 505, pp. 1056 – 1068. doi:10.1016/j.physa.2018.04.063
[210]	Zhu T, Haugen S, Liu Y (2021) Risk information in decision-making: definitions, requirements and various functions. Journal of Loss Prevention in the Process Industries, 72, art. no. 104572, p.1-13. doi:10.1016/j.jlp.2021.104572
[211]	Zilberstein S (1996) Using Anytime Algorithms in Intelligent Systems. AI Magazine, 17(3), 73, doi.org/10.1609/aimag.v17i3.1232
[212]	Zobel C (2010) Comparative visualization of predicted disaster resilience, Proceedings of the 7th International ISCRAM Conference, 2010, pp. 1–6
[213]	Zobel C (2011) Representing perceived tradeoffs in defining disaster resilience, Decis. Support. Syst. 50:394–403. doi:10.1016/j.dss.2010.10.001
[214]	Zobel CW, MacKenzie CA, Baghersad M, Li Y (2021) Establishing a frame of reference for measuring disaster resilience. Decision Support Systems, 140, art. no. 113406:11, p.1-12.. doi:10.1016/j.dss.2020.113406

Wykaz aktów prawnych, dokumentów wewnętrznych i standardów istotnych dla projektowania systemów wspomagania decyzji w sytuacji zagrożeń

[P.1] Jarmuszkiewicz C, Szymański T (2019) Ocena stanu bezpieczeństwa obiektu Kopalnia Wapienia Czatkowice - perymetr + ochrona fizyczna

[P.2] Plan Ruchu Zakładu Górniczego „Czatkowice" na lata 2018-2024

[P.3] PN-ISO 31000:2012 Zarządzanie ryzykiem - Zasady i wytyczne

[P.4] PN-ISO 31000:2018-08 Zarządzanie ryzykiem - Wytyczne

[P.5] PN-EN IEC 31010:2020-01 Zarządzanie ryzykiem - Techniki oceny ryzyka

[P.6] Polityka Systemu Zarządzania Bezpieczeństwem w Grupie TAURON

[P.7] Polityka Bezpieczeństwa fizycznego w Grupie TAURON

[P.8] Słownik pojęć i skrótów z zakresu Bezpieczeństwa fizycznego w Grupie TAURON

[P.9] Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. z 2002 r. Nr 62, poz. 558 z późn. zm)

[P.10] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. nr 89, poz. 590 z późn. zm.)

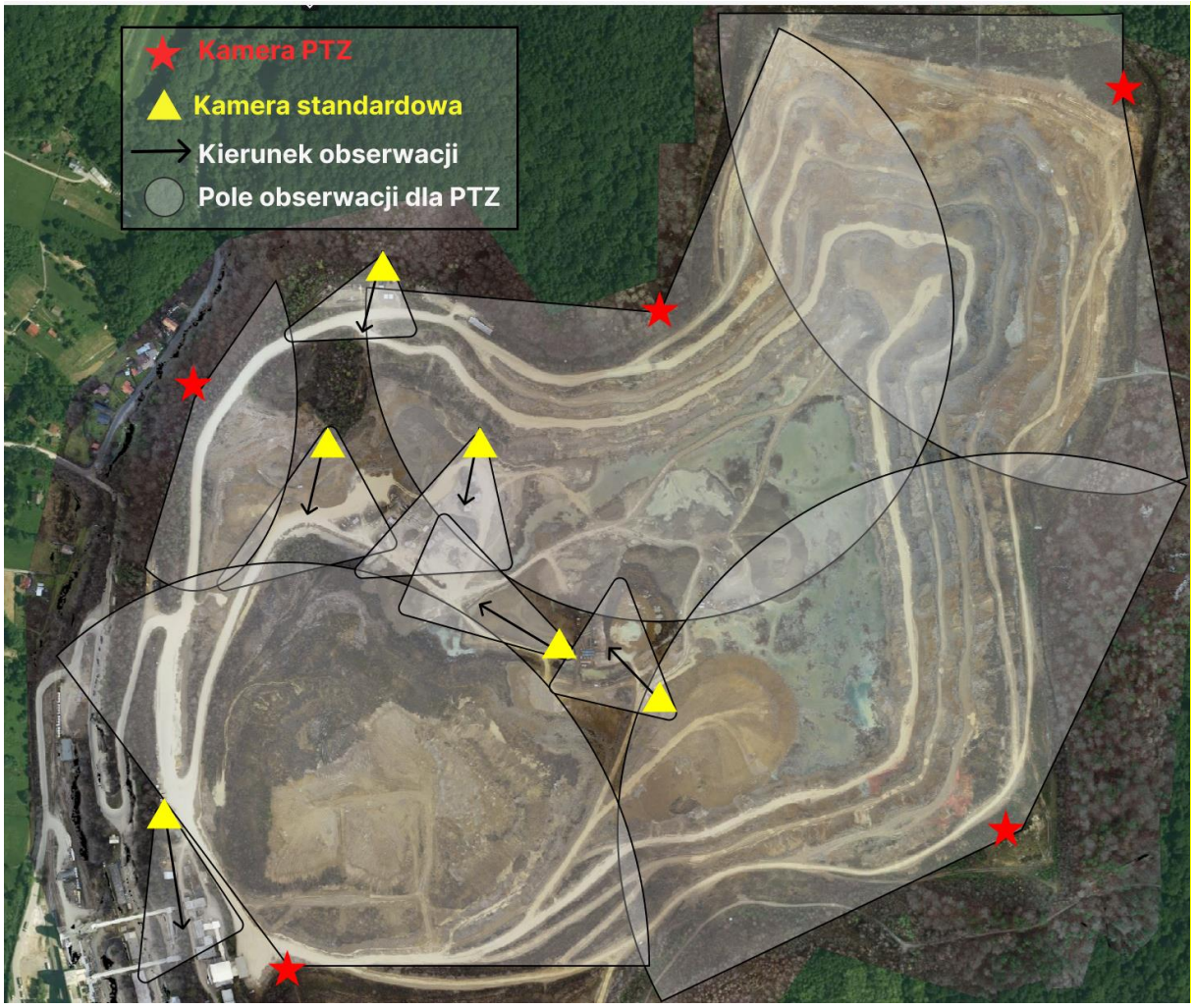
[P.11] Wsparcie Grupa Tauron Praca zbiorowa,: Techniczne środki zapewnienia bezpieczeństwa fizycznego koncepcja wstępna dla obiektu Kopalnia Wapienia Czatkowice.; 2019)

[P.12] Zasady komunikowania w sytuacjach kryzysowych w Grupie TAURON (Grudzień, 2020)

Dodatek A - specyfikacja istniejącego systemu monitoringu bezpieczeństwa KWC

Tab. 31. Kamery i pozostałe istotne elementy wybrane do budowy systemu monitoringu wizyjnego w KWC.

Lp.	Urządzenie	Producent	J.m.	Szt.
1	Kamera stacjonarna zewnętrzna IP 5Mpix, 2,8-8 mm, F1.2, IR 50m, elektroniczna stabilizacja obrazu	Axis	szt.	22
2	Kamera stacjonarna zewnętrzna IP 8Mpix, 3,9-10 mm, F1.5, IR 50m, elektroniczna stabilizacja obrazu	Axis	szt.	4
3	Kamera bullet IP 2Mpix, 2,8-8,5 mm, F1.2, IR 40m	Axis	szt.	19
4	Kamera kopułkowa wewnętrzna IP 2Mpix, 3,4-8,9 mm, F1.8, IR 40m	Axis	szt.	5
5	Kamera kopułkowa zewnętrzna IP 2Mpix, 3-9 mm, F1.3, IR 40m, IK10+, elektroniczna stabilizacja obrazu	Axis	szt.	4
6	Kamera obrotowa IP 2Mpix, 30-krotny zoom, IR 200m, elektroniczna stabilizacja obrazu	Axis	szt.	2
7	Kamera obrotowa IP 2Mpix, 30-krotny zoom, IR 400m, elektroniczna stabilizacja obrazu	Axis	szt.	5
8	Serwer 64TB	Axis	szt.	1
9	Stacja robocza 4 monitorowa	Axis	szt.	3
10	Monitor LCD 46"	NEC	szt.	3
11	Monitor LCD 27"	NEC	szt.	3
12	Panel sterowania systemem dozoru wizyjnego	Axis	szt.	1
13	Przełącznik przemysłowy 20x GE TX ports (4x PoE ports), 4x GE SFP combo ports	Hirschmann	szt.	1
14	Switch wyposażony w 4 x COMBO 100/1000Mbps, 8xRJ45 100Mbps PoE, dwa gniazda na moduły rozszerzeń	Hirschmann	szt.	1
15	4 x SFP 100/1000Mbps; 8 x RJ45 100Mbps PoE, zasilanie redundantne 24VDC	Hirschmann	szt.	8
16	Switch niezarządzalny 100/1000Mbps, 5 x RJ45 w tym 4xPoE, 1xSFP, zasilanie napięciem 24/48V DC (12 - 57 V DC)	Hirschmann	szt.	17
17	Wkładka SFP, 1x100Base- FX, LC connector	Hirschmann	szt.	34
18	Wkładka SFP, 1x1000Base- SX, LC connector	Hirschmann	szt.	18
19	Wkładka SFP-TX RJ45 1G	Hirschmann	szt.	3



Rys. 106. Przykładowe rozmieszczenie kamer monitoringu w obrębie wyrobiska.