Prof. dr hab. inż. Artur Babiarz
Politechnika Śląska
Katedra Automatyki i Robotyki
ul. Akademicka 16, 44-100 Gliwice

Gliwice, 12.01.2026 r.

Recenzja

rozprawy doktorskiej mgr. inż. Jana Kapusty pt.

"Elektroniczne Systemy Zabezpieczenia Technicznego jako źródło danych w procesie automatycznej obrony przed cyberatakami oraz wykrywania sprawcy przestępstwa"

Promotor rozprawy: Prof. dr hab. inż. Jerzy Baranowski
Promotor pomocniczy: Dr inż. Waldemar Bauer
Dyscyplina naukowa: automatyka, elektronika, elektrotechnika i technologie kosmiczne

Recenzja została opracowana na prośbę Przewodniczącego Rady Dyscypliny Automatyka, Elektronika, Elektrotechnika i Technologie Kosmiczne Akademii Górniczo-Hutniczej w Krakowie, dr. hab. inż. Ryszarda Sroki, prof. AGH z dnia 7 listopada 2025 r.

1 Ocena formalna rozprawy

Przedłożona do recenzji rozprawa doktorska została zrealizowana w ramach programu *Doktorat Wdrożeniowy* i dotyczy ona problemu Cyber-Fizycznych Systemów Ochrony (*CPPS*). W ramach przedłożonej rozprawy Doktorant wykorzystał metody sztucznej inteligencji do analizy i modelowania wspomnianych systemów. Podjęta przez Doktoranta tematyka badawcza jest wynikiem dogłębnej analizy literatury i dostępnych rozwiązań technicznych.

Rozprawa doktorska zawiera łącznie 155 stron i została podzielona na siedem rozdziałów, spis literatury i jeden dodatek. Rozprawa została napisana w języku polskim.

Rozdział pierwszy zawiera krótkie wprowadzenie do tematyki rozprawy doktorskiej, uzasadnienie prowadzonych przez Doktoranta badań oraz krótki opis poszczególnych rozdziałów.

W podrozdziale 1.6 autor wskazuje założenie rozprawy definiujące trzy obszary, których integracja jest niezbędne do skutecznej oceny *CPPS*. Są to:

1. *degradacja komponentów i infrastruktury ochronnej w czasie,*

2. *wpływ zagrożeń cybernetycznych na elementy fizyczne,*

3. *specyfika operacyjna i kontekstualna chronionego obiektu.*

W tym samym podrozdziale Doktorant wskazuje pięć głównych obszarów badawczych opisanych w rozprawie doktorskiej:

1. *Opracowanie probabilistycznego modelu degradacji CPPS oraz jego parametryzację na podstawie danych eksperckich i symulacyjnych.*

2. *Implementację procesu COG umożliwiającego automatyczną interpretację planów technicznych i symboli zabezpieczeń.*

3. *Zastosowanie algorytmu A^* z kontekstową funkcją kosztu do oceny ścieżek ataku przeciwnika.*

4. *Integrację dużych modeli językowych (LLM) do analizy kontekstu operacyjnego i generowania zrozumiałych raportów ryzyka.*

5. *Walidację modelu na rzeczywistych przypadkach testowych, z porównaniem skuteczności podejścia klasycznego i zintegrowanego.*

Natomiast w podrozdziale 1.7 Doktorant zamieścił główną tezę rozprawy:
Możliwe jest opracowanie zintegrowanego, probabilistycznego modelu oceny skuteczności Cyber- Fizycznych Systemów Ochrony (CPPS), który jednocześnie uwzględniał będzie: degradację komponentów technicznych w czasie, zagrożenia cybernetyczne oraz operacyjny kontekst funkcjonowania systemu.

Rozdział drugi został poświęcony praktycznym aspektom oceny systemów bezpieczeństwa. Doktorant przedstawił krótkie przypomnienie klasycznej metodologii *EASI* jako punktu wyjścia, precyzyjnie zidentyfikował jej kluczowe deficyty w kontekście współczesnych zagrożeń, a następnie zaproponował autorskie rozwiązania: rozszerzenie *EASI* o komponent cyberodporności (CR) oraz model probabilistyczny degradacji systemów.

W rozdziale trzecim Doktorant opisał narzędzia wykorzystane do detekcji elementów budynku i infrastruktury bezpieczeństwa. Rozdział ten zawiera dokładny opis architektury $YOLOv8$, charakteryzację parametrów tej architektury i założone wartości tych parametrów przez autora rozprawy. Istotną częścią tego rozdziału jest interpretacja symboli systemów bezpieczeństwa z wykorzystaniem metody *COG* (Contextual Object Grouping), która jest wskazana jako autorska metoda umożliwiająca uczenie się interpretacji symboli w kontekście użytej legendy.

Rozdział czwarty dotyczy teorii grafów i wybranych algorytmów przeszukiwania grafów w ujęciu systemów bezpieczeństwa. Doktorant przedstawił założenia teoretyczne i uzasadnił wykorzystanie opisanych metod do modelowania systemów bezpieczeństwa.

Rozdział piąty został poświęcony opisowi dużych modeli językowych i ich użyteczności do konsolidacji i analizy danych bezpieczeństwa. Podobnie, jak w rozdziale czwartym, Doktorant uzasadnił użycie takich modeli w rozprawie doktorskiej.

Rozdział szósty, w mojej ocenie, jest najważniejszą częścią recenzowanej rozprawy, ponieważ przedstawia on jej główny wynik w postaci narzędzia *AI-SecPA* (AI – Security Paths Analyzer). Zgodnie z opisem narzędzie *AI-SecPA* zostało skonstruowane w oparciu o założenia zarządzania ryzykiem, gdzie fundamentalnym podejściem było porównanie ryzyka inherentnego (nieodłącznego) z ryzykiem rezydualnym. Opis powyższego narzędzia jest bardzo dokładny i został podzielony na odpowiednie etapy.

Podsumowanie dotyczące przeprowadzonych badań, głównych osiągnięć badawczych, wkład własny Doktoranta w stan wiedzy dotyczący systemów bezpieczeństwa oraz możliwe kierunki dalszych badań autor rozprawy zawarł w rozdziale siódmym.

Oceniając rozprawę doktorską pod względem edytorskim pierwszą istotną rzeczą, która jest dyskusyjna to stosowanie w narracji pierwszej osoby liczby mnogiej. Stosowanie tej reguły występuje tylko w przypadku wskazywania konkretnych osiągnięć badawczych zawartych w rozprawie. Jest to oczywiście dopuszczalne, ale w konkretnych sytuacjach może wskazywać na sytuację, w której przedstawione osiągnięcie nie jest indywidualnym wkładem Doktoranta. Bardzo dobrze jest to widoczne na stronie 43, pierwszy akapit: "W wyniku naszej pracy zaproponowaliśmy modyfikację podejścia...". Kolejną rzeczą jest forma odwołania do jedynego numerowanego (z założenia) równania (2.2). Niestety odwołanie w tekście do tego równania jest nieaktywne, ponieważ nie ma równania o takim numerze. Taka sytuacja występuje na stronie 41. W rozprawie pojawia się kilka tabel, ale niestety w licznych przypadkach brak odwołania do konkretnej tabeli, a prawie we wszystkich brak jakiegokolwiek komentarza do danych zawartych w tabelach. Kolejnym dość istotnym niedociągnięciem jest pozycja literatury o numerze "[105] A. Author, "Computational title," Journal Name, vol. 1, pp. 1–10, 2008."Tym bardziej, że w treści rozprawy pojawia się do tej pozycji odwołanie. W tekście pojawia się kilka błędów interpunkcyjnych, ale ogólnie trudno doszukać się większych uchybień edytorskich niż wspomniane powyżej.

Podsumowując, rozprawa doktorska jest napisana poprawnie (pomijając powyższe uwagi). Spis literatury jest poprawny i zawiera raczej aktualną literaturę. Podział rozprawy na rozdziały nie budzi żadnych wątpliwości.

2 Ocena merytoryczna rozprawy

Głównym celem Doktoranta, który został przedstawiony w rozprawie doktorskiej była analiza i modelowanie Cyber-Fizycznych Systemów Ochrony *(CPPS)* z wykorzystaniem metod sztucznej inteligencji. Podjęcie takiego zagadnienia w ramach tematy rozprawy Doktorant uzasadnia istniejącymi brakami w dotychczasowych podejściach metodologicznych, a w szczególności:

- braku reprezentacji cyberzagrożeń w tradycyjnych modelach oceny skuteczności,
- ograniczeń w modelowaniu współczesnych scenariuszy hybrydowych,
- nieadekwatności klasycznych miar prawdopodobieństwa dla zagrożeń cyber-fizycznych,
- potrzeby nowych metodologii integrujących domenę fizyczną i cybernetyczną.

Jako główne źródło danych do analizy systemów bezpieczeństwa autor rozprawy wskazuje Elektroniczne Systemy Zabezpieczenia Technicznego *(ESZT)*.

Podstawą analizy i modelowania systemów zabezpieczeń jest metodologia *EASI* (Estimated Adversary Sequence Interruption) zaproponowana i wprowadzona przez Bennetta w 1977 roku. Doktorant, w wyniku analizy dostępnych rozwiązań, zaproponował kilka modyfikacji modelu *EASI*.

Pierwszą modyfikacją, która ma niwelować lukę związaną z brakiem uwzględnienia cyberzagrożeń, jest wprowadzenie współczynnika cyberodporności *(CR)* dla każdego cyfrowego komponentu systemu. Zaproponowana modyfikacja polega na skorygowaniu prawdopodobieństwa detekcji ataku.

Kolejnym krokiem analizy przeprowadzonej przez Doktoranta było uwzględnienie Fizycznych Systemów Ochrony *(PPS)*. W wyniku analizy tych systemów autor rozprawy zaproponował modyfikację narzędzia *EASI* opartego na Excelu, w której całkowite prawdopodobieństwo detekcji kroku przeciwnika jest obliczane jako iloczyn prawdopodobieństwa detekcji i skuteczności cyberbezpieczeństwa elementów fizycznych systemów ochrony.

W wyniku dalszej analizy systemów bezpieczeństwa autor rozprawy wprowadził kolejne rozszerzenie *EASI* polegające na uwzględnieniu modelu degradacji w modelu *EASI* poprzez modyfikację prawdopodobieństw detekcji każdego elementu na ścieżce ataku.

Zaproponowane powyżej rozszerzenia *EASI* stanowiły podstawę do przeprowadzenia przez Doktoranta eksperymentów symulacyjnych, w wyniku których pojawiła się kolejna koncepcja modyfikacji. Polegała ona na integracji wskaźnika efektywności (wynikającego z wieku i degradacji każdej warstwy systemu ochrony) z klasycznym modelem *EASI*.

Finalnie, autor rozprawy zaproponował model zintegrowany uwzględniający wpływ cyberzagrożeń i degradacji.

Zgodnie z postawionymi przez Doktoranta celami, następnym krokiem był dobór systemów detekcji elementów graficznych znajdujących się na schematach pomieszczeń objętych systemami ochrony oraz algorytmów umożliwiających wyznaczanie potencjalnej ścieżki ataku w reprezentacji grafowej. W tym celu autor rozprawy opisał architekturę $YOLOv8$ oraz jej parametry, a następnie przedstawił podstawy teoretyczne rożnych algorytmów przeszukiwania grafów, ze wskazaniem algorytmu A^*, jako wybranego do autorskiego narzędzia oceny efektywności Cyber-Fizycznych Systemów Ochrony.

W efekcie powyżej opisanych modyfikacji modelu *EASI* oraz wyboru odpowiednich metod i algorytmów, Doktorant zaimplementował narzędzie *AI-SecPA*.

Podsumowując ocenę merytoryczną stwierdzam, że przedstawione wyniki analizy systemów bezpieczeństwa wskazują na szeroką wiedzę Doktoranta w zakresie cyber-fizycznych systemów ochrony, jak również znajomości metod sztucznej inteligencji i ich wykorzystania do modelowania systemów ochrony. Doktorant jednoznacznie wykazał realizację postawionych celów badawczych i udowodnił postawioną tezę.

3 Ocena dorobku publikacyjnego Doktoranta

W bazie Web of Science (WoS) indeksowane są 3 prace Doktoranta (dostęp 7.01.2026). Według bazy WoS indeks Hirscha wynosi **1**, a liczba cytowań **2** (bez auto cytowań **1**).

W bazie Scopus również indeksowane są 3 prace. Indeks Hirscha wynosi **1** przy całkowitej liczbie cytowań równej **2**.

Są to dane na bardzo niskim poziomie i można wysunąć wniosek, że osoba Doktoranta raczej nie jest rozpoznawalna w środowisku krajowym, jak i międzynarodowym.

4 Uwagi krytyczne i dyskusyjne

Ogólna struktura pracy jest jasna i czytelna, tak jak opisano w poprzednich punktach recenzji. Problem pojawia się w przypadku, gdy czytelnik chciałby dotrzeć do szczegółowych danych źródłowych oraz wartości parametrów użytych w eksperymentach symulacyjnych oraz w przedstawionym narzędziu *AI-SecPA*. Poniżej przedstawiono uwagi krytyczne:

1. Na stronach $40-48$ przedstawiono propozycję rozszerzenia modelu *EASI*. Pierwsze propozycje zostały przedstawione w postaci zaktualizowanego wzoru opisującego model *EASI* (patrz strona 41). W podrozdziale 2.4 zaproponowano uwzględnienie

Ale

wpływu cyberzagrożeń i degradacji, jednak autor nie przedstawił w jaki sposób to rozszerzenie wpływa na standardowy model *EASI*. Jak wygląda wówczas równanie modelu?

2. Kolejna uwaga dotycząca rozszerzenia modelu *EASI* nawiązuje do informacji zawartych na stronie 136: *Szczególną wartością przedstawionej pracy jest integracja różnych metodologii w spójne podejście analityczne. Model degradacji oparty na symulacjach Monte Carlo łączy się z klasyczną metodologią EASI, tworząc rozszerzoną wersję EASI-Δ, która uwzględnia czasową zmienność parametrów systemu.*

   Gdzie jest przedstawiona wersja EASI-Δ? Jaka jest postać modelu EASI-Δ

3. W podrozdziale 3.3 Doktorant charakteryzuje zbiór danych, który został wybrany/stworzony, jako obrazy treningowe i walidacyjne. Źródłem tych danych mają być publiczne repozytoria i dokumentacja. W mojej opinii jest to bardzo ogólne stwierdzenie. Brak konkretnych informacji o strukturze tych obrazów. Ponadto, na stronie 137 Doktorant pisze:

   Metodologia COG, mimo osiągnięcia wysokich wskaźników skuteczności detekcji, wykazuje pewne ograniczenia techniczne. Model został trenowany na zbiorze danych ograniczonym do siedmiu podstawowych klas architektonicznych,...

   W tekście rozprawy nigdzie wcześniej nie zdefiniowano tych siedmiu klas architektonicznych. Jak ta informacja wiąże się z danymi z podrozdziału 3.3?

4. Doktorant wskazuje, że metodologia *COG* jest znaczącym wkładem w zaproponowaną metodę analizy systemów bezpieczeństwa. Zgodnie z informacją zawartą w spisie literatury metodologia *COG* została opisana w artykule, który został wysłany do wybranego czasopisma. Na tym etapie trudno ocenić jej znaczenie merytoryczne i naukowe, tym bardziej, że w rozprawie *COG* jest opisany w minimalistyczny sposób, z ograniczeniem do celu jej stosowania.

5. Na stronie 89 autor rozprawy pisze:

   Zaimplementowano detekcję elementów architektonicznych opartą o ML (YOLO) oraz algorytmiczną eksplorację ścieżek ataku (własna funkcja heurystyki dla A).*

   oraz

   Opracowane podejście wnosi następujące elementy do teorii analizy bezpieczeństwa:

   ...

2. Rozwój specjalizowanych funkcji heurystycznych dostosowanych do specyfiki scenariuszy bezpieczeństwa, wykraczające poza klasyczne metryki geometryczne i uwzględniających czynniki takie jak prawdopodobieństwo wykrycia, czas reakcji oraz dostępność zasobów, czy przygotowanie adwersarza.

Niestety w całej rozprawie brak dokładnej formuły dla opracowanej funkcji heurystycznej. Ponadto, w powyższym fragmencie Doktorant pisze o wielu funkcjach heurystycznych. Jedyna wzmianka pojawia się na stronie 42 mówiąca o tym, że funkcja heurystyczna jest zależna od prawdopodobieństwa detekcji P_d, skuteczności cyberbezpieczeństwa elementów PPS P_{ce}, czasu opóźnienia T_{dl} oraz pozostałego czasu reakcji do określonego punktu na grafie T_{rr}, oraz na stronach 135 i 137 w konkluzjach rozprawy.

Wymienione powyżej uwagi krytyczne mają istotny wpływ na merytoryczną ocenę zaproponowanych modyfikacji i rozszerzeń znanych z literatury metod oraz modeli wykorzystywanych do analizy systemów bezpieczeństwa.

Natomiast poniższe uwagi mają charakter dyskusyjny i nie mają wpływu na końcową ocenę rozprawy doktorskiej.

- W rozprawie doktorskiej autor definiuje specyfikację sprzętową i programową (strona 53). Jakie są minimalne wymagania sprzętowe i jak te wymagania wpływają na działanie narzędzia *AI-SecPA*? Czy Doktorant przeprowadzał testy działania narzędzia *AI-SecPA* w zależności od konfiguracji sprzętowej wobec założenia o uniwersalności tego narzędzia?

- Na stronie 62 autor formułuje wniosek, że należy rozwijać algorytmy przetwarzania obrazów architektonicznych w celu niezmienności względem transformacji geometrycznej. Jednak w założeniach przyjęto tylko 10 stopniową rotację obiektów. Ponadto, na schematach zamieszczonych w rozprawie widać dużo większą rotację symboli architektonicznych w stosunku do orientacji uwzględnionej w legendzie. Jaki ma to wpływ na uzyskane wyniki i jakie było końcowe założenie w przedstawionym narzędziu *AI-SecPA*?

- Na stronach 124 i 125 autor rozprawy doktorskiej analizuje dwie ścieżki **Path 1: Cost** 271.42 oraz **Path 110: Cost** 946.09. Nie jest jasne w jakich jednostkach koszt ścieżki został wyrażony i w jaki sposób został wyliczony. Dodatkowo, ścieżka 1 składa się tylko z jednego segmentu linii prostej. Jak należy interpretować taką

ścieżkę, która (zgodnie z rysunkiem 6.8) reprezentuje pojawienie się przeciwnika w ciągu komunikacyjnym bez dalszego przemieszczania się?

Podsumowując, w rozprawie doktorskiej autor nie zamieścił szczegółowych informacji stanowiących fundamenty zaimplementowanego narzędzia oraz zaproponowanych modyfikacji modeli i metod niezbędnych do analizy systemów bezpieczeństwa. Brak takich informacji znacząco utrudnia analizę zaprezentowanych przez Doktoranta wyników.

5 Wniosek końcowy

Mimo wielu uwag krytycznych, minimalnego dorobku naukowego oraz braków dotyczących szczegółów zaproponowanych rozszerzeń metody *EASI*, moja ocena rozprawy doktorskiej jest następująca:

- Praca zawiera oryginalne wyniki oraz przedstawia rozwiązanie wszystkich postawionych celów i problemów badawczych oraz potwierdza tezę rozprawy doktorskiej.
- Doktorant posiada ogólną wiedzę teoretyczną z zakresu modelowania systemów bezpieczeństwa, co potwierdził analizą stanu wiedzy zamieszczoną w rozdziałach $2-5$.
- Doktorant zdobył i posiada umiejętności samodzielnego prowadzenia pracy badawczej, co udowodnił licznymi eksperymentami symulacyjnymi i analizą otrzymanych wyników.
- Przedstawione w rozprawie doktorskiej wyniki badań wpisującą się w dyscyplinę automatyka, elektronika, elektrotechnika i technologie kosmiczne.

Uwzględniając powyższą ocenę, stwierdzam, że rozprawa doktorska mgr. inż. Jana Kapusty spełnia w stopniu dostatecznym warunki określone w Ustawie z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. 2023, poz. 742) i wnoszę o jej przyjęcie oraz dopuszczenie do publicznej obrony.

Artur Babiarz