

dr hab. inż. Rafał Stanisławski, prof. uczelni  
Katedra Systemów Informatycznych i Sterowania  
Wydział Informatyki  
Politechnika Opolska  
e-mail: r.stanislawski@po.edu.pl

Opole, 19.01.2026

SEKRETARIAT  
Rady Dyscypliny AEEITK

Wpłynęło dnia 2.02.2026

Zarejestrowano pod nr 510.6-7/25

Podpis 

## RECENZJA ROZPRAWY DOKTORSKIEJ

**Tytuł rozprawy:**

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

**Autor rozprawy: mgr inż. Jan Kapusta**

**Promotor rozprawy: prof. dr hab. inż. Jerzy Baranowski**

**Promotor pomocniczy: dr inż. Waldemar Bauer**

Niniejsza recenzja została opracowana na zlecenie Przewodniczącego Rady Naukowej Automatyka, Elektronika i Elektrotechnika Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie dra hab. inż. Ryszarda Sroki, prof. AGH, z dnia 7 listopada 2025 roku.

### 1. Zawartość pracy i ocena formalna

Przedłożona do oceny rozprawa doktorska zawiera łącznie 155 stron podzielonych na siedem rozdziałów, literatury liczącej 165 pozycji oraz streszczeń w języku polskim i angielskim. Dysertacja została napisana w języku polskim. Zawartość rozprawy zaprezentowano poniżej.

W Rozdziale pierwszym przedstawiono wprowadzenie do zagadnień poruszanych w pracy. Scharakteryzowano kontekst podejmowanego problemu badawczego oraz omówiono luki badawcze w obszarze systemów zabezpieczenia technicznego, które stanowiły genezę niniejszej dysertacji. Na tej podstawie określono cel i zakres pracy oraz sformułowano jej tezę. Ponadto w Rozdziale pierwszym zaprezentowano strukturę rozprawy.

Rozdział drugi poświęcony jest prezentacji zasad oceny systemów bezpieczeństwa fizycznego. Zarówno w tym rozdziale, jak i w całej pracy Doktorant opiera się na metodologii *Estimated Adversary Sequence Interruption* (EASI), co należy uznać za podejście właściwe. W rozdziale szczególnie omówiono ograniczenia klasycznych metod oceny, których analiza umożliwiła zdefiniowanie rozszerzenia metody EASI o zaproponowany przez Doktoranta współczynnik uwzględniający aspekty cyberbezpieczeństwa systemu. Ponadto zaproponowano model degradacji systemów elektronicznych oparty na podstawowych narzędziach probabilistycznych oraz dokonano jego implementacji w bazowym modelu EASI. Przeprowadzono również badania symulacyjne metodologii uwzględniającej wprowadzone rozszerzenia. Zaprezentowane w rozdziale wyniki częściowo opierają się na pracach współautorstwa Kandydata, zawierają jednak także elementy dotychczas niepublikowane.

Zagadnienie detekcji elementów budynku i infrastruktury bezpieczeństwa na planach architektonicznych 2D w kontekście automatycznej oceny bezpieczeństwa obiektów został przedstawiony



w Rozdziale trzecim. Na wstępie przedstawiono motywację problemu, wskazując na wykładniczy wzrost liczby potencjalnych ścieżek ataku oraz ograniczenia ręcznej analizy. Następnie zaprezentowano ewolucję metod detekcji obiektów, od klasycznych podejść opartych na deskryptorach cech do współczesnych metod głębokiego uczenia. Kluczową część rozdziału stanowi opis architektury i konfiguracji systemu detekcji opartego na modelu YOLOv8, wraz z charakterystyką zbioru danych, strategią augmentacji oraz uzasadnieniem doboru hiperparametrów. Omówiono również etapy post-processingu wyników detekcji, w tym eliminację duplikatów z wykorzystaniem miary IoSA oraz walidację geometryczną. Rozdział zamyka podsumowanie wyników eksperymentalnych, wskazujące na skuteczność zaproponowanego podejścia oraz jego znaczenie jako warstwy wejściowej do dalszych etapów analizy bezpieczeństwa przedstawionych w kolejnych rozdziałach.

Rozdział czwarty poświęcony jest zagadnieniom konstrukcji grafów obiektów oraz heurystycznej analizie ścieżek ataku z wykorzystaniem algorytmu A\*. Znaczną część rozdziału stanowi obszerny przegląd klasycznych zagadnień teorii grafów oraz algorytmów przeszukiwania, w tym *Breadth-First Search* (BFS), *Depth-First Search* (DFS), algorytmu *Dijkstry* oraz podstaw i wariantów algorytmu A\*. Treści te mają w dużej mierze charakter ogólny i odtwórczy, a ich związek z właściwym problemem badawczym bywa pośredni. Elementy stanowiące wkład autorski pojawiają się w dalszej części rozdziału i dotyczą sposobu konstrukcji grafów bezpieczeństwa na podstawie wyników detekcji, zaproponowanych funkcji heurystycznych uwzględniających specyfikę analizy ścieżek ataku oraz integracja z metodologią EASI.

Rozdział piąty poświęcony jest zastosowaniu dużych modeli językowych (LLM) jako narzędzia wspomagającego konsolidację, interpretację oraz raportowanie wyników analizy bezpieczeństwa. Przedstawiono w nim podstawy teoretyczne działania LLM, w tym architekturę transformera, mechanizm uwagi oraz proces tokenizacji, a następnie omówiono rolę tych modeli w przejściu od fragmentarycznych danych technicznych (wyników detekcji, analiz grafowych i heurystycznych ocen ścieżek ataku) do spójnych wniosków o charakterze strategicznym. Rozdział akcentuje znaczenie strukturyzacji kontekstu, inżynierii promptów oraz kontrolowanej generacji jako warunków uzyskania powtarzalnych i interpretowalnych rezultatów, a także wskazuje na możliwość integracji LLM z procesem decyzyjnym poprzez generowanie rekomendacji, priorytetyzację zagrożeń oraz wsparcie analityka w środowiskach cyber-fizycznych. Rozdział ma w przeważającej części charakter odtwórczy i zdaniem recenzenta w sposób nadmiarowy prezentuje informacje teoretyczne dotyczące omawianego obszaru.

Zwieńczenie rozprawy w postaci Rozdziału szóstego, poświęcono implementacji zaproponowanej w poprzednich rozdziałach metodologii w postaci narzędzia AI-SecPA (AI-Security Paths Analyzer). Autor przedstawia w nim praktyczne przełożenie wcześniejszych rozważań teoretycznych na funkcjonalny system wspomagający ocenę efektywności cyber-fizycznych systemów ochrony, obejmujący cały proces analizy – od przygotowania danych i kontekstu, przez automatyczną detekcję oraz analizę grafową, aż po syntezę wyników i generowanie raportów z wykorzystaniem dużych modeli językowych. Rozdział akcentuje rolę eksperta w procesie decyzyjnym, wskazując, że zaproponowane narzędzie pełni funkcję wspomagającą, a nie zastępującą analizę ekspercką, oraz podkreśla znaczenie transparentności, interaktywności i możliwości walidacji wyników. Zaprezentowana implementacja potwierdza wykonalność zaproponowanej koncepcji i pokazuje, w jaki sposób opracowane modele i algorytmy mogą zostać wykorzystane w realistycznych scenariuszach oceny bezpieczeństwa, stanowiąc spójne i logiczne domknięcie całej pracy.



W Rozdziale siódmym zostało zawarte podsumowanie i wnioski z przeprowadzonych badań, wraz z odniesieniem do postawionej tezy dysertacji. W Rozdziale przedstawiono również krytyczną ocenę ograniczeń narzędzi zastosowanych w dysertacji, a także kierunki potencjalnych przyszłych prac Doktoranta.

Układ rozprawy jest poprawny i przejrzysty. Treść dysertacji została logicznie podzielona na kolejne rozdziały, a zakres oraz struktura poszczególnych rozdziałów, podrozdziałów i sekcji nie budzą zastrzeżeń recenzenta.

Jednocześnie należy zauważyć, że sposób prezentacji wyników w znacznych fragmentach pracy jest mało czytelny. W rozprawie występują obszerne fragmenty tekstu, w których w formie pojedynczych zdań wyliczane są wnioski, cechy lub obserwacje, co utrudnia odbiór i zrozumienie przedstawianej treści. Ponadto praca zawiera fragmenty poświęcone podstawom teoretycznym, które często pozostają jedynie luźno powiązane z zasadniczym problemem badawczym ocenianej dysertacji.

Dodatkowe uwagi budzi również sposób prezentacji równań. Doktorant w wielu miejscach nie podaje wymiarów macierzy, nie definiuje jednoznacznie użytych symboli, ani nie precyzuje stosowanych operatorów, co negatywnie wpływa na jednoznaczność i czytelność zapisu matematycznego.

Strona edycyjna pracy jest dobra i świadczy o starannej redakcji dysertacji. Rysunki zostały przygotowane z dużą dbałością o precyzję oraz estetykę, a także o czytelne przedstawienie zastosowanych algorytmów i uzyskanych wyników badań. Pewne wątpliwości natury formalnej budzi natomiast sposób wykorzystania i cytowania rysunków pochodzących z prac współautorstwa Doktoranta, co zostanie omówione w dalszej części recenzji.

Choć w powyższym opisie wskazano pewne uchybienia dotyczące strony formalnej pracy, należy podkreślić, że pomimo nich recenzent pozytywnie ocenia stronę formalną rozprawy.

## 2. Ocena merytoryczna pracy

Rozwój elektronicznych systemów zabezpieczeń stanowi istotny nurt badań na styku dyscyplin *automatyka, elektronika, elektrotechnika i technologie kosmiczne, informatyka techniczna i telekomunikacja* w dziedzinie nauk inżynieryjno-technicznych oraz *nauk o bezpieczeństwie* w naukach społecznych. Jednak w ujęciu rozpatrywanych w dysertacji rozwiązań elektronicznych zabezpieczeń mienia, bardziej adekwatne do tej problematyki są ww. dyscypliny nauk inżynieryjno-technicznych. Początki tego obszaru sięgają prostych, autonomicznych układów alarmowych opartych na czujnikach analogowych i mechanicznych, projektowanych głównie do sygnalizowania naruszeń chronionej strefy. Postęp elektroniki cyfrowej, miniaturyzacja układów scalonych oraz upowszechnienie systemów mikroprocesorowych doprowadziły do stopniowej ewolucji tych rozwiązań w kierunku złożonych, wielowarstwowych systemów cyber-fizycznych, integrujących komponenty sprzętowe, oprogramowanie oraz infrastrukturę telekomunikacyjną. Współczesne elektroniczne systemy zabezpieczeń obejmują szerokie spektrum technologii, od klasycznych systemów ochrony fizycznej, takich jak kontrola dostępu, systemy sygnalizacji włamania i monitoring wizyjny, po rozwiązania wykorzystujące Internet Rzeczy, analizę dużych zbiorów danych oraz algorytmy sztucznej inteligencji, co umożliwia przejście od reaktywnego do proaktywnego modelu zarządzania bezpieczeństwem. Z perspektywy naukowej obszar ten oferuje rozległe możliwości badawcze, obejmujące zagadnienia fuzji danych z heterogenicznych źródeł, modelowania procesów decyzyjnych w warunkach niepewności, analizy odporności

systemów na zakłócenia i ataki oraz formalnej oceny skuteczności środków ochrony. Szczególne znaczenie ma integracja warstwy technicznej z kontekstem operacyjnym i strategicznym, wymagająca łączenia metod inżynierskich, matematycznych i informatycznych, co czyni elektroniczne systemy zabezpieczeń obszarem o wysokim potencjale innowacyjnym, pozwalającym na uzyskiwanie wyników o istotnym znaczeniu zarówno poznawczym, jak i aplikacyjnym.

W związku z powyższym autor podejmuje badania w ważnym i aktualnym obszarze, który posiada podstawy w światowej literaturze naukowej, a jednocześnie stwarza możliwości uzyskania nowych, istotnych wyników, w szczególności o charakterze aplikacyjnym. Recenzent lokuje przedmiotową dysertację w obszarze dwóch dyscyplin naukowych, tj. *automatyka, elektronika i elektrotechnika oraz technologie kosmiczne* oraz *informatyka techniczna i telekomunikacja* należących do dziedziny nauk inżynierijno-technicznych, jednak ze względu na zastosowane narzędzia naukowe większy ciężar badawczy spoczywa na pierwszej z ww. dyscyplin.

Doktorant postawił sobie istotny cel badawczy, polegający na opracowaniu zintegrowanego, opartego na danych modelu oceny skuteczności cyber-fizycznych systemów bezpieczeństwa. Proponowany model uwzględnia dynamikę degradacji komponentów technicznych, rosnącą rolę zagrożeń cybernetycznych oraz wpływ kontekstu operacyjnego, w którym funkcjonuje dany system. Finalne w wyniku pracy powstało narzędzie, nazwane przed Autorem AI-SecPA (*AI – Security Path Analyzer*), które doskonale wpisuje się w aplikacyjny charakter pracy realizowanej w ramach programu *Doktorat Wdrożeniowy*.

Sformułowana została następująca teza rozprawy:

**Możliwe jest opracowanie zintegrowanego, probabilistycznego modelu oceny skuteczności Cyber-Fizycznych Systemów Ochrony (CPPS), który jednocześnie uwzględnił będzie: degradację komponentów technicznych w czasie, zagrożenia cybernetyczne oraz operacyjny kontekst funkcjonowania systemu.**

Ponadto w pracy zostały postawione następujący cel pracy:

**Opracowanie zintegrowanego, opartego na danych modelu oceny skuteczności cyber-fizycznych systemów bezpieczeństwa. Proponowany model uwzględni dynamikę degradacji komponentów technicznych, rosnącą rolę zagrożeń cybernetycznych oraz wpływ kontekstu operacyjnego, w którym funkcjonuje dany system.**

Zwartość rozprawy, omówiona w poprzednim punkcie recenzji, wynika ze sformułowanych pytań badawczych i prowadzi do weryfikacji postawionej tezy. Osiągnięcia kandydata koncentrują się na pewnych zagadnieniach teoretycznych związanych z implementacją dodatkowych aspektów w metodologii EASI, tj. aspekty cyber-bezpieczeństwa i degradacji elementów systemu. Jednak w szczególności praca koncentruje się na aspektach praktycznych zwięzonym opracowaniem systemu AI-SecPA. Ostatecznie do podstawowych osiągnięć rozprawy można zaliczyć:

- Opracowanie probabilistycznego modelu degradacji, uwzględniającego zarówno procesy degradacji komponentów fizycznych, jak i zagrożenia cybernetyczne, jego parametryzację na podstawie danych oraz integrację z modelem EASI.
- Implementację procesu umożliwiającego automatyczną interpretację planów technicznych i symboli zabezpieczeń, opartego na metodach komputerowej analizy obrazu oraz interpretacji wykrytych elementów infrastruktury w kontekście analizy bezpieczeństwa.

- Zastosowanie algorytmu  $A^*$  z kontekstową funkcją kosztu do oceny ścieżek ataku przeciwnika, uwzględniającą parametry detekcji, degradację komponentów oraz uwarunkowania operacyjne chronionego obiektu.
- Integrację dużych modeli językowych (LLM) do analizy kontekstu operacyjnego i generowania zrozumiałych raportów ryzyka.
- Walidację modelu na rzeczywistych przypadkach testowych oraz analizę porównawczą skuteczności podejścia klasycznego i zaproponowanego przez Doktoranta.

Recenzent zgłosił uwagi odnoszące się również do strony merytorycznej rozprawy, które zostały przedstawione w dalszej części recenzji. Należy jednak stwierdzić, że wszystkie wyżej wymienione osiągnięcia, rozpatrywane łącznie, stanowią znaczący wkład Kandydata w rozwój dyscypliny naukowej *automatyka, elektronika, elektrotechnika i technologie kosmiczne*. Przedstawione wyniki badań prowadzą do weryfikacji postawionej tezy rozprawy oraz umożliwiają osiągnięcie założonego celu pracy.

Rozprawa ma wyraźnie charakter praktyczny, co pozostaje spójne z realizacją pracy w ramach programu *Doktorat Wdrożeniowy*. Głównego wkładu Kandydata należy upatrywać w rozdziałach drugim, trzecim, czwartym i piątym, których rezultaty zostały zintegrowane w opracowanym systemie zaprezentowanym w rozdziale szóstym.

### 3. Analiza źródeł, pozycja rozprawy i znaczenie wyników Autora

Motywacja dla podjęcia tematu rozprawy wniknęła z dobrze przeprowadzonej przez Autora analizy literatury przedmiotu, liczącej 165 pozycji. Dzięki szerokiej analizie literaturowej został poprawnie odzwierciedlony aktualny stan wiedzy na temat wszystkich zagadnień podejmowanych w pracy.

Pozycja rozprawy w stosunku do stanu wiedzy reprezentowanej w literaturze światowej jest zadowalająca. Doktorant jest współautorem jednego artykułu w czasopiśmie indeksowanym na liście JCR, tj. *Algorithms* i trzech referatów na konferencjach międzynarodowych *IEEE International Conference on Methods & Models in Automation Robotics* oraz *50th Conference of the Industrial Electronics Society*. Należy również zauważyć, że wg bazy *Web of Science* publikacje Doktoranta zostały zacytowane 3 razy. Jest to wartość poniżej średniej jednak z drugiej strony pokazuje, że prace zostały zauważone przez środowisko naukowe.

### 4. Wady rozprawy, słabe strony, uwagi i pytania

Recenzentowi nasunęły się uwagi i wątpliwości dotyczące zarówno strony merytorycznej, jak i formalnej dysertacji. Zostały one przedstawione w punktach:

- 1) W pracy Doktorant opiera się na metodzie *Estimated Adversary Sequence Interruption* (EASI). Metoda została przedstawiona i omówiona w sposób poprawny, jednak recenzent nie dostrzegł pogłębionego przeglądu literatury obejmującego alternatywne podejścia, które są dość licznie reprezentowane w literaturze przedmiotu.

R. Shm

- 2) Konwencja przedstawiania części równań budzi wątpliwości. Po pierwsze, w pracach technicznych operator  $'\cdot'$  jest zwykle interpretowany jako iloczyn skalarny (np. wektorów), co może prowadzić do niejednoznaczności zapisu. Ponadto sposób stosowania nawiasów jest dyskusyjny i nie zawsze zapewnia czytelność (por. str. 18, 32).
- 3) Pewne wątpliwości budzi zamienne stosowanie zapisu prawdopodobieństw w wartościach bezwzględnych oraz procentowych. Ujednolicenie tej konwencji zapisu zwiększyłoby czytelność ocenianej pracy.
- 4) Przy lekturze strony 57 można odnieść wrażenie, że sekcje: *Studia porównawcze*, *Wpływ strategii treningu* i *Wpływ post-processingu* nie zostały opatrzone opisami.
- 5) W opisie konfiguracji eksperymentalnej brakuje jednoznacznej informacji, czy zastosowany model YOLOv8m był trenowany od losowej inicjalizacji wag, czy też wykorzystano wagi wstępnie wytrenowane (pretrained). Jest to istotna informacja z punktu widzenia interpretacji uzyskanych wyników, zwłaszcza przy relatywnie niewielkiej liczności zbioru danych.
- 6) Choć w pracy przedstawiono rozbudowaną strategię augmentacji danych, przy relatywnie niewielkiej liczności zbioru treningowego zasadne byłoby uzupełnienie tej części o rozważania dotyczące generowania danych syntetycznych (np. proceduralnych), które w analizowanej domenie planów architektonicznych mogłyby stanowić naturalne rozszerzenie augmentacji i istotnie zwiększyć różnorodność danych uczących.
- 7) Rozdział czwarty jest nadmiernie rozbudowany w części teoretycznej, która w znacznej mierze ma charakter odtwórczy i podręcznikowy. Obszerne omówienia klasycznych algorytmów grafowych zajmują istotną część rozdziału, co prowadzi do rozmycia elementów stanowiących rzeczywisty wkład autorski Kandydata. Skrócenie tej części i wyraźniejsze wyeksponowanie nowych rozwiązań znacząco zwiększyłoby czytelność oraz wartość poznawczą rozdziału. Ponadto części dotyczące argumentacji wyboru określonych narzędzi w ocenie recenzenta mogłyby być dogłębsze.
- 8) Równanie przedstawione na stronie 92 mogłoby zostać sformułowane w sposób bardziej jednoznaczny i konsekwentny. Po pierwsze, nazwa funkcji attention powinna być zapisywana konsekwentnie małą literą. Po drugie, w zapisie nie podano wymiarów macierzy  $Q$ ,  $K$  i  $V$  co utrudnia jednoznaczną interpretację formalną równania. Warto również zauważyć, że w równaniu występuje iloczyn skalarny, natomiast Doktorant zapisał go w postaci iloczynu macierzy bez użycia operatora  $'\cdot'$ . Rozwiązanie to jest poprawne i czytelne, jednak pozostaje niespójne z innymi fragmentami pracy.
- 9) W rozprawie występują obszerne fragmenty tekstu, w których w formie pojedynczych zdań wliczane są wnioski, cechy lub obserwacje, co utrudnia odbiór oraz zrozumienie prezentowanej treści. Zdaniem recenzenta zasadne byłoby przeniesienie tego rodzaju zestawień do załączników, natomiast w głównym tekście pracy ograniczenie ich do syntetycznego podsumowania uzupełnionego o odpowiedni komentarz opisowy.
- 10) Niektóre rysunki zostały przeniesione bezpośrednio z publikacji współautorstwa Doktoranta. Pewne wątpliwości natury formalnej budzą opisy zamieszczone pod tymi rysunkami. W przy-



padku wykorzystania rysunków autorstwa Doktoranta opublikowanych wcześniej, należy jednoznacznie wskazać odpowiednie źródło w postaci odnośnika do danej publikacji. Zastosowane sformułowanie „opracowanie własne na podstawie ...” jest w tym kontekście mylące. Można domniemywać, że intencją Kandydata było podkreślenie własnego autorstwa rysunków, jednak z formalnego punktu widzenia sposób ich cytowania stanowi uchybienie. Dotyczy to w szczególności rysunków: 3.1, 3.2, 3.3 oraz 3.4.

- 11) Autor w dysertacji konsekwentnie stosuje formę pierwszej osoby liczby mnogiej. Należy jednak zauważyć, że forma ta nie jest właściwa w samodzielnych pracach naukowych, do których, zgodnie z obowiązującymi przepisami, zalicza się rozprawa doktorska.
- 12) W kilku miejscach pracy w zapisie równań nie podano wymiarów macierzy, nie zdefiniowano jednoznacznie użytych symboli ani stosowanych operatorów, co negatywnie wpływa na jednoznaczność oraz czytelność zapisu matematycznego.
- 13) Pozycja [27] w wykazie literatury została podana z błędem. W pracy wskazano czasopismo *Sensors*, podczas gdy w rzeczywistości cytowana publikacja została opublikowana w czasopiśmie *Algorithms*.

Należy podkreślić, że przedstawione powyżej uwagi i wątpliwości nie wpływają na pozytywną ocenę pracy.

## 5. Podsumowanie recenzji i wniosek końcowy

Recenzowana rozprawa doktorska stanowi, zdaniem recenzenta, oryginalne rozwiązanie ważnego problemu naukowego oraz wykazuje ogólną wiedzę teoretyczną i aplikacyjną Kandydata w dyscyplinie naukowej *automatyka, elektronika, elektrotechnika i technologie kosmiczne*, a także Jego umiejętność samodzielnego prowadzenia pracy naukowej. Zatem stwierdzam, że **rozprawa mgr inż. Jana Kapusty spełnia** w wystarczającym stopniu warunki określone w ustawie z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz.U. z 2024 r. poz. 1571 z późn. zm.) w dziedzinie nauk inżynieryjno-technicznych, w dyscyplinie *automatyka, elektronika, elektrotechnika i technologie kosmiczne*.

W związku z powyższym **wnoszę o dopuszczenie rozprawy doktorskiej mgr inż. Jana Kapusty do publicznej obrony.**

*Rafał Staniszewski*