prof. Jerzy Józefczyk
Katedra Informatyki i Inżynierii Systemów
Wydział Informatyki i Telekomunikacji
Politechnika Wrocławska

Wrocław, 13 stycznia 2025 r.

RECENZJA

rozprawy doktorskiej mgra inż. Piotra Piątka

pt. „*Systemowa analiza bezpieczeństwa układów sterowania w pojazdach o wysokim stopniu automatyzacji jazdy*"

Recenzję wykonano na prośbę Przewodniczącego Rady Dyscypliny Automatyka, elektronika, elektrotechnika i technologie kosmiczne AGH, dra hab. inż. Ryszarda Sroki, prof. AGH, wyrażoną w piśmie L. Dz. RD AEEiTK/510-9-4/24 z dnia 8 listopada 2024 r.

I. OBSZAR PROBLEMOWY ROZPRAWY

Opiniowana rozprawa doktorska ma charakter aplikacyjny, związany z zachodzącym i obserwowanym obecnie intensywnym rozwojem przemysłu motoryzacyjnego, a przede wszystkim innowacjami w projektowaniu i produkcji samochodów. Rozwój ten, który jest możliwy dzięki postępowi w zakresie elektroniki, automatyki oraz informatyki, jest wielowątkowy. Jednym z celów, istotnych dla rozważań prezentowanych w rozprawie jest dążenie do pogłębienia automatyzacji, czyli zastępowania przez urządzenia techniczne człowieka, kierowcy w wykonywaniu czynności związanych z kierowaniem i obsługą samochodu. Celem dzisiaj jeszcze dosyć odległym jest opracowanie samochodów w pełni zautomatyzowanych, czyli tak zwanych samochodów autonomicznych, w których udział człowieka w jego kierowaniu i obsłudze byłby całkowicie wyeliminowany. Ważne i aktualne są także cele pośrednie, cechujące się przejmowaniem kolejnych czynności kierowcy przez urządzenia techniczne, ale z zachowaniem decydującego wpływu człowieka na kierowanie pojazdem. Współczesne samochody są wyposażone w wiele urządzeń wspomagających kierowcę i znanych pod wspólną nazwą zaawansowanych systemów wspomagania kierowcy (ang. ADAS, *Advanced Driver Assistance System*). Są one realizowane przez wyspecjalizowane urządzenia elektryczne i elektroniczne. Działanie tych urządzeń musi być bezpieczne, co jest regulowane odpowiednimi normami międzynarodowymi i urzeczywistniane przez producentów zarówno wspomnianych urządzeń, jak i samochodów, rozumianych jako produkt końcowy. Całokształt zagadnień związanych z tak pojmowanym bezpieczeństwem systemów (układów) wspomagających kierowcę jest w rozprawie określany mianem bezpieczeństwa funkcjonalnego (ang. FuSa, *Functional Safety*). Warto zauważyć, że wzrost liczby urządzeń wspomagających kierowcę rodzi nowe problemy, np. koordynacji ich działania oraz właściwej wymiany informacji między nimi. Należy podkreślić, że rozwój charakteryzowanych tutaj urządzeń elektronicznych do wspomagania kierowców pociągnął za sobą konieczność wykorzystywania coraz bardziej zaawansowanego oprogramowania, ale na tym etapie rozwoju automatyzacji kierowania sa-

mochodami, nie była to jeszcze kwestia krytyczna i kluczowa z punktu widzenia bezpieczeństwa. Specyficzne projekty takich urządzeń bazowały na osiągnięciach metodologicznych z obszaru systemów mechatronicznych i wbudowanych.

Rozwój technicznych i metodologicznych środków informatyki, przede wszystkim w zakresie szybkiego przesyłania, przetwarzania i gromadzenia dużych wolumenów danych (informacji) umożliwił rozszerzanie zakresu omawianej automatyzacji, dostarczanie kierowcy na bieżąco różnych informacji przydatnych w trakcie kierowania oraz jedno- albo dwukierunkowy kontakt z otoczeniem samochodu. Możliwość wykorzystania tego typu dodatkowych funkcjonalności w samochodach sprawia, że obecnie wyzwania w motoryzacji nie tylko polegają na doskonaleniu systemów mechanicznych, elektrycznych, czy elektronicznych, ale raczej na właściwych sposobach wykorzystywania środków informatyki, w tym zwłaszcza oprogramowania, w którym zaimplementowano często złożone algorytmy przetwarzania informacji. Dlatego można się spotkać w literaturze przedmiotu ze stwierdzeniami, że obecnie samochód jest to pojazd definiowany programowo (ang. SDV, *Software Definied Vehicle*) albo „zaawansowane urządzenie elektroniczne na kołach, skoncentrowane na oprogramowaniu". Jest oczywiste, że dla takich produktów, jakimi są wspomniane nowoczesne samochody, kwestie bezpieczeństwa związanego z pozyskiwaniem, transmisją, przetwarzaniem, gromadzeniem i wykorzystywaniem danych, mające wpływ na funkcjonowanie samochodów, są szczególnie ważne i krytyczne. Kwestie takie zwykle określa się wspólnym mianem „cyberbezpieczeństwa", a w ocenianej pracy jest wykorzystywany akronim CySe (ang. *Cybersecurity*).

Cyberbezpieczeństwo w samochodach jest stosunkowo nowym i aktualnym obszarem badań oraz rozwoju, z oczywistym zastosowaniem w przemyśle samochodowym oraz o charakterze interdyscyplinarnym, dotyczącym zarówno informatyki, ale także elektroniki i automatyki. Z punktu widzenia ostatnich dwóch wymienionych dyscyplin (będących poddyscyplinami dyscypliny Automatyka, elektronika, elektrotechnika i technologie kosmiczne) opisywane zagadnienia i wyzwania są istotne, m.in. dla rozwoju systemów mechatronicznych oraz cyberfizycznych.

Szeroko rozumiane bezpieczeństwo działania samochodów jest zasadniczą motywacją podjęcia badań przez doktoranta, które zaowocowały ocenianą rozprawą doktorską. Doktorant słusznie zauważył, że bezpieczeństwo funkcjonalne (FuSa) oraz cyberbezpieczeństwo (CySe) są ze sobą powiązane i w całym cyklu życia samochodu należy je rozpatrywać łącznie. Efektem końcowym prac, które bardziej dokładnie będą omówione w następnym punkcie tej recenzji, jest propozycja procesu CyberSafety, czyli oryginalnego rozwiązania projektowego, który może być wykorzystany w branży motoryzacyjnej. Oryginalnym wkładem doktoranta w opracowanie ram procesu CyberSafety jest wykorzystanie podejścia holistycznego, które jest oferowane przez inżynierię systemów i może być stosowane w różnych działach gospodarki.

Podsumowując, uważam, że zagadnienie badawcze, o charakterze głównie aplikacyjnym, do rozpatrzenia w trakcie realizacji pracy doktorskiej zostało wybrane prawidłowo i może być ulokowane w dyscyplinie Automatyka, elektronika, elektrotechnika i technologie kosmiczne.

II. ZAWARTOŚĆ ROZPRAWY

Podstawą recenzji jest rozprawa doktorska napisana w języku polskim. Doktorant przedstawił również jej wersję w języku angielskim. Tekst liczy 318 stron, w tym 137 stron zawierających dodatek z modelem procesu CyberSafety, który utworzono z wykorzystaniem narzędzia Bizagi Modeller, a także streszczenia, spisy treści i rysunków oraz z wykaz skrótów. Część zasadnicza przedstawiona na 181 stronach została podzielona na pięć rozdziałów i zawiera wykaz 131 pozycji literaturowych. W rozdziale 1. przedstawiono motywację podjęcia pracy, jej zakres i strukturę, sfomułowano hipotezy i cele rozprawy, a także scharakteryzowano wkład w dyscyplinę Automatyka, elektronika, elektrotechnika i technologie kosmiczne. Ostatni, piaty rozdział zawiera podsumowanie i wnioski.

Rozdział 2. jest poświęcony wyjaśnieniu używanych dalej pojęć i metod oraz przeglądowi literatury ze szczególnym uwzględnieniem pozycji na temat aktualnych wyzwań i innowacyjnych rozwiązań w zakresie bezpieczeństwa i cyberbezpieczeństwa w branży motoryzacyjnej. Scharakteryzowano metodę (model) V, czyli stosowaną dalej w rozprawie metodę obejmującą całokształt działań związanych z wytwarzania produktów, m.in. oprogramowania, szeroko wykorzystywaną w inżynierii systemów. Omówiono problematykę bezpieczeństwa funkcjonalnego oraz cyberbezpieczeństwa w sektorze motoryzacyjnym. Zaprezentowano rozszerzenie standardowego zakresu bezpieczeństwa funkcjonalnego FuSa, zgodnego z normą ISO 26262:2018, poprzez uwzględnienie tzw. bezpieczeństwa zamierzonej funkcjonalności SOTIF, (ang. *Safety of Intended Functionality*). Takie szersze rozumienie bezpieczeństwa funkcjonalnego wraz z cyberbezpieczeństwem jest rozwijane w dwóch kolejnych rozdziałach rozprawy. Przedyskutowano wyzwania związane z rozwojem, a zwłaszcza projektowaniem i utrzymaniem produktów przemysłu motoryzacyjnego typu SDV i niezależnych od sprzętu. Miedzy innymi wskazano na różne możliwe architektury takich produktów. Omówiono sposoby zapewniania odpowiedniej jakości oprogramowania wytwarzanego na potrzeby przemysłu motoryzacyjnego i implementowanego w jego produktach, poprzez stosowanie rygorystycznych standardów bezpieczeństwa, np. ASPICE, (ang. *Automotive Software Process Improvement and Capability Determination*) w połączeniu z modelem V i w pełnym cyklu życia produktu.

Szczegółowo scharakteryzowano także zagrożenia bezpieczeństwa oraz konieczność wdrażania adekwatnych sposobów ochrony dla różnych przewidywanych wizji systemów motoryzacyjnych. Osobne punkty poświecono przedstawieniu różnych metod zarządzania projektami oraz inżynierii systemów opartej na modelach. Oba te zagadnienia są bardzo ważne i stosowane przez doktoranta w opracowaniu autorskiego systemu CyberSafety.

Dobór treści rozdziału 2., sposób ich prezentacji oraz właściwe posługiwanie się źródłami literaturowymi potwierdzają wiedzę teoretyczną doktoranta, m.in. w zakresie nowoczesnych systemów wbudowanych w tym ich oprogramowania, inżynierii systemów oraz projektowania układów elektronicznych stosowanych w nowoczesnych pojazdach samochodowych, z uwzględnieniem ich bezpieczeństwa funkcjonalnego oraz cyberbezpieczeństwa.

Dwa kolejne rozdziały przedstawiają oryginalne osiągnięcia doktoranta. W rozdziale 3. jest przedstawiona ogólna postać procesu CyberSafety; w kolejnych podpunktach są prezentowane jego części składowe. Do zapisu wykorzystano notację BPMN (ang. *Business Process Model and Notation*) oraz język SysML (ang. *Systems Modeling Language*) i posłużono się w tym celu programem Bizagi Mo-

deller. Proces ten zapewnia łączne rozpatrywanie ogólnie pojętego bezpieczeństwa funkcjonalnego, tzn. FuSa i SPOTIF oraz cyberbezpieczeństwa CySe. Do integracji wymienionych aspektów bezpieczeństwa wykorzystano wybrane narzędzia inżynierii systemów, które ogólnie mają szeroki zakres zastosowań, wykraczający poza branżę motoryzacji. Proces CyberSafety jest dedykowany wytwarzaniu oprogramowania na potrzeby przemysłu motoryzacyjnego. Przyjęte podejście systemowe (holistyczne) oznacza nie tylko integrację różnych aspektów bezpieczeństwa, ale również wszystkich etapów cyklu życia produktu, począwszy od przygotowania projektu, poprzez opracowanie koncepcji, projektowanie, wdrożenie, wydanie, utrzymanie, aż do wycofania produktu i jego utylizacji. Zgodnie z metodą V zarządzania projektami przewidziano równoległe testowanie produktu poprzez jego walidację i weryfikację, co jest szczególnie istotne w etapach projektowania i wdrażania. Etapy są kolejno prezentowane, a pełna wersja powstałego modelu procesu CyberSafety jest przedstawiona w Dodatku A. Szczególnie obszernie zaprezentowano etap projektowania.

W rozdziale 4. doktorant podjął próbę oceny procesu CyberSafety. Ograniczył ją jedynie do rozpatrzenia jednego przykładu, studium przypadku, którym był system wspomagania jazdy autostradą HP (ang. *Highway Pilot*). Do badania procesu CyberSafety dla rozważanego przykładu, a w szczególności do analizy zapewnianego przez niego bezpieczeństwa wykorzystano narzędzie Ansys Medini. Dla przyjętych w tym rozdziale założeń i danych określono poziom bezpieczeństwa systemu HP, jeśli jego aspekty FuSa, SPOTIF i CySe są w kolejnych etapach uwzględniane łącznie. Do oceny poziomu bezpieczeństwa wykorzystano znane oraz własne wskaźniki oceny, w tym ważony współczynnik bezpieczeństwa WSS (ang. *Weighted Safety Score*), który umożliwia różnicowanie znaczenia bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa. Oceniano także wpływ zastosowanej integracji aspektów bezpieczeństwa na zmniejszenie nakładu pracy (wysiłku) przy realizacji projektu. W celu przeprowadzenia badania dla opisywanego studium przypadku wykorzystano narzędzie Ansys Medini w zakresie symulacji ataków na działanie systemu HP przy różnych scenariuszach. Wyróżniono scenariusze uszkodzeń dla CySe i zdefiniowano zagrożenia dla FuSa. Na tej podstawie zaproponowano potencjalne scenariusze ataków. Następnie zasymulowano 15 różnych ataków, dla których przeprowadzono łączną analizę bezpieczeństwa. Narzędzie Ansys Medini umożliwiło ocenę wykonalności ataków oraz wyznaczenie stopni i rodzajów zagrożeń i strat, które mogą one spowodować. Przeprowadzona analiza dla rozpatrywanego przypadku użycia systemu HP potwierdziła skuteczność projektowania oprogramowania na potrzeby pojazdów samochodowych z wykorzystaniem procesu CyberSafety, w którym aspekty bezpieczeństwa funkcjonalnego w szerszym sensie i cyberbezpieczeństwa są uwzględniane łącznie. Kluczowy wynik jest zaprezentowany na rys. 4.43. Ciekawy wynik ilościowy przedstawiono w tabeli 4.19. Ze względu na ograniczony zakres przeprowadzonych badań, nie ma podstaw do wyciągania bardziej ogólnych wniosków.

Wyniki przedstawione w rozdziałach 3. i 4. potwierdzają umiejętność samodzielnego prowadzenia badań przez doktoranta.

III. ORYGINALNE OSIĄGNIĘCIA

Głównym osiągnięciem doktoranta jest

1. Opracowanie oryginalnej metody projektowania i wdrażania zaawansowanych systemów informatycznych, implementowanych w zaawansowanych elektronicznych układach wspomagania kierowców i zapewniających bezpieczne funkcjonowanie pojazdów i skuteczną ochronę przed cyberatakami – większe niż przy stosowaniu metod tradycyjnych. Wspomniana oryginalność metody polega na łącznym uwzględnianiu w trakcie projektowania i wdrażania, a także w pozostałych etapach cyklu życia produktu różnych aspektów bezpieczeństwa, w tym bezpieczeństwa funkcjonalnego, bezpieczeństwa związanego z funkcjonalnościami przewidywanymi do wprowadzenia oraz cyberbezpieczeństwa.

Inne osiągnięcia, na które warto zwrócić uwagę, to:

2. Przeprowadzenie analizy bezpieczeństwa modelu systemu wspomagania jazdy autostradą HP, traktowanego jako przykład do oceny możliwości zastosowania i skuteczności procesu CyberSafety.
3. Sformułowanie i wykorzystanie do analizy bezpieczeństwa współczynnika WSS, służącego do łącznej oceny bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa.
4. Prawidłowe wykorzystanie do opracowania procesu CyberSafety, w miejsce podejścia bazującego na dokumentach, podejścia systemowego, w tym metody V i podejścia bazującego na modelach MBSE (ang. Model Based Systems Engineering).

Wymienione osiągnięcia, mimo uwag krytycznych przedstawionych w następnym punkcie tej recenzji, w stopniu zadowalającym uzasadniają stwierdzenie, że oceniana rozprawa doktorska stanowi oryginalne rozwiązanie w zakresie zastosowania własnych wyników badań naukowych doktoranta w branży motoryzacyjnej.

IV. UWAGI KRYTYCZNE I POLEMICZNE

W stosunku do rozprawy można sformułować szereg uwag krytycznych i polemicznych, odnoszących się zarówno do meritum rozważań, jak i do sposobu prezentacji:

1. W punkcie 1.2 są podane hipotezy i cele badawcze rozprawy. W mojej ocenie, w rozprawach doktorskich realizowanych w dziedzinie nauk inżynieryjno-technicznych często trudno jest formułować hipotezy, czy też tezy badawcze. Ważniejsze są cele badawcze. Doktorant podał dwie hipotezy, z których pierwsza jest kontrowersyjna. Brzmi ona następująco: „*Wczesna współpraca w zakresie zintegrowanego bezpieczeństwa i ochrony w całym cyklu życia produktu zapewni najwyższą niezawodność i jakość wbudowanych systemów samochodowych o wysokiej autonomii, minimalizując ryzyko i zapewniając wysoką efektywność procesu projektowania*". Stawianie takiej hipotezy jest bardzo ryzykowne, ponieważ bardzo trudno byłoby zweryfikować, że wspomniane w niej systemy samochodowe cechują się najwyższą niezawodnością i jakością oraz powstałe ryzyko jest najmniejsze. Doktorant w ogóle nie podejmuje w rozprawie próby uzasadnienia albo przetestowania tak postawionej hipotezy. Brak jest informacji o jakichkolwiek działaniach optymalizacyjnych. Porównuje jedynie swoje podejście z innym podejściem, standardowo wykorzystywanym w rozpatrywanym zagadnieniu i wykazuje przewagi tego pierwszego. Nie ma jednak żadnych podstaw

do wyciągnięcia wniosku o optymalności proponowanego podejścia w sensie podanym w treści hipotezy.

Podane cele badawcze nie budzą większych wątpliwości i analiza całości pracy doktorskiej pozwala uznać, że zostały one osiągnięte. Wydaje się tylko, że nie było potrzeby odnoszenia celów do systemów sterowania. Fraza „systemy sterowania" występuje także w tytule rozprawy. Natomiast w całej pracy nie ma w ogóle mowy o systemach sterowania. Doktorant nie używa tej nazwy. Mówi o oprogramowaniu wykorzystywanym w układach elektronicznych. Oczywiście, te układy spełniają również funkcje sterowania, ale nie sterowanie jest przedmiotem badań, tylko bezpieczeństwo związane z funkcjonowaniem tych układów, zapewniane przez właściwe zaprojektowanie i wykorzystanie w nich systemów informatycznych/oprogramowania. Te uwagi nie podważają zasadności ulokowania treści i wyników rozprawy w dyscyplinie Automatyka, elektronika, elektrotechnika i technologie kosmiczne, chociaż umieszczenie jej w dyscyplinie Informatyka techniczna i telekomunikacja również byłoby możliwe.

2. Badania opracowanego procesu CyberSafety ograniczono do jednego przypadku użycia i do jednego zestawu danych. Rozszerzenie badań nawet w ramach tego samego przypadku użycia mogłoby być podstawą do bardziej wszechstronnej oceny zaproponowanej metody.
3. Rysunek 4.43 przedstawia wartości współczynnika AFR dla różnych rodzajów ataków w dwóch wersjach: przed (a) i po (b) zastosowaniu kontroli CySe. Co konkretnie oznacza przypadek (a)? Ponadto, dlaczego przedstawiono wyniki zagregowane tylko dla czterech przypadków ataków a nie dla każdego z rozważanych ataków osobno?
4. W rozprawie podano jedynie zalety łącznego rozpatrywania bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa, np. w postaci wzrostu bezpieczeństwa produktu oraz zmniejszenia nakładu pracy na realizację projektu. Jakie są „koszty" takiego podejścia systemowego, rozumiane ogólnie? Czy integracja FuSa, SOTIF i CySe spowodowała pojawienie się dodatkowych zadań do wykonania?
5. Kolejna moja uwaga dotyczy sposobu prezentacji analizy, przedstawionej w rozdziale 4. Lektura tego rozdziału jest utrudniona z powodu nieuporządkowanego sposobu prezentacji. Preferowany sposób prezentacji polegałby na tym, że po opisowym podaniu celu badań (analizy) następuje prezentacja wraz z uzasadnieniem przyjętych założeń, danych i używanych sposobów/wskaźników oceny, z kolei powinien być podany plan badań, następnie sposób przeprowadzenia badań, uzyskane wyniki oraz wnioski – dla każdego badania osobno. Tymczasem w rozprawie nie wyjaśniono, dlaczego takie a nie inne możliwe badania przeprowadzono, a używane do oceny wskaźniki wprowadzono dopiero w dalszej części rozdziału.

   Z tą ogólną uwagą łączą się uwagi szczegółowe 13 i 18.

Inne uwagi szczegółowe; kolejność ich przedstawienia nie ma znaczenia.

6. Nie wiadomo, dlaczego w rozprawie odnoszono się do firmy Aptiv, np. na s. 6 i w podrozdziale 2.9, a nie do innych firm działających w branży motoryzacyjnej?
7. Co to jest Delta w tabeli 2.2?
8. Nie dość precyzyjnie wyjaśniono w rozprawie relacje między bezpieczeństwem a ochroną.

9. Na s. 9 znajduje się następująca informacja: „*Ponadto w załączniku B, w oparciu o wyniki prac doktorskich, przedstawiono analizę cyberbezpieczeństwa struktury Highway Pilot ADAS...*". O jakie prace doktorskie chodzi?
10. W drugim od dołu akapicie na s. 115 jest mowa o relacjach między scenariuszami? Relacje takie należało wyjaśnić i podać ich przykłady.
11. W pierwszym akapicie na s. 119 wskazano na związki między CySe i FuSa. Charakter tych zależności powinien być w rozprawie (niekoniecznie w tym miejscu) dokładniej wyjaśniony, np. czy jest to zależność obustronna i na czym konkretnie polega?
12. Na s. 126 jest zdanie "*Narzędzie pozwala również na określenie środków i celów cyberbezpieczeństwa w celu zminimalizowania określonych zagrożeń*". O jaką minimalizację chodzi, w jaki sposób jest ona przeprowadzana?
13. Uwaga łącząca się z uwagą nr 5: Opis podstaw badań podany pod rys. 4.28 na s. 134 powinien być bardziej dokładny, m.in. wraz z podaniem wykazów wszystkich rozpatrywanych elementów, zagrożeń, scenariuszy, zasobów itp. Nie jest ich dużo w tym badaniu. Taka informacja poprawiłaby czytelność i możliwość lepszego zrozumienia wywodu.
14. W ostatnim akapicie na s. 134 czytamy: „*Badanie wzmacnia pogląd, że wspólne podejście TARA i HARA, uzupełnione o rozważania SOTIF, stanowi solidną podstawę do identyfikacji i rozwiązywania potencjalnych wyzwań związanych z bezpieczeństwem.*" Jest to bardzo ważny wniosek, tyle tylko, że bardzo słabo uzasadniony wynikami przeprowadzonej analizy.
15. Treść tabeli 4.3 jest niezrozumiała. Wymagałaby bardziej szczegółowego wyjaśnienia.
16. Postać wskaźnika AFR jest nieintuicyjna, tzn. wyższa wykonalność ataku jest reprezentowana przez niższą liczbową wartość wskaźnika AFR. Czy nie powinno być odwrotnie?
17. W ostatnim akapicie na s. 143 użyto sformułowania „*bardziej zoptymalizować*". Oczywiście, niczego nie można bardziej zoptymalizować.
18. Dlaczego nazwy analizowanych piętnastu ataków wprowadzono dopiero na rys. 4.37? We wcześniejszej prezentacji w podrozdziale 4.2 ataki powinny mieć swoje identyfikatory (numery), a na odpowiednich rysunkach powinny się pojawiać nie tylko zbiorcze liczby ataków zakwalifikowanych do poszczególnych kategorii (np. bespoke, specialized, standard na rys. 4.35), ale także ich identyfikatory, po to, aby można było określić, które konkretnie ataki należą do tych kategorii.
19. Na s. 149 jest zapis: „*Dzięki zastosowaniu odpowiednich mechanizmów kontroli bezpieczeństwa*". O jakie mechanizmy chodzi i gdzie zostały one opisane?
20. We wzorach (4.4) oraz (4.5) brak jest wyjaśnienia indeksów, odpowiednio i oraz j. Dlatego te wzory oraz powiązane z nimi rozważania nie są zrozumiałe.
21. Wartości podane w ostatniej kolumnie tabeli 4.12 nie mogą być prawdopodobieństwami, ponieważ nie należą do przedziału [0, 1].

Część z tych uwag, zwłaszcza dotyczących sposobu prezentacji, ma charakter polemiczny i potencjalnie może być wykorzystana przy dalszym publikowaniu wyników pracy.

V. KONKLUZJA

Biorąc pod uwagę opinie przedstawione w poprzednich punktach recenzji, stwierdzam, że rozprawa doktorska przygotowana przez mgra inż. Piotra Piątka zawiera oryginalne rozwiązanie w zakresie

zastosowania wyników własnych badań naukowych w sferze gospodarczej, a także pozwala stwierdzić, że doktorant posiada ogólną wiedzę teoretyczną w dyscyplinie Automatyka, elektronika, elektrotechnika i technologie kosmiczne oraz umiejętność samodzielnego prowadzenia pracy naukowej, a więc spełnia wymagania stawiane rozprawom doktorskim w art. 187 Ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (z późniejszymi zmianami).

Na tej podstawie wnoszę o dopuszczenie mgra inż. Piotra Piątka do dalszych etapów przewodu doktorskiego.