RDIMe 512.28.2023

POLITECHNIKA RZESZOWSKA
im. IGNACEGO ŁUKASIEWICZA

al. Powstańców Warszawy 12
35-959 Rzeszów, http://w.prz.edu.pl
NIP: 813-02-66-999

dr hab. inż. Paweł Woś, profesor uczelni

POLITECHNIKA RZESZOWSKA
im. Ignacego Łukasiewicza
WYDZIAŁ BUDOWY MASZYN I LOTNICTWA
Katedra Pojazdów Samochodowych
i Inżynierii Transportu

Al. Powstańców Warszawy 12
35-959 Rzeszów
tel. 17 865 1355, pwos@prz.edu.pl

Rzeszów; 29.01.2024 r.

RECENZJA
rozprawy doktorskiej mgr inż. Marcina Gajdzika
pt. „Identification and minimization of threats in embedded systems during the car vehicles maintenance, in accordance with Industry 4.0 concept"

1. Formalna podstawa opracowania recenzji

Podstawę do opracowania i wydania niniejszej recenzji stanowi pismo z dnia 28.09.2023 r. Przewodniczącej Rady dyscypliny inżynieria mechaniczna Politechniki Śląskiej z siedzibą w Gliwicach, Pani prof. dr hab. inż. Ewy Majchrzak (znak pisma RDIMe.512.28.2023) w sprawie sporządzenia recenzji rozprawy doktorskiej Pana mgr inż. Marcina Gajdzika pod wymienionym tytułem.

2. Przedmiot i ocena istotności problemu naukowego rozprawy

Rozwój motoryzacji na przestrzeni ostatnich dziesięcioleci, podobnie jak wielu innych obszarów gospodarki i całości życia społecznego, pozostaje pod bardzo silnym wpływem rozwoju technologii informacyjnej i komputerowych systemów sterowania. W wyniku fuzji osiągnięć o niezaprzeczalnie epokowym znaczeniu w dziedzinie informatyki, algorytmiki, automatyki, sensoryki technicznej, przy szerokim wykorzystaniu opracowanych w XX w.

elektronicznych układów wielkiej skali integracji, pojawiła się i podlega nieustannemu, intensywnemu rozwojowi dziedzina wiedzy inżynierskiej określanej mianem mechatroniki.

Implementacja pierwszych systemów mechatronicznych w pojazdach samochodowych została niejako wymuszona próbą kontroli i ograniczenia szybko narastających w obliczu skali rozwoju transportu drogowego zagrożeń środowiskowych, mających istotne znaczenie dla ochrony środowiska naturalnego, jak również minimalizacji negatywnego oddziaływania na zdrowie indywidualne i publiczne oraz jakość życia społeczeństw. Wśród tych zagrożeń wymienia się w pierwszej kolejności emisję szkodliwych składników spalin powstających w wyniku eksploatacji pojazdów, napędzanych za pomocą silników wewnętrznego spalania. Spaliny samochodowe zawierają w swym składzie liczne związki i substancje chemiczne m.in. tlenek węgla (CO), węglowodory (HC), tlenki azotu (NOx), cząstki stałe (PM) oraz wiele innych, które przyczyniają się do pogorszenia jakości powietrza a w bezpośrednim oddziaływaniu mogą prowadzić do poważnych problemów zdrowotnych u ludzi - schorzeń układu oddechowego, alergii, chorób nowotworowych.

W następstwie rozpoznania i ciągłego narastania skali problemu emisji spalin samochodowych prowadzono od wielu lat intensywne badania nad metodami skutecznego ograniczania tych niekorzystnych zjawisk. Głównym celem w tym zakresie pozostaje ukierunkowany rozwój technologiczny pojazdów samochodowych w postaci opracowania i wdrażania skutecznych technologii poprawy sprawności energetycznej silników spalinowych, redukcji poziomu emisji spalin, wprowadzenie odpowiednich regulacji i norm dotyczących systemów kontroli emisji spalin oraz metod i procedur pomiarowych. Wynikiem tych działań była m.in. implementacja różnych rozwiązań i udoskonaleń w konstrukcji i technologii silników spalinowych oraz nowych systemów technicznych, w tym mikroprocesorowych jednostek sterowania silnikiem ECU i pokładowych systemów diagnostycznych OBD.

Stopniowo elektroniczne systemy sterowania zaczęły obejmować kontrolę działania innych podzespołów i układów funkcjonalnych w pojazdach, tj. układów bezpieczeństwa czynnego i biernego (ABS, ESP), układów zarządzania energią elektryczną, układów przeniesienia napędu (automatyczne skrzynie biegów), zabezpieczenia przeciwkradzieżowego (immobiliser), zawieszenia i kierowania kół czy wreszcie systemów komfortu jazdy (np. inteligentne systemy wspomagania skrętu kół, tempomat, automatyczna klimatyzacja, oczyszczanie szyb) i innych, nawet mniej istotnych elementów w samochodzie. Obecnie praktycznie całość konstrukcji pojazdu ze wszystkimi jej komponentami, wyposażonymi w odpowiednie czujniki i mechatroniczne elementy wykonawcze jest pod kontrolą centralnego, komputerowego systemu sterowania o wielopoziomowej strukturze funkcjonalnej, łącznie z komunikacją bezprzewodową na linii pojazd – kierowca czy też pojazd – obsługa serwisowa. Niewątpliwą zaletą takiego rozwiązania jest znaczna poprawa jakości eksploatacyjnej i obsługowej pojazdu, komfortu pracy kierowcy, bezpieczeństwa w ruchu drogowym oraz zmniejszenie negatywnych oddziaływań na środowisko. Systemy te bowiem wyposażone są w

funkcję autodiagnostyki, która w przypadku wystąpienia usterki technicznej, zwłaszcza zagrażającej czy to bezpieczeństwu ruchu czy też bezpieczeństwu środowiskowemu, natychmiastowo powiadamia obsługę pojazdu o tym zdarzeniu i umożliwia szybkie podjęcie akcji serwisowo-naprawczej lub nawet zdalne wyłączenie pojazdu z ruchu. Systemy te wciąż bardzo szybko ewoluują w kierunku coraz szerszego przejmowania zadań i decyzyjności kierowcy, co sprawia, że stoimy u progu ery pojazdów autonomicznych.

Pomimo niezaprzeczalnych zalet wynikających z postępującej mechatronizacji pojazdów samochodowych to jednak złożoność i rozległość tych systemów może rodzić określone problemy obsługowe i eksploatacyjne, a także zagrożenia związane z możliwością nieuprawnionego ingerowania w ich działanie. Jak każdy system komputerowy, pomimo zastosowania wielu zabezpieczeń sprzętowych i programowych, posiadają bowiem pewne luki, niezidentyfikowane na etapie budowy i wdrażania, a jakie mogą być wykorzystane później do przeprowadzenia „cyberataku" np. w celu przejęcia kontroli nad pojazdem i ewentualnie kradzieży lub jego uszkodzenia. Niniejsza praca Pana mgr inż. Marcina Gajdzika zatytułowana *„Identification and minimization of threats in embedded systems during the car vehicles maintenance, in accordance with Industry 4.0 concept"*, zrealizowana pod opieką naukową Pani promotor dr hab. inż. Anny Timofiejczuk prof. PŚ oraz przy wsparciu merytorycznym i metodycznym promotora wdrożeniowego, Pana dr inż. Wojciecha Sebzdy dotyka sedna powyższych zagadnień. Jej tematyka wpisuje się bowiem w aktualne obszary problemowe obejmujące cyberzagrożenia systemów technicznych i antropotechnicznych oraz poszukiwanie skutecznych metod ochrony przed nimi. **Problematyka badawcza pracy określona przez jej Autora jako ogólny cel badawczy pracy dotyczy konkretnie systemów mechatronicznych w pojazdach samochodowych, identyfikacji zagrożeń zewnętrznych dla ich funkcjonowania, opracowanie tanich i skutecznych metod szyfrowania przepływu danych, w tym z wykorzystaniem metod sztucznej inteligencji.** W szczególności praca ta obejmuje swym zakresem analizę stanu wiedzy oraz techniki, badania eksperymentalne w zakresie możliwości przeprowadzenia i wykrywania cyberataku na systemy wbudowane pojazdu oraz próbę opracowania skutecznej ochrony przed nimi.

Można zatem stwierdzić, że przedstawiona praca doktorska Pana mgr inż. Marcina Gajdzika wpisuje się swoją tematyką i zrealizowanym zakresem prac w interesujące i aktualne obszary badań poznawczych i aplikacyjnych nauk technicznych w dyscyplinie inżynieria mechaniczna, w szczególności badań nad poprawą bezpieczeństwa systemów mechatronicznych pojazdów, a w szerszym ujęciu - współczesnych systemów transportowych i systemów służących obronności kraju. Obecnie bowiem, we wszystkich pojazdach sił zbrojnych, czy to pojazdach walki bezpośredniej czy wsparcia taktycznego i technicznego stosuje się powszechnie komputerowe systemy sterowania.

3. Charakterystyka rozprawy i ocena strony metodycznej – uwagi o charakterze redakcyjnym

3.1. Problematyka i struktura rozprawy

Opiniowana rozprawa doktorska zawiera w swojej treści część studialną, opartą na analizie dostępnego materiału źródłowego z zakresu problematyki pracy oraz część eksperymentalno-rozwojową, która obejmowała przeprowadzenie serii badań testowych z wykorzystaniem współcześnie produkowanych samochodów osobowych. Testy te obejmowały przeprowadzenie celowych prób destabilizacji lub przejęcia kontroli nad wybranym systemem mechatronicznym pojazdu, ocenę skuteczności przeprowadzonego cyberataku, opracowanie koncepcji zabezpieczenia danego systemu przed tego rodzaju ingerencją i kolejno ocenę skuteczności wprowadzonych modyfikacji/zabezpieczeń. Jako efekt utylitarny wykonanych prac zaproponowano wybrane rozwiązania sprzętowo-programowe do ewentualnego wdrożenia produkcyjnego systemów zabezpieczeń współcześnie produkowanych pojazdów.

Praca jest napisana w języku angielskim stylem umożliwiającym przystępny odbiór i zrozumienie treści dla czytelnika nieanglojęzycznego, z użyciem poprawnej terminologii technicznej. Całość opracowania zawiera 119 stron tekstu skonfigurowanego w formacie A4, łącznie ze stroną tytułową, spisem treści, wykazem ważniejszych skrótów i oznaczeń, streszczeniem w języku polskim i angielskim oraz bibliografią, na którą składają się łącznie 73 pozycje. Autorskie lub współautorskie cytowania dzieł Doktoranta obejmują 6 pozycji bibliograficznych. W pracy zamieszczono 85 rysunków i 7 tablic – materiał ilustracyjny w większości czytelny i dobrej jakości graficznej. Rozprawa jest podzielona na 4 główne rozdziały, w tym rozdział zawierający wprowadzenie do tematu pracy, podsumowanie a ponadto wykaz literatury, spis rysunków i tabel. Rozdziały, stanowiące trzon merytoryczny pracy w większości są rozbudowane o kilka podrozdziałów.

Pracę rozpoczyna usystematyzowany wykaz użytych w pracy skrótów i oznaczeń wraz z opisem ich znaczenia. **Rozdział 1** stanowi zwięzłe wprowadzenie do tematyki pracy. Zasygnalizowano w nim główne przesłanki do podjęcia się przez Autora analizy tejże tematyki, przedstawiono cel i plan badawczy. Scharakteryzowano rodzaje potencjalnych zagrożeń dla systemów mechatronicnzych stosowanych w pojazdach samochodowych oraz podkreślono znaczenie cyberbezpieczeństwa z obliczu obecnego stanu rozwoju technologii pojazdów.

Rozdział 2 zwięźle zatytułowany „State-of-the-art" stanowi dalsze rozwinięcie informacji uzasadniających wybór podjętej problematyki badawczej. Jest to szczegółowy opis stanu zaawansowania i perspektywy rozwoju systemów mechatronicznych i teleinformatycznych w motoryzacji. Wskazano tutaj potencjalne zagrożenia dla bezpieczeństwa operacyjnego pojazdów oraz ruchu lądowego w przypadku przeprowadzenia

niepowołanych, zdalnych ingerencji w działanie układów funkcjonalnych pojazdu, które w znakomitej większości są pod kontrolą elektronicznych systemów sterujących z komunikacją wewnętrzną poprzez magistralę CAN. Wskazano możliwości i przykłady dokonania cyberataków zakłócających spójność i poprawność przesyłu danych w magistrali CAN oraz pewne możliwości zabezpieczenia się przed takimi atakami. Jako ciekawostkę w świetle rozwijających się instrumentów opartych na uczeniu maszynowym podane zostały możliwe zastosowania sztucznej inteligencji w obszarze motoryzacji i komunikacji.

W świetle przeprowadzonej dyskusji problemowej, w **rozdziale 3** sformułowano i przedstawiono realizację celów i zadań badawczych. Podano, że głównym celem rozprawy było sprawdzenie możliwości wykonania skutecznego cyberataku na wybrany element wykonawczy warstwy mechatronicznej pojazdu i propozycja wdrożenia mechanizmów utrudniających tego rodzaju destabilizujące działania. W zakresie zadaniowym, służącym realizacji celów pracy Autor przedstawia wykonanie czterech scenariuszy cyberataku, począwszy w kolejności od najmniejszej złożoności i trudności technicznej, kończąc na przykładzie zastosowania procedur sztucznej inteligencji do wykrycia cyberataku na magistralę CAN pojazdu w trybie aktywnego asystenta kontroli pasa ruchu. Każdorazowo zaproponowano proste rozwiązania programowe lub programowo-sprzętowe oraz bardziej zaawansowane metody oparte o samouczące się sieci neuronowe, które pozwoliłyby uniknąć tego rodzaju zakłóceń w działaniu magistrali CAN, jak w przeprowadzonych eksperymentach, i w efekcie zwiększyć poziom bezpieczeństwa użytkowania pojazdu.

Należy w tym miejscu podkreślić rozległy zakres oraz spójny z celem naukowym i utylitarnym oraz komplementarny charakter zaplanowanych do realizacji i przedstawionych w treści rozważań teoretycznych i prac eksperymentalnych, zarówno o charakterze pomiarowo-sprzętowym jak i informatyczno-programistycznym.

Podsumowanie pracy zawarto w **rozdziale 4**, gdzie wskazano najistotniejsze osiągnięcia naukowe i poznawcze w odniesieniu do założonego celu i zakresu pracy a także propozycje i możliwości wykorzystania opracowanych metod i wyników badawczych do wdrożenia przemysłowego w obszarze motoryzacji.

Przedstawiony układ pracy jest zatem logicznie poprawny i spójny tematycznie. Autor konsekwentnie rozwija podjętą, stosunkowo unikatową tematykę, począwszy od analizy aktualnego stanu wiedzy i techniki, wskazania obszarów badawczych i celu pracy, sposobu opisu i rozwiązania problemu badawczego, następnie poprzez realizację eksperymentów, rejestrację i analizę wyników aż po sformułowanie właściwych merytorycznie wniosków. Materiał ilustracyjny zamieszczony w pracy i dotyczący przedmiotu analiz oraz opracowanych wyników (tabele, wykresy) jest w większości czytelny, co pozwala na prawidłową ich interpretację. Pod względem metodycznym praca stanowi więc dzieło naukowe odpowiadające

wymaganiom prac badawczych, w tym rozprawom doktorskim o profilu technicznym. Znaczniejszych uwag o charakterze redakcyjnym nie wnosi się, poza tym, że w pracy **brak numeracji stron**, co nieco utrudnia jej czytelność i analizę treści. Z kolei szczegółowych uwag dotyczących stylu i języka pracy nie sformułowano, z uwagi na użycie języka nie natywnego, zarówno dla Autora pracy jak i jej recenzenta. Jak jednak wspomniano powyżej, sposób zredagowania pracy pozwala na pełne zrozumienie treści zarówno w sensie ogólnym jak i specjalistycznym.

4. Ocena merytoryczna rozprawy i uwagi dyskusyjne

Rozprawę doktorską pod względem merytorycznym należy ocenić wysoce pozytywnie. Przede wszystkim na podkreślenie zasługuje wybór aktualnej i jednocześnie unikatowej tematyki badawczej w świetle zaawansowania mechatronicznego i stopnia złożoności technicznej współczesnych pojazdów samochodowych. Również uzyskane w pracy efekty poznawcze są istotne, zarówno z praktycznego punktu widzenia jak i pod względem ich wkładu w rozwój dyscypliny naukowej inżynieria mechaniczna w zakresie bezpieczeństwa nowoczesnych i wciąż rozwijających się technologii oraz procedur z zakresu tzw. internetu rzeczy stosowanych we współczesnej motoryzacji.

W szczególności na pozytywną ocenę składają się m.in.:

- dogłębna analiza problematyki w zakresie rozwijającej się technologii systemów sterowania w pojazdach samochodowych i związanych z tym potencjalnych zagrożeń dla ich użytkowania i bezpieczeństwa ruchu drogowego,
- złożony charakter i komplementarny zakres wykonanych badań eksperymentalnych, obejmujący testy demonstracyjne możliwości dokonania ingerencji w działanie systemów wbudowanych, opracowania stosunkowo prostych do wdrożenia mechanizmów zabezpieczających przed tego rodzaju atakami wraz z walidacją ich skuteczności,
- opracowanie metodyki wykorzystania metod sztucznej inteligencji do wykrywania zaawansowanego cyberataku na sieć teleinformatyczną pojazdu i również w tym przypadku opracowanie metody minimalizującej powodzenie takiej akcji,
- szczegółowa prezentacja metodyki prowadzonych prac i wykorzystanych narzędzi, w tym opracowanie algorytmów testowych i prewencyjnych,
- przejrzysta analiza i merytoryczna dyskusja z w zakresie uzyskanych efektów badawczych, potencjalnych zagrożeń dla samego pojazdu, kierowcy oraz wszystkich uczestników znajdujących się w strefie ruchu pojazdu poddanego niebezpiecznej ingerencji w system sterowania,
- trafnie sformułowane wnioski poznawcze i utylitarne oraz wskazanie potencjalnych odbiorców wyników pracy.

Szczegółowa analiza treści rozprawy, biorąc pod uwagę zarówno aspekty metodyczne i merytoryczne, w niektórych fragmentach, sformułowaniach, przedstawionych wynikach, nasuwa jednak pewne wątpliwości o charakterze dyskusyjnym, wobec których oczekuje się stosownego odniesienia Doktoranta podczas publicznej obrony pracy doktorskiej, a mianowicie:

- w pracy, przy realizacji eksperymentów technicznych nie podano bardziej szczegółowej charakterystyki obiektów badawczych, tj. opisu technicznego (marka, model, konstrukcja czy też architektura zastosowanych systemów sterowania, osiągi, parametry robocze etc.) pojazdów wykorzystanych do badań, jak to powszechnie stosuje się w raportowaniu prac badawczych; czy takie pominięcie było intencją Autora wynikającą np. z zachowania poufności czy też po prostu swego rodzaju uproszczeniem?
- czy wg Doktoranta wykonane testy demonstracyjne lub innego rodzaju cyberataki byłyby możliwe bez fizycznej ingerencji w rozumieniu bezpośredniego podłączenia przewodowego urządzeniem testowym do magistrali CAN pojazdu, a jeżeli nie, to czy takie podłączenie się jest możliwe np. z zewnątrz pojazdu przez osobę niepowołaną?
- w nawiązaniu do poprzedniego pytania, czy pojazdy wyposażone w tzw. system „bezkluczykowy" są bardziej podatne na cyberatak? – znane są bowiem doniesienia o udanych próbach przechwycenia i zdekodowania zdalnych sygnałów sterujących immobiliserem pojazdu; czy w ten sposób można ingerować w działanie innych modułów sterujących pojazdu, np. w czasie jazdy, co niosłoby wysokie zagrożenie dla bezpieczeństwa ruchu o czym również wspomina Doktorant w swej pracy?
- czy okazjonalny, bezpośredni dostęp do magistrali CAN poprzez złącze diagnostyczne pojazdu (np. podczas naprawy pojazdu w warsztacie) może stanowić dla osoby atakującej możliwość skutecznego ataku (destabilizacji funkcjonowania pojazdu) odłożonego w czasie?
- czy Doktorant może wskazać konstruktywne aspekty (cele, funkcje) do zrealizowania poprzez podobną jak pokazaną w pracy ingerencję w systemy wbudowane pojazdów i ewentualnie jakie podmioty, oprócz wskazanego literalnie w pracy mogą korzystać z wyników pracy Doktoranta?

Proszę jednak mieć na względzie, że wyżej wymienione kwestie mają charakter czysto dyskusyjny – mogą wynikać z subiektywnej oceny recenzenta lub wręcz niezrozumienia danego problemu w świetle bądź to niepełnego opisu lub też specyfiki tematycznej, zapewne w wielu kwestiach oczywistej dla Autora pracy jako znawcy tematu, a niekoniecznie tak powszechnie znanej dla ogółu specjalistów z dziedziny motoryzacji.

Uwagi te w żaden sposób nie wpływają na pozytywny odbiór i ogólnie bardzo wysoką ocenę całości rozprawy, jaka skłania recenzenta do postawienia wniosku do Rady dyscypliny inżynieria mechaniczna Politechniki Śląskiej o jej wyróżnienie.

5. Podsumowanie oceny rozprawy doktorskiej i wnioski końcowe

Zrealizowana praca doktorska mgr inż. Marcina Gajdzika pt. *„Identification and minimization of threats in embedded systems during the car vehicles maintenance, in accordance with Industry 4.0 concept"* wpisuje się w prorozwojowe tendencje dotyczące bezpieczeństwa obecnych i podlegających intensywnemu ekspandowaniu systemów mechatronicznych stosowanych w pojazdach samochodowych. Stanowi oryginalne opracowanie naukowe i jednocześnie prezentuje interesujące rozwiązanie metodyczne dla osiągnięcia celu i wykazania słuszności przyjętych założeń objętych zakresem tematycznym rozprawy.

Doktorant wykazał się znajomością podjętej problematyki, umiejętnością prowadzenia eksperymentów badawczych w zakresie identyfikacji i zapobiegania ingerencji w strukturę danych i działanie tzw. „systemów wbudowanych" pojazdu, w tym wykorzystania zaawansowanych instrumentów pomiarowych, algorytmów i kodowania, analizy wyników oraz poprawnym formułowaniem wniosków. Świadczy to o posiadaniu ugruntowanej wiedzy teoretycznej i kompetencjach Autora rozprawy do samodzielnego prowadzenia prac badawczych w dziedzinie nauk inżynieryjno-technicznych, w szczególności w obszarze systemów mechatronicznych i internetu rzeczy.

Podsumowując stwierdzam zatem, że **rozprawa doktorska mgr inż. Marcina Gajdzika pt. *„Identification and minimization of threats in embedded systems during the car vehicles maintenance, in accordance with Industry 4.0 concept"* spełnia warunki zapisane w Ustawie z dnia 20 lipca 2018 r. „Prawo o szkolnictwie wyższym i nauce" (Dz.U. z 2018r., poz. 1668 z późn. zm.) i na tej podstawie wnioskuję o przyjęcie rozprawy i dopuszczenie jej do publicznej obrony przed Radą dyscypliny inżynieria mechaniczna Politechniki Śląskiej z siedzibą w Gliwicach.**

Jednocześnie wnioskuję o wyróżnienie rozprawy doktorskiej Pana mgr inż. Marcina Gajdzika pod wyżej wymienionym tytułem, o ile spełnione są inne warunki dotyczące zasad wyróżniania rozpraw doktorskich przyjęte na Uczelni.

PODPIS ZAUFANY
PAWEŁ
WOŚ
29.01.2024 09:27:02 (GMT+1)
Dokument podpisany elektronicznie
podpisem zaufanym

Rzeszów, 29 stycznia 2024 r.

Paweł Woś