RDINe. 512. 28.2023

Prof. dr hab. inż. Zbigniew Dąbrowski
Instytut Podstaw Budowy Maszyn
Politechniki Warszawskiej

Warszawa, dn. 12.12.2023 r.

Opinia o rozprawie 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"

Identyfikacja i minimalizacja zagrożeń w systemach wbudowanych przy eksploatacji samochodów zgodnie z założeniami koncepcji „Przemysł 4.0"

(Na zlecenie pani Przewodniczącej Rady Dyscypliny Inżynieria Mechaniczna prof. dr hab. inż. Ewy Majchrzak)

1. Wprowadzenie

Śmiało można stwierdzić, że przez ostatnie ćwierć wieku samochód z urządzenia mechanicznego sterowanego w zakresie wszystkich swoich funkcji przez człowieka stał się systemem mechatronicznym potencjalnie zdolnym do działania w trybie autonomicznym. Ewolucja przebiegająca niesłychani szybko nastąpiła w trzech etapach. W pierwszym dotyczącym głównie regulacji silnika i mechanizmów wspomagających automatyczne działanie układów mechanicznych, mechaniczno-hydraulicznych i mechaniczno-elektrycznych zostało zastąpione systemem sterującym działającym na podstawie obserwacji (pomiaru) aktualnych parametrów pracy i składu spalin (pomiar położenia wału korbowego, sonda λ itp.). Wprowadzenie systemów ABS i kontroli trakcji rozpoczęło drugi etap, którym jest kontrola działania zawierająca możliwości regulowania tego działania w warunkach, gdy zostanie ono uznane przez system za szkodliwe (niebezpieczne). Dotyczy to przebiegu hamowania, trybu zmiany biegów przez automatyczne skrzynie oraz pracy układów nazywanych przez producentów „asystentami" (asystent pasa ruchu, asystent parkowania, inteligentny tempomat itp.). Etap trzeci to możliwości kontaktowania się pojazdu z innymi obiektami infrastruktury drogowej, systemem GPS, czy wreszcie innymi pojazdami. Można już wyobrazić sobie decyzję „zbiorową" podjętą przez „n" pojazdów w celu optymalizacji ruchu i nie jest to science fiction. Jednak nawet ograniczenie kontaktu między obiektami do przesyłu informacji może stać się niesłychanie niebezpieczne w przypadku możliwości zakłócenia/zafałszowania tego przepływu.

Każdy układ autonomicznej regulacji może doznać awarii i zadziałać w sposób niebezpieczny bądź szkodliwy, lecz układ cyfrowego sterowania zwłaszcza wykorzystujący Internet Rzeczy i koncepcję Przemysł 4,0 jest bezustannie narażony na zagrożenia cyberatakami pozwalającymi na kradzież danych, dezorganizację pracy systemu, czy przejęcie kontroli nad systemem, co w efekcie

doprowadzić może do użycia pojazdu niezgodnie z jego przeznaczeniem, a w konsekwencji do zagrożenia zdrowia i życia kierowcy.

Ponieważ rozwój koncepcji inteligentnych autonomicznych pojazdów bardzo przyspiesza problem walki z wymienionymi zagrożeniami może stać się niedługo niezwykle aktualny. Autor rozprawy podjął się zadania zwrócenia uwagi na ten problem na drodze eksperymentalnego wykazania zagrożeń i zaproponowania metod i kierunków przeciwdziałań.

Uważam tematykę rozprawy za aktualną, a sam problem za wybitnie istotny.

2. Omówienie rozprawy

Przedstawiona do oceny praca liczy 119 stron tekstu i uzupełniona jest wykazem skrótów, rysunków i tablic oraz krótkimi streszczeniami w języku polskim i angielskim.

Całość rozprawy napisana jest w języku angielskim. Bibliografia zawiera 73 pozycje (w tym 5 autorskich i współautorskich doktoranta). Wybór literatury należy uznać za aktualny i prawidłowy.

Praca została podzielona na 4 rozdziały o nierównej długości. Rozdział 1 definiuje zwięźle cel rozprawy, którym jest identyfikacja potencjalnych zagrożeń poprawnej pracy wbudowanych systemów sterujących stosowanych w przemyśle motoryzacyjnym oraz opracowanie propozycji przeciwdziałania tym zagrożeniom. Realizację tych celów Autor widzi jako przeprowadzenie serii eksperymentów wskazujących na możliwość kradzieży informacji i destabilizacji (przejęcia kontroli) systemu oraz weryfikujących zaproponowane rozwiązania zabezpieczające. Rozpisane w 11 punktach zadania szczegółowe są de facto równoważne z postawieniem tezy, że współczesne pojazdy są narażone na poważne zagrożenia funkcjonalne spowodowane między innymi przez cyberatak, że zagrożenie to szybko wzrasta oraz że możliwe i celowe jest stosowanie właściwych zabezpieczeń.

W rozdziale 2 Autor zajmuje się aktualnym stanem wiedzy i szczegółowo przedstawia współczesny samochód jako złożony system mechatroniczny, potencjalne ryzyka na jakie narażone są układy pojazdu oraz stosowane zabezpieczenia przed cyberatakiem. Ostatni punkt rozdziału dotyczy krótkiego omówienia zastosowania sztucznej inteligencji w organizacji ruchu drogowego z uwzględnieniem koncepcji autoenkodera jako sposobu na wykrycie anomalii mogącej świadczyć o cyberataku.

Kluczowym dla pracy jest rozdział 3, w którym Autor opisuje wykonane przez siebie 4 eksperymenty badawcze. Celem ich było po pierwsze zbadanie możliwości podsłuchu, zakłócenia i zmiany zawartości ramek podczas transmisji danych magistralą CAN. Po drugie zaproponowanie

rozwiązania zwiększającego poziom bezpieczeństwa i po trzecie sprawdzenie skuteczności proponowanych zabezpieczeń. Poszczególne eksperymenty dotyczyły:

1. Przejęcia kontroli nad elektronicznymi modułami sterującymi odpowiedzialnymi za oświetlenie wewnątrz pojazdu.
2. Równoległego odczytu wartości diagnostycznych oraz podmiany sygnałów sterujących (zmieniono sygnał sterujący hamulca w sposób niezauważalny przez samochód).
3. Zakłóceń działania kierunkowskazu przez zamaskowanie sygnału w taki sposób, że kierowca widzi wskaźnik informujący go o aktywności kierunkowskazu podczas, gdy on nie działa.
4. Przejęcia kontroli nad układem kierowniczym i sprawdzenie czy przy wykorzystaniu sztucznej inteligencji możliwe jest wykrycie anomalii świadczących o cyberataku.

W każdym przypadku Autor zaproponował sposób przeciwdziałania atakowi. Wyraźnie zwrócił uwagę na metody niskokosztowe (szyfrowanie) i złożone, wykorzystujące głębokie sieci neuronowe.

Rozdział 4 to krótkie podsumowanie , w którym Autor podkreśla dwa wymienione podejścia do zagadnienia poprawy bezpieczeństwa. Zwraca uwagę na aplikacyjność proponowanych rozwiązań i podkreśla znaczenie wyników rozprawy w koncepcji Przemysł 4,0.

3. Uwagi krytyczne i zapytania

Praca wykonana jest na tyle starannie pod względem koncepcyjnym i edycyjnym, że wywody Autora nie budzą istotnych wątpliwości. Kierując się pewnym uczuciem niedosytu można by zadać oczywiście pytanie, czym kierował się Autor przy wyborze systemów, na których przeprowadzono eksperymenty? Interesują mnie również kryteria rozróżniania układów, dla których wystarczą rozwiązania niskokosztowe, a dla których nie. Spotykana w literaturze klasyfikacja zagrożeń jest bowiem co najmniej kontrowersyjna. Istnieją w ruchu drogowym sytuacje, gdy brak kierunkowskazu niesie poważniejsze konsekwencje, niż zakłócenie pracy układu kierowniczego.

Znakomita redakcja rozprawy nie zmienia faktu, że otrzymany przeze mnie egzemplarz miał nienumerowane strony (!).

Ocena końcowa

W moim przekonaniu praca pod względem wyboru tematu i jego realizacji nie wzbudza zastrzeżeń. Autor w pełni zrealizował postawione cele, wykorzystując przy tym wiedzę z zakresu szerokorozumianej mechatroniki oraz wykazał się umiejętnością zaprojektowania i realizacji złożonych eksperymentów badawczych. Rezultaty rozprawy mają niewątpliwie istotny potencjał aplikacyjny i tworzą bazę do dalszych działań w podjętej tematyce.

Całość rozprawy oceniam jednoznacznie pozytywnie.

Konkluzja

Uważam, że przedstawiona do oceny praca spełnia wymagania Ustawy z dnia 20 lipca 2018 r. „Prawo o Szkolnictwie Wyższym i Nauce" w dyscyplinie Inżynieria Mechaniczna i wnioskuję do Rady Dyscypliny Inżynieria Mechaniczna Politechniki Śląskiej o dopuszczenie Pana mgr. inż. Marcina Gajdzika do publicznej obrony.

Wnioskuję również o wyróżnienie pracy za nowatorstwo podjętej tematyki i wysoki poziom naukowy.