dr hab. inż. Marcin Śliwiński, prof. PG
Katedra Automatyki
Wydział Elektrotechniki i Automatyki
Politechnika Gdańska
ul. G. Narutowicza 11/12
80-233 Gdańsk

Gdańsk, dnia 12 I 2025 r.

Recenzja rozprawy doktorskiej
mgra inż. Piotra Piątka

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

1. Podstawa recenzji

Recenzja została przygotowana w odpowiedzi na uchwałę Rady Dyscypliny Naukowej Automatyka, Elektronika, Elektrotechnika i Technologie Kosmiczne Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie z dn. 7 listopada 2024 r. w sprawie powołania recenzentów rozprawy doktorskiej Pana mgr. inż. Piotra Piątka pt. *„Systemowa analiza bezpieczeństwa układów sterowania w pojazdach o wysokim stopniu automatyzacji jazdy"*, przekazaną przez Przewodniczącego Rady Dyscypliny Automatyka, Elektronika, Elektrotechnika i Technologie Kosmiczne AGH dr. hab. inż. Ryszarda Srokę, prof. AGH, pismem z dnia 8 listopada 2024 r. (pismo RD AEEiTK/510-9-3/24).

Promotorem rozprawy doktorskiej jest Pan dr hab. inż. Paweł Skruch, prof. AGH, a promotorem pomocniczym jest Pan dr inż. Szczepan Moskwa.

2. Ocena aktualności tematu, celu i zakresu rozprawy

Rozprawa doktorska Pana mgr. inż. Piotra Piątka przedstawia praktyczne zastosowanie koncepcji bezpieczeństwa funkcjonalnego oraz cyberbezpieczeństwa w analizie rozwiązań systemów sterowania w pojazdach o wysokim stopniu autonomiczności. Problematyka bezpieczeństwa funkcjonalnego realizowana w oparciu o systemy automatyki zabezpieczeniowej, a w szczególności elektryczne, elektroniczne i programowalne elektroniczne związana jest z normą ogólną IEC 61508. Recenzowana rozprawa doktorska stanowi istotny wkład w rozwój wiedzy w obszarze autonomicznych pojazdów, szczególnie w kontekście integracji analiz bezpieczeństwa funkcjonalnego oraz cyberbezpieczeństwa. W obliczu rosnącej złożoności systemów autonomicznych, a zwłaszcza w branży motoryzacyjnej, opracowanie kompleksowej metodyki oceny bezpieczeństwa, która uwzględnia zarówno aspekty techniczne, jak i zagrożenia cybernetyczne, jest niezwykle istotnym wyzwaniem. Praca doktorska skupia się na zintegrowanym podejściu w analizach bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa, z odniesieniem do międzynarodowych standardów normatywnych, takich jak ISO 26262, ISO 21434 oraz ISO 21448.

Norma ISO 26262 dotycząca bezpieczeństwa funkcjonalnego systemów elektronicznych w pojazdach stanowi podstawowy punkt odniesienia dla identyfikacji i oceny ryzyka związanego z bezpieczeństwem

pojazdów autonomicznych. Z kolei standard ISO 21434 koncentruje się na cyberbezpieczeństwie w motoryzacji, ustanawiając zasady ochrony przed zagrożeniami wynikającymi z ataków poprzez sieci komputerowe, które mogą mieć poważne konsekwencje dla bezpieczeństwa pojazdu i jego użytkowników. Natomiast norma ISO 21448, uzupełnia dwa powyższe standardy, zapewniając wytyczne w zakresie minimalizowania ryzyka związanego z błędami systemów oraz nieoczekiwanymi awariami w kontekście niezawodności układów autonomicznych.

Praca doktorska wykazuje głęboką znajomość powyższych standardów oraz ich zastosowania w kontekście nowoczesnych pojazdów autonomicznych, wskazując na konieczność zintegrowanego podejścia do analizy zagrożeń, które uwzględnia zarówno aspekty techniczne, jak i cybernetyczne. Doktorant przeprowadza szczegółową analizę ryzyka, posługując się zaawansowanymi metodami oceny poziomów nienaruszalności bezpieczeństwa ASIL (ang. *Automotive Safety Integrity Level*) i uzasadnionej ochrony CAL (ang. *Cybersecurity Assurance Level*) oraz proponuje narzędzia umożliwiające skuteczną weryfikację i walidację wymagań związanych z bezpieczeństwem funkcjonalnym i cyberbezpieczeństwem. W pracy uwzględniono również wytyczne normatywne, które stanowią fundament do dalszego rozwoju systemów autonomicznych, ze szczególnym uwzględnieniem ich bezpieczeństwa w kontekście realnych zagrożeń.

Niniejsza rozprawa zasługuje na szczególną uwagę w kontekście dynamicznego rozwoju technologii autonomicznych pojazdów, w których bezpieczeństwo (zarówno funkcjonalne, jak i cybernetyczne) odgrywa kluczową rolę. Celem pracy jest nie tylko zaproponowanie kompleksowego podejścia do oceny i zarządzania ryzykiem, ale także wniesienie istotnego wkładu w kierunku projektowania nowoczesnych i bezpiecznych systemów, które będą stanowiły fundament przyszłości transportu autonomicznego.

Uwzględniając powyższe, uważam, ze tematyka poruszana w pracy jest aktualna i ma potencjalne znaczenie praktyczne.

Podstawowym celem rozprawy doktorskiej Pana mgra inż. Piotra Piątka było **opracowanie praktycznego i możliwego do wdrożenia podejścia do projektowania i wdrażania zaawansowanych systemów sterowania w wysoce zautomatyzowanych pojazdach, mającego na celu poprawę niezawodności systemu, wspieranie synergii między zespołami programistycznymi, minimalizację powielania wysiłków i przyspieszenie ogólnego rozwoju**. Zdaniem autora cel ten stanowił odpowiedź na pilną potrzebę synergii między bezpieczeństwem funkcjonalnym a cyberbezpieczeństwem w dynamicznym przemyśle motoryzacyjnym i został osiągnięty poprzez opracowanie procesu CyberSafety (CySa).

Kolejnym celem pracy było **zaproponowanie referencyjnego modelu projektowania organizacyjnego i metodologii technicznej dostosowanej do zastosowania w działach badawczo-rozwojowych firm motoryzacyjnych, koncentrującej się na zaawansowanych systemach sterowania w wysoce zautomatyzowanych pojazdach, integrującej bezpieczeństwo i ochronę w całym procesie rozwoju oraz usprawniającej współpracę i komunikację w zespołach**. Propozycja modelu organizacyjnego została zweryfikowana poprzez jego zastosowanie w analizie rzeczywistego systemu ADAS (tj. Highway Pilot HP). Zaproponowana metodyka może zostać zaimplementowana w aplikacjach wspomagających zarządzanie bezpieczeństwem funkcjonalnym i cyberbezpieczeństwem w cyklu życia zaawansowanych systemów sterowania.

Uważam, że cele pracy są istotne i spełniają wymagania stawiane rozprawom doktorskim.

Główne tezy pracy zostały sformułowane w sposób jawny w podrozdziale 1.2 i brzmią 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."

„Opracowanie nowatorskiego modelu rozwoju, który wyposaża firmy w kompleksowe narzędzi i metodologie do efektywnego zarządzania skomplikowanym projektowaniem złożonych systemów wbudowanych o wysokiej autonomii, przy jednoczesnej integracji bezpieczeństwa i ochrony w całym procesie, znacznie poprawi niezawodność systemu, skróci czas opracowywania i zwiększy ogólne bezpieczeństwo i ochronę pojazdu."

Tezy rozprawy są poprawne i odpowiednio sformułowane.

Aby udowodnić postawione tezy pracy, przyjęto i zrealizowano następujące zadania:

a. dokonano szczegółowego przeglądu literatury, dokumentów normatywnych oraz opracowań technicznych z zakresu bezpieczeństwa, bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa systemów motoryzacyjnych;
b. dokonano krytycznej analizy istniejących metodologii i procesów analitycznych w dziedzinie bezpieczeństwa, bezpieczeństwa funkcjonalnego, cyberbezpieczeństwa i systemów motoryzacyjnych;
c. opracowano proces CyberSafety (*CySa*) z wykorzystaniem narzędzia programowego Bizagi Modeler;
d. dokonano porównania wyników symulacji w zakresie czasu trwania procesu projektowego, liczby wykrytych oraz wyeliminowanych błędów, a także osiągniętego poziomu nienaruszalności bezpieczeństwa ASIL oraz poziomu cyberbezpieczeństwa CAL;
e. zaproponowano wskaźniki KPI (ang. *Key Performance Indicators*) do oceny skuteczności procesu;
f. zaproponowano ważony spółczynnik bezpieczeństwa WSS (ang. *Weighted Safety Score*) do oceny efektywności procesów integracji bezpieczeństwa funkcjonalnego (*FuSa*) i cyberbezpieczeństwa (*CySe*) w projektowaniu systemów złożonych, z uwzględnieniem różnych aspektów bezpieczeństwa i ochrony w zintegrowanym podejściu, co pozwala na bardziej kompleksową i dokładną ocenę projektowanych systemów;
g. przeprowadzono empiryczne badania na przykładzie zaawansowanego systemu wspomagania kierowcy ADAS (ang. *Advanced Driver Assistance Systems*) Highway Pilot HP poprzez zademonstrowanie praktycznych korzyści wynikających z wczesnej integracji bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa w procesie projektowym;
h. dokonano weryfikacji zaproponowanego modelu procesu CyberSafety na przykładzie analizy funkcji bezpieczeństwa realizowanych przez system Highway Pilot (HP) z wykorzystaniem pakietu Ansys Medini;
i. dokonano identyfikacji oraz analizy potencjalnych zagrożeń w procesie projektowania i eksploatacji systemu Highway Pilot (HP);

j. przeprowadzono symulację skutków zagrożeń w zintegrowanym podejściu oraz wykazano zmniejszenie ryzyka w wyniku stosowania zaproponowanego modelu procesu;

k. w badaniach wykorzystano wieloaspektowe podejście, poprzez przeprowadzenie analiz: drzew niezdatności FTA (ang. *Fault Tree Analysis*) i ataków ATA (ang. *Attack Tree Analysis*) oraz zagrożeń i oceny ryzyka w tym: TARA (ang. *Threat Analysis and Risk Assessment*), HARA (ang. *Hazard Analysis and Risk Assessment*) i HIRE (ang. *Hazard Identification and Risk Evaluation*), a także rodzajów skutków i krytyczności uszkodzeń FMECA (FMEDA) (ang. Failure Mode Effect and Criticality Analysis) oraz SOTIF;

l. dokonano weryfikacji wpływu zintegrowanego podejścia na jakość, niezawodność oraz czas procesu projektowania systemu ADAS (na przykładzie Highway Pilot HP).

3. Charakterystyka rozprawy doktorskiej

Recenzowana rozprawa doktorska liczy 307 stron. Praca zawiera 5 głównych rozdziałów, w tym spis literatury obejmujący 131 pozycji. Stronicowaną częścią rozprawy są także: streszczenia w języku polskim i angielskim, spis treści oraz dwa załączniki (pierwszy bardzo obszerny), do których wielokrotne odwołania można znaleźć w zasadniczej części rozprawy.

Pierwszy rozdział stanowi wprowadzenie do podjętego tematu. W rozdziale tym zawarto cele, jak również tezy pracy. Uzupełnieniem rozdziału pierwszego stanowi przedstawienie struktury recenzowanej rozprawy doktorskiej.

Drugi rozdział zawiera obszerny przegląd literatury i aktualnych najnowszych technologii motoryzacyjnych, przygotowując grunt pod prowadzenie badań. W rozdziale tym autor przedstawił metodologię badań opierającą się na krytycznej analizie istniejących podejść i procesów analitycznych w dziedzinie bezpieczeństwa, cyberbezpieczeństwa i systemów motoryzacyjnych. Skupił się także na kluczowej terminologii, identyfikując błędy, wady oraz kwestie związane z obecnymi metodami, zarówno w literaturze naukowej, jak i raportach branżowych. Odnosząc się do literatury, doktorant szczególny nacisk położył na publikacje z renomowanych naukowych baz danych i bibliotek badawczych, takich jak Scopus i IEEE Xplore, dostarczających aktualnych i zweryfikowanych informacji. Przeprowadzając analizę raportów branżowych zdefiniował najnowsze trendy, wyzwania oraz innowacyjne rozwiązania w zakresie bezpieczeństwa i cyberbezpieczeństwa w sektorze motoryzacyjnym. Przedstawione przez autora analizy stanowią podstawę dla całej rozprawy, umożliwiając zaproponowanie innowacyjnych rozwiązań dostosowanych do aktualnych oczekiwań branży motoryzacyjnej wraz z opracowaniem i wprowadzeniem na rynek nowego złożonego produktu pod względem metodyki projektowej jak i rozwiązań technicznych.

Trzeci rozdział rozprawy przedstawia opracowane ramy procesu CyberSafety. W tej części autor rozprawy skoncentrował się na strategicznym badaniu narzędzi do analizy ryzyka i modelowania procesów, dostosowując ich wybór do rozwiązań stosowanych w przemyśle motoryzacyjnym w celu zwiększenia ich praktycznego zastosowania. Autor wykorzystując *Business Process Model and Notation* (BPMN) i *Systems Modeling Language* (SysML) jako języki modelowania, zoptymalizował złożone procesy projektowe w celu poprawy jakości i bezpieczeństwa systemów motoryzacyjnych. Wykorzystał w tym celu wieloaspektowy proces gromadzenia danych bazując na standardach branżowych, wytycznych i odpowiednich studiach przypadków, aby zapewnić kompleksowy wgląd w bezpieczeństwo i inżynierię systemów w branży motoryzacyjnej.

Czwarty rozdział rozprawy zawiera ocenę proponowanych ram projektowania i rozwoju w kontekście aktywnych systemów bezpieczeństwa ADAS. W celu walidacji i udoskonalenia proponowanego modelu procesu organizacyjnego przedstawionego w rozdziale trzecim, przeprowadzono dogłębne badanie funkcji systemu ADAS, w szczególności modelu systemu Highway Pilot (HP) dostarczonego przez AnsysMedini. Autor rozprawy wykorzystał ten model jako praktyczny punkt odniesienia w procesie weryfikacji zaproponowanych ram projektowania, a także do oceny możliwości zastosowania i skuteczności proponowanej metodyki.

Piąty rozdział zawiera podsumowanie rozprawy poprzez prezentację wniosków ilustrujących główny wkład i wnioski uzyskane na podstawie przeprowadzonych badań a także zawiera rozważania dotyczące przyszłych ulepszeń proponowanych rozwiązań i wdrożonych aspektów metodycznych.

Integralną częścią recenzowanej rozprawy doktorskiej Pana mgra inż. Piotra Piątka są dwa załączniki:

Załącznik A zawiera kompletny eksport schematu zaprojektowanego procesu CyberSafety z środowiska Bizagi zapewniający szczegółowy wgląd w jego strukturę oraz komponenty.

Załącznik B zawiera analizę cyberbezpieczeństwa struktury funkcjonalnej systemu (ADAS) Highway Pilot HP, wykonaną w oprogramowaniu AnsysMedini.

Za najważniejsze w rozprawie doktorskiej uważam rozdziały: trzeci oraz czwarty, które zawierają koncepcję opracowanej metodyki jej weryfikację oraz wyniki autorskich badań doktoranta.

4. Główne osiągnięcia rozprawy

Do najważniejszych osiągnięć naukowo-badawczych doktoranta zaliczam:

- przeprowadzenie bardzo starannego przeglądu literaturowego dotyczącego problematyki bezpieczeństwa funkcjonalnego oraz cyberbezpieczeństwa na przykładach rozwoju nowych produktów w sektorze motoryzacyjnym;
- przedstawienie kierunku rozwoju architektury systemów sterowania autonomicznych pojazdów w kontekście zapewnienia cyberbezpieczeństwa;
- zaprezentowanie metod zarządzania projektami w procesie projektowania i rozwoju złożonych systemów na przykładzie zaawansowanego systemu wspomagania kierowcy ADAS (ang. *Advanced Driver Assistance Systems*);
- określenie kierunku rozwoju metod zarządzania w projektowaniu złożonych systemów z sektora motoryzacyjnego;
- propozycja zintegrowanego modelu rozwoju systemów cyberfizycznych o wysokiej niezawodności;
- projekt procesu zintegrowanego podejścia w przeprowadzaniu analiz bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa systemów ADAS z wykorzystaniem nowych ram w metodyce projektowania modułów sterowania elektronicznego;
- wdrożenie zaprojektowanego procesu CyberSafety w organiacji z wykorzystaniem narzędzia programowego Bizagi Modeler (Bizagi – CyberSafety Framework);
- wykorzystanie ważony spółczynnik bezpieczeństwa WSS (ang. *Weighted Safety Score*) do oceny efektywności procesów integracji bezpieczeństwa funkcjonalnego (FuSa)

i cyberbezpieczeństwa (CySe) w projektowaniu złożonych systemów sterowania z uwzględnieniem różnych aspektów bezpieczeństwa i ochrony w zintegrowanym podejściu;

- wprowadzenie wskaźników oceny procesu KPI;
- zdefiniowanie oraz wykorzystanie w badaniach dziewięciu wskaźników oceny procesu KPI (ang. *Key Performance Indicators*) tj.: wskaźnik identyfikacji ryzyka bezpieczeństwa i ochrony SSRIR (ang. *Security and Safety Risk Identification*); wskaźnik pokrycia oceny ryzyka RAC (ang. *Risk Assessment Coverage*); skuteczność przeglądu projektu DRE (ang. *Design Review Effectivenes*); kompletność strategii łagodzenia skutków MCS (ang. *Mitigation Strategy Completeness*); wskaźnik zgodności projektu DCR (ang. *Design Compilance Rate*); poziom ryzyka rezydualnego RRL (ang. *Residual Risk Level*); Pokrycie wymagań bezpieczeństwa I ochrony SSRC (ang. *Security and Safety Requirement Coverage*); wskaźnik złożoności projektu DCI (ang. Design Complexity Index); wskaźnik wniosków o zmianę projektu DCRR (ang. *Design Change Request Rate*);
- wykonanie studium przypadku zintegrowanej analizy bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa zaawansowanego systemu wspomagania kierowcy ADAS (Highway Pilot HP) z użyciem gotowego modelu w oprogramowaniu Ansys Medini (Medini Analyze – CyberSafety Analysis Highway Pilot);
- zaproponowanie modelu oceny systemów aktywnego bezpieczeństwa opartego na zdefiniowanych wskaźnikach celem weryfikacji wdrożonego procesu CyberSafety.

Doktorant w stopniu biegłym opanował tematykę rozprawy w warstwie nie tylko teoretycznej, ale także praktycznej, w oparciu o dobre rozeznanie problemów technologicznych i naukowych związanych z integracją analiz bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa zaawansowanych i złożonych systemów sterowania w sektorze motoryzacyjnym. W opinii recenzenta przyjęte przez autora pracy tezy rozprawy zostały udowodnione, a zaproponowana przez doktoranta systemowa analiza bezpieczeństwa układów sterowania w pojazdach o wysokim stopniu automatyzacji jazdy na przykładzie zaprojektowanego procesu CyberSafety może zostać zaimplementowana w aplikacjach wspomagających projektowanie systemów autonomicznych oraz zarządzanie bezpieczeństwem funkcjonalnym i cyberbezpieczeństwem.

Przedmiotowa rozprawa doktorska Pana mgra inż. Piotra Piątka stanowi istotny wkład w rozwój wiedzy w obszarze autonomicznych pojazdów, szczególnie w kontekście integracji analiz bezpieczeństwa funkcjonalnego oraz cyberbezpieczeństwa. W obliczu rosnącej złożoności systemów autonomicznych, szczególnie w branży motoryzacyjnej, opracowanie kompleksowej metodyki oceny bezpieczeństwa, która uwzględnia zarówno aspekty techniczne, jak i zagrożenia cybernetyczne, jest niezwykle istotnym wyzwaniem.

Stwierdzam, doktorant dysponuje wymaganym do prowadzenia badań naukowych zasobem wiedzy w zakresie dyscypliny naukowej Automatyka, Elektronika, Elektrotechnika i Technologie Kosmiczne.

5. Ocena poziomu edytorskiego rozprawy

Podział treści rozprawy jest logiczny i uporządkowany. Przedstawiona do recenzji rozprawa została napisana w języku angielskim. Styl i poziom językowy nie budzi większych zastrzeżeń. Szata graficzna jest dość staranna i dopracowana. Praca została zredagowana stylistycznie poprawnie. Wywody

matematyczne, objaśnienia wzorów i wyników graficznych zostały przedstawione czytelnie. Sposób przekazywania treści jest poprawny i wystarczający.

Zagadnienia prezentowane w pracy tworzą tematycznie merytoryczną spójność i nie wymagają zmian. Ujęcie graficzne rysunków i wykresów uważam za wystarczające. Czytając rozprawę doktorską odnosi się wrażenie o wysokiej kompetencji merytorycznej autora, który potrafi przedstawić wyniki swoich badań w dość przyjazny i czytelny dla odbiorcy sposób.

Wszystkie pozycje literaturowe zamieszone w bibliografii mają swoje odniesienie w treści recenzowanej pracy. Rozprawa jest zdaniem recenzenta zbyt obszerna, zajmuje 307 stron (a dokładnie 316 stron uwzględniając stronę tytułową, abstrakt, streszczenie, spis treści oraz wykaz akronimów) maszynopisu z czego 120 zajmują załączniki. W rozprawie można też odnaleźć nieliczne błędy literowe, interpunkcyjne, czy edycyjne, wśród których można wymienić:

- strona 58 - nie wszystkie opisy na rysunku 3.2 (A high level view of CyberSafety Framework ...) są czytelne;
- strona 64 - część opisów wewnątrz bloków z rysunku 3.9 (Example design work flow for CySe activities) jest nieczytelnych;
- strona 113 - rysunek 4.3 (CyberSafety Analysis HP – Item Architecture) jest nieczytelny podobna kwestia dotyczy kolejnego rysunku 4 .4 (str. 114);
- strona 114 - rysunek 4.4 (CyberSafety Analysis HP – Item Functions ....) jest nieczytelny;
- strona 123 - rysunki przedstawiające drzewa niezdatności (drzewa ataku) FTA tj.: 4.15 (CyberSafety Analysis HP – Denial of Service of Object List Attack Tree) oraz 4.16 CyberSafety Analysis HP – Denial of Service of EmeBrk Attack Tree) są zbyt małe i całkowicie nieczytelne;
- strona 124 - rysunek 4.17 (CyberSafety Analysis HP-FTA for [SG1} – CyberSafety Analysis Highway Pilot) przedstawiający analizę FTA w kontekście analizy cyberbezpieczeństwo systemu ADAS na przykładzie układu pilota autostradowego HP jest nieczytelny;
- strona 125 - rysunek 4.17 (CyberSafety Analysis HP – Denial of Service of EmeBrk Attack Tree – IDS Disabled) jest zbyt mały i całkowicie nieczytelny;
- strona 129 – rysunek 4.23. (CyberSafety Analysis HP – Requirement Diagram for CSG1) jest nieczytelny;
- strona 131 - napisy zamieszczone wewnątrz rysunku 4.26 (CyberSafety Analysis HP – Safety and Security Mechanisms) są zbyt małe i nieczytelne;
- strony 297-307 - przedstawiony wykaz bibliografii (str. 297-307) nie jest uporządkowany w sposób alfabetyczny, co z reguły czyni się w rozprawach doktorskich;
- w spisie treści rozprawy zawarte są rozdziały i podrozdziały. Nie uwzględniono natomiast podpodrozdziałów, (np.: 2.4.1. Distributed Approach (str. 32); 2.4.2. Domain Based Approach (str. 33); Zone Based Appoach oraz 2.4.4. Centralised Based Approach (str. 34); 2.5.1. Vehicle Cybersecurity Threats and Challenges (str. 36); 2.7.1. Systems Modeling (str. 46); 2.7.2. Model-Based Systems Engineering (str. 47); 2.8.1. Key Elements of the Lean Process (str. 50); 2.8.2. Revelance in Complex Systems Design (str. 52); 3.1.1. Introduction – Analysis Coordination (str. 57); 3.1.2. Project Preparation Phase (str. 62); 3.1.4. Design Phase (str. 75); 3.1.5. Implementation Phase (str. 82); 3.1.6. Verificationa Phase (str. 84); 3.1.7. Validation Phase (str.

86); 3.1.8. Release Phase (str. 88); 3.1.9. Maintenance Phase (str. 90); 3.1.10. Decommissioning Phase oraz 3.1.11. Summary (str. 98); 4.2.1. Cybrsecurity Impact on Safety (str. 134); 4.2.2. Attack Analysis HP System Attack Analysis (str. 135); 4.2.3. Risk Mitigation Analysis (str. 147); 4.2.5. Proposal of the Weighted Safety Score (str. 150); 4.2.6. Highway Pilot Weighted Safety Score Evaluation (str. 156); 4.3.1. CyberSafety Process Indicators Evaluation (str. 160)), które zdaniem recenzenta powinny się wraz ze stosowną numeracją znaleźć w spisie treści.

Pragnę zaznaczyć, że zawarte w recenzji drobne uwagi i zastrzeżenia edytorskie nie wpływają w żaden sposób na wartość merytoryczną przedłożonej rozprawy doktorskiej.

6. Uwagi merytoryczne i pytania dyskusyjne

W części teoretycznej doktorant dokonał bardzo szczegółowego i obszernego przeglądu literatury oraz aspektów wytycznych projektowych wg najnowszych norm dla przemysłu motoryzacyjnego z zakresu bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa. W części praktycznej tj. wdrożeniowej zaproponował proces CyberSafety (CySa) integrujący najważniejsze wytyczne trzech norm: ISO 26262 (IEC 61508), ISO/IEC 21448 oraz ISO/SAE 21434. Można powiedzieć, że autor rozprawy Pan mgr inż. Piotr Piątek przygotował pewne „podwaliny" do nowego standardu stanowiącego zintegrowane podejście w analizach bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa. W kontekście zintegrowanego podejścia do analiz bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa w przemyśle motoryzacyjnym, zaproponował wykorzystanie ważonego współczynnika bezpieczeństwa (WSS), który stanowi narzędzie do oceny całkowitego poziomu ryzyka, z uwzględnieniem zarówno aspektów związanych z awariami systemów sterowania (bezpieczeństwo funkcjonalne), jak i potencjalnymi zagrożeniami związanymi z atakami cybernetycznymi. W takim podejściu, zarówno bezpieczeństwo funkcjonalne, jak i cyberbezpieczeństwo muszą być traktowane jako komplementarne, a nie niezależne elementy systemu, aby uzyskać pełną ocenę ryzyka i skutecznie zarządzać bezpieczeństwem systemów w pojazdach autonomicznych i zaawansowanych systemach wspomagania kierowcy (ADAS).

Zintegrowane podejście w analizach bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa w przemyśle motoryzacyjnym oznacza konieczność współdziałania dwóch kluczowych obszarów. Bezpieczeństwa funkcjonalnego, które odnosi się do zdolności systemu do zapobiegania uszkodzeniom lub zagrożeniom dla zdrowia i życia użytkownika pojazdu w wyniku awarii systemów elektronicznych i mechanicznych. Dotyczy to standardów takich jak ISO 26262 (dla funkcji bezpieczeństwa w systemach elektronicznych pojazdów) oraz IEC 61508 (dla systemów automatyki i sterowania). Cyberbezpieczeństwo zajmuje się ochroną systemów przed atakami, które mogą zmienić ich funkcjonowanie, w tym atakami na systemy komunikacyjne, pojazdy autonomiczne i inne elementy elektroniczne w pojeździe. Obejmuje normy takie jak ISO 21434 (dotyczące cyberbezpieczeństwa w motoryzacji) oraz ISO 21448 (dotyczące bezpieczeństwa operacyjnego w kontekście pojazdów autonomicznych). W przypadku zintegrowanego podejścia do oceny bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa w systemach motoryzacyjnych, ważony współczynnik bezpieczeństwa (WSS) jest wykorzystywany do oceny ryzyka, uwzględniając zarówno: ryzyko związane z awarią systemu (np. uszkodzenie czujników, błąd algorytmu sterowania), które może prowadzić do wypadków lub niebezpiecznych sytuacji oraz ryzyko związane z atakami cybernetycznymi, które mogą wpłynąć na

integralność, dostępność i poufność danych w systemach sterowania pojazdu, a także kontrolować fizyczne funkcje pojazdu (np. przejęcie kontroli nad kierowaniem, przyspieszaniem czy hamowaniem).

Autor rozprawy udowodnił skuteczność zaproponowanego procesu zintegrowanego podejścia w analizach bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa wykonując szczegółową analizę systemu ADAS na przykładzie układu autopilota (Highway Pilot HP) z wykorzystaniem oprogramowania AnsysMedini. Uzyskano wyniki świadczące o podniesieniu wydajności przy projektowaniu zintegrowanym systemów ADAS w oparciu o proponowaną technologię. Uzyskane wskaźniki oceny procesu KPI dowiodły wzrost wydajności, oszczędność czasu zespołów projektowych oraz eliminację błędów projektowych w tym ukrytych błędów systematycznych, w odniesieniu do przypadku gdyby przeprowadzane poszczególne analizy odbywały się oddzielnie, każda według wytycznych konkretnych standardów tj.: ISO 26262 (IEC 61508), ISO/IEC 21448 oraz ISO/SAE 21434.

Warto podkreślić, że autor rozprawy posiada duży potencjał badawczy oraz długoletnie doświadczenie zawodowe (ponad dziesięcioletnie w branży motoryzacyjnej) związane z projektowaniem i wdrażaniem systemów ADAS. Proponowana przez autora rozprawy metodyka zintegrowanego podejścia w analizach bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa zdecydowanie większy nacisk kładzie na aspekty związane z cyberbezpieczeństwem niż na bezpieczeństwo funkcjonalne, które stanowi tło w rozważaniach doktoranta na łamach niniejszej rozprawy. Niemniej zdaniem recenzenta, przy zauważalnym braku równowagi, zaproponowana metodyka może być wykorzystana w firmach z branży motoryzacyjnej i przyczynić się do rozwoju technologii projektowania nowej generacji wpół autonomicznych i w pełni autonomicznych pojazdów przy użyciu możliwości oferowanych przez AI. Podobne dążenie do wykorzystania zmodyfikowanego zintegrowanego podejścia w analizach niezawodności, bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa będzie można w przyszłości zaadoptować w innych branżach tj. przemyśle: kolejowym, morskim, lotniczym oraz kosmicznym.

Biorąc pod uwagę kwestie poruszone w recenzowanej rozprawie nasuwają się pewne pytania z nią związane.

a. Czy dla rozpatrywanych funkcji bezpieczeństwa wykonywanych przez analizowany system ADAS (Highway Pilot HP) określono i zweryfikowano poziomy nienaruszalności bezpieczeństwa ASIL?
b. W jaki sposób weryfikowany jest poziom ASIL warstwy sprzętowej systemu ADAS realizującego funkcję lub funkcje bezpieczeństwa?
c. Czy dla rozpatrywanego systemu ADAS (Highway Pilot HP) określono i zweryfikowano poziomy uzasadnionej ochrony CAL?
d. Czy w rozpatrywanym systemie poziomy CAL mają wpływ na poziomy ASIL? Jeżeli mają to na jakim etapie (określenia wymagań, czy też ich weryfikacji)?
e. Jaka jest relacja poziomów ASIL wg ISO 26262 do poziomów SIL wg IEC 61508?
f. Jaka jest relacja poziomów CAL wg SAE/ISO 21414 do poziomów SAL wg ISO/IEC 62443?
g. Jaki wpływ na bezpieczeństwo funkcjonalne systemu ma proponowana metodyka zintegrowanego podejścia?
h. Czy w ramach rozprawy wykonano analizę FMEA, FMECA lub FMEDA dla układu ADAS (Highway Pilot HP), jeżeli tak to jakim celu?

i. Przedstawiona metodyka zintegrowanego podejścia główny nacisk kładzie na kwestię zagadnień cyberbezpieczeństwa. Bezpieczeństwo funkcjonalne stanowi w danym przypadku pewne tło z wypełnieniem podejścia SOTIF. Czy te aspekty tzn. bezpieczeństwa funkcjonalnego i cyberbezpieczeństwo nie powinny być równoważne w proponowanej metodyce?

7. Podsumowanie i wniosek końcowy

Przedstawiona rozprawa doktorska stanowi istotny wkład w rozwój zintegrowanego podejścia do analizy bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa w kontekście autonomicznych pojazdów. W pracy szczegółowo omówiono i zintegrowano kluczowe normy międzynarodowe, takie jak ISO 26262, ISO/SAE 21434 oraz ISO 21448, które stanowią fundamenty bezpieczeństwa w nowoczesnych systemach motoryzacyjnych.

Doktorant wykazał, że w obliczu rosnącej złożoności systemów autonomicznych pojazdów, istnieje pilna potrzeba integracji bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa. W tym kontekście, norma ISO 26262 dotycząca bezpieczeństwa funkcjonalnego została zaadoptowana do oceny i zarządzania ryzykiem w systemach E/E/PE, co pozwoliło na identyfikację i klasyfikację zagrożeń dla systemów sterowania pojazdami autonomicznymi. Podjęto również szczegółową analizę poziomów ASIL, wskazując na konieczność ich precyzyjnego określenia, zwłaszcza w przypadku funkcji krytycznych, takich jak autonomiczne hamowanie czy systemy wspomagania kierowcy.

Równocześnie, norma ISO/SAE 21434 dotycząca cyberbezpieczeństwa w motoryzacji była podstawą w opracowywaniu metodologii oceny ryzyka związanego z cyberzagrożeniami w procesie projektowania i eksploatacji pojazdów autonomicznych. Doktorant wskazał, że uwzględnienie zagrożeń wynikających z ataków cybernetycznych oraz ich wpływu na bezpieczeństwo funkcjonalne jest kluczowe w kontekście rosnącej liczby złożonych interakcji między systemami wewnętrznymi pojazdu a zewnętrznymi sieciami i urządzeniami. Zintegrowane podejście w analizie bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa, zaprezentowane w pracy, pozwala na skuteczną identyfikację ryzyka i wprowadzenie adekwatnych środków ochrony.

Dodatkowo, odniesienie do normy ISO 21448 dotyczącej bezpieczeństwa zamierzonej funkcjonalności (SOTIF) umożliwiło włączenie do analizy ryzyka związanego z niepełnym lub błędnym działaniem poprawnie zaprojektowanych systemów. W pracy podkreślono, że dla pojazdów autonomicznych konieczne jest rozważenie ograniczeń wynikających z trudnych do przewidzenia warunków rzeczywistych. Doktorant zaproponował metodykę weryfikacji i walidacji takich systemów w scenariuszach granicznych, w których może wystąpić niezamierzona utrata funkcji lub błędna reakcja systemu, co ma kluczowe znaczenie dla bezpieczeństwa użytkowników pojazdu.

Zintegrowana metodyka w analizach bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa zaprezentowana w pracy doktorskiej stanowi nowatorskie podejście do analizy i zarządzania bezpieczeństwem w autonomicznych pojazdach. Integracja analiz bezpieczeństwa funkcjonalnego, cyberbezpieczeństwa i bezpieczeństwa zamierzonej funkcjonalności SOTIF zapewnia kompleksową ochronę systemów autonomicznych. Praca ta wnosi istotny wkład w rozwój normatywnych ram dla projektowania bezpiecznych, niezawodnych i odpornych na cyberzagrożenia systemów motoryzacyjnych, stanowiąc ważny krok w kierunku zapewnienia bezpiecznej eksploatacji pojazdów autonomicznych w coraz bardziej złożonych i dynamicznych warunkach.

Przedstawioną do recenzji rozprawę należy zaliczyć do grupy prac interdyscyplinarnych o charakterze koncepcyjno-eksperymentalnym, które wymagają od autora dość znacznego nakładu czasowego w celu ich poprawnego zrealizowania. Ponadto wymagają one od badacza dużych umiejętności, w tym przypadku z co najmniej dwóch różnych dziedzin: nauk inżynieryjno-technicznych (dyscyplina automatyka, elektronika, elektrotechnika i technologie kosmiczne, a także dyscyplina informatyka techniczna i telekomunikacja) oraz nauk ścisłych i przyrodniczych (dyscyplina matematyka). W opinii recenzenta doktorant posiadł umiejętność planowania eksperymentu naukowobadawczego oraz realizacji opracowanych przez siebie metod i procesów na obiekcie eksploatowanym w warunkach rzeczywistych. W dobrym stopniu doktorant opanował także technologię przygotowania materiału badawczego i technicznego przeprowadzonych prac analitycznych. Wykazał się także umiejętnością oceny wyników otrzymanych badań. Doktorant udowodnił, iż ma niezbędne kwalifikacje do prowadzenia badań naukowych oraz rozwiązał w sposób oryginalny zagadnienie naukowe będące tematem rozprawy.

Rozwiązanie problemu postawionego w rozprawie jest ciekawe nie tylko z naukowo poznawczego punktu widzenia, lecz przede wszystkim z tego, że zaproponowana w pracy metodyka zintegrowanego podejścia w przeprowadzaniu analiz bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa układów sterowania w pojazdach o wysokim stopniu automatyzacji jazdy może zostać, a zdaniem recenzenta zapewne zostanie w przyszłości zaimplementowana w aplikacjach wspomagających zintegrowane zarządzanie bezpieczeństwem funkcjonalnym i cyberbezpieczeństwem w przemyśle motoryzacyjnym. Praca zawiera elementy nowości w sensie naukowym stanowiące udokumentowany dorobek własny doktoranta.

Stwierdzam, że opiniowana praca jest kompletna i nie wymaga zmian ani uzupełnień. W mojej opinii spełnia ona wymagania stawiane rozprawom doktorskim określone w stosownej ustawie. Wnioskuję o przyjęcie niniejszej dysertacji jako rozprawy doktorskiej. Wnoszę jednocześnie o dopuszczenie Pana mgra inż. Piotra Piątka do publicznej obrony przedłożonej pracy w dyscyplinie Automatyka, Elektronika, Elektrotechnika i Technologie Kosmiczne.

Marcin Śliwiński