

dr hab. inż. Krzysztof Pietruszewicz, prof. ZUT
Katedra Automatyki i Robotyki
Wydział Elektryczny
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie
Al. Piastów 17, 70-310 Szczecin

Szczecin, dnia 10 lutego 2025 r.

SEKRETARIAT
Rady Dyscypliny AEEITK

Wpłynęło dnia 7.03.2025

Zarejestrowano pod nr 510-9-7/24

Podpis *dm*

Recenzja rozprawy doktorskiej mgra inż. Piotra Piątka

Tytuł rozprawy: **Systemowa analiza bezpieczeństwa układów sterowania w pojazdach o wysokim stopniu automatyzacji jazdy**
Autor rozprawy: **mgr inż. Piotr Piątek**
Promotor rozprawy: **dr hab. inż. Paweł Skruch, prof. AGH**
Promotor pomocniczy: **dr inż. Szczepan Moskwa**
Dziedzina: **nauki inżynieryjno-techniczne**
Dyscyplina: **automatyka, elektronika, elektrotechnika i technologie kosmiczne**

1. Wstęp i podstawa prawna sporządzenia recenzji

Recenzowana przeze mnie rozprawa doktorska porusza istotne, zarówno z naukowego jak i przede wszystkim praktycznego a w tym wdrożeniowego punktu widzenia, zagadnienia zarządzania projektami związanymi z bezpieczeństwem funkcjonalnym, cyberbezpieczeństwem oraz bezpieczeństwem zamierzonej funkcjonalności systemów sterowania w pojazdach o wysokim stopniu autonomiczności.

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 dnia 7 listopada 2024 r. w sprawie powołania recenzentów rozprawy doktorskiej mgr. inż. Piotra Piątka pt. „Systemowa analiza bezpieczeństwa układów sterowania w pojazdach o wysokim stopniu automatyzacji jazdy”, przekazaną przez Przewodniczącą Rady Dyscypliny Automatyka, Elektronika, Elektrotechnika i Technologie Kosmiczne AGH dr. hab. inż. Ryszarda Srokę, prof. AGH, pismem z dnia 8 listopada 2024 r. (pismo L.Dz. RD AEEITK/510-9-2/24).

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

2. Ocena formalna, charakterystyka pracy

Praca doktorska pt. „Systemowa analiza bezpieczeństwa układów sterowania w pojazdach o wysokim stopniu automatyzacji jazdy” obejmuje łącznie 327 stron (strony techniczne, w tym Spis treści, Spis skrótów, Streszczenie w języku polskim oraz angielskim: I-XVI; rozprawa: 1-175; Dodatek A: 1-119; Dodatek B, Spis rysunków, Bibliografia: 295-311). Składa się z 5 zasadniczych rozdziałów, w tym Bibliografii obejmującej 131 pozycji. Bibliografia zawiera odwołania do niezbędnych z perspektywy celu pracy i jej zakresu standardów, licznych artykułów w czasopiśmie, materiałów konferencyjnych oraz not technicznych. Niestety zabrakło w rozprawie odwołań do publikacji Autora (<https://orcid.org/0000-0003-2081-4776>):

1. **P. Piątek**, P. Mydłowski, A. Buczacki and S. Moskwa, "Concept of Using the MBSE Approach to Integrate Security Patterns in Safety-Related Projects for the Automotive Industry," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 11, pp. 15477-15492, Nov. **2024**, doi: 10.1109/TITS.2024.3444048. keywords: {Security; Automotive engineering; Safety; Industries; Computer security; System analysis and design; Standards; Model-based systems engineering (MBSE); cybersecurity (CySe); functional safety (FS); security pattern (SP); automotive};
2. **P. Piątek**, "Incident Management Process Model for Automotive CyberSafety Systems Using the Business Process Model and Notation," 2022 26th International Conference on Methods and Models in Automation and Robotics (MMAR), Międzyzdroje, Poland, **2022**, pp. 232-237, doi: 10.1109/MMAR55195.2022.9874288. keywords: {Industries; Robot kinematics; Vehicle safety; Phantoms; Maintenance engineering; Proposals; Computer security; CyberSafety; cybersecurity; functional safety; SOTIF; automotive; BPMN; incidents management};
3. Buczacki, A.; **Piątek, P.** Proposal for an Integrated Framework for Electronic Control Unit Design in the Automotive Industry. *Energies* **2021**, 14, 3816. <https://doi.org/10.3390/en14133816>

które z perspektywy celu pracy są niezwykle istotne.

Praca jest uzupełniona dwoma dodatkami, do których Autor nawiązuje w rozprawie. Dodatek A zatytułowany „Załącznik A. Bizagi – CyberSafety Framework” zawiera wydruk projektu opracowanych z zastosowaniem oprogramowania **Bizagi Modeler** (<https://www.bizagi.com/en>) w ramach rozprawy ram projektowych (ang. Framework). Dodatek B zatytułowany „Załącznik B – Medini Analize – CyberSafety Analysis Highway Pilot” zawiera link do pobrania kompletnego projektu oprogramowania **Ansys medini analize**. Dodatek A jest ściśle powiązany z Rozdziałem 3, podczas gdy Dodatek B jest produktem prac opisanych w Rozdziale 4.

Praca napisana jest zarówno w języku angielskim jak i w języku polskim. Niniejsza recenzja odnosi się do rozprawy jako całości, nie zaś do wybranej wersji językowej. Przedstawiona do oceny praca jest zorganizowana jak poniżej:

2.1. Rozdział 1. Wstęp

W Rozdziale 1 wskazano tło dla podjęcia problematyki pracy. Wielokrotnie podkreśla się konieczność integracji działań z obszarów bezpieczeństwa funkcjonalnego (FuSa – *Functional Safety*), cyberbezpieczeństwa (CySe – *CyberSecurity*) oraz bezpieczeństwem zamierzonej funkcjonalności (SOTIF – *Safety of Intended Functionality*) na czesnym etapie projektowania pojazdu o wysokim poziomie autonomiczności. W rozprawie wskazuje się zagadnienie rosnącej informatyzacji pojazdów jako kluczowe dla rozwoju metod projektowania. Konieczne staje się współcześnie, z uwagi na rosnącą złożoność pojazdów, których funkcjonalność rekonfigurowana jest z pomocą oprogramowania, wykorzystanie metod bazujących na modelach, jak koncepcja Model-Based Design (MBD), czy bardziej szczegółowo Model-Based Systems Engineering (MBSE). Autor rozprawy wskazuje MBSE jako sposób efektywnego rozwiązania problemu integracji analizy ryzyka według wskazanych standardów (i metod) w ramach narzędzia zarządzania procesem wytwarzania bezpiecznych produktów.

Przyjęte przez Autora założenie, jakim jest zwiększenie efektywności procesów projektowych dla tak wielowymiarowego zagadnienia jest prawidłowe – obecnie jedynie podejście MBSE daje szansę na opanowanie złożoności, będącej przedmiotem pracy.

W Rozdziale 1 sformułowano najważniejsze hipotezy pracy:

1. „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.”;
2. „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.”

Związane z nimi cele pracy:

1. „Sformułowanie 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.”;
2. „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.”

W Rozdziale 1 zawarto również szczegółowy plan rozprawy oraz trafnie określono wkład rozprawy w rozwój dyscypliny naukowej:

1. Pionierska integracja analizy cyberbezpieczeństwa i bezpieczeństwa;
2. Naświetlenie zależności technicznych i ich wpływu na ryzyko;
3. Rozwój nowatorskich, elastycznych i kwantyfikowalnych ram analizy ryzyka;
4. Koncentracja na wczesnym ograniczaniu ryzyka i proaktywnej kulturze bezpieczeństwa;
5. Promocja perspektywy inżynierii systemów w celu zwiększenia bezpieczeństwa i ochrony;
6. Doskonalenie metodologii analizy ryzyka.

2.2. Rozdział 2. Przegląd literatury

Autor bardzo szczegółowo przeanalizował wszystkie standardy, które następnie wykorzystywał oraz integrował w ramach rozprawy (ISO 26262:2018, ISO 21434:2021, ISO 21448:2019). W przyjazny sposób przybliżył procesy, związane z opracowaniem nowego produktu (Rys. 2.1). Wyjaśnił zagadnienia marnotrawstwa w obszarach zarządzania: procesami NPD (New Product Development, Tabela 2.1) oraz procesami inżynieryjnymi (Tabela 2.6).

Bardzo cennym jest z pewnością omówienie kierunków rozwoju architektury pojazdów i powiązane z tym problemy. W Tabeli 2.4 podsumowano wszystkie możliwe kategorie komunikacji w ramach ekosystemu, w jakim funkcjonują pojazdy, zaś Rys. 2.13 pokazuje jak złożony problem Autor próbuje rozwiązać w swojej pracy badawczej.

Rozdział jest bardzo rozbudowany, jednakże dzięki temu bardzo dobrze przygotowana jest baza do omówionych w kolejnych rozdziałach wyników badań.

Kluczową wartością Rozdziału 2 jest Rys. 2.6, prezentujący zintegrowany z perspektywy standardów bezpieczeństwa, cyberbezpieczeństwa oraz bezpieczeństwa zamierzonej funkcjonalności model V.

Z kolei dyskusja związana z zawartością Rys. 2.20 świadczy o bardzo zaawansowanym warsztacie Autora rozprawy – łączenie podejść zaprezentowanych na nim w procesach opracowania nowych produktów wymaga wysokiej kultury organizacyjnej wykorzystującego takie procesy przedsiębiorstwa oraz wysoko wykwalifikowanej kadry działów badawczo-rozwojowych.

Z dużą szkodą dla Rozdziału 2, Autor nie omówił osiągnięć, wynikających ze wskazanych publikacji, których był autorem lub współautorem.

W Rozdziale 2 czuje się niedosyt cytowania prac, opisujących różne obszary wykorzystania podejścia MBSE w motoryzacji. Bezpieczeństwo funkcjonalne i cyberbezpieczeństwo w procesach projektowania oprogramowania to jeden z obszarów. Chciałoby się dowiedzieć, jak wygląda kwestia wykorzystania podejścia na różnych etapach procesów, wynikających ze standardu ISO 26262:2018. W normie tej wskazuje się również na formalne lub półformalne języki/metody modelowania. W Rozdziale 2 nie wskazano również, czy i jeżeli tak, to jak zagadnienie integracji podejść wynikających z różnych uwarunkowań (standardów, wytycznych) jest rozwiązywane w innych niż motoryzacyjna, branżach. Dyskusja taka istotnie podniosłaby i tak już bardzo wysoki poziom Rozdziału 2.

2.3. Rozdział 3. Nowe ramy procesów projektowania modułów sterowania elektronicznego

Jest to najważniejszy z perspektywy celu pracy oraz postawionych przez Autora hipotez rozdział. Zaprezentowano w nim (Rysunek 3.1. Widok wysokiego poziomu ram CyberSafety – tzw. *Top-level architecture*) koncepcję referencyjnego modelu architektury nowego zintegrowanego procesu projektowania. To w mojej ocenie główne osiągnięcie pracy. Do opracowania nowych ram procesu projektowego wykorzystano notację BPMN 2.0 (Business Process Model and Notation). Użyto notacji bazowej, bez żadnych modyfikacji metamodelu. Dzięki temu Autor mógł wykorzystać wbudowane w narzędzie Bizagi Modeler funkcje weryfikacji poprawności (w tym kompletności) tworzonych modeli.

W ramach nowego zintegrowanego procesu (CySa – CyberSafety Framework) powiązано trzy procesy projektowe: FuSa (*Functional Safety*; zagadnienie opisane w ramach normy ISO 26262), CySe (*Cybersecurity*; zagadnienie będące przedmiotem standardu ISO 21434) oraz SOTIF (*Safety of Intended Functionality*; zgodnie z normą ISO 21448). Opracowano kompletne ramy nowego procesu projektowania modułów sterowania pojazdu o wysokim stopniu autonomiczności.

W rozdziale 3 przedstawiono wszystkie elementy tzw. Frameworka: proces projektowy, przybornik modelowania, perspektywy/ widoki modelowania, obiekty modelowania, definicje relacji oraz role w relacjach pomiędzy obiektami modeli). Przedstawiono elementy ram procesu projektowania, związane z przeprowadzonymi dla zintegrowanego podejścia analizami:

1. HARA – Hazard Analysis and Risk Assessment (ISO 26262);
2. HIRE – Hazard Identification and Risk Evaluation (ISO 21448);
3. TARA – Threat Analysis and Risk Assessment (ISO 21434).

W rozdziale 3 bardzo szczegółowo omówiono zagadnienie ujednoczenia standardów oraz związanych z nimi analiz łącząc je w jednym procesie projektowym. Było to niezwykle ambitne zadanie zarówno z analitycznego jak i syntetycznego punktu widzenia. Doktorant opisał proponowane ramy projektowania ze wszystkich możliwych i jednocześnie niezbędnych perspektyw/ faz: fazy koncepcji lub przygotowania projektu (1); fazy projektowania (2); fazy wdrożenia (3); fazy weryfikacji (4); fazy walidacji (5); fazy produkcji/ wydania (6); fazy utrzymania (7) oraz fazy wycofania z eksploatacji (8).

W podsumowaniu rozdziału 3 zaprezentowano w formie bardzo dobrze przygotowanych zestawień tabelarycznych (tabele 3.3 do 3.9) wszystkie możliwe produkty robocze (efekty pracy projektowej w poszczególnych fazach). Z jednej strony wskazano produkty, charakterystyczne dla każdego z integrowanych w pracy standardów (ISO 26262:2018, ISO 21434:2021 oraz ISO 21448:2019), z drugiej zaś zaproponowano zestaw produktów zintegrowanego podejścia CyberSafety (CySa).

Na koniec rozdziału 3 omówiono rekomendacje dla wdrażania zaproponowanego w rozprawie zintegrowanego podejścia projektowego, co dopełnia głównego osiągnięcia recenzowanej rozprawy.

2.4. Rozdział 4. Proponowany model oceny systemów aktywnego bezpieczeństwa oparty na zdefiniowanych wskaźnikach

Rozdział 4 poświęcono ocenie zaproponowanego podejścia poprzez realizację kompletnego studium przypadku wdrożenia zaawansowanej funkcji wspomagającej jazdę autonomiczną, jaką jest Highway Pilot. Ramy CyberSafety zostały ocenione poprzez walidację ich skuteczności przy użyciu funkcji aktywnego wspomagania kierowcy (Highway Pilot), funkcji automatyzacji pojazdu na poziomie 3. Do analizy funkcji HP wykorzystano w pracy oprogramowanie ANSYS *medini analyze*. Jednym z powodów była wyjątkowa cecha tego narzędzia, jaką jest możliwość prowadzenia analiz związanych ze wszystkimi, integrowanymi w ocenianej rozprawie standardami. *Medini analyze* udostępnia narzędzia dla: *Failure Mode and Effect Analysis* (FMEA), *Fault Tree Analysis* (FTA) oraz *Event Tree Analysis* (ETA).

W kolejnych podrozdziałach zaprezentowano analizy związane z fazami zintegrowanego procesu projektowania. Zaprezentowano komplet metryk dla wykorzystanej funkcji HP. Istotny dla pracy jest zdefiniowany wskaźnik, opisujący redukcję wysiłku (nakładu pracy) w zakresie wytworzenia wymaganych dla procesu produktów pracy.

W rozdziale 4 zdefiniowano również tzw. ważony współczynnik bezpieczeństwa (WSS – *Weighted Safety Score*), będący kombinacją wskaźnika bezpieczeństwa zagrożeń (HaSI – *Hazard Safety Indicator*) oraz oceny zagrożenia ryzyka (ThRS – *Threat Risk Score*).

W rozdziale 4 zaprezentowano serię różnego rodzaju wskaźników oceny procesu, wyznaczono również ich wartości dla przykładu projektu funkcji Highway Pilot:

1. Wskaźnik identyfikacji ryzyka bezpieczeństwa i ochrony (SSRIR – *Security And Safety Risk Identification Rate*);
2. Wskaźnik pokrycia oceny ryzyka (RAC – *Risk Assessment Coverage*);
3. Skuteczność przeglądu projektu (DRE – *Design Review Effectiveness*);
4. Kompletność strategii łagodzenia skutków (MSC – *Mitigation Strategy Completeness*);
5. Wskaźnik zgodności projektu (DCR – *Design Compliance Rate*);
6. Poziom ryzyka rezydualnego (RRL – *Residual Risk Level*);
7. Pokrycie wymagań bezpieczeństwa i ochrony (SRC – *Security and Safety Requirement Coverage*);
8. Wskaźnik złożoności projektu (DCI – *Design Complexity Index*);
9. Wskaźnik wniosków o zmianę projektu (DCRR – *Design Change Request Rate*).

W bardzo czytelny sposób wykazano wyższość proponowanego zintegrowanego procesu CyberSafety na podejściem z indywidualnym wykorzystaniem podejść projektowych opisanych w odpowiednich standardach.

W.

2.5. Rozdział 5. Wnioski i rekomendacje

W ostatnim numerowanym rozdziale Autor podsumowuje wyniki badań opisane w rozdziałach od 2 do 4. Wykazuje odpowiedź na najważniejsze problemy przywołane w rozdziale 2 rozprawy. Podkreśla i omawia konieczność przyjęcia nowego sposobu myślenia o bezpieczeństwie pojazdów (rysunki 5.1, 5.2), z silosowego na zintegrowane podejście, dla którego wsparcia w rozdziale 3 doktorant proponuje nowy referencyjny model architektury procesu projektowego. Podsumowuje użyte w przykładowym modelu (i procesie) wskaźniki, łącznie zintegrowane w rozprawie podejścia.

2.6. Załączniki

Istotną częścią recenzowanej rozprawy doktorskiej są dwa załączniki:

1. Załącznik A zawiera kompletny eksport schematu zaprojektowanego procesu *CyberSafety* ze środowiska Bizagi Modeler;
2. Załącznik B zawiera analizę cyberbezpieczeństwa struktury funkcjonalnej systemu Highway Pilot, wykonaną w oprogramowaniu *ANSYS Medini* analizie. Projekt jest dostępny do pobrania z linka zawartego w rozprawie.

3. Ocena merytoryczna pracy

3.1. Istotność zagadnienia, celu i zakresu rozprawy

Tematyka recenzowanej rozprawy, związana z wykorzystaniem podejścia *Model-Based Systems Engineering* do systemowej analizy bezpieczeństwa układów sterowania w pojazdach. Doktorant w bardzo uporządkowany sposób, charakterystyczny dla podejścia MBSE prezentuje autorską koncepcję integracji rozłącznych dotychczas zagadnień projektowania: bezpieczeństwa funkcjonalnego, cyberbezpieczeństwa oraz bezpieczeństwa zamierzonej funkcjonalności.

Niniejsza rozprawa wpisuje się w aktualny i bardzo dynamicznie rozwijający się obszar rozwoju motoryzacji, jakim jest „współczesny samochód, definiowany jako platforma sprzętowa definiowana programowo”. Taki kierunek rozwoju autonomicznych pojazdów sprawia, że zagadnienie bezpieczeństwa funkcjonalnego w powiązaniu z cyberbezpieczeństwem nabiera kluczowe znaczenia.

Uważam, że tematyka poruszana w pracy jest bardzo aktualna i ma olbrzymie znaczenie praktyczne. Proponowane rozwiązanie wpisuje się w trendy, co potwierdza m.in. dostępność integrowanych w pracy analiz w oprogramowaniu *ANSYS medini* analizie.

W rozprawie postawiono dwie główne hipotezy badawcze:

1. „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”;
2. „Opracowanie nowatorskiego modelu rozwoju, który wyposaża firmy w kompleksowe narzędzia 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”.

Według mnie tezy recenzowanej rozprawy są poprawne i odpowiednio sformułowane.

Najważniejsze cele recenzowanej rozprawy to:

1. „Sformułowanie 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”;
2. „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”.

Uważam, że cele pracy są istotne i spełniają wymagania stawiane rozprawom doktorskim. Według mnie, oba cele pracy zostały w rozprawie osiągnięte.

3.2. Zawartość merytoryczna pracy

W recenzowanej przeze mnie rozprawie zdecydowanie najważniejszym rozdziałem jest rozdział 3, opisujący zaproponowane przez Autora ramy nowego zintegrowanego procesu projektowania. Rozdział 2, stanowiący bardzo szczegółowe studium dostępnej dla zagadnienia literatury, stanowi solidny fundament zarówno dla propozycji z rozdziału 3 jak i potwierdzającego postawione przez doktoranta hipotezy w równie ważnym rozdziale 4. Praca ma wyraźny podział zarówno z uwagi na charakter jak i zawartość merytoryczną – podział między rozdziały od 2 do 4. Całość uzupełniają Załączniki A oraz B.

Za najważniejsze osiągnięcie rozprawy doktorskiej uważam rozdziały: trzeci oraz czwarty. Zawierają one bowiem koncepcję opracowanej metodyki oraz jej weryfikację w toku autorskich badań doktoranta.

3.3. Uwagi merytoryczne i pytania dyskusyjne

Biorąc pod uwagę kwestie poruszone w recenzowanej przeze mnie rozprawie, chciałbym poruszyć i prosić o wyjaśnienie podczas obrony następujących, opisanych poniżej kwestii.

Pytanie 1

W rozdziale 3 wykorzystano notację BPMN 2.0 do opisania referencyjnego modelu projektowania zintegrowanego przez autora w ramach procesu *CyberSafety*. Czy Autor dokonywał modyfikacji metamodelu przyjętej notacji, jeżeli tak to w jakim zakresie? Czy było to potrzebne? A jeżeli nie, to jakie były tego powody.

Pytanie 2

W rozdziale 2 dokonano bardzo szczegółowego przeglądu literatury. Proszę o uwzględnienie dyskusji na temat publikacji autora rozprawy i ich związku z recenzowaną pracą w prezentacji podczas obrony.

Pytanie 3

W pracy niewiele miejsca poświęcono zagadnieniu wykorzystania podejścia MBSE w motoryzacji. Czy Autor mógłby odpowiedzieć, w jakich obszarach, poza analizą bezpieczeństwa, pomaga podejście MBSE – które procesy związane z branżą motoryzacyjną wspiera?

Pytanie 4

Podsumowanie pracy (rozdział 5) precyzyjnie domyka postawione w rozprawie hipotezy badawcze oraz przyjęte cele. W rozdziale podsumowującym zabrakło w mojej ocenie kierunków przyszłych badań, jakie na kanwie osiągnięcia doktoranta mogłyby być prowadzone. Czy mogę prosić o uzupełnienie tego punktu podczas obrony?

Pytanie 5

„Załącznik A. CyberSafety Framework” zawiera eksport z projektu oprogramowania Bizagi Modeler kompletnego projektu. Dużą wartością dla pracy byłby syntetyczny raport kluczowych dla celu pracy fragmentów, choć całość modelu też pokazuje nakład pracy. Proszę o informację, czy oprogramowanie Bizagi Modeler posiada moduł projektowania personalizowanych raportów?

Pytanie 6

W pracy bardzo szczegółowo przedstawiono wiele elementów modelowania w różnych narzędziach. Czy podczas obrony doktorant mógłby na syntetycznym slajdzie zaprezentować, jakich narzędzi używał do którego z fragmentów swojej pracy badawczej. Będzie to duża wartość dla osób uczestniczących w obronie. Ciekawym aspektem dla słuchaczy będzie perspektywa ekonomiczna wdrożenia: koszt oprogramowania, liczba osób zaangażowanych w realizację procesów w podejściu zintegrowanym a w podejściu z rozdzielonymi analizami bezpieczeństwa.

Pytanie 7

W tabeli 2.4. Kategorie komunikacji w połączonym ekosystemie zamieszczono kilkanaście powiązań: IV, V2V, V2S, S2V, V2I, I2V, V2E, E2V, V2T, T2V, S2I, I2S, I2E, E2I, V2G. Proszę o przedstawienie tych kategorii oraz łączących ich w formie graficznej. Z tekstu bowiem nie wynika, jakie są różnice pomiędzy *Surrounding*, *Infrastructure*, *Ecosystem* oraz *Grid*. Jest to ciekawe zagadnienie. Nie oczekuję prezentacji tego zagadnienia podczas obrony.

3.4. Ogólna ocena pracy

Według mnie przedstawiona do recenzji rozprawa jest naukowo kompletna. Potwierdzeniem tego jest występowanie w rozprawie: (1) odniesień do bogatej literatury przedmiotu badań; (2) niezbędnych do zrozumienia przedstawionych zagadnień definicji – choć jest ich wiele, to autor dołożył starań, bo obszar pojęć był kompletny; (3) szczegółowego omówienia głównego osiągnięcia pracy, jakim jest zintegrowany proces projektowania; (4) szczegółowego opisu wykorzystanych w studium przypadku rodzajów analiz, wskaźników; (5) opisu użytego w pracy oprogramowania oraz notacji; (6) analizy i omówienia wyników badań własnych; (7) podsumowania wyników, problemów i wskazania rekomendacji dla zainteresowanych wdrożeniem wyników doktoranta w praktyce.

Poszukiwania naukowe doktoranta zaowocowały uporządkowanymi, logicznie spójnymi oraz implementacyjnie atrakcyjnymi rozwiązaniami z obszaru analizy bezpieczeństwa i cyberbezpieczeństwa systemu sterowania pojazdu o wysokim stopniu automatyzacji jazdy.

Zaprezentowane w pracy badania mają charakter rozwojowy, zmierzający ku opracowaniu kompleksowego narzędzia/ standardu integrującego trzy opisane w pracy podejścia projektowania. Przedstawiona do recenzji rozprawa doktorska stanowi w mojej ocenie oryginalne rozwiązanie zdefiniowanego na wstępie problemu naukowego. Zaprezentowane wyniki badań wykazują ogólną wiedzę teoretyczną kandydata w dyscyplinie naukowej automatyka, elektronika, elektrotechnika i technologie kosmiczne zaś poziom precyzji opisu postawionej w pracy a następnie udowodnionej tezy badawczej dowodzą umiejętności doktoranta do zespołowego oraz samodzielnego prowadzenia pracy naukowej.

4. Główne osiągnięcia rozprawy

Za najistotniejsze osiągnięcia doktoranta w związku z recenzowaną rozprawą uważam:

1. opracowanie i szczegółową prezentację przeglądu literatury w obszarach integrowanych podejść w aspekcie bezpieczeństwa w motoryzacji;
2. omówienie aspektów zarządzania projektami rozwoju oprogramowania w systemach wspomagających jazdę o wysokim stopniu automatyzacji;
3. kompletną propozycję integracji metod projektowania w ramach procesu *CyberSafety*;
4. opracowanie kompletnego zintegrowanego procesu projektowania z wykorzystaniem notacji typowej dla modelowania procesów – BPMN 2.0;
5. zaproponowanie ważonego współczynnika bezpieczeństwa (WSS – *Weighted Safety Score*);
6. przedstawienie opracowanych w rozprawie metod i narzędzi w studium przypadku, potwierdzając wszystkie stawiane hipotezy i osiągając zdefiniowane cele.

Stwierdzam, że doktorant dysponuje wymaganym do prowadzenia badań naukowych zasobem wiedzy oraz umiejętnościami, jak również kompetencjami z zakresu dyscypliny naukowej **automatyka, elektronika, elektrotechnika i technologie kosmiczne**.

5. Ocena poziomu edytorskiego rozprawy

Praca w zakresie treści charakteryzuje się logicznym i bardzo uporządkowanym podziałem. Rozprawa napisana w języku angielskim, z prawidłowym użyciem bardzo hermetycznego dziedzinowo języka. Styl oraz poziom językowy prawidłowe. Praca zredagowana starannie, rysunki w większości czytelne.

Jedyną uwagą jest brak spójności w zakresie podejścia Załączników. Dodatek A występuje w pracy w formie wydruku projektu – niestety z uwagi na użycie standardowego szablonu eksportu niezbyt starannie sformatowanej. Dodatek B stanowi link do pobrania kompletnego projektu.

Sprawia to, że praca jest dość obszerna. Wystarczyłoby załączenie Dodatku A w analogicznej formie jak Dodatek B.

Należy zaznaczyć, że zawarta tutaj drobna uwaga edytorska nie wpływa w żaden sposób na wartość merytoryczną przedłożonej rozprawy doktorskiej.

6. Wnioski końcowe

Po zapoznaniu się z pracą doktorską pt. „**Systemowa analiza bezpieczeństwa układów sterowania w pojazdach o wysokim stopniu automatyzacji jazdy**” stwierdzam, że:

przedstawiona rozprawa spełnia

właściwe ustawowe wymagania stawiane rozprawom doktorskim oraz mieści się w dyscyplinie automatyka, elektronika, elektrotechnika i technologie kosmiczne i w związku z powyższym

wnioskuje o przyjęcie rozprawy doktorskiej oraz dopuszczenie

mgr inż. Piotra Piątka do publicznej obrony w wyżej wspomnianej dyscyplinie.

Pietruszewicz

Krzysztof Pietruszewicz