Prof. Czesław Smutnicki
Politechnika Wrocławska

Wrocław 2.02.2023

Recenzja rozprawy doktorskiej

Tytuł: Jakość i bezpieczeństwo oprogramowania w przemyśle motoryzacyjnym – analiza standardów oraz opracowanie metody wspomagającej proces tworzenia oprogramowania

Autor: mgr inż. Patryk Pankiewicz

Promotor: dr hab. inż. Andrzej Białas, prof., Lukasiewicz-EMAG

Przedmiot oceny

Przedmiotem oceny jest rozprawa doktorska z dziedziny nauk technicznych w dyscyplinie informatyka techniczna i telekomunikacja mgra. inż. Patryka Pankiewicza pt. „Jakość i bezpieczeństwo oprogramowania w przemyśle motoryzacyjnym – analiza standardów oraz opracowanie metody wspomagającej proces tworzenia oprogramowania" napisana pod kierunkiem dra hab. inż. Andrzeja Białasa, prof. Łukasiewicz-EMAG. Rozprawa ma całkowitą objętość 164 stron, w tym w szczególności zawiera: 93 pozycje bibliograficzne, 24 rysunki, 14 kodów programowych, 2 słowniki ze skorowidzem, 2 spisy rzeczy. Rozprawa została przygotowana w ramach programu doktoratów wdrożeniowych, mającego na celu połączenie badań naukowych z przemysłem i jednostkami biznesowymi.

Informacje o Autorze rozprawy

W dokumentacji brak jest danych dotyczących przebiegu kariery zawodowej i naukowej Autora rozprawy. W rozprawie wymieniono 10-letnie doświadczenie komercyjne Autora (str 133). Wg mojej wiedzy, dotychczas nie realizowano rozprawy w tej tematyce.

Tematyka rozprawy

Tematyka, zakres i przedmiot rozprawy mieści się całkowicie w zakresie dyscypliny informatyka techniczna i telekomunikacja. W rozprawie formalnie nie podano listy słów kluczowych, choć łatwo je zidentyfikować, są to: inżynieria oprogramowania, systemy mobilne, systemy wbudowane, bezpieczeństwo, standardy, komunikacja, IoV. Problem badawczy, który autor sformułował wynika z rosnącej i niekontrolowanej liczby błędów w oprogramowaniu projektowanym i stosowanym w przemyśle motoryzacyjnym wraz ze wzrostem skomplikowania oprogramowania, które wpływają bezpośrednio na niezawodność pojazdów, bezpieczeństwo i komfort kierowców. Problem jest nietrywialny, bowiem odnosi się prac gremiów międzynarodowych oraz ekspertów lokalnych dotyczących ustanowienia wspólnych standardów projektowania, wdrażania, monitorowania i aktualizacji oprogramowania dla pojazdów samochodowych różnych firm produkowanych i używanych w

skali całego świata. Rozprawa skupia się na jednostkach wbudowanych w pojazdy samochodowe, używających standardu AUTOSAR Classic, czyli systemach powiązanych z krytycznymi układami dotyczącymi bezpieczeństwa użytkowników samochodów. Problem jest niewątpliwie istotny, ponieważ skomplikowanie oprogramowania prawdopodobnie nie osiągnie limitu w kolejnych latach i będzie stale rosnąć. Według Autora rozprawy potrzebne są nowe metody i procedury postępowania by utrzymać jakość i bezpieczeństwo systemów samochodowych na odpowiednim poziomie poprzez rygorystyczne przestrzeganie procedur projektowania, testowania i modyfikacji oprogramowania. Jednym z celów rozprawy było wykazanie złożoności procesu tworzenia oprogramowania tego typu oraz wynikających z tego eliminacji ryzyka błędów. Jednak zasadniczym celem naukowo-badawczym opisanym i udokumentowanym w rozprawie było przeprowadzenie badań i ocena jakości rozwiązań sprzętowych i programowych na wybranych projektach komercyjnych systemów samochodowych realizowanych przez Autora. Uważam, że tematyka rozprawy jest wyjątkowo istotna zarówno z teoretycznego jak i z praktycznego punktu widzenia. Co więcej, udokumentowano bezpośrednie zastosowanie proponowanych rozwiązań w praktyce.

Ocena układu rozprawy

Rozprawa rozpoczyna się od dość ogólnie nakreślonego problemu projektowania i tworzenia oprogramowania dla pojazdów samochodowych. Wskazano krytyczne elementy tego procesu. Znaczenie tego zagadnienia jest istotne, bowiem wpływa na bezpieczeństwo i komfort użytkowników pojazdów. I tak, w rozdziale 2 opisano procesy, standardy technologiczne oraz normy o zasięgu międzynarodowym, które wpływają na jakość i bezpieczeństwo oprogramowania. Na uwagę zasługuje bardzo dobra znajomość przez Autora obowiązujących norm oraz wyczerpujące ich omówienie. W rozdziale 3 przedstawiono zidentyfikowane przez Autora problemy badawcze (mianowicie: problem skalowalności ekstraktów diagnostycznych, ograniczone zasoby sprzętowe, wysoka złożoność oprogramowania, problem czasu wykonywania) wraz z powiązanymi zagadnieniami badawczymi. Każdy omawiany problem i zagadnienie badawcze Autor omawia na tle dotychczasowej wiedzy oraz istniejących i stosowanych rozwiązań w tym zakresie. W rozdziale 4 opisano sprzętowe stanowiska badawcze używane podczas badań i analiz oraz wszystkie wykorzystane metody badawcze. Metody odniesiono do celów badawczych. W rozdziale 5 zaprezentowano nowo proponowane elementy składające się na pakiet rozwiązań oraz finalną metodę wspomagającą proces tworzenia oprogramowania. Ponadto wskazano tamże relację każdego zaproponowanego rozwiązania do zidentyfikowanych wcześniej problemów oraz zagadnień badawczych. Pracę podsumowano w rozdziale 6.

Układ rozprawy jest organizacyjnie poprawny. Opisuje kolejno kluczowe elementy i ich cechy związane z projektowaniem i realizacją oprogramowania dla pojazdów samochodowych. Dalej dokumentuje badania Autora oraz prezentuje wyniki Jego badań. Struktura pracy, podział na rozdziały i podrozdziały został zrealizowany prawidłowo. W mojej ocenie kompozycja pracy została wykonana nie tylko poprawnie, ale także właściwie z punktu widzenia tematyki rozprawy .

Merytoryczna i formalna ocena rozprawy

Na uwagę zasługuje co najmniej kilka pozytywnych cech rozprawy. Po pierwsze, dostarcza ona wyczerpującego kompendium wiedzy na temat dość specyficznej dziedziny projektowania i

realizacji oprogramowania dla pojazdów samochodowych (patrz rozdz. 2). Odmienność tego zagadnienia w stosunku do innych problemów inżynierii oprogramowania polega na wdrożeniu i rygorystycznym przestrzeganiu standardów międzynarodowych dla eliminacji błędów oprogramowania zagrażających bezpieczeństwu uczestników ruchu pojazdów. Po wtóre: przegląd problematyki stał się podstawą do sformułowania oryginalnej tezy rozprawy: „Poprzez wykorzystanie zaproponowanego w pracy pakietu rozwiązań stanowiącego metodę wspomagającą proces tworzenia oprogramowania, istnieje możliwość poprawy jakości, bezpieczeństwa funkcyjnego i cyberbezpieczeństwa oprogramowania w rozumieniu norm o zasięgu międzynarodowym – ISO 25010, ISO 26262 i ISO 21434". Teza ta została wykazana poprzez zdefiniowanie i przygotowanie właściwych narzędzi wspomagających proces tworzenia „właściwego" oprogramowania tego typu oraz do oceny jakości tego oprogramowania. Rozwiązania, które zostały wzięte pod uwagę to: automatyzacja stosu diagnostycznego, automatyzacja oraz architektura DLT, automatyzacja oraz architektura stosu NvM, obserwator systemu. Autor rozprawy zidentyfikował problemy badawcze (patrz rozdz. 3) w omawianym obszarze, sformułował zadania badawcze oraz przedstawił je w kontekście istniejących badań naukowych, które zostały sformułowane podczas analizy procesu tworzenia oprogramowania. Dla postawionych problemów Autor zaproponował pewne konkretne rozwiązania następnie badane i oceniane przy życiu różnych wskaźników. Ostatecznie pozwoliło to na precyzyjną lokalizację osiągnięć Autora na tle dziedziny. Praca zawiera staranną dokumentację stosowanych metod badawczych oraz stanowiska dla badań (patrz rozdz. 4). Efektem finalnym badań i działań Autora rozprawy jest pakiet oprogramowania oraz ogólna metoda wspomagająca proces tworzenia oprogramowania. Wskazano także relację każdego zaproponowanego rozwiązania do zidentyfikowanych wcześniej problemów oraz zagadnień badawczych. Odniesiono otrzymane wyniki badań do spełnienia kluczowych norm międzynarodowych.

Praca ma charakter eksperymentalny, a nie teoretyczny. Jest oryginalna z punktu widzenia zastosowania inżynierii oprogramowania (doktorat wdrożeniowy) ze względu na specyficzne wymagania użytkowników pojazdów, a także twórców oprogramowania dla przemysłu motoryzacyjnego. Tworzy pomost pomiędzy naukowym oraz komercyjnym podejściem do inżynierii oprogramowania. W mojej ocenie wykonane badania mają charakter nietrywialny i świadczą o wysokiej wiedzy dziedzinowej doktoranta.

Ocena zastosowanego piśmiennictwa

Rozprawa zawiera 93 pozycje bibliograficzne, wszystkie anglojęzyczne. W zdecydowanej większości są to prace naukowe, materiały konferencyjne i opracowania techniczne (raporty, normy, etc.) publikowane w okresie ostatnich 5-6 lat. Autor rozprawy wykazał się doskonałą znajomością przywoływanych standardów międzynarodowych, rozwiązań technicznych i programowych, inżynierii oprogramowania, systemów wbudowanych oraz problemów i metod projektowania wchodzących w zakres rozprawy. Jest dobrze zorientowany w najnowszej literaturze dotyczącej tematyki rozprawy. Bardzo dobrze oceniam zarówno dobór źródeł jak i ich multi-dyscyplinarność.

Ocena celu rozprawy

Głównym celem pracy było stworzenie pakietu rozwiązań oraz narzędzi, stanowiących metodę wspomagającą proces tworzenia oprogramowania dla systemów wbudowanych, stosowanych w samochodach osobowych wykorzystujących standard AUTOSAR Classic. (patrz str. 8-9). Tak postawiony cel jest racjonalny i uzasadniony względami praktycznymi, co wynika z wcześniejszego uzasadniania tematyki rozprawy (patrz wyżej „Tematyka rozprawy"). Odpowiednio do celu ogólnego, w rozprawie podano cele szczegółowe, a mianowicie:

1. Analiza elementów wpływających na jakość oprogramowania stosowanego w przemyśle samochodowym, w szczególności skupiając się na systemach powiązanych z jednostkami czasu rzeczywistego, najbardziej wpływającymi na bezpieczeństwo kierowcy.
2. Zidentyfikowanie działań projektowych, które posiadają jakiegokolwiek rodzaju wady lub luki.
3. Przeprowadzenie analiz oraz badań prowadzących do zminimalizowania możliwości wystąpienia błędów, zwiększenia jakości i bezpieczeństwa całego systemu.
4. Zaproponowanie rozwiązań dotyczących procesu tworzenia oprogramowania.
5. Zaproponowanie odpowiednej architektury, która zwiększy jakość produktu.
6. Zaproponowanie sposobu zmniejszenia ryzyka wynikającego z wzrastającego stopnia skomplikowania oprogramowania.
7. Wskazanie obszarów, na które należy zwracać największą uwagę podczas realizowania projektów dotyczących systemów wbudowanych.
8. Ulokowanie wyników analiz oraz zaproponowanych rozwiązań na modelu jakości oprogramowania, opisanego w normie ISO 25010.
9. Ulokowanie wyników analiz w kontekście norm bezpieczeństwa funkcjonalnego ISO 26262 i cyberbezpieczeństwa ISO 21434.

Cele szczegółowe są konsekwencją celu ogólnego. Uważam, że zarówno cel ogólny, jak i cele szczegółowe zostały określone nie tylko poprawnie, ale także są istotne z punktu widzenia praktycznego i aplikacyjnego dla wskazanego specyficznego obszaru zastosowań.

Ocena zastosowanych metod badawczych

W celu weryfikacji zidentyfikowanych problemów oraz zagadnień badawczych Autor przeprowadził badania i analizy w trzech projektach komercyjnych opisanych w rozdziale 4.1.1 (metody badawcze opisano także w rozdziale 4). W przypadku części badań Autor stworzył specjalne oprogramowanie, którego celem była analiza danych lub modyfikacja kodów źródłowych, tak aby zaobserwować działanie konkretnych obszarów systemu. Oprogramowanie napisane przez Autora jest dołączone do pracy, ale z powodu przeprowadzania badań w projektach komercyjnych objętych klauzulami poufności, wszystkie dane komercyjne są zanonimizowane, a dokładne nazwy czy fragmenty kodów źródłowych nie zostały dołączone do pracy. Dla każdego rozwiązania przedstawiono instrukcje wdrożeniowe, jak wykorzystać dane rozwiązanie w dowolnym innym projekcie komercyjnym. Weryfikacja każdego elementu metod wspomagającej proces tworzenia oprogramowania polegała na prezentacji wyników badań oraz zaprezentowaniu wpływu na normę jakości oprogramowania ISO 25010, normę bezpieczeństwa funkcyjnego ISO 26262 oraz normę cyberbezpieczeństwa ISO 21434. Wykorzystane metody badawcze to: analiza statyczna kodu, badanie czasu

wykonania kodu, badanie obciążenia CPU, analiza dokumentów, analiza przebiegu wykonania kodu, analiza przy użyciu obserwatora systemu. Są to typowe, ale poprawne, miary i oceny kodu. W mojej ocenie użyto właściwych metod badawczych.

Ocena omówienia wyników badań

Podsumowaniem wyników badań jest rozdz. 6, pt. „Wnioski i uwagi końcowe". Zgodnie z opisanymi w rozdziale 1.1 celami pracy, przedstawiono przez autora pakiet rozwiązań, stanowiący metodę wspomagającą proces tworzenia oprogramowania. Wszystkie opracowane metody zostały wdrożone w opisanych projektach komercyjnych, co jest świadczy o wysokiej przydatności wyników badań. Zdaniem Autora: „Wgląd w świat naukowej analizy problemów w bardzo dużej mierze pomógł autorowi w pracy komercyjnej oraz otworzył oczy na wiele kluczowych aspektów, na które wcześniej nie zwracał uwagi." Uważam, że przedstawione przez Autora analizy i rozwiązania będą mogły być wykorzystane przez innych inżynierów oraz naukowców w celu dalszego rozwoju współpracy przemysłu z nauką. Uważam, że dla wdrożenie doskonalszych technologii dla pojazdów samochodowych wymaga silnej współpracy nauki z przemysłem, co też osiągnięto w tym doktoracie.

Praktyczne zastosowanie wyników badań

Autor rozprawy jest na stałe zatrudniony w przemyśle, co umożliwiło wdrożenie opracowanych wyników badań naukowych. Rezultaty pracy zostały wdrożone w projektach komercyjnych w tym także dla partnerów zagranicznych. Wprawdzie wdrożone kody źródłowe są własnością klientów, ale wszystkie elementy koncepcyjne i architektoniczne proponowanej metody wspomagającej proces tworzenia oprogramowania, zostały opisane w taki sposób, aby czytelnicy rozprawy mogli je zaimplementować we własnych projektach lub badaniach bez naruszeń prawnych. Dlatego też rozwiązania problemów badawczych zaprezentowano w postaci wzorców projektowych do wykorzystania przez twórców oprogramowania tego typu. zaproponowany pakiet rozwiązań mógł być użyty w wielu innych projektach komercyjnych. Dzięki osadzeniu badań i analiz w kontekście norm o zasięgu międzynarodowym oraz standardu AUTOSAR, które są uznawane jako „zgodne ze sztuką" w przemyśle motoryzacyjnym, elementy metody można wykorzystać w systemach wbudowanych stosowanych w każdym seryjnie produkowanym samochodzie.

Uwagi i komentarze

Lektura rozprawy generuje następującą listę uwag i komentarzy:

1. Od strony redakcyjnej, pożądane jest rozpoczęcie rozprawy od bardzo krótkiego „Streszczenia" (polskie, angielskie) oraz podania słów kluczowych.
2. Autor rozprawy wskazuje umieszczenie kodów źródłowych oraz wyników badań na platformie GitHub pod adresem: https://github.com/PatrykPankiewicz/Materialy (patrz str. 12). Recenzentowi nie udało się znaleźć wskazanej kolekcji. Nie jest to poważny mankament, bowiem zarówno kody jak i wyniki badań są równocześnie umieszczone w rozprawie.

3. Bibliografia jest obszerna, lecz przygotowana nieprofesjonalnie. Jest ułożona niealfabetycznie co do nazwisk, być może według kolejności cytowania w pracy (co jeśli cytowania są wielokrotne?). Styl pozycji bibliograficznych jest niejednolity, głównie pełne_imię+nazwisko, czasami prof. XXX (patrz np. [10]). Ostatecznie utrudnia to analizę samej bibliografii. Ponieważ praca jest napisana w TeX, to sugeruję obejrzeć portal scholar.google.pl dla poprawnego cytowania każdej publikacji (see link „cite").

Ogólna wiedza kandydata

W rozprawie omówiono kompleksowo problematykę tworzenia i modyfikacji programowania w przemyśle motoryzacyjnym, z punktu widzenia standardów, bezpieczeństwa, użytkownika jak i producenta oprogramowania. Doktoranta postrzegam jako jednego z ekspertów w obszarze dziedziny oprogramowania dla przemysłu motoryzacyjnego. Praca dostarcza dobrą wiedzy i analizę syntezę stanu badań oraz wyczerpujące kompendium wiedzy na wymienione wcześniej tematy. Uważam, że w kontekście pracy, wiedza kandydata jest nie tylko udowodniona rozprawą, ale także wyjątkowo szeroka.

Ważniejsze osiągnięcia zawarte w rozprawie

Za ważniejsze osiągnięcia Autora zawarte w rozprawie uważam:

1: identyfikacja kluczowych problemów oprogramowania w przemyśle motoryzacyjnym,

2: zaproponowanie pakietu rozwiązań dla problemów badawczych

3: zaprojektowanie i przeprowadzenie badań empirycznych

4: odniesienie do norm międzynarodowych

Reasumując, pragnę również podkreślić następujące elementy rozprawy:

A: rozprawa analizuje istotną klasę problemów występujących w przemyśle motoryzacyjnym,

B: rozprawa zawiera konstruktywne propozycje rozwiązania postawionych problemów

C: Autor posiada dużą wiedzę i dojrzałość w samodzielnym rozwiązywaniu trudnych zagadnień, projektowaniu algorytmów i prowadzeniu badań eksperymentalnych.

D: rozprawa łączy badania naukowe z przemysłem, zatem spełnia założenia doktoratu wdrożeniowego

Ocena końcowa

Uważam, że mimo pewnych mankamentów redakcyjnych rozprawa mgra. inż. Patryka Pankiewicza spełnia wszystkie wymagania stawiane rozprawom doktorskim w aktualnej Ustawie z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz stopniach i

tytule w zakresie sztuki z późniejszymi zmianami. Przedstawione w pracy wyniki stanowią niewątpliwie oryginalne rozwiązanie istotnego problemu naukowego-badawczego. Rozprawa wykazuje także ogólną wiedzę teoretyczną Kandydata w dyscyplinie informatyka techniczna i telekomunikacja oraz umiejętność samodzielnego prowadzenia pracy naukowej.

Wnioskuje o przyjęcie recenzowanej pracy doktorskiej i dopuszczenie mgra. inż. Patryka Pankiewicza do dalszych etapów przewodu doktorskiego, w tym do publicznej obrony pracy.

Czesław Smutnicki