Wpł. RDITT-3.02.2023
M. Sikora

Warszawa, 21 stycznia 2023 r.

Prof. dr hab. inż. Ewa Niewiadomska-Szynkiewicz
Wydział Elektroniki i Technik Informacyjnych
Politechnika Warszawska
ewa.szynkiewicz@pw.edu.pl

RECENZJA ROZPRAWY DOKTORSKIEJ DLA RADY DYSCYPLINY INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA POLITECHNIKI ŚLĄSKIEJ

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

Autor rozprawy: mgr inż. Patryk Pankiewicz

1. Ogólna charakterystyka rozprawy. Cel badań.

Systematycznie wzrastający poziom złożoności oprogramowania instalowanego w pojazdach samochodowych powoduje, iż coraz trudniej jest zagwarantować jego niezawodność, odporność na błędy oraz ataki zewnętrzne, w tym cyberzagrożenia. Można spodziewać się, że w najbliższej przyszłości, wraz z rozwojem technologii informacyjnych i zwiększaniem się liczby usług oferowanych za pomocą nowoczesnych narzędzi informatycznych integrujących sprzęt i oprogramowanie, problem zapewnienia bezpieczeństwa systemów wbudowanych będzie narastał. W przypadku samochodów efektem błędnie działającego oprogramowania jest bezpośrednie zagrożenie zdrowia i życia użytkowników.

Przedmiotem badań udokumentowanych w rozprawie są metody, techniki i narzędzia informatyczne wspomagające proces tworzenia oprogramowania systemów wbudowanych stosowanych w samochodach osobowych. Uwaga koncentruje się na oprogramowaniu zgodnym ze standardem AUTOSAR (AUTomotive Open System Architecture). Celem jest poprawa jakości kodu oraz podniesienie poziomu niezawodności i bezpieczeństwa w rozumieniu powszechnie uznanych norm międzynarodowych ISO 25010, ISO 26262, ISO 21434. Cel ten jest konsekwentnie realizowany, począwszy od identyfikacji problemów występujących w procesie tworzenia oprogramowania, przez opis metod i środowisk badawczych, po prezentację wykonanych przez Doktoranta praktycznych narzędzi do poprawy jakości oprogramowania oraz podniesienia poziomu jego niezawodności i bezpieczeństwa.

Realizując zadania badawcze związane z osiągnięciem celu rozprawy Doktorant sformułował następującą tezę (str. 9):

„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, ISO 21434."

Słuszność tezy została potwierdzona wynikami testów laboratoryjnych oraz wdrożeniem opracowanych i wykonanych narzędzi w firmach komercyjnych.

Rozprawa została zrealizowana w ramach programu doktoratów wdrożeniowych. Ma więc głównie charakter konstrukcyjny i doświadczalny. Rozważania teoretyczne koncentrują się na zdefiniowaniu głównych problemów występujących w procesie tworzenia oprogramowania, któremu stawia się wysokie wymagania odnośnie niezawodności i gwarancji bezpieczeństwa. Część konstrukcyjna pracy obejmuje opracowanie i realizację zestawu narzędzi wspierających tworzenie oprogramowania i automatyzację tego procesu. Część doświadczalna zawiera wyniki analiz kodu oraz eksperymentów, a także podsumowanie efektów wdrożenia rozwiązań. Doktorant osiągnął założony cel oraz potwierdził ogólną słuszność podjętych przez siebie badań.

W dobie upowszechniania się usług cyfrowych w dziedzinie motoryzacji i jednocześnie rosnącej liczby ataków cybernetycznych, uważam podjętą w rozprawie problematykę za bardzo aktualną i istotną, zarówno z poznawczego, jak i praktycznego punktu widzenia.

2. Syntetyczna analiza treści rozprawy. Charakter rozprawy

Zasadnicza część rozprawy składa się z sześciu rozdziałów. Rozdział pierwszy zawiera wprowadzenie w tematykę pracy. Obejmuje przedstawienie kontekstu rozważanego zagadnienia, główny cel pracy i cele szczegółowe, uzasadnienie podjętego problemu badawczego oraz jego usytuowanie na tle aktualnego stanu badań. Zawarty w nim materiał stanowi punkt wyjścia dla treści prezentowanych w dalszej części pracy.

W rozdziale drugim Doktorant opisał proces wytwarzania oprogramowania systemów wbudowanych stosowanych w pojazdach. Zaprezentował model referencyjny tego procesu (ASPICE – Automotive Software Process Improvement and Capability Determination) oraz przedstawił uwagi dotyczące tego modelu i jego wdrożenia bazując na własnych doświadczeniach w pracy z tym modelem. Omówił również proces tworzenia oprogramowania, przy założeniu wielowarstwowej weryfikacji, gdzie każda faza koncepcyjna jest odpowiednio sprawdzana pod względem postawionych wymagań (V-Model). Następnie, uwaga została skoncentrowana na przyjętych w przemyśle motoryzacyjnym standardach i stosowanych normach. Autor opisał szczegółowo standard AUTOSAR definiujący wysokie wymagania na jakość i bezpieczeństwo, w tym cyberbezpieczeństwo. Jest to standard stosowany m.in. w systemach czasu rzeczywistego instalowanych w urządzeniach o ograniczonych zasobach, które w znacznym stopniu decydują o bezpieczeństwie kierowcy. Ostatnia sekcja tego rozdziału została poświęcona trzem normom ISO, do których autor odwołuje się w kolejnych rozdziałach.

W rozdziale trzecim zostały zdefiniowane cztery szczegółowe problemy badawcze, wokół których koncentrowały się prace prowadzone przez Autora. Były to:

- P1: skalowalność ekstraktów diagnostycznych.
- P2: ograniczone zasoby sprzętowe.
- P3: wysoka złożoność oprogramowania.

- P4: skomplikowane ograniczenia i zależności czasowe.

W przypadku każdego problemu została krótko omówiona jego istota, sformułowane zadanie badawcze oraz zaproponowane w literaturze sposoby jego rozwiązania. Rozdział ten zawiera więc przegląd literatury, a tym samym wiedzy w zakresie metod tworzenia oprogramowania oraz dostępnych obecnie systemów informatycznych wspierających ten proces. Autor przytacza publikacje branżowe i naukowe przedstawiające problemy oraz różne podejścia i techniki wykorzystywane podczas projektowania i wytwarzania systemów wbudowanych.

Rozdział czwarty zawiera opis sześciu metod badawczych zastosowanych w pracy. Była to analiza dokumentacji i analiza statyczna kodu oraz cztery scenariusze badań eksperymentalnych wykonanych w ramach trzech projektów komercyjnych. Do badań użyto układy montowane w seryjnie produkowanych trzech modelach pojazdów: samochód średniej klasy, samochód wysokiej klasy oraz samochód elektryczny. Tworzone oprogramowanie dotyczyło tego samego typu sterownika. Przedstawiono opis stanowiska badawczego, w którym rozważano dwie architektury mikrokontrolerów, tj. PowerPC oraz ARM. Wspomniane scenariusze badań dotyczyły oceny wydajności oprogramowania, obciążenia CPU i analizy wykonania oprogramowania oraz obejmowały obserwacje działania systemu z wykorzystaniem autorskiego narzędzia - „Obserwatora".

Istotną częścią rozprawy jest rozdział piąty zawierający opis autorskiego pakietu narzędzi wspierającego proces tworzenia oprogramowania i jego automatyzację. Autor, po szczegółowej analizie dokumentacji oraz obowiązujących norm, opracował i wykonał szereg skryptów pozwalających na automatyzację tych procesów, które mogły być poddane takiej automatyzacji. Celem wytworzonych narzędzi są m.in. weryfikacja pobieranych danych oraz automatyczne generowanie kodu. Opisując wspomniane narzędzia Autor odnosi się do zdefiniowanych w rozdziale trzecim problemów badawczych oraz obowiązujących norm. Rozdział zawiera również wyniki weryfikacji, walidacji i oceny zaproponowanych rozwiązań, w tym porównanie z podejściem, gdy modyfikacje w oprogramowaniu są wprowadzane w sposób manualny.

Podsumowanie rozprawy zawiera rozdział szósty. Przedstawiono w nim również wnioski końcowe i perspektywę dalszych badań oraz rozszerzenia zakresu wdrożenia na inne urządzenia. Autor podkreśla również oryginalność przedstawionego w rozprawie rozwiązania.

3. Ocena analizy źródeł i sposobu sformułowania wniosków wynikających z analizy źródeł.

Ogółem Autor w całej rozprawie odwołuje się do 93 pozycji literatury związanych z tematyką pracy. Przegląd obejmuje liczne pozycje z ostatnich lat. Niemniej, można zwrócić uwagę, iż w prezentowanej literaturze dominują publikacje w materiałach konferencyjnych, stosunkowo niewielka część przytoczonych prac to artykuły w renomowanych czasopismach o wysokich wskaźnikach wpływu. Możliwe, że jest to uzasadnione w przypadku rozważanego obszaru badawczego.

Doktorant analizuje literaturę głównie w rozdziałach pierwszym, drugim i trzecim. Na podstawie literatury omawia obowiązujące normy i standardy, do których odnosi się w dalszych rozdziałach. Publikacje wykorzystuje również do identyfikacji i wskazania problemów badawczych. Doktorant analizuje możliwość zastosowania opisanych w pracach autorstwa innych badaczy technik i narzędzi, wskazuje na ich ograniczenia. Szkoda, że w rozdziale prezentującym własne rozwiązanie nie odniósł się do opisywanych w tych rozdziałach prac, nie porównał wskaźników ilościowych.

Przegląd literatury jest zawężony do rozwiązań koncentrujących się na tworzeniu oprogramowania zgodnego ze standardem AUTOSAR. Wskazane byłoby spojrzenie nieco szersze, dokonanie ogólnego przeglądu podejść do automatyzacji kodu również w innych zastosowaniach przemysłowych. Jednym z wskazanych przez Autora problemów jest wydajność i skalowalność oprogramowania. W przedstawionym przeglądzie źródeł brakuje odniesienia do technik zrównoleglania obliczeń. Konkretnie, nie ma głębszej analizy jak tego typu techniki wykorzystać i jakie technologie byłyby możliwe do wdrożenia w rozważanym przypadku.

Podsumowując, uważam, że mimo pewnych braków przedstawiona w rozprawie analiza źródeł oraz postawione na podstawie przeglądu wnioski świadczą o wiedzy autora w przedmiocie rozprawy. Doktorant analizuje przedstawione w literaturze podejścia i rozwiązania do wspierania tworzenia oprogramowania zgodnie z obowiązującymi standardami, formułuje zagadnienia badawcze i proponuje autorskie metody i narzędzia. Należy podkreślić, że problematyka tworzenia niezawodnego i bezpiecznego oprogramowania stanowi obszerny i dynamicznie rozwijający się nurt badań. Przeglądy literatury są z góry skazane na bycie niekompletnymi i stosunkowo szybko nieaktualnymi.

4. Analiza poprawności rozwiązania przedstawionego zadania, poprawność przyjętych założeń i wybranych metod.

Doktorant rozwiązał postawione w pracy zagadnienia. Wykorzystując wnioski z przeglądu literatury naukowej i branżowej opracował autorskie metody i narzędzia pozwalające na automatyzację tworzenia oprogramowania systemów wbudowanych w przemyśle motoryzacyjnym. Wykazał eksperymentalnie, że zaproponowane rozwiązania wpływają na jakość oraz podniesienie poziomu niezawodności i bezpieczeństwa oprogramowania. Dokonał wnikliwej analizy obowiązujących standardów i norm. Przygotował odpowiednie środowisko badawcze do prowadzenia eksperymentów w celu weryfikacji poprawności działania wykonanych autorskich narzędzi oraz oceny ich skuteczności. Wykonał liczne eksperymenty. Rezultaty badań przeanalizował pod kątem spełnienia wymagań standardów i norm ISO. Należy podkreślić, że wyniki pracy doktorskiej zostały wdrożone w trzech typach pojazdów i są komercyjnie wykorzystywane przez spółki z sektora motoryzacyjnego.

Zdaniem recenzenta przyjęte metody badawcze obejmujące przegląd norm, standardów i dokumentacji, analizę statyczną kodu oraz eksperymenty w zbudowanym środowisku badawczym, i ostatecznie walidację w środowisku docelowym są właściwe dla badanego zagadnienia. Uzyskane wyniki potwierdzają poprawność rozwiązania. Autor w rozprawie doktorskiej uzasadnia, że zaproponowana technika może skutecznie wspierać proces tworzenia oprogramowania, a uzyskane rezultaty pokazują wyższą skuteczność w stosunku do powszechnie stosowanych podejść.

5. Oryginalność rozprawy, samodzielny dorobek autora, pozycja rozprawy w stosunku do stanu wiedzy prezentowanego w literaturze światowej.

Rozprawa zawiera nowe oryginalne rezultaty. Do szczególnie ważnych należy zaliczyć:

- zaproponowaną metodykę obejmującą szereg działań skutkujących podniesieniem jakości oraz poziomu bezpieczeństwa oprogramowania zgodnego z standardem AUTOSTAR,
- metodę i narzędzia do automatyzacji tworzenia oprogramowania przetwarzającego dane diagnostyczne w systemach zgodnych ze standardem AUTOSTAR,

- metodę i narzędzia do automatyzacji tworzenia infrastruktury logowania danych w komponentach oprogramowania umożliwiającą szybkie pozyskiwanie danych o działaniu systemu,
- metodę i narzędzia do ciągłej kontroli zużywanej pamięci, w sytuacji wielokrotnych, jednoczesnych zapisów z wielu komponentów oraz algorytm równoważenia zapisów,
- projekt i wykonanie autorskiego obserwatora systemu.

Przedstawione wyniki mają istotne znaczenie dla tworzenia oprogramowania gwarantującego wysoki poziom niezawodności i bezpieczeństwa.

6. Analiza poprawności prezentacji wyników pracy

Recenzowana rozprawa doktorska liczy 164 strony, zawiera 24 rysunki, 18 tabel, 14 kodów źródłowych, oraz bibliografię obejmującą 93 publikacje. Zasadnicza treść obejmuje 142 stron, pozostałe zawierają spis treści, wykaz rysunków, kodów, skrótów i terminów oraz bibliografię.

Praca jest bardzo techniczna, więc dobrym rozwiązaniem było wprowadzenie rozdziału, w którym Autor szczegółowo definiuje rozważane problemy badawcze (rozdz. 3), do których odnosi się przy okazji omawiania opracowanych przez siebie rozwiązań. W rozdziale 5 brakuje ogólnego schematu architektury z zaznaczonymi blokami, w których Autor ulokował napisane przez siebie skrypty. Poza tym praca jest zredagowana dość starannie, zarówno pod względem językowym, jak i graficznym. Występują pewne błędy językowe, gramatyczne i redakcyjne, ale nie wpływają one w sposób istotny na jakość tekstu. Czasami pojawiają się kontrowersyjne, niezbyt zrozumiałe lub nieprecyzyjne sformułowania, np. „aspekty identyfikowalności" (str. 33), „analiza czasowa oprogramowania" (str. 37) – czy Autor miał na myśli wydajność?, „w systemie przetwarzania równoczesnego" (str. 37) – czy chodziło o przetwarzane równoległe, czy też współbieżne, „Jak zarządzać .... ograniczeniami czasowymi?" (str. 45) – czy chodzi w tym przypadku o równoważenie obciążeń? Autor wielokrotnie dotyka problemów typowych dla przetwarzania równoległego, tj. równoważenie obciążeń, alokacja zadań, wydajność. Konsekwentnie jednak unika używania tych pojęć. Ich wykorzystanie poprawiłoby czytelność pracy. Na rysunku 2.2 w opisach bloków mamy słowo „weryfikacja". Podpis rysunku mówi o wielowarstwowej walidacji kodu. Nie jest oczywiste czy prezentowany proces dotyczy weryfikacji, czy też walidacji oprogramowania. Oba słowa mają w tym kontekście inne znaczenie.

Układ oraz zawartość większości rozdziałów są generalnie prawidłowe, aczkolwiek niektóre z nich mogłyby być nieco lepiej napisane. Opisy są czasami chaotyczne. W rozprawie, która nie jest zbiorem artykułów, nie wydaje się zasadne jawne wskazywanie przez podtytuły typu „Analizy wykonane w ramach artykułu badawczego", że dane rozwiązania zostały opublikowane. Wystarczyło się odwołać do tych prac. Ponadto, brakuje rozdziału w całości poświęconego ogólnej prezentacji opracowanej i wdrożonej przez Autora metodyki wspierania procesu tworzenia bezpiecznego i niezawodnego oprogramowania systemów wbudowanych.

Zastrzeżenia można zgłosić do opracowania bibliografii – wskazana byłaby większa staranność. W przypadku większości publikacji konferencyjnych brakuje numerów stron, w innych (np. praca [8]) oraz książkach Doktorant nie podaje nazwy wydawnictwa.

7. Słabe strony rozprawy i jej główne wady

Rozprawa doktorska została wykonana w ramach doktoratu wdrożeniowego, niemniej można byłoby oczekiwać większego wkładu w rozwój badań naukowych. Główny nacisk jest położony na zagadnienia inżynierskie, co w przypadku doktoratu wdrożeniowego nie należy traktować jako błędne działanie. Niemniej, wydaje się, że był, w zakresie rozważanej problematyki, potencjał na rozwinięcie wątku badawczego. Za główną słabą stronę rozprawy uważam brak opracowania przez Autora, w miarę możliwości, uniwersalnej metodyki wspierania procesu tworzenia oprogramowania instalowanego w urządzeniach, w tym w przemyśle motoryzacyjnym. Wskazane by było przedstawienie w sposób uporządkowany kolejnych działań, wraz z oceną ryzyka, ograniczeń, zagrożeń oraz szacowanych zgrubnie kosztów i czasochłonności. Opisy większości z wspomnianych elementów metodyki znajdują się w rozprawie, w różnych rozdziałach (rozdziały 3, 4, 5). Brakuje jednak rozdziału wprowadzającego, ilustrującego proponowane przez Autora kompleksowe podejście do rozwiązania postawionego problemu badawczego.

Drugi słaby punkt wiąże się z niemożliwością oceny przez recenzenta wysiłku włożonego w przygotowane oprogramowanie (wykonane skrypty), które stanowią istotny wkład Autora. Doktorant prezentuje części kodów źródłowych lub ich ogólne wzorce, tłumacząc niemożliwość przedstawienie pełnego kodu tajemnicą handlową instytucji wdrażającej. Na tej podstawie dość trudno zweryfikować recenzentowi poprawność rozwiązania. Pozostaje akceptacja deklaracji złożonych przez Doktoranta, że skrypty zostały wdrożone i poprawnie realizują założone zadania.

Ponadto Autor nie zawsze dostatecznie precyzyjnie wskazuje na to, co stanowi jego oryginalne osiągnięcie. W rozdziale 1.1 wymienia szczegółowe cele badawcze, w rozdziale podsumowującym (rozdział 6) omawia wykonane prace. Niemniej, wskazane byłoby wypunktowanie w rozdziale 1.3 lub rozdziale 6 głównych osiągnięć będących wynikiem prac badawczych prowadzonych w ramach doktoratu.

8. Przydatność rozprawy dla nauk technicznych

Mimo wymienionych powyżej słabych stron pracy uważam, że przedstawione w rozprawie wyniki wnoszą istotny wkład w dyscyplinę informatyka techniczna i telekomunikacja, a konkretnie w rozwój badań w zakresie projektowania i wytwarzania oprogramowania systemów wbudowanych wykorzystywanych w przemyśle motoryzacyjnym. Opracowane i wykonane rozwiązania zostały wdrożone w pojazdach o różnych charakterystykach i wymaganiach. Wykonane eksperymenty badawcze pokazują ich znaczną skuteczność i efektywność.

9. Podsumowanie i wniosek końcowy

Uważam, że rozprawa mgr inż. Patryka Pankiewicza spełnia wymagania stawiane rozprawom doktorskim, w tym doktoratom wdrożeniowym, przez przepisy ustawy o tytułach i stopniach naukowych. Stawiam wniosek o przyjęcie rozprawy i dopuszczenie do obrony doktorskiej.

podpis