RDITT-25.01.2023
M. Skow

Warszawa, 19.01.2023

dr hab. inż. Janusz Furtak

Wydział Cybernetyki
Wojskowa Akademia Techniczna

Recenzja rozprawy doktorskiej

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

Autor rozprawy: **mgr inż. Patryk Pankiewicz**

Promotor rozprawy: **dr hab. inż. Andrzej Białas, prof. Łukasiewicz_EMAG**

Dziedzina: **nauki techniczne**

Dyscyplina: **Informatyka Techniczna i Telekomunikacja**

1. Cel, zakres i charakter rozprawy

Recenzowana rozprawa jest dość obszerna, ma 164 strony tekstu, który został podzielony na 6 rozdziałów zasadniczych. Zawiera także spis rysunków, listę kodów źródłowych, słownik skrótów ze skorowidzem, słownik terminów ze skorowidzem i wykaz cytowanej literatury.

Rozdział pierwszy stanowi krótkie wprowadzenie, w którym przedstawiono cele pracy, tezę rozprawy oraz opis pracy. W tym rozdziale autor zadeklarował, że przedstawiana praca została wykonana w ramach programu doktoratów wdrożeniowych.

Głównym celem pracy było opracowanie metody wspomagającej proces tworzenia oprogramowania dla systemów wbudowanych stosowanych w samochodach osobowych wykorzystujących standard AUTOSAR Classic. Osiągnięcie celu głównego warunkowały cele szczegółowe, do których można zaliczyć:

- zidentyfikowanie elementów istotnie wpływających na jakość oprogramowania samochodowych komponentów, które pracują w czasie rzeczywistym i mają istotny wpływ na bezpieczeństwo użytkowników ruchu (szczególnie w zakresie występujących podatności);

- opracowanie odpowiednich architektur i cząstkowych rozwiązań zapewniających ograniczanie ryzyka występowania błędów, podnoszenie jakości oprogramowania i zwiększanie bezpieczeństwa całego systemu;
- zidentyfikowanie najbardziej wrażliwych obszarów w trakcie projektowania systemów wbudowanych;
- ulokowanie rozwiązań w modelu jakości oprogramowania opisanego w normie ISO 25010 z uwzględnieniem norm bezpieczeństwa funkcjonalnego ISO 26262 i cyberbezpieczeństwa ISO 21434.

W dzisiejszych czasach każdy nowo wyprodukowany samochód jest wyposażony w komputer pokładowy, którego zadania są bardzo liczne i z pewnością obejmują zadania związane z szeroko rozumianym bezpieczeństwem uczestników ruchu, diagnostyką komponentów pojazdu, wspomaganiem kierowcy, a także różnymi usługami ułatwiającymi podróżowanie pasażerów. Tego typu systemy zwykle mają ograniczone zasoby pamięci i mocy obliczeniowej, są bardzo skomplikowane i wytwarzane przez różne i bardzo liczne zespoły tworzące rozwiązania programowe i sprzętowe. Bardzo dużym wyzwaniem jest proces integracji poszczególnych komponentów takiego systemu. Jednym ze środków ułatwiających tworzenie tego typu rozwiązań jest stosowany powszechnie standard AUTOSAR. Autor rozprawy, który zawodowo od wielu lat zajmuje się tą problematyką, zwrócił uwagę, że wiele procedur bazujących na tym standardzie obejmuje szereg czynności wykonywanych manualnie przez integratorów tego typu systemów, co jest źródłem wielu problemów we wdrażaniu i użytkowaniu tego typu systemów. Wiele wyzwań dotyczy również fazy eksploatacji takiego systemu szczególnie w obszarze dużych wymagań czasowych dla realizacji poszczególnych zadań i ograniczonych zasobów sprzętowych systemu.

Przeprowadzone w rozprawie badania dotyczą istotnych elementów procesu wytwarzania systemów wbudowanych i skupiają się na następujących problemach:

1) skalowalność tzw. ekstraktów diagnostycznych w projektach wykorzystujących standard AUTOSAR Classic;
2) minimalizowanie zużycia zasobów sprzętowych przez wybrane komponenty oprogramowania w projektach wykorzystujących standard AUTOSAR Classic;
3) minimalizowanie skutków dynamicznego wzrostu złożoności oprogramowania systemów wbudowanych ze szczególnym uwzględnieniem rosnącego rozmiaru kodu, liczby interfejsów, liczby podsystemów i różnych technik wytwarzania poszczególnych komponentów oprogramowania przez różne zespoły;
4) zarządzanie skomplikowanymi zależnościami i wyrafinowanymi ograniczeniami czasowymi.

Problematyka rozprawy jest niezwykle ważna dla rynku motoryzacyjnego ze względu na bezpieczeństwo. Wystąpienie awarii może narazić na szwank życie bądź zdrowie ludzi albo wyrządzić olbrzymie straty materialne. Jakość diagnostyki tego typu systemów ma decydujące znaczenie dla niezawodnego i bezpiecznego ich użytkowania. Projektanci tego typu systemów muszą już na etapie ich projektowania uwzględnić szereg czynników i rozwiązań, które umożliwią identyfikację, w czasie zbliżonym do rzeczywistego, stanów awaryjnych systemu mogących stwarzać zagrożenie. Rozpatrywane w rozprawie zagadnienia mieszczą się w kilku obszarach badawczych dyscypliny Informatyka Techniczna i Telekomunikacja. Należą do nich: projektowanie systemów wbudowanych, diagnostyka systemów, systemy czasu rzeczywistego, wiarygodność i bezpieczeństwo systemów.

Praca ma charakter wdrożeniowy. Rozpatrywane w niej zagadnienia są bezpośrednio powiązane z projektami systemów wbudowanych dla samochodów. Badania i weryfikacja zaproponowanych rozwiązań były przeprowadzone z wykorzystaniem trzech komercyjnych systemów. Niestety w pracy nie ma informacji jakich konkretnych systemów to dotyczy. Taka sytuacja jest tłumaczona przez Doktoranta poufnością rozwiązań komercyjnych.

Pierwszy z tych systemów był poligonem doświadczalnym, który był wykorzystywany w szczególności do identyfikowania problemów. W drugim systemie potwierdzono spostrzeżenia z badań pierwszego systemu i wprowadzone wstępne rozwiązania problemów. W trzecim systemie zostały wdrożone i przebadane wszystkie rozwiązania przedstawione w pracy. Warto zaznaczyć, że zaproponowane rozwiązania bazują na uznanych międzynarodowych standardach, opracowane dodatkowe wymagane struktury danych są przygotowane w formacie ARXML i pozostają otwarte do wykorzystania w innych dziedzinach, w których są stosowane systemy wbudowane.

2. Zawartość rozprawy

Zasadnicze treści rozprawy zostały zawarte w 4 rozdziałach (rozdziały od drugiego do piątego).

W rozdziale drugim zostały przedstawione dwa modele (ASPICE i V-Model) procesów tworzenia oprogramowania w przemyśle motoryzacyjnym, standardy technologiczne (AUTOSAR Classic, MISRA C i HIS) oraz krótko opisano międzynarodowe normy dotyczące jakości i bezpieczeństwa oprogramowania.

W rozdziale trzecim zidentyfikowano cztery istotne problemy występujące w procesie tworzenia oprogramowania. Należą do nich:

- skalowalność ekstraktów diagnostycznych tzn. pewnych struktur danych wymaganych dla procedur diagnostycznych, których liczba może osiągać setki egzemplarzy – dla każdego ekstraktu trzeba przygotować odpowiednie oprogramowanie;
- ograniczone zasoby sprzętowe, które dotyczą rozmiaru pamięci RAM, ROM i NVRAM oraz mocy obliczeniowej i obciążenia magistral komunikacyjnych;
- duża złożoność oprogramowania rozumiana jako liczba modułów, bibliotek i funkcji, których wytwórcą są rożne zespoły programistów;
- wyrafinowane ograniczenia i zależności czasowe występujące pomiędzy różnymi komponentami systemu.

Każdy problem został opisany i dla każdego problemu przedstawiono dotychczasowy sposób rozwiązywania tych problemów w świetle dotychczasowych badań i opracowań naukowych.

Rozdział czwarty został poświęcony opisowi stanowiska badawczego, krótkiej charakterystyce trzech komercyjnych projektów oraz sześciu metodom badawczym, które były wykorzystywane w pracy.

Kluczowe treści dla postawionej w rozprawie tezy zostały omówione w rozdziale 5. W tym rozdziale przedstawiono pakiet czterech rozwiązań poprawiających jakość i bezpieczeństwo oprogramowania dla systemów wbudowanych wykorzystujących standard AUTOSAR Classic. Należą do nich:

- automatyzacja stosu diagnostycznego – zastąpienie manualnego tworzenia kodu przez generowanie kodu na poziomie około 90%;
- automatyzacja i architektura DLT – wprowadzenie trybu „non-verbose" przy tworzeniu logów systemowych skutkuje zmniejszeniem wolumenu przesyłanych danych przez magistrale systemowe i zmniejszenie rozmiaru pamięci Flash do przechowywania tych danych na poziomie przekraczającym 90%;
- automatyzacja i obsługa pamięci NVRAM – likwidacja sytuacji braku pomiarów i zmniejszenia czasu zapisu i odczytu;
- obserwator systemu – ciągłe monitorowanie zachowania oprogramowania i zależności czasowych oraz tworzenie dodatkowych zapisów w logach systemu w newralgicznych chwilach działania systemu.

Opis każdego narzędzia obejmuje odniesienie do opisanych w rozdziale problemów i zagadnień badawczych, sposób rozwiązania problemu badawczego, walidację i ocenę zaproponowanego rozwiązania oraz odniesienie do norm jakości, bezpieczeństwa i zabezpieczeń. Każdy opis rozwiązania kończy pakiet wiedzy i wzorców projektowych dla

inżynierów oprogramowania, co jest bardzo cenne z punktu widzenia łatwości korzystania z narzędzi przez różnych wytwórców.

Rozdział szósty stanowi podsumowanie rozważań oraz wyników badań. Przedstawione są w nim wnioski z przeprowadzonych prac, zdobyte doświadczenia krytyczna ocena zaproponowanych rozwiązań.

3. Ocena poprawności i oryginalności postawionej tezy oraz stopnia, w jakim została ona wykazana

Sformułowaną w rozprawie tezę pracy w brzmieniu:

„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."

należy uznać za oryginalną i trafną. Jedyną wątpliwość budzi nie treść tezy, a sformułowanie tematu pracy i co za tym idzie, sformułowanie tezy. Trudno jest mi uznać, że „pakiet rozwiązań stanowi metodę". Raczej Doktorant opracował metodę, w której w specjalny sposób wykorzystuje przygotowane narzędzia. Przecież mając do dyspozycji takie narzędzia jak np. łopata, grabie, konewka i nawet wiedząc jak każde z tych narzędzi używać, nie będziemy jeszcze w stanie skutecznie uprawiać tulipanów.

Niezależnie od użytego sformułowania potwierdzam prawdziwość tezy. Taką myśl potwierdza również fakt, iż uznane na świecie podejście do budowania systemów wbudowanych dla samochodów bazujące na standardzie AUTOSAR Classic pomimo niedostatków wykazanych przez Doktoranta jest użytkowane. Dlatego należy uznać, że rozwiązania zaproponowane przez Doktoranta, które w istotny sposób poprawiają dotychczas stosowane rozwiązania jest dużym osiągnięciem Doktoranta, które będzie oddziaływało na przemysł motoryzacyjny. Wdrożenie zaproponowanych rozwiązań w „projekcie nr 3" jest kolejnym potwierdzeniem tego faktu.

Nieliczne ważniejsze uwagi natury merytorycznej są przedstawione poniżej:

1) Pewnym problemem w rozprawie jest nazewnictwo i często niekonsekwentne używanie pojęć. Należą do nich:
   - wspomniane wcześniej utożsamiane pakietu opracowanych narzędzi z metodą;
   - „stos NvM" – brakuje definicji pojęcia. Po lekturze pracy oznacza to chyba pamięć nieulotną, ale pojawiają się sformułowania mówiące o „funkcjach stosu NvM" (np. w podpisie Kod źródłowy 5.10, a także na str. 102), o „skomplikowanej

architekturze NvM" (str. 101), a także o „analizie stosu NvM" (str. 101). Używanie takich pojęć bardzo utrudnia zrozumienie treści pracy.

- w treści pracy używane są polskojęzyczne pojęcia np. „ekstrakt diagnostyczny" (str. 60), „Weryfikacja danych", „Generowanie kodu". Do zilustrowania często są używane np. diagramy (odpowiednio na Rysunek 5.1, Rysunek 5.4), na których jest treść w języku angielskim. Nie jest to błędem, ale praca byłaby bardziej klarowna, gdyby Doktorant podawał w treści angielskie odpowiedniki polskich pojęć.
- Tablica 5.7. Pojawiają się pojęcia: „liczba wiadomości", „ilość logów (tekstu)" i „Liczba logów (wiadomości)". Tym pojęciom towarzyszą pewne liczby i są podane też wartości procentowe. Nie wiadomo, skąd to się wzięło i jak to interpretować.

  W podpisie tablicy 5.7 jest też mowa o największych komponentach programowych oznaczonych enigmatycznie przez SWC1, SWC2 i SWC3 – też nie wiadomo o jakie oprogramowanie chodzi.

2) W kilku miejscach w pracy Dyplomant podaje zanonimizowane wyniki powołując się na tajemnicę przedsiębiorstwa – to jest zrozumiałe. Jednak tak podane wyniki nie pozwalają ocenić wartości rozwiązania bez szerszego komentarza ze strony autora pracy. Przykładami takiej sytuacji jest kod źródłowy 5.2, 5.3, 5.13. Tutaj warto zaznaczyć, że ochronie podlega całe oprogramowanie, natomiast zaprezentowanie tylko pewnego małego oryginalnego wycinka tego oprogramowania z pewnością nie ujawni tajemnicy, a zdecydowanie lepiej zilustruje problem.

   Z podobnego powodu w pracy nigdzie nie umieszczono wykonanych przez autora skryptów, ani nawet krótkiego opisu jak one działają. Udostępnienie źródeł tych skryptów bez żadnych komentarzy na platformie „github", tylko w pewnym stopniu łagodzi problem oceny wkładu pracy Doktoranta.
3) W podrozdziale 5.2.2 powinien być umieszczony diagram pokazany na rysunku 5.10. Nie pojawiałyby się wtedy pytania dotyczące tworzonego pliku konfiguracyjnego, o którym mowa na stronie 92.

Po zapoznaniu się z treścią pracy pojawiają się następujące pytania:

1) Gdy statycznie analizowany jest kod programu, to jakie znaczenie ma liczba linii komentarzy? (dane w tabeli 5.1)
2) W diagramie na rysunku 5.4 występują dwa bloczki opisane jako „Code Generation" i „Generation". Wynikiem ich działania są pliki DiagApplTemplate.o i RteDiagApplTemplate.h. Czym różnią się te dwa bloczki?

3) W tablicy 5.10 podano wiele danych odnoszących się do bajtów. Na koniec podano „estymowaną żywotność pamięci" w latach. Pytanie: jak przelicza się podane w tabeli dane na lata?
4) Jak rozumiane jest pojęcie „wolnobieżności kodu", o którym mowa na stronie 108?

4. Analiza wykorzystanych źródeł

Cytowana w rozprawie literatura obejmuje 93 pozycje. W większości są to aktualne i znaczące dla problematyki rozprawy pozycje literatury światowej, które obejmują szereg istotnych obszarów wiedzy w dyscyplinie Informatyka Techniczna i Telekomunikacja

Analiza literaturowa przeprowadzona w rozprawie wskazuje na dobrą orientację i wystarczającą wiedzę Autora w dyscyplinie naukowej Informatyka Techniczna i Telekomunikacja. Autor dość obszernie i bardzo wnikliwie analizuje pozycje literaturowe dotyczące zagadnień rozpatrywanych w pracy. Warto odnotować, że wśród podanej listy publikacji występują cztery publikacje, których jedynym autorem jest Doktorant. Dwie z tych publikacji ukazały się w latach 2021 i 2022 w materiałach konferencji International Conference on Dependability of Computer Systems [DEPCoS] – ta konferencja jest umieszczona na liście punktowanych czasopism i konferencji.

5. Znaczenie uzyskanych wyników dla danej dyscypliny naukowej

Efektem przeprowadzonych badań i eksperymentów jest metoda wykorzystania czterech narzędzi do zwiększenia jakości i bezpieczeństwa oprogramowania dla samochodowych systemów wbudowanych. Każde z tych narzędzi ma inne własności i inne przeznaczenie. Bardzo istotnym jest to, że opracowane narzędzia wkomponowują się procesy tworzenia oprogramowania zdefiniowane w uznanych i powszechnie stosowanych standardach (AUTOSAR Classic) i zdecydowanie przyczyniają się do poprawienia jakości i bezpieczeństwa oprogramowania w zakresie generowania spójnego oprogramowania diagnostycznego, efektywnego tworzenia logów systemowych i wykorzystania zasobów pamięci Flash i NVRAM, efektywne zarządzanie obszernym i często modyfikowanym oprogramowaniem systemu i stałe monitorowanie działania oprogramowania.

Największe znaczenia ma fakt wdrożenia zaproponowanych rozwiązań w projekcie oznaczonym w pracy jako projekt nr 3, chociaż to moje stwierdzenie bazuje tylko na zapisach w treści pracy (np. na str. 52). Nie znalazłem w pracy jakiegokolwiek dokumentu potwierdzającego takie wdrożenie.

6. Ocena strony formalnej rozprawy

Strona formalna pracy jest najsłabszym elementem pracy. Strona edycyjne pracy nie budzi większych zastrzeżeń. Jednak pracę czyta się trudno. Przyczyniają się do tego niedostatki sygnalizowane w sekcji nr 3 recenzji. Inne uwagi natury formalnej są przedstawione poniżej:

1) Niepoprawne użycie określenia „funkcjonalność", gdy z kontekstu wynika, że mowa jest o „funkcji". Przykłady można znaleźć na stronach 7, 56, 128 i 140.
2) Niepoprawne użycie określenia „ilość" zamiast „liczba" w odniesieniu do rzeczowników policzalnych. Przykłady można znaleźć na stronach 46, 57, 89, 97, 107, 140.
3) Wątpliwym jest używanie sfomułowania „ilość informacji" w stosunku do wolumenu danych podanego w bajtach. Przykłady można znaleźć na stronach 136, 137, 138.
4) Niepoprawne użycie określenia „posiada" zamiast „ma" lub „dysponuje". Przykłady niepoprawnego użycia: „obszar ... posiada ... wady lub luki" (str. 9), „systemy czasu rzeczywistego ... posiadają największe wymagania (str. 19), „największe ograniczenia ... posiada platforma AUTOSAR" (str. 20). Inne przykłady można znaleźć na stronach 22, 28, 46, 88, 98,128, 131,139.
5) Niepoprawne użycie określenia „optymalizowanie" zamiast „poprawianie" (str. 39).
6) Niepoprawne użycie określenia „w szybkim czasie" zamiast „w krótkim czasie" (str39).
7) Dziwne sformułowanie „stos NvM jest wykonywany tylko z jednego miejsca" (str. 108).
8) Przy redagowaniu tekstu w języku polskim nie pozostawia się pojedynczych liter na końcu linii.

Niezależnie od stwierdzonych uchybień pozytywnie oceniam umiejętności Autora rozprawy w zakresie poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników.

7. Podsumowanie oceny rozprawy

W podsumowaniu oceny rozprawy stwierdzam, że opiniowana praca w odpowiada wymaganiom stawianym rozprawom doktorskim ze względu na dobry poziom merytoryczny oraz osiągnięcia w zakresie wdrażania rozwiązań w przemyśle samochodowym. Praca stanowi dobry przykład połączenia zastosowania metod naukowych do rozwiązywania problemów w zakresie projektowania i eksploatacji samochodowych systemów wbudowanych.

Opiniowaną rozprawę doktorską oceniam pozytywnie.

Konkluzja

Uważam, że opiniowana rozprawa stanowi oryginalne rozwiązanie problemu naukowego oraz potwierdza ogólną wiedzę teoretyczną i praktyczną Doktoranta w dyscyplinie naukowej Informatyka

Techniczna i Telekomunikacja, a także dowodzi umiejętności prowadzenia przez Niego samodzielnej pracy naukowej.

W oparciu o przedstawioną powyżej ocenę potwierdzam, że opiniowana praca spełnia wymagania stawiane rozprawom doktorskim, określone w Ustawie z dnia 20 lipca 2018 r. (Prawo o szkolnictwie wyższym) (Dz. U. Nr 2018, poz. 1668, z późn. zm.) i w związku z tym **wnioskuję o dopuszczenie mgr. inż. Patryka Pankiewicza do publicznej obrony rozprawy doktorskiej**. Chociaż wydaje mi się, że w dalszych krokach procedury Doktorant powinien przedstawić jakiekolwiek potwierdzenie faktu wdrożenia opracowanych rozwiązań. Zwracam uwagę na to, że moje spostrzeżenia bazują tylko na opisie przygotowanym przez Doktoranta i mojej wierze słowo tam zapisane.