Gliwice 30.09.2022

Promotor pracy:

dr hab.inż. Andrzej Białas, prof. Łukasiewicz-EMAG

Autor pracy:

mgr inż. Patryk Pankiewicz

Streszczenie

rozprawy doktorskiej pt. „Jakość i bezpieczeństwo oprogramowania w przemyśle motoryzacyjnym – analiza standardów oraz opracowanie metody wspomagającej proces tworzenia oprogramowania”

Nowoczesne samochody to o wiele więcej niż tylko środki transportu umożliwiające dostanie się do celu podróży. Dzięki rozwojowi elektroniki i oprogramowania, pojazdy oferują szereg systemów wspomagających kierowcę, multimedialne systemy ‘’Infotainment’’, systemy bezpieczeństwa itp. Producenci przescigają się w opracowywaniu kolejnych udogonień, które przekonają potencjalnego klienta do wyboru konkretnej marki. Większość innowacyjnych funkcji jest realizowana przez oprogramowanie, którego opracowanie staje się głównym kosztem przy produkcji pojazdu. Niestety wraz z ilością oprogramowania rośnie poziom jego skomplikowania i liczba potencjalnych błędów.

Przemysł motoryzacyjny wymaga zgodności z bardzo dużą ilością norm i standardów, aby zapewnić wymaganą końcową jakość produktu i uniknąć narażania użytkowników samochodów na niebezpieczeństwo. Wszystkie elementy samochodu muszą być zrealizowane zgodne z tzw. ‘’state of the art’’ czyli realizując wymagania dotyczące procesu tworzenia produktu, wymagania jakościowe, podążające za określonymi modelami i wzorcami oraz wpisujące się w odpowiednie metryki.

W celu nadążenia za potrzebami rynku, największe firmy motoryzacyjne nawiązały ścisłą współpracę i utworzyły konsorcjum AUTOSAR (AUTomotive Open System ARchitecture), które opracowało standard tworzenia oprogramowania dla systemów wbudowanych. Obecnie AUTOSAR jest stosowany w większości produkowanych seryjnie samochodów i zapewnia m.in. odpowiednią architekturę, znane przez inżynierów standardowe moduły oprogramowania oraz wiele poziomów abstrakcji dla sprzętu.

Pomimo istnienia wszystkich wymaganych norm i standardów, skala oprogramowania znacznie przekraczająca setki milionów linii kodu w pojedynczym samochodzie, stanowi nielada wyzwaznie dla wszystkich jego twórców. Wolumen produkcyjny często przekraczający setki tysięcy pojazdów, zmusza także do minimalizacji kosztów sprzętu, przez co inżynierowie muszą wykonywać wielokrotne iteracje optymalizacji oprogramowania, aby zrealizować wymagane funkcje na dostępnych platformach sprzętowych.

Autor niniejszej rozprawy proponuje pakiet rozwiązań oraz narzędzi, dedykowany dla układów wbudowanych stosowanych w pojazdach samochodowych, który stanowi metodę wspomagającą proces tworzenia oprogramowania. Autor osadza swoje rozwiązanie w projektach korzystających ze standardu AUTOSAR, aby umożliwić jego wykorzystanie jak największej liczbie inżynierów.

Tezą autora brzmi:
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 – ISO25010, ISO26262 i ISO21434.

Aby opracować pakiet rozwiązań, autor wykonuje analizę głównych elementów wpływających na jakość, bezpieczeństwo oraz cyberbezpieczeństwo oprogramowania. Zidentyfikowanymi elementami są standard AUTOSAR Classic, proces tworzenia oprogramowania ASPICE, model tworzenia oprogramowania V-Model, metryki oprogramowania HIS, standard budowanie oprogramowania MISRA oraz wymienione wcześniej normy ISO. Dzięki tej analizie, autor rozprawy wyznacza granicę jego dalszych prac badawczych.

Korzystając z wieloletniego doświadczenia w przemyśle, autor określa 4 główne problemy i zagadnienia badawcze, powiązane ze skalowalnością oprogramowania, ograniczonymi zasobami sprzętowymi, negatywnymi skutkami wysokiej złożoności oprogramowania oraz skomplikowanymi zależnościami czasowymi oprogramowania. Autor opisuje szereg metod badawczych, które są wykorzystane do przeprowadzenia badań w projektach komercyjnych. Dzięki wdrożeniowemu charakterowi doktoratu wszystkie badania i analizy zostały przeprowadzone na stanowisku badawczym używającym komercyjnych sterowników komunikacyjnych, nad którymi autor pracował jako architekt oprogramowania oraz główny architekt oprogramowania. Sterowniki te były dedykowane dla trzech kolejnych modeli samochodów jednego z największych europejskich producentów.

W celu ułatwienia nawigowania po rozprawie autor używa w pracy oznaczeń:

- P1, P2... dla problemów badawczych,
- MB1, MB2, ... dla metod badawczych,
- ZG1, ZG2, ... dla zagadnień badawczych,
- Rozwiązanie 1, Rozwiązanie 2, ... dla proponowanych rozwiązań,
- Projekt 1, Projekt 2, ... dla komercyjnych projektów badawczych.

Bazując na przeprowadzonych badaniach autor przedstawia szereg rozwiązań powiązanych z zagadnieniami badawczymi:

- koncepcję automatyzacji stosu diagnostycznego,
- koncepcję automatyzacji i architektury systemu przetwarzania logów systemowych DLT,
- koncepcję automatyzacji i architektury stosu pamięci nieulotnej NvM,
- koncepcję modułu obserwatora systemu.

Zaprezentowane rozwiązania zwiększają ilość informacji na temat działania systemu wraz z automatyczną możliwością agregracji danych. Autor przeprowadził walidację, która wykazała następujące usprawnienia: skrócenie czasu wykonywania operacji na pamięci, zmniejszenie zajętości pamięci, zmniejszenie obciążenia mikrokontrolera, skrócenie czasu integracji oprogramowania, zwiększenie czytelności kodu przez generowanie komentarzy, zwiększenie ilości automatycznie generowanego kodu źródłowego.

Kody źródłowe rozwiązań są własnością intelektualną klientów komercyjnych, dlatego autor zapewnia opracowane rozwiązania w formie wzorców projektowych i instrukcji dla innych architektów realizujących oprogramowanie wbudowane korzystające ze standardu AUTOSAR. Autor prezentuje możliwe kierunki kontyuacji badań i analiz dla każdego elementu proponowanej metody.