Gliwice 30.09.2022

Supervisor:

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

Author:

mgr inż. Patryk Pankiewicz

Abstract

doctorate dissertation „Quality and safety of automotive software – analysis of standards and definition of software development process enhancement method.”

Modern cars nowadays are so much more than just means of transportation, that enable us to get to our destination. Thanks to development of automotive electronics and software, vehicles are providing a range of driver support systems, infotainment units, safety systems, etc. The car manufacturers are competing to offer the most innovative solutions, that will attract the customers. The most of the modern functionalities are realized by software, that is rapidly becoming the main cost of car manufacturing. Unfortunately, the bigger the software base, the more complex it becomes and the more errors it potentially has.

Automotive industry is one of the most regulated and standardized markets out there, all to protect the cars quality and ensure the users of the vehicles are safe. All sub-systems of the car have to be developed in conformance with the “state-of-the-art”, meaning that they have to adhere to all process requirements, quality requirements, development models, quality metrics, international norms, etc.

In order to keep up with such a demanding environment, the biggest automotive companies have created the AUTOSAR (AUTomotive Open System ARchitecture) partnership, and developed a standard for software development. Currently AUTOSAR is required for almost all mass-produced cars and ensures appropriate architecture, common reusable sub-modules known by automotive engineers and multiple layers of software abstraction. The main idea behind AUTOSAR is „Cooperate on standards, compete on implementation”.

However, despite of all the existing norms and standards the scale of automotive embedded software, which has grown over hundreds of millions of lines of code in a single car, poses a huge challenge to all of its creators. The production volumes of over hundreds of thousands of vehicles, requires hardware costs minimization, what forces the engineers to execute multiple iterations of software optimization, to realize all required functionalities on available hardware platforms.

The author of the dissertation proposes a set of solutions and tools, dedicated for embedded software used in commercial vehicles, that forms a software development process enhancement method. The author creates the solution for projects using the AUTOSAR standard, in order to enable the most engineers to benefit from it, and be able to use it themselves.

The prosed thesis states that:
By employing the proposed set of solutions, forming the software development process enhancement method, one can enhance software quality, functional safety and cybersecurity in accordance with ISO25010, ISO26262, ISO21434 international norms.

In order to develop the set of solutions, the author analyses the main elements influencing software quality functional safety and cybersecurity. The identified elements are: the AUTOSAR standard, ASPICE software development process, V-Model software development model, HIS software metrics, software development standard MISRA and beforementioned ISO norms. Said analysis allows to establish clear boundaries of research activities.

By using his industrial experience, the author defines 4 main problems and research tasks, that are related to: software scalability, limited hardware resources, negative effects of software complexity and complicated software time relationships. The author describes a set of research methods, that he uses to carry out the research in commercial projects' environments. Thanks to applicative character of the doctorate, all the research and analyses were executed on a research stand using real commercial ECUs (Electronic Control Units), on which the author worked on as a software architect and head software architect. The ECUs were dedicated for three consecutive car lines of one of the biggest European manufacturers.

In order to easy navigation throughout the dissertation, following abbreviations are used:

- P1, P2... for research problems,
- MB1, MB2, ... for research methods,
- ZG1, ZG2, ... for research tasks,
- Rozwiązanie 1, Rozwiązanie 2, ... for proposed solutions,
- Projekt 1, Projekt 2, ... for commercial research projects.

The author presents the following set of solutions, that are based on executed research tasks:

- concept for automation methods related to the diagnostic stack management,
- concept for architecture and automation methods related to DLT logs management,
- concept for architecture and automation methods related to non-volatile memory stack,
- concept for the System Monitor component.

Presented solutions are increasing the available information about the system activities together with a possibility of automated data aggregation. The author validated his proposals and proved the following enhancements: minimization of flash operations timings, minimization of memory consumption, minimization of CPU (Central Processing Unit) load, minimization of software integration time, enhancement of code readability by automated comments generation, enhancement of automatically generated source code amount.

All source code of the implemented solutions are under a non-disclosure agreement, and are the intellectual property of the commercial customers, therefore the author provides the solutions in form of templates and instructions for other software architects that are developing embedded software in accordance with AUTOSAR standard. The author also provides possible research continuation areas for all presented elements of the software development process enhancement method.