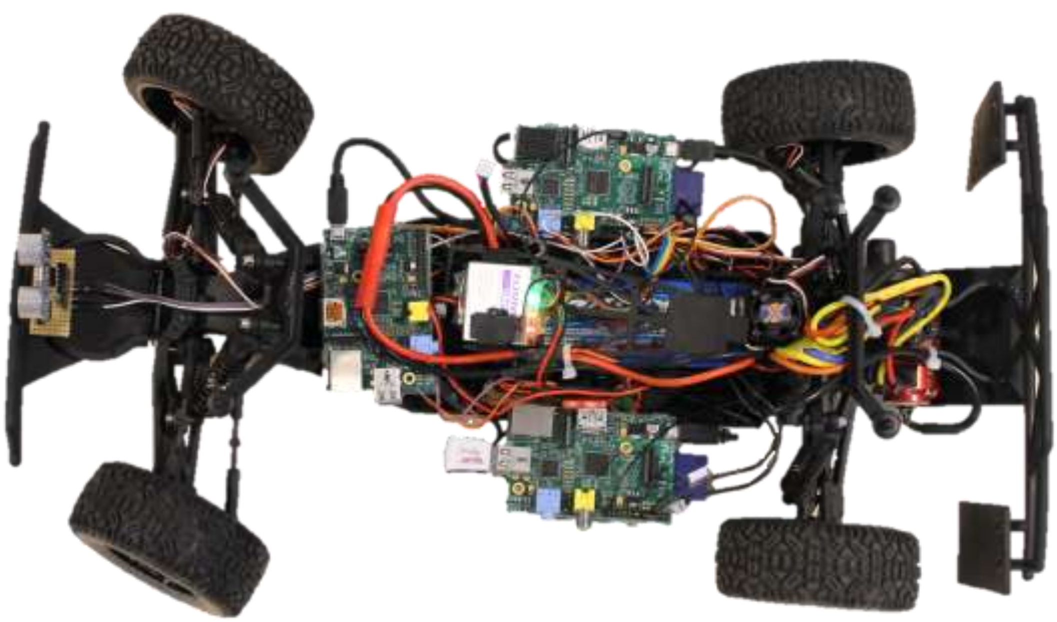
FFI

Federated Resilient Embedded Systems Technology for AUTOSAR (FRESTA)



Project within the FFI Vehicle development program

Author: Jakob Axelsson

Date: 2015-03-09

FFI

Content

FFI in short

FFI is a partnership between the Swedish government and automotive industry for joint funding of research, innovation and development concentrating on Climate & Environment and Safety. FFI has R&D activities worth approx. €100 million per year, of which half is governmental funding. The background to the investment is that development within road transportation and Swedish automotive industry has big impact for growth. FFI will contribute to the following main goals: Reducing the environmental impact of transport, reducing the number killed and injured in traffic and Strengthening international competitiveness. Currently there are five collaboration programs: **Vehicle Development, Transport Efficiency, Vehicle and Traffic Safety, Energy & Environment and Sustainable Production Technology.**

For more information: www.vinnova.se/ffi

FFI

1. Executive summary

The FRESTA project aimed at implementing mechanisms for flexible plug-in software in the context of AUTOSAR. This concept is called federated embedded systems. It offers the potential for shortening the lead time, the ability to build systems-of-systems, and the opportunity for open innovation.

The project has successfully demonstrated the technical concept that has been in focus. The demonstration was carried out on an open demonstration platform which has been developed in the project, and published as open source on the website moped.sics.se. This platform gives both industry and academia access to a prototype implementation that can be processed further in future product development, and also for educational purposes.

The project has also directly and indirectly contributed to several other projects, among others, is studying how the concept affects business models, architecture, methods, processes, tools and quality assurance. The results have been disseminated in 11 scientific publications (one of which received a conference best paper award), including two MSc theses. There have also been numerous presentations and demonstrations.

2. Background

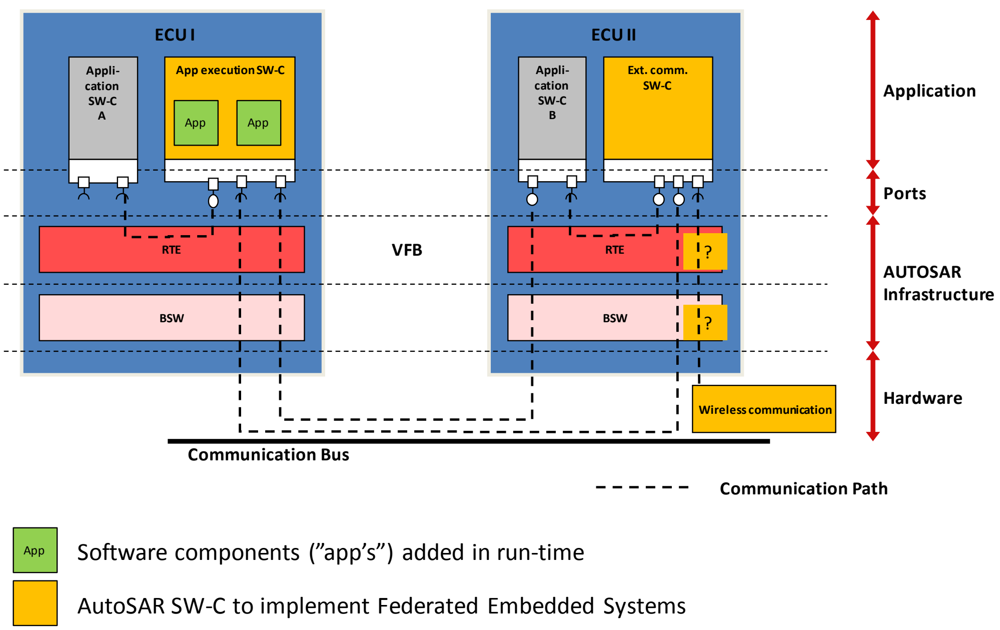
The FRESTA project (Vinnova 2012-02004) was initiated in the spring of 2012, as a result of an internally funded pre-study conducted by Swedish Institute of Computer Science (SICS), in co-operation with a handful of companies, including AB Volvo and Volvo Cars, who also became the partners in FRESTA. The pre-study performed a broad investigation of the concept called Federated Embedded Systems (FES), which aims at providing flexibility to embedded systems using mechanisms similar to “apps” in a modern smart phone, while respecting the characteristics of embedded systems. The mechanisms used in FES are (1) connectivity to the outside world, and (2) possibilities to install plug-in software dynamically on top of the pre-installed applications and basic software. The assumed benefits of FES are:

- Reduced time to market, since new features can be added much faster (and even to systems already in operation), by decoupling software development from the development of the mechanical system.
- Possibility to build systems-of-systems, where the plug-in modules act as broad interfaces to other products.
- Provision for open innovation, where third party actors can extend a product, thereby creating new market opportunities and increased customer value.

In the pre-study, an idea emerged how to introduce plug-in software in AUTOSAR-based systems. Such systems are used in almost all new vehicles today, but they are inherently static, and the AUTOSAR approach instead focuses on providing flexibility during development.

3. Objective

The basic idea explored in the FRESTA project was to embed a Java Virtual Machine (JVM) inside an AUTOSAR software component, and let the plug-in modules execute in this "sandbox". In that way, there is no need to change anything in the AUTOSAR standard, and it becomes easy to enable plug-in execution in a new control unit. The sandbox also provides protection of the underlying software from disturbances caused by non-functional or malicious plug-ins. The concept further included a software component for managing external connectivity, including plug-in installation and uninstallation, and sending and receiving of data during the execution of plug-ins. This concept is illustrated in the following figure:



The objectives of the project were to develop the AUTOSAR software components for plug-in execution and external communication, and validate them in a realistic setting. Also, supporting tools were to be considered.

4. Project realization

The project formally started on Oct. 1 2012, and ended Dec. 31 2014. The project plan consisted of the following phases:

1. Elicitation and preparation (3 months): Formulation of requirements and concepts (TRL 2).
2. Simulated environment (4 months): Detailed concepts tested in a simulator (TRL 3).
3. Single ECU environment (7 months): Integration of the high-level concepts in a realistic ECU running AUTOSAR (TRL 4).
4. Distributed ECU environment (6 months): Integration of complete implementation in a distributed test environment running AUTOSAR (TRL 5-6).
5. Vehicle environment (7 months): Porting the implementation to a real vehicle environment (TRL 6-7).

On a high-level, the project has followed this work plan, although there have of course been minor adjustments. At regular intervals, the whole project team has held full-day meetings to report status and plan ahead. There have been eight such meetings, or approximately once per quarter, and the meetings have been rotating between SICS (Kista), Volvo Cars (Göteborg), and AB Volvo (Göteborg and Eskilstuna). In addition to this, the SICS team has held weekly stand-up meetings for detailed follow-up and planning.

During the project, a test and demonstration platform has been developed, which is called Mobile Open Platform for Experimental Design (MOPED). It consists of a chassis from a standard radio controlled car from the hobby market. Inside the car, an electronic system consisting of three ECUs have been installed, two of them running AUTOSAR and one running Linux. The ECUs are based on Raspberry Pi hardware, and complemented with various sensors and actuators. In this way, a platform has been achieved which is very close to a real car when it comes to the software characteristics, but completely open for modifications and much cheaper. This platform has been used throughout the project, and remains a valuable asset for the future. The AUTOSAR version running on the system is based on ArcCore's open source release, but was ported by the project as part of an MSc thesis project. So far, three copies of the car have been built, and two of them remain at SICS while the third has been delivered to AB Volvo. (During early 2015, the platform was also replicated by a group of students at Chalmers.)

As in every research project, there have been deviations from the original idea that were not foreseeable during the pre-project planning. In this project, it did not affect the overall results, but some of the major deviations are listed anyway.

The most significant deviation was a decision, encouraged by the industrial partners, to not implement the concepts in a real vehicle. This is a sign that the industrial partners found the MOPED test bed so trustworthy, that they did not find it meaningful to also try it in their own hardware. Instead, it was decided to spend the last months of the project refining the implementation on MOPED, and making an open source release of the software and building instructions. Still, some activities were carried out also in a real industrial setting, primarily as an MSc project by Gerard Duff, who investigated the FRESTA concepts in a simulator of one of the control units used by Volvo CE. Originally, there was a plan to develop also an emulated version of the ECUs used in MOPED, to make it easier to do fault tracing, and other development activities. The idea was to do an MSc thesis project on this, but no suitable student could be found, and the idea was dropped.

A major difficulty encountered in the development of the MOPED test bed was the communication networks. Initially, the idea was to use Ethernet communication, since it is already prepared for in the Raspberry Pi hardware, and since it is believed to be a future protocol also in the automotive industry. However, moving the Ethernet stack to AUTOSAR turned out to be a nightmare, and eventually the project decided to instead revert to traditional CAN communication. Even though some time was lost on this, it was still a valuable experience, and the complexity of the Ethernet protocols raises some serious questions when it comes to its use in safety-critical systems like vehicles.

Another technical hurdle was the selection of which JVM to use. There is a wide range of JVM's available, both commercially and as open source, and a thorough investigation was initiated to select the most appropriate one. The choice was to go for KVM, developed by Sun Microsystems, because it was widely used, had small memory requirements, could run without an operating system, had source code available, and had documentation for porting. However, there turned out to be many hidden problems with this, and it is also quite old, thus running an outdated version of Java. Therefore, a decision was later made to change to the Squawk VM, also developed by Sun (now Oracle). It uses a much more modern Java version, and is to a large extent written in Java, meaning that there is only a very small part which is machine dependent. Squawk VM was successfully implemented inside an AUTOSAR component, and extended with mechanisms for app development. The whole exercise has provided valuable insights into the difficulties of selecting a complex software component, which will be leveraged on in follow-up projects.

Before the project started, the focus was almost entirely on the software to be installed in the vehicles. However, as the project proceeded, it became increasingly apparent that the information systems outside the vehicle play a very important role, in particular the so-called trusted server, where the plug-ins are fetched. Therefore, a bit more effort than planned had to be spent on the server side. This has however also triggered many more ideas for future work, including how to connect the development systems to the server, and work on continuous deployment strategies.

5. Results and deliverables

5.1 Delivery to FFI-goals

The goals of the FFI program are, and should be, fluid, and therefore this section refers to the goals of the program when the project was initiated in 2012. However, most of those goals remain today.

Many of the goals are related to the direct use of vehicles, in particular safety and environmental effects. Many of the services that can be realized using FES relate to these areas, and hence the overall concept has a great innovation potential within FFI core objectives.

The direct contributions relate to the objectives regarding the vehicular industry's competitiveness. Today, it is common to have very long development cycles, where basic functions are developed 2-5 years ahead of start of production. With the concept developed in this project, new services can be developed much faster (within weeks or a few months), and even after the start of production. This gives an enormous potential in revitalizing the industry, and it will also have an effect on the whole software ecosystem, since third party developers can contribute with creativity and innovation.

The project has been unique in that it has addressed flexibility in the otherwise very static deeply embedded systems. This has a large interest also for industries using other standards than AUTOSAR, such as automation, which has also been confirmed in contacts with ABB.

6. Dissemination and publications

6.1 Knowledge and results dissemination

Apart from scientific publications, there have been numerous external presentations of the project, including at ABB, KTH, VICTA Roundtable, Springworks, Mälardalen University, etc. The project has also been demonstrated twice at the SICS annual open house, and at different internal events at the partners.

A major effort was to turn the project's results into an open source release, and this was achieved at the end of 2014, when the home page moped.sics.se was launched. It contains an overview of the project, descriptions how to build copies of the MOPED car, and a link to GitHub, where the source code of the software can be downloaded.

6.2 Publications

The project has actively published results throughout its execution, resulting in a total of 11 publications. The paper describing the MOPED platform (ref. 10) received the best paper award at a fairly large conference, which proves the good quality of the results.

1. Jakob Axelsson and Avenir Kobetski. On the Conceptual Design of a Dynamic Component Model for Reconfigurable AUTOSAR Systems. In Proc. 5th Workshop on Adaptive and Reconfigurable Embedded Systems and in ACM SIGBED Review, April, 2013.
2. Avenir Kobetski and Jakob Axelsson. Paving the Way for Apps in Vehicles. ERCIM News, No. 94, pp. 12, July, 2013.
3. Avenir Kobetski and Jakob Axelsson. On the Technological and Methodological Concepts of Federated Embedded Systems. In Proc. First Open EIT ICT Labs Workshop on Cyber-Physical Systems Engineering. Trento, Italy, May 24, 2013.
4. Efi Papatheocharous, Jakob Axelsson, and Jesper Andersson. Issues and Challenges in Ecosystems for Federated Embedded Systems. In Proc. International Workshop on Software Engineering for Systems-of-Systems, Montpellier, France, July 2, 2013.
5. Shuzhou Zhang, Avenir Kobetski, Eilert Johansson, Jakob Axelsson, and Huifeng Wang. Porting an AUTOSAR-Compliant Operating System to a High Performance Embedded Platform. In Proc. 3rd Embedded Operating Systems Workshop, Aug. 26-27, 2013.
6. Shuzhou Zhang. Porting AUTOSAR to a high-performance embedded platform. Master's thesis, Mälardalen University, 2013.
7. Jakob Axelsson, Efi Papatheocharous, and Jesper Andersson. Characteristics of Software Ecosystems for Federated Embedded Systems: A Case Study. Information and Software Technology, 56(2014), pp. 1457-1475, 2014. DOI: 10.1016/j.infsof.2014.03.011.
8. Ze Ni, Avenir Kobetski, and Jakob Axelsson. Design and Implementation of a Dynamic Component Model for Federated AUTOSAR Systems. In Proc. 51st Design Automation Conference, San Fransisco, June 1-5, 2014.
9. Jakob Axelsson and Avenir Kobetski. Architectural Concepts for Federated Embedded Systems. In Proc. 2nd Intl. Workshop on Software Engineering for Systems of Systems, Vienna, Austria, Aug. 26, 2014.
10. Jakob Axelsson, Avenir Kobetski, Ze Ni, Shuzhou Zhang, and Eilert Johansson. MOPED: A Mobile Open Platform for Experimental Design of Cyber-Physical Systems. In Proc. Euromicro SEAA 2014, Verona, Italy, Aug. 27-29, 2014.
11. Gerhard Duff. App enabling environment for Volvo CE platform. Master's thesis, Mälardalen University, 2013.

7. Conclusions and future research

In summary, the FRESTA project was set up to investigate the implementation of the FES concept in an AUTOSAR environment, with focus on the execution mechanisms for plug-in software. This goal has definitely been reached, and successfully demonstrated in a realistic software and hardware environment, thus landing at or close to the TRL levels planned. The project has resulted in a number of publications, including one best paper award and two MSc theses, and a number of external presentations. It has also led to a number of follow-up activities, both inside and outside FFI. A remaining asset from the project is the MOPED test bed, which will continue to be refined and used for a number of years, both at SICS, and hopefully also by others who can make use of the open source release achieved in the project.

The FRESTA project has led to several side-effects in terms of new projects, or reuse of results in other settings.
About one year into the project, Vinnova granted funding for a project that studies the software ecosystem that emerges from the technical concepts developed in FRESTA. Here, SICS and partners study the business effects, implications on architecture, processes, methods, and tools, and quality assurance, from introducing FES. The project takes over the responsibility for the MOPED platform and uses it as a research tool.
Late 2014, FFI approved the Next-Generation Electrical Architecture project, led by Volvo Cars, and with SICS as one partner. Several parts of that project are influenced by the work done in FRESTA, and SICS will also participate, with a focus on how to build systems-of-systems.

SICS, together with Mälardalen University and Blekinge Institute of Technology, will also start a co-operation on decision support for component based systems. This project will be directly influenced by the experiences gained in FRESTA when it comes to building complex cyber-physical systems, and the MOPED platform will be used also in this project.

8. Participating parties and contact person

This project has been a cooperation between Swedish Institute of Computer Science (SICS), AB Volvo, and Volvo Cars.

For more information about the project, please contact the project leader Jakob Axelsson, e-mail jakob.axelsson@sics.se.