INNOVATION REPORT

Trustworthy software secures key applications - dependable embedded software will meet future needs

Author: Jean Gelissen, Philips, The Netherlands

Problem description

The amount and importance of software in embedded systems is growing at a very rapid pace, for instance in the automotive, home medical care and domotica domains. It is also known from many cases that embedded software is the main reason for failure of the complete system. The economic value of the related products and/or function and the fact that individuals and societies depend more and more on the correct functioning of these embedded systems are the main motivators behind Trust4All.

Due to the change from closed and static stand-alone systems to open, dynamic and interconnected systems, making the embedded software easily manageable poses ever-growing challenges. It offers great opportunities to enhance the usability of systems; but also gives rise to growing threats with respect to the trustworthiness of the software behaviour.

When analysing the needs envisaged for future application domains from the users' viewpoint, there is clearly an expectation that such systems should be able to provide higher levels of dependability. Meeting this demand will require the establishment of defined levels of trustworthiness – ranging from medium to high – in several respects:
Security during critical actions to guarantee the promised behaviour; Reliability throughout a reasonable lifetime to deliver the expected benefits; and Robustness during operation to guarantee functionality.

Research Description

Trust4All has defined, designed and developed a middleware software architecture specifically targeted at embedded systems that require a predefined level of trust, due to the nature of the services they provide. The project focuses on the trustworthiness-related aspects of the middleware software architecture in domains such as home medical care, security and automation, as well as on-the-move applications, for which dependability is particularly important.

The major result of the project is a model to represent and Trust supported by an architecture that makes it possible at any point in time to verify and reason about the level of trust offered by a composed system. Its provides associated metrics and a methodology for dynamic monitoring of system status with respect to the model after requested or unrequested updates, upgrades or extensions. On the basis of this validation process, systems will be allowed to, or prevented from, executing applications or services that require a defined level of confidence.

These project results have been validated in a large variety of application domains: mobile navigation, document-management systems, monitoring for elderly people, taxi-driver assistance and home

medical care. In addition to these applications, a large range of validation tools has been developed and used for the development of the applications required for the validation but can and will also be applied for different cases.

The project has disseminated its results in more then 70 scientific papers and has been present at several international conferences and fairs. The project has contributed to the ISO/IEC MPEG standardisation body and is responsible for the majority of a complete new standard for middleware named ISO/IEC 23004 consisting of eight parts, including the reference software also contributed by the project.

Business Value

The value of the project results are in the area of deployment in actual products or platforms and in tools that support these deployment activities but will also be used in a scientific context.

Depending on this business model, Trust4All solutions can be deployed for:

- The reduction in the cost-of-non-quality of a product – CE domain;
- The improvement of the reliability and robustness of a product – medical/health and wellness domain;
- Managing the software obsolescence and life-cycle issues of a product – automotive domain; and
- The improvement in the time to market and reduction of the integration/testing effort of a product – CE domain.

Examples of the deployment of the project results in these domains include:

Software has grown to become a considerable and complex part of semiconductor products. Component technology as developed in a series of the ITEA projects that includes Robocop, Space4U and Trust4All has played a key role in tackling the challenges raised by this exponentially growing amount of software. Not only development efficiency but also quality, robustness and reliability of products have benefited from the innovative technology developed in these projects. Component-based architectures have been an important cornerstone for the semiconductor platform strategy. Developments such as the universal home API (UHAPI) interface modelling and component technology being used in digital TV products in the market today is rooted in the component model developed by the projects. Standardisation of these technologies initially via the UHAPI Forum, followed by the adoption by the CE Linux Forum, and finally being promoted to an ISO middleware standard will lead to easier integration of third-party middleware and application components. Extensions of the initial Robocop model for quality-of-service-based resource management have lead to new insights and technologies for efficient use of scarce resources, such as memory and power in mobile phones. These new insights are currently being deployed and productised inside the semiconductors industry.

In the domain of multi-functional devices (MFD) that offer basic printing and scanning solutions to users, the functionality needs to be extended to allow also for advanced scanning functionality such as scan to a document-management system, scan to a thumbdrive or to allow for optical character recognition. These additional functionalities are typically created by third-party developers and need to be hosted on the same platform that executes the basic functions. However the operation and reliability – for example the responsiveness and remote diagnostics – of the complete systems should not be harmed by these extensions. Based on the concepts and technologies developed within Trust4All, it has been proven that it is possible to extend the functionality for an end user without introducing additional processing power.

INNOVATION REPORT

In the domain of mobile communication devices, the containment mechanisms developed in Trust4All are under discussion regarding their suitability for Linux-based communications platforms. In particular, the trust-management functionality could be applied to allow for future third-party solutions in the area of Internet services.

The gradual introduction currently under way of ambient intelligence – mainly new services created by software components and including monitoring for medical applications – in home systems looks promising. However there is some reservation from the end user, he/she needs more confidence in the trustworthiness before delegating various tasks to the system. The methods and technologies developed in the context of Trust4All will make it possible for system integrators and service providers to get to the desired level of confidence in these systems requested by the users that depend on a contiguous and correct operation of these systems.