OVERSEE
A Secure and Open Communication and Runtime Platform for Innovative Automotive Applications

André Groll, Jan Holle, Christoph Ruland
University of Siegen, Institute for Data Communications Systems
{andre.groll,jan.holle,christoph.ruland}@uni-siegen.de

Marko Wolf, Thomas Wollinger, Frank Zweers
escrypt GmbH – Embedded Security
{marko.wolf,thomas.wollinger,frank.zweers}@escrypt.com

Abstract

The next generation of intelligent vehicular information and communication technology (ICT) applications strongly depends on the availability of an ICT infrastructure combining both dependability and security attributes. Thus, future intelligent vehicles (i) have to provide an appropriate wireless access point to their onboard IT systems and in-vehicle applications, (ii) need itself in turn appropriate access to external information and applications, and (iii) have to execute multiple independent applications with different level of criticality concurrently in a trusted manner.

To meet these challenges, OVERSEE (Open VEhiculaR SEcurE platform) will realize an open vehicular IT platform that provides a protected, standardized in-vehicle runtime environment and onboard access and communication point. Therefore, the main objectives of the OVERSEE platform will be dependability and IT security that means enforcing a strong level of isolation between independent applications and means ensuring that vehicle functionality and vehicle safety cannot be harmed by any application.

OVERSEE will first carry out a requirements analysis based on a security risk and dependability analysis and will then specify and implement the in-vehicle platform architecture. OVERSEE will also specify and develop the capabilities that are needed to validate today's and future open vehicle platform implementations as well as different vehicular applications.

1 Introduction and Motivation

Modern vehicles are an integral part of the daily life in industrial nations. In 2005 more than 170 million cars were registered in the European Union [4]. Besides the use of cars for individual transport of European citizen, commercial road vehicles are an inherent part of flexible logistic chains and an additional load to the European road network. With respect to the amount of vehicles and the vehicle miles travelled per year there are two main goals for the use of vehicles and the operation of the European road network. For one thing the number of fatalities and injuries on the road has to be reduced in order to provide safety; for another thing the use of vehicles should be as efficient as possible with regard to the emission of CO_2, consumption of fossil fuels and the use of road infrastructure.

1.1 Automotive applications

Modern automotive applications and traffic telematics solutions like wireless local danger warning, emission-based road tolling systems, etc. which could add a valuable contribution to achieve these goals are mostly software based with the need of secure access to a wide range of vehicle internal and external networks. Additionally, there is a wide range of new automotive OEM and non-OEM applications which could add new functions to vehicles and increase the comfort for vehicle users.

Today, every new automotive project implies the development of a new and project-specific Electronic Control Unit (ECU), which causes immense costs and additional risks. Furthermore, currently there is no universal device obtainable that is able to connect vehicle internal and external networks in a secure and standardized way (e.g., for downloading tolling information or transmitting diagnosis information). This gap, the high costs, and additional risks impede the development of new products and services that could be helpful to make vehicular traffic safer and more efficient.

Future innovative automotive applications require an open and secure vehicular platform:

- **Open** in a way that the platform provides protected runtime environments for the simultaneous and secure execution of multiple OEM and also non-OEM applications with secure access to vehicle internal and external networks. The interfaces of that platform should be standardized and public in order to enable the development of vehicle independent "plug & play" applications even by third party providers. This would reduce the amount of ECUs needed in a vehicle and thus save costs for vehicle productions. Furthermore, fewer devices will save weight, maintenance efforts and hence increase the efficiency of vehicles.
- **Secure** in a way that the interfaces to vehicular internal and external networks are protected against passive and active attacks. In this way the platform should act as a secure single point of access to vehicle networks.

A generic approach for the implementation capable to support a wide range of recent and future automotive applications is required and may solve many of the problems regarding the development and the deployment of various innovative vehicular applications and solutions.

1.2 Use Cases:

Already today, there are many possible use cases for an open and secure vehicular platform with the requirements listed above. In this paper, just a few of them are mentioned to convey the impression of the potential of such platform. Except the general possibility for third-party "plug & play" applications, nearly every application communicating with the "outside world" of the car and depending on authentic and correct information from inside the car (sensors, etc.) is able to benefit from the platform services.

For example in Germany, the Electronic Toll Collection systems [7] needs a special "On Board Unit" (OBU) and correct data to provide the necessary services as well as for toll accounting. But as stated by the provider of this system, it usually should not be the provider's part to produce and supply the hardware unit, because he just wants to deploy the accounting software. Due to the open and standardized interfaces, this type of applications could be executed on such platform.

Other possible use cases are the upcoming eCall service for automatic emergency calls after accidents or theft intervention applications that are able to obtain the correct vehicle location and condition through the platform. Furthermore, remote diagnosis as well as remote service support and remote software updates for ECUs can be executed easier and more flexible in a secure way.

Additionally, all kinds of vehicle to vehicle (V2V) as well as vehicle to infrastructure (V2I) communication and synchronization applications regarding infotainment or traffic management services can be used and realized also by third party providers very easily.

2 Objectives and functions

Within the following section the objectives of the OVERSSE project and the functions of the OVERSEE platform are presented.

2.1 Objectives of the OVERSEE project

The motivation and use cases lead to the following set of objectives for the OVERSEE project:

1. Providing a generic and open source platform for spatial and temporal partitioning of secure simultaneous execution of multiple innovative automotive applications on one single OVERSEE ECU
2. Providing a secure and dependable runtime environment
3. Create an open and standardized secure single point of access to in-vehicle networks
4. Providing a standardized interface for accessing security and dependability services
5. Providing validation support capabilities and tools
6. Providing the capabilities of secure and non-deniable recording

The achievement of these objectives will solve some of the most recent and important requirements of the automotive industry and also social motivated projects in the automotive domain, e.g.:

- Objectives 1 and 2 will lead to a reduced quantity of ECUs in vehicles (improve efficiency of vehicles), reduced costs and less risks for innovative automotive projects (especially for SMEs and start-ups). Moreover, the standardized OVERSEE platform could establish a new market for vehicle independent, software based automotive applications.
- Objectives 3 and 4 will promote the development and deployment of innovative automotive applications (especially in the field of cooperative automotive applications, e.g., V2V and V2I) through the availability of a platform that supports generic and not only project-specific tasks (e.g., secure and dependable communication and runtime environments).
- Objective 5 will offer the possibility to proof, if other platform implementations fulfill the OVERSEE specifications and hence offer the possibility to build a new market for manufactures of OVERSEE ECUs. Furthermore, the standardization of the platform and the availability of tools to proof the compliance of implementations with this standard will speed up the spread of the platform (e.g., because OEMs are able to combine the OVERSEE platform with their own developments).
- Objective 6 will facilitate the development of innovative automotive applications which depends on the secure and non-deniable recording of data. Possible applications that could benefit from these functions are electronic tolling or pay-as-you-drive insurances or taxes.

The availability of the OVERSEE platform as a secure execution environment for novel ICT applications in the automotive domain could also help to achieve the objectives as described in the “Action Plan for the Deployment of Intelligent Transport Systems in Europe” [6]:

- Greening of transport
- Improving transport efficiency
- Improving road safety and security

2.2 Functional overview of the OVERSEE platform

The following sketch shows the generic functions of the OVERSEE platform, which will be developed and prototypically implemented within the project.

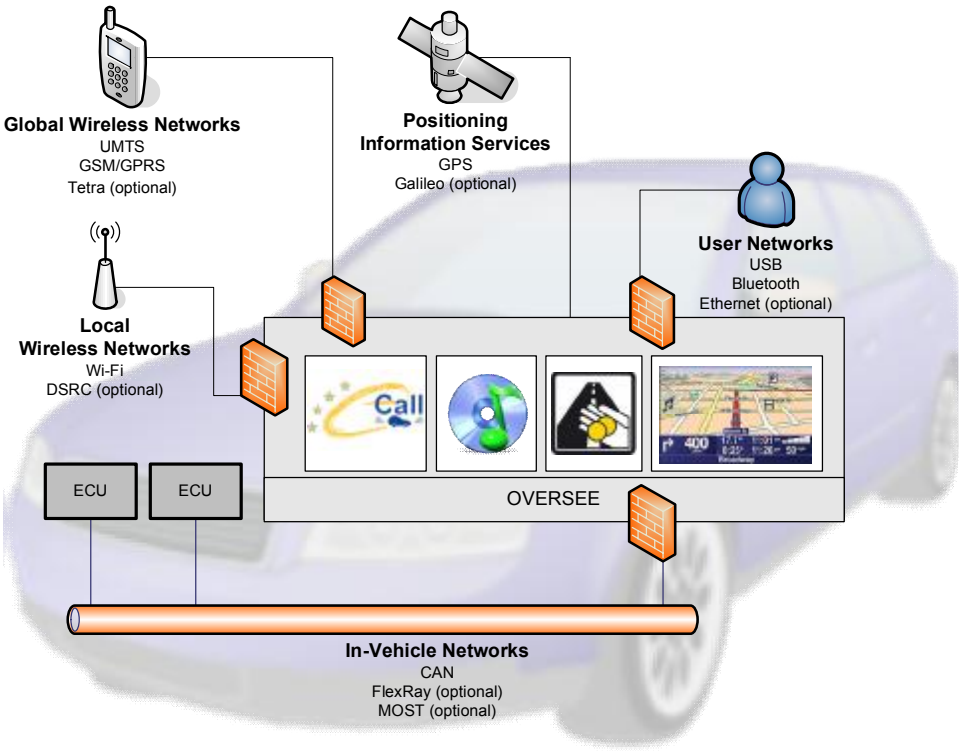

Figure 1: Functional Overview of the OVERSEE platform

The functions can be divided in two main groups: Communication functions and runtime environment functions. Nevertheless, only the combination of these function blocks in one single ECU will offer the aimed innovations for the automotive field.

- Communication functions (secure single point of access):
  - Generic communication interface for a customable set of vehicle internal and external networks: This function will enable the easy development of new automotive applications, which strongly depend on communication processes (especially cooperative automotive applications).
  - Firewalls with user specific rules for internal and external network interfaces: The firewall will protect the internal networks and the OVERSEE platform against intrusion. Moreover, the firewall will preserve the vehicle internal data (e.g., GPS data or information concerning the behavior of the driver) against non-authorized transmission to external parties and hence will care for the privacy of the driver.
- Runtime environment functions (virtualization):
  - Secure simultaneous execution of applications: Within one OVERSEE ECU multiple applications can be executed in parallel in a secure manner by the use of virtualization mechanisms. This will lead to a reduction of necessary ECUs in vehicles and corresponding synergy effects.
  - Standardized execution environment: The standardized interface offered by the OVERSSE platform for applications development will establish a new market for vehicle independent automotive applications.

3 Underlying Key Technologies

This chapter shortly introduces the two key technologies and approaches applied by OVERSEE.

3.1 Virtualization in the automotive domain

Until a few decades ago (virtually until the 1990s) cars were closed, electro-mechanical systems with only a few, isolated, and mainly uncritical IT systems. Today, even compact class vehicles contain dozens of interconnected digital microprocessors with up to several hundred megabyte of software installed. In addition, the ongoing integration of non-OEM applications (e.g., third party applications, passenger applications) and non-OEM devices (e.g., cell phones, multimedia players) is becoming more and more essential. Thus, vehicles will include more and more (internal and external) interfaces, applications, and communications that are no more subject to exclusive and solely control of the OEMs or suppliers. However, further increasing the quantity of individual electronic control units (ECU) and hence also the network and maintenance complexity is neither technically nor economically justifiable [1]. Consequently, future vehicular IT architectures will try to merge several single control units into a few powerful ones [2]. The parallel execution of several ECU applications allows for a noticeable more efficient and more flexible utilization of the always scantily hardware resources. Thus, it decreases efforts and costs during production, operation, and maintenance of (redundant) automobile IT hardware and necessary wiring. Furthermore, virtualization enables various novel vehicular IT mechanisms, which can increase the vehicle's safety as well as its security. Nevertheless, reliable IT mechanisms are needed to secure ECU applications executed in parallel against each other. That means, neither an accidental malfunction (IT safety) nor a systematic manipulation (IT security) of one application should affect or compromise any other application executed in parallel. The virtualization technologies, however, allow for an efficient and flexible hardware sharing while reliably enforcing the strict isolation of all parallel-executed ECU applications. Thus, applying virtualization technologies in vehicular IT architectures amongst others allows for:

- Reduction of hardware costs and energy consumption
- Higher hardware efficiency and valuable synergy effects
- Simplified, standardized development
- Increased IT safety
- Increased IT security
- Multi-level security and multi-level safety on a single ECU
- Increased flexibility, interoperability, portability and backwards-compatibility
- New application use cases and business models

Even though, except for a few sandboxing implementations for isolating applications inside an ECU (e.g., a GSM portal access application), virtualization solutions are actually not deployed in current vehicles. Nevertheless, virtualization solutions are already a prevalent IT safety and IT security technology for most upcoming vehicular IT architectures (i.e., 2012 ff). Hence, the migration of individual and dedicated ECUs into central, high performance, multipurpose ECUs, the integration of non-OEM applications and non-OEM devices could hardly be realized efficiently, reliably, and securely without applying strong runtime isolation mechanisms such as virtualization technology provides. Currently, the processor manufacturer Intel and the automotive Linux developer WindRiver are already cooperating on the development of an automotive Linux distribution that employs the hardware virtualization extensions of Intel’s Atom processor [3]. Thus, the application of virtualization solutions in vehicular IT environments will be virtually inevitable on the one hand, but on the other hand, offer also a great chance to considerably increase safety and security for all vehicular IT applications.

3.2 Secure single point of access

Today, the implementation of new interconnections between in-vehicle networks and external networks – e.g., GPS or UMTS – which is often necessary to achieve innovative automotive applications in most cases will result in the development of a new ECU. During the development of an ECU for matching the requirements very often the same challenges have to be considered again. The typical challenges are:

- Defining (and restricting) the information flow between external and internal networks
- Conversion of messages and commands between the network package formats
- Considering strong security requirements, e.g., authentication and communication policies

At the moment, there is no single protected and standardized access and communication point to the IT infrastructure of the vehicle to enforce a dedicated security policy. But this would be very important, because the current situation opens the door for a wide range of problems due to non-authentic and non-confidential communications. A single intentional or non-intentional faulty application could harm the whole network and therefore many – including safety critical – applications that may have impacts on road safety (e.g., ESP). Especially regarding data security and privacy of in-vehicle applications, a controlled information flow together with a strong isolation of different applications is necessary. A firewall mechanism that integrates user rules specified by the OEM or third parties – but proved by the OEM – can help to realize a security policy in a way that unauthorized access to other components of the inside network is impossible. OVERSEE will help to provide such a protected and standardized access and control point, that is able to realize an integrated and effective protection against internal and external (malicious) faults.

4 System design

The following section gives a short overview of the underlying OVERSEE system architecture and describes the inherent security approach to secure this architecture against any unauthorized encroachments.

4.1 Architecture Overview

Figure 2 shows the general OVERSEE architecture that consist of a hardware layer at the bottom, a system layer as middleware and the application layer on top.

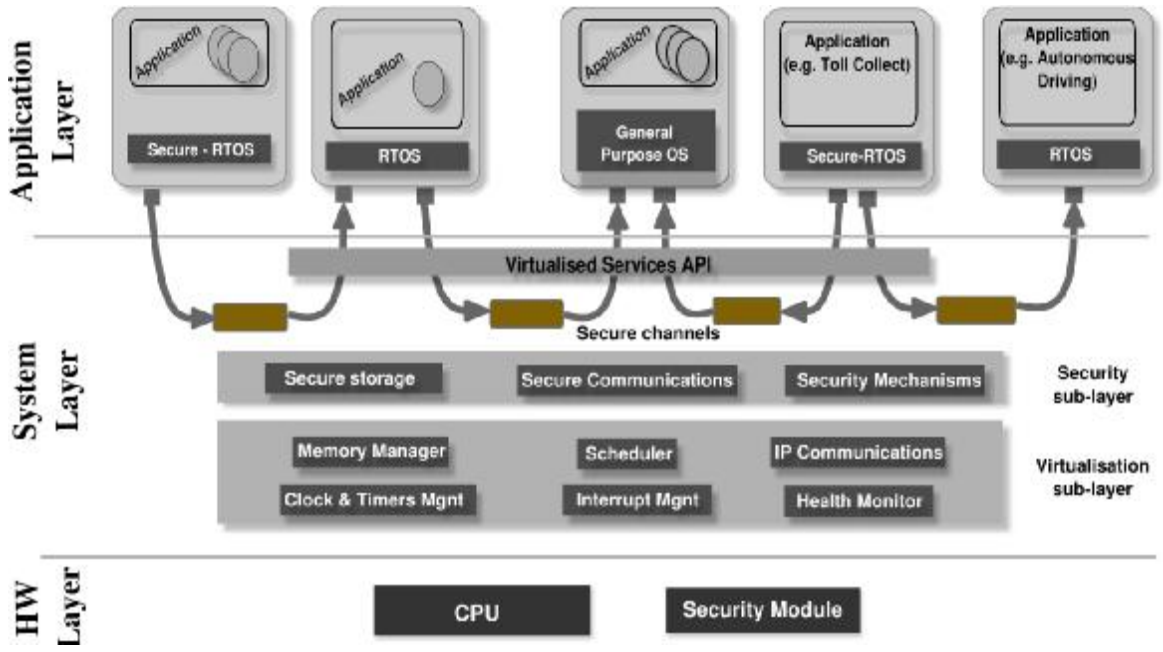

Figure 2 General OVERSEE architecture

The **hardware layer** includes standard hardware modules such as CPU, memory, and peripherals, but includes also a dedicated hardware security module. The security module is important for, e.g., secure storage and secure processing of critical data (e.g., keys, certificates, signatures).

The OVERSEE project intends to reuse an existing automotive IT platform that fits best the requirements and is already available. For now, OVERSEE has not done its final decision, but probably will deploy a powerful (i.e., about 400 MHz 32-bit CPU @ 128 MB RAM) Intel or PowerPC-based embedded platform providing all necessary on-board periphery such as CAN and Ethernet interfaces, support for GPS and DSRC modules, and sufficient storage capabilities (e.g., PCMCIA, Flash and USB). The platform has also to fulfill the physical requirements, for instance regarding temperature ranges, humidity or mechanical stress that is typical for an application in the automotive domain (these requirements are independent from the OVERSEE project and therefore no part of the development process). Final OVERSEE realizations (beyond prototypical states) will meet the spatial requirements of the ISO 77335 vehicle head unit slot standardization that allows a simple installation in virtually all existing vehicles. The in-vehicle deployment of the OVERSEE platform around the head unit location, moreover allows the efficient utilization of existing periphery such as power supply or outside antennas without causing any further installation costs.

The **system layer** virtualizes the hardware resources and offers virtualized services to the execution environments. It also guarantees the temporal and spatial partitioning of the system resources. The main virtualized resources are CPU, memory, interrupts, clock, timers and the security module. The Health Monitor included in this layer performs an early detection of possible errors and reacts to anomalous events or states trying to solve or isolate the faulting subsystem in order to avoid or reduce the possible consequences. The main issues in the design of this layer for dependable and secure real-time embedded systems consider:

- Spatial isolation: partitions should be isolated from others avoiding the access from them.
- Temporal isolation: partitions should be executed under real-time scheduling policies, which can guarantee the real-time constraints independently of other partitions.
- Resources virtualization: basic hardware components as clock and timers, interrupts, memory, CPU, time, and serial I/O need to be virtualized to partitions.
- Efficient and deterministic system services
- Efficient and secure inter-partition communication
- Cryptographic services to partitions
- Health monitoring
- Low overhead and footprint

Finally, the **application layer** includes the execution environments (partitions) where the applications are executed. A partition is composed by an operating system and the applications. Partitions can be built using a specific operating system according to the application needs (real-time, secure real-time or general purpose operating system). Prototypical instantiation of the application layer will execute a tolling application as well as an autonomous driving application.

4.2 IT Security Approach

Security is the crucial part of OVERSEE, since it ensures the protection against attacks from the “outside world” into the vehicle as well as from the vehicle towards other entities. The concept for the OVERSEE security is based on three pillars:

The first security pillar is the virtualization technology. It allows the strong runtime isolation of different applications sharing the same hardware resources. Using virtualization technology, one application cannot illicitly access or maliciously affect any application executed in parallel. Virtualization allows efficient multilateral security architectures and therefore the equally strong enforcement of different security policies for different parties sharing the same platform. Parties

with different security policies could be for example the end-user and the application provider, both having different security objectives.

The second pillar of the IT security realization for OVERSEE is the vehicular security (services) software layer that uses various security primitives in order to realize different high-level security services. This security layer applies cryptographic primitives such as encryption and signature algorithms, hash functions, and random number generators. Based on these functions, OVERSEE will provide high-level security services for secure communication, entity authentication, secure storage, secure software management, secure policy decision as well as secure policy management.

The third pillar, the hardware security anchor, primarily serves as a platform protection mechanism enforcing foremost the integrity of the (upper) software security layer and its cryptographic primitives. Due to the secure hardware, the execution of all cryptographic primitives is isolated from the main processor and thus prevents any malicious impacts or compromise from all other activities concurrently handled by the main processor. This ensures protection against virtually all software attacks such that a potential, successful compromise would indeed require sophisticated and costly physical attacks. In addition, the security hardware would compute most cryptographic primitives with a much higher efficiency (i.e., throughput). OVERSEE plans to build up on the vehicular security hardware provided by the EVITA project [5] in order to protect the integrity of the security services as stated above and to realize all the advantages.

5 Project Structure and Related Projects

For the development and implementation of the OVERSEE platform an international consortium has been founded. The project structure and the schedule will be briefly presented within the following section. Afterwards a short overview about the relationships to other recent automotive projects will be given.

5.1 Project Structure and Milestones

The specification and implementation of the OVERSSE platform will be done in a project founded within the 7th European Framework Programme. The consortium consists of eight partners from four European countries (Austria, France, Germany, and Spain).

Besides the typical boards and instruments the consortium agreed to integrate an advisory board. In this advisory board important stakeholders in the automotive field will be represented to be sure that the OVERSEE platform will fulfill the described requirements and respect the constraints in the automotive domain. The advisory board is open to be joined within the whole project.

The consortium agreed on the following milestones:

- The initial version of the requirements document will be available in June 2010. It will be the base of the decisions within the design phase of the project.
- The design of the OVERSEE platform will be available in December 2010. The design will be the foundation for the platform implementation and the validation support.
- The platform implementation will be available in December 2011.
- The validation support of OVERSEE will be available in March 2012. The tools provided will help to validate the platform implementations provided within this project and also additional implementations from other manufactures.
- The proof of concept implementations will be available in June 2012 and will demonstrate the benefits of the OVERSEE platform through the use of the OVERSSE platform within real life applications (e.g., eCall and tolling).

5.2 Related Projects

The following sketch shows some of the most recent projects and standardization activities in the automotive domain and their relation to OVERSEE. While OVERSEE builds on the results and requirements of current research projects and standardization bodies, it will feed back requirements, specification and a prototype for the open vehicular secure platform for later use in field test activities.

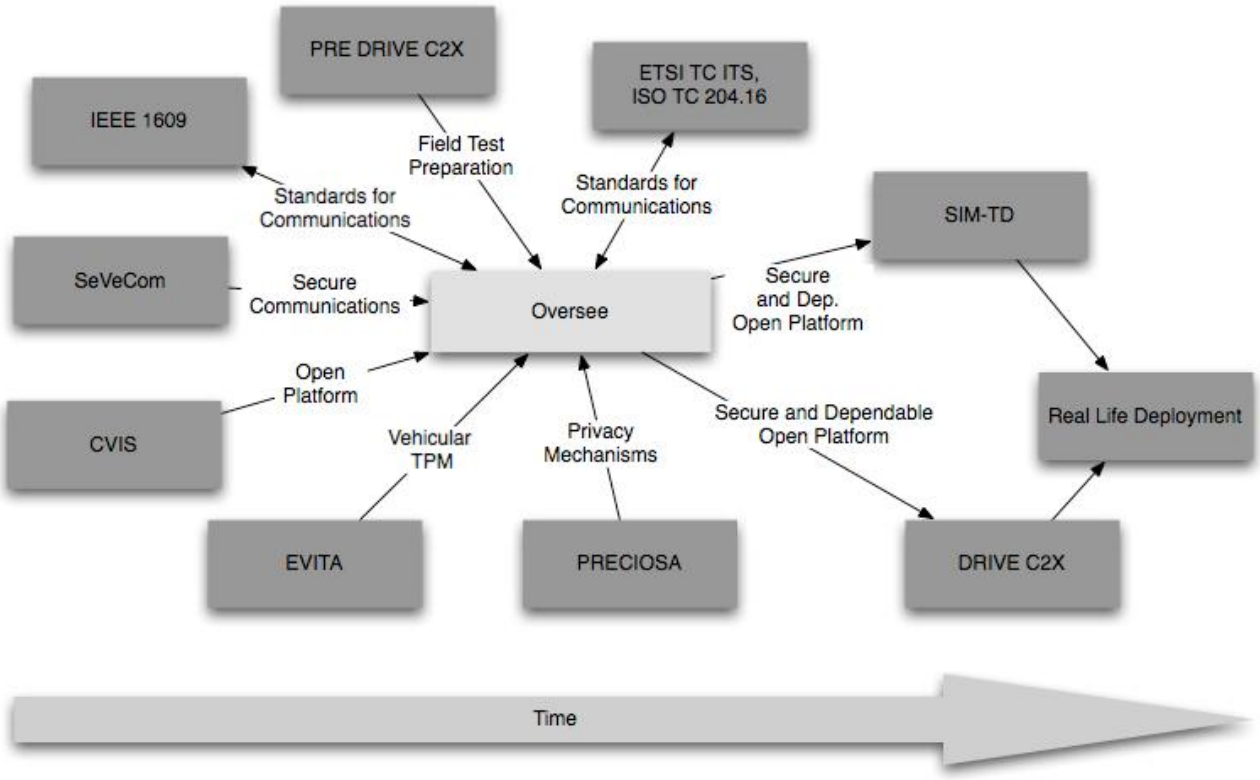

Figure 3 Relation with other research and standardization activities

Fortunately, some of the participants of the OVERSEE consortium are also involved in some of the listed projects (e.g., EVITA, PRECIOSA) and therefore a short link will be easily achievable. For the other projects and activities formal liaisons will be build within the dissemination and exploitation activities of the OVERSEE project.

6 Conclusion and Outlook

In this paper the concept of a secure and open communication and runtime platform called OVERSEE (Open VEhiculaR SEcurE platform) that will be developed and prototypical implemented within a FP7 project of the European Commission, has been introduced. The article described the benefits of such a platform such as (i) faster, less costly and easier development of innovative automotive applications, (ii) foundation of a new market for vehicle independent automotive applications, and (iii) security enhancements for automotive applications and hence improvements for vehicle safety and efficiency.

Because of the magnitude of the automotive market, we are aware that a new platform like OVERSEE cannot be part of every vehicle within a short period. Therefore an incremental introduction into the market has to be the consequence. To sustain this process it is necessary that the OVERSEE platform fits to a wide range of application requirements. Hence the involvement of a wide range of stakeholders from the automotive domain is essential, already in the early stages of the project. Thus, OVERSEE consortium invites appropriate candidates to join the advisory board and hence become part of the OVERSEE project.

7 Acknowledgments

We like to thank all the members of the OVERSEE consortium for their contributions in jointly developing the OVERSEE concept. Namely we would like to thank Alfons Crespo and Matthias Gerlach for providing figure 2 and figure 3 of this paper.

8 Bibliography

[1] E. Coelingh, P. Chaumette, M. Andersson. Open-Interface Definitions for Automotive Systems – Application to a Brake-By-Wire System, Technical Paper 2002-01-0267, SAE International, March 2002.

[2] H.-G. Frischkorn. Automotive Software – The Silent Revolution. In Workshop on Future Generation Software Architectures in the Automotive Domain. San Diego, USA, 2004.

[3] WindRiver Inc. Wind River and Intel Align to Market Optimized Multicore Solutions for Embedded Market. Press Report. www.windriver.com/news/press/pr.html?ID=6661, 2009.

[4] Eurostat Home page. epp.eurostat.ec.europa.eu

[5] E-safety vehicle intrusion protected applications (EVITA) project, www.evita-project.org/

[6] European Commission, Action Plan for the Deployment of Intelligent Transport Systems in Europe. http://ec.europa.eu/transport/its/road/road_en.htm

[7] Toll Collect GmbH, www.toll-collect.de