Project acronym:	OVERSEE
Project title:	Open Vehicular Secure Platform
Project ID:	248333
Call ID:	FP7-ICT-2009-4
Programme:	7th Framework Programme for Research and Technological Development
Objective:	ICT-2009.6.1: ICT for Safety and Energy Efficiency in Mobility
Contract type:	Collaborative project
Duration:	01-01-2010 to 30-06-2012 (30 months)

Deliverable D8.3:
OVERSEE Final Report

Authors:	OVERSEE Concortium
Dissemination level:	Public
Deliverable type:	Report
Version:	1.0
Submission date:	04 November 2013

Abstract

This deliverable is a summary of the OVERSEE results and provides an overview for the reader of the results of OVERSEE.

Contents

List of Figures

List of Tables

List of Abbreviations

API	Application Programming Interface
APT	Debian Advanced Packaging Tool
ARINC	Avionics Radio INC.
ARM	Advanced RISC Machines
CAM	Co-operative Awareness Message
CAN	Controller Area Network
CPU	Central Processing Unit
CU	Communication Unit
DMA	Direct Memory Access
ECU	Electronic Control Unit
EV	Emergency vehicle
EVITA	E-safety vehicle Intrusion protected applications
EXLAP	Extensible Lightweight Asynchronous Protocol
GPL	GNU General Public License
GPOS	General Purpose Operating System
GPS	Global Positioning System
GPSD	GPS Daemon
GRUB	GRand Unified Boot Loader
GWN	Global Wireless Networks
HM	Health Monitor
HMI	Human Machine Interface
HSM	Hardware Security Module
IO	Input Output
IP	Internet Protocol
IPC	Inter Process Communication
IPVI	Inter-Partition Virtual Interrupt
ITS	Intelligent Transportation System
IVN	In-Vehicle Network
LUT	Lookup Table
LWN	Local wireless network
MAF	Major Frame

MCU	Micro Controller Unit
NIC	Network Interface Card
OEM	Original Equipment Manufacturer
OS	Operating System
OSEK	Open Systems and their Interfaces for Electronics in Motor Vehicles
PCI	Peripheral Component Interconnect Bus
PCIe	PCI Express
PKI	Public Key Infrastructure
POC	Proof Of Concept
POSIX	Portable Operating System Interface
PS	Positioning service
PoC	Proof of Concept
RE	Runtime environment
RISC	Reduced Instruction Set Computer
RSW	XtratuM Resident Software
RTOS	Real time Operating System
SDK	Software Development Kit
SKPP	Separation Kernel Protection Profile
SM	Security Module
SVAS	Secure Vehicle Access Service
SecS	Secure Services Partition
TVRA	Threat, Vulnerability and Risk Analysis
UML	Universal Modelling Language
UN	User networks
USB	Universal Serial Bus
V2V	Vehicle-to-vehicle
V2X	Vehicle-to-vehicle or Vehicle-to-Infrastructure
VDX	Vehicle Distributed Executive
VNC	Virtual Network Computing
VNET	Virtual Network
WiFi	Wireless Local Area Network
XAL	XtratuM Abstraction Layer
XM	XtratuM Hypervisor
XM-SDK	XtratuM Software Development Kit

XMCF	XtratuM Configuration File
XMIO	XtratuM IO Virtualization
XML	Extended Markup Language

Document History

Version	Date	Changes
1.0	31.10.2013	Public Version

1 Executive Summary

Until a few decades ago cars were closed, electro-mechanical systems with only a few, isolated, and mainly uncritical IT systems. However, this setting has changed dramatically. Today even compact vehicles have already multiples of the computing power of an Apollo spacecraft from the 1970s while having a few tens of interconnected microprocessors with up to several hundred megabyte of software installed together with first integrated communication capabilities to the outside world. Moreover, this very impressive and dynamic development is still at its very beginning. With the constantly increasing number of vehicular applications, functions, and various (new) stakeholders involved, the requirements for in-vehicle IT performance, flexibility, and complexity will further notably increase.

OVERSEE provides an approach to handle the problems of this complexity by providing a flexible and open platform while ensuring dependability and security by design. The OVERSEE architecture provides isolated runtime environments for deploying applications with different security and dependability requirements. This means that e.g. an application with soft real-time requirements, a safety relevant OEM application and a third party infotainment application can run on the same platform without affecting each other. These applications can share the communication interfaces or hardware resources whereas the access rights to these resources can be restricted by the OVERSEE architecture in a secure way.

The OVERSEE architecture provides mechanisms to securely share the HW and SW resources of the system. The access rights can be defined by the platform owner and are enforced by the architecture. OVERSEE provides various runtime environments (Linux based, OseK, bare metal) and interfaces (drivers for accessing shared interfaces, interface to the HSM, etc.) through widely used standard API's. This enables easy integration of existing applications into the platform.

Furthermore OVERSEE features many security solutions fitted for a multi-partitioned system. The security features are isolated by the architecture, access rights are defined by fine grained policies and enforced by the architecture. The security anchor is provided through a HSM. Furthermore many solutions for encrypting data, secure boot, secure communication, Linux authentication and user management are provided.

2 Description of Main S&T Results

2.1 Summary description of Project Context and Objectives

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. 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.

Modern automotive applications (e.g. postulated in the ITS action plan) and traffic telematics solutions (e.g. theft intervention by Car2X communication, differentiated charging of vehicles by Electronic Toll Collection systems for circulating on certain routes as a way to influence traffic demand) 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 modern automotive applications which could add new functions to vehicles and increase the comfort for vehicle users. These new products and services could stimulate the automotive market and strengthen the innovation leadership of European automotive manufactures and hence sustain and create jobs in the automotive sector.

Today, every new automotive project causes the development of a new and project specific Electronic Control Unit (ECU) which causes immense costs and project risks. Furthermore currently there is no universal device obtainable that is able to connect vehicle internal and external networks in a secure and common way (e.g. for accessing the internet or transmitting of diagnose information). This gap, the high costs and project risks impede the development of new products and services that could be helpful to make automotive traffic safer and more efficient. Additionally the impeded development impairs the growth of the European automotive industry. Therefore new concepts which are currently not available in the automotive field are necessary.

Within this project an open and secure vehicular platform has been developed:

- 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. These will reduce the amount of ECUs needed in a vehicle and thus safe costs for vehicle production. Furthermore the less devices will safe weight 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 OVERSEE acts a secure single point of access to vehicle networks. OVERSEE will provide amongst others a secure interface to the CAN bus.

Additionally the interfaces of OVERSEE are standardized and public which enables the development of vehicle independent plug & play applications. This could be the starting point of a new generation of automotive applications similar to the open source sector in the IT. OVERSEE is a generic approach for the implementation of a wide range of most of the recent and future automotive applications. OVERSEE may solve many of the problems

concerning the development and distribution of new innovative automotive applications and solutions.

Imagine an automotive application designed for a fictive cash transport provider. The customer wants to track the positions of his vehicles. Of course, no eavesdropper is allowed to track the positions of the vehicles due to the fact that the eavesdropper could be able to easy observe the vehicles and hijack the vehicle at an appropriate site. Addition nobody is allowed to forge the vehicles positions as the knowledge of the true actual position at the transport provider control centre could be essential in case of an emergency (e.g. a robbery or accident). Furthermore the control centre of the cash transport provider should be able to monitor the car's status such as motor condition, door sensors, and additional customized devices (e.g. a video control system) to notice a robbery early.

To achieve the requirements of the customer, the application needs access to a Positioning Service, internal vehicle network (e.g. CAN), GPRS or UMTS and cryptographic functions (e.g. encryption and signing). Developing software and hardware as a customer-specific solution would be very expensive and complex, but imagine you can use a generic device providing secure access to vehicle internal networks, external communication networks as well as Positioning Information services and also a protected standardized runtime environment for the execution of the application. OVERSEE provides the mechanisms to overcome these challenges.

The main goals of OVERSEE are:

- Open for new automotive applications also from non OEMs.
- Low price in contrast to project specific solutions because OVERSEE is generic and could be manufactured in mass customisation. Additional software developed for OVERSEE is vehicle independent and therefore safe the effort for adaption to different vehicle environments.
- Protected standardized access to vehicle internal and external networks.
- Protected runtime environments for executing multiple applications on one OVERSEE-ECU, standardized access to cryptographic and security services.

OVERSEE provides a flexible, efficient, dependable and secure platform which enables the deployment of solutions for of many different use cases. Following is a short list of possible use cases which could be efficiently solved with the OVERSEE Platform:

- Reducing of CO2 emissions by secure and non-deniable recording of fuel consumption, driving behaviour and data from motor sensor to enable fair eco-taxes
- Special interest groups (e.g., governmental and authority vehicles, rental vehicles, taxi companies, transport companies, staff vehicles)
- Remote diagnosis / service support and remote software updates
- Automatic theft intervention (e.g., vehicle location and condition)
- Comfort applications (e.g., remote door opener vehicle locating, online navigation, route tracking)
- Integration of (nomadic) user devices (e.g., mobile phones, mobile players, notebooks)

- Vehicle-to-home communication/synchronization (garage opener, music/map downloads, driving data upload such as driven distance, fuel consumption)
- All kinds of V2V and V2I applications (emergency warning, vehicle interactions, intelligent traffic management, infotainment, etc.)
- Digital Rights Management and remote feature activation for vehicular applications (e.g., Rent-a-Car flexible, different driving profiles – gas saving versus fast, different rights for different drivers)

2.2 General OVERSEE Architecture

2.2.1 Virtualization

Virtualization is the enabling technology to run simultaneously into the same hardware independent subsystems with strong isolation and mixing different criticality levels.

Virtualization is one of the key technologies of OVERSEE. Virtualization in OVERSEE is performed by the XtratuM hypervisor. XtratuM is a “Type 1” hypervisor specially designed for real-time embedded systems. XtratuM provides a framework to run several operating systems (or runtime environments) in a robust partitioned environment ensuring strong temporal and spatial isolation properties.

2.2.2 Policy based Information Flow

As stated above, one of the goals of OVERSEE is the provision of a "single point of access" for communication from the outer world to the vehicle components and especially the applications hosted on the OVERSEE platform. Having this single point of access, allows the enforcement of a communication policy controlling access from outside, e.g. by external attackers, as well as limiting the communication capabilities of the installed application, e.g. to reduce the risk of data leaking.

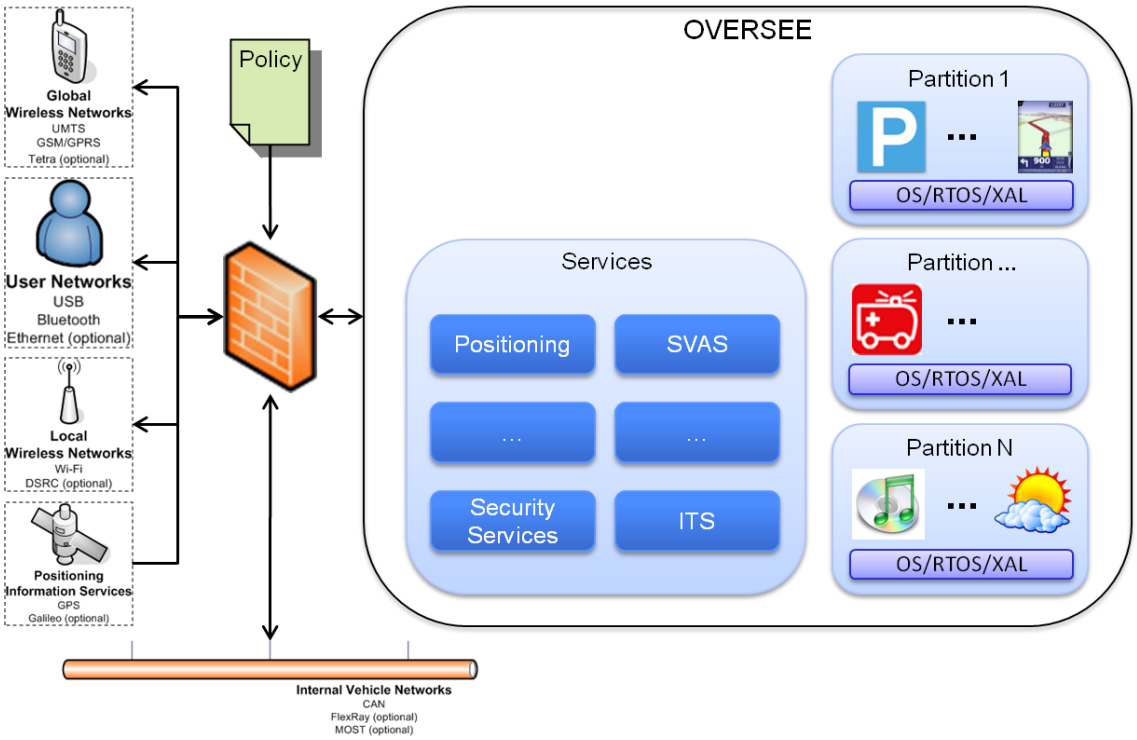


Figure 1 OVERSEE Single Point of Access

In OVERSEE the communication policy is not limited to the connections to the outer world, but comprises also the communication links between the partitions hosting the applications, i.e. inter partition communication (IPC) and the services provided by the OVERSEE platform. Hence, access control to all services, e.g. access to vehicular data or the current position, is enforced on partition level.

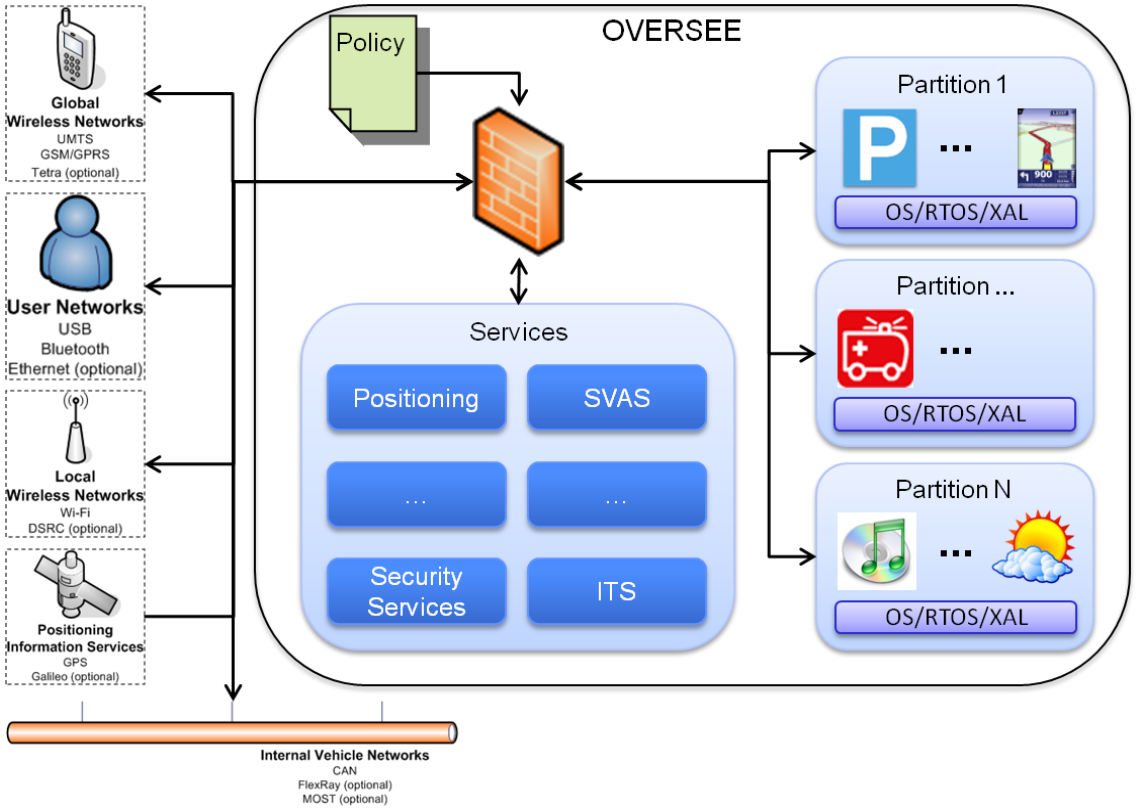


Figure 2 OVERSEE Controlled Infromation Flow

2.2.3 Overall Structure of Security Services

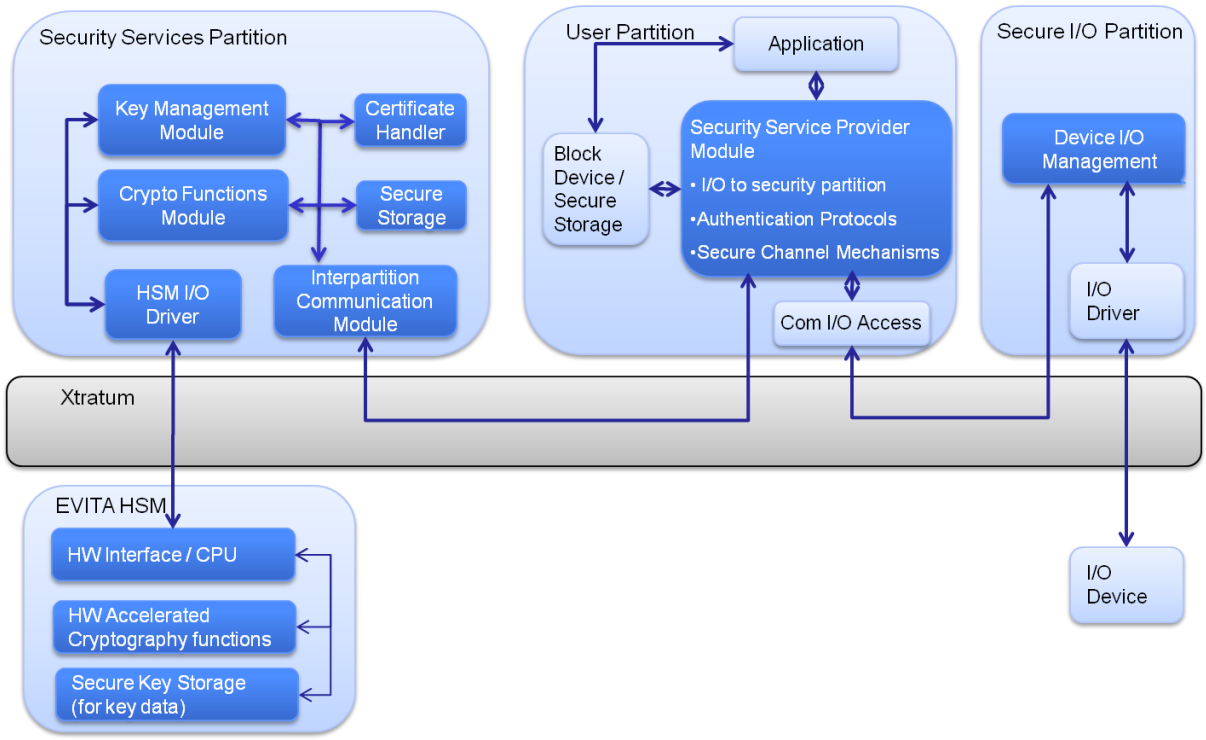


Figure 3: Structure of Security Services

Two main facts play a key role defining the requirements of the security services. First of all OVERSEE aims to provide a platform for ICT applications, which require a set of dependable security services. The second aspect is that OVERSEE provides multiple isolated runtime environments. This demands a strong level of isolation, which also has an impact on the security services.

The OVERSEE security architecture basically consists of two parts. The first part is the hardware security module (HSM). The HSM provides accelerated cryptographic function execution, secure key and certificate storage, and registers for secure boot services. The second part is a dedicated partition for the security services. This partition owns exclusive rights to access the HSM and also hosts building blocks for further security services. The security services partition provides a secure and isolated runtime for the shared security services. Furthermore this partition provides a secure interface for the user partitions to access the security services provided by the secure service partition.

2.3 Virtualization

XtratuM is a “Type 1” hypervisor specially designed for real-time embedded systems. XtratuM provides a framework to run several operating systems (or runtime environments) in a robust partitioned environment ensuring strong temporal and spatial isolation properties.

XtratuM provides services to the partitions running on top of the hypervisor through a well defined interface, depicted in Illustration 1: XtratuM virtualization architecture. The services

provided are grouped under the following categories: scheduling, timing, management, communication and health monitoring services to the running partitions.

The key features of the XtratuM hypervisor are:

- *Temporal isolation*: the hypervisor ensures that the execution of each partition does not depend on the temporal behaviour of any other partitions.
- *Spatial isolation*: the hypervisor ensures that a partition does not have access to another partition's memory area.
- *Static Resource assignment*: The system designer assigns the platform resources (time, memory and devices) to partitions.
- *Spare Server*: Spare time can be assigned dynamically to partitions on demand.
- *Secure I/O partition*: When devices have to be shared among partitions, a Secure I/O partition acting as a I/O server provides virtual devices to the I/O client partitions.
- *System Manager*: A Privileged (and trusted) "system partition" can monitor and manage other partitions.

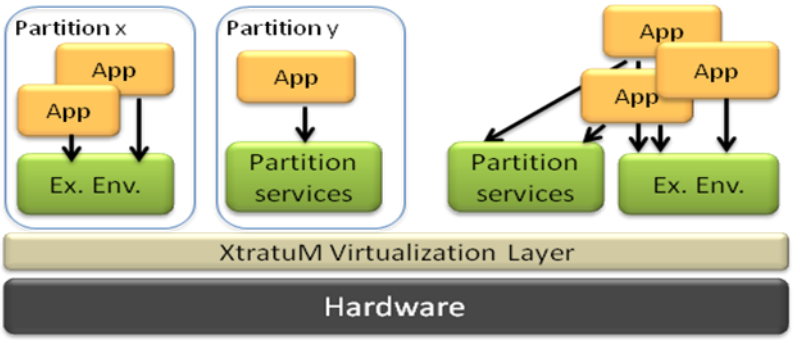


Illustration 1: XtratuM virtualization architecture

The XtratuM hypervisor provides the following major benefits: First, critical OVERSEE components can run in a reliable environment not being perturbed by other components. Next faults are isolated at the partition level, enabling the recovery of faulty partitions without interfering with the rest of running partitions.

The isolation offered by XtratuM provides for an ease of the certification effort by reducing the side effects, while at the same time easing system reconfiguration and upgrading. Last but not least, the system configuration allows for improve the control of real time behaviour.

2.3.1 Temporal Isolation

XtratuM ensures strong temporal isolation between partitions through a fixed scheduling plan to achieve deterministic scheduling following the ARINC-653 philosophy. Time windows are allocated statically for the partitions through the configuration file. While on run-time, each partition will only be executed inside its predefined slot(s) of time.

However, within the OVERSEE project, there have been included several mechanisms to increase scheduling flexibility while retaining the temporal isolation. These mechanisms

include, first, the ability to define several scheduling plans and, second, the possibility of dynamically schedule partitions inside certain allowed time windows.

2.3.2 Spatial Isolation

XtratuM ensures strong spatial isolation between partitions thanks to the MMU provided by the Intel processor. Memory protection on Intel processors is a complex subject. In the simplified view, Intel processors provide four levels of memory protection, also known as rings. Ring 0 has the highest privileges and full access to system resources, while the lowest ring 3 is the more restricted one. Here, XtratuM runs on ring 0, and makes sure that permissions granted to partitions do not jeopardize the spatial isolation.

2.3.3 Static Configuration

The system configuration is specified through a configuration file (XM_CF) using XML. The configuration is translated to static data structures that are used by the hypervisor to ensure the isolation properties. Fully static (unmodified) system specification ensures all information flows specified are secured.

2.4 Controlled Information Flow

OVERSEE offers a set of sophisticated services – especially for communication - to applications installed in the OVERSEE partitions. Which applications have access to which services is formulated in a per partition communication policy. This policy realizes the controlled information flow in the OVERSEE platform. The current chapter summarizes how the enforcement of this policy is implemented.

2.4.1 General Introduction & Architecture

The isolation based architecture of OVERSEE provides the foundation for the implementation of the enforcement of the communication policy. Isolation based means that in principal all applications installed in one partition are isolated, i.e. having no communication means, from all other applications - executed in other partitions - and the OVERSEE services. Only by explicit definition of a communication mean in the hypervisor, communication among partitions – including the communication with the OVERSEE services – is possible. This is the first - and most strict - layer of the implementation of the communication policy and the foundation for the implementation of the finer grained communication policy described in the rest of this chapter.

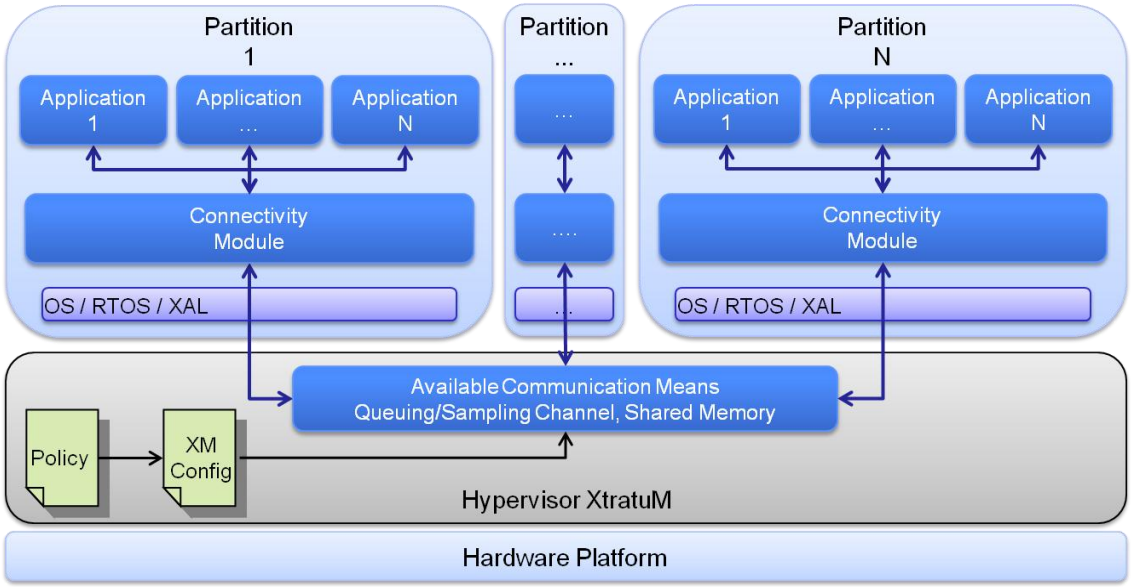


Figure 4 OVERSEE Communication Policy and XM Config

All external communication interfaces – including the interface to the vehicle internal network – are bound to the so called secure I/O partition. This partition runs the drivers for the interfaces and is connected – via the hypervisors internal communication means as described above – to the other partitions, executing the applications. For each service provided in the secure I/O partition a communication policy is enforced. This policy restricts – depending on the current service – access at all or access to specific capabilities of the service, e.g. a special set of vehicle information in SVAS.

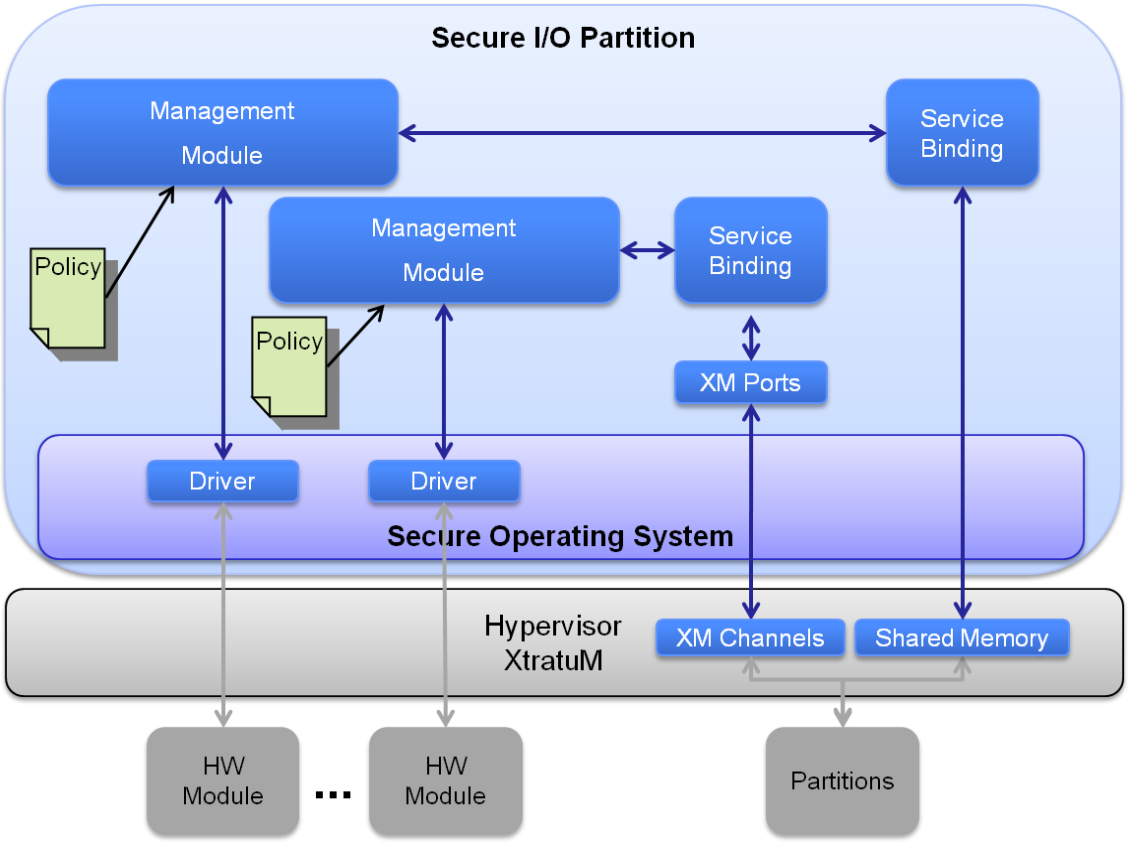


Figure 5 Generic Secure I/O incl. Policy

2.4.2 List of Interfaces/Services

The following list of interfaces/services, according to, have been considered and largely implemented in OVERSEE:

No.	Abbr.	Interface / service runtime environment layer	Physical interfaces or devices
1	SVAS	Secure Vehicle Access Service	CAN-Transceiver
2	USB	Universal Serial Bus	Universal Serial Bus module
3	SecS	Security Services	Hardware Security Module
4	SMem	Secure Memory	Protected memory area within the OVERSEE memory
5	PoS	Positioning Service	GPS receiver, vehicle sensor if applicable
6	IPaC	Inter-partition communications	No physical representation
7	ITS	ITS Communication	ITS G5, CEN-DSRC transceivers
8	IP	IP Connection	WiFi, GPRS, UMTS modules
9	BT	Bluetooth	Bluetooth module
10	Cell	2G/3G Voice Connection	GSM, UMTS module
11	HMI	Human Machine Interface	Graphic output, keyboard, pointer device
12	Audio	Audio	Audio in/out device

Table 1 Mapping of the interfaces and services to the physical interfaces and devices

2.4.3 IP

The IP (Internet Protocol) is the most common communication protocol in current IT systems. For OVERSEE, IP communication will be used to connect to extern entities, e.g. servers in the internet, as well as to more advanced services in the secure I/O partition, e.g. SVAS as described below.

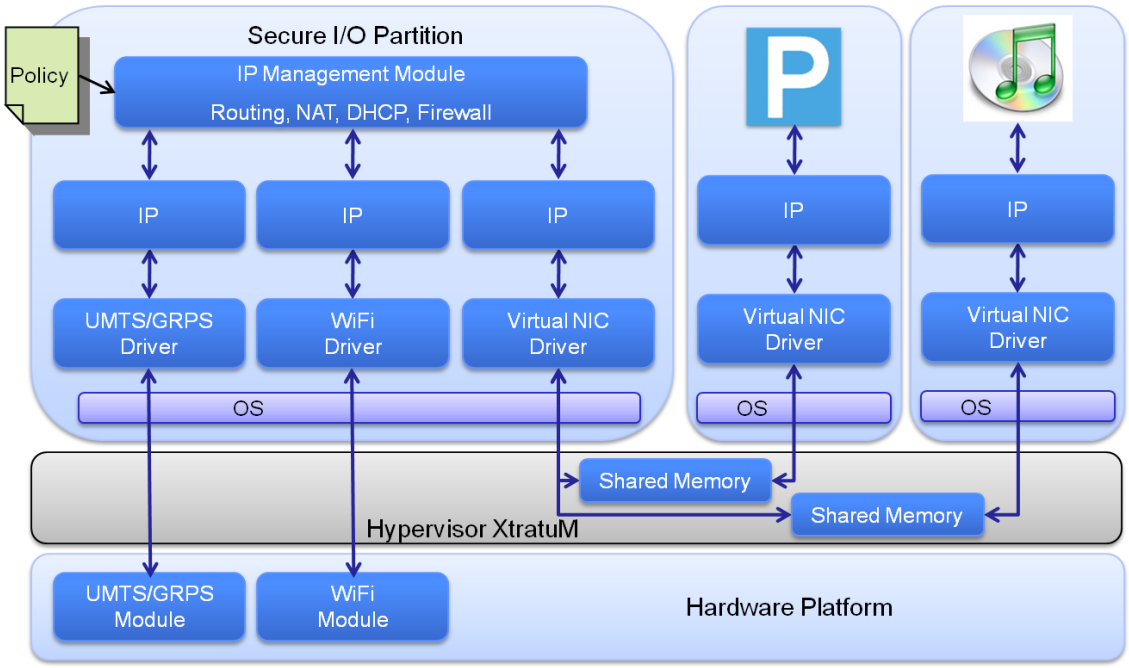


Figure 6 IP based communication with Policy

Each partition which should have access to IP based communication shares a memory area with the secure I/O, which is used for the implementation of a virtual network interface. This virtual network interface is bound to a static IP address which identifies the current partition. IP tables, which is part of the Linux stack used in the secure I/O, is used to enforce the communication policy for IP based communication. Thus, for IP based communication controlled information flow is enforced by:

- Configured shared memory areas (XM configuration file)
- Configured virtual network interfaces in the secure I/O
- IP routing configured for IP tables in the secure I/O

2.4.4 PoS – Positioning Service

The positioning service exhibits its functionality via two communication means, c.f.:

- Shared memory with IP connection, for the well known GPSD service
- Sampling Channel, for the provision of a virtual com port driver and native access to positing data

For GPSD based access to the current position information flow is enforced by:

- Configured shared memory areas (XM configuration file)
- Configured virtual network interfaces in the secure I/O
- IP table rule stating network interfaces with access to the port of the GPSD daemon in the secure I/O

For the sampling channel based implementations (native access and virtual com port) the controlled information flow will be enforced via the XM configuration.

2.4.5 Audio

Access to the audio output interface of the platform is provided via Pulse Audio and ALSA, which are both part of the used Linux stack in the secure I/O, c.f. Thus, the same rules for controlled information flow apply than given above for the GPSD. Furthermore, a mixer was implemented to mix audio streams of different criticality, c.f.

2.4.6 USB – Universal Serial Bus

Access to USB devices is currently limited to USB storage devices. The memory area of the USB storage devices will be forwarded as a virtual disk to the partitions. Virtual disks are implemented by utilization of shared memory in the XM hypervisor. The partitions which should be able to access the content of USB storage devices are further limited in a configuration file. Thus, controlled information flow - with respect to USB storage devices - is enforced by:

- Shared memory for the virtual disks, as configured in XM hypervisor
- Configuration file in the secure I/O restricting partitions with USB access

2.4.7 SVAS – Secure Vehicle Access Service

The secure vehicle access service provides the capability to access data on the vehicle internal bus, i.e. Controller Area Network (CAN) in the current OVERSEE version. Currently SVAS is implemented on top of IP. Each SVAS server in the secure I/O exhibits therefore a specific set of data objects - representing vehicle signals. Thus, controlled information flow concerning vehicular data is enforced by:

- Configured shared memory areas (XM configuration file)
- Configured virtual network interfaces in the secure I/O
- Configured SVAS servers with their specific sets of data objects.
- IP rules binding the IP addresses of the virtual network interfaces to the SVAS instances

2.5 Security Architecture

The virtualized architecture of OVERSEE enables different possibilities to enhance security on an IT platform. Main features are the possibility to minimize the attack surfaces of many modules of the platform and also to minimize the effects of a successful attack. The security architecture of OVERSEE benefited from this fact and focused on building upon the opportunities a virtualized architecture can provide.

2.5.1 Secure Service Partition

From the architectural aspect a separate isolated partition (the Secuity Service Partition) has been proposed for the security services provided by the platform. The main reason is to

minimize the attack surface to the security services by providing clean interfaces to them. XTratum assures the security services to run dependably and uninterrupted in the isolated partition and avoids any attack by malicious software or backdoors in other partitions. Also any interference with software from other partitions is prevented and a more stable execution is assured. Although this has not been realized in the proof of concept implementation due to insufficient resources of the platform this architecture has been suggested throughout the project. Instead the Secure I/O Partition has been also used as the Security Service Partition.

2.5.2 Hardware Security Module

The integration of a hardware security module builds the core (and trust anchor) of the security services provided by the platform. For the proof of concept the EVITA HSM has been chosen. The EVITA HSM is a security module designed for the needs of an automotive telematic device and/or electronic control unit. The security architecture of OVERSEE aims to make effectively use of the capabilities of the HSM but also restrict the access to the HSM services. The risk of an attack to a software module having access to the HSM can so be restricted in an effective way. For this reason the logical access to the HSM has been granted to the security service partition in OVERSEE and forwarded to the other partitions through dedicated interfaces. Another focus of OVERSEE, sticking with standardized interfaces, has also been followed in this approach. A PKCS#11 interface has been build around the HSM driver. This interface has been shared with the other partitions with a server in the Security Service, again as a PKCS#11 interface. This enables the use of the many applications readily using pkcs#11 interface for accessing security modules. Furthermore this enables also the integration of other security modules providing a PKCS#11 interface. The server in the Secure Services Partition provides a layer of access control between the other partitions and the HSM Services which can enforce any access policy to the HSM per partition.

2.5.3 Secure Communication

Further on secure communication facilities have been built to ensure secure communication between a partition and an external entity. The enforcement of the secure communication is done in the Secure Services Partition which means no software in the user partition or any user accessing the user partition can manipulate or read the configuration or keys used for the secure connection.

2.5.4 Secure Data Storage

A telematic or infotainment platform also hosts a lot of sensitive data which have to be stored in a secure way. OVERSEE provides a central service for providing secure storage. The data can be stored on a disk which is encrypted with a key securely stored in the HSM. This disk can be forwarded to the user partition as a standard disk making the whole process transparent for the user partition.

2.5.5 Central Directory Service

In a multipartitioned system with multiple runtime environments the handling of authentication and authorization data is also an essential issue. Furthermore this information also has to be maintainable in a secure and easy way. OVERSEE provides for the proof of concept a central directory service and a library for the user partitions to easily access the service. The access rights to the directory server can be defined in the Secure Service Partition. Furthermore a service for injecting/modifying/deleting entries into the directory service in a secure way is implemented. With this service new users and policies can be introduced to the platform by the authorized authority through secure tokens (certificates). These certificates can be signed by the authorized authority (e.g. OEM) and verified by the platform. This enables injecting new users, access rights to resources or policies for various services. An example would be granting access to the repair shop for updating the software. In this way only authorized repair shops can be granted access to the platform. Furthermore the access rights of the new software can also be managed with the certificate.

Again a standardized interface has been used, the LDAP protocol, to access the directory service. The central handling of authentication and authorization data is essential for the security and flexibility of the system. To enable such a service an LDAP (Lightweight Directory Access Protocol) server (e.g. openLDAP) is provided by the security service partition. This server can be invoked by the other partitions by NSS (Name Switch Service) or LDAP based PAMs (Pluggable Authentication Modules). Also direct usage of the LDAP server through look-up services can be used to retrieve data to validate information as authorization or roles of a specific user, partition or any other entity. Further functionalities like single sign-on are built upon this infrastructure. The access right to the LDAP server and individual data is restricted in the partition level.

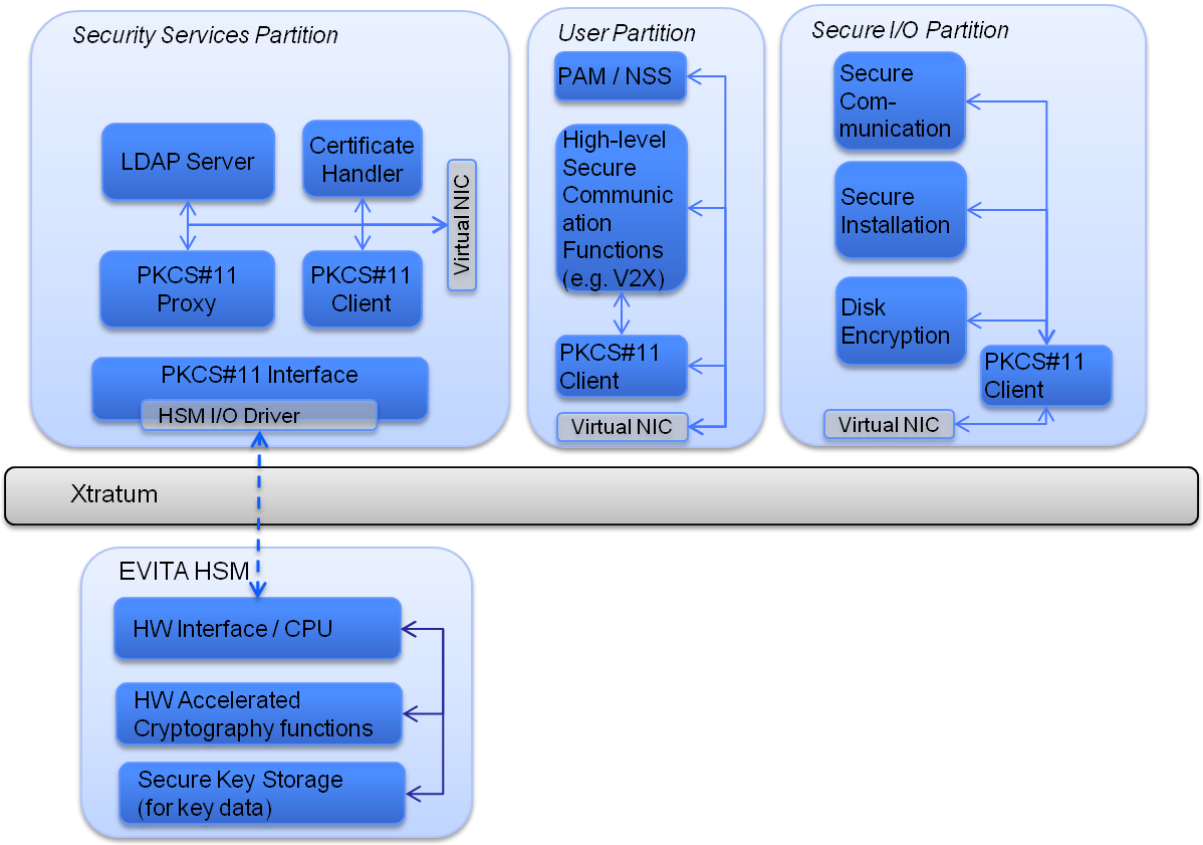


Figure 7 - OVERSEE Security Architecture

2.5.6 ITS Communications

The access to ITS networks is controlled by the ITS Communications Service within the Secure I/O partition. It constitutes the single point of access to all kinds of ITS communications within OVERSEE. It unifies different ITS technologies like CEN-DSRC and ETSI ITS-G5. All ITS messages are received, sent, assembled, signed, verified, encrypted, respectively decrypted within the ITS communications component (possibly using functions provided by the security services partition). ITS applications running in user partitions may receive or send messages through the ITS Communications Service using the OVERSEE ITS API. Figure 8 shows an architectural overview on the usage of ITS services by the means of the use case “Emergency Vehicle Warning”.

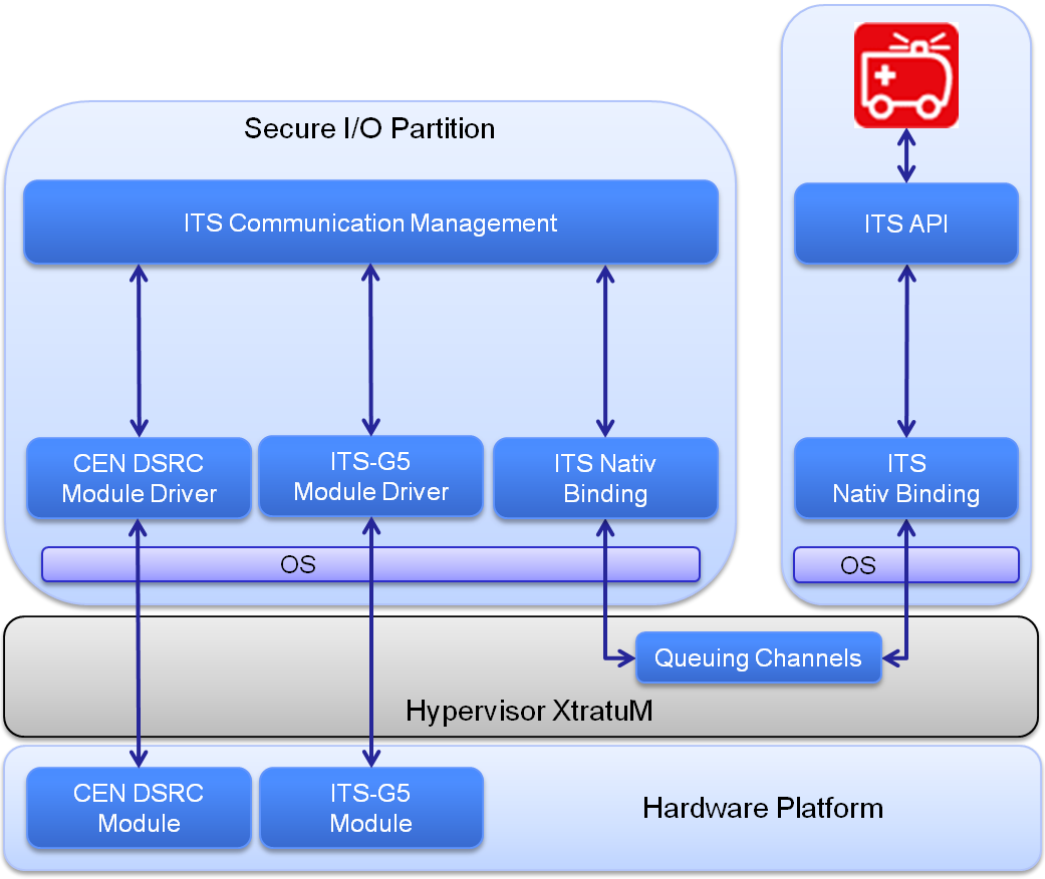


Figure 8: ITS communication

The ITS communication service provides all necessary functions for ITS communications and manages basic communication functions independently. Its field of duty covers the following tasks:

- Receive incoming Cooperative Awareness Messages (CAMs) from neighbouring cars. CAMs may be delivered to privileged user partitions or optionally evaluated and incorporated into a Local Dynamic Map (LDM).
- Optionally, the relevance of incoming messages may be checked. Based on the LDM and the vehicle's location a received message can be determined as relevant or not in the current context.
- Broadcast the current vehicle status periodically into the ITS-G5 network. Therefore, information like the vehicle's location and speed is gathered and condensed into CAMs.
- Deliver incoming Decentralized Environmental Notification Messages (DENM) to registered (and privileged) user partitions.
- Send different types of message (e.g., DENMs) on demand of ITS applications, which are running in privileged user partitions.
- Perform cryptographic operations and plausibility checks on all kinds of ITS messages:
    - Verify and/or decrypt incoming messages

- Sign and/or encrypt outgoing messages

- Optional support for further protocols like CEN-DSRC

The respective standards already define security measures for ITS communications. Some of them (e.g., signing and verifying of messages) will be implemented in OVERSEE's ITS communication service.

2.5.7 ITS - Internal Architecture and Components

Figure 9 shows an overview to involved modules within the ITS communications component and interfaces to other services, which includes

- The **ITS authorization layer** controls any access from user partitions to the ITS building block, so that only authorized applications can use functions of the OVERSEE ITS API. The authorization layer must not necessarily be part of the ITS building block; alternatively, a global authorization layer for the secure I/O partition could ensure authorized access of applications to all building blocks inside the partition.
- The largest module of the ITS communication building block provides **ITS facilities**. It is divided into multiple subcomponents:
  - The **message dispatcher** handles incoming as well as outgoing messages. Depending on an incoming message's type, it is delivered to the local dynamic map for CAMs and DENMs, or registered ITS applications for application specific messages.
  - According to ITS standards and protocols messages are encoded in a binary format. Hence, conversion from this format to an internal representation and vice versa is required. The respective components assemble outgoing messages and parse incoming messages. Additionally, security function such as message signing and verification could be invoked at this point.
  - Incoming CAMs and DENMs from neighbouring vehicles and road-side units are examined and incorporated to the **local dynamic map** (LDM), so that the LDM always holds the vehicles current environment. Specific messages and situations may trigger events that are presented to subscribing ITS applications.
  - The **ego state register** (ESR) holds the ITS relevant information of the current vehicle state. Most state information – such as the vehicle's geographic location, its speed, or its steering angle – is gathered from the SVAS. Additionally, ITS applications may set optional application specific attributes, e.g., the state of emergency lights and siren of an ambulance.
  - The **event generator** periodically analyses the current attributes of the ESR, typically with a frequency of at least 1Hz. Depending on the state, it creates appropriate events that are broadcasted as CAM or DENM.
- The **ITS transport and networking** module provides low-level networking features, such as geo-routing. This module may alternatively be implemented outside the ITS building block as part of an bigger-sized ITS-G5 networking adapter.

- The **ITS security** module examines incoming messages in terms of integrity, confidentiality (if encrypted), and freshness. Outgoing messages may be signed. Additionally, it provides facilities to encrypt and decrypt messages. OVERSEE's security services should be used for cryptographic operations and secure storage of private keys.
- The **key management** module maintains certificates belonging to the vehicle including its long-term identity and short-term pseudonyms as well as cached public keys of CAs and other communication participants. One of its responsibilities is periodic renewing of pseudonyms. To ensure integrity and confidentiality of private keys, the secure storage of the OVERSEE security services should be used.
- The **CEN-DSRC** module provides CEN-DSRC specific functions. It sends messages to CEN-DSRC network and dispatches incoming messages to subscribed applications.

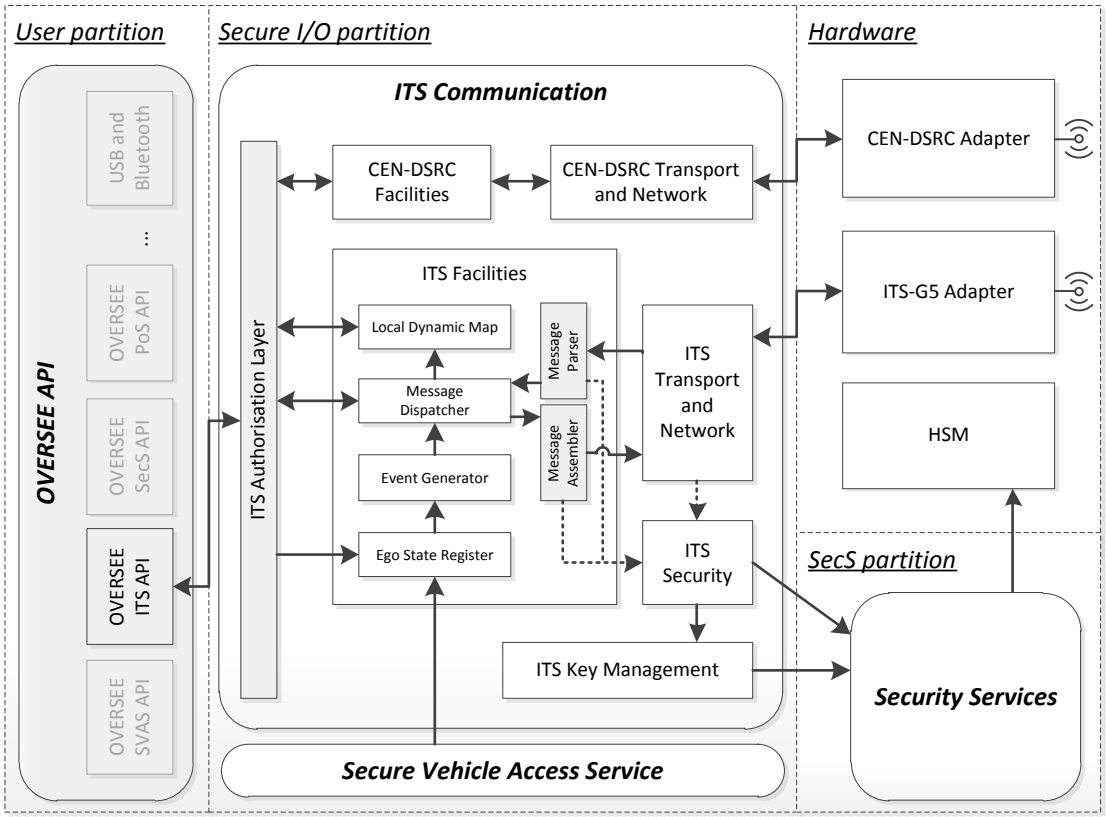


Figure 9: ITS communications building block

3 Main Dissemination Activities

3.1 Main Dissemination Activities

Along the three years of the project, the OVERSEE consortium promote the projet through dissemination. The following table provide the list of the dissemination activities held during the project in terms of conference attends and papers published.

Date	Description	Communication Activity	Impact & Audience
02/2010	Participation at eSecurity Working Group Meeting of the eSafety Forum	Discussion regarding recommendations for the automotive industry	Clarification of different opinions concerning future security recommendations; Automotive security experts
04/2010	Participation at a local industry trade show "Automotive Forum Südwestfalen"	Poster	Information of security challenges fur supplier industry; Local automotive suppliers
04/2010	ETSI ITS WG5 Security Meeting ITSWG5#14	Validation if ETSI standardization approaches for ITS communication do influence OVERSEE approaches and vice versa	Raising the awareness of ETSI ITS standardization experts concerning OVERSEE; ITS standardization experts
04/2010	Preparation of a general OVERSEE press release a version of the OVERSEE press release for the local press sections for the OVERSEE website OVERSEE fact sheet	Publication of information for different receivers	Provision of information concerning the OVERSEE vision, facts and figures as well as the planned timeline; Different audience (EU, interested people, experts)
04/2010	Participation at ISO Subcommittee 27 meeting	Discussion about standardization in the field of embedded security (light weight cryptography, group key cryptography)	Information concerning future standardization activities regarding light-weight embedded security; ISO SC 27 members
05/2010	3rd ETSI/CEN Workshop Berlin, Germany	Contact and discussions with experts from CEN.	Collect viewpoints out of other standardisatio bodys; ITS standardisation experts
05/2010	Preparation and submission of accepted paper "Upcoming Trends in the Automotive IT and Associated Security Challenges" for 3rd International Conference on Telecommunications,	Paper	Influence on future in-vehicle security aspects; Communication experts

	Electronics and Informatics		
05/2010	Joint Meeting eSecurity WG and article 29 Working Group	Discussion privacy issues for ITS related applications and systems	Raising the awareness for OVERSEE as a possible solution to overcome privacy breaches; Automotive security and privacy legislative experts
05/2010	Participation in the Eighth European Dependable Computing Conference, EDCC-8 2010, Valencia, Spain, 28-30 April 2010	Partitioned Embedded Architecture Based on Hypervisor: The XtratuM Approach. Alfons Crespo, Ismael Ripoll, Miguel Masmano, pp 67-72. .	
05/2010	Submission of the paper and presentation "AppStore für Autos: Über neue Anwendungsfelder und die zuverlässige Absicherung zukünftiger automobiler IT-Plattformen" , 2. Elektronik automotive congress, Ludwigsburg, Germany	Paper; Presentation of Open Platforms for Cars and security aspects.	Influence on future in-vehicle security aspects; Automotive experts
06-2010	15th Ada-Europe International Conference on Reliable Software Technologies, Valencia, Spain, June 14-18, 2010	Tutorial: "HYPERVISOR TECHNOLOGY FOR BUILDING SAFETY-CRITICAL SYSTEMS: XTRATUM A. Crespo, I Ripoll (3 hours)	
06/2010	ETSI TC ITS WG5#15 Trondheim, Norway	Discussions and information exchange about ITS related topics.	Keeping in touch with the on-going standardisation work; ITS standardisation experts
06/2010	"Open platform" workshop of DG trans	Discussing different opinions of open platforms in the automotive domain	Provision of information of the OVERSEE vision an approach; Open platform experts related to DG trans
06/2010	eSafety Forum Steering Group meeting	Presentation and discussion regarding recommendations concerning automotive security aspects to the eSafety Forum	Provision of automotive security information; eSafety Forum decision makers
07/2010	Radio interview for the	Publication of information for	Provision of information concerning the OVERSEE

	"Westdeutscher Rundfunk"	everybody (mass media)	vision; Everybody (mass media)
07/2010	Participation at the workshop "Privacy in ITS" (Preciosa)), Berlin	Discussion privacy issues for ITS related applications and systems	Raising the awareness for OVERSEE as a possible solution to overcome privacy breaches; Privacy legislative experts
07/2010	Preparation and submission of accepted paper "Next Generation of Automotive Security: Secure Hardware and Secure Open Platforms" for 17th ITS World Congress, Busan, Korea	Paper	Influence on future in-vehicle platform development; Automotive experts
10/2010	C2C-CC Security & Privacy WG Meeting	Presentation of the OVERSEE project	Introducing the vision of OVERSEE to V2X security experts from the Car to Car Communication Consortium
11/2010	Participation at the ESCAR conference. (Bremen)	Discussion of security issues for ITS related applications and systems	Raising the awareness for OVERSEE as a solution for a secure and open platform; Automotive and security experts
11/2010	Car to Car Forum 2010, Paris, France	Discussions and information exchange in the ITS communications domain. Side note: Florian Friederici (Fraunhofer FOKUS) had a talk on ITS Security on the Forum, which was however not OVERSEE centric.	Staying in close contact with stakeholders, disseminating the importance of secure vehicular communication systems.
12/2010	Preparation and submission of paper "Open platforms on the way to automotive practice" for 8th ITS European Congress, Lyon, France	Paper	Nothing yet (hoping to influence activities regarding open in-vehicle platforms); ITS experts
10/2010	conversations with different departments within the Volkswagen Group	Presentation of the project	Other Departements of the VW group are aware of the OVERSEE existence.
12/2010	2. NRW Forschungstag IT-Sicherheit, Düsseldorf (2nd IT-Security Research Symposium of the German Federal State North Rhine-Westphalia)	Presentation and discussion of Open Platforms for Cars and security aspects.	Influence on future in-vehicle security aspects; IT-Security experts

02/2011	Paper in a journal (Planned publication Feb 2-3)	Device Virtualization in a Partitioned System: the OVERSEE Approach J. Sánchez, S. Peiró, J. Simó, M. Masmano, A. Crespo Jornadas de Tiempo Real. Madrid	
03/2011	Presentation with the title "OVERSEE - Potentials and Challenges for the Automotive Industry" at embedded world, Nuremberg	Presentation and Discussion	Experts on embedded systems and automotive.
04/2011	Presentation of OVERSEE in ICT for transport concertation meeting	Presentation of OVERSEE. Discussion on platforms.	Awareness within the ICT community
04/2011	Participation at ISO Subcommittee 27 meeting	Discussion about standardization in the field of embedded security (light weight cryptography, group key cryptography)	Information concerning future standardization activities regarding light-weight embedded security; ISO SC 27 members
05/2011	Presentation with the title "Open Platforms On the Way To Automotive Practice" at ITS in Europe in Lyon	Presentation and Discussion	Presentation of OVERSEE open platform approach for automotive and ITS; ITS experts
10/2011	Presentation with the title "Towards A Shared Digital Communication Platform for Vehicles" ITS world in Orlando	Presentation and Discussion	Presentation of OVERSEE open platform approach for ITS development and deployment; ITS experts
Misc.	Participation at Escar (Dresden), Evita Workshop (Erlensee), Final year event EuroBITS (Bochum)	Informal dissemination of OVERSEE results and concepts	Information concerning OVERSEE and the open platform approach for ITS; automotive vendors (e.g. Hyundai), other research projects, experts on embedded security
	Publication of a paper with the title "Platforma de TI para veículos," in RTI - Redes, Telecom e Instalações, vol. XII, no. 136, pp. 84–94,http://www.arandanet.com.br/midiaonline/rti/2011/setembro/index.html, 2011.,	Paper	Dissemination of OVERSEE results to south America, especially Brazil.

07/2011	Presentation at CAST Workshop "Embedded Security" (12. July Darmstadt Germany)	Presentation	Presentation with topic "On the way to a secure and open in-vehicle platform"
07/2011	Meeting with ADAC (Mr. Coldewey) for a general discussion on future of open platforms.	Discussion	Joint demonstration and possible cooperation's were discussed.
12/2011	Telephone conference with Hyundai	Discussion	Discussion on possible cooperations with Hyundai
12/2011	Application to the ETSI Workshops (Security Workshop 18 January, France and ITS Workshop 9. February Qatar) (Accepted for both and presentations done)	Presentation	Consortium requested slots at the ETSI workshops. Both got accepted and presentations were done in first quarter 2012.
	Participation in the C2C-CC TC Meeting,	general dissemination of OVERSEE	
	Included OVERSEE interface idea into ETSI DRAFT TS 102 723-9 (SF-SAP)	Standardization	A proposal has been prepared and forwarded to ETSI.
02/2012	Miguel Masmano, Salva Peiró, Jordi Sánchez, Jose Simó, Alfons Crespo. "Virtualisation in a Partitioned System". Embedded Real Time Software and Systems (ERTSS2012). Toulouse, France.	Paper and presentation	
	Participating and presenting at the ETSI ITS workshop in Doha.	Presentation with the title "Designing Open Computing Platforms with Security in Mind", afterwards discussion with the auditorium concerning the pros and cons as well as the feasibility of an "open" ITS platform.	ETSI ITS Community as well as international stakeholder from the ITS and related domains.
	Discussions on OVERSEE interfaces within ETSI		
07/2012	A presentation was made for the I-Mobility Legal Issue Working Group: Isolation (and OVERSEE	Dissemination toward standardization activity. Antonio Kung	Presentation of the possible solutions for legal issue about data privacy, including

	platform) as a possible solution to ensure data privacy		OVERSEE.
10/2012	ITS World 2012, "Enabling the Deployment of Open In-vehicle ITS Station" long paper.	Long paper and presentation, Hakan Cankaya*, Cyril Grepet, Jan Holle and José Simo	Raising awareness of the need, hurdles and solution to enable the use of open ITS station as OVERSEE platform. International ITS community and stakeholders from related domain.
10/2012	ITS World 2012, "OVERSEE - Investigation of requirements and analysis of solutions for an in-vehicle open and secure platform"	Paper and Presentation	A presentation was held in the ITS World 2012 Conference about handling security requirements for an open in-vehicle platform.
10/2012	ITS World 2012, "OVERSEE - A secure and open in-vehicle ITS station"	Presentation and publication of a related paper in the conference Proceedings, title "OVERSEE - A secure and open in-vehicle ITS station". Discussion with the auditorium after the presentation and at the booth of the EC.	International ITS community and stakeholders from related domains. Draw of interest concerning the applied technologies, e.g. virtualization in the automotive domain, especially from OEM stakeholders. Several discussions concerning the term "open" and the related skepticism in the automotive industry
	papers for RTLWS14		
12/2012	OVERSEE Final Event in Brussels	Presentation, discussion, exhibition of the results of OVERSEE Project	Presentation of the results of the OVERSEE project to an audience composed of car manufacturer, automotive associations, automotive suppliers, European commission representative.

4 Potential Impact

This section is based on material presented in **Fehler! Verweisquelle konnte nicht gefunden werden.**. It also contains individual exploitation information as presented during the Final Review of the OVERSEE Project held in January 2013.

4.1 Automotive Market Situation

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. 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:

- The use of vehicles should be as safe as possible for the user and all other traffic participants, especially with regard to accidents with injury of persons and fatalities.
- The use of vehicles should be as efficient as possible, especially with regard to the emission of CO_2 and the consumption of fossil fuels, but also with regard to the efficient use of road infrastructure.

Modern automotive applications (e.g. postulated in the ITS action plan) and traffic telematics solutions (e.g. theft intervention by Car2X communication, differentiated charging of vehicles by Electronic Toll Collection systems for circulating on certain routes as a way to influence traffic demand) 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 modern automotive applications which could add new functions to vehicles and increase the comfort for vehicle users. These new products and services could stimulate the automotive market and strengthen the innovation leadership of European automotive manufactures and hence sustain and create jobs in the automotive sector.

Today, every new automotive project causes the development of a new and project specific Electronic Control Unit (ECU) which causes immense costs and project risks. Furthermore currently there is no universal device obtainable that is able to connect vehicle internal and external networks in a secure and common way (e.g. for downloading tolling information or transmitting of diagnose information). This gap, the high costs and project risks impede the development of new products and services that could be helpful to make automotive traffic safer and more efficient. Additionally the impeded development impairs the growth of the European automotive industry. Therefore new concepts which are currently not available in the automotive field are necessary.

The Automotive Industry is a fast growing innovative and economic key industry segment. In addition the Automotive Industry is a very cost sensitive and on the other hand needs to take as much effort as possible to provide safety measures for all road users.

The OVERSEE project provides access to vehicular internal and external network in a secure manner and therefore enables e-safety use cases, which will be crucial for vehicular

applications to meet the future trends. In addition OVERSEE offers an open and secure application platform, hence the high costs and risks for the development of new safety application will be limited. There is no project known up to date, that provides an automotive platform providing an open platform using virtualization.

Therefore, with the knowledge and technology, the industry will be able to further decrease time to market for innovative and connected car functionality, as well as reduce the cost and risks. This will lead into new global market shares and safeguarding existing shares due to technological leadership.

The strategy is to aggregate all key stakeholders, the automotive industry (i.e. OEMs and suppliers), the application providers (i.e., leading tolling system provider), security experts in the project in order to achieve a complete and consistent system solution, which subsequently can be transformed into an industrial series development. The envisaged to provide the Open VEhiculaR SEcurE platform as an open specification will speed up the economic success for the automotive and the dissemination of safety related car functions.

4.2 Business Model Consideration

Business model considerations will have a strong impact on how the platform will be exploited. The business model will in particular depend on the underlying value chain that is used and the channel through which ITS applications are deployed (e.g. through OEMs, through road operators or telecom operators).

It is believed that the flexibility and cost efficiency introduced of such a platform as OVERSEE could enable a new way to study the market in the ITS (for cars) and the automotive domain.

Currently three business models have been identified. *

4.2.1 Application-Centric Business Model

This business model will mainly be the focus of companies involved in application software development. It could be applied to the three main application domains identified for OVERSEE (ITS, Infotainment, Automotive).

This model relies on the vision that there is a widely deployed standardized secure open platform with standardized interfaces for automotive ITS, (e.g. API, Middleware, virtual driver to access ready-to-use hardware transparently). These interfaces make it easy to develop applications. This model is inspired from the android or iphone model. It is also the model implied in past FP projects such as GST or CVIS (note that with respect to these projects, Oversee is focussing on security and dependability, while GST and CVIS focused on application support).

Many discussions related to the application centric business model have taken place within the ITS community. The eSecurity WG report[1] provides the following conclusion: a clear

[1] http://www.esafetysupport.org/en/esafety_activities/esafety_working_groups/esecurity.htm and http://www.esafetysupport.org/download/working_groups/eSecurity/finalreport/v1/esecurity_vulnerabilitiesinroadtransport_v1.pdf

separation should be made between interactive systems and independent vehicle-based electronics. Consequently, the following recommendation is made: "*Ensure separation between independent vehicle-based systems and interactive systems. Vehicle based systems should remain under the responsibility of the OEMs and should not be affected by interactive systems*"

We therefore conclude that to make the application centric business model a reality, any platform solution should (1) create separation of concern and (2) ensure that the result legally ensures separation of responsibility. OVERSEE platform use virtualisation as a foundation and therefore creates separation f concern. OVERSEE platform is also based on virtualisation technology that can be certified (i.e. XtratuM is used in space applications). To be adopted, stakeholders in the ITS community would have to agree on a level of assurance of the platform that would legally ensure separation of responsibility/liability.

But agreeing on the use of a virtualisation platform and on a level of certification is not sufficient. Applications themselves would have to be certified (e.g. by a public authority) to avoid a potential driver distraction caused by applications or a potential malfunction of applications.

To make this model work, the resulting ecosystem should include the following:

- A platform approach ensuring separation of concern between interactive systems and independent vehicle-based electronics.
- An assurance approach that would legally ensure separation of responsibility and liability. Essentially, the OEM will not be liable for malfunctioning of applications.
- An Application Store dedicated for 3rd-party applications. Applications could be provided by any developer. Such application store would need some governance structure[2].
- An agreed level of application assurance, and agreed verification/certification scheme.

4.2.2 Service Centric Business Model

This business model will mainly be the focus of companies involved in providing services to end users. The difference with application centric business models is that the service provider is responsible for applications provisioning. A service provider could develop its own applications or could subcontract other companies for application development. Also note that the service centric business model could coexist with the application centric business model.

Services take more and more space in the private and the public areas. The main goals of ITS (e.g. enhance traffic efficiency, ease travel in Europe) should be mainly provided by public or private companies. As OVERSEE can run critical applications safely and securely and protect important data, a lot of services can emerge for the use of such a platform, e.g:

- Insurance can provide "pay as you drive" services based on reliable information

[2] For instance Apple provides the governance for its application store.

- Eco taxes can rely on your everyday consumption
- Travel services, including a perfect integration between plane, car, bus with no time to wait, can be put in place involving a vast number of companies
- Dynamic traffic management to reduce traffic can be set

The services can be also interesting at other levels. For example an SME can specialise to certify some services according to standards.

The difference between the service centric and the application centric business model relates to stakeholder roles and responsibilities/liability in the supply chain. In the service centric approach the service provider can endorse a level of responsibility/liability. To make this model work, the resulting ecosystem should include the following:

- A platform approach ensuring separation of concern between interactive systems and independent vehicle-based electronics.
- An assurance approach that would legally ensure separation of responsibility and liability. Essentially, the OEM will not be liable for malfunctioning of applications, but *the service provider can be liable.*
- An Application development ecosystem set up by the service provider (it would be an application store).
- An agreed level of application assurance, and agreed verification/certification scheme.

4.2.3 OEM Centric Business Model

This business model will mainly be the focus of an OEM. The difference with the service provider centric model is that services are directly offered by the OEM. This solves the problem of separation of concern on responsibility and liability, i.e. the OEM is liable. On the other hand, the OEM still has to organise its supply chain so that responsibility/liability are well identified. This still justifies the use of a platform like OVERSEE enabling the execution of ITS applications next to Infotainment applications on a single ECU. Different exploitation scenarios are imaginable:

- Customisation of vehicles after Start of Production for different user groups of special-purpose vehicles or fleet operators
- Maintenance of rapid changing online services without reverification of the whole system
- Enabling an OEM application store to offer new functionalities to any customer after the start of production

To make this model work, the resulting ecosystem should include the following:

- A platform approach ensuring separation of concern between interactive systems and independent vehicle-based electronics.
- An assurance approach that would legally ensure separation of responsibility and liability. Essentially, the OEM will have to negotiate with supplier's responsibility and liabilities. The use of virtualisation could actually be a requirement for suppliers to negotiate such liabilities.

- An ecosystem for applications, this would be decided by the OEM.
- An agreed level of application assurance, and agreed verification/certification scheme. This would be decided by the OEM.

4.2.4 OVERSEE Can Enable Multiple Business Models Simultaneously

The considered business models have pros and cons, but as they can be beneficial for different companies, they can be combined.

This is made possible by the isolation and security capabilities of the OVERSEE platform, i.e. the three business models can be supported by the same OVERSEE platform.

Note that in all cases, there could be restrictions on applications that are allowed. Public authorities could have to decide on policies for restricting applications and possibly verifying/certifying them, in order to guarantee that they are harmless for road safety.

The consortium is now in the stage of liaising with the ITS community. If needed, this section will be revisited for the end of the project.

4.3 OVERSEE as Part of a Roadmap

OVERSEE has worked on understanding a roadmap. This work was started further to the second Advisory Board meeting. It focuses on the creation of an ecosystems using OVERSEE technology.

4.3.1 Making the OVERSEE Platform a Reality

4.3.1.1 Current Challenges

The current challenges in the foreseen automotive platform come from different categories:

- Integrating innovation: innovations come mainly from research and are the basis of R&D projects. Therefore, the integration of these innovations can be split into integration in a research oriented platform, and integration in (pre-)industrial platform.
- Integrating transversal features: A lot of transversal features are increasingly important in the ITS part of the automotive world, e.g. Scalability or Quality of Service.
- Interoperability: interoperability is a main concern as soon as communicating systems are involved. The definition of the interoperability between components, modules, or systems has to reflect a consensus including on items that have not been formally defined. Moreover, standards have to be taken into account. Nonetheless some existing standards may defeat interoperability.
- Technology independence: to enable the three points above, the automotive platform should not depend strongly on specific technologies, i.e. specific hardware or specific proprietary resources.

- Multiple business models and multiple service providers: an automotive platform should be able to be updated, or to have new applications from various providers downloaded and installed. Thus on one hand complete isolation has to be available between independent vehicle-based systems and interactive systems, and on the other hand isolation between different interactive systems is needed.

4.3.1.2 OVERSEE Viewpoint on Automotive Platform Related Applications Market

The advent of an ecosystem depends on:

1. Widely available technology
2. Associated standards
3. Compatible business models.

These three points can be addressed through an initiative and a consensus. 1. is usually the result of an initiative for an open platform such as OVERSEE. 2. and 3. can be addressed though a consensus building forum involving the stakeholders.

Thus it is possible to summarize the process that leads to a successful ecosystem by the following picture:

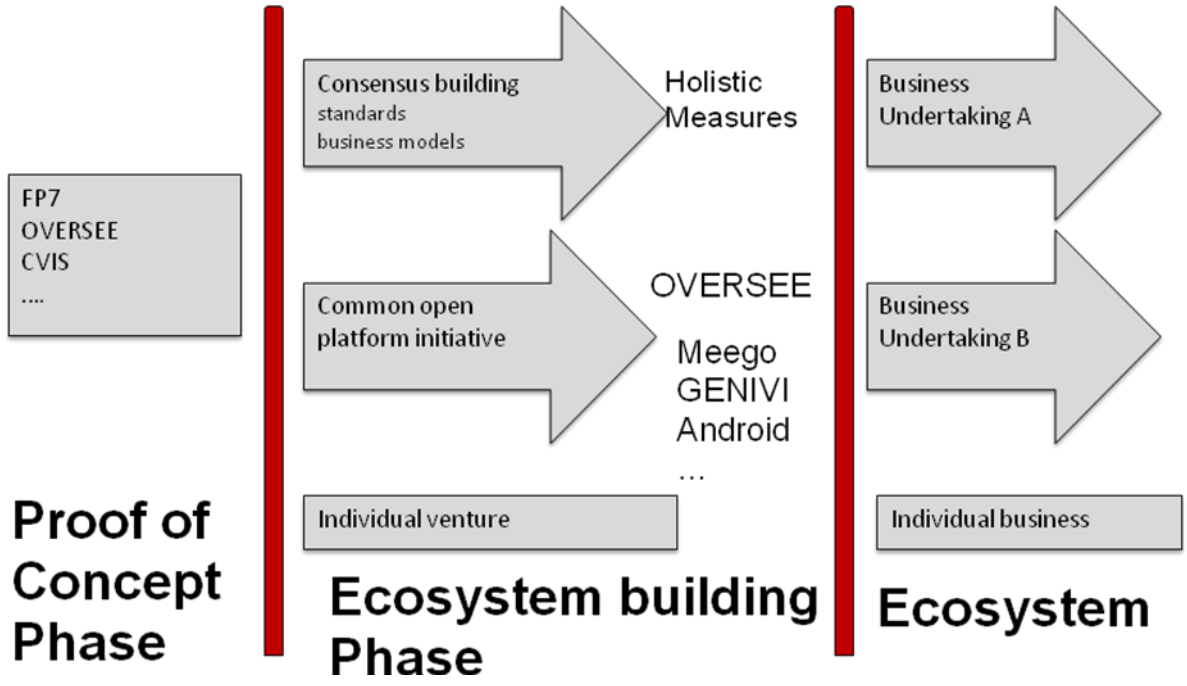


Figure 10: Building an Ecosystem for an automotive open platform.

From this structure of the Ecosystem, several mainstream markets should emerge. One of them is already foreseen and will rely on the architecture of the platform by itself, i.e. a strict separation of concerns between platform and applications. The application level will be composed by both applications and services. Thus, four actors can be defined:

- Consumer: the end user of the system. In the OVERSEE project it is mainly the driver
- Service Provider: provides many end-to-end solutions to the consumer

- Application Developer: designs, develops and sells many applications to the Service Provider or the Consumer.
- Platform provider: develops and enhances the open platform to fit all the requirements of the applications and/or the services provided by the above actors.

To enable this business model, it is necessary to define on one hand an interface between the platform providers and the applications-services actors, and on the other hand a mainstream offer.

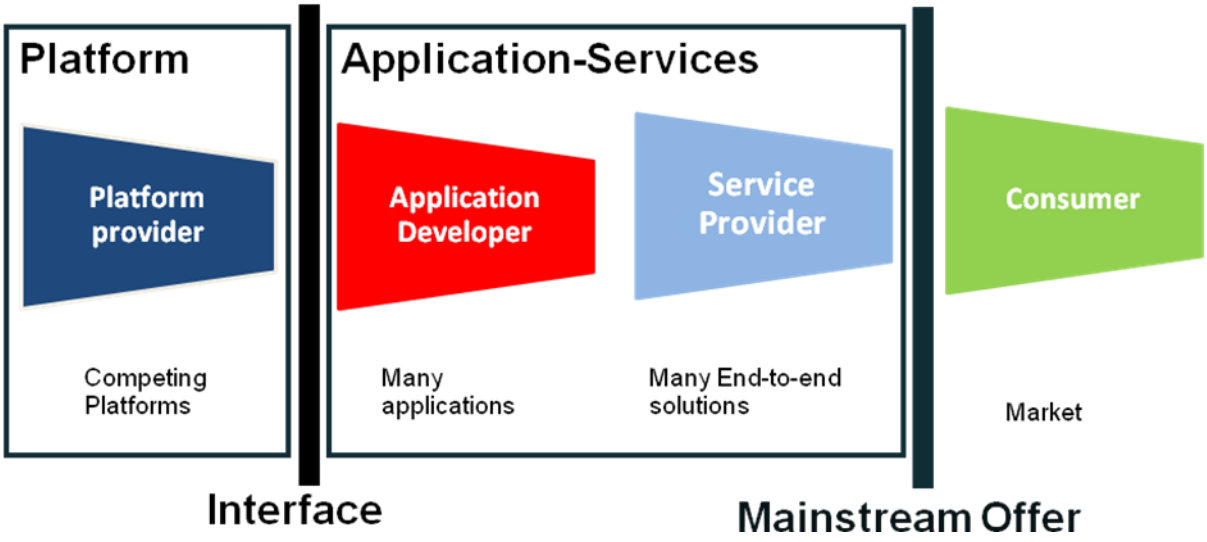


Figure 11: One interface for one mainstream market.

4.3.1.3 Building the Ecosystem

To build an ecosystem, the various stakeholders have to struggle with some hurdles. These stakeholders, as presented in Figure 11 are: the Platform Provider (PP), the Application Developer (AD), and the Service Provider (SP). An ideal process to establish the ecosystem could be the following steps:

1. PPs agree with ADs on an interface
2. PPs create several platforms
3. PPs agree on how the platform should meet market expectations
4. PPs bring research to industry and synchronize with the mainstream market
5. ADs invent many applications relying on the platform
6. SPs use the application to develop end-to-end solutions and get it to market

In recent years, the design of several platforms was supported by the European Commission, for example through FP6 and FP7 projects. Unfortunately, the step 1. has not been yet carried out. Nonetheless, various platforms have been designed and successfully used in proof-of-concept situations (e.g. CVIS). Thus, step 2. can be considered essentially done. To successfully build the ecosystem, all the community members must synchronize their work and converge it to form a perfect solution suited for the market.

One of the main steps toward the broader use of an open ITS platform in the automotive domain, e.g. the OVERSEE platform, is standardization.

Currently some standardization work has already been done or is in progress. For instance, ETSI is standardising ITS communication architecture, and there is already existing safety standards such as DO178B, IEC 61508, and the recommendations provided by the eSafety Forum. However, some standardisation aspects have not yet been taken into account. Assuming that the future European open ITS platform will be based on a virtualization mechanism, such as OVERSEE, standards have to be provided on different levels. For instance:

- Interfaces and middleware: to abstract the hardware from the software. This will help to reduce the time-to-market of software, ease the interoperability of applications, and make them portable on any vehicle using the standard platform.
- Partition of resources and accesses: Another possible point of standardisation is the characterisation of a "standard partition" dedicated to a certain kind of application and recommendations for resource access (e.g. an ITS partition must have access to ITS 5.9 GHz communication, to GSM, and to GPS system).
- Certification: an ITS platform must be provided with a Security partition that enforces some defined properties and policies, and which could be certified according pre-defined criteria such as a particular Common Criteria Protection Profile. Moreover, the scheduling must provide a certain percentage or some priority for emergency situations or other critical applications.

This standardization clearly has to involve all the actors (e.g., academics, service providers, OEMs, application developers, suppliers) of the community. In this way, it should be possible to establish a dedicated task force within the (probably future) iMobility Forum that will be a follow-up of the eSafety Forum. One of the main tasks of the forum will be to detail the entire set of requirements to build this platform.

OVERSEE should be a main building block in this cooperative effort due to the experience gained during the project, and the fact that it is the first open ITS platform for the automotive domain able to support multiple applications with a mix-criticality at the same time. Moreover, some existing results (e.g. CVIS, CALM) can be integrated on top of the OVERSEE platform. Furthermore, the OVERSEE consortium is sure that some of the requirements for an ideal ITS automotive platform are already solved by OVERSEE: hardware transparency, flexibility, isolation, cost reduction (both hardware and software), and opening market opportunities.

This topic will be submitted as a paper for ITS World 2012 which will refine the final results of OVERSEE. We believe strongly that the OVERSEE project and its consortium should be a leading part of such initiative.

4.4 Individual Exploitation

4.4.1 Escrypt

4.4.1.1 Escrypt GmbH's background

As a system provider, escrypt offers solutions for all aspects of embedded security from one source. The services include system design, specification, prototyping up to product development and certification. escrypt works in all areas of embedded applications with need for security. escrypt's unique branch expertise and technical competence is based on many years of experience in the field of embedded security and an extensive number of successful projects in the automotive domain.

4.4.1.2 Escrypt GmbH's interest in OVERSEE

Today's market does not offer an open und secure platform fitting the needs of today's and future automotive applications such as, e.g., tolling. These kinds of applications require specific properties like virtualisation on basis of a sound security architecture.

The experience and result of this project will extend escrypt's expertise not only for embedded applications in the automotive domain. Moreover, the expertise will be helpful for many other industries with security problems in embedded applications. The common challenge of many companies in the embedded industry is the small volume of devices produced per year and the unavailability of an open common security platform.

escrypt is convinced that the production of such a cost-efficient platform will help many embedded applications to efficiently improve the security. escrypt will support their customers by designing and implementing the security into their systems on the basis of OVERSEE.

4.4.1.3 Exploitation Results

Following the end of the project, escrypt identified 3 main outcomes for exploitation.

1. The project provides a *Know-How in shared security services and virtualized environments* that can be a benefit not only for the automotive domain but also for other domains.
2. The project helped escrypt to *market the concept of security in virtualized systems*. The recognition of the OVERSEE project was proven during ITS World 2012 and the OVERSEE Final Event even if there is not yet concrete industrial project. Moreover, since escrypt is now a subsidiary of ETAS (part of the Robert BOSCH group) the issue of security and virtualized systems is taken seriously at the group level.
3. OVERSEE was also a successful integration of the EVITA results.

4.4.2 Fraunhofer-Institut für offene Kommunikationssysteme

4.4.2.1 Fraunhofer's background

The Fraunhofer-Gesellschaft is an autonomous organization with a decentralized organizational structure, which currently maintains 58 research institutes and a patent office in locations throughout Germany. Fraunhofer-Gesellschaft is the leading organization of institutes of applied research and development in Europe. Future-oriented strategic research commissioned by the government and public authorities are carried out with the aim of promoting innovations in key technologies with an economic and social relevance in the next five to ten years.

Work focuses on specific tasks across a wide spectrum of research fields including communications, energy, microelectronics, manufacturing, transport, and the environment. Based on its vision of a user-centric ubiquitous computing and communication environment, Fraunhofer FOKUS (www.fokus.fraunhofer.de), the Institute for Open Communication Systems, researches and develops communication systems in wireless and wired fixed and ad-hoc networks. Thereby, Fraunhofer FOKUS designs, specifies, implements, and evaluate communication protocols, services, and applications. Furthermore, Fraunhofer FOKUS is actively working in protocol testing and developing tools for automated and formalized test systems.

4.4.2.2 Fraunhofer's interest in OVERSEE

Fraunhofer FOKUS will exploit the results achieved in OVERSEE in different fields. First of all, according to the "Fraunhofer model", the expertise gained will be used in the acquisition of new industry and research projects. The expertise will therefore be made substantial by publishing papers in the relevant conferences and journals. If applicable, Fraunhofer FOKUS aims at founding spin-offs, which can market its own solutions and create new jobs in the region of Berlin. Finally, Fraunhofer FOKUS, through its membership in the European Telecommunication Standards Institute, can influence and create standards for, e.g., ITS and the use of secure platforms in the domain. Therefore, FOKUS can disseminate the project results of OVERSEE to standards bodies, which in turn will create a benefit for all partners, if the OVERSEE platform, or parts of it are backed by standards.

4.4.3 TRIALOG

4.4.3.1 Trialog's background

TRIALOG is a system and software engineering company in the fields of real-time and embedded systems. It focuses on innovative systems for the automotive and home / consumer electronics marketplaces. Most of the devices being developed for these markets today have networking capabilities and can communicate with their environment, such as other peer devices and Internet access. Trialog core competencies are therefore oriented towards the right combination of real-time embedded software and networking technologies which are the keys to building such communicating devices and their interfaces

to large business information systems. TRIALOG engineering process focuses on system, network and software architecture, design-to-cost and design-to-security.

Some work carried out recently include:

- Network protocols and connectivity solutions, in the area of automotive applications (VAN, CAN, TTP, Flexray, etc.), in the area of home networking including control buses such as the EHS/KNX bus, in the area of audio/video high-speed buses such as the IEEE1394 / HAVI bus, Hiperlan 2, etc. Connectivity solutions focus on embedded gateways with Internet Capabilities (integration of OSGi technology) and wireless communications (GSM./GPRS, 802.11, Bluetooth, etc.).
- Coordination of security projects such as e-PASTA IST project (e-Protection of Appliances through Secure and Trusted Access) or GST-SEC (security subproject of GST IST IP). Technical coordination of the TEAHA (The European Home Application Alliance) IST project with support of security aspects. Coordination of the Sevecom (Secure Vehicle Communication) IST Project. Technica coordination of the e-Inclusion MonAMI IST project.

More information on Trialog can be found in http://www.trialog.com.

4.4.3.2 Trialog's interest in OVERSEE

Trialog has 20 years involvement in automotive systems, in particular in telematics applications. The results of this project will allow it to enhance its business activities along two directions:

- Validation tools for open secure vehicle platforms. In particular, Trialog will lead WP4 (Open Platform Validation Support), an area where it has already a wealth of building blocks available, in particular in the area of testing based on ISO 9646 and TTCN3 test technology. Trialog plans to develop specific enhancement of test tools that can be use to validated Oversee types of platforms.
- Trialog also plans to provide consulting and services around the use of such platforms. For instance the development of specific test suite could be of interest.
- OVERSEE is an example of the fact that transversal aspects (security, interoperability, privacy, liability) have a profound impact on the ICT solutions used in ITS. The ICT ecosystem is impacted. Trialog plans to be active in this area (ecosystem building)

Note that we plan to extend the scope of our business to other area than automotive (e.g. home control, industry control in machine-to-machine (M2M) configurations ...)

4.4.3.3 Exploitation Results

As a results of the OVERSEE project, Trialog developed specific test suites to validate PKCS#11 which a "de facto" standard for cryptographic services call. It should be reuse in other research and development projects.

Trialog also improved is knowledge and expertise about virtualized systems and the relative security issues. The Common Criteria approach studied in OVERSEE perfectly match the latest project of the company:

- Security analysis using TVRA (ETSI TR 102 893) for automotive customers (2012)

- Validation and testing of ITS communication (FP7 Preserve project)
- Methodology and security concerns in heterogeneous mix critical virtualized systems using hypervisor (FP MultiPARTES project).

OVERSEE also provides evidence that the need for an open ITS platform suitable for automotive is strong, and the relative expectation of the market stringent. It matches the results of industrial project done together with city bus fleet managing companies that are looking forward such solutions.

For the coming years, the exploitation strategy relatives to OVERSEE will be service-oriented.

The first activity is to raise the awareness of our customers and our networks about the mix criticality issues (mainly about security) and the relative existing solutions. It also includes the need to communicate about the benefits of the hypervisor-based solution ensuring spatial and temporal isolation.

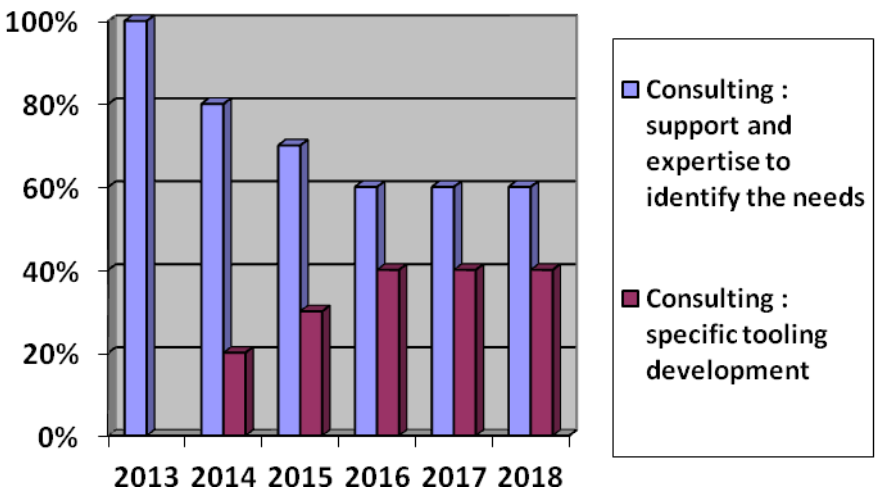
From the created awareness, it is possible to sale consulting activities to gain design win based on Xtratum as our customers are very confident in us to bring them innovative solutions.

At the same time, it is necessary for us to extend and reinforce our expertise in the security area (using TVRA for instance as a first step to achieve a full Common Criteria approach) to provide a good guidance to our customers in the selection of their solution.

The design win and a strong expertise in security and mix criticality allow us to develop new tools and techniques to ensure consistency between applications needs and platform solutions resulting in a more trustable system. This activity is also supported by our expertise and tools to validate systems (for instance cryptographic interface as PKCS#11)

The last activity is to establish a revenue stream through support to customer using hypervisor-based solution.

The revenue stream will be divided between expertise and specific tooling development. We assume that the first design win will only arise after one year. The table here below describe the division between the two sources of revenue.



Trialog estimates an average design win to 50.000€.

The goal of the company is to reach 5 design wins per year till 2018 that is equivalent to 250.000€ per year. For information the whole revenue company in 2012 was of 2.500.000 thus the estimated income will represent about 5-9% of the foreseen global revenue of the company in 2018.

4.4.4 Technical University Berlin

4.4.4.1 Technical University Berlin's Background

The department for Open Communications Systems (OKS) at Technische Universität (TU) Berlin is researching and developing methods for a cooperative but autonomic behaviour of system elements. OKS has years of experience in the design, specification, and development of open distributed systems.

As part of OKS, the Daimler Center for Automotive Information Technology Innovations (DCAITI), has been founded in 2006 as a public-private partnership between Daimler AG and TU Berlin.

DCAITI is specialized on future scenarios for vehicular electronics, including embedded systems, networked cars, as well as human machine interfaces. Focus is on research in platform and application development and evaluation.

4.4.4.2 Technical University Berlin's interest in OVERSEE

DCAITI will use the expertise and integrated platform gained for further input to research, improved quality of teaching, and acquisition of new projects. The results will be published in international conferences and journals. Further, where appropriate, the results will be used in internal collaborations with Daimler.

4.4.4.3 Exploitation Results

TUB could improve the quality of teaching with the OVERSEE project. Many researchers and students were involved in the development and integration process. Especially the deployment of the model car functionality into the OVERSEE architecture was a valuable experience for TUB to enhance expertise in the field of virtualized embedded platforms.

4.4.5 Universidad Politécnica de Valencia

4.4.5.1 UPV's Background

The Real-Time Systems Group at the Universidad Politécnica de Valencia has a relevant experience in the real-time field. It has developed scheduling analysis techniques for real-time applications. Also, It has been involved in the design and implementation of real-time operating systems which have been distributed in the community by GPL licenses. This group has developed the real-time operating system Partikle which is the substitute of RTLinux-GPL distribution. During last 4 years, it has develop the hypervisor XtratuM which is the first

open source virtualiser for critical real-time systems. The group has also made contributions in the field of real-time systems scheduling and control.

4.4.5.2 UPV's interest in OVERSEE

As an academic partner, the individual exploitation plans will be focused in dissemination of the ideas resulting from the research via academic and industrial channels by submitting scientific papers into the appropriate conferences and journals, and by organizing workshops and tutorials related to the new technology. As a group interested in the technology transfer to the industry, the development will be offered to the scientific and industrial communities providing the sources through GPL like licenses.

4.4.5.3 Exploitation Results

During the project UPV has opportunity to extend research and development on virtualization solutions. OVERSEE is a successfull demonstration of the XtratuM capabilities.

The major outcome is the creation in 2012 of FentISS, a spin-off to transfer the research discovering toward enterprises. FentISS opens the door to a wide range of applications and markets. "*We have the solutions you need, delivering products into the Aerospace, Aeronautics, Automotive & Transportation, Industrial Automation, Network Equipment, and Consumer Electronic markets*"

4.4.6 University of Siegen

4.4.6.1 University of Siegen's Background

Partner is the Chair for Data Communications Systems of the University of Siegen. Main research area of the chair is the integration of security and cryptography in communications systems considering all layers of the ISO model. Encryption devices for SDH (622 MBit/s) and ATM (155 MBits/s) have been developed as well as secure multimedia applications or XML signatures. The institute was already responsible for the security aspects of 7 EU projects (SCARAB, WEBSIG, ELIAS, GNIUS, USBCRYPT, SETIC, eMAYOR). The chair is member of ISO/IEC SC 27 (Security Techniques) for more than 20 years and was editor of more than 5 international standards. The team includes more than 10 scientific assistants and around 20 persons in total. More than 20 doctors and 180 graduates finished their studies at the institute.

The chair works on security of automotive systems since 12 years. These activities started in 1997, when the chair participated in the realization of the security and cryptographic system of the Toll Collect System in Singapore ("ERP" Electronic Road Pricing). On behalf of the German Security Agency it has performed security studies on the security of TMC/TPEG and the security of automotive bus systems (CAN, FLEXRAY, MOST, LIN). One dissertation has been already published "Informationssicherheit in Automobilen" by S. Goss (Volkswagen AG), another four doctor theses are under research work (automotive sensor protection, security of the diagnosis interface, secure in-car communication, secure gateway). The leader of the chair is co-chair of the eSecurity Working Group of the eSafety Forum of the EU

Commission. The chair has a lot of connections and relations to the automotive stakeholders by this activity and became one of the known players in this area.

4.4.6.2 University of Siegen's interest in OVERSEE

USiegen will use the expertise and the knowledge gained from the OVERSEE project in the following fields of its work and research areas:

- Science: USiegen has academic interests in the project. It is planned that the know-how and results trigger continuation activities after the end of this project and will be used in current research work as well as may be transferred into other research projects with similar or different but intersected subjects. Furthermore, USiegen will publish results as papers in scientific journals and by presenting at conferences.
- Education: Being a university, project results will be directly forwarded to university students, especially in the area of engineering and computer science. Thus, the OVERSEE results can be directly used for educating tomorrow's engineers. Additionally, diploma, master and Ph.D. theses will be written on the project's topics.
- Consultancy: USiegen's strategic goal is to increase the number of direct consultancy and industry collaborations. Collaboration and cooperation with other academic institutions will be done. We would also look to provide research consultancy services to government and industry.

4.4.6.3 Exploitation Results

During the OVERSEE project, the chair for Data Communications Systems had the chance to investigate security challenges of shared communication systems in a virtualized architecture. Members of the project team have worked on PhD thesis related to the project topics, e.g., Security Protocols for Vehicular Networks and secure resource sharing. Furthermore, several publications and (invited) talks attracted attention on the topic in the industry. Application of the concept of isolated domains with different trust levels, executed on the same hardware in parallel, securely connected via an policy based communication domain is a fruitful concept, which will find its way into further security concepts to be created at the chair for other industry domains.

4.4.7 Volkswagen AG

4.4.7.1 Volkswagen AG's Background

With 48 production facilities in 19 countries and a broad product range stretching from passenger car to luxury and sports cars, light & heavy duty trucks and commercial vehicles, the Volkswagen Group has grown up to one of the largest globally active automotive manufacturers with world-wide sales of roughly 6,27 million units in 2008 (market share 10,3 %). The company consists of 8 independent brands from six European countries. Since many years VW is market leader in Western Europe with last year sales of about 3 million cars (market share 20,3 %). Volkswagen Group's annual turnover exceeded 113,8 billion EUROS in 2008 with expenditures for R&D of approx. 3 billion EUROS. The average number

of employees worldwide was 369.928 of which 8.954 were occupied in Group-wide RTD activities.

In 2008, research and development activities mainly focused on expanding the product portfolio and improving the functionality, quality, safety and environmental compatibility of Group products. The ideas contributed by our employees and the expertise of external partners played a key role here.

Volkswagen's aim is to produce vehicles with ever increasing quality, comfort, safety and technology standards and at the same time reduce fuel consumption and emission levels. VW is interested in the application of new developments in all automotive areas not only to meet all relevant technical and legal requirements but also to satisfy customer demands on a consistently high level.

Volkswagen's Group Research is working on every field of automotive application and is responsible for identifying, evaluating and transferring innovative technologies to advanced engineering or series development departments of all brands of the Volkswagen Group i.e. AUDI, SKODA (Czech Republic), SEAT (Spain) etc.

Research areas include: Electronics, Environmental and Mobility Science, Vehicle Technology and Dynamics, Manufacturing Science, Powertrain and Engine Technology and Control, Pedestrian Protection, Pre-Crash, Accidentology

4.4.7.2 Volkswagen AG's interest in OVERSEE

Volkswagen is the leading European car manufacturer. Its products are long lasting and incorporate the most recent and sophisticated automotive technology. For further competitive products in the global market the introduction of additional new functions and technologies, mostly driven by the development of electronics, into the car will be very important. The next big technological steps within the next years for the automotive industry will be the interconnection of single cars to other cars and recipients.

By means of workshops and meetings of research projects, many possible use cases with different needs of communication and security issues were elaborated. To fulfil these different requirements for each application in series production, a wide spectrum of electronic control unit variants and complicated vehicle architecture would be the result.

If Volkswagen would like to offer versatile C2C and C2I functions with e.g. safety functionality to decrease fatalities in road traffic or e.g. convenience functionality to offer an additional value to the costumer with this internal and external car infrastructure, a fusion of these applications in one electronic control unit and one communication architecture is needed.

To increase the controllability of such a total system, virtualisation could be used as a powerful instrument. That technology would avoid a mutual influence of those applications running on one machine and using the same interfaces. OVERSEE could close this gap by offering an encapsulated runtime environment for each application and an adjustable access to all internal and external interfaces by security policies.

The automobile industry partners could directly implement the methodologies created within this project into the product development process.

4.4.7.3 Exploitation Results

VW has enhanced its knowledge about virtualized platforms and gathered fruitful technical information about the feasibility, advantages and disadvantages of a virtualized, multi-partitioned platform for the use in the automotive area.

4.4.8 OpenTech EDV Research GmbH

4.4.8.1 OpenTech's Background

OpenTech EDV Research GmbH, registered in Mistelbach Austria, was founded in 2003 and is primarily engaged in research projects for industrial customers in the area of distributed embedded and real-time systems. The fields covered in OpenTechs activities include automation, mobile and telecom systems, thus including safety-related as well as security relevant systems components. As a consequence of the research activities OpenTech has been involved in training worldwide both for the commercial and academic arena.

Some of the open-source related projects

- Real Time Audio Tools
- XtratuM PowerPC porting efforts (PPC 405/440)
- RT-Preempt MIPS porting effort (RT-Preempt 2.6.29-rc8 for Longsoon 2F)
- Melita - Digital filter library for Linux kernel
- RTL_REDD_UDP - real-time UDP protocol implementation for
- RTLinux/GPL
- Assessment related tools (KFT, GDB-tracepoints).
- XtratuM real-time nanokernel components (XM tracer).

As strong advocate of open-source, OpenTech runs its project under open-source compliant licenses, and has also been involved in a number of migration activities, moving commercial entities to open-source solutions.

General activities in the OVERSEE context: OSS assessment (technical and risk), core system specification and development of missing components, support in the base distribution both host and target parts, testing and documentation review. Project management review, documentation review, system validation issues, assistance in community infrastructure setup. Implementation and technical documentation. Dissemination activities.

Specific activities in the OVERSEE context:

With the knowhow background of OpenTech we see main contributions in support for multiple hardware platforms including porting of key low level technologies to specific hardware (i.e. real-time services, fault tolerant resource infrastructure elements, etc.).

Notably as this projects covers not only demanding safety issues but at the same time stringent security demands our experience in both safety related system and security fit the demands of OVERSEE well. This experience not only covers specific tools for validation efforts but, based on a good understanding of relevant safety standards, also covers

procedural issues of system certification (RAMS). While current safety standards have generally neglected security issues, these have been an active work field for OpenTech in the context of industrial systems based on current security standards (notably FIPS) covering secure communication issues as well as security issues of storage systems.

4.4.8.2 OpenTech's interest in OVERSEE

As an SME that builds its business on Software being a service rather than a product, we intend to provide our contributions under an FLOSS license (preferably EUPL V1.1). Our primary exploitation activities is to promote core technical concepts along with our competence to provide services based on these technologies, thus OpenTech will focus on dissemination of concepts at industrial workshops (i.e. embedded world Nuremberg) as well as at academic and open-source community conferences. OpenTech, which is deeply involved in industrial open-source (Nicholas Mc Guire is the chair of OSADLs safety critical Linux working group at OSADL), will utilize its channels to bring the concepts and most notably the specific implementation to the attention of potential users

4.4.8.3 Exploitation Results

The deployment of an automotive real time OS into the OVERSEE architecture enhanced understanding the capableness of a virtualized environment for automotive RTE's. This experience has been flowing and will continue to flow into the dissemination efforts at industrial workshops as well as at academic and open-source community conferences.

5 Project Website and Relevant Contact Details

5.1 Webpage

The website URL is https://www.oversee-project.com/

5.2 Documents

The project public deliverables and other documents are available on the project website.

5.3 SW Components and Examples

A Vmware virtual machine has been prepared for evaluation, containing several XtratuM project examples ready to run, together with the complete development environment already installed and ready to develop partitioned applications.

The machine can be obtained visiting the following link [12][13] :
http://xtratum.org/downloads or alternatively on the fentISS website
http://www.fentiss.com/en/rdi/downloads.html

The list of available SW Components can be obtained on the website. Furthermore the website also provides ready configurations of several demonstration setups in form of raw images which can be executed either in a virtual machine or on the real target.

5.4 "SDK"

The XtratuM Software Development Kit, XM-SDK for short contains the tools, libraries and documentation for the development of partitions running on XtratuM. The XM-SDK can be obtained on the http://xtratum.org/downloads

6 Summary and Conclusion

According to some studies today up to %50 of the cost of a modern vehicle are caused by the electronic systems and up to %90 of the innovation in the automobile industry is done in this area. These are astonishing numbers showing the trend of the car industry. OVERSEE aimed to fill a gap in this trend by providing an open and secure IT platform without leaving out the needs of an automotive environment. To achieve this goal OVERSEE provided virtualized runtime environments on a standard x86 HW platform and added many services and features making OVERSEE secure and dependable and without losing openness and flexibility. The virtualized runtime environments provide isolation and guaranteed access to resources, and furthermore can host many different applications and/or operating systems. This opens many possibilities for the integrator of the platform to deploy their applications. To introduce flexibility into the design the many services provided by OVERSEE break the hard isolation of the runtime environments in a secure way by providing secure and standardized interfaces for the many services provided by OVERSEE. These services include among others a secure gateway to the external communication modules, ITS services, access to the HSM, access to various security services and many more. The main idea behind these interfaces is providing standardized interfaces to the user partitions which provide easy to use services and are easy to integrate. On the other side OVERSEE provides secure mechanisms to restrict the capabilities of these interfaces for each user partition through policies which can be defined by the platform owner.

During the development of OVERSEE OseK (FreeOseK) and many Linux variants have been ported to run in top of the virtualization. This enables easy integration of many applications and provides the integrators familiar runtime environments. Nevertheless the architecture does not restrict any further OS to be ported to the OVERSEE platform.

To sum up OVERSEE provides an open and flexible platform without compromising the security needed by an in-vehicle IT platform. OVERSEE is a brave step to realize an IT platform for vehicles which provides a more secure, flexible, cost efficient way to implement applications from the ITS, telematic, infotainment and many other domains for vehicles.

References

[1] OVERSEE Project, *D7.2 Plan of Use and Dissemination Year 2*

[2] OVERSEE: OVERSEE – Open Vehicular Secure Platform. Project flyer. Oct 2012

[3] OVERSEE: D2.1 List of interfaces and specifications of information flow. Dec 2010

[4] OVERSEE: D2.2 Specification of security services incl. virtualization and firewall mechanisms. Dec 2010

[5] OVERSEE: D2.3 Definition of Building Blocks Dec 2010

[6] OVERSEE: D2.4 Specification of Secure Communication Dec 2010

[7] OVERSEE: D3.2 Resource management layer implementation and description. Dec 2012

[8] OVERSEE: D3.3 Security Services Architecture and Services Implementation Dec 2012

[9] OVERSEE: D4.3 Run-time support for validation. Dec 2012

[10] OVERSEE: Documentation – Setup Guide for USB Flash Drive Media Access and Audio Sharing on the OVERSEE platform. Jan 2012

[11] OVERSEE Project Website, www.oversee-project.com

[12] XtratuM Website, http://xtratum.org/

[13] Fentiss Website, http://www.fentiss.com/