

University of Piraeus
Department of Informatics



Doctoral Dissertation

**DESIGNING SECURE, INTEROPERABLE & SUSTAINABLE
AUTOMOBILES & GLOBAL TRANSPORTATION SERVICES & SYSTEMS**

By Kleanthis P. Dellios

Supervisor: Associate Professor, Dr. **Despina Polemi**

Submitted in partial satisfaction of the requirements
for the degree of **Doctor of Philosophy**

Piraeus, 2015



University of Piraeus
Department of Informatics

Doctoral Dissertation

**“Designing Secure, Interoperable and Sustainable Automobiles
and Global Transportation Services and Systems”**

by **Kleanthis P. Dellios**

Advisory Committee: Despina Polemi, Associate Professor, University of Piraeus
Christos Douligeris, Professor, University of Piraeus
Angelos Amditis, Researcher Grade A, NTUA-ICCS

Approved by the seven (7) member committee in **09-02-2015**

.....
Despina Polemi,
Associate Professor,
University of Piraeus

.....
Christos Douligeris,
Professor,
University of Piraeus

.....
Angelos Amditis,
Researcher Grade A
NTUA-ICCS

.....
Michael Sfakianakis,
Professor,
University of Piraeus

.....
Michalis Psarakis,
Assistant Professor,
University of Piraeus

.....
Panayiotis Kotzanikolaou,
Lecturer,
University of Piraeus

.....
Constantinos Patsakis,
Lecturer,
University of Piraeus

Piraeus, 2015

**“Thinking is the hardest work there is
which is probably the reason so few engage of it.”**

- Henry Ford (July 30, 1863 – April 7, 1947)

Πανεπιστήμιο Πειραιώς

ACKNOWLEDGEMENTS

I dedicate this Doctoral Dissertation
To my Family
To my Professors and
To all my friends & to the Medical Doctors
& to Father Eirinaios of the Holy Monastery of Saint Rafail

Πανεπιστήμιο Πειραιώς

Πανεπιστήμιο Πειραιώς

© 2014 Kleantlis P. Dellios

All rights reserved. This Doctoral Dissertation is submitted in partial satisfaction of the requirements for the degree of Doctor of Philosophy. No part of the material protected by this Copyright notice may be reproduced or utilized from or by any means, electronic or mechanical, including prototyping, recording or by any information storage and retrieval system, without the prior permission of the author. Requests can be sent at kdellios@unipi.gr & kledellios@gmail.com

SUMMARY

Modern automobiles are often cited as “connected cars” or “networked vehicles” due to the emerging Information and Communication Technology (ICT) concepts they rely upon. Their traditional mechanical substance is enhanced with power electronics modules, embedded control systems and numerous communication and network interfaces, composing a mechatronic automotive platform with tremendous ICT capabilities. Unfortunately, this evolution in modern automobiles has characterized them as the next cyber targeted platform for any kind of attackers (i.e. hackers, crackers, common thieves) using various types of attacks (i.e. physical, cyber, hactivisms). Due to the plethora of cyber-attacks and vulnerabilities rising against the automotive platform, not only the automobile itself is threatened, but also the entire Intelligent Transport Systems (ITS) and the whole Transportation domain, including human lives are endangered.

A central vision of the automotive vendors is to deliver cooperative ITS services by implementing emerging technological innovations. Unfortunately, during their enthusiasm to achieve this goal interoperability issues in the ITS standards have been not appropriately considered. As a consequence, extensive research and development efforts are required for hosting and delivering interoperable services and cooperative ITS applications, yielding if the industry wants to achieve sustainability in the transportation domain.

Driven by the above mentioned lack of interoperability and sufficient security problems the research goals of this Doctoral Dissertation focus on enhancing the:

- I. Cyber-security capabilities of the modern automobile platform;
- II. Interoperability among the automotive platform and the ITS services;
- III. Sustainability of the global transportation systems.

The methodological approach followed in this Dissertation for reaching the **first goal** may be described within the following achievements:

- Reformulate the modern automobile into an Information and Telecommunication (IT) platform (modern automotive-platform) by identifying its components and correlating them with assets in traditional IT systems.
- Identify the physical and cyber threats of the automotive platform and then perform a detailed threat analysis.
- Perform a detailed vulnerability analysis for all the components (assets) of automotive platform. Through the applied threat model, not only the threats and vulnerabilities will be identified, but also the entry points as well as the impact caused to the entire ITS will be studied.

- Characterize major design flaws (among the identified vulnerabilities) with a high impact not only to the automotive platform but also to the most valuable functional elements and components of the ITS.
- Design and implement a protocol namely the Mutually Authenticated Secure Components (MASC) protocol which will enhance the communication among the components of the automotive platform in order to implement security controls. MASC enhances the security of the automotive platform and it constitutes the first main innovative milestone in this dissertation.

However, in the transportation cyber-ecosystem not only individual automotive platforms need to communicate between themselves but also there is a need of communication among a cluster of automotive platforms, nomadic devices, roadside units and base stations. All the above components of the transportation eco-system when accompanied by ICT technologies formulate an Intelligent Transportation System, which needs to provide interoperable services. Providing interoperable services has not addressed appropriately within the ITS standards, and has become the **second goal** of this dissertation which is met by the following:

- Introduce the Service Oriented Architecture (SOA) design approach to enhance the ITS standardized reference architecture (ITS-RA).
- Integrate the Service Discovery Mechanism (SDM) in order to formulate a holistic upgraded ITS-RA framework, enabling the offering of not only the traditional (cooperative applications based on wireless sensor networks) but also a new set of interoperable automotive services.
- Design parameterized version of the MASC protocol in order to enhance the communication among the road side infrastructure in order to implement security controls. The latter enables the upgraded ITS-RA framework to offer interoperable and secure services.
- Provide specific use cases illustrating the functionality of the interoperable and secure enhanced ITS-RA framework.

The above outcomes will change the existing view regarding the capabilities of the automotive platforms, since they:

- provide robust networking capabilities;
- transform the automotive platform into service providers;
- act as autonomous networking nodes over any ITS.

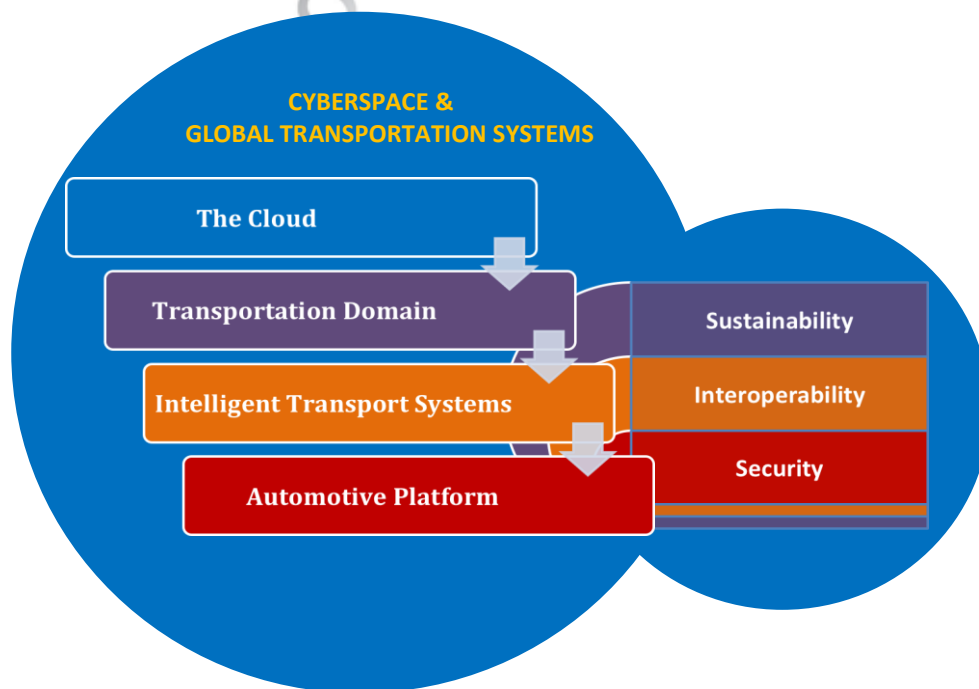
The **final goal** of this thesis is to enhance the sustainability of the ITS-RA framework at all levels: local, regional, national, international and global. The proposed contribution concerning the sustainable development of the entire transportation domain must meet the needs of the present forms of computing without compromising the ability of future generations to meet their own needs. This last objective is met by:

- Proposing a cloud computing architecture based on relevant principles and requirements;
- Designing the cloud-based legacy system hosting the ITS-RA framework;
- Providing the functional and technological characteristics;
- Generating various delivery and deployment models for innovative interoperable and secure ITS services;
- Proposing a transition strategy from traditional IT systems to cloud systems.

The philosophical approach to reach the above mentioned objectives spanned around:

- the mechatronics fundamentals for the deeper understanding of the automotive field;
- the reverse-engineering for the de/composition of the automotive platform;
- the Ford Theory of Pacifism in order to compose simple yet practical and easy to implement solutions;
- the 1987 Report of the World Commission on Environment and Development on “Our Common Future”, as the inspiration for the development of a sustainable transportation cyberspace.

FIGURE 1: THESIS OUTLINE



To summarize, the three goals of this thesis are presented into a scalable environment (fig.1) beginning from the vehicle (automotive platform), moving to the ITS domain where vehicles and road-side units interact with each other to obtain and utilize cooperative services. When adding interaction with other transport modes and services are obtained from any other sources in the network, like from the cloud, the global transportation systems can interoperate with the rest of the cyberspace as a single system.

This thesis outline consists of three parts as described below:

Part I: The Automotive Platform and the Intelligent Transport Systems

Chp.1: The Automotive Platform

Chp.2: The Intelligent Transport Systems

Part II: Assessing and Securing the Automotive Platform

Chp.3: Automotive Platform Threat Modelling

Chp.4: The MASC-Protocol: Redefining the Automotive Platform Security

Part III: Building Interoperable and Sustainable i-Transport Services and Systems

Chp.5: The Upgraded ITS-RA Framework

Chp.6: A Sustainable i-Transport Cloud System

LIST OF FIGURES

| | |
|--|------|
| FIGURE 1: THESIS OUTLINE..... | viii |
| FIGURE 2: TECHNOLOGICAL PARADIGM OF THE ‘AUTOMOTIVE PLATFORM’ | 15 |
| FIGURE 3: MASC OVERVIEW..... | 64 |
| FIGURE 4: MODULES MUTUAL AUTHENTICATION PROCEDURE..... | 71 |
| FIGURE 5: MODULES TICKET ISSUING PROCEDURE..... | 73 |
| FIGURE 6: COOPERATIVE SERVICES OF THE ITS-STATION REFERENCE ARCHITECTURE | 86 |
| FIGURE 7: INTEROPERABLE AND COOPERATIVE PROCEDURE OVERVIEW | 92 |
| FIGURE 8: PROPOSED INTEROPERABLE AND COOPERATIVE ITS FRAMEWORK | 93 |
| FIGURE 9: PLATFORM-TO-ROAD_SIDE_UNITS MUTUAL AUTHENTICATION PROCEDURE..... | 96 |
| FIGURE 10: PLATFORM-TO-ROAD_SIDE_UNITS MUTUAL AUTHENTICATION PROCEDURE..... | 97 |
| FIGURE 11: CASE I - V2V DECENTRALIZED SDM SCENARIO A | 99 |
| FIGURE 12: CASE II - V2V DECENTRALIZED SDM SCENARIO A | 100 |
| FIGURE 13: CASE I - V2V CENTRALIZED SDM SCENARIO B..... | 101 |
| FIGURE 14: CASE II - V2V CENTRALIZED SDM SCENARIO B..... | 102 |
| FIGURE 15: CASE III - V2V CENTRALIZED SDM SCENARIO B..... | 102 |
| FIGURE 16: OPEN CLOUD PROJECTS | 110 |
| FIGURE 17: THE ‘ITRANSPORT CLOUD’ ARCHITECTURE MODEL..... | 112 |
| FIGURE 18: THE ‘ITRANSPORT CLOUD’ SYSTEM..... | 114 |

LIST OF TABLES

| | |
|---|-----|
| TABLE 1: THE ‘AUTOMOTIVE PLATFORM’ ARCHITECTURE | 3 |
| TABLE 2: COMPOSITION OF THE ‘AUTOMOTIVE PLATFORM’ STACK..... | 14 |
| TABLE 3: CROSS LAYER FUNCTIONALITY OF THE ISO MODEL AND THE ITS-STATION ARCHITECTURE..... | 18 |
| TABLE 4: THE ITS BASIC SET OF APPLICATIONS..... | 22 |
| TABLE 5: DECOMPOSITION ANALYSIS OF THE AUTOMOTIVE PLATFORM | 33 |
| TABLE 6: CYBER-ATTACKS ANALYSIS OF THE ‘AUTOMOTIVE PLATFORM’ | 34 |
| TABLE 7: WIRED NETWORK INTERFACE RELATED ATTACKS | 45 |
| TABLE 8: WIRELESS COMMUNICATION INTERFACE RELATED ATTACKS | 45 |
| TABLE 9: SECURITY INTERFACE RELATED ATTACKS..... | 46 |
| TABLE 10: SERVICE INTERFACE RELATED ATTACKS | 46 |
| TABLE 11: AUTOMOTIVE PLATFORM RELATED ATTACKS (ACTIVITY SUMMARY) | 47 |
| TABLE 12: AUTOMOTIVE PLATFORM RELATED THREATS..... | 48 |
| TABLE 13: ITS RELATED CYBER-ATTACKS | 49 |
| TABLE 14: ISO REFERENCE MODEL & 802.11 PROTOCOL STACK | 51 |
| TABLE 15: ‘ITRANSPORT CLOUD’ TRANSITION PLAN..... | 119 |
| TABLE 16: ISO/ITS RELATED STANDARDS | 130 |
| TABLE 17: OTHER ITS RELATED STANDARDS..... | 130 |

TABLE OF CONTENTS

| | |
|---|-----------|
| ACKNOWLEDGEMENTS | IV |
| SUMMARY | VI |
| LIST OF FIGURES..... | X |
| LIST OF TABLES..... | X |
| | |
| PART I: THE AUTOMOTIVE PLATFORM AND THE INTELLIGENT TRANSPORT SYSTEMS..... | 1 |
| 1. THE AUTOMOTIVE PLATFORM..... | 2 |
| 1.1 AUTOMOTIVE PLATFORM ARCHITECTURE..... | 2 |
| 1.2 AUTOMOTIVE PLATFORM CONTROL MODULES..... | 3 |
| 1.3 AUTOMOTIVE TELECOM INTERFACES | 5 |
| 1.4 AUTOMOTIVE SECURITY MODULES | 9 |
| 1.5 ADVANCED AUTOMOTIVE SYSTEMS..... | 11 |
| 1.6 THE AUTOMOTIVE AS AN ICT SYSTEM | 13 |
| 1.7 CONCLUSIONS | 15 |
| | |
| 2. THE INTELLIGENT TRANSPORT SYSTEMS..... | 16 |
| 2.1 ITS COMMUNICATION (ITSC) PRINCIPLES | 16 |
| 2.2 THE ITS-STATION ARCHITECTURE | 17 |
| 2.3 THE ITS-STATION FUNCIONAL COMPONENTS..... | 19 |
| 2.4 ITS-S RA BLOCK ANALYSIS..... | 19 |
| 2.5 ITSC FUNCTIONAL ELEMENTS | 21 |
| 2.6 ITS-STATION APPLICATION CLASSES | 22 |
| 2.7 CONCLUSIONS | 23 |
| REFERENCES..... | 24 |
| | |
| PART II: ASSESSING AND SECURING THE AUTOMOTIVE PLATFORM..... | 27 |
| 3. AUTOMOTIVE PLATFORM THREAT MODELING..... | 28 |
| 3.1 AUTOMOTIVE CYBER-SECURITY AWARENESS..... | 28 |
| 3.2 AUTOMOTIVE PLATFORM THREAT MODELING..... | 31 |
| 3.3 AUTOMOTIVE-PRATFORM THREAT MODELING PROCESS..... | 32 |
| 3.4 AUTOMOTIVE PLATFORM VULNERABLE ENTRY-POINTS..... | 50 |
| 3.5. CONCLUSIONS..... | 52 |
| REFERENCES..... | 53 |

| | | |
|-----|--|-----------|
| 4. | THE MASC-PROTOCOL: REDEFINING THE AUTOMOTIVE PLATFORM SECURITY..... | 55 |
| 4.1 | MASC MOTIVATION | 55 |
| 4.2 | MASC CONTRIBUTION | 59 |
| 4.3 | THE FUNDAMENTAL PRINCIPLES OF MASC..... | 61 |
| 4.4 | MASC-PROTOCOL POLICY MODULES | 66 |
| 4.5 | MASC-PROTOCOL FUNCTIONALITY..... | 70 |
| 4.6 | VERIFICATION OF MASC | 74 |
| 4.7 | CONCLUSIONS | 75 |
| | REFERENCES..... | 77 |
| | | |
| | PART III: BUILDING INTEROPERABLE & SUSTAINABLE GLOBAL TRANSPORT SERVICES & SYSTEMS .. | 79 |
| 5. | THE UPGRADED ITS-RA FRAMEWORK..... | 81 |
| 5.1 | MOTIVATION AND CONTRIBUTION | 82 |
| 5.2 | FUNDAMENTALS AND PRINCIPLES | 84 |
| 5.3 | MASC-PROTOCOL MODIFIED FUNCTIONALITY..... | 94 |
| 5.4 | INTEROPERABLE FRAMEWORK UPGRADE | 98 |
| 5.5 | CONCLUSIONS | 103 |
| | REFERENCES..... | 104 |
| | | |
| 6. | A SUSTAINABLE 'ITRANSPORT CLOUD' SYSTEM | 106 |
| 6.1 | MOTIVATION AND CONTRIBUTION | 106 |
| 6.2 | CLOUD PRINCIPLES AND FUNDAMENTALS..... | 107 |
| 6.3 | THE 'ITRANSPORT CLOUD' SYSTEM..... | 110 |
| 6.4 | 'ITRANSPORT CLOUD' SYSTEM INTEROPERABILITY | 118 |
| 6.5 | 'ITRANSPORT CLOUD' TRANSITION PLAN | 118 |
| 6.6 | CONCLUSIONS | 121 |
| | REFERENCES..... | 122 |
| | | |
| 7. | CONCLUSIONS AND FUTURE DIRECTIONS..... | 125 |
| | | |
| | APPENDIX I: LIST OF ITS STANDARDIZATION ORGANIZATIONS | 130 |
| | APPENDIX II: LIST OF ITS RESEARCH PROJECTS | 135 |
| | APPENDIX III: PUBLICATIONS, DISSEMINATION ACTIONS & RESEARCH PROJECTS | 141 |

PART I: THE AUTOMOTIVE PLATFORM AND THE INTELLIGENT TRANSPORT SYSTEMS

The first part of this doctoral dissertation is entitled “The Automotive Platform and the Intelligent Transport Systems” and it focuses on exploring the technology of the Automotive Platform and the Intelligent Transport Systems (ITS). The scope of this part is to familiarize the reader with the basic concepts used in this thesis. More precisely, the first part is organized as follows:

Chapter 1: This chapter provides the basic knowledge and sets the architectural and technological fundamentals in the automotive platforms. The areas of the automotive platform covered include the design chain, the control systems, the network interfaces, the security and the advanced automotive systems. The purpose of this analysis is to view and present the automotive platform within the context of ICT terms and to move away from the traditional automotive view as a mechanical object.

Chapter 2: This chapter (ITS) presents a comprehensive analysis of how clusters of vehicles (e.g. automobiles, motorbikes), roadside infrastructures (e.g. traffic lights), hand held systems (e.g. nomadic devices) and centralized systems (e.g. traffic control, base stations) interact with each other (e.g. communicate, exchange, store data) over a reference architecture. Based upon the related ITS standards, the fundamentals of the communication interactions that set the cyber transport terrain and compose the ITS communication interface are described in this chapter.

Both chapters pave the background in order to proceed with the description of the open issues in automotive security, ITS interoperability and transportation domain sustainability that this thesis is addressing.

1. THE AUTOMOTIVE PLATFORM

The ‘automobile’ is defined as a machine that assists personal mobility using motors. The term automobile is most commonly used for urban vehicles, including motorized wheelchairs and bicycles, motorbikes and cars. In addition, the term ‘automotive’ is used for defining a machine that moves an object using motors, including automobiles, planes, trains, ships, trucks, buses, escalators, lifts, etc. Modern automobiles rely on a wide variety of microelectronic components and embedded systems to operate properly. This evolution in automotive technology (i.e. manufacturing methods and microcontrollers) has forced forward the transformation of the mechanical automobile into a mechatronic platform with networking capabilities [1]-[12]. The automotive architecture design chain, the control systems, the network interfaces, the security and the advanced systems are presented in this chapter, in an effort to view the modern automobile within the context of ICT terms. The goal in this chapter is to analyze the ‘automotive platform’ of the automobile from an architectural and technological viewpoint in order to collectively reformulate the automobile as an ICT system characterized by its physical and cyber components.

1.1 AUTOMOTIVE PLATFORM ARCHITECTURE

Advances in embedded systems and multiple serial buses in today’s modern automotive designs have made possible communications through and of a network of internally connected automotive control units [13][14]. However, the extended use of the embedded systems and the need to exchange information throughout the vehicle has increased the complexity of the automobile platform.

Today’s high-end automobiles contain over a hundred embedded processors and even more sensors and data acquisition/telemetry components optimized for robust functioning and safe driving, but they also include thousands lines of code in order to achieve geo-syncing locations, provide in-car wireless access points, embedded links that enable services and wireless interaction to the infrastructure or even coordinate with other automobiles [15]. The architectural complexity of the automotive platform is related with the mechatronic¹ design of the automobile. Table 1 illustrates the layers that compose the automotive architectural platform:

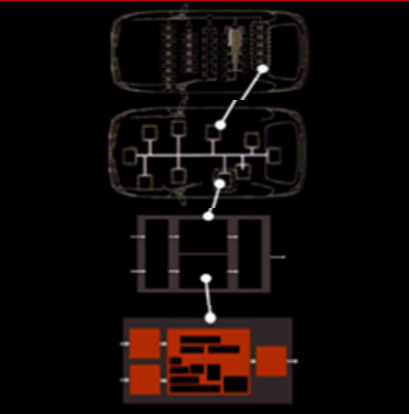
- *Layer I* (unit) – It includes the Microprocessor Control Unit (MCU). The manufacturers and suppliers (peripheral providers) provide the semiconductor components of the automotive processors blocks and graphics cores and the drivers of the chip interfaces.
- *Layer II* (module) – The Electronic Control Unit (ECU) of the automotive design chain integrates the MCUs into the ECUs that hold the automotive information as well as the

¹ Mechatronic Engineering: interaction of four engineering sectors: control, electronic, mechanical and computers systems.

networks and the necessary firmware so that all the units communicate between themselves.

- *Layer III* (systems) – The Control Systems and the Electronic Management Units of the architecture design use the ECUs to create systems that form the entire structure of the automotive platform in order to communicate with the network interfaces (e.g. protocols, communication protocols) [17].
- *Layer IV* (Platform) – The layer that provides the actual automotive platform and includes the automotive services and the applications that are supported for the user experience [18].

TABLE 1: THE 'AUTOMOTIVE PLATFORM' ARCHITECTURE

| Layers | Scope | Hardware | Software |
|------------------------|--|---|------------------------|
| Layer IV (Platform) |  | Automobile Platform | Services & Application |
| Layer III (System) | | Control Systems & Electronic Management Units | Middleware |
| Layer II (Module) | | Electronic Control Units | ECU Firmware |
| Layer I (Unit) | | Microprocessor Control Units | MCU Drivers |

The goal of the illustrated layered automotive architecture (Table 1) is not only to help in understanding the relation among the automotive components, systems and services [14][15] participating in the automobile platform synthesis, but also to compose the ICT stack of the automobile. In the next sections the technological analysis of the above electronically-oriented architecture will be provided. In particular, the automotive control systems, network interfaces, security modules and other advanced systems will be presented.

1.2 AUTOMOTIVE PLATFORM CONTROL MODULES

As already seen in Table 1, all of the layers of the 'automotive platform' includes electronic systems all controlled by microprocessors. In this section, the paradigm of a complete automotive control system, which is based on the automotive ignition system, will be presented. The ignition system consists of the ECUs, the EMSs, the sensors, the actuators and the exchanged data, components to be found in the entire spectrum of the automotive design. The goal of this section is to explain how different types of components and control units are used to compose the automotive control systems of the automobile, and also to identify the common points with the ICT structure.

1.2.1 IGNITION SYSTEM

The electronic ignition system, placed in Layer III of the automotive architecture design, makes use of electrical components and electronic devices (Layer I) to produce the electrical pulse by switching the ignition coil primary current 'on and off', so that a high voltage is induced in the coil secondary winding in order to produce a spark in the required cylinder at the correct time [19][20]. In terms of ICT, the vehicle is being initialized. The first generation of electronic ignition systems of this type is known as 'constant energy systems' [21]. The next generation of ignition systems [21] were the digital, also called programmed, implementing the computer technology and included the ECU or the ECM (Layer II). Either the ECU or the ECM has the ability to read the input signals such as speed, crank position, and load data [22] from the engine sensors (as described in Section 1.2.3).

1.2.2 ENGINE MANAGEMENT SYSTEM AND DATA

Because some of the sensors' signals can be used for multiple functions simultaneously, such as for ignition and fuelling, it has become a common practice to place them under the control of a single computer system. The resulting system is known as an Engine Management System (EMS) [27][28] found in Layer III. EMS is designed to ensure that the vehicle complies with emissions regulations (restrictions) and that it provides improved automotive performance. The performance characteristics of the engine and the drive ability of the vehicle are determined by the 'quality' of the input signals of the ECUs. These input signals forms the coded data that are represented as binary codes of 0s = 0.0–0.8 V and 1s = 2–5 V. The speed of transmission is measured in the number of 0s and 1s that are sent in 1 s and the number of bits per second is known as the 'Baud' rate. These values are stored into the memory of the ECU so that they can be accessed (Read) and compared with the stored values of the EMS digital map [23][24]. Then, the EMS can determine the calibration and duration of the ECUs' fuel injection pulses [25][26].

1.2.3 SENSORS, ACTUATORS & FAULT CODES

The sensors provide the input signals, in the form of pulses that enable first the ECUs and then the EMS to carry out the operations and make the system function properly [25]. As already mentioned (Sec. 1.2.2), in the case of automotive sensors a voltage is represented by a code in the microprocessor of the ECM. Actuators are electromechanical devices (e.g. fuel injectors, ignition coils, ABS modulators) operated by the outputs results of the input sensor readings from the ECMs [29][30]. If the input reading is not within the required (factory-default) limits it will be read again and if it continues to be 'out of limits' a fault code will be stored in a section of the Read Access Memory (RAM) [31]. The fault codes, also called diagnostic trouble codes (DTCs) [32][33][34], are of great importance to the safety and continuity functions of the automotive platform. As an automotive system is relies upon input data from a plethora of sensors, the diagnostics are based on the fault findings of these

sensors. The method for accessing the fault codes that the automobile manufacturers have developed is known as the Onboard Diagnostic System (OBD). The OBD system provides a very rich set of information about parameters such as the coolant temperature and the revolutions per minute (RPM) and it defines the state of the automobile. The fault codes are represented at the scan tools with five digits, e.g. A0123 = insufficient coolant temperature for the closed loop fuel control. Digit 1, at the left end, identifies the vehicle system. Digit 2 identifies the subgroup. Digit 3 identifies the sub-assembly. Digits 4 and 5 identify the localized system components. Full details are enclosed in the standard SAE J2012 document [Appendix I].

Both the hardware and software components presented in Table 1 participate actively in the composition of the automotive platform. The integration of a controlled system (Layer III) [35][36], as seen in the previously presented example of the ignition system increases the need for the implementation of network interfaces linking both Layer I (e.g. sensors, microprocessors) and Layer II (e.g. ECUs, EMSs) components [37][38]. Nowadays, it is quite common for control systems (e.g. engine management, traction control, anti-lock braking drivers' assist, tire pressure, airbags and other safety and infotainment systems) to communicate between themselves, composing the internal automotive network environment, or in terms of ICT, the network stack.

1.3 AUTOMOTIVE TELECOM INTERFACES

The automotive internal network interface improved the effectiveness of automotive control and offered safety for both the body chassis (physical ICT stack) and the passengers (user ICT stack) [39][40]. All the components and control systems (infrastructure stack) are linked together via multiple hard-wired buses, estimated to account approximately to the 25% of the automobile value [42], and wireless interfaces [41]. In this section, the wired-based network protocols used for data transfer and connectivity are described, including the Controller Area Network (CAN), the Local Interconnected Network (LIN), the Media Oriented System Transport (MOST) and the FlexRay Transport Protocol (FRTP) for higher-end applications. The wireless connections of choice include Bluetooth, Wi-Fi and Cellular interfaces [43][44][45][46]. Both of them are composing the network stack of a traditional ICT structure.

1.3.1 HARD-WIRED NETWORKING

The essential hard-wired network interfaces for the internal communication of the automotive platform include:

1.3.1.1 CAN: In 1994 the Controller Area Network (CAN) [37][38][47][48][49][50] (originally developed in the 1980s by Robert Bosch) due to its electrical noise tolerance, minimal wiring, excellent error detection capabilities, and high speed data transfer, became the ISO-11898 standard and gained acceptance in a series of applications such as in

industrial control, marine, medical and aerospace. CAN is the most widely spread automotive network protocol running at 1Mbps, dealing with active safety, body and chassis, enabling functions like millimeter wave radar, dashboard, brakes control and seat belts (collision detection system). Even though LIN, as described in the next paragraph, has displaced CAN in a number of applications, CAN is still the primary bus used for engine timing controls, anti-lock braking systems, and power train controls because of its balanced (differential) 2-wire interface running over a shielded twisted pair (STP), un-shielded twisted pair (UTP), or ribbon cable. The CAN interface uses an asynchronous transmission scheme where any node may begin transmitting at any time and messages are broadcasted to all the nodes of the automotive network. In cases where multiple nodes initiate messages at the same time, a bitwise arbitration is used to determine which message is of higher priority. Messages can be of one of four types of frame: data, remote transmission request (RTR), error, or overload. Any node on the bus that detects an error transmits an error frame which causes all the nodes on the bus to view the current message as incomplete and obliges transmitting node to resend the message. Overload frames are initiated by receiving devices to indicate that they are not ready to receive data yet. Data frames are used to transmit data while remote frames request data. Data and remote frames are controlled by start and stop bits at the beginning and at the end of each frame. A number of different data rates are defined, with 1Mbps being the fastest, and 5 Kbps the minimum rate. All modules must support at least 20 Kbps. The cable length depends on the data rate used. The maximum line length can be thousands of meters at low speeds, although 40 meters at 1 Mbps is typical. Termination resistors are used at each end of the cable.

1.3.1.2 LIN: The Local Interconnect Network (LIN) [37][38][44][45][46][50] is a low cost bus for body applications which operates at 19.2 KBauds with Universal Asynchronous Receiver/Transmitter (UART) interfaces. It was developed by the LIN consortium in 1999 as a low-cost alternative to the CAN protocol for applications where the cost, versatility, and speed of CAN were excessive. It can be used for elements and applications that demand communications between intelligent sensors and actuators such as the multifunction keyless system, window controls, door locks, rain sensors, windshield wiper controls, and climate control. LIN networks have a single master and one or more slave nodes as the LIN bus is a single-wire implementation based on the enhanced ISO-9141 standard. All messages are initiated by the master node with only one slave responding to each message, so controversy to CAN collision detection and arbitration capabilities are not needed. In the LIN topology data are exchanged in eight-bit bytes along with a start bit, stop bit, and no parity due to the UART Serial Communications Interface (SCI). Data rates range from 1 to 20 Kbps. While this may sound slow, it is suitable for the intended applications and minimizes

electromagnetic interference (EMI). The LIN bus is always in one of two states: active or sleep. When it is in the active state, all the nodes on the bus are awake, listening for relevant bus commands. Nodes on the bus can be put to sleep by either the master issuing a sleep frame or when the bus goes inactive for longer than a predetermined amount of time. The LIN bus is then awakened by any node requesting a wake up or by the master node issuing a break field. LIN frames consist of two main parts, the request and the response headers. The request header is sent by the master while the response header is sent by the slave.

1.3.1.3 MOST: The Media Oriented Systems Transport (MOST) [37][38][44][45][46][50] protocol is designed for multimedia traffic using optical fiber topology for up to 150 Mb/s in automotive telematics and infotainment networks, and has been smoothly brought to the road in its third generation with MOST150 in 2012. Considering the dramatic increases in bandwidth demands (e.g. camera, display link, consumer electronics, system interconnection, and flexible topology) and general requirements (e.g. low-cost, scalability, future-proof design) the MOST Cooperation has proved to be an excellent body, permitting direct specification and implementation processes.

1.3.1.4 FlexRay: The FlexRay Protocol [37][38][44][45][46][49][50] is a relatively new automotive network communication protocol that is in the process of being converted into an ISO standard. As automotive vehicles get smarter and electronics find their way into an increased number of automotive applications, existing automotive serial standards such as CAN and LIN do not have the speed, reliability, or redundancy required for X-by-wire applications such as brake-by-wire or steer by-wire. FlexRay is a deterministic and secure high performance bus at 10Mbps mainly used in X-by-wire and high performance applications, returns the voids² with a faster, fault tolerant, and time-triggered architecture that ensures the dependable delivery of messages for safety applications. It is a differential bus running over either an STP or an UTP at speeds up to 10 Mbps, which is significantly faster than LIN's 20 Kbps or CAN's 1 Mbps rates. FlexRay uses a dual-channel architecture that has two major benefits. The two channels can be configured either to provide redundant communication in safety-critical applications ensuring that the messages get through, or they can be configured to send unique information on each of the channels at 10 Mbps, giving an overall bus transfer rate of 20 Mbps in less safety-critical applications. The FlexRay frame is made up of three major segments: the header segment, the payload segment and the trailer segment and uses a time-triggered protocol that incorporates the advantages of prior synchronous and asynchronous protocols via communication cycles for devices that include both static (time slots of predetermined length allocated for each device) and dynamic frames (vary in length and time).

² Void is the type for the result of a function that returns normally

1.3.2 WIRELESS COMMUNICATION

The essential wireless network interfaces [37][38][41][43][50] for the communication of the automotive platform's components with wireless capabilities include both short and long range communications as follows:

1.3.2.1 Short-Range Communications:

- 1.3.2.1.1. Bluetooth: Bluetooth has become the de-facto standard for supporting hands-free calling in automobiles and is standard in mainstream vehicles sold by all major automobile manufacturers. While the lowest level of the Bluetooth protocol is typically implemented in hardware, the management and services component of the Bluetooth stack is often implemented in software. Bluetooth devices used in automotive implementations have a range of approximately ten (10) meters, but others have demonstrated that this range can be extended through amplifiers and directional antennas.
- 1.3.2.1.2. Emerging short-range channels: A number of manufacturers have started to implement 802.11 Wi-Fi access in automobiles, typically to provide a "hotspot-based" Internet access via bridging to a cellular 3G data link. As an example, Ford offers this capability in the 2012 Ford Focus³.
- 1.3.2.1.3. Dedicated Short-Range Communications (DSRC): While not currently deployed or fully implemented in the main automobile models, an emerging wireless channel is defined in the Dedicated Short-Range Communications (DSRC) standard, which is being incorporated into the proposed standards for Cooperative Collision Warning/Avoidance and Cooperative Cruise Control. In the U.S. it is investigated by the Department of Transportation's Cooperative Intersection Collision Avoidance Systems (CICAS-V) and by the Vehicle Safety Communications Consortium's VSC-A project. In such systems, forward vehicles communicate digitally to trailing cars to inform them of sudden changes in acceleration to support improved collision avoidance and harm reduction.
- 1.3.2.1.4. RFID: The Radio Frequency Identification (RFID) interface is encountered in the security mechanisms of the automobile, which is the immobilizer and in the remote keyless entry systems. Therefore, it is as a separate control system even though it belongs to the short-range communication interface layer.

³ Several other models also provided Wi-Fi receivers, but we understand they were used primarily for assembly line programming.

1.3.2.2 Long-range Communications: The automobiles' long distance (greater than 1 km) digital access channels and can be divided into two categories: broadcast channels and addressable channels.

1.3.2.2.1. Broadcast channels: Broadcast channels are the channels that are not specifically directed towards a given automobile but can be "tuned into" by receivers-on-demand. The modern automobile includes a plethora of broadcast receivers for long-range signals: Global Positioning System (GPS), Satellite Radio (e.g. SiriusXM receivers commonly found in Honda/Accura, GM, Toyota, Saab, Ford, Kia, BMW and Audi models), Digital Radio, the Radio Data System (RDS) and the Traffic Message Channel (TMC) signals transmitted as digital subcarriers on existing FM-bands. The range of such signals depends on transmitter power, modulation, terrain, and interference delivering the signal reliably over distances up to 10 km at a speed of 1,2 Kbps. In general, these channels are implemented in an automobile's media system known as the infotainment system.

1.3.2.2.2. Addressable channels: These systems provide a broad range of features supporting safety (crash reporting), diagnostics (early alert of mechanical issues), anti-theft (remote track and disable), and convenience (hands-free data access such as driving directions or weather). They are two-way channels supporting interactive control and are individually addressable. The most important part of the long-range wireless communication surface is that of the remote telematics systems (e.g. Ford's Sync, GM's On-Star, Toyota's Safety-Connect, Lexus' Enform and BMW's BMW Assist) providing continuous connectivity via cellular voice and data networks.

1.4 AUTOMOTIVE SECURITY MODULES

As already mentioned in the previous section a specific short range communication interface used for the security of the automotive platform is the RFID [52][53][54][55]. The RFID technology is applied both in the immobilizer and in the remote keyless entry systems of the automobile due to the potential that has in the automatic identification (unique ID) of physical objects through a radio interface. A typical composition of an RFID system includes:

1. Tags (transponders): a microchip attached to an antenna carrying the identifying data;
2. Readers (transceivers): query tags via radio signals responding to identifying data ;
3. Back-end databases: associate records with tag data collected by readers.

In the next two sections the immobilizer and the Remote Keyless Entry (RKE) systems will be described in detail as they compose the Passive Keyless Entry and Start (PKES) security system for physical and cyber access (authentication and authorization) in the automotive platform.

1.4.1 IMMOBILIZER SYSTEM

The immobilizer integrates the concept of RFID with the active role of the automobile security mechanism for a secure initialization of the automobile, triggering the participating components of the ignition system. The main idea of the automotive electronic immobilizer is to prevent an unauthorized vehicle entry and engine ignition unless the correct individual electronic key code, integrated as a microchip into the automobile fob key, is properly provided. The immobilizer mechanism that enables the driver to start the automobile engine includes the following standard immobilizer components:

- (1) Stand-Alone transponder, integrated into the key-fob.
- (2) Remote Keyless Entry Microcontroller with RF Transmitter and Immobilizer function,
- (3) Passive Entry / Go Microcontroller with 3D LF Receiver and Immobilizer function,
- (4) Smart Immobilizer base-station with embedded microcontroller.

The 125 kHz full duplex (FDX) immobilizer device with a load modulation data transfer is used in conjunction with an embedded RFID protocol to interoperate with any of the devices listed above. A program code (e.g. battery-less RFID Immobilizer) stored in the flash memory is typically used as a read only procedure, once the initial programming has occurred. In addition, the key-code consists of a permanent personal code and of a second code changed by the immobilizer each time the engine is started. The RFID reader communicates with the automotive electronics. This communication is protected by cryptographic procedures and the reader authenticates itself regard to the motor electronics to prevent the manipulation of the reader. The three procedures used to check the authenticity of the key are the following:

- 1.4.1.1 Unique S/N check: The transponder has a simple individual serial number (unique number). Very simple systems (first generation immobilization) read the transponder's serial number and compare it with a reference number stored in the reader. If the two numbers are identical the motor electronics are released. The fact that the transponder serial number is not protected against unauthorized reading, allows it for being read by an attacker and copied to a special transponder with a writable serial number.
- 1.4.1.2 Rolling code procedure: Every time the key is operated a new number is written to the key transponder's memory. This number is generated by a pseudo-random generator in the reader. It is, therefore, impossible to duplicate the transponder if this system is used. If several keys are used within a single vehicle each key should run its own pseudo-random sequence.
- 1.4.1.3 Cryptographic procedures (authentication) with fixed keys: The use of cryptographic procedures offers much greater security (2nd generation immobilizer). In the authentication sequence (challenge response) knowledge of a secret (binary) key is checked without this key being transmitted. In automotive applications, the unilateral authentication of the key transponder by the reader

in the ignition lock is used. Besides the fact that the immobilizer unit controls the fuel and starter ignition, it also blocks all the automobile's crucial functions in case the authentication sequence is not the proper one. The immobilizer function is only deactivated when the ignition is switched on with a registered key and it is activated automatically when the ignition is switched off. For an authentication system like an immobilizer, the objective is to prove knowledge of an identifier without compromising the identifier to any potential attacker.

1.4.2 REMOTE KEYLESS ENTRY SYSTEM

Traditionally, access and authorization have been achieved by inserting the correct physical key into the lock system. In the last decade, this system has been augmented with remote access in which users are able to open their automobiles remotely by pressing a button on their key fobs, introducing the Remote Keyless Entry systems which do not require any action from the user. The communication between the key and the vehicle is characterized by a magnetically coupled radio frequency signal, following the same principles of the RFID systems as defined before. In RKES, the automobile concludes that the key is within close proximity communications range using the LF-RFID tag (within 1-2 m in active and a few centimeters in passive mode) and a fully-fledged UHF transceiver for longer range communication (within 10 to 100 m). The RKE protocols vary depending on the manufacturer, but similar principles to the immobilizer system are applied. Typically, two modes of operation are supported, the normal mode that relies on a charged and working battery and the backup mode that operates without a battery (e.g., when the battery is exhausted). Immobilizer and keyless entry systems combined into one integrated and embedded mechanism for authorized access control, initialization and ignition of the automobile are known as the Passive Keyless Entry and Start (PKES) system. Often, such a combination of ICT development techniques in the automotive components and control systems is used to address efficiently hardware verification and software development challenges of the automotive architecture design chain (Table 1) that require advanced automotive computing power (i.e. driver assistance systems, digital instrument clusters or head units with infotainment) [56].

1.5 ADVANCED AUTOMOTIVE SYSTEMS

Nowadays, that the growing number of hardware components and complex heterogeneous control systems (Layer III-Subsystems) is at odds with the declared goal of the automotive industry to produce lighter and more fuel-efficient (and electric) vehicles [57], the already used generation of automotive microprocessors is simply not up to the task anymore, as the need for high performance multi-core processors and advance software increases [58]. In order to unfold the automotive platforms' full potential and be equipped with sophisticated, compatible, cooperative and interoperable software and hardware systems [59][60], advanced

ICT systems need to be utilized, including multi-core systems, virtualization technology and embedded software-based automotive platforms.

1.5.1 MULTI-CORE SYSTEMS

While the end-users are familiar with new applications and to the high performance offered to them by consumer electronics, the automotive manufacturers need to provide the same experience. Unfortunately, advanced user interfaces require extreme amounts of computing power as the existing single-core processors have arrived at their physical limits. But the solution to increase a system's performance is not to increase the maximum computing power but to increase the processor's throughput by employing multiple independent cores. The result is that highly-integrated Systems-on-Chips (SoCs) [57][60] with integrated multi-core processors have been developed and used for advanced control systems and services (service layer of the ICT stack) in the automotive platforms. Therefore, there are three new main-points to be taken into consideration in the automotive architecture design chain (Table 1):

- **Critical Functions Continuity:** Different critical functions need to be able to run simultaneously (in so-called partitions) without affecting each other or being affected by non-safety-critical functions.
- **Multi-OS support and integration:** The multi-core system needs to be flexible to run multiple operating systems at the same time (i.e, AUTOSAR for safety-critical functions, GenIVI Linux for automotive infotainment, Android for user applications);
- **Efficient SoC resource-sharing:** Different functions make use of the same dedicated system resources (i.e. accelerated graphics and communication channels).

1.5.2 VIRTUALIZATION TECHNOLOGY

Due to the heterogeneous structure of the 'automotive platform' architecture consisting of real-time and reactive automotive systems as discussed before (Sec.1.1), a shift on the hardware level needs also to be accompanied by matching software development [57]. One approach, that has proved to be successful in the ICT world, is the virtualization technology where transaction-level representations of the hardware (virtual prototypes) are able to execute the same code that will be loaded on the actual hardware (.hex and .elf files) [64][65]. Within this concept the multi-core System-on-Chip (SoC) can host several partitions acting independently. Nowadays, virtualization technologies based on micro-Kernels are becoming increasingly popular in automotive software, a trend that started even before multi-core processors were launched [62][63]. Aviation technology has been making use of the so-called 'separation micro-Kernels' for more than a decade now as micro-Kernels have decreased the number of control systems used in an aircraft by replacing them with software. Because the advantages of virtual architectures [66][67] were recognized in aviation long before they were recognized in the automotive industry, all the necessary software, development guidelines and safety standards already exist.

1.5.3 SOFTWARE FRAMEWORKS

Multi-core systems and the virtualization technology are the new technological standards which the automotive industries are adopting [68] for creating automotive systems including:

- 1.5.3.1. AUTOSAR [69]: Driven by the need for flexible software and network topologies among the design layers, dynamic frameworks like AUTOSAR (AUTomotive Open System ARchitecture) have been developed to support both hardware and software services. The AUTOSAR objectives are the standardization of automotive systems' functions, the scalability to different vehicle and platform variants, the maintainability throughout the entire product life-cycle and lifetime software updates and upgrades. The AUTOSAR allows original equipment manufacturers (OEMs) to define functionality independently of the implementation on the development stacks, hiding the hardware to the Run Time Environment (RTE) layer and the stack can be mapped to AUTOSAR compliant applications. The RTE handles the information exchanged between the application software components and connects them to the appropriate hardware with a virtual bus.
- 1.5.3.2. OpenSynergy-COQOS [69]: The most sophisticated standardized software framework that virtualizes automotive control systems is the COQOS. COQOS was originally designed by the OpenSynergy software house for avionics purposes. The COQOS design is based on SYSGO's Pike-OS microkernel. It integrates Linux and Android-based systems as well as AUTOSAR-compliant software. The microkernel creates logical partitions, each of which is used to run safely and independently various Operating Systems (e.g. Android or Linux distributions). All of the partitions share full access to exploit the multi-core resources, thus providing the required flexibility for integrating different types of functions and simplifying the interplay among multi-core processors and automotive functions.

Multi-core systems, micro-kernels, virtualization technology, logical partitions, efficient SoC resource-sharing, dynamic frameworks, flexible software and network topologies, multi-OS support and integration, functionality to support hardware and software services, critical-functions and real-time monitoring are only some of the features that the advanced automotive systems implement in this new era of the automotive evolution.

1.6 THE AUTOMOTIVE AS AN ICT SYSTEM

To accelerate a sustainable automotive development and in parallel industrial growth in support of ICT, the need to transfer and correlate the automotive platform into an ICT-based structure is vital. In this section, a correlation synthesis of the automotive platform under the context of a traditional ICT system is performed, in order to comprehend the dual nature (physical and cyber) of the automotive platform. The automobile is viewed as an ICT system (Table 2) consisting of its physical (body chassis) and cyber layers (telecom, services,

software, ICT equipment, data and users) correlating it with the ‘automotive platform’ architecture Table 1:

TABLE 2: COMPOSITION OF THE ‘AUTOMOTIVE PLATFORM’ STACK

| AUTOMOBILE PLATFORM: PHYSICAL LAYER | | | | | |
|--|--|---|-------------------|---|--|
| INFRASTRUCTURE | Body chassis of the automotive platform | | | | |
| USERS | Operator driver and passengers | | | | |
| AUTOMOTIVE PLATFORM: CYBER LAYER | | | | | |
| EQUIPMENT | LAYER I LAYER II LAYER III | Hardware Peripheral Components Subsystems & Control Systems | | | |
| NETWORK | LAYER III | Middleware Communication and Network Interfaces | Hard-Wired | CAN – LIN – MOST FLEXRAY – OBD | |
| | | | Wireless | Short Range | Bluetooth RFID Emerging Comm. Dedicated Comm. |
| | | | | Long Range | Broadcast Channels Addressable Channels |
| SERVICES | Security Mechanism | Immobilizer - RKES/PKES | | | |
| | LAYER I LAYER II LAYER IV | Drivers, Firmware, Software, Applications ODB-Diagnostic Software Platform OS (infotainment Systems) | | | |
| DATA | LAYER I-IV | Signals, Frames, Packets, Data Information | | | |
| USERS | - | Profiling is not defined (issue to be addressed) | | | |

In particular the physical layer includes the infrastructure, i.e. the body chassis of the ‘automobile platform’ and the user represents the operator-driver of the automobile or the passengers. The cyber layer comprises of the:

- The infrastructure, which represents the hardware and the peripheral components of the ‘automotive platform’;
- The network, which represents the communication and network interfaces for the components of the systems to communication with each other but also with the services of the next block.
- The services, which represent all the software used in ‘automotive platform’. They also include the security mechanisms for the reasons explained in Section 1.4.
- The data, which represents the signals, frames and packets exchanged between the components of the infrastructure layer.

A more concrete automotive technological analysis is shown in Figure 2 by combining the above correlation with the technological flows as they arise from the FlexRay backbone paradigm. Figure 2 illustrates that a modern automobile is a complex ICT system composed of various engineering, technological, mechanical and networking modules.

FIGURE 2: TECHNOLOGICAL PARADIGM OF THE 'AUTOMOTIVE PLATFORM'

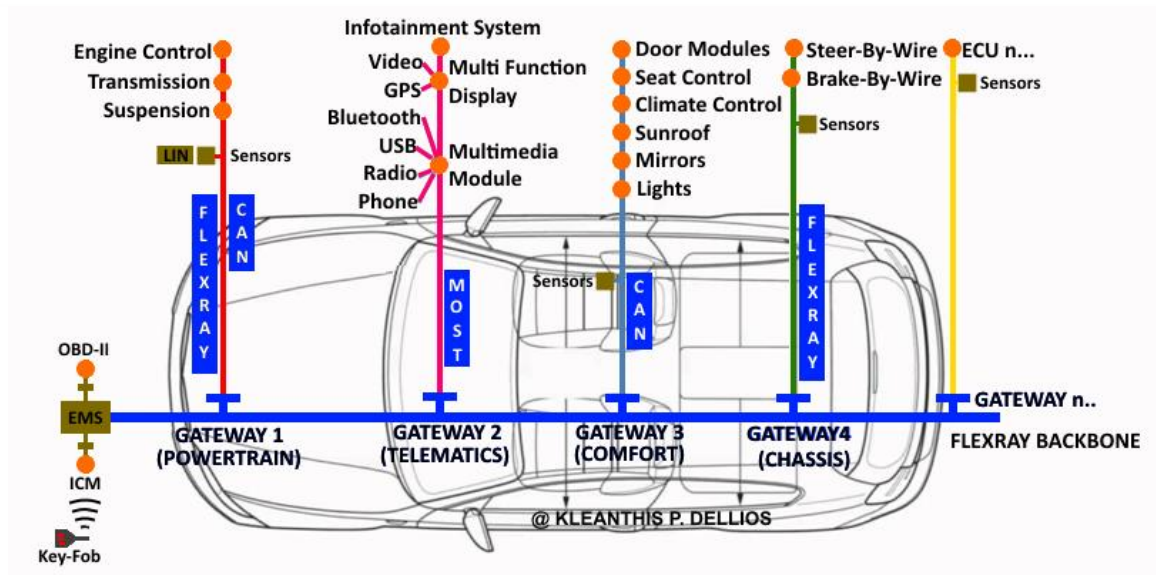


Table 2 and Figure 2 illustrate the 'automotive platform' which will become the basis for analyzing the cyber and physical threats of the automobiles in this thesis.

1.7 CONCLUSIONS

The first chapter of this thesis provides the basic knowledge and sets the architectural and technological fundamentals in the automotive platforms. This analysis leads to alternate the traditional automotive view from a mechanical object to an ICT system. This first thesis result will enable us to perform in the next chapters a concrete security analysis of the automobiles compliant with the various ICT security standards.

2. THE INTELLIGENT TRANSPORT SYSTEMS

In the previous chapter we considered the automobile as a single ICT system in the transportation domain. In this chapter, we will study how clusters of various and heterogeneous systems such as vehicles (e.g. automobiles, motorbikes), the roadside infrastructure (e.g. traffic lights), hand held systems (e.g. nomadic devices) and centralized systems (e.g. traffic control base stations) communicate, exchange and store data and information. These systems are known as Intelligent Transport Systems (ITS⁴) [71]. The supported modes in ITS include the road transport (e.g. infrastructure, vehicles and users) and the transport systems management (e.g. traffic and mobility management), without excluding interfaces for other modes of transport (e.g. railway, marine and aviation) [72][73]. The overall ITS environment comprises of the ITS Communication (ITSC), the ITS-Station Reference Architecture (ITS-S), the ITSC elements, the ITS-S components and the Application Classes (standardized by a number of organizations⁵) are also described in the following sections.

2.1 ITS COMMUNICATION (ITSC) PRINCIPLES

ITS Communication (ITSC) is the type of communication systems dedicated to transportation scenarios based on two domains⁶; that of the ITS domain and that of the Generic domain. The "ITS domain" refers to all the elements of ITSC which are specified in the ITS standards, while the "Generic domain" refers to other elements used for ITSC. The fundamental communication model of the ITSC consists of the ITS Station (ITS-S) reference architecture which includes the internal functional blocks and the interfaces between these blocks (access layer; networking and transport layer; facilities layer; ITS applications; management entity and security entity), various general addressing mechanisms and the ITS Station management information base. Furthermore, all of the participating ITSC objects are addressable instances of the ITS-S functionality and the ITS applications. Both the ITSC objects and the ITS-Applications use:

- wireless communications between mobile ITS stations (vehicles), and between mobile ITS stations and fixed ITS stations (roadside installations), with single-hop or multiple hop distance between the source and the destination ITS stations;
- access to public and private (local) networks including the global Internet, and satellite broadcast.

⁴ Chapter 2 is based on the ISO/ETSI ITS standards specifications as found in **References [74]-[81]**.

⁵ Found in Appendix I: ITS Standardization Organizations.

⁶ In ISO TC204 WG16 the domains are distinguished by the terms "CALM-aware" (ITS domain) and "Non-CALM-aware" (generic domain).

The essential aspects that are considered in the process of developing ITSC standards are the following:

- the mobility of ITS-Stations which causes high dynamics in their topology;
- the support of every kind of communication technology, networks and legacy systems;
- the dynamic and flexible consideration of user needs with respect to communications capacity (data rate), communications reliability, availability and privacy;
- the efficient prioritization of application classes and the dedicated relations between applications and communication technologies which are dependent on regional requirements;
- the support of global applicability and cooperativeness.

2.2 THE ITS-STATION ARCHITECTURE

In order to better comprehend the essential aspects of the developed ITSC standard the 'ITS-Station Reference Architecture' (ITS-S RA) is described here. The ITS-S RA follows the principles of the OSI communication model for layered communication protocols, but in the case of ITS it is extended with the inclusion of the ITS-Applications. More specifically, the ISO communication model consists of seven layers. The physical, data-link, network and transport layers form the lower layers of the OSI model implementing the units of bits, frames, packets and segments respectively. The remaining three layers, namely session, presentation and application layers, form the upper layers where data are represented. Each layer is self-contained and only deals with the interfaces of the layer immediately above and below. It performs its functions and tasks, transferring the results to the layer above or the layer below. This function enables product manufacturers to design ICT products operable in a particular layer that will interface with the hardware of other manufacturers.

- The Physical Layer delimits and encodes the bits onto the physical medium and defines the electrical, mechanical and procedural formats.
- The Data-Link Layer transfers data units from one network node to another over the transmission circuit (physical addressing) and ensures data integrity between nodes (Media access and logical link control).
- The Network Layer (3) routes and relays data units across the network nodes (Path determination and logical addressing) and manages flow control and call establishment procedures (addressing and routing).
- The Transport Layer function (4) ensures end-to-end data transfer and integrity across the network and assembles the packets for routing by the Network Layer.
- The Session Layer function (5) coordinates the connection and the interaction between the applications and performs the tasks of managing and synchronizing the direction of the data flow.

- The Presentation Layer function (6) negotiates the syntactic representation to perform the task of data transformation (e.g. compression, code conversion).
- The Application Layer (7) provides the network access to the lower layered functions for performing the task of software application interaction.

Although the concept of the layered OSI model is based on isolated layers, where each layer contains a complete set of functionality as described above, ITSC provides cross layer functionality, as presented in Table 3 below, related to all of the ISO model layers. The ITS-S RA blocks include:

- "Access" representing ITSC functionality of OSI Layers 1-2;
- "Networking & Transport" representing ITSC functionality of OSI Layers 3-4;
- "Facilities" representing ITSC functionality of OSI Layers 5, 6;
- "Applications" representing ITSC functionality of OSI Layer 7.

TABLE 3: CROSS LAYER FUNCTIONALITY OF THE ISO MODEL AND THE ITS-STATION ARCHITECTURE

| ISO/OSI MODEL | | FUNCTION | TASK | ITS-Station RA | | |
|------------------|---------|--|---|----------------|------------|----------|
| LAYER | UNIT | | | Blocks | | |
| [7] Application | Data | Network process to application | Software application interaction | Applications | | |
| [6] Presentation | | Data representation, encryption, conversion | Formats and encrypts data to be sent over the network | Management | Facilities | Security |
| [5] Session | | Communication and managing sessions between applications | Establishes, manages and terminates the network connections | | | |
| [4] Transport | Segment | End-to-End connections and flow control | Reliable link via segmentation, flow and error control | | | |
| [3] Network | Packet | Path determination and logical addressing | Addressing and Routing | | | |
| [2] Data-Link | Frame | Physical addressing | Media access and logical link control | | Access | |
| [1] Physical | Bit | Signal and binary transmission | Electrical and physical specifications for devices | | | |

Furthermore, the functional blocks are interconnected either via observable interfaces or via Service Access Points (SAPs) or via Application Programming Interfaces (APIs). In all the ITSC standards, the specification of SAPs can only be informative functional specifications.

2.3 THE ITS-STATION FUNCIONAL COMPONENTS

In order to analyze the ITS-S RA blocks of Table 3, the functional components which participate actively need to be defined as follows:

- i. ITS-S host: An ITS-S host contains the ITS-S applications and the functionality of the ITS station reference architecture necessary for the ITS-S applications.
- ii. ITS-S gateway: An ITS-S gateway interconnects two different OSI protocol stacks at layers 5 to 7 converting protocols connected to the ITS station-internal network and to a proprietary network.
- iii. ITS-S router: An ITS-S router provides the functionality interconnecting and converting two different ITS protocol stacks at layer 3 of the ITS station-internal network.
- iv. ITS-S border router: An ITS-S border router basically provides the same functionality as the ITS-S router with the difference that the protocol stack related to the external network may not follow the management and security principles of ITS.
- v. ITS-S interceptor: An ITS-S interceptor, in the context of ITSC, is either equal to an ITS-S gateway, an ITS-S router, or an ITS-S border router, or it may provide an implementation specific method to connect the ITS station-internal network to another network.

2.4 ITS-S RA BLOCK ANALYSIS

In this section, the analysis of the ITS-S RA blocks is presented. In addition, as already mentioned in previous section all of the functional blocks of ITS-S RA shown in Table 4 are interconnected via four SAPs which located in the “Access”-block:

- i. The Facilities/Applications-SAP (FA) interface which enables the full duplex exchange of data between the application layer and the facilities layer.
- ii. The Security/Facilities-SAP (SF) interface which enables the full duplex exchange of data between the facilities layer and the security layer. In particular, the facility layer may request from the security layer the certification of transmitted messages and the authentication of received messages.
- iii. The Management/Facilities-SAP (MF) interface which enables the full duplex exchange of data between the facilities layer and the management layer. In particular, the management layer communicates to the facilities layer the management policies that are necessary to guarantee an optimized global system operation and a consistent cross-layer operation.
- iv. The Network-Transport/Facilities-SAP (NF) interface which enables the full duplex exchange of data between the facilities layer and the networking and transport layer.

The rest of the blocks are formed and analyzed as follows:

1. ITSC supports the “Networking and Transport” block from a top-level point of view. The ITS station connects to access networks via ITS-S border routers or the ITS station connects to ITS ad hoc networks via ITS-S router. The ITS station internal network is not necessarily physically available. It may be realized simultaneously with different access technologies, both wired, e.g. Ethernet, or wireless, e.g. BlueTooth. The ITS station typically connects to a proprietary network via an ITS-S gateway, i.e. the central ITS-S gateway, the vehicle ITS-S gateway and the roadside ITS-S gateway.
2. The “Facilities” block provides generic support facilities to applications. This layer is further composed of three main components:
 - i. The application support is the kernel of the common functions supporting the applications. It consists of the station lifecycle management, the automatic services discovery, download and initialization of new services, the HMI generic capabilities, and many others. A key concept in ITS is the ability of the transport entities (vehicles, roadside infrastructure, pedestrians, etc.) to collect knowledge regarding their local environment from a range of sensor equipment, and to share that knowledge in order to achieve a more intelligent use of the transport infrastructure. This is described in the term "co-operative awareness".
 - ii. The information support covers the presentation layer of the OSI reference model and holds the role of data management. In any ITS system, there will exist an abundance of data sources, both mobile and static ones. Most of these data will be location-referenced, time-specific and attached with a life time value and with accuracy and reliability parameters. Therefore, fusing data and keeping the information up to date is one of the challenges of information support. The main entity that supports this function is the Local Dynamic Map (LDM) which is able to take data both from various sources and from received ITS messages to build a data model of the local environment. Furthermore, the information support takes on many functions of the OSI Presentation Layer.
 - iii. The communication support, which includes the session layer of the ‘OSI Reference Model’, cooperates with the transport and network layer to achieve the various communication modes required by the applications.
3. The block "Applications" present the ITS-S applications which use the ITS-S services to connect to one or more other ITS-S applications. An association of two or more complementary ITS-S applications constitutes an ITS application which provides an ITS service to a user-entity of the ITS environment.
4. The "Management" entity is in charge of managing communications in the ITS station and grants access to the Management Information Base (MIB).

5. The "Security" entity provides security services to the OSI communication protocol stack, to the security entity and to the management entity. "Security" can also be considered as a specific part of the management entity.

Nevertheless, both the management and the security blocks are not clearly presented in the ITS standards. As the ITS are based on the communication among their participating parties-entities with a number of functional elements and components, in order to obtain certain cooperative services, as discussed in the following sections, the entire ITS-Station RA is designed on a sensor-based and device-embedded implementation of the existing communication interfaces. Therefore, interoperability and security among the automotive platforms stack is difficult to be achieved and different approaches need to be adopted.

2.5 ITSC FUNCTIONAL ELEMENTS

The participating functional elements of the ITS-S RA, which interact with the blocks and the components previously presented but also interact with each other, are the following:

- i. personal ITS sub-system; in hand-held devices,
- ii. central ITS sub-system; part of an ITS central system,
- iii. vehicle ITS sub-system; in automobiles, trucks, motorbikes etc., in motion or parked,
- iv. roadside ITS sub-system; on gantries, poles, etc.

Dependent on the context they are applied each of these ITS sub-systems will contain other functional components. The ITSC functional elements can be implemented into a single physical unit or in several physical units as follows:

- i. The Personal sub-system provides the application and communication functionality of ITSC in hand-held devices, such as PDAs, mobile phones, etc. It contains a personal ITS station. The device used as a personal ITS station may also perform Human Machine Interface (HMI) functionality as part of another ITS sub-system, connected to the first via the ITS station internal network.
- ii. The Central ITS sub-system contains a central ITS station and may contain ITS-S interceptors. Typically, the ITS-S interceptors in the central ITS sub-system typically are a central ITS-S gateway and an ITS-S border router. The central ITS-S gateway provides the necessary functionality to connect the components of the central system to the ITS station internal network.
- iii. The Vehicle ITS sub-system contains a vehicle ITS station and may contain one or more ITS-S interceptors. The ITS-S interceptors in the vehicle ITS sub-system typically are the vehicle ITS-S gateway and the ITS-S route. The vehicle ITS-S gateway provides functionality to connect the components of the proprietary network, e.g. ECU, to the ITS station-internal network. The interface of the in-

vehicle components such as the ECU was described in Chapter 1. Access to components such as to ECU can be achieved in an implementation specific way as shown in Chapter 3.

- iv. The Roadside ITS sub-system contains a roadside ITS station and may contain ITS-S interceptors. Typically the ITS-S interceptors in the roadside ITS sub-system typically are a roadside ITS-S gateway, an ITS-S router and an ITS-S border router. The roadside ITS-S gateway provides the necessary functionality to connect the components of the roadside system, e.g. the inductive loops and the variable message signs (VMS), of the proprietary network to the ITS station-internal network.

2.6 ITS-STATION APPLICATION CLASSES

The management of the ITS applications, which are specified in the main context of ITSC (Section 2.3) is an association of two or more complementary ITS-S applications. The ITS Basic Set of Applications (BSA) resides in the block "Applications" of the ITS-S RA architecture (Table 3) and depending on how these applications rely on communication services, security, latency and other performance parameters they are grouped into "Road Safety", "Traffic Efficiency" and "Other Applications" classes as shown in Table 4.

TABLE 4: THE ITS BASIC SET OF APPLICATIONS

| Application Class | Application Taxonomy | Application (Use Case) |
|--------------------------------|--|--|
| Active Road Safety | Driving Assistance (Cooperative Awareness) | Emergency Vehicle Warning |
| | | Slow Vehicle Indication |
| | | Intersection Collision Warning |
| | | Motorcycle Approaching Indication |
| | Driving Assistance | Stationary Vehicle Accident –Problem |
| | Road Hazard Warning | Emergency Electronic Brake Warning |
| | | Wrong Way Driving Warning |
| | | Traffic Condition – Signal Violation Warning |
| | | Road-Work & Collision Risk Warning |
| | Decentralized Floating Data | Hazardous Location |
| | Road Adhesion - Visibility | |
| Cooperative Traffic Efficiency | Speed Management | Regulatory Speed Limits Notification |
| | | Traffic Light Optimal Speed Advisory |
| | Cooperative Navigation | Traffic Information |
| | | Route Guidance & Navigation |
| Cooperative Local Services | Location-based Services | Limited Access Warning |
| | | Point of Interest notification |
| | | Automatic Access control |
| | | Parking Management |
| | | ITS local e-commerce |
| Global Internet Services | Communities Services | Media Downloading |
| | | Insurance & Financial Services |
| | ITS-Station Lifecycle Management | Fleet Management |
| | | Vehicle software provision/upgrade |
| | Vehicle and RSU data Calibration | |

Table 4 includes the detailed group (Use Cases) of all the ITS-Basic Set of Application Class List participating in the ITS-Station RA. The description of the primary application classes includes:

- i. The ‘Cooperative Road Safety’ application class: The primary objective of the applications in the active road safety class is the improvement of road safety.
- ii. The ‘Cooperative Traffic Efficiency’ application class: The primary objective of the applications in the traffic management class is the improvement of traffic flow.
- iii. The ‘Cooperative Local Services’ and the ‘Global Internet Services’ application classes: Applications in the co-operative local services and global internet services classes provide on-demand information to passing vehicles and include the life cycle management.

2.7 CONCLUSIONS

This second chapter is devoted to the Intelligent Transport Systems. It extends the automotive communication and provision of services among all elements in the ITS. The standards for ITS have been assessed, concluding that the interoperability and security have not been appropriately addressed. In particular, the management and the security of the ‘ITS-S RA’ blocks are not described clearly in the standards. As an overall conclusion from the previous chapters we can notice that security and interoperability are neither addressed in individual ‘automotive platforms’ nor in their clusters (e.g. in the ITS). The following parts of this thesis will contribute towards enhancing the security, interoperability and sustainability of the ‘automotive platform’ and the ITS.

REFERENCES

- [1] A. Richardson, T. Collins, Electricity: A Question and Answer Book, Fact Finders, 2006
- [2] M. Brumbach, Industrial Electricity, Delmar-Cengage Learning, 8th edition, 2011
- [3] D. J. Griffiths, Introduction to Electrodynamics, Prentice Hall, 3rd edition, 1999
- [4] S. Robertson, Automotive Electrical Maintenance, Butterworth-Heinemann, 2011
- [5] A. Santini, Automotive Electricity & Electronics, Delmar-Cengage Learning, 2nd edition, 2013
- [6] US Department of Commerce, Electric Current Abroad, US Government Printing Office, 1991
- [7] E. Lakervi, E. J. Holmes, Electricity Distribution Network design, Peter Peregrinus Lts, 3rd edition, 2003
- [8] V.A.W. Hillier, Fundamentals of Automotive Electronics, Hutchinson Education, 2nd edition, 2001
- [9] S. Srinivasan, Automotive Mechanics, Tata McGraw-Hill Publishing, 4th edition, 2006
- [10] S. Dhameja, Electric Vehicle Battery Systems, Butterworth-Heinemann, 2002
- [11] T. Gilles, Automotive Service: Inspection, Maintenance, Repair, Delmar-Cengage Learning, 4th edition, 2012
- [12] S. L. Herman, Industrial Motor Control, Delmar-Cengage Learning, 7th edition, 2012
- [13] R. Bosch, Bosch Automotive Networking: Expert Know-how on Automotive Technology, Bentley Publishers, 2007
- [14] J. E. Duffy, Modern Automotive Technology, Goodheart-Willcox Pub, 2008
- [15] M. Emmelmann, B. Bochow, C. Kellum, Vehicular Networking, Automotive Applications and Beyond, Willey and Sons Ltd, 2010
- [16] R. Bosch, Audio, Navigation and Telematics in Vehicles: Technical Instruction, Bentley Publishers, 2002
- [17] A. Emadi, Handbook of Automotive Power Electronics and Motor Drives, CRC Press, 2005
- [18] J. Huntington, Show Networks and Control Systems: Formerly Control Systems for Live Entertainment, Zircon Designs Press, 2012
- [19] CDX Automotive, Fundamentals of Automotive Technology: Principles and Practice, Jones & Bartlett Learning, 2014
- [20] J. Erjavec, Automotive Technology: A Systems' Approach, Delmar-Cengage Learning, 5th edition, 2010
- [21] C. Jacobs, Performance Ignition Systems, Berkley Publishing Group, 1999
- [22] A. Bonick, Automotive Computer Controlled Systems, Butterworth-Heinemann, 2007
- [23] A. Bonnick, D. Newbold, A Practical Approach to Motor Vehicle Engineering and Maintenance, Butterworth-Heinemann, 2005
- [24] W. Ribbens, Understanding Automotive Electronics, Butterworth-Heinemann, 5th edition, 1998
- [25] J. Turner, Automotive Sensors, Momentum Press, 2009
- [26] G. Meijer, Smart Sensor Systems, Wiley & Sons Ltd, 2008
- [27] T.K. Garrett, K. Newton, W. Steeds, The Motor Vehicle, Butterworth-Heinemann, 13th edition, 2001.
- [28] J. Hirst, R. Brooks, Engines, Electronics and Related Systems, Vehicle Maintenance and Repair Series - Level 3, Thomson Learning, 3rd edition, 2006
- [29] A. M. Pawlak, Sensors and Actuators in Mechatronics: Design and Applications, CRC Press, 2007

- [30] J. Marek, H.P. Trah, Y. Suzuki, I. Yokomori, *Sensors for Automotive Technology*, Wiley-VCH, vol.4, 2003
- [31] T. Denton, *Advanced Automotive Fault Diagnosis*, Routledge Publishing, 2012
- [32] K. McCord, *Diagnostic Systems, Understanding OBD-I & OBD-II*, Cartech Inc, 2011
- [33] Haus Der Technik, *Onboard-Diagnose III*, Expert-Verlag, 2009
- [34] M. Concepcion, *Automotive Computer Network Repair*, Mandy Conception, 2nd edition, 2011
- [35] U. Kiencke, L. Nielsen, *Automotive Control Systems For Engines, Driveline and Vehicle*, Springer-Verlag, 2005
- [36] S. V. Hatch, *Computerized Engine Controls*, Delmar-Cengage Learning, 9th edition, 2012
- [37] Society of Automotive Engineers, *In-vehicle Networks 2002*, SAE SP-1658, 2002
- [38] Society of Automotive Engineers, *In-vehicle Networks and Software, Electrical Wiring Harnesses and Electronics and Systems Reliability*, SAE International, 2004
- [39] R. Bosch, *Bosch Automotive Handbook*, Wiley and Sons Ltd, 3rd edition, 2004
- [40] H. Hunter, *Automotive & Transportation Technology, Digital Overdrive*, 2007
- [41] T. Kosch, C. Schroth, M. Strassberger, M. Bechler, *Automotive Internetworking*, Wiley and Sons Ltd, 2012
- [42] R. Bosch, *Automotive Electrics, Automotive Electronics*, Bentley Publishers, 2007
- [43] D. Paret, *Multiplexed Networks for Embedded Systems*, Wiley and Sons Ltd, English edition, 2007
- [44] G. Held, *Inter-and Intra-Vehicle Communications*, Auerbach Publications, 2008
- [45] Federal Transit Administration, *TCRP Report-43: Understanding and Applying Advance On-Board Bus Electronics*, Transit Cooperation Research Program, 1999
- [46] Federal Transit Administration, *TCRP Synthesis-44: Training for On-Board Bus Electronics*, Transit Cooperation Research Program, 2002
- [47] W. Voss, *A Comprehensible Guide to CAN*, Copperhill Technologies, 2000
- [48] M. Di Natale, H. Zeng, P. Giusto, A. Ghosal, *Understanding and Using the CAN Communication Protocol*, Springer, 2012
- [49] M. Alkan, *Inter-Connector Flexray and CAN Networks for In-Vehicle Communication*, VDM Publishing, 2010
- [50] B. Sosinsky, *Networking Bible*, Wiley Publishing, 2009
- [51] D. Paret. *Flexray and its Applications: Real-Time Multiplexed Network*, Wiley and Sons Ltd, English edition, 2012
- [52] V.D. Hunt, A. Puglia, M. Puglia, *RFID-A Guide to Radio Frequency Identification*, Wiley and Sons Inc, 2007
- [53] H. Lehpamer, *RFID Design Principles*, Artech House, 2nd edition, 2012
- [54] S. Ahson, M. Ilyas, *RFID Handbook: Applications, Technology, Security and Privacy*, CRC Press, 2008
- [55] J. Banks, *RFID Applied*, Wiley and Sons Inc, 2007
- [56] M. Domeika, *Software Development for Embedded Multi-Core Systems: A Practical Guide*, Newnes-Elsevier, 2008
- [57] W. Ecker, W. Muller, R. Domer, *Hardware Depended Software: Principles and Practice*, Springer Science, 2009
- [58] G. Meyer, *Advanced Microsystems for Automotive Applications*, Springer-Verlag, 2012

- [59] S.W. Keckler, K. Olukotum, H.P Hofstee, *Multicore Processors and Systems*, Springer Science, 2009
- [60] B. Moyer, *Real World Multicore Embedded Systems*, Newnes-Elsevier, 2013
- [61] H. Kopetz, *Real-Time Systems: Design Principles for Distributed Embedded Applications*, Springer-Verlag, 2nd edition, 2011
- [62] J. Kisielnicki, *Virtual Technologies*, IGI Global Snippet, 2008
- [63] H. Wen, P.K. Tiwary, T. Le-Ngoc, *Wireless Virtualization*, Springer, 2013
- [64] W. Mauerer, *Professional Linux Kernel Architecture*, Wiley Publishing, [Online] http://www.e-reading-lib.org/bookreader.php/142109/Professional_Linux_kernel_architecture.pdf
- [65] D. P. Bover, M. Cesati, *Understanding the Linux Kernel*, O'Reilly Media, 3rd edition, 2006
- [66] VMware, *Virtualization Overview*, [Online] <http://www.vmware.com/pdf/virtualization.pdf>
- [67] VMware, "Understanding Full Virtualization, Paravirtualization and Hardware Assist", Whitepaper, [Online] http://www.vmware.com/files/pdf/VMware_paravirtualization.pdf
- [68] Open Automotive Alliance, 2014 [Online] www.openautoalliance.net
- [69] AUTOSAR, *Automotive open system architecture*, 2013 [Online] www.autosar.org
- [70] OpenSynergy Software Framework, 2013 [Online] www.opensynergy.com
- [71] EU-US ITS Task Force, *Status of ITS Communication Standards – Document HTG3-1*, 2012
- [72] B. McQueen, J. McQueen, *Intelligent Transportation Systems Architectures*, Artech House, 1999
- [73] B. Williams, *Intelligent Transport Systems Standards*, Artech House, 2008
- [74] ETSI EN 302 665, *Intelligent Transport Systems (ITS) – Communication Architecture*, 2010
- [75] ETSI TR 101 607, *Intelligent Transport Systems (ITS) – Cooperative ITS (C-ITS)*, 2013
- [76] ETSI TR 102 638, *Intelligent Transport Systems (ITS) – Vehicular Communication*; BSA, 2009
- [77] ETSI TR 102 698, *Intelligent Transport Systems (ITS) – Vehicular Communication; Use Cases and Technical Specifications*, 2010
- [78] ETSI TR 102 962, *Intelligent Transport Systems (ITS) – Framework for Public Mobile Networks in Cooperative ITS (C-ITS)* 2012
- [79] ETSI TS 102 723 (part 1-11), *Intelligent Transport Systems (ITS) – OSI Cross Layer Topics*, 2012
- [80] ETSI TS 102 860, *Intelligent Transport Systems (ITS) – Classification and management of ITS application objects*, 2011
- [81] ETSI TS 102 894 (part 1-2), *Intelligent Transport Systems (ITS) – Users and Applications Requirements*, 2013

PART II: ASSESSING AND SECURING THE AUTOMOTIVE PLATFORM

As already presented in the first part of this dissertation, modern automobiles have evolved to automotive-platforms with networking capabilities and several advanced functionality, safety, performance and comfort features. Such a rapid evolution has set the automotive platform as an active functional element of the Intelligent Transport Systems (ITS), as presented in the second chapter.

Unfortunately, the fact that the automobiles are still being stolen clearly indicates that the preventive and protective security mechanisms used for the physical security of the automobile are not adequate enough. On top of that, the implementation of embedded ICT interfaces also raises security issues concerning whether the automotive platform must be treated as a critical asset of the cyberspace or just as a machine in the era of Internet of Anything [41]. And if the automotive platform is recognized as a cyber-asset, what is the impact caused to the entire Intelligent Transport Systems' structure?

In this part of the dissertation, security efforts of numerous organizations are cited presenting the automotive platform as the next trend of hactivisms, before proceeding in creating a threat model suitable for the automotive platform. The goal of the conducted threat analysis is to contribute to the discovery of the vulnerable to cyber-attacks interfaces of the automotive platform. The output results of the threat analysis will point out the root of automotive lack of security and the impact such a lack causes to ITS. In addition, major design flows affecting the most valuable functional element of the ITS will be identified in order to proceed in the next chapter where the MASC-Protocol is presented. MASC represents the proposed solution of the previous mentioned cyber security vulnerabilities of the automotive platform.

3. AUTOMOTIVE PLATFORM THREAT MODELING

Based on the analysis of the automotive technology as presented in the first chapter of the thesis, the progress in automotive electronics still proceeds and modern automobiles already contain a multiplicity of interact controllers. In addition, the automotive communication networks connected to several crucial mechatronic components of the automobile and compose the automotive systems and set the automobile as an autonomous networking platform. Such a rapid technological progress in the automotive domain introduces the possibility of threats and vulnerabilities across the automobile surface, opening a new promising avenue for malicious attackers to exploit [1][2].

Motivated by the already published automotive cyber-security awareness reports and whitepapers of numerous organizations, the primary goal of this chapter is to present an extended security analysis of the automobile attack-surface [3][4] based on the results of Chapter 1. The final result of the automotive analysis will not only to point out the automobile entry-points (vulnerabilities) that can be exploited to perform an automotive cyber-attack, but they will also capture the reasons of the existing lack of security and the magnitude of the impact (human, automobile and ITS) caused this lack may cause.

3.1 AUTOMOTIVE CYBER-SECURITY AWARENESS

In the past two decades, the underlying automotive control systems have changed dramatically. Today's automobile contains a myriad of embedded microcontroller systems coordinating and monitoring sensors and components, as they encapsulate over 100 MB of binary code and multiple Electronic Control Units (ECUs) communicating over one or more shared internal network buses. While modern automobiles rely on online systems (both electronic and internet based) from safety to onboard entertainment, the automotive industry, which has always considered safety as a critical engineering concern has not anticipated in the vehicles manufacturers' designs the possibility of an adversary.

Therefore, the automotive cyber-security awareness defined, as the knowledge, attitude and training of the automotive experts and anyone involved in the automotive domain regarding the physical and cyber protection of the modern automobile and the entire Intelligent Transport Systems and Transportation Domain, is missing. In this section, a number of organizations working on automotive security awareness and their points of view will be presented before proceeding with any further automotive security research activity of the domain.

3.1.1 AUTOSEC

AUTOSEC [5][6][7] investigated automotive security with experiments involving two passenger automobiles, testing their components in isolation in the lab (controlled settings) and live in road tests on a closed course. They assessed comprehensively how much resilience a conventional automobile has against a digital attack mounted against its internal components. Their findings proved that the answer was “little.” In addition, rather than just focus on individual attacks, they demonstrated the ability to systematically control a wide array of automobile components (such as the engine, the brakes, the heating and cooling, the lights, the instrument panel, the radio, the locks etc.) and evaluated the security properties of these components. AUTOSEC provided valuable contributions towards framing the automobile security and privacy issues and towards outlining the security limitations of the popular CAN bus protocol. In addition, AUTOSEC pointed out that the efforts to design fully autonomous vehicles would introduce even more new security concerns and raise even more security issues.

3.1.2 US DEPARTMENT OF TRANSPORTATION

Even though the US Department of Transport (DoT) [8] shared the same vision of a networked vehicle with the automotive industry, it foresaw that a plan for protecting the vehicles and safeguard the wired roadway from cyber-attacks was vital. For this reason the US DoT [1] issued the Request for Information (RFI) [9] and according to it: “The DoT is collecting relevant information to characterize needs and establish a strategic research roadmap to meet the rising challenges of ensuring the safety of automotive safety-critical systems due to increasing complexity of motor vehicle systems using advanced electronic controls to improve drivability, safety, efficiency, and operational reliability; escalating use of information technology in motor vehicles ...”.

In addition, the DoT requested input to help the automotive industry to make strategic decisions about the next research steps and to justify initiatives relative to research possibilities as well as revised approaches to regulation, enforcement, incident/forensics, vehicle testing, communications /outreach /professional capacity building, or recommended electronic hardware/software systems architecture and engineering design safeguard principles and/or practices, including human factors and training considerations" by thoroughly investigating cyber-security topics including:

- threats, vulnerabilities and risk of the automotive safety-critical systems, components and communication systems;
- security and penetration testing, forensic approaches and impact caused to other entities and/or domains;

Such an approach shows that the US DoT is aware not only that the future networked roadways and the existing automotive cyber threats will evolve rapidly, but also that preparation and prevention are the best actions to take.

3.1.3 MCAFEE

McAfee's automotive security report [10][11] presented the analysis of emerging security risks in automotive systems. They concluded that as trend of the vehicle becoming computerized and connected is increasing, so does the need to apply security in both the engine compartment and the dashboard console. Nevertheless, little has been done to ensure the security of these systems. Starting from the Remote Keyless Entry Systems (RKES) that did not implement any security functions and were easily compromised, they pointed out to the next security lesson (e.g. the bypassing of the ignition lock by shorting the electric link to start the engine). The infotainment system was also identified as a very attractive arena for attackers (e.g. it runs standard software for embedded devices) revealing various software vulnerabilities and bugs. Interconnected embedded systems, cellular networking and Internet connectivity also introduce another set of exploitable security flaws.

3.1.4 AUTOSAR

AUTOSAR [12] is a de-facto standard for the embedded automotive software architecture but unfortunately in its previous specification releases there was no explicit focus on safety and security applications. As functional safety is becoming one of the most important topics in automotive development, AUTOSAR published a series of new embedded features that allow both safety and non-safety applications to operate on the same controller into its software architecture. In AUTOSAR Release 4.0 new concepts were introduced, adding functional safety features [13][14][15][16] to support:

- the building of automotive safety-related applications;
- the detection and handling of safety issues like hardware faults at runtime;
- the detection and handling of requirements on timing and logical order of the execution of the applications;
- the communication protection of the applications, the data corruption, and the wrong service calls.

AUTOSAR has also established an embedded crypto-module framework into its basic software which is called Crypto Service Manager (CSM). CMS provides the means to restrict access to certain functions or to their usage by authorized users and to detect the unauthorized usage or access. However, the global networking, provided most of the times by the internet into the vehicle emerging technologies exposed the vehicle and turned it "visible" to the cyberspace. This exposure is an action that requires a security level higher than the

one that AUTOSAR is offering. Such security level is currently not covered by any standardization body or other organization.

3.2 **AUTOMOTIVE PLATFORM THREAT MODELING**

Beside the automotive security efforts presented in the previous sections, the increasing coupling of automotive control systems with multimedia networks and the integration of wireless interfaces are transform the unprotected automobile platform into a hackathlon arena [1][2][3][4]. In addition, the automobile is the key element of the entire ITS structure since as without a proper operating automotive, the entire ITS structure, services and applications would not exist. Nevertheless, such an extended automotive technology revolution hides multiple security threats capable to affect the entire Transportation Domain and in some cases the human life of the driver and the passenger. In addition, existing information security approaches (standards, methodologies and tools) [17], including the ISO 26262⁷ standard [18], do not exclusively cover the complex, heterogeneous and rapidly growing automobile platform and the impact caused to ITS by modern cyber-threats.

For these reasons, an asset-centric threat model⁸ [19] applied in the automotive platform is essential to view through security glasses all the entire automotive platform structure and give us a feedback of the security threats posing in it. Unfortunately, no current existing threat modeling method is designed for the cyber (information, application and mobile) and physical nature of the automotive platform. To satisfy the requirements of such a demanding environment like the automobile platform is itself; the asset-centric threat model will be manually configured. The manually configured threat model is based in the traditional threat model⁹ and the newly developed OWASP¹⁰ mobile threat modeling project [20]. The security model applied in the threat model to guide the information and mobile security policies within the automobile platform is the CIA triad (Confidentiality, Integrity, Availability) with the adaption of the authenticity principle from the alternative CIA model¹¹.

All of the investigated security objectives of the attacked surface of the automotive platform will be related to the confidentiality, integrity, availability and authentication of the produced threats.

- Confidentiality the concealment of information or resources. It can also be formulated as the act of keeping unauthorized users from gaining possibly sensitive information.

⁷ ISO 26262 Automotive Safety and Security Standard

⁸ Threat model is based on Microsoft's SDL (Security Development Lifecycle) process.

⁹ STRIDE & DREAD methodologies for Automotive Threat Modeling design are not excluded.

¹⁰ The Open Web Application Security Project (OWASP) is worldwide not-for-profit charitable organization focused on improving the security of software

¹¹ In 2002, Donn Parker proposed an alternative model for the classic CIA triad that he called the six atomic elements of information. The elements are confidentiality, possession, integrity, authenticity, availability, and utility.

- Integrity is the trustworthiness of data or resources. Another definition used for integrity is that the data state be the same as in the data source and not be exposed to accidental or malicious alteration or destruction.
- Availability is the ability to use information or resources as desired.
- Authenticity is the genuine validation of the data, transactions and communications and of the participating entities.

In addition, when referring to automotive safety and security, it is important to highlight and clarify the differences between these two concepts. Automotive security addresses the protection against malicious manipulations and the threats against the automobile cyber attacked surface, whereas automotive safety protects against random failures in the produced automotive systems implemented into the automobile. The semantic meaning of the word "threat" is often overlooked and has been defined in numerous ways in today's literature. In this section, attacks or acts of malicious manipulations are defined as threats for the system. Such a threat involves:

- a threat agent; the attacker who utilizes different means (e.g. viruses, jamming equipment and rogue hardware to carry out an attack);
- the action (method) that the attacker takes against a system (target) by exploiting known weaknesses of the system (vulnerabilities);

3.3 AUTOMOTIVE-PLATFORM THREAT MODELING PROCESS

The Automotive-Platform Threat Modeling process is consists of the following six (6) steps:

1. Identification of the automotive platform threat model security objectives.
2. Decomposition of the automotive platform.
3. Listing of the major cyber-attacks and vulnerabilities.
4. Analysis of the targeted automotive attacks and vulnerabilities.
5. Identification of the threats (related to the CIA model) and the impact they cause to the ITS.
6. Identification of the vulnerable and insecure entry-points of the automotive platform.

3.3.1 THREAT MODELING OBJECTIVES

The objectives of the automotive platform of the previously presented threat model include activities for:

- a) identifying the cyber-threats of the automotive platform;
- b) identifying the impact of the ITS structure and entities interdependences;
- c) identifying the security design flaws and the vulnerable entry-points.

3.3.2 AUTOMOTIVE PLATFORM DECOMPOSITION

In previous section 1.6, the automobile boundaries within a traditional ICT stack were identified and the cyber nature of the ‘automotive platform’ was defined (Table 2). In this section, the decomposition of the automobile platform stack is of great value in order to define the vulnerable cyber-surface of the automotive platform and to proceed with the related cyber-attacks analysis. Most of the threats unleashed against the infrastructure layer of the automotive platform stem from the implemented hardware interfaces and from the peripheral components and control systems of the automobile. Therefore, the automotive platform interfaces of interest are those of network and communication, security, services, data and users. Data are not excluded from the decomposition analysis as they participate with different forms (e.g. signals, frames, packets, etc) in all of the interfaces of the automotive platform stack. Users are also included because no current automotive platform recognizes the cyber aspect of user profiling. Table 5 presents the automotive platform decomposition. Five interfaces are identified; their vulnerabilities on cyber-attacks will be analyzed in the following section.

TABLE 5: DECOMPOSITION ANALYSIS OF THE AUTOMOTIVE PLATFORM

| AUTOMOTIVE PLATFORM STACK | | | |
|---------------------------|--|--|---|
| TELECOM | Wired Networking | CAN – LIN – MOST- FLEXRAY – OBD – Other Interfaces | |
| | Wireless Communication | Short Range | Near Field Channels RFID (see Security Layer) Bluetooth WAVE12-802.11p DSRC13 (5.8-5.9 GHz) |
| | | Long Range | Satellite ¹⁴ (Radio, GPS) RDS ¹⁵ Cellular (3GPP) ¹⁶ |
| SECURITY MODULES | RFID - Immobilizer - RKES/PKES | | |
| SERVICES | Drivers, Firmware, Software, Applications ODB-Diagnostic Software Platform OS (infotainment Systems) | | |
| DATA | Signals, Frames, Packets, Data Information | | |
| USERS | Driver, Passenger, Cyber aspect of the driver is not defined | | |

¹² IEEE 802.11p standard adds Wireless Access in Vehicular Environments (WAVE). Wi-Fi refers to any interoperable implementations of the IEEE 802.11 Wireless LAN standards certified by the Wi-Fi Alliance.

¹³ The Dedicated Short Range Communications (DSRC) is either one or two-way communication channels specifically designed for automotive use.

¹⁴ a) Satellite radio is a radio service broadcast, from satellites primarily to automobiles, in a much wider geographical area than terrestrial radio stations, mostly commercial free. b) An automotive navigation system is a satellite navigation system (GPS) designed for specific use in automobiles.

¹⁵ Radio Data System (RDS) is a communications protocol standard for embedding small amounts of digital information (time, station identification and programme information) in conventional FM radio broadcasts.

¹⁶ 3GPP (GSM-2G, GPRS-2.5G, EDGE-2,75G, UMTS-3G, HSDPA/HSUPA-3.5G, LTE-4G, LTE-Advanced)

3.3.3 ATTACKS AND VULNERABILITIES

In this section, the security analysis of the automotive platform interfaces is performed based on the layered decomposition of Table 5. The first part of the security analysis presents the list of cyber-attacks that are able to compromise any of the above automotive platform interfaces and the second part presents the analysis of the attacks and the vulnerabilities of each interface of Table 5 separately. Table 6 describes an extended list of well-known cyber-attacks and of their vulnerabilities as they can be applied in any type of system threatening all kinds of hardware, software and other interfaces.

TABLE 6: CYBER-ATTACKS ANALYSIS OF THE 'AUTOMOTIVE PLATFORM'

| CYBER ATTACKS | DESCRIPTION | VULNERABILITIES |
|--|---|--|
| Malware Injection | <ul style="list-style-type: none"> ▪ Malicious software programs or software code (Virus, Trojan, Spam and Worm) that comes in different forms of hacking techniques, capable of deleting files, damaging or taking control of the system. ▪ They all run independently into systems though network connections and they can record the traffic of a region of the network and replay it into another region. | <ul style="list-style-type: none"> ▪ Missing updates, patches or service packs. ▪ Enabled unused functionality or default configuration settings including protocols, ports and services. ▪ Not limited, unregistered message traffic. ▪ Lack of digital message/packet signature. ▪ Lack of Kerberos/PKI-like or other authentication token system. ▪ Lack of anti-spam filtering. ▪ Lack of monitoring systems to identify unusual messages or traffic changes. |
| Eavesdropping Espionage | <ul style="list-style-type: none"> ▪ The attacker obtains a complete image of the network activity of sensitive/ confidential information (passwords, data) during a communication session. | <ul style="list-style-type: none"> ▪ Unencrypted transmission channel and data. |
| IP Spoofing | <ul style="list-style-type: none"> ▪ The attacker accesses the unauthorized wireless network with packet crafting in order to impersonate the authorization of that entity or network. | <ul style="list-style-type: none"> ▪ Weak access control mechanisms ▪ Weak authentication token system. |
| Denial of Service | <ul style="list-style-type: none"> ▪ The attacker sends messages or communication packets (flooding attack) to set a target-service unavailable. | <ul style="list-style-type: none"> ▪ Weak framework development. ▪ Software-hardware configuration faults and errors. ▪ Out of date security patches and updates. ▪ Weak firewall configuration and security policies. |
| Man in the Middle Attack | <ul style="list-style-type: none"> ▪ The attacker makes independent connections with the target-victim and relays messages impersonating each endpoint to the satisfaction of the other. | <ul style="list-style-type: none"> ▪ Weak mutual authentication. ▪ Lack of secure endpoints (active SSID). |
| Wireless Signal Jamming and Interference | <ul style="list-style-type: none"> ▪ Transmitted signals that disrupt communications by decreasing the signal to noise ratio. | <ul style="list-style-type: none"> ▪ Weak or lack of the frequency agility within mobile spectrum. ▪ Weak antenna for a signal generator. |

| | | |
|----------------------------------|--|--|
| Denial of Sleep | <ul style="list-style-type: none"> ▪ In some cases wireless networks do not use radio transmission. So in order to reduce power consumption, the network regulates the communication of that particular node. An attacker may drain the power supply of the sensor device in order to make a node's life short, or attack the MAC layer to reduce its sleep period. | <ul style="list-style-type: none"> ▪ Exploit MAC protocol weaknesses (if the number of drained nodes goes high, the whole network can be disrupted). ▪ Disruption of the wireless network session. |
| Collision and De-synchronization | <ul style="list-style-type: none"> ▪ The attacker tries to modify the control flags in order to forge the packets or the messages and the limit of the messages exchanged, causing an infinite cycle of retransmission that consumes a lot of energy. | <ul style="list-style-type: none"> ▪ Digital signature algorithms cannot sign a large amount of data efficiently; most implementations use a hash function to reduce ("compress") the amount of data that needs to be signed down to a constant size making them vulnerable to hash collisions. |
| Replay Attack | <ul style="list-style-type: none"> ▪ In this process, transmission data is repeated maliciously. An attacker intercepts the data in order to retransmit it further. It is part of masquerade attack which can be carried out by the substitution of an IP packet. A stream cipher attack can take place. Replay attack can exhaust the energy or power supply of a network. | <ul style="list-style-type: none"> ▪ Weak pseudo random session tokens. ▪ Lack of packet-filtering methods. ▪ Lack of timestamps to prevent unwanted synchronization. ▪ Not limited or unlimited time sessions and message traffic. ▪ Weak inspection of data traffic. ▪ Poorly designed applications can crash. |
| Forwarding Attack | <ul style="list-style-type: none"> ▪ The attacker may stop the node creating non-trusted routing information due to packet forwarding or message dropping to any wrong path within the network (aka gray-hole attack). Other examples of forwarding attacks include worm-hole (tunneling), sinkhole and unauthorized routing update attacks. | <ul style="list-style-type: none"> ▪ Not limited or unlimited message traffic and time sessions ▪ Weak inspection of data traffic. ▪ Weak pseudo random session tokens. ▪ Lack of packet-filtering methods. ▪ Any type of attack to penetrate the network, masquerade or modify the messages can be vulnerability. |
| Rogue of Access Points | <ul style="list-style-type: none"> ▪ A wireless access point that has either been installed on a network without explicit authorization from an authorized administrator or has been created to allow the attacker to conduct a MITM attack against the access point. | <ul style="list-style-type: none"> ▪ Lack of wireless intrusion prevention systems. ▪ Missing monitoring system of the radio spectrum for unauthorized access points. |
| Masquerade and Sybil Attack | <ul style="list-style-type: none"> ▪ The attacker impersonates in order to acquire a legitimate user's IP address or MAC address (masquerade) to modify information and/or privilege status. ▪ A Sybil attack is an advanced version of an impersonation attack in which the attacker may steal multiple identities. | <ul style="list-style-type: none"> ▪ Lack of timestamps to prevent synchronization/digital message and packet signature. ▪ Weak pseudo random session & authentication tokens. ▪ Lack of packet-filtering methods to identify unusual traffic changes and of access control ▪ Weak inspection/monitoring of data traffic. |

| | | |
|---|--|---|
| Reverse Social Engineering (RSE) | <ul style="list-style-type: none"> ▪ A term used for attackers tricking other entities into revealing some form of security information to gain system access. | <ul style="list-style-type: none"> ▪ Weak or sensitive code to reverse engineered or modified. ▪ Weak user names, passwords, network authentication, security policies, verification etc. |
| GNSS Spoofing GPS Tracking | <ul style="list-style-type: none"> ▪ Fake transmitted Global Navigation Satellite System-like (GNSS) signals, force the receiver to compute erroneous positions of another location aiming to reveal the geographic location of the automobile. | <ul style="list-style-type: none"> ▪ Lack of GNSS system monitoring and GNSS corrections to provide positional data. |
| Traffic Analysis | <ul style="list-style-type: none"> ▪ The attacker can intercept, monitor and analyze the packet transmission. | <ul style="list-style-type: none"> ▪ Eavesdropping, MITM, Replay, Masquerade attacks. |
| Software and Hardware Weaknesses | <ul style="list-style-type: none"> ▪ Control of privileges or installation errors that can be exploited for gaining software-based access to a system. | <ul style="list-style-type: none"> ▪ Lack of software updates and patches from official sources. ▪ Weak quality code, access control flaws in the software, poor installation procedures. ▪ Improperly secured wireless networks |
| Exploit Errors and Malfunctions | <ul style="list-style-type: none"> ▪ Exploit malfunctions, errors or inappropriate configuration or compatibility of the hardware or software. | <ul style="list-style-type: none"> ▪ Lack or weak hardware or software testing to prevent malware and ensure the security and the quality of the delivery. ▪ Lack of H/W and S/W updates. |
| Network Intrusion | <ul style="list-style-type: none"> ▪ In network intrusion, the attacker can corrupt, block or modify information and data on the network communication by sniffing, spoofing or eavesdropping. | <ul style="list-style-type: none"> ▪ Traffic analysis, exploit malfunctions and errors, GNSS spoofing, GPS tracking, signal jamming. |

The above cyber-attacks and vulnerabilities will be specified for all the layers of the automotives (as an ICT system).

3.3.4 TARGETED AUTOMOTIVE ATTACKS & VULNERABILIES

This section explores the vulnerabilities and the attacks that may occur in any of the five decomposed automotive platform in the five ICT layers presented in Table 5:

3.3.4.1. TELECOM: This layer includes the wired networking and the wireless communication.

3.3.4.1.1. Wired Networking

The automotive control units and the infotainment system implement advanced computing abilities and connectivity capabilities and they are responsible for the proper manipulation and storage of the automotive data. These functionalities make them vulnerable to cyber-threats. Based on Tables 5 and 6, an analysis of the hard-wired networking interface (Layer 1) threats and vulnerabilities¹⁷ will be listed and described.

¹⁷ Chp.3.2.3 threats and vulnerabilities survey found on References [4][6][7][11] & [21]-[29] & [40]

- i. CAN: The priority driven CSMA/CD access control method of CAN network enables attacks that jam the communication channel. Constantly introduced top-most priority nonsense messages will be forwarded always first, even though they will be immediately discarded by the receiving controllers. Thus they will permanently prevent the transmission of all other CAN messages. Moreover, utilizing the CAN mechanisms for automatic fault localization, malicious CAN frames may allow the disconnection of every single controller by posting several well-directed error flags.
- ii. LIN: Utilizing the dependency of the LIN slaves on their corresponding LIN master, attacking this single point of weakness is the main approach. Introducing well-directed malicious sleep frames deactivates completely the corresponding subnet until a wake-up frame posted by the higher-level CAN bus restores the correct state again. The LIN synchronization mechanism can be another point of attack. Sending frames with synchronization bytes within the SYNCH field may make the local LIN network inoperative or may cause serious malfunctions.
- iii. MOST: Since in a MOST network one MOST device handles the role of the timing master, which continuously sends timing frames that allow the timing slaves to synchronize, malicious timing frames are suitable may be used for to disturb or interrupt the MOST synchronization mechanism. Moreover, continuous channel requests reduce the remaining bandwidth to the minimum. Therefore, a feasible jamming attack on MOST buses is likely to occur. A manipulated false bandwidth statement for the synchronous and asynchronous area within the boundary descriptor of a MOST frame can also make the network completely inoperative. Due to the utilized CSMA/CD access control method used within the asynchronous and the control channel, both are vulnerable to jamming attacks similar to to the ones performed against CAN.
- iv. FlexRay: Similarly to the CAN automatic fault localization, FlexRay's procedures can be utilized for a well-directed deactivation of any controllers through the use of appropriately faked error messages. Attacks on the common time base, which would make the FlexRay network completely inoperative, are also feasible, if within one static communication cycle more than one malicious SYNC messages are posted into a FlexRay bus. Moreover, introducing well-directed sleep frames deactivates the corresponding power-saving capable FlexRay controllers.
- v. OBD-II Port: The most significant automotive interface is the OBD-II port which provides direct access to the automobile's primary CAN buses, which may be sufficient for an attacker to compromise the full range of automotive systems. The OBD-II port is common for both the diagnostics and the ECU programming. This access is achieved using

dedicated handheld “scan” tools programmed via OS-based operated terminals (usually Windows OS). For modern vehicles, most manufacturers have adopted an approach that is PC-centric. Under this model, a portable terminal interfaces with a pass-thru-device (typically directly via USB or Wi-Fi) that in turn is plugged into the vehicle OBD-II diagnostic port. Software on the portable device can then interrogate or program the car’s ECUs via this device (typically using the standard SAE J2534 API). In all these situations, the terminals directly or indirectly control the data to be sent to the automobile. Thus, if an adversary were able to compromise such systems it could amplify this access to attack any cars under service. In addition, electric vehicles may also communicate with external chargers via the charging cable. An adversary able to compromise the external charging infrastructure may thus be able to leverage that access to subsequently attack any connected automobile.

- vi. Other Interfaces¹⁸: Nowadays all automobiles provide a wide variety of a set of multimedia devices (e.g. USB, SD, SIM, and Disk) able to interpret different format data types, allowing users to control the infotainment system of the automotive platform. Compromising an infotainment system itself is a limited threat. Unfortunately, automotive infotainment systems are not standalone devices but they are CAN bus interconnected, either to directly interfacing with other automotive platform’s interfaces of (e.g., hands-free features, GPS display console) or simply to supporting is a common maintenance path for updating all automotive firmware. Thus, a compromised system can offer an effective vector for attacking other automotive components such as sensors, on-board control units, other software and applications or even the OS.

3.3.4.1.2. Wireless Communication

The major merit of wireless networking is to eliminate the big and untidy cables which add space, weight and cost. The major function of all wireless protocols implemented in an automobile is to establish connection with other ITS entities equipped with a transmitter and a receiver and to connect to the wireless network in order to exchange services, information and data using radio signals. All the signals have a unique set of information and network identification that the receiver detects before converting the radio signals into digital signals and vice-versa. Unfortunately, wireless networking comes with a high likelihood of attacks¹⁹, therefore automotive and network security is crucial to ensure the CIA model’s principles over the wireless communication interface of the automobile platform. In this section, two

¹⁸ Attacks related to the MAC layers are exploiting the Ranging Request-Response (RNG-REQ, RNG-RSP) messages in an initial network entry as a vulnerability to intercept the RNG-REQ and interrupt the RNG-RSP sequence.

¹⁹ There is a large number of wireless communications threats and vulnerabilities in numerous professional ICT research journals and magazines.

major attacks threatening the wireless communication interface are listed²⁰, namely signal jamming and wireless interference.

a) **Signal Jamming:** Along with the increasing use of satellite and mobile technology and their rising potential for privacy violations, signal jamming is listed as a major cyber-threat possible to compromise not only the automobile but also the entire ITS structure (impact). The basic purpose of a signal jammer is to prevent GPS loggers, passive tags and sensors from either receiving or transmitting signals back to the wireless network. Signal jamming is categorized into the four case:

- constant jammers that continuously emit noise;
- deceptive jammers that continuously broadcast fabricated messages or replay old ones;
- random jammers that alternate between periods of continuous jamming and inactivity;
- reactive jammers who jam only when transmission activity is detected.

b) **Wireless Interference:** Breaking into a wireless network requires no physical breach. Since a signal is broadcasted, the network interface is simply up for grasp, available for anyone to latch on. The use of direct-sequence spread spectrum (DSSS) technology is what modulates the radio frequency and disperses transmission over the entire frequency band designated for wireless communication, adding a redundant pattern to every bit transmitted, compromising both the short and the long range communications of the Wi-Fi and Bluetooth communication interfaces. Other sources of wireless interference can be the microwave interference, the damaged cable connectors, the signal or power leakage. The effects of wireless interference can be:

- a decrease in the wireless range between devices;
- a decrease in data throughput over Wi-Fi;
- intermittent or complete loss of the wireless connection;
- difficulty pairing during a Wi-Fi or Bluetooth device discovery phase.

i. **Short Range Communications:** Indirect physical access has several drawbacks including operational complexity, difficulties in precise targeting and inability to control the time of a compromise. If the operational requirements are weakened by the attacker, then the attack surface for automotive wireless interfaces that operate over short ranges (e.g. Bluetooth, RFID²¹, Wi-Fi of Emerging and Dedicated Short-Range Communications).

²⁰ Section.3.2.3 threats and vulnerabilities survey can be found on in [4][6][7][11] & [26]-[30] and [40]

²¹ RFID & RKES threats and vulnerabilities as found in References [31]-[37] & [40]

- ii. Long-range Communications: The long distance (greater than 1 km) digital access channels found in automobile are divided into two categories: broadcast channels and addressable channels.
- Broadcast channels: These channels can be “tuned into” by receivers-on-demand. This function may extend the automotive attack-surface as the modern automobile includes a plethora of broadcast receivers for long-range signals (e.g. GPS, Satellite Radio, Digital Radio and RDS) transmitted as digital subcarriers on existing FM-bands. As a result, the long-range broadcast media can be manipulated to become control channels (i.e., for triggering attacks) and to command multiple receivers at once without forcing the attacker to obtain the precise addressing of the cyber-target. Since, these channels are implemented in the infotainment system of the automotive platform which provides access via internal automotive networks (hard-wired or wireless communication interfaces) to other key automobile components (e.g. ECUs) they extend the cyber-attack surface of the automotive platform.
 - Addressable channels: The channels are used to expose a broad range of features remote telematics services of supporting safety (crash reporting), diagnostics (early alerts of mechanical issues), anti-theft (remote track and disable), and convenience (hands-free data access such to driving directions or weather) and they provide continuous connectivity via cellular voice and data networks. Unfortunately, these cellular channels offer many advantages to attackers as they can be accessed over an arbitrarily long distance (due to the wide coverage of cellular data infrastructure) in a largely anonymous way with a relatively high bandwidth.

3.3.4.2. SECURITY MODULES:

The security interface (3rd Layer) of the automotive platform consists of the immobilizer unit and the RKES (or PKES), which are both based in RFID (short range communication) technologies with embedded cryptographic procedures and access control mechanisms. Unfortunately, in a passive RFID tag the proprietary encryption keys used to transmit data between the key fob, the receiver, and the automobile engine are so poorly implemented, that they can easily become cracked. Most of the vehicles still use either a 40 or 48-bit key or the 128-bit AES, which are not considered by the security professionals as the minimum standards to protect an ICT-based system. The crack of the automotive platform is made possible because the proprietary algorithms that the firms use to encode the cryptographic keys shared between the immobilizer and the receiver, and the receiver and the engine, do not even match the security controls as found in ISO 27001 standards or other on related with the classified data encryption. Furthermore, in many cases the encryption key is very short causing a lack of security of the direct link.

3.3.4.2.1. Immobilizer Control Module

Three crucial works exist concerning the lack of security of the ICM:

- i. KeeLoq: KeeLoq is a block cipher used in wireless devices that unlocks the doors and the alarms in vehicles manufactured by Chrysler, Daewoo, Fiat, GM, Honda, Jaguar, Toyota, Volvo, Volkswagen and others. It was an inexpensive way to implement and provide DES-like security. The authentication protocol based on KeeLoq is a lightweight block cipher with a 32-bit block size and a 64-bit key used both in remote keyless entry systems and other wireless authentication applications. It has been shown that KeeLoq may suffer from their attacks that can be used to subvert the security of real systems, as the attacker can acquire chosen plaintexts. Moreover, one of the two suggested key derivation schemes for KeeLoq allows the recovery of the master secret from a single key. The KeeLoq encryption attack [31][32] is based on the slide attack and on a novel approach to meet-in-the-middle attacks with the same time complexity. Both attacks have been fully implemented and tested. When 16 key bits are given, a well-known plaintext attack completes successfully in almost ten minutes [31][32].
- ii. HiTag2: Hitag2, introduced in 1996, is currently the most widely used transponder in the car immobilizer industry. It is used by at least 34 car makers and it has been fit in more than 200 different car models. Hitag2 uses a proprietary stream cipher with 48-bit keys for authentication and confidentiality. Many keyless ignition or entry vehicles sold nowadays are still based on the Hitag2 cipher. In some keyless entry cars Hitag2 is also used as a backup mechanism for opening the doors, e.g., when the battery of the remote is depleted. Nevertheless, several weaknesses [33][34] have been revealed in the design of the cipher and three practical attacks have been presented that recover the secret key using only wireless communications. The most crucial attack recovers the secret key from a car in less than six minutes using ordinary hardware. This attack allows an adversary to bypass the cryptographic authentication, leaving only the mechanical key as a safeguard. This is even more sensitive on vehicles where the physical key has been entirely replaced by a keyless entry system based on Hitag2. During their experiments the secret key has been recovered and the engine of many vehicles from various automobile manufacturers has been started using their own transponder emulating device. These experiments also revealed several implementation weaknesses in the immobilizer units.
- iii. TI-DST: A similar immobilizer transponder is produced by Texas Instruments under the name Digital Signature Transponder (DST) protected by a different proprietary cryptographic algorithm that uses a secret key of only 40 bits. A reversed engineering [35][36] of the workings of these algorithms demonstrated that it is possible to relay in real-time the (encrypted) communication of several keyless entry systems. In some cases

such a communication can be intercepted over a distance of 100 meters when exploiting vulnerabilities in the following three practical attacks. The first attack they exploit the malleability of the cipher and the fact that the transponder does not have a pseudo-random number generator. The second attack is slower but the same attack strategy can be applied to other linear-feedback shift register (LFSR) based ciphers. The attack uses a time/memory tradeoff exploiting the linear properties of LFSR and generates the lookup table, reducing the complexity from 248 to 237 encryptions. This attack recovers the secret key regardless of the read protection configuration of the transponder. The third attack only requires only a few authentication attempts by the car immobilizer to recover the secret key (assuming that the adversary knows a valid transponder id). This cryptanalytic attack exploits dependencies between different sessions of the filter function used in the cipher. In order to execute this attack, an adversary first gathers 136 partial authentication attempts from the car. This can be done within one minute. Then, the adversary needs to perform 235 operations to recover the secret key. This takes less than five minutes on an ordinary laptop.

3.3.4.2.2. Keyless Entry and Ignition

Researchers have analyzed the security of RKES/PKES systems [35][36][37] and proved that they are vulnerable to three types of relay attacks:

- i. **Traditional Relay Attack:** In a relay attack, the attacker places one of the devices in the proximity of the key, and the other device in the proximity of the car. The attacker then relays messages between the car, enabling the car to be opened and started even if the key is physically far from the car. This corresponds to the scenario where the key is e.g., in the owner's pocket in the supermarket, and the vehicle is at the supermarket parking lot. The tested scenario revealed that the PKES systems are vulnerable to certain types of relay attacks, and they would attack allow the opening and starting of the vehicle while the true distance between the key and car remained large (tested up to 50 meters, non-line-of-sight). The achieved attack took place without physically compromising the key or raising any suspicion of the owner-user.
- ii. **Over the Cable Relay Attack:** In order to perform the relay attack over cable, a relay was used. That was composed of two loop antennas connected together with a cable that relays the LF signal between those two antennas. An optional amplifier can be placed in the middle to improve the signal power. When the loop antenna is placed close to the door handle, it captures the car beacon signal as a local magnetic field. This field excites the first antenna of the relay, which creates by induction an alternating signal at the output of the antenna. This electric signal is then transmitted over the coaxial cable and reaches the second antenna via an optional amplifier. The need for an amplifier depends on several parameters, such as the quality of the antennas, the length of the cable, the

strength of the original signal and the proximity of the relaying antenna from the vehicle's antenna. When the relayed signal reaches the second antenna of the cable it creates a current in the antenna which in turn generates a magnetic field in the proximity of the second antenna. Finally, this magnetic field excites the antenna of the key which demodulates the signal and recovers the original message. In all the passive keyless entry systems, this is sufficient to make the key sending the open or the start authorization message over the UHF channel. The message sent by the key will depend on what was originally sent by the vehicle. Then, the vehicle will send on the open command to the key from the outside antennas and the start command from the inside antennas. Therefore, the attacker (e.g., a car thief) first needs to present the relaying antenna in front of the door handle such that the key will send the open signal. Once the door is unlocked, the attacker brings the relaying antenna inside the vehicle and after he operates the brakes pedal or the start engine button the vehicle will send the start message to the key.

- iii. Over-The-Air Relay Attack: The over-the-air attack relays the LF signals from the vehicle over a purpose-built RF link with minimal delay. The link is composed of two parts, the emitter and the receiver. The emitter captures the LF signal and up-converts it to 2.5 GHz. The obtained 2.5 GHz signal is then amplified and transmitted over the air. The receiver part of the link receives this signal and down-converts it to obtain the original LF signal. This LF signal is then amplified again and sent to a loop LF antenna which reproduces the signal that was emitted by the vehicle in its integrity. The procedure for opening and starting the engine of the vehicle remains the same as in (ii). Using the concept of analog up and down conversion the attacker reaches larger transmission/reception relay distances, while at the same time the size, the power consumption and the cost of the attack is kept low.

3.3.4.3. SERVICE

Embedded software used to be low-level code written in C or assembly. Even a relatively straight-forward task like throttle control uses a sophisticated real-time OS (RTOS) and tens of thousands of lines of code [38][39]. With all this sophistication, standards and practices for design, coding, and testing become paramount when the function involved is safety-critical. Failure is not an option. There is a case where the unintended acceleration led to the loss of a human life. In that case a fault of the Engine Control Module's (ECM) firmware was found. That shows that if mirroring (where key data is written to redundant variables) is not always done, stack overflow may happen, as the stack-killing rules in the CPU code do not have a memory protection. The two key items that were not mirrored were the RTOS critical internal data structures and the final result of all this firmware, the `Target_Throttle_Angle` global variable. Although automotive testers and experts had performed a stack analysis,

developers had missed some of the calls made via a pointer, missed the stack usage by library and assembly functions (about 350 in total), and missed RTOS use during task switching. They also failed to perform run-time stack monitoring. In addition OSEC, a version of the automotive standard RTOS API was used, but the CPU vendor-supplied version was not certified compliant. An unintentional RTOS task shutdown was investigated too as a potential source of the incident. As single bits in memory control each task, corruption due to hardware or software faults will suspend needed tasks or start unwanted ones. Automotive vehicle tests confirmed that one particular dead task would result in the loss of throttle control, and that the driver might have to fully remove their foot from the brake during an unintended acceleration event before being able to end the unwanted acceleration. The conclusions were that:

- The electronic throttle control system (ETCS) source code was of low quality, defective and contained bugs, including bugs that can cause unintended acceleration (UA).
- Fail safes were defective and inadequate (referring to them as a “house of cards” safety architecture) and the code-quality metrics predicted the presence of additional bugs.
- Many other faults were found in the code, including buffer overflow, unsafe casting, and race conditions between tasks, inadequate and untracked peer code reviews and the absence of any bug-tracking system.

3.3.4.4. DATA

Signals and bits from sensors and actuators, bits and packets from ECUs, MCUs and automotive control systems, packets, segments and frames from the network interfaces, and data and information from the services, software and applications all together compose Data layer of the automotive platform stack. Thus, data are vulnerable to the entire list of cyber-attacks in all layers of the ‘automotive platform’.

3.3.4.5. USERS

As presented in Table 5, the user interface of the cyber layer of the automotive platform stack does not cover the case of user profiling neither the authentication of the driver or other user of the platform. The only authentication and authorization scenario-case existing in the automotive platform is the implemented mechanisms of the immobilizer and the PKES/RKES based on RFID wireless technology. However the authentication and authorization occurs between the component-control unit and the key-fob as it has been described in Section 1.4. The security interface or any other interface of the automotive platform stack does not authenticate the owner or any other user of the key-fob with the platform for an authorized access the ‘automotive platform’.

3.3.5 CYBER-ATTACKS ACTIVITY SUMMARY

In this section the cyber-attacks related to each layer of the automotive platform are presented in a tabular form. The summary table at the end of this section is an example of how to create a table score for further security investigation. Tables 7 and 8 present the attacks related to the wired network and the wireless communication interfaces of the automotive platform while Tables 9 and 10 present the attacks related to the security and the service interfaces of the automotive platform.

TABLE 7: WIRED NETWORK INTERFACE RELATED ATTACKS

| CYBER-ATTACKS | WIRED NETWORK INTERFACE |
|----------------------------------|--------------------------------|
| Malware Injection | ✓ |
| Eavesdropping Espionage | ✓ |
| IP Spoofing | — |
| Denial of Service | ✓ |
| MITM attack | — |
| Signal Jamming & Interference | — |
| Denial of Sleep | ✓ |
| Collision & De-synchronization | ✓ |
| Replay Attack | ✓ |
| Forwarding Attack | — |
| Rogue of Access Points | — |
| Masquerade & Sybil Attack | — |
| Reverse Social Engineering (RSE) | ✓ |
| GNSS Spoofing GPS Tracking | — |
| Traffic Analysis | ✓ |
| Software & Hardware Weaknesses | — |
| Exploit Errors & Malfunctions | ✓ |
| Network Intrusion | ✓ |

TABLE 8: WIRELESS COMMUNICATION INTERFACE RELATED ATTACKS

| CYBER-ATTACKS | WIRELESS COMMUNICATION INTERFACE |
|--|---|
| Malware Injection | ✓ |
| Eavesdropping Espionage | ✓ |
| IP Spoofing | ✓ |
| Denial of Service | ✓ |
| MITM attack | ✓ |
| Wireless Signal Jamming & Interference | ✓ |
| Denial of Sleep | — |
| Collision & De-synchronization | ✓ |
| Replay Attack | ✓ |
| Forwarding Attack | ✓ |
| Rogue of Access Points | ✓ |
| Masquerade & Sybil Attack | ✓ |
| Reverse Social Engineering (RSE) | ✓ |
| GNSS Spoofing GPS Tracking | ✓ |
| Traffic Analysis | ✓ |
| Software & Hardware Weaknesses | — |
| Exploit Errors & Malfunctions | ✓ |
| Network Intrusion | ✓ |

TABLE 9: SECURITY INTERFACE RELATED ATTACKS

| CYBER-ATTACKS | SECURITY MODULES INTERFACE |
|--|----------------------------|
| Malware Injection | — |
| Eavesdropping Espionage | ✓ |
| IP Spoofing | — |
| Denial of Service | ✓ |
| MITM attack | — |
| Wireless Signal Jamming & Interference | ✓ |
| Denial of Sleep | ✓ |
| Collision & De-synchronization | ✓ |
| Replay Attack | ✓ |
| Forwarding Attack | — |
| Rogue of Access Points | — |
| Masquerade & Sybil Attack | — |
| Reverse Social Engineering (RSE) | ✓ |
| GNSS Spoofing GPS Tracking | — |
| Traffic Analysis | — |
| Software & Hardware Weaknesses | — |
| Exploit Errors & Malfunctions | ✓ |
| Network Intrusion | — |

TABLE 10: SERVICE INTERFACE RELATED ATTACKS

| CYBER-ATTACKS | SERVICE INTERFACE |
|----------------------------------|-------------------|
| Malware Injection | ✓ |
| Eavesdropping Espionage | — |
| IP Spoofing | ✓ |
| Denial of Service | ✓ |
| MITM attack | ✓ |
| Signal Jamming | — |
| Denial of Sleep | — |
| Collision & De-synchronization | — |
| Replay Attack | — |
| Forwarding Attack | — |
| Rogue of Access Points | — |
| Masquerade & Sybil Attack | — |
| Reverse Social Engineering (RSE) | — |
| GNSS Spoofing GPS Tracking | — |
| Traffic Analysis | — |
| Software & Hardware Weaknesses | ✓ |
| Exploit Errors & Malfunctions | ✓ |
| Network Intrusion | — |

These tables present the cyber-attacks that can occur in every single interface-layer of the automotive platform stack. In order to summarize the attacks in a grading system of low, medium and high risk a Table 11 is generated.

Table 11 presents the activity summary of the previous individually presented attacks list (Table 6) related to the automotive platform interface.

TABLE 11: AUTOMOTIVE PLATFORM RELATED ATTACKS (ACTIVITY SUMMARY)

| CYBER ATTACKS | WIRED INTERFACE | WIRELESS INTERFACE | SECURITY INTERFACE | SERVICE INTERFACE |
|----------------------------------|-------------------|----------------------|------------------------|-------------------|
| Malware Injection | ✓ | ✓ | — | ✓ |
| Eavesdropping Espionage | ✓ | ✓ | ✓ | — |
| IP Spoofing | — | ✓ | — | ✓ |
| Denial of Service | ✓ | ✓ | ✓ | ✓ |
| MITM attack | — | ✓ | — | ✓ |
| Signal Jamming | — | ✓ | ✓ | — |
| Denial of Sleep | ✓ | — | ✓ | — |
| Collision & De-synchronization | — | ✓ | ✓ | — |
| Replay Attack | ✓ | ✓ | ✓ | — |
| Forwarding Attack | — | ✓ | — | — |
| Rogue of Access Points | — | ✓ | — | — |
| Masquerade & Sybil Attack | — | ✓ | — | — |
| Reverse Social Engineering (RSE) | ✓ | ✓ | ✓ | — |
| GNSS Spoofing GPS Tracking | — | ✓ | — | — |
| Traffic Analysis | ✓ | ✓ | — | — |
| Software & Hardware Weaknesses | — | — | — | ✓ |
| Exploit Errors & Malfunctions | ✓ | ✓ | ✓ | ✓ |
| Network Intrusion | ✓ | ✓ | — | — |
| Threat Model Score | 1=Low Risk | 2=Medium Risk | 3>=High Risk | |

In the bottom of Table 11, a simplified threat model scoring scale (grading) is included as an example for further research work on the security analysis (e.g. Risk Analysis); this grading system is currently out of the scope of this dissertation. In the next section, threats in the automotive platform will be identified and presented in a table and discussed in detail.

3.3.6 AUTOMOTIVE THREAT ANALYSIS

Any disruption of the CIA model and the authenticity principle related to the attacks against the automotive platform stack as presented in Table 11 can cause disastrous consequences to the security and safety of the automobile, the passengers, and the ITS structure. In this section, threats are described as the lack of the confidentiality, integrity, availability and authenticity principles caused by the cyber-attacks.

Threats that are identified must be seen in relation not only to the automotive platform stack but also to what affect can have in the environment of ITS. As already stated in the previous Sec. 3.2.4, the use of a grating system will assist in further research concerning the quantification of risk. However the scoring system can provide a clear justification for the protection of the interfaces and to discover the vulnerable entry-points and design flaws. This is also one of the final tasks of the threat modeling, to assess whether or not there are safeguards in place to provide adequate protection in the automotive platform stack. In cases

where no safeguards exist in place, it can be assumed that there are vulnerabilities in the automotive platform that need to be treated. In the following Table 12, the threats against the automotive platform are cited. The threats are expressed in terms of lack of the CIA model and the authenticity principle caused by the attacks.

TABLE 12: AUTOMOTIVE PLATFORM RELATED THREATS

| CYBER ATTACKS | THREATS (related to lack of) | | | |
|----------------------------------|------------------------------|-----------|--------------|--------------|
| | Confidentiality | Integrity | Availability | Authenticity |
| Malware Injection | — | ✓ | — | ✓ |
| Eavesdropping Espionage | ✓ | — | — | ✓ |
| IP Spoofing | — | ✓ | — | — |
| Denial of Service | — | — | ✓ | ✓ |
| MITM attack | ✓ | ✓ | — | ✓ |
| Signal Jamming | — | — | ✓ | ✓ |
| Denial of Sleep | — | — | ✓ | — |
| Collision & De-synchronization | — | ✓ | ✓ | — |
| Replay Attack | — | ✓ | ✓ | ✓ |
| Forwarding Attack | — | ✓ | ✓ | ✓ |
| Rogue of Access Points | — | — | — | ✓ |
| Masquerade & Sybil Attack | ✓ | ✓ | — | ✓ |
| Reverse Social Engineering (RSE) | ✓ | ✓ | ✓ | ✓ |
| GNSS Spoofing GPS Tracking | ✓ | — | — | — |
| Traffic Analysis | ✓ | — | — | ✓ |
| Software & Hardware Weaknesses | — | ✓ | ✓ | — |
| Exploit Errors & Malfunctions | — | ✓ | — | — |
| Network Intrusion | ✓ | — | ✓ | ✓ |
| Threat Model Score | 1=Low | 2=Medium | 3=>High | |

Furthermore, as already mentioned in Chapter 2, all the ITS activities in order to optimize their operations, routines and functions, and to provide a basis for sustainable development are increasingly relying the ICT. Due to the dynamic nature of ICT, ITS²² have extended their influence to the surroundings, including multiple transportation aspects (e.g. aviation, railway and maritime), interdependencies between the participating parties. Therefore any disruption or unavailability of their communication capabilities can have disastrous consequences to the entire transportation domain, including human lives. As a result, cyber security awareness must be raised before other emerging ICT concept (e.g. cloud²³, android²⁴) are implemented without proper guidance of safety and security and trust and privacy compliance. For these reasons the same cyber-attacks that affect the automotive platform stack causing threats to the platform and to the automobile must be studied also within the context of the ITS environment. In addition, because the automotive platform of the modern

²² Based on Homeland Security–Critical Infrastructures division, ITS can be also considered as part of the Transportation CI Domain,

²³ FORD's Sync AppLink with Amazon Cloud Player on iOS

²⁴ Open Automotive Alliance [Online] <http://www.openautoalliance.net>

automobile is an ITS-Station-based system (Section 2.5), the cyber-attacks may affect the roadside, central and personal Stations (subsystems). Therefore, the ITS-Station functional components of host, gateway, router, border router and interceptor (Section 2.3) which are included in each of the ITSC elements can also be targets of the cyber-attacks as shown in Table 6 affecting the entire ITS structure. Table 13 represents this relation of ITS targets and attacks.

TABLE 13: ITS RELATED CYBER-ATTACKS

| CYBER ATTACKS | ITS TARGETS | | | | | | | | |
|----------------------------------|---------------------|----------|---------|----------|-----------------------|---------|--------|---------------|-------------|
| | FUNCTIONAL ELEMENTS | | | | FUNCTIONAL COMPONENTS | | | | |
| | vehicle | roadside | central | personal | host | gateway | router | border router | interceptor |
| Malware Injection | ✓ | ✓ | ✓ | ✓ | ✓ | — | ✓ | — | ✓ |
| Eavesdropping Espionage | — | ✓ | ✓ | — | ✓ | ✓ | ✓ | ✓ | ✓ |
| IP Spoofing | — | ✓ | ✓ | — | — | ✓ | ✓ | ✓ | ✓ |
| Denial of Service | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| MITM attack | — | ✓ | ✓ | — | ✓ | ✓ | ✓ | ✓ | ✓ |
| Signal Jamming | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Denial of Sleep | ✓ | ✓ | — | — | ✓ | ✓ | ✓ | — | — |
| Collision & De-synchronization | ✓ | ✓ | ✓ | — | ✓ | ✓ | ✓ | ✓ | ✓ |
| Replay Attack | ✓ | ✓ | ✓ | ✓ | — | — | ✓ | ✓ | ✓ |
| Forwarding Attack | — | ✓ | ✓ | — | ✓ | ✓ | ✓ | ✓ | ✓ |
| Rogue of Access Points | ✓ | ✓ | ✓ | — | ✓ | ✓ | ✓ | ✓ | ✓ |
| Masquerade & Sybil Attack | ✓ | ✓ | ✓ | ✓ | ✓ | — | — | — | — |
| Reverse Social Engineering (RSE) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| GNSS Spoofing GPS Tracking | ✓ | — | — | — | ✓ | ✓ | ✓ | ✓ | ✓ |
| Traffic Analysis | — | — | ✓ | — | — | ✓ | ✓ | ✓ | ✓ |
| Software & Hardware Weaknesses | ✓ | ✓ | ✓ | ✓ | ✓ | — | ✓ | — | — |
| Exploit Errors & Malfunctions | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Network Intrusion | ✓ | ✓ | ✓ | ✓ | — | ✓ | ✓ | — | — |

Then if Tables 12 and 13 are combined the impact caused to the ITS domain can be analyzed as follows:

- Confidentiality in ITS is related to the following threats of eavesdropping, espionage, MITM attack, masquerade, sybil, RSE, GNSS spoofing, GPS tracking, traffic analysis and network intrusion attacks. More specifically:
 - The transaction data are threatened by eavesdropping, espionage, masquerade, sybil attacks and RSE.
 - The collection of location-based information is threatened by GNSS Spoofing, GPS tracking, network intrusion attacks and traffic analysis of the messages.
 - Data are threatened by eavesdropping, espionage and masquerade attacks via traffic analysis.

2. Integrity in ITS is related to the threats of malware injection, IP spoofing, MITM attack, collision and de-synchronization, forwarding, replay, masquerade and sybil attacks, RSE, software and hardware weaknesses and exploit errors and malfunctions. More specifically:
 - Unauthorized access to restricted information is caused by malware injection, IP spoofing, masquerade and sybil attacks and RSE.
 - Unauthorized access and manipulation to restricted information and loss of information is caused by MITM attack, collision and de-synchronization, forwarding and replay attacks).
 - Corruption or manipulation of information exchanged among ITS entities and communication layers is caused by RSE, software and hardware weaknesses, and exploit errors and malfunctions).
3. Availability in ITS is related with the following threats of denial of service, signal jamming, denial of sleep, collision and de-synchronization, replay and forwarding attacks, RSE, software and hardware weaknesses and network intrusion. All of the above may:
 - Artificially generate a high volume of false messages or affecting the exchanging capabilities of the ITS elements and components.
 - Accidentally generate a high volume of false I/O messages in cases of multi-hop broadcast messaging.
4. Authenticity in ITS is compromised due to the following threats of malware injection, eavesdropping, espionage, network intrusion, traffic analysis, replay attack, forwarding attack, rogue of access points, masquerade and sybil attacks, RSE, denial of service, MITM attack and signal jamming.

In this section, the threat model applied in the ‘automotive platform’ provided not only the threats of the automotive platform but also ITS related cyber-attacks. The final step of the threat model is to identify the vulnerable entry points and also the existing design flaws of the ‘automotive platform’.

3.4 AUTOMOTIVE PLATFORM VULNERABLE ENTRY-POINTS

In this section of this chapter, the vulnerable entry points (i.e. the vulnerabilities which may lead to the total loss of the automotive integrity, availability and control) and possible design flaws of the automotive platform stack are identified. Based on the summary activity of Table 12, the wired network and the wireless communication interfaces are the most vulnerable interfaces of all. When incorporating wireless technology into existing wired-based automotive networks, it is important to examine the automotive platform interfaces and determine what the hardware and software offers in the way of wireless compatibility and

security. For example, a centralized monitoring application would allow the management of the mixed network from one location (e.g. infotainment system) and strengthen the core of the automotive platform by implementing several layers of security defense to effectively block out the intruders while permitting access to authorized users.

Although no system will ever be 100% secure, wireless communications come with a possibility of attacks and they can be easily compromised by someone with some technical knowledge. Looking into the wireless network protocol architecture in Table 14, one notices that there is no inbuilt security beside the authentication and encryption mechanisms (Wireless Equivalent Privacy-WEP and Wi-Fi Protected Access-WPA) implemented on the top of the 802.11 protocol stack (Application Layer).

TABLE 14: ISO REFERENCE MODEL & 802.11 PROTOCOL STACK

| | | | | | | |
|----------------------------|----------------|-----------------|---|-------------------|--------------|---------------|
| OSI REFERENCE MODEL | 7.Application | | | | | |
| | 6.Presentation | | | | | |
| | 5.Session | | | | | |
| | 4.Transport | | | | | |
| | 3.Network | | | | | |
| | 2.Data Link | | 802.2 Logical Link Control (LLC) | | | |
| | 1.Physical | MAC | 802.3 | 802.4 | 802.5 | 802.11 |
| | PHY | Ethernet | Token Bus | Token Ring | WLAN | |

This is the main reason why wireless network signals can be effortlessly intercepted and tampered with, pointing out why both the wired network and the wireless communications interfaces of the ‘automotive platform’ stack are the most vulnerable entry points and the most valuable for attackers. In addition, if Table 13 is combined with Table 3 it is easy to understand why the entire ITS structure is endangered.

For the same reason, the security interface of the ‘automotive platform’ (the RFID-based mechanisms) is compromised. Furthermore, although the authentication principle although it is perfectly implemented between the RFID-based key-fob and the ICM (unit), it not occurring between the user of the key-fob (e.g. owner, driver, co-driver, passenger or other user), the key-fob, the ICM and the rest of the ‘automotive platform’. This is also the reason that in Tables 2 and 5, the user block is marked as null and it is not defined in the cyber layer of the automotive platform stack. The lack of user profiling may be considered as a vulnerable entry point and a major design flaw for an attacker to exploit. The OBD-II port and sensors are often exploited by the attackers, as they extend the attack surface of the automobile platform and the ITS. In these systems the attackers may exploit the lack of security and authentication policies, protocols and access control mechanisms of the communication of the mechatronic components. Furthermore the lack of any type of a module-based mutual authentication or security policy is extending the problem.

The unsecured software interface (component drivers, firmware, OS, applications and embedded services) are also entries with flaws for the attackers to exploit. In combination with the vulnerable network and communication interface or the easily penetrated OBD-II port, the attacker can alter and modify most of the unprotected and unencrypted data, or in other cases inject malicious data into the software, security and network and communication interface of the automotive platform. The threat analysis results pointed out that the vulnerable entry points of cyber-attacks and major security design flaws in the implemented interfaces of the automotive platform stack are more than expected and the need for implementing an embedded security is crucial.

3.5 CONCLUSIONS

This chapter presents the extended security analysis of all the layered interfaces of the 'automotive platform'. In addition, these automotive security efforts led to the creation of an asset-centric threat model. The threat model was designed to investigate the threats that stem from known cyber-attacks against the automobiles but also to imprint the impact caused to the ITS structure. The output results of the threat analysis pointed out the most vulnerable entry points that cyber-attacks target and the major design flaws in the implemented interfaces of the automotive platform. RFID-based automotive mechanisms, the OBD-II port and sensors and wireless and cellular technologies are some of the vulnerable interfaces that are shown to be prone to a large set of hacktivisms (attacks, hacks and cracks). All of the above interfaces introduce the automobile into the next trend of cyber targeted platforms, not only compromising the ITS structure but also putting human lives at stake. In the next chapter, a solution will be designed and presented in an effort to address most of the above security issues.

REFERENCES

- [1] E. Fok, An introduction to Cybersecurity Issues in Modern Transportation Systems, ITE Journal, vol. 83, 2013, pp. 18-21
- [2] M. Gercke, Cyber-Attacks Against Transportation Infrastructure, NATO Science for Peace and Security Series - E: Human and Societal Dynamics, Vol. 54, pp. 151 – 161
- [3] W. Jones, Cars: The next Victims of Cyber-attacks, IEEE spectrum, 2012, [Online] spectrum.ieee.org/
- [4] K. Gerhard-Haas, Hacker übernehmen das steuer, Technology Review Magazine, Interview of K. Dellios and C. Patsakis, pp. 46-49, 2012, [Online] www.heise.de/tr/artikel/
- [5] AUTOSEC [Online]: www.autosec.org/
- [6] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, Experimental Security Analysis of a Modern Automobile, IEEE Symposium on Security and Privacy, 2010
- [7] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, Comprehensive Experimental Security Analysis of a Modern Automobile, USENIX Security, 2011
- [8] US Department of Transport [Online] www.dot.gov/
- [9] US DoT RFI: Connected Vehicle-Next Stage Certification Environment, Solicitation Number: Connected_Vehicle_NextStage_Certification [Online] <https://www.fbo.gov/>
- [10] McAfee [Online] www.mcafee.com/
- [11] McAfee, Caution: Malware ahead, whitepaper, 2011, [Online] www.mcafee.com/us/resources/reports/
- [12] AUTOSAR [Online] www.autosar.org/
- [13] J. Leitch, Process Hollowing, Autosar, 2011
- [14] J. Leitch, IAT Hooking Revisited, Autosar, 2011
- [15] J. Leitch, Anti - Debugging With Exceptions, Autosar, 2011
- [16] J. Leitch, Improve Web Application Security With jQuery Mobile, Autosar, 2011
- [17] K. Dellios, D. Papanikas, Information Security Compliance over the Intelligent Transport Systems: Is IT Possible, IEEE Security & Privacy, 2014, (to be published)
- [18] ISO 26262 standard [Online] <http://www.iso.org/iso/>
- [19] Microsoft SDL Threat Model [Online] <http://www.microsoft.com/security/sdl/>
- [20] OWASP Mobile Security Project [Online] <https://www.owasp.org/>
- [21] T. Hoppe, S. Kiltz, and J. Dittmann. Security threats to automotive CAN networks – practical examples and selected short-term countermeasures. In M. D. Harrison and M.-A. Sujan, editors, SAFECOMP 2008, volume 5219 of LNCS, pages 235–248. Springer-Verlag, Sept. 2008.
- [22] T. Hoppe, J. Dittman, Sniffing/replay attacks on can buses: a simulated attack on the electric window lift classified using adapted cert taxonomy, workshop on embedded systems security 2007. pp. 66e72.
- [23] D.K. Nilsson, U.E. Larson, Simulated attacks on can buses: vehicle virus, Proceedings of the IASTED International conference on communication systems and networks (AsiaCSN) 2008, pp. 66-72.

- [24] J. J. Blum, A. Neiswender, and A. Eskandarian, Denial of Service Attacks on Inter-Vehicle Communication Networks, Proceedings of the 11th International IEEE Conference on Intelligent Transportation Systems, 2008, pp. 797-802.
- [25] C. Szilagy, P. Koopman, Flexible multicast authentication for time-triggered embedded control network applications in dependable systems networks, IEEE/IFIP International Conference on Dependable Systems Networks, 2009, pp. 165-174
- [26] F. Kargl, P. Papadimitratos, L. Buttyan, M. Müter, E. Schoch, B. Wiedersheim, T.-V. Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux. Secure vehicular communication systems: implementation, performance, and research challenges, IEEE Communications Magazine, 46(11):110–118, 2008.
- [27] A. Groll, C. Ruland, Secure and authentic communication on existing in-vehicle networks, Proceedings of the IEEE Intelligent vehicles symposium 2009. pp. 1093e7.
- [28] P. Kleberger, T. Olovsson, E. Jonsson, Security aspects of the in-vehicle network in the connected car, Proceedings of the IEEE Intelligent vehicles symposium 2011. pp. 528e33.
- [29] D. K. Nilsson, U. E. Larson, Efficient in-vehicle delayed data authentication based on compound message authentication codes, Proceedings of the 68th IEEE Vehicular Technology Conference, 2008, pp.1-5
- [30] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, I. Seskar, Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. USENIX Security Proceedings of the 19th USENIX conference on Security, ACM, 2010
- [31] S. Indesteege, N. Keller, O. Dunkelman, E. Biham, and B. Preneel. A practical attack on KeeLoq. In N. Smart, editor, Eurocrypt '08 , volume 4965 of LNCS, pages 1–18. Springer-Verlag, Apr. 2008.
- [32] T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, and M. Manzuri Shalmani. On the power of power analysis in the real world: A complete break of the KeeLoq code hopping scheme. In D. Wagner, editor, Crypto '08, volume 5157 of LNCS , pages 203–20. Springer-Verlag, Aug. 2008.
- [33] N.T. Courtois, S. O'Neil, J.J. Quisquater, Practical Algebraic Attacks on the Hitag2 Stream Cipher, Information Security, Springer Link, LNCS, vol. 5735, 2009, pp167-76
- [34] R. Verdult, F.D. Garcia, J. Balasch, Gone in 360 seconds: Hijacking with Hitag2, 21st USENIX security symposium proceedings, 2012
- [35] S. Bono, M. Green, A. Stubblefield, A. Juels, A. D. Rubin, and M. Szydlo. Security analysis of a cryptographically-enabled RFID device. In P. McDaniel, editor, USENIX Security 2005, pages 1–16. USENIX Association, 2005.
- [36] A. Francillon, B. Danev, and S. Capkun. Relay attacks on passive keyless entry and start systems in modern cars. In A. Perrig, editor, NDSS 2011. ISOC, Feb. 2011.
- [37] RFID Zapper [Online] [https://events.ccc.de/congress/2005/static/r/ff/i/RFID-Zapper\(EN\)_77f3.html](https://events.ccc.de/congress/2005/static/r/ff/i/RFID-Zapper(EN)_77f3.html)
- [38] R. Charette. This car runs on code. [Online] www.spectrum.ieee.org, Feb.2009.
- [39] Toyota's killer firmware: Bad design and its consequences Toyota killer, article [Online] <http://www.edn.com/design/automotive/4423428/Toyota-s-killer-firmware--Bad-design-and-its-consequences>
- [40] C. Patsakis, K. Dellios, Patching Vehicle Insecurity, Invited Talk - In-depth Security conference 2011 Europe (Deep-Sec), [Online] <http://www.youtube.com/watch?v=BA2J7O6cqzQ>
- [41] CISCO, Internet of Everything [Online]<http://www.cisco.com/web/about/ac79/innov/IoE.html>

4. THE MASC-PROTOCOL: REDEFINING THE AUTOMOTIVE PLATFORM SECURITY

Nowadays, any driver holding the key-fob of the automobile is considered as the authenticated and authorized “administrator” of the automotive platform. Such an adopted policy creates major security gaps especially in case where the attacker manages to physically access the automobile. Security issues are also found in cases where the intrusion needs to be traced as soon as possible in order to either back-track the automobile or to properly alarm and notify the legal authorities. For these reasons, in order to address the sources of the highlighted vulnerable entry points against cyber-attacks and exploitations presented in Chapter 3, a Module Authentication and Secure Components (MASC) protocol²⁵ is proposed. The rest of this chapter presents the motivation behind to design of the MASC-Protocol, the fundamental principles that are being used, the structure of the procedures and its evaluation.

4.1 MASC MOTIVATION

An emerging trend among automotive manufacturers is to implement wireless communications for real-time information exchange between the automotive platform’s modules and between vehicles and infrastructures. The integration of communications technology enabled a number of services for the participating units (vehicles, road-side, personal, base-station, or internal components), but also extended the surface of the automotive platform for cyber-attacks. Since the safety of the driver is depended on correct and proper mechatronic operations and functions it is of utmost importance that the automotive platform must be always protected against cyber-attacks.

Larson et al. presented their “approach to specification-based attack detection for in-vehicle networks” [1]. The researchers explored the applicability of a specification-based approach to detect cyber-attacks within the in-vehicle network, creating security specifications for communication and ECU behavior from the CANopen draft standard [2]. They concluded their research by proposing a suitable location for the attack detector to be placed, and evaluated the detection using a set of attack actions. Hoppe et al. presented their research work on “applying intrusion detection to automotive IT” [3]. Based on the increasing potential of the automotive infotainment systems and the capabilities of a human computer interface (HCI) they identified the intrusion detection approach as a promising supplemental measure for the automotive security. In addition, they investigated how an automotive intrusion detection system (IDS) could communicate security-related information to the

²⁵ A Protocol is a predefined set of procedural methods in the design and implementation of security and communication rules in fields of applied sciences.

driver. They proposed the adaptive dynamic concept to address the frequently changing environmental conditions of the automotive domain. Verendel et al. presented “their approach to using honey-pots in in-vehicle networks” [4]. The researchers discussed how to design an automotive honey-pot, how to gather data from attackers and how to process and analyze the gathered data and they highlighted important issues related to honey-pots implemented in vehicles. Through today’s availability of modern and highly efficient virtualization solutions, virtualization becomes extremely interesting also for embedded applications. Pelzl et al. presented their concept of “Virtualization technologies for cars” [5] and proposed several runtime environments in parallel but strictly isolated hardware. Their work presented possible advantages and implications as well as feasible fields of application and implementation examples for automotive vehicles. They introduced several concrete virtualization solutions and evaluated their feasibility in the vehicular area. The gap between automotive technology and applied information security has been mitigated by the EVITA FP7 funded Project [6]. The project was funded to “design, verify, and prototype an architecture for automotive on-board networks, where security-relevant components are protected against tampering and sensitive data are protected against compromise”. During the project a Hardware Security Module (HSM) of three “flavors” was designed, namely light, medium and full, depending on cost constraints, security, protection and functional requirements. Their proposed hardware architecture included different features that each flavor of the HSM supported. The deliverables of the project were a major contribution to the state of the art. They provided a real-world implementation of an architecture, in which all the traffic could be encrypted. AES, RSA and ECC-256 were selected for encryption, while WHIRLPOOL was selected for hashing. The developed architecture was designed to be compliant with previous AUTOSAR framework, version 3.0.

Unfortunately, the above presented works present novel automotive implementations but they have not been tested in real-time, dynamically adaptive transportation environments of high mobility besides EVITA Project. The implementation of intrusion detection and prevention systems or of virtualization techniques in the automotive systems is time and energy consuming due to the mechatronic nature of the ‘automotive platform’. They are not viable solutions because of the multiple and complex constraints that are inherent in the embedded automotive systems include. In addition, in EVITA there was no provision for stream ciphers, but only for different modes of operation of AES-128. What is crucial to notice here is the lack of support for certificates for the automotive platform components’ communication, since neither hashing algorithms, nor public key encryption is supported in medium and light HSM. This means that a symmetric key authentication protocol has to be used for authentication, requiring a trusted third party inside the vehicle. The existence of one Trusted Third Party (TTP) policy without certificates is something that cannot be considered secure. In many attack scenarios one might try to change the TTP to reboot the

automotive platform with new keys, freshly created by the attacker and the automotive platform's modules will trust these fresh created credentials. Moreover, all the used components have to be signed by the vehicle manufacturer, creating many problems related to vehicle maintenance and original or after-market product support.

When designing secure protocols, it has to be taken into account that the automotive platform of an automobile is an embedded real-time adaptive mechatronic [14] system which is controlled by the driver|user in real time. With more than 2000 decisions per second to be taken and the time to react in a cyber-attack scenario is less than a second, any of the above presented proposed solutions is more than limited and the users-operators-passengers' lives may be endangered. Nobody wants their automobiles while their engines are running to buffer overflow or run-out of memory, or by design flaw "log out" the user and reboot the system. All these implications for the real time embedded systems set these ICTs solutions too difficult to support. In addition, they affect the already well-structured architecture of the automotive data buses, setting their implementation at this time not fully feasible. A data bus provides numerous physical and logical configurations for the automotive architecture, data units/packets, protocols, message traffic, and so forth. This allows considerable design flexibility for system designers, but it can make it extremely difficult to establish and maintain a certain type of design. The multitude of embedded controllers and communications equipment found on an automotive platform need to communicate with each other to collect data, pass commands, and health-monitoring status. The increased amount of information shared on the data buses within and between systems and subsystems, with many of the shared parameters being vital for the operation of the automobile, asks for automotive networks with high throughput, availability, and reliability. The throughput, however, always comes second to the need for reliability. In the automotive industry and the vehicles in general, there are unidirectional and bidirectional data bus architectures supported by protocols. However, they require labor-intensive wirings, which are also expensive and heavy, require higher power consumption and lead to high operational costs. This motivates the replacement of point-to-point wiring and unidirectional data buses, as they do not seem adequate for the majority of the future automotive systems and applications, with faster and lighter bidirectional data buses. Additionally, the cost pressure for development and operation is constantly rising and calling for the reusability of software and hardware components, network and communication interfaces.

In addition as already presented in the previous chapter, the only existing automotive security policy found in the automotive platform, is the one lying between the immobilizer module and the EMS, functioning as an accept-to-anything (Accept2X) policy towards the rest of the automotive modules. The instant moment that the immobilizer is triggered, the ignition of the motor-engine and simultaneously the initialization and the module check in

the automotive platform²⁶ take place. As a result, the immobilizer and the key-fob are authenticated to each other, “releasing” the rest of the modules’ authorization to enable their functions. Therefore, not only user authorization and authenticity are bypassed and do not take place in the entire security process, but neither the driver, nor the key-fob, nor the components are being mutually authenticated with a trusted entity of the automobile platform. In addition, there is little available open knowledge concerning the automotive technology and how the automobile actually function, because the entire automotive industry is a closed environment due to patents. The result is that the security researchers can use only experience-based and literature-based knowledge to working with. Furthermore, if the previously presented proposals are investigated in depth, the following may be identified:

- a) they assume how the ‘automotive platform’ and components should work so their proposed security solutions fits in the vehicle;
- b) they target their proposed security solutions without presenting a detailed composition or decomposition of the automotive architecture design;
- c) they miss and neglect the Mechatronic²⁷ perception of the automotive platform for the security problems they try to address.

As already stated, setting the PKES/RKES and the immobilizer systems as the sole entities for authentication and authorization of the all other critical systems and as the only protection mechanisms against unauthorized cyber-physical entry and ignition of the automobile is not considered a secure good-practice. In addition, it has become evident that the authentication between the immobilizer unit and the key-fob cannot be considered a sufficient security mechanism capable of covering the range of cyber threats that the automotive platforms are exposed to. It is vital to redefine the role of the security interface of the automotive platform stack, taking into consideration the following questions as well:

- How drivers and accessories are authenticating to the vehicle?
- What rights/privileges has an authenticated user?
- What rights/privileges has an authenticated accessory-subsystem?

Due to the fact that many of the aforementioned vulnerabilities are the result of inefficient security policies (e.g. the immobilizer) regarding the access levels of the participating peripheral components of the automotive network and of the communication interfaces, many outsourced hardware components can be easily plugged-in and become authenticated immediately. For these reasons, the proposed solution must be able to:

- Enforce the mutual authentication of the entire automobile control modules.

²⁶ This action-function is known as the “check-engine” process

²⁷ Mechatronics is the synergistic combination of precision mechanical engineering, electronic control and systems thinking in the design of systems, devices and products aimed at achieving an optimal balance between basic mechanical structure and its overall control. Practical developments in mechatronics application areas include not only the consumer product design, instrumentation and manufacturing methods but also computer integration, process and device control for both the industrial and academic research spectrum.

- Block plug 'n' play attacks undertaking the role of an Intrusion Prevention System.
- Detect attacks that originate from:
 - arbitrary access of the ECUs;
 - a lack of discrete user roles and access rights;
 - the attached devices.
- Provide an additional layer to the communication and security interface.

Driven by this motivation, redefining and securing the vulnerable automotive platform interfaces, as previously presented, a hybrid protocol implementing a series of security and communications task sets is proposed in the following section, in order to:

- detect and prevent cyber-attacks;
- trigger adequate alarms against detected threats;
- introduce the mutual authentication of the automotive components;
- create users with different access rights and roles (user profiling).

4.2 MASC CONTRIBUTION

In order to generate a safe environment related to the design of the distributed embedded systems, novel event-triggered and time-triggered sets of procedures that are able to securely communicate over the heterogeneous bus protocols consisting of both static and dynamic phases, must be defined. Nevertheless, the redefinition of the automotive platform interfaces instead of the redesign of the entire stack is not an easy task to accomplish. All of the so far proposed security systems need a considerable time for data process and even more time for data analysis. Therefore, even with the latest generation of multi-core processors it will be very hard to support these systems. The two basic approaches for handling tasks in real-time systems of cyber-physical, embedded and mechatronic nature [14] are the event-triggered and time-triggered (TT) approaches. However, there has been a long debate [7][8] and several views in the real-time and embedded systems communities concerning the advantages of each approach and which one to prefer based on flexibility, predictability, jitter control, processor utilization, testability, etc. This same duality is reflected at the layered interfaces of the automotive platform where communication activities of the services can be triggered either dynamically, in response to an event (e.g. CAN bus), or statically at predetermined moments in time (e.g. TTP²⁸ or TDMA²⁹ protocols). But in the case of the embedded automotive security systems, strict time requirements must be satisfied, therefore they are implemented as distributed systems where the predictability of the task and the timing behavior are important aspects. In order to guarantee the predictability for both communication and security interfaces between the various components and modules of the automotive platform, task scheduling has been proposed [9]. Task scheduling takes into

²⁸ TTP: Time Triggered Protocol

²⁹ TDMA: Time Division Multiple Access

consideration both event-triggered and time-triggered tasks in distributed real-time systems similar to the automotive platform. It is based on the generic TDMA protocol [10] allowing dynamic task offsets for tighter bounds in task response times and considering particular communication protocols, like the CAN bus [11], or the TTP bus.

The Mutual-Authenticated and Secured Components (MASC) Protocol introduces a series of novel embedded security and communications set of procedures in a bus protocol backplane. MASC's scope are:

- to redefine the role and use of the immobilizer unit into a module capable of hosting the protocol procedures and to mutually authenticate all the other modules toward itself and to the authorized user profile;
- to be modeled in a high level of abstraction in both the communication and security interfaces of the automotive platform.

More specifically, for the efficient implementation of the security and communication task sets, MASC entails both Time-Triggered (TT) and Even-Triggered (ET) task sets, implemented on top of the communication and the immobilizer module interface of the automotive platform stack, acting as a dynamically mixed event-triggered security and time-triggered communication protocol. Such an approach, has the potential of a highly efficient, fine-tuned, and flexibly optimized implementation of a communication protocol, that will meet the timing and event constraints of the high demanding mechatronic interface of the automobile. In addition, because of the fact that the automotive industry has adopted an "Accept2X" policy for the automobile "boot" as a substitute authorization policy and process, all the recently recorded cyber-attacks against the automotive platform prove that there is a great need for adopting a reverse security strategy, technique and policy. Reverse engineering³⁰ is defined as the process of discovering the basic technological principles of a device, object, or system through the analysis of its structure, functions, and operations [12][13]. The analysis of a system based on reverse-engineering often involves disassembling a mechanical device, electronic component or computer program and analyzing in detail its variants and variables for maintenance, update, reconfiguration or creation of a replica-system that has the same capabilities, without duplicating the original and with little or no additional knowledge about the procedures involved. The same philosophy was used in the first chapter where the automotive architecture design chain and the composition of the automotive platform stack were presented.

Based on the reverse-engineering security philosophy, a "Deny2X" policy will be designed versus the existing "Accept2X" policy, resulting to:

³⁰ Reverse engineering has its origins in the analysis of hardware for commercial or military advantage

- a) the minimize to the maximum of the known cyber threats against the 'automotive platform' and the incorporation of novel security features;
- b) the redefinition of the security interface without affecting the originally builds automotive platform stack and the safety-levels offered to the user-driver and to the passengers.

MASC is targeted towards the automotive component controls as the complexity of the overall system grows and requires higher levels of safety, reliability, availability and security but it also implements the adopted "Deny2X" policy toward the automotive modules. In the following section the fundamental principles of MASC [15][16][17] are described in detail.

4.3 THE FUNDAMENTAL PRINCIPLES OF MASC

The MASC architecture integrates the heart of the time-triggered architecture which is the generic distributed platform for highly dependable real-time systems in the transport industry applications. The time-triggered protocols are also used in mission critical data communications applications such as in aircraft engine management and in other aerospace applications where the deterministic operation is the ultimate requirement. Time Triggered protocols also enable the implementation of effective consistency services and error detection mechanisms to provide a maximum degree of fault tolerance dependent on the network topology, the safety and the availability of the network used.

4.3.1 THE COMMUNICATION CHANNELS OF MASC

The reason for using the time-triggered basis is to design MASC as a fault-tolerant protocol that provides autonomous fault-tolerant message transport at known times and with minimal jitter due to the embedded TDMA communication channels. In addition, in automotive applications the networks must be able to operate separately with separate hardware interfaces but with coordinated configurations. This means that event-triggered messages must be supported and sent via the same communication channels.

A. Event Triggered Communication:

The transmission of event-triggered messages is performed over an event channel. Bandwidth is reserved for event transmissions inside the TDMA slots and the messages use identifiers. A typical event channel mechanism is the CAN emulation, in which a CAN-compatible interface is provided and the CAN messages are transmitted inside time-triggered data frames. The modularity of MASC is maintained when using event transmission between different nodes but only between different functions within a node. Therefore, timing and bandwidth analysis for event transmissions is done on a per-node basis and does not need system-level design.

B. Time Triggered Communication:

MASC as being a time-triggered-backplane protocol can be implemented in a bus or star topology with controllers as bus interface units. The bus topology uses a broadcast bus where all the nodes are electrically connected to each other. The star topology has all the nodes connected to each of the replicated channels of the interconnection network via bidirectional links. In the bus topology, each node is equipped with a local bus guardian; in the star topology two redundant central bus guardians (CBG) are implemented. A central bus guardian is a unit that acts as a failure mode converter to protect the communication channels from temporal transmission errors. Media access and data communication is organized in rounds controlled by a conflict-free Time Division Multiple Access (TDMA) strategy. A TDMA round is divided into slots. Every node is assigned to a sending slot in a TDMA round and it must send frames in every round. The frame size allocated to a node can vary from 2 to 240 bytes in length, each frame usually carrying several messages. The cluster cycle is a recurring sequence of TDMA rounds; in different rounds different messages can be transmitted in the frames, but in each cluster cycle the complete set of state messages is repeated. The data is protected by a 24-bit CRC (Cyclic Redundancy Check). The schedule is stored in the default MEDL (Message Descriptor List) within the communication controller. Additional slots can be defined for nodes to be added later. Every MASC controller contains the dispatching MEDL table that contains the information about which node is allowed to send which message at a particular point in time. The MEDLs of a cluster are constructed before run time and are common knowledge to all the nodes. In addition, each controller contains two replicated communication channels in order that the loss of one channel can be tolerated, as it can also operate only on one channel.

4.3.2 MASC-PROTOCOL FEATURES

MASC implements features of both a security and a communication protocol. It is an embedded rule engine for securing data exchange within or between the modules. Each message has a precise meaning intended to elicit a response from a range of possible responses pre-determined for a particular function. Nevertheless, MASC's behavior is independent of how it is to be implemented (as hardware, software or both).

A. Communication Features:

All the communications protocols have to be agreed upon by the parties involved and to reach an agreement. Similarly MASC is a communication rule engine that describes the only way in which modules can be accessed by other modules including:

- the messages that are understood by the entities;
- the arguments that these messages may be supplied with;
- the output results that these messages return;
- the invariants that are preserved despite modifications to the state of a module;
- the exceptional situations that will be required to be handled by the modules.

B. Security Features:

The security features of MASC are a set of security-related procedures, acting as rules with applied cryptographic methods and sequences and describing how to be used. They undertake the role of the security policies. The MASC security policies that will be used for securing the data transport must incorporate at least one of these aspects:

- key agreement or establishment;
- entity authentication;
- message authentication construction;
- secured data transport;
- sharing method.

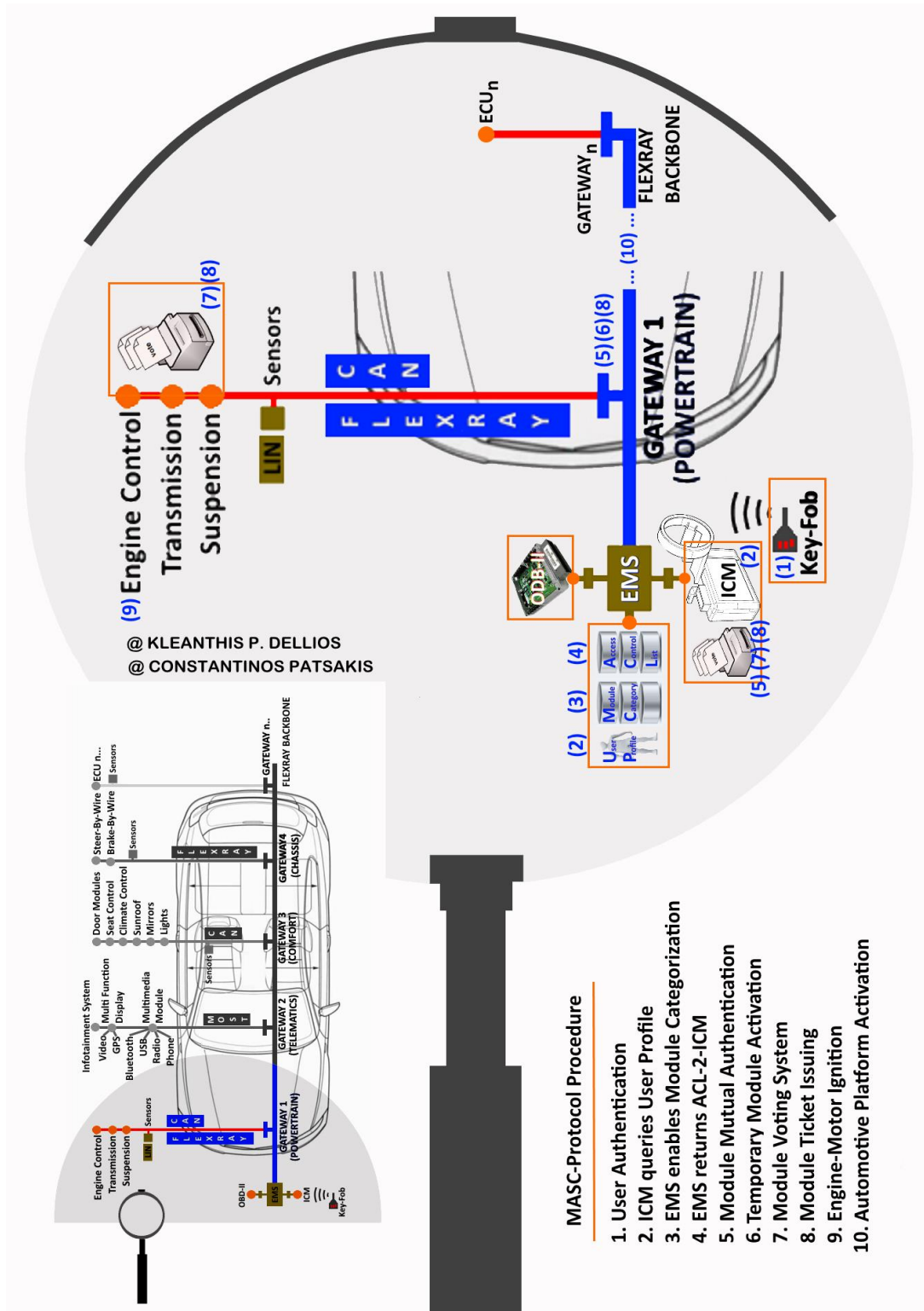
C. MASC Overview

The main goal of our proposal is to create an embedded infrastructure that is closer to computer security systems than the existing one. For this reason, we block unauthenticated devices, as we would in computer systems. For example, an attempt to install an unsigned driver triggers alerts in a modern operating system. Moreover, only users with proper privileges are allowed to install new modules on the automotive platform. Currently, any user is considered as an “administrator” as long as he has a key, which creates a big security gap that needs to be filled with the development of processes which the block engine’s ignition if a malicious activity has been detected. Finally, in the cases where an attacker manages to access the vehicle, we want to enable as many traces of his acts as possible during his attempt to steal or tamper it. This will either allow the vehicle’s backtracking or trigger proper alarms to legal authorities. The overview of the MASC procedure steps are illustrated in Figure 3 and enumerated in the following list:

1. Firstly, the user is being authenticated to the immobilizer unit. The redefined role of the immobilizer unit is to interact instantly with the EMS that hosts the Module Categorization the user profiling and the Access Control List (ACL).
2. The immobilizer queries the local database to find whether the user has access rights (user profile).
3. All of the automotive platform’s modules are connected to the ECM as shown in Chapter 1, Figure 1. ECM manages which modules are powered and controlled by the immobilizer (module categorization table) and enables the Module Categorization
4. ECM returns the ACL, dictating to the immobilizer which modules can be accessed. Therefore, if the immobilizer decides that a random module (module_n) should not receive any power, the power source is cut off by the ECM. If it is independently-powered, then the ECM will drop the packets and will block the packet traffic to and from that module_n. The Immobilizer Unit is aware of the

automotive platform's network topology (e.g. where the parts are located, which parts can communicate with which, where the available entry points are for external devices) as this information is included in the ECM mapping. The redefined of ECM is to act as a proactive hardware-based firewall of the Immobilizer, hosting most of the MASC procedures (rules and exceptions).

FIGURE 3: MASC OVERVIEW



5. The procedure of the Module Mutual Authentication (MMA) occurs.
6. The modules that are mutually authenticated with the Immobilizer are temporarily activated.
7. The Module Voting System (MVS) procedure of MASC begins.
8. The Module Ticket Issuing (MTI) procedure of MASC is completed
9. The motor engine ignition occurs if the MVS procedure is completed and all the modules are secure to operate their functions.
10. The automotive platform is fully activated and controlled by the authorized administrator, based on User Profiling and ACL.

D. MASC's Key Attributes:

- Family of fault tolerant TDMA-based protocols.
- Security Patch and Communication features update
- Mutually Authenticated Modules
- High speed control units for real-time control
- Real-time communication protocol for the secure interconnection of modules in distributed real-time fault tolerant systems.
- Onboard Diagnostic level 2 support
- Bit rates: currently available TTP controllers support up to 25 Mbit/s synchronous and up to 5 Mbit/s asynchronous transmissions. The upper range is not limited by TTP itself and it can be extended with new implementations of the TTP communication controller.
- Topology: dual channel linear bus and star topology or mixed
- Media: copper and optical fiber
- Number of nodes: up to 64 nodes
- User Profiling: The electronics and electro-mechanics ('Mechatronics') replace hydraulic and mechanical components in the modern automobiles. The role of the driver changes from machine operator to supervisor of the transportation system-automotive platform
- Support X-by-Wire Systems: Mechanical and hydraulic subsystems controlling safety-related functions are replaced by computer control systems.
- Fault tolerance: no single fault may lead to a system failure
- Predictable and timely system behavior (scheduling)
- Synchronized time base (global time)
- Cost reduction, embedded design, assembly and maintenance, security, design compatibility
- Support and compatible to future EVs and hybrids

4.4 MASC-PROTOCOL POLICY MODULES

As it has already been discussed, in order to stop many of the aforementioned cyber-attacks against the automotive platform stack, strict security policies need to be enforced. In MASC, three policy modules are implemented that define the access rights of modules and users based on credentials and on time constraints; the module categorization, the user profiling and the Access Control List (ACL).

4.4.1 MODULE CATEGORIZATION IN MASC

Currently existing automotive platforms have, in IT terms, an “Accept all” policy towards almost all of their modules. Only the immobilizer and the Key-Fob are authenticated, but no other security policy is applied or exists for the other modules of the automotive platform [18]. In addition, since in many cases the installation of new components is used to manipulate and bypass the immobilizer system, enforcing a security policy as a set of rules and to define the access rights of modules and users based on credential, time or even geo-location constraints retrieved from the GPS will stop many of the cyber-attacks. Therefore, the adoption of a “Deny all” policy towards all the mechanical and the peripheral modules is crucial in providing new security features, in decreasing the number of the compromised or eventually stolen automobiles and in maintaining current status of the ‘automotive platform’ functionality. Another reason for implementing module categorization is because the automotive platform has a plethora of modules, each focusing on a different exclusive task. If a module is not properly managed, the safety features of the automobile, the driver and the passengers may be endangered. The proposed module categorization is based on the network topology of the automotive peripheral components separating them into Primary and Secondary modules. A paradigm of a brief categorization of the automotive parts and components in primary and secondary modules may include:

1. Primary Modules: Motor Engine and Gear Box, Steering and Braking systems, Child Safety Block and Airbags, Lights and Handbrake which enable the functionality and the security of the vehicle.
2. Secondary Modules: Air-Condition/Climatronic, Infotainment System, Sunroof, e-mirrors, Heated Seats, Parking Systems.

If a malfunction or a possible attack is discovered in a Secondary module, the overall operation of the automobile must not be affected and the mechanical usability should not be suspended but the secondary module must be deactivated and any packet from it must be blocked. In this context, a false authentication is also considered as a malfunction. Up till now, an automobile’s engine ignition is not allowed if there is a mechanical problem detected for security reasons related to the passengers’ lives. Therefore, taking into consideration passengers’ security, in case a Primary module has not been authenticated, meaning that either it is malfunctioning or it has been tampered, the automotive platform should not be

“booted” at all and the engine ignition should not be allowed either. The module categorization in Primary and Secondary is not new as similar categorizations have been applied for decades in ECU management but each manufacturer has adopted different automotive network architecture of the systems, setting the security interaction between modules difficult to establish. A globally redefined module categorization of the systems regardless of the automotive network architecture of each manufacturer adopts for the purposes of automotive security could simply overcome this problem. For more details regarding how automobiles manage functionality over the malfunctioning parts based on such categorizations, the interested reader may refer to [18][19][20][21].

4.4.2 USER PROFILING IN MASC

User Authentication can be achieved by several methods, depending on the manufacturer, ranging from biometrics to common keys or e-keys. The proposed User Profiling is a type of categorization that goes beyond offering advanced infotainment experience or simple preferences. It is a built-in database of multiple user profiling linked with the entire automotive platform stack (e.g. driver, vehicle technicians/ mechanics, parental control for children/elderly person, guest). Each user-profile will be able to provide passengers of an automobile with a different setup and use of the vehicle. The importance of user-profiling can be clarified by the following profiling:

- A technician/mechanic cannot drive the car for more than 20 km and should have limited top-speed.
- Parental control may allow a young/new driver to use the car in a certain radius away from home or restrict the use of the vehicle in certain areas (limited speed can be adopted too).
- A driver is allowed to use the car in pre-assigned routes or emergency buildings, such as in hospitals, police departments etc.
- Infotainment functionality like mp3 player, GPS, A/C is enabled only by for certain groups of users.

The goal of the user authentication over a build-in database for user profiling is to provide different access levels to all possible users of the automotive platform. Such a capability is applied and exists in almost any modern operating system nowadays. By applying constraints in a software platform, fine-grained policies can be enforced to control any possible information and data leakage, while any arbitrary automotive usage is eliminated. Unfortunately, in the automotive platform the same policy does not exist or applied As a result, everyone who simply holds the key-fob is immediately the administrator/root of the entire automobile. On the other hand, with user-profiling each user can be equipped with an access control list to the platform’s modules and be authenticated for authorized use (either for the automobile or to gain access into the ITS environment) every time the vehicle is being

initiated. Extending these policies to all the modules, a privilege escalation from attacks that exploit specific module vulnerabilities, can be prevented. When applying different access levels to users, malicious attempts to use the platform can be traced back to their source. For example, if a mechanic has kept a copy of the car keys that he was assigned to repair, then if he tries to drive the car or change a part of the car beyond a specific timeframe, several alerts will be triggered, making his attempts known. Given that the platform recognizes the rights of the key holder, the redefined role of the immobilizer can deduce who is trying to violate the platform. The same example can be extended to parental control scenarios or to lending/renting automobiles. Of course, one could argue that policies like user-profiling may create ethical and social issues in cases where emerging use of the car is needed (e.g. accident, health incident). A typical example is that of someone getting wounded and having to be transferred to the hospital by a relative who does not have the proper privileges to drive the car in a specific region due to parental control. While, the scenario is very realistic, there can be sophisticated solutions which allow drivers to predetermined emergency routes (using GPS/GPRS), or more practical ones, such as using somebody else's keys to bypass the security, if the credentials are not biometric. To address such problems instead of using simple forms of user authentication in user-profiling, other approaches can be selected to provide an "escape mode" in cases of emergencies, such as the Risk-Adaptable Access Control (RAAdAC) [22] or the RBAC model [23]. However, these solutions although they may enable the desired functionality, they also open up a new back-door for attackers to simulate an emergency event and take control of the car.

4.4.3 ACCESS CONTROL LIST IN MASC

The role of Access Control List (ACL) is a crucial component and a vital ingredient of MASC as they can provide one more line of defense against several cyber-attacks and threats. As discussed before, many attackers exploit vulnerabilities found in the automotive infotainment systems and use them to gain full access to the platform. However, if each module has a personalized ACL when accessing other modules, a privilege escalation of this type can be minimized. Generating and providing ACLs from the immobilizer unit with a dynamic creation, the ACLs can be modified and altered not only depending on the modules but also on time and spatial constraints that the time-triggered backplane provides. Going a step forward, Internet-based solutions can also be used to enforce security policies in automotive components (factory and OEMs) installation. Hardware profiling over an Internet-based global database which must be updated every time a new component is installed would be a great defensive measure to take under consideration. Thus, malicious acts can be securely traced back for sure. An example to comprehend the concept would be the attempt of someone trying to install a new infotainment dashboard component (e.g. an mp3 player) at 2am, or a new steering system when the car is parked on a public road. Using the Internet with realistic, dynamic and behavioral scenarios as constraints of policies to

trigger the alarm of a malicious act, might seem a far-fetched solution but the automotive industry has already started to use it and is gradually making the transition to such concepts. For instance, BMW's Tele-services send vehicle's usage statistics over the Internet, whenever the proper resources (3G connected devices, open network etc.) are found, in order to arrange the next service appointments. This means that a hardware profile of the car is already kept, so in these terms we propose the extended use of the concept with modifications for security purposes. The advantages of such an approach are that vulnerable entry points can be easier traced by the manufacturers and owners|users or legal authorities and cyber-threats and attacks on the automotive platforms can be properly recorded and security analysis may be performed. Furthermore, depending on GPS availability, geographic footprints of the cyber-attack can be detected and traced back. The privacy issues introduced by these approaches can be considered minimal. If the hardware update is legitimate, then the disclosed information is the time and the location of the update, which simultaneously indicate the location of the vehicle at a specific time. The unification of these databases of updates to the hardware profile of a platform, whenever a new module is installed, is not leaking further information than the already suggested. Additionally, the checks regarding the location and time constraints can be made locally, so that no information is leaked and privacy is compromised or violated. As for the case of the legitimate usage of the platform, there is not any tracking nor any recording of the driver but in case the actions are not legitimate or according to the security policy and rules set by the owner of the vehicle, the violations can be traced back to their source and recorded according to the policies that have been set. Explanatory messages on the automobile dashboard or on the infotainment system or from the engine compartment or other platform interfaces can be used to notify/remind the driver of his rights and the constraints that are set by the owner for users with the recognized credentials. The proposed scheme unavoidably introduces conflicts between the safety and the security circuit of the platform. These conflicts may be raised either during the initialization or during a journey due to a violation of time and other constraints. In the first case, if there is a device that is not authenticated, the immobilizer disables it, so it is removed from the network. If it is a primary module, the engine will not start and the passengers' lives will not be jeopardized, as an unauthenticated module may result in unsafe situations. If the device is a secondary module, obviously safety is not endangered by disabling it; it may only affect the passengers' comfort. Nevertheless, primary modules cannot be disabled in order to safeguard the passengers, yet proper alerts should be raised inside the platform, and if possible remote alerts should be triggered using any available internet connection. The aforementioned measures might seem to introduce additional limitations on the automobile's availability and on the freedom of users to modify on by themselves, but these restrictions are minimal. The automobile platform is made unavailable only if the hardware changes are not legitimate or if they are legitimate but no Internet connectivity for their validation to occur exists. In the first case, this is not a problem, and

the chances of the second are quite low. In advance, if the hardware update involves primary modules, this means that a serious problem has occurred in the vehicle. It is highly unlikely that a primary module (e.g. the hydraulic steering wheel system) will be possibly changed at a location where no Internet access is available and the functionality of the vehicle will be limited already. In case of software tuning, in the proposed policy it is assumed that the alternation of a limited set of parameters or commands will not trigger any alert.

In this section, the modeling of the MASC policy modules, including the Module Categorization, User Profiling and the ACL were presented. To further ensure automotive safety and security other preventive and protective measures can be adopted as well. In the next section, the functionality of MASC over the redefined immobilizer and over the automotive modules will be analyzed.

4.5 MASC-PROTOCOL FUNCTIONALITY

Since a stronger and stricter policy module modeling is applied via MASC, all the modules need to prove their factory originality. Moreover, the automotive platform security needs to be distributed over its modules in order to easily detect any of the compromised components. In order to enforce the desired policies, the following set of procedures, security and communication, as introduced in the previous subsections, will certify that all the modules act as they are originally programmed and tuned:

- Modules Mutual Authentication (MMA).
- Modules Secure Voting (MSV).
- Modules Ticket Issuing (MTI).

In order to apply the above three procedures, on the first initialization of the platform or after hardware changes have been performed, the immobilizer module is considered to be in a secure state. Since hardware changes may be triggered on malicious grounds, after such alternations or modifications the automotive platform must be allowed to access the Internet to check whether such actions are authenticated. For the above to be achieved:

- the Immobilizer hosts a table with all the public keys of the installed modules;
- each module keeps a hash of this table as well, enabling it to check for changes and updates.

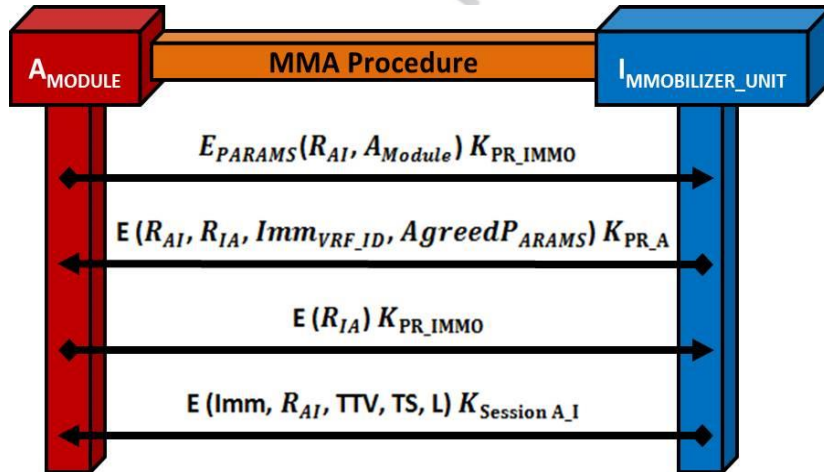
The following issues are discussed in the next paragraphs:

- The analysis of the proposed procedures (subnet protocols) of MASC and how a tampered immobilizer can be detected;
- The type of the preventing actions to be implemented in the modules, in order to trigger the modules instantly when a cyber-attack occurs.

4.5.1 MODULES MUTUAL AUTHENTICATION

On initialization of the platform, a mutual authentication procedure of each module with the immobilizer takes place. On receiving a user's credentials, the immobilizer queries the User-Profiling Database (DB) and the GPS device, retrieving the Access Control List (ACL) for each module. From this point on, the immobilizer knows which modules have to be initialized and their respective functionality. The next step is the broadcasting of a "Hello"-type message from the immobilizer to all the modules along with their names, so that the appropriate modules can start the authentication. The encrypted communication channel is constructed by using two (2) nonces. The nonce R_{A_I} being submitted by the module and the nonce R_{I_A} constructed by the Immobilizer Module with the use of the session key K_{A_I} . Since all the exchanged messages in the established channel of the communication process must be encrypted, the values that are encrypted in the first three messages can only be extracted by someone having access to the proper private key (K_{PR}). After the third message both sides know the values of the nonces R_{A_I} and R_{I_A} so they are able to create the key $K_{A_{IMMO}}$ (e.g. by calculating the hash of R_{A_I} and R_{I_A}). The analysis of the initialization and the rest of the MMA procedure of MASC are presented in Figure 4.

FIGURE 4: MODULES MUTUAL AUTHENTICATION PROCEDURE



The definitions of the variables of the procedure are listed as follow:

- the verified Immobilizer unit ID (Imm_{VRF_ID})
- the encryption parameters E_{PARAMS} ;
- the module to immobilizer Random number (nonce) R_{A_I}
- the immobilizer to module Random number (nonce) R_{I_A}
- the time-to-vote (TTV) or broadcast which will be used in the next phase;
- a timestamp (TS) which can be used later to renew the session;
- the lifetime (L) of the session;
- the session key ($K_{Session\ A_I}$) to be used from that point on;

Moreover, if only one of the parties applies the protocol while the other tries to replay old messages, then this act will be traced since the unauthorized party will not be able to present the fresh version of either the $R_{A,I}$ or the $R_{I,A}$ nonce. After the initialization, this step can periodically be repeated to trace possible attacks, guarantee the robust and secure continuity of each module.

4.5.2 MODULES SECURE VOTING

The previously presented MMA process can deliver three possible outcomes:

- I. The module and the immobilizer are mutually authenticated, therefore no module has been compromised or attacked.
- II. The module has not been authenticated to the immobilizer; therefore it has been attacked and exploited. If it is a primary module, the immobilizer halts the system. If it is a secondary module its traffic is blocked.
- III. The module has detected that the immobilizer is not authenticated and it should inform the rest of the modules without notifying the immobilizer (to prevent the immobilizer from blocking its vote as described below).

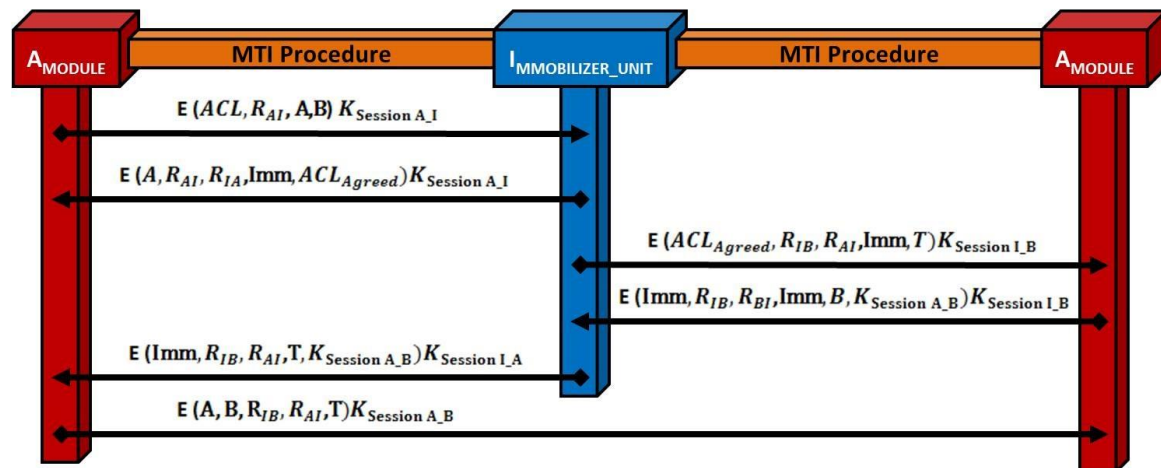
One could argue that each module has to be authenticated with all the other modules; however, this could increase the number of transmitted messages and the execution time. A more effective solution would be the use of an e-voting scheme, which provides additional advantages. Firstly, the number of messages is linear to the number of modules and not quadratic. Therefore, it is easier to check whether the other parties are voting and acting according to the created policy rather than establish a Module-to-all (M2X) communication. The votes are counted by an ECU/EMS randomly selected by the immobilizer in the previous initialization. Each module knows how many and which modules are going to vote, from the broadcast at the initialization. If the authentication of the immobilizer is successful, then the module's ballot will be "yes proceed" (e.g. 1) otherwise it will be "do not proceed" (e.g. 0). One of the reasons why the votes should be counted by a random ECU is that an affected immobilizer will attempt to forge the votes of the modules which vote against it. The votes have to be cast in TTV seconds, in order for the result to become known in κTTV seconds. An example protocol for the e-voting can be found in [24]. Any other lightweight protocol focusing on yes/no elections can also be used. Since the module that is going to count the votes cannot be considered trusted, other schemes can be used as well [25]. The result of the voting needs to be explained further. At first, all the entities check that their ballots are summed correctly in the final result. The modules also check if the proper entities have voted. If all the entities have sent a "1", then all the modules work properly and no compromise has taken place. If any of the modules has voted a "0", then obviously this module will not operate properly either will have a malfunction. Simultaneously, the other modules become aware of the invalid process during the mutual authentication with the immobilizer and according to the

Module Categorization procedure, the modules decide whether they are going to request a new round of the MMA procedure, halt or continue working. The same thing happens if several modules have been blocked from the process. In addition, the failure of a module to vote in TTV seconds results in an automatic block, not only from voting but also from sending traffic data. The failure of the module that counts the votes to provide the result in κ TTV seconds results in the rejection of the voting result from the modules.

4.5.3 MODULES TICKET ISSUING

After the previous procedures have been completed, the modules have been authenticated and communication and connection between the modules have been authorized. Yet, in order to be completely sure for the automobile's continuity of the procedures and functions time (and geographical form GPS/GPRS) constraint policies are being applied. Therefore, modules are allowed only to temporarily communicate with each other. The responsible for the Modules Ticket Issuing (MTI) procedure is the immobilizer. Whenever any modules (MODULE_1) want to communicate with another module (MODULE_2), it must communicate with the immobilizer (IMMO), requesting access permission for the Access Control List (ACL). The immobilizer checks whether ACL is valid for this user (User-Profiling). In case it is, then the IMMO issues a ticket T to MODULE_1 to access MODULE_2. The analysis of the MTI procedure of MASC is presented in Figure 5.

FIGURE 5: MODULES TICKET ISSUING PROCEDURE



The definitions of the variables of the procedure are listed as follow:

- Access Control List (ACL)
- Ticket (T)
- Lifetime of session (L)
- the module to immobilizer Random number (nonce) R_{AI}
- the immobilizer to module Random number (nonce) R_{IA}
- the module to module Random number (nonce) R_{AB}, R_{BA} ,
- $K_{session}$ =session key

Using the proposed ticketing policy, the $IMMO$ firstly checks the ACL of $MODULE_1$ request and forwards the accepted list to $MODULE_2$. Therefore, $MODULE_1$ cannot arbitrarily access $MODULE_2$. Furthermore, since the automobile is a mobile automotive platform, by periodically issuing tickets, $IMMO$ may check whether timing or geographical restrictions of the user have been or are about to be violated, triggering the proper alerts and acting accordingly. This is achieved by embedding the desired restrictions on a primary charged ACL. The secrecy of the messages is guaranteed by the use of the keys generated in the previous steps, while their freshness stems from the use of new nonces. Thus, arbitrary requests that originate from modules to other modules or requests that exceed the time, ACL (or geo-location) constraints should be considered suspicious by the receiving module, as they can only be triggered by a malicious entity that is under attack.

All of the above aforementioned measures of security and communication rules are the key processes that compose the MASC and enable the cooperation and compatibility among the mechatronics modules of the ‘automotive platform’. Thus, MASC sets a twofold structure by:

- Implementing the mutual authentication and blocking the arbitrary use of the automotive modules (e.g. control units, immobilizer). By applying this measure, the cyber-attacks based on plugging malicious or vulnerable devices in order to gain access to the ‘automotive platform’ and to components fail to be authenticated. Therefore, the automotive platform implementing the MASC is able to detect and deter the cyber threats and plays the role of an active intrusion prevention mechanism.
- Creating active distinctive roles in the ‘automotive platform’ so that specific privileges will be assigned to every user. These role privileges will authenticate and authorize each unique user to perform specific tasks and to trigger alarms in case of possible violations or of privilege escalation attacks. The security policies that govern each user will enable different access levels and functionality to vehicle modules.

4.6 VERIFICATION OF MASC

The aim of MASC is to redefine the role in the immobilizers as they are proved to be the most valuable and simultaneously the most easily exploited entry point and component. MASC’s main function is to inform every node about the consistency of data transmission. It offers the unique feature of having all the nodes in a network know instantly and simultaneously when any other node fails to communicate or sends unreliable data. Updates of status of each node are sent to all nodes several times each second. MASC also takes advantage of the fault-tolerant clock synchronization that establishes the global time base without relying on a central time server. This mechanism can be viewed as a distributed acknowledgment service that informs the main module hosting the operation if an error in the communication system

has occurred. If an attacker manages to change a module of the automotive platform, then its credentials will be modified and the immobilizer will block its communication or will not allow the 'automotive platform' initialization. The other modules must be able to detect this attack and inform MASC that there is a breach of security. There MASC has been formally checked for its security using the automated approach of the Scuther tool [26][27] and proved to be secure [17] for the following as defined in [28][29]:

- Non-injective agreement.
- Non-injective synchronization.
- Aliveness of all entities.
- All the exchanged values are only disclosed to the proper entities and remain secret to outside parties.

MASC provides a well-structured solution to the challenges of the 'automotive platform' security control which were presented in the Chapter 3. It is a fault-tolerant deterministic data protocol supporting the presented integrated automotive architecture design chain and the challenges of network and communication interfaces. The MASC security and communication features are designed as patches according to the principles of the event and time-triggered technology that guarantee new levels of safety and security translated directly into benefits such as ease of system integration and system upgradeability, as well as compatibility, reliability and performance of the overall system and architecture.

4.7 CONCLUSIONS

In this chapter MASC was introduced and described in detail. MASC proposes a new architecture for in-vehicle communication that incorporates many lessons learned from the computer and the network security fields. MASC is a set of time-triggered security protocol procedures which support event triggered communication, based on the simplicity of the reverse engineering philosophy applied on mechatronics. MASC offers a practical embedded solution to the existing automotive safety and security issues that cyber threats are generating in modern automobile. The role of the immobilizer was redefined and the security of in-vehicle communications was distributed between all its modules. In MASC all the traffic is encrypted, the modules are authenticated and participate in an e-voting or a secure multi-party computation scheme, which will determine whether or not the system is considered secure to be initialized. The immobilizer acts as a ticket issuing server as well, enabling communication between modules only when the issued ticket is presented. MASC enables us to apply further security and functionality policies. Various user profiles which have different access levels in the vehicle have been implemented. Therefore, geographical and time constraints can be applied and enforced by the tickets that the immobilizer issues.

The patching of the automotive platform with the described protocol procedures offers an open-source security-based approach of an active detection and prevention system for cyber-attacks and acts of threat against the automotive and the ITS environment. It also provides a proactive system to prevent any type of privilege escalation to occur. Summarizing, the presented work provides all the necessary tools to develop security embedded hardware-based protocols compatible with the automotive platforms and a way to protect the automobiles, drivers and passengers since cyber-attacks are detected and prevented, enforcing security policies on their platforms. Even though the automotive security issues are addressed in this section, the ITS domain should not be neglected and left unsecured, as it supports the 'automotive platforms' with transport services.

Πανεπιστήμιο Πειραιώς

REFERENCES

- [1] U. Larson, D. Nilsson, E. Jonsson, An approach to specification based attack detection for in-vehicle networks. In: Proceedings of the IEEE Intelligent vehicles symposium 2008. pp. 220-225.
- [2] CAN open standard communication protocol, [Online] <http://www.can-cia.org>
- [3] T. Hoppe, S. Kiltz, J. Dittmann, Applying intrusion detection to automotive it e early insights and remaining challenges, Inderscience JIAS 2009, pp 226-235.
- [4] V. Verendel, DK. Nilsson, UE. Larson, E. Jonsson, An approach to using honeypots in in-vehicle networks. In: Proceedings of the 68th IEEE vehicular technology conference (VTC) 2008. pp. 1-5.
- [5] J. Pelzl, M. Wolf, T. Wollinger, Virtualization technologies for cars: solutions to increase safety and security of vehicular buses. In: Proceedings of the embedded world conference, Nuremberg 2009.
- [6] B. Czerny, Towards a System Security Engineering Process for Automotive Embedded Control Systems, 30th International System Safety Conference, Atlanta, 6-12 August 2012.
- [7] H. Lönn, J. Axelsson, "A Comparison of Fixed-Priority and Static Cyclic Scheduling for Distributed Automotive Control Applications", Euromicro Conf. on RTS, 1999.
- [8] N. Audsley, A. Burns, et. al., "Fixed Priority Preemptive Scheduling: An Historical Perspective", Real-Time Systems, 8(2/3), 1995.
- [9] J. C. Palencia, M. González Harbour, "Schedulability Analysis for Tasks with Static and Dynamic Offsets", Proceedings of the 19th IEEE Real-Time Systems Symposium, 1998.
- [10] K. Tindell, J. Clark, "Holistic Schedulability Analysis for Distributed Hard Real-Time Systems", Microprocessing & Microprogramming, Vol. 50, Nos. 2-3, 1994.
- [11] R. Dobrin, G. Fohler, "Implementing Off-Line Message Scheduling on Controller Area Network (CAN)", Proceedings of the 8th IEEE International Conference on Emerging Technologies and Factory Automation, 1, 2001.
- [12] V. Raja, K. Fernandes, Reverse engineering: An industrial Perspective, Springer Series in Advanced Manufacturing, Springer 2008
- [13] W. Wang, Reverse engineering Technology of reinvention, CRC Press, 2011
- [14] R. Bishop, Mechatronics an introduction, CRC Press, 2006
- [15] C. Patsakis, K. Dellios, Patching Vehicle Insecurity, Invited Talk - In-depth Security conference 2011 Europe (Deep-Sec), [Online] <http://www.youtube.com/watch?v=BA2J7O6cqzQ>
- [16] C. Patsakis, K. Dellios, Securing in-vehicle communication and redefining the role of the automotive immobilizer. International Conference on Security and Cryptography (SECRYPT), 2012, pp 221-227
- [17] C. Patsakis, K. Dellios, M. Bouroche, Towards a distributed secure in-vehicle communication architecture for modern vehicles, Computer and Security, Elsevier, vol. 40, Feb. 2014, pp 60-74
- [18] H. Heisler: Advanced vehicle technology. Butterworth-Heinemann; 2002.
- [19] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway et al., Experimental security analysis of a modern automobile, IEEE Symposium on Security and Privacy, Oakland, CA 2010. pp. 447-462.
- [20] N. Naver, F. Simonot-Lion, Automotive embedded systems handbook: industrial information technology, CRC Press; 2009.
- [21] M. Bonnick, Automotive computer controlled systems, diagnostic tools and techniques. Butterworth-Heinemann, 2001

- [22] RW. McGraw, Risk-adaptable access control (Radac), In: Privilege (Access) management Workshop. NIST: National Institute of Standards and Technology Information Technology Laboratory; 2009.
- [23] A. Ferreira, D. Chadwick, P. Farinha et al., How to securely break into rbac: the btg-rbac model, In: Computer security applications conference, 2009. ACSAC'09. Annual, IEEE 2009. pp. 23-31.
- [24] H-T Liaw. A secure electronic voting protocol for general elections. Journal of Computer Security 2004, Vol. 23 pp.107-119.
- [25] H Kikuchi, J. Nakazato, a compact modular arithmetic java class library for cellular phones, and its application to secure electronic voting, In: Security and protection in information processing systems, IFIP, Vol. 147. Springer; 2004. pp. 177-192.
- [26] Scyther tool, [Online] <http://www.cs.ox.ac.uk/people/cas.cremers/scyther/>
- [27] The Scyther Tool: [Online] people.inf.ethz.ch/cremersc/scyther/index.html; 2012.
- [28] C. Cremers, The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols, LNCS, Vol. 5123, 2008, pp 414-418
- [29] G. Lowe, A hierarchy of authentication specifications. IEEE Computer Society; 1997. pp. 31-43

PART III: BUILDING INTEROPERABLE & SUSTAINABLE GLOBAL TRANSPORT SERVICES & SYSTEMS

In the first chapter of this dissertation, an analysis of the automotive technology was performed, and the modules of the automotive platform stack were identified. The second chapter depicted the standardized reference architecture of the Intelligent Transport Systems (ITS) and the participating functional components and elements, as well as the basic set of ITS applications. In the third chapter of this dissertation, the reasons of the automotive platform vulnerabilities against cyber-attacks were investigated. The output results of the threat model contributed into identifying not only cyber-threats, but also vulnerable entry points, design flaws and the impact caused to the ITS structure (functional elements and components). In the fourth chapter a new security protocol called MASC-Protocol was presented. MASC-Protocol provides-equips the automotive platform with an embedded real-time triggered security mechanism for the detection and prevention of cyber-attacks. In addition, the proposed redefinition of the Immobilizer and the EMS role implementing the subnet protocol procedures of User Profiling, Module Categorization, Access Control List (ACL) and the applied Modules Mutual Authentication (MMA), Modules Voting System (MVS) and Modules Ticket Issuing (MTI) set the automobile cyber-stack secured towards internal and external cyber-threats.

The third part of this dissertation consists of two chapters. The fifth chapter includes the implementation of an operational model implementing a Service Discovery Mechanism (SDM) of service registry. The proposed operational model role is to function as the top layer of the Cooperative-ITS reference architecture (RA) so that web-services technologies as well as any Service Oriented Architectures can be adopted in a holistic interoperable ITS architecture model. Unfortunately, as found in the context of ITS standards both the management and the security blocks of the ITS-station reference architecture lack of proper and detailed analysis, leaving space for further research and innovation including the interoperability of services and applications. For this reason, a proposed Service Discovery Mechanism (SDM) is implemented as a framework upgrade of the management block. Retrieving the unique SessionID, User Profile and the e-ticket of the MTI subnet protocol of the MASC procedures, a token hosted in the service registry of the SDM in each automotive platform (ITS Vehicle Station) can be generated, securing all types of the service transactions, data or information exchanges. In addition, due to the fact that all the ITS-station functional components are embedded in every single ITSC functional element of the ITS-Station RA, the programming source code nature of the MASC along with the SDM mechanism can be implemented in all the participating ITS-substations (vehicle, roadside, personal of base-station). This the contribution of the interoperable SDM and the MASC can

be extended beyond the strict environment of the statutory cooperative-ITS to the entire Transportation cyberspace, thus transforming the automobile platform into an autonomous interoperable high-mobility node and taking full advantage of all types of communication interface capabilities.

The last chapter of the third part considers the sustainable development of the entire transportation domain. Inspired by the 1987 Brundtland Report of the World Commission on Environment and Development entitled “Our Common Future” [1]. Driven by this motivation and based on today’s needs without excluding the possibilities of future updates and upgrades, a cloud-based system called ‘iTransport Cloud’ system is designed. The ‘iTransport Cloud’ system is transportation-oriented and will host all of the previously proposed solutions presented in this dissertation.

Πανεπιστήμιο Πειραιώς

5. The upgraded ITS-RA framework

Inside the complex ICT world of converging yet diverse technologies, the entire transportation domain must communicate and inter-operate at all levels; components, elements, systems, architecture models, services and applications. Unfortunately, the cooperative ‘Basic Set of Applications’ of the ITS is exclusively based on the communication interfaces of sensor networks. As a result, the syntactic, semantic and cross domain interoperability for the future generation of the ITS services have been neglected.

In this chapter, this interoperability issue of the ITS services is addressed with the design of an embedded operational model, that implements the Service Discovery Mechanism (SDM) of service registries. The role of the proposed operational model is to encapsulate the entire Cooperative-ITS reference architecture (RA) so that web-services technologies and service oriented architecture can be adopted and adapted in a holistic interoperable ITS architecture model. Both the management and the security blocks of the Cooperative-ITS RA, presented in Chapter 2, are still subjects of research and innovation for secure interoperability of services and applications in the context of standards, a new SDM is introduced and implemented as a framework upgrade, patching both blocks.

Furthermore, because all of the ITS-Station functional components are embedded in every single ITS communication functional element of the ITS-Station RA, the MASC along with the SDM mechanism can be implemented in all the participating ITS-substations (vehicle, roadside, personal or base-station). Thus, the contribution of the interoperable SDM and the modified MASC:

- can be extended beyond the strict environment of the statutory Cooperative ITS,
- enabling the management and the security blocks to participate in the transportation cyberspace, transforming the automobile platform into an autonomous interoperable high mobility node,
- taking advantage of the wired and wireless communication medium of the ITS network.

5.1 MOTIVATION AND CONTRIBUTION

The Intelligent Transport Systems (ITS) are one of the most promising fields of the wider Transportation domain [1][2]. The cooperative-ITS [3] is the emerging sub-domain of the ITS responsible for enabling the communication between the vehicles and the surrounding infrastructure for the exchange of services and data. Such a technological evolution is based on the utilization and integration of the Information and Communications Systems (ICS) of the emerging ICT world, involving the interaction of a plethora of participating entities (e.g. drivers, vehicles, road-side units, nomadic devices, base-stations, authorities, components and elements) [4][5]. Simultaneously, the changing and evolved fast evolving face of the cyberspace into a massive networking technological entity is expected to affect the transportation systems positively providing a basis for interoperable and efficient development [6]. Furthermore, all of the existing and the newly designed and generated entities and objects can be uniquely identified in the interconnected cyberspace (e.g. Internet of Things-IoT) [7], while interacting with mobile services and applications [8][9].

5.1.1 MOTIVATION

The definition of cooperative systems according to the 3rd eSafety Forum [10] (2004) of the European Commission is the following: "Road operators, infrastructure, vehicles, their drivers and other road users will cooperate to deliver the most efficient, safe, secure and comfortable journey. The vehicle-vehicle and vehicle-infrastructure co-operative systems will contribute to these objectives beyond the improvements achievable with stand-alone systems". Data are acquired from vehicles and transmitted to a server for central fusion and processing. These data can be used to detect conditions such as traffic congestion and weather events, which are grouped in the Basic Set of Applications (BSA) of the section 2.6. The server processes a driving recommendation of a single or a specific group of drivers and transmits it wirelessly to the surrounding vehicles, as presented in sections 1.3 and 1.6.

The vision for a future transportation domain of zero accidents, zero delays, interoperable services and applications governed with privacy and security, is the one that the automotive industry shares with the research community. However, besides the fact that vehicles are not so easy to be redesigned due to their mechatronic cyber-physical nature and the costs involved, the automotive industry over the last years has managed to successfully equip vehicles with new emerging ICT and provide the driver with advanced levels of mobility and communication [11]. Such an example was the exploitation of the Cloud Computing concept over vehicles in order to provide end-users with new kinds of services. This revolutionary attempt has been achieved with the partnership for research and development (R'n'D) of Ford, Microsoft, Intel and the University of Michigan. The main concept included the scenario of a vehicle accessing the Windows Azure Cloud Platform and consuming the cloud-services of the driver's interest. In addition, most of the Intelligent Transport Systems

research is focused on how to improve transport safety and provide service cooperation, network efficiency, mobility and reduced environmental impact. However, the Cooperative-ITS are still under development and continuous research³¹ in order to provide quality applications and services. Therefore, the R'n'D efforts to address the interoperability of the ITS structure beyond the communication and sensor infrastructure implementation of the cooperative-ITS is encouraged. The US Transportation Secretary Ray LaHood stated that 'cars talking to each other is the future of motor safety' [39], the management and the security of the ITS-S RA are areas that need further research and development in the transportation domain [12][13][14].

5.1.2 CONTRIBUTION

Driven by this motivation this chapter address the interoperability issues of the ITS environment. In the following paragraphs an efficient way to transform vehicles into autonomous platform nodes able to operate over any packet based network, is discussed [15][16]. A framework upgrade of the ITS-Station Reference Architecture based on a dynamic operational model is designed and developed. For the implementation of the proposed operational model into the ITS-Station RA (ITS-S RA) blocks, an embedded Service Discovery Mechanism (SDM), having the role of the main service registry, will be introduced. The adaption of the entire proposed design must be performed with minimum modifications on the entire ITS structure. Therefore, the proposed operational model will be placed on the top layer of the Cooperative-ITS architecture.

Due to the fact that the Cooperative-ITS are exclusively based on communication-based interfaces between the participating entities, the design of the interoperable operational model and the SDM will be based on the efficient utilization of web-services technologies of the Service Oriented Architectures (SOA). The SDM will substitute the management block, of the ITS-Station RA [17] in order to attribute the interoperability element to all the existing or future generated ITS services and applications. All of the ITS-Station functional components are embedded in every single ITSC functional element of the ITS-Station RA. Therefore, the MASC-protocol, as presented in chapter 4, can be implemented as an Application Programming Interface (API) [18][19] in all the ITS-substations (vehicle, roadside, personal or base-station). Then all of the ITS-substations will be equipped with the service registry of the service discovery process in order to update the security block.

Summarizing the contribution of the proposed interoperable and cooperative 'upgraded ITS-RA framework', which includes the Operational Model, SDM and MASC has an interoperable multiple-functioning structure of:

³¹ APPENDIX II: ITS RESEARCH PROJECTS

- Extending the interoperability of the currently available and of the future generated automotive and ITS services beyond the strict environment of the statutory Cooperative ITS management block.
- Offering an interoperable embedded security solution for all the participating ITS-substations of the ITS environment addressing the security issues of the ITS-S RA
- Transforming the automobile platform into an autonomous interoperable high mobility node and taking full advantage of the capabilities of the embedded network and communication interface capabilities.
- Forming a holistic approach of intermodality and interoperability for the entire Transportation cyberspace.

In the following section the fundamental principles of the proposed interoperable framework are described in detail.

5.2 FUNDAMENTALS AND PRINCIPLES

In this section, the fundamentals of the cooperative and interoperable systems, the principles of the Service Oriented Architecture (SOA) and the proposed framework are analyzed.

5.2.1 COOPERATIVE AND INTEROPERABLE SYSTEMS

A cooperative system is defined as a system of multiple dynamic entities that share information or tasks to accomplish a common objective. The cooperative control systems include entities operating within a manufacturing communication interface (e.g. WSN, radar, software agents). The term "entity" is often associated with vehicles capable of physical motion³² (e.g. automobiles, ships, aircrafts) but the definition extends to any entity concept that exhibits a time-dependent behavior³³. Critical to cooperation is communication, which may be accomplished through active message passing or through passive observation. Communication cooperation (e.g. Wireless Sensor Networks) is being used to accomplish a common purpose that is greater than the purpose of each individual, who may have other objectives or being a member of more than one groups. This implies that cooperation uses hierarchical forms and the decision-making process of the control is typically distributed or decentralized. A cooperative system may be modeled as a single and stand-alone entity. The level of cooperation may be indicated by the amount of information exchanged between the entities (e.g. data traffic and monitoring). The cooperative systems involve task sharing and can consist of heterogeneous systems in case they are composed of humans and machines. Research concerning the cooperative systems has addressed the issue of how to perform under noisy or adversary conditions.

³² Applied Mechatronics theory (Chp.1)

³³ MASC-Protocol proposed solution (Chp.4)

One of the key motives for the development of ICT standards is to facilitate interoperability between systems, services and products in a multi-vendor, multi-network and multi-service environment. Complex systems and products are often based on the utilization of multiple systems and set services cooperating altogether as one. Interoperability is the ability of making different systems to interoperate. Nowadays, interoperability is used in the task of building services for users when the individual components are technically complex and heterogeneous to allow for information exchange. Three types of interoperability exist; syntactic, semantic and cross-domain:

- Syntactic Interoperability is defined as the communication and data exchange between two or more systems. Specified data formats (e.g. ASCII or Unicode formats), communication protocols, XML and SQL standards are among the tools of syntactic interoperability.
- Semantic interoperability is defined as the ability to interpret accurately the information exchanged between two or more systems in order to produce output results and functions according to the specifications defined by the end users of both systems. To achieve semantic interoperability, both sides refer to a common information exchange reference model.
- Cross-domain interoperability is defined as the state where multiple heterogeneous entities interoperate for a common interest (e.g. ITS entities during an information exchange)

In practice the interoperability process has several facets including the:

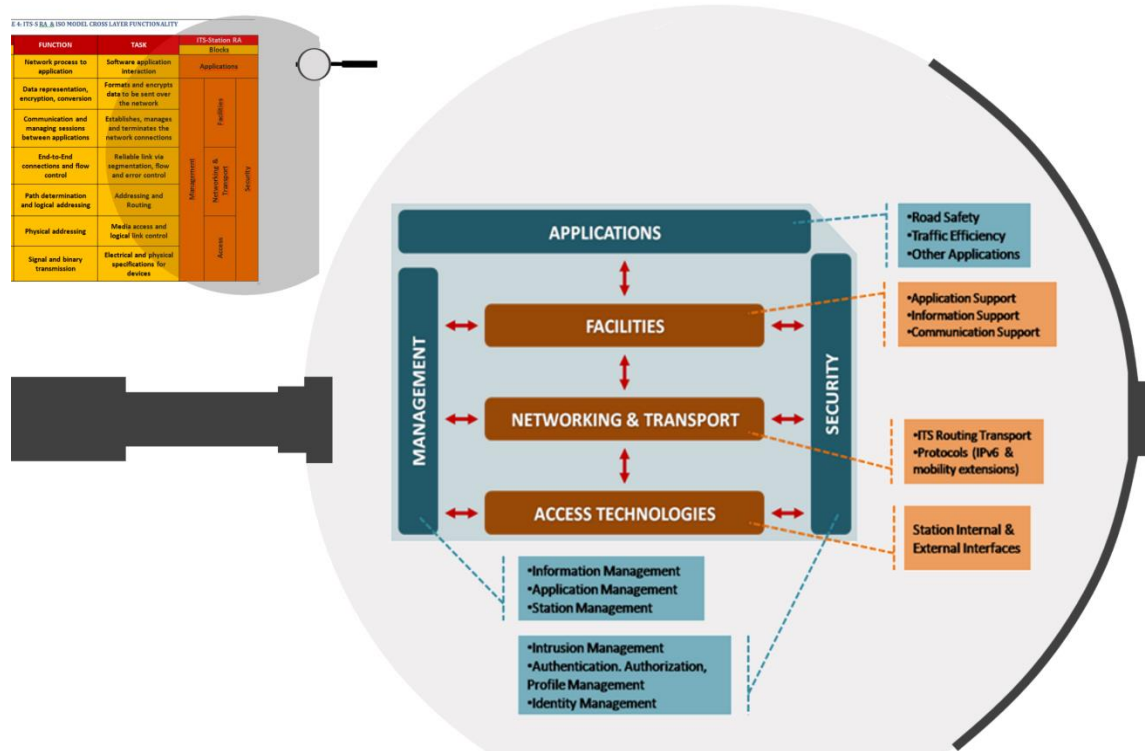
- development of procedures for a homogeneous framework implementing the essential requirements on technical compatibility, verification, reliability, availability;
- research for the level of technical compatibility that is necessary and adequate the heterogeneous systems, services and applications to operate/function;
- research for the level of technical harmonization contributing to the gradual establishment of the services and the future upgrading of the system's operations.

5.2.2 SERVICE ORIENTED ARCHITECTURE

Vehicles should be able to operate over functional oriented architectures and any type of packet based networks. Nevertheless, the interoperability between the different ITS-Stations (central, roadside, vehicle, and personal), the BSA and e-services is the missing link. In addition, the lack of specific directives of how to develop, implement or adapt interoperable services over the already deployed services, applications, vehicles and infrastructures in heterogeneous ITS environments is the actual problem to address. Moreover although the SOA are referred in the ITS standards, it is not extensively and properly used or developed within the cooperative-ITS architecture. In Figure 6, the cooperative-ITS services of the ITS-

S RA blocks are illustrated, as presented in previous chapter 2. Driven by this motivation, a sustainable and interoperable operation model is crucial to be implemented and carefully designed.

FIGURE 6: COOPERATIVE SERVICES OF THE ITS-STATION REFERENCE ARCHITECTURE



The SOA are not a product, but it is the premier integration and architecture framework in today's complex and heterogeneous computing environments. SOA provide the architect with registry mechanisms essential to minimally discover services using a set of design principles, patterns and programming techniques when developing mission-critical applications and processes delivered as services over the network [20]. For the integration of the service deployment, playing the role of the middleware system to support the platform and the software interaction over any kind of packet based networking environment selected for delivery [21], Web Services are used. Web Services are the actual implementation of SOA services delivered over the Web or the Cloud using a common set of standards and technologies such as XML[22], Web Services Description Language (WSDL) [23], Simple Object Access Protocol (SOAP) [24], and Universal Description, Discovery, and Integration (UDDI) [25]. Specifically, the UDDI standard is defined as a set of services and it is considered as a specification of Application Programming Interfaces (APIs) [18][19] with built-in metadata extensibility. It supports the description and discovery of the published and provided services and the technical interface to access the web services, including nodes and registries. The UDDI mechanism can provide the interoperable infrastructure we need for a Web Service-based environment when publishing or finding services. Interoperability,

therefore, is the most important principle of SOA and one of the key benefits of Web Services which allows different distributed web services to run on a variety of software platforms and hardware architectures [26].

Nowadays, web-based enterprise applications utilize extensively the Web Services over the “Cloud” and several efforts are being made by the automotive industry to exploit the “Cloud Computing” concept on vehicles in order to provide end-users with new kinds of services. Automotive vendors focus also in new technological developments addressing the vehicular network requirements in order to enhance vehicular services. SOA is the key environment for the dynamic discovery, provision and use of services over a network or networks of their own choice [27][28][29], transforming the vehicle into an actual autonomous computing node with communication capabilities. Therefore, SOA represents the ideal environment for developing portable and interoperable web services, sharing the exact same vision of providing new generation services for the ITS environment. In the following sub-sections the implementation of the operational model as a framework over the existing ITS-Station RA will be described without further disturbance of the already defined architecture as found in Chapter 2 and seen in Figure 6.

5.2.3 INTEROPERABLE & COOPERATIVE ITS ARCHITECTURE

SOA is the architectural style used in this dissertation for building software applications that use services available in a network. Services are software components with well-defined interfaces that are implementation-independent. The most important aspect of SOA is the separation of the service interface; the what, from its implementation: the how. The Service Provider uses a Web Services Description Language (WSDL) document in order to describe the functional characteristics of each service and application available. For the above stated purpose, we can assume that the web-based services will be provided either by the automotive vendors or by other certified parties (i.e. automotive enterprises, automotive suppliers, public ministries, government authorities and private enterprises). The SOA find-publish-invoke process (or operational model) is the backbone of the architecture design of the proposed Service Discovery Mechanism (SDM) for the proper integration of the Interoperable Framework upgrade of the C-ITS.

The framework states that a vehicle station with fewer capabilities than other vehicles should be able to request any type of service (interoperable or cooperative) from any other sub-station (central, roadside, vehicle, and personal). In the various modes of V2X communication scenarios, network capabilities are under consideration to support new programming APIs, applications and cooperative services. This functionality can be achieved using the WS interaction anatomy [20][29] which defines the roles and the relationships

between the entities holding the Service Registry and the entities holding the Service Discovery Mechanism of the overall framework as defined below:

- i. Role – Service Requestor|Consumer: In the proposed interoperable framework update of the cooperative-ITS, a Service-Requestor (SREQ) is a vehicle or a nomadic device (personal device) inside the vehicle that requires an interoperable service (e/m-service). The vehicle initiates the enquiry of the service in the registry, binds to the service over the transport layer, and executes the service function. The Service-Requestor executes the service according to the interface layer contract.
- ii. Role – Service-Provider: A Service-Provider (SPRO) is any type of a network-addressable entity in a transportation environment (vehicle, road-side, personal or central) that accepts and executes requests from SREQ. It publishes the services and the interface contract to the Service-Registry (SREG) so that SREQ can discover and access the requested service of interest.
- iii. Role – Service-Registry: A Service-Registry (SREG) is the enabler for the service discovery process. It contains a repository of all available services and allows SREQ to scan different interfaces of interested SREQ.

All entities participate in the service-oriented operational model can have more than one of the following roles. The roles' operations in the service-oriented architecture can be:

- i. Publish: A service description must be published in order to be accessible discovered and invoked by a Service-Requestor.
- ii. Find: A Service-Requestor searches and locates a cooperative-service of interest by querying the Service-Registry.
- iii. Use: After the service description is retrieved, the Service-Requestor proceeds to invoke the selected service of interest.

5.2.4 ADDITIONAL SPECIFICATIONS

Due to the fact that SOA is not a new notion and that it has expanded to include the web, the Web-Services and other emerging concepts of computing, the elements in the presented service-oriented proposal include, but are not limited to the following:

- Module Management Control System (MMCS): The role of MMCS is to interact with the main DB Repository and the rest of the ITS structure. The MMCS based on the MASC principles substitutes the redefined role of the Immobilizer and the EMS acting. It also acts as the security mechanism for the operators' authentication to the Trusted and Regulatory Authority (e.g. the Ministry of Transportation), before MASC's default initiation or periodical control check of the Interoperable and Cooperative ITS proposed framework upgrade.

- **Operators:** The users responsible for the trusted Service Registry (SREQ) updates and of the control of all the ITS services types (interoperable and cooperative) into the ACL.
- **Hardwired-Backbone:** The end-to-end wired-based communication interface of the entire ITS infrastructure (Database Repository, MMCS, Road-side units)
- **Wireless-Backbone:** the end-to-end wireless based communication interface that supports the wireless exchange of interoperable services or cooperative data with the road-side stations.
- **Interoperable Services:** The set of interoperable ITS services that are made available for use through a published interface (Service Registry) and allow the services to be invoked by a Service-Requestor, provided by the Service-Provider and consumed by the original Service-Requestor.
- **Cloud Portal:** Even though the cooperative data exchange is based on wireless sensor networks, the cloud portal is responsible for the interoperable services and data exchange between all the ITS-Station elements of the ITS stack.
- **MASC Modifications:** The set of procedures of the originally created MASC modified to be implemented in the Interoperable and Cooperative ITS framework upgrade.
- **Central DB Repository:** It is consisted of the Operators Profiling, the main Service Registry Table, the Module Categorization and the Access Control List (ACL). In addition, the ACL is retrieved by the MMCS.
- **Service Registry (Additional Specs):** The service-registry implementations essential to create the service discovery mechanism, the clustering features, the repositories and the data structures for searching or publishing interoperable services. The various implementations are described below:
 - i. **Java Implementations:** There are two UDDI implementations for Java. The IBM UDDI4J [30] and the open source Java implementation of jUDDI [31] for accessing web-services.
 - ii. **Python Implementation:** The UDDI4Py [32] is used for inquiry and for processing the responses from the service registry catalogue.
 - iii. **Perl and Ruby Implementation:** The UDDI Lite [33] and UDDI4r [34] provide a basic client service-registry for inquiry and publishing.

In addition, Service Registries and interoperable services can be developed and implemented over any network either by the automotive vendors, the suppliers or any other involved parties and uploaded to the Trusted and Regulatory Authority by the Operators. The Service Registries must be part either of a global federated network or of a privately owned and operated registry. Components and entities such as the programming engineering techniques, the methods and the constructs, the reference architectures, the frameworks and APIs, the end-users and the already existing e/m-

services form the basis framework for the interoperable locating and publishing services within the ITS service registry. The three categories of the traditional registries include:

- i. white pages that contain the basic information about the vendor/supplier/developer with its firmware information or with a unique identifier to allow the web service to be securely discovered;
 - ii. yellow pages that contain the description of the capabilities of the provided service for an easier search, provision and consumption via the Service-Registry;
 - iii. green pages that contain the technical information about the provided service including the interfaces of the URL-locations and the discovery information required to find and consume the service of interest.
- Service Discovery Mechanism (SDM): The embedded client-server and hardware-based mechanism acting simultaneously as a wireless scanner for available wireless interfaces and as the ITS portal that enables the discovery of the SREG during a request for interoperable services among the participating ITS-Station elements.
 - Interoperable and Cooperative ITS Services (additional Specs): Anyone who wants to offer an automotive portfolio of next generation ITS services will rely on shared services among vehicles (e.g. governance, account management, workflow, single-sign-on, social networking) and not on stand-alone web or cloud-based applications. Vehicles are able to provide more than hardware infrastructure (i.e. on-board memory, GPS receiver) to users whose vehicles are not equipped with the same hardware capabilities as long as the automotive platform is “loaded” with an OS and equipped with a multi-function display screen as discussed in chapter 1 and shown in figure 3. A fully networked vehicle is able to deliver an integrated set of software and hardware-based services developed for both software and hardware runtimes. Vehicles with network access can be used by vehicle users not only to obtain internet service (i.e. e-mail, RSS feeds) but also to be the gateway for vehicles to gain access to any other network or the Web/Cloud. Treating traditional cooperative applications (e.g. such as navigation, traffic, warning and weather information) as Interoperable and Cooperative-ITS services, interoperability and cooperativeness can be implemented in the following application classes of:
 - i. traffic information and management (e.g. cooperative traffic information & forecasting, dynamic free parking space information, location based information and warning);
 - ii. safety and security (e.g. hazard warning, theft recovery, tracking and trace, emergency calls);
 - iii. comfort (e.g. adaptive cruise control systems and infotainment systems with music/video on demand or business information);

5.2.5 INTEROPERABLE AND COOPERATIVE-ITS PROCEDURE

In this section, the overview of the entire interoperable and cooperative-ITS procedure as well as the main processes of the Service Discovery Mechanism (SDM) are described:

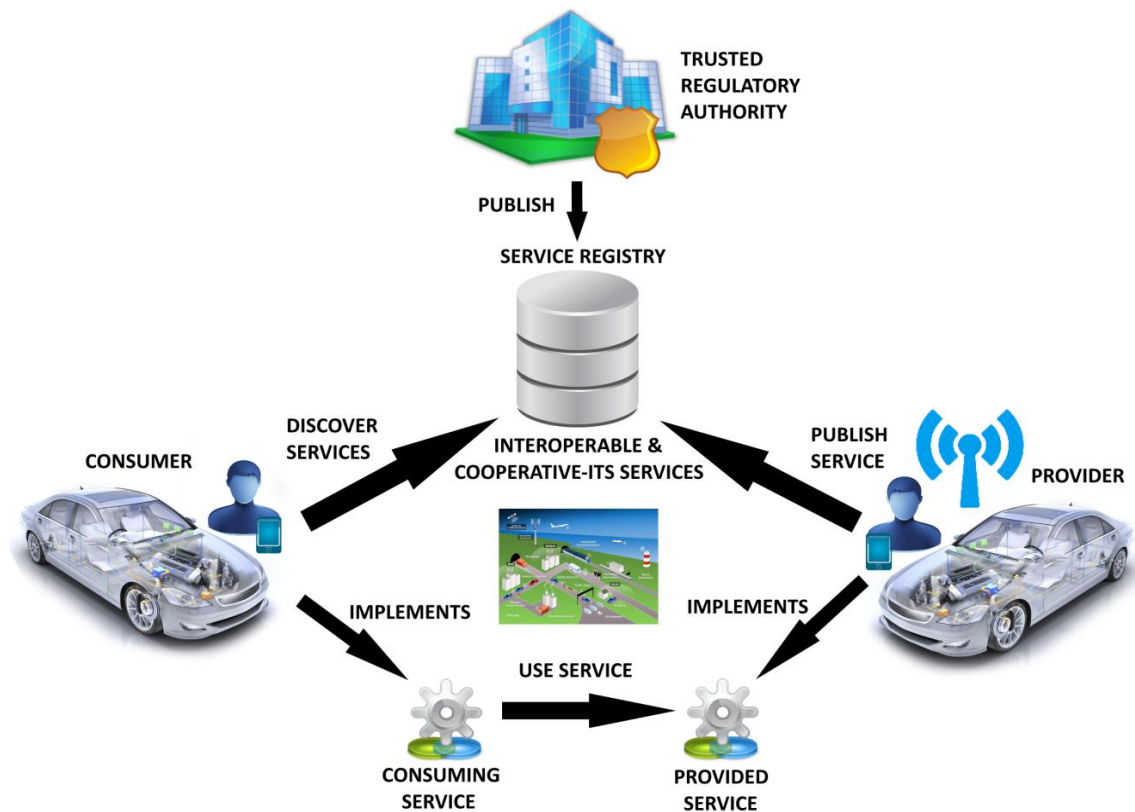
- Firstly, the operators are being authenticated to the Module Management Control System (MMCS). Then a temporary ACL list is generated by the enabled Module Categorization and the operator's profile.
- MMCS queries the main DB repository to retrieve the operators profile access rights. The proposed structure is hosted into the Trusted and Regulatory Authority and it is connected to the MMCS.
- MMCS is responsible for managing and controlling the linked modules through the Module Categorization list. For this action to take place after the successful operator authentication, the MMCS retrieves the Module Categorization.
- The finalized ACL dictates to the MMCS which modules can be securely temporarily enabled. Therefore, if the MMCS decides that a module_n should not receive any power the power source of the connection is cut off by the MMCS. If the modules_n are independently-powered, then MMCS will drop the packets and will block the packet traffic to and from those modules_n.
- Furthermore, MMCS is aware of the ITS platform network topology (e.g. where the parts are located, which parts can communicate with which and, where the available entry points are for external devices) via the monitoring of a default mapping table, as described in section 1.1, hosted in a default registry in the MMCS unit (for reasons of efficiency and performance).
- The MMCS role is also to act as a proactive hardware-based firewall of the ITS proposed framework, hosting the modified MASC procedures (rules and exceptions) as they will be analyzed in the following sections of this chapter.
- The Module Mutual Authentication (MMA) is performed.
- The road-side modules that are mutually authenticated with the MMCS are at this state temporary activated.
- The Module Voting System (MVS) procedure of MASC begins.
- The Module Ticket Issuing (MTI) procedure of MASC is completed
- The initial Interoperable and Cooperative ITS framework update occurs if the MASC procedures are completed and all the modules are secured to operate their functions.
- After the initial update, the procedure can be periodically repeated either for booting the entire ITS structure (e.g. maintenance reasons, shifting operators) or for updating the existing one (new modules installed) in order to ensure the proper operation of the proposed framework.
- In addition, retrieving the unique SessionID, the User Profile and the e-ticket of the MTI subnet protocol of the MASC procedure, a token hosted in the service registry of the SDM

in each automotive platform (ITS Vehicle Station) can be generated, securing (a timestamp or any other type of security method may be used) any type of service transaction of data and information during the SDM procedure of the search-find-retrieve-consume process.

After the proposed framework has been fully activated and controlled based on Operators Profiling and ACL by the authorized operators, MMCS enables SDM for the find-publish-invoke process (Figure 7) to take place as described below:

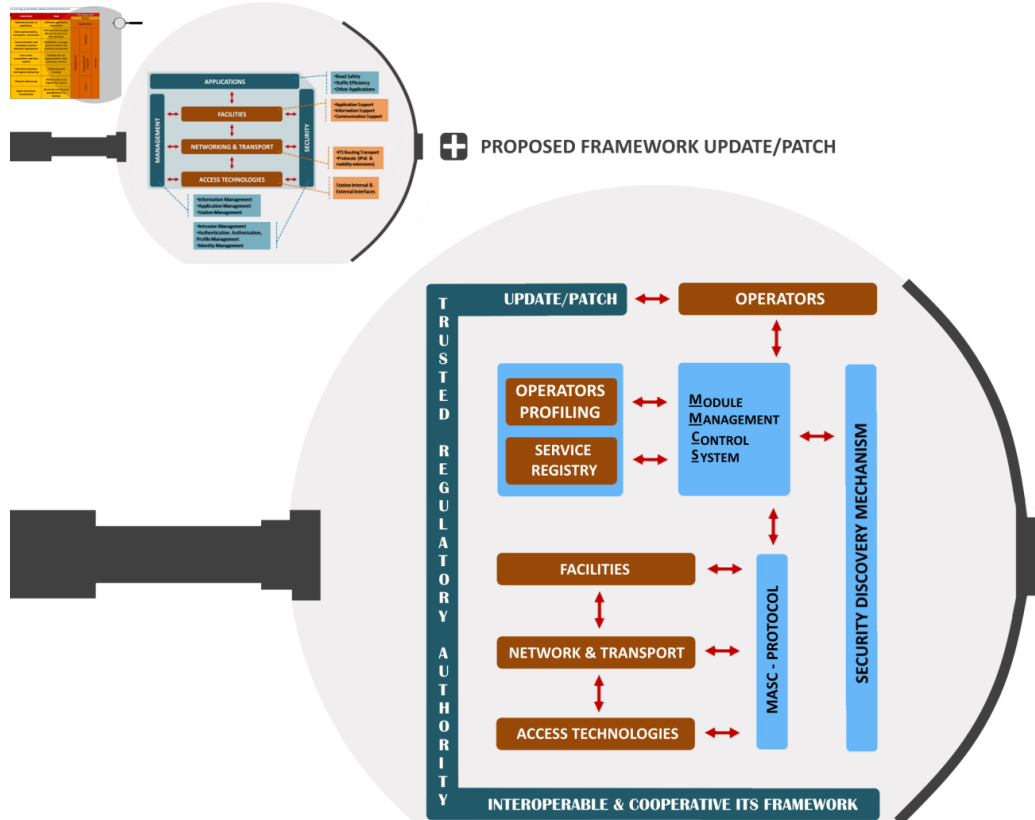
- The ITS Central Station (Trusted Regulatory Authority), hosting the entire structure as already described and including the Interoperable and Cooperative Applications, provides the environment for the deployment and operation of the Service Registry over the MMCS.
- The Service Registry hosts the services' catalogue (as they have been previously defined) and the SDM (server-side) publish them via the wireless and wired backbone interface of the MMCS.

FIGURE 7: INTEROPERABLE AND COOPERATIVE PROCEDURE OVERVIEW



- Any other mode of the ITS-Station (vehicle, road-side or personal) can host the SDM (client side) in their EMS module in order to complete the functions and the operations of the interoperable and cooperative proposed framework. SDM also supports a function of automotive server-side in case the entire structure is out not working.
- i. In the case of the decentralized SDM, two scenarios of the SDM procedure can take place; between two vehicles or between more than two vehicles with a random selected leader hosting the Service Registry. Both the scenarios of the decentralized vehicle-to-vehicle (V2V) SDM case are described in section 5.4.1.
- ii. In any other case, the standard client-server SDM procedure takes place between the vehicles and the road-side infrastructure (V2I) for a centralized operation of the framework. The scenarios of the centralized vehicle-to-infrastructure (V2I) SDM case are described in section 5.4.2.

FIGURE 8: PROPOSED INTEROPERABLE AND COOPERATIVE ITS FRAMEWORK



- The Service Registry is responsible for the service registration, as it lists the various service types, descriptions, and locations of the interoperable and cooperative ITS services of interest.
- During the Service Publication operation, any participating Service Provider can register the service type information in the registry.
- In the Service Discovery Mechanism process, the Service Requestor is able to find the service of interest (Service Registry Catalogue Indexing) such as the service description,

the interface description and the service access points managed by the access, network, transport and facilities layers.

- Finally, the Service Requestor finds the required interoperable and cooperative ITS service of interest and retrieves it to consume it on demand from the Service Provider.

Using the proposed Interoperable and Cooperative ITS framework update/patch, all the services can be consumed by clients without the clients being concerned how their requests will retrieve the services of interest, because the services can be dynamically discovered using the well-known SOA find-publish-invoke sequence. Figures 7 and 8 depict the overview of the previously described procedures and the updated/patched proposed interoperable & cooperative-ITS framework respectively. The analysis of both the modified MASC and the framework procedures are presented respectively in the next two sections 5.3 and 5.4.

5.3 MASC-PROTOCOL MODIFIED FUNCTIONALITY

As it has been discussed, in order to stop many of the cyber-attacks against the automotive platform stack, strict security policies need to be enforced. The Module Management Control System (MMCS) is modified and new policy modules are implemented. The three introduced policy modules; the RS_{MODE} categorization, the operators profiling and the Access Control List (ACL) are based on credential and time constraints define the access rights of the road-side units (RS_{MODE}) and of the operators of the entire Transportation Platform.

A. RS_{MODE} CATEGORIZATION: The adoption of a “Deny all” policy towards all mechanical and peripheral parts (RS_{MODE}) of the ITS platform is crucial to provide new security features, to decrease the number of cyber attacked and compromised RS_{MODE} and to maintain the current status of MMCS functionality. Another reason for implementing RS_{MODE} categorization is because the MMCS platform has a plethora of RS_{MODE} , each focusing on a different set of tasks including the hosting of the proposed SDM and the service registry. If a module is not properly managed, the safety features of the MMCS, the automobile, the driver and the passengers can be endangered. The proposed RS_{MODE} categorization is based on the network backbone topology of the MASC platform separating them into Primary and Secondary modules:

- a) Primary RS_{MODE} : traffic control signals, warning indications and emergency types of RS_{MODE} .
- b) Secondary RS_{MODE} : the rest of the modules connected to the backbone of MMCS.

B. MMCS PLATFORM OPERATOR PROFILING: The operators’ authentication to the MMCS platform can be achieved by several methods depending on the infrastructure used by the Ministry of Transportation. These methods may range from biometrics to common smart-cards. The proposed operator profiling offers an additional security measure for enabling a built-in database of multiple user profiling linked with the entire

MMCS. The scope of the operator's authentication over a build-in database for user profiling is: a) to properly authenticate the operators to the critical cyber nature of the MMCS platform and b) to provide different access levels to operators each time as specified by the Ministry of Transportation needs.

C. ACCESS CONTROL LIST: The role of the Access Control List (ACL) is a crucial component and a vital ingredient of MASC as they can provide one more line of defense against several cyber-attacks and threats. As discussed before, by exploiting vulnerabilities existing in RSMODE many attackers are possible to provide access to the MMCS platform. However, if each RSMODE has a personalized ACL when accessing other RSMODE, a privilege escalation of this type can be minimized. Generating and providing the ACLs from the MSC_{MODE} with a dynamic creation, the ACLs can be modified and altered not only depending on the RSMODE, but also on time and spatial constraints that the time-triggered MASC backbone interface (wired-wireless) provides.

In the previous paragraphs, the modeling of the MASC policy modules over the MMCS Platform, including the RSMODE Categorization, Operator Profiling and the ACL was presented³⁴. To further ensure the MMCS Platform safety and security all of the other preventive and protective measures of MASC are adopted.

D. MODULES MUTUAL AUTHENTICATION (MMA): Since hardware changes may be triggered on road-side units, the ministry's ITS platform must be allowed to access them through the wireless and the wired backbone and to check whether such actions have occurred.

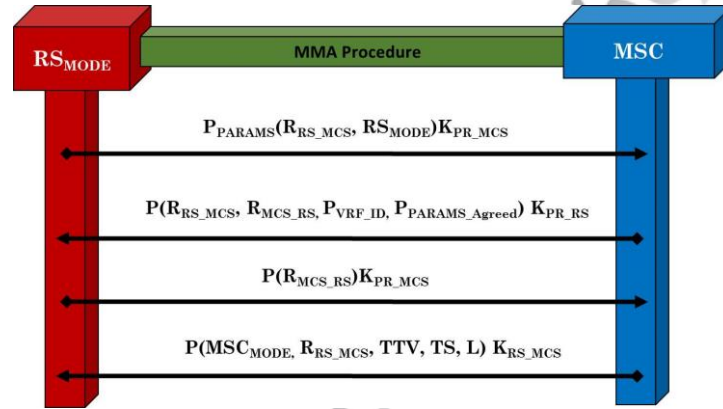
- MMCS hosts a table with all the public keys of the installed road-side units capable of providing ITS services (RSMODE). Each RSMODE keeps a hash of this table as well, enabling it to check for changes and updates.
- On initialization of the platform, the mutual authentication procedure of each RSMODE with the MMCS takes place.
- On receiving the credentials of the Ministry ITS platform operators, MMCS queries the User-Profiling DB, the Access Control List (ACL) for all the RSMODE installed, and the table with the public keys. From this point on, MMCS knows which RSMODE has to be initialized and their respective functionality.
- The next step is the broadcast of a "Hello" type message from the MMCS to all the RSMODE along with their unique IDs so that the mutual authentication can take place.
- The encrypted communication channel is constructed by using two nonces. The nonce R_{RS_MCS} is submitted by the RSMODE and the nonce R_{MCS_RS} is constructed by the MMCS with the use of the session key K_{RS_MCS} .

³⁴ For further details of the three procedures please refer to Chapter 4

- Since all the exchanged messages in the established channel of the communication process must be encrypted, the values that are encrypted in the first three messages can only be extracted by someone having access to the proper private key (K_{PR}).
- After the third message exchange, both sides know the values of the R_{RS_MCS} and of the R_{MCS_RS} so they can create the session key K_{RS_MCS} (e.g. by calculating the hash of $H:(R_{RS_MCS} | R_{MCS_RS})$).

The analysis of the Initialization and the rest of the MMA procedure of MASC are presented in Figure 9.

FIGURE 9: PLATFORM-TO-ROAD_SIDE_UNITS MUTUAL AUTHENTICATION PROCEDURE



The definitions of the variables of the procedure are listed as follow:

- MSC_{MODE} is the MMCS and RS_{MODE} is the Road-Side Unit (modules);
- P_{VRF_ID} is the verified MMCS and P_{PARAMS} are the MMCS encryption parameters;
- R_{RS_MCS} is the random number of the RS_{MODE} to MMCS nonce (same for the R_{MCS_RS});
- TTV is the time-to-vote, TS is the timestamp and L is the lifetime of the session ;
- K_{RS_MCS} is the session key to be used from that point on.

Moreover, if only one of the parties (either the MMCS or the RS_{MODE}) applies the protocol, while the other tries to replay old messages, this act will be traced since the unauthorized party will not be able to present the fresh version of either the R_{RS_MCS} or the R_{MCS_RS} nonce. After the initialization, this step can be periodically repeated to trace possible attacks, guaranteeing the robust and secure continuity of each RS_{MODE} as described in section 5.2.5.

E. MODULES VOTING SYSTEM (MVS): The previous process of the MMA can deliver three possible outcomes:

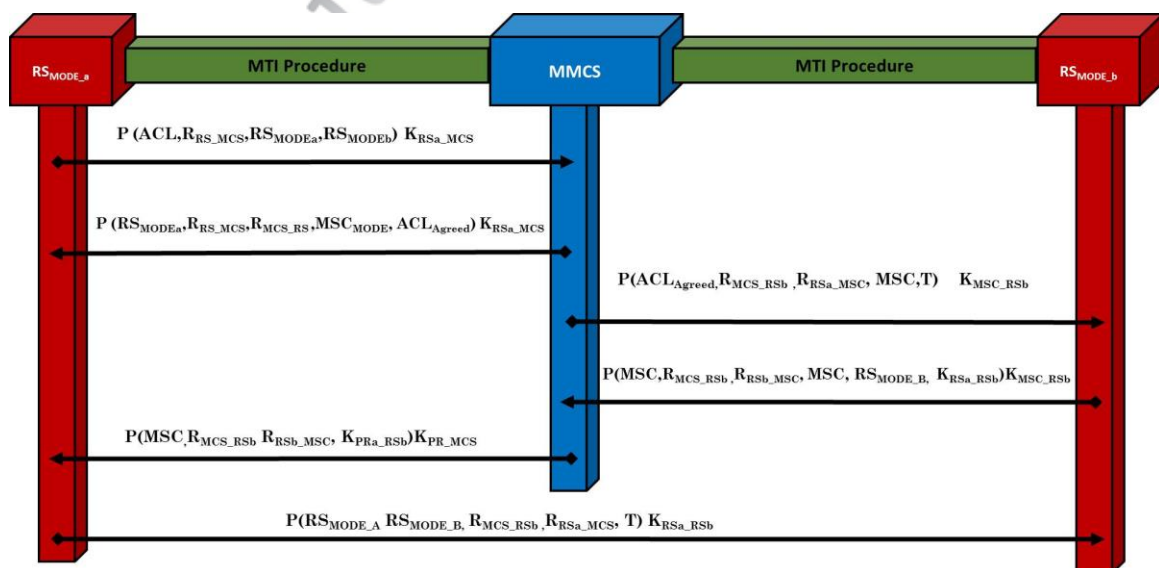
- RS_{MODE} and MMCS are mutually authenticated. Therefore, no other party has been compromised or attacked.
- A number of RS_{MODE} have not been authenticated to the MMCS; therefore there are or there have been under cyber-attacks and exploitation. The RS_{MODE} Categorization is enabled and the data traffic is blocked in both states (primary and secondary). In addition, in the primary state the traditional functions of the RS_{MODE} can be allowed.

- c) The RS_{MODE} has detected that the MMCS is not authenticated and notifies rest of the modules, without notifying the MMCS (to prevent the MMCS from blocking its vote) and returns to the basic default functions (system safe mode and boot).

One could argue that each module has to be authenticated with all the other modules; however, this would increase the number of transmitted messages and the execution time. The rest of the MVS process description is similar to the one described Chapter 4, where the immobilizer is substituted with the MMCS Platform and the automotive module with the RS_{MODE} .

F. MODULES TICKET ISSUING (MTI): After the previous procedures have been completed, RS_{MODE} has been authenticated and the communication and the connection between the modules are authorized. Yet in order to be completely sure for the MMCS continuity of the procedures and functions time constraint policies are being applied. Therefore, RS_{MODE} is allowed only to temporarily communicate with each other. The responsible for the Modules Ticket Issuing (MTI) procedure is the MMCS (Figure 10). Whenever any modules (RS_{MODE}) want to communicate with another module (RS_{MODE} or Vehicle, Personal Station), it must communicate with the MMCS, requesting access permission from the Access Control List (ACL). MMCS checks whether ACL is valid. In case it is, then MMCS issues a ticket T to RS_{MODE} to access $MODULE_2$ (RS_{MODE} , Vehicle or Personal Station). The rest of the MTI process is similar to the one described in Chapter 4, where the immobilizer is substituted with the MMCS Platform and the automotive module with the RS_{MODE} .

FIGURE 10: PLATFORM-TO-ROAD_SIDE_UNITS MUTUAL AUTHENTICATION PROCEDURE



The definitions of the variables of the procedure are listed as follow:

- P is the MTI encryption parameters;
- MSC, RSMODE_A, RSMODE_B are the verified MMCS and Road-Side Units modules ();
- RRS_MCS is the RSMODE (a or b) to MCS random number (nonce);
- KRS_MCS is the session key to be used from that point on (a or b module);
- ACL is the Access Control List
- T is the Ticket

The overall process includes the scenarios outcomes of the SDM procedure as described in the next sections.

5.4 INTEROPERABLE FRAMEWORK UPGRADE

The proposed interoperable and cooperative-ITS framework upgrade is a dynamic operational model that brings together vehicles, road-side units (RSUs) and automotive vendors to define applicable case scenarios of the Service Discovery Mechanism (SDM). The generic procedure that takes place every time that a service is requested is the following:

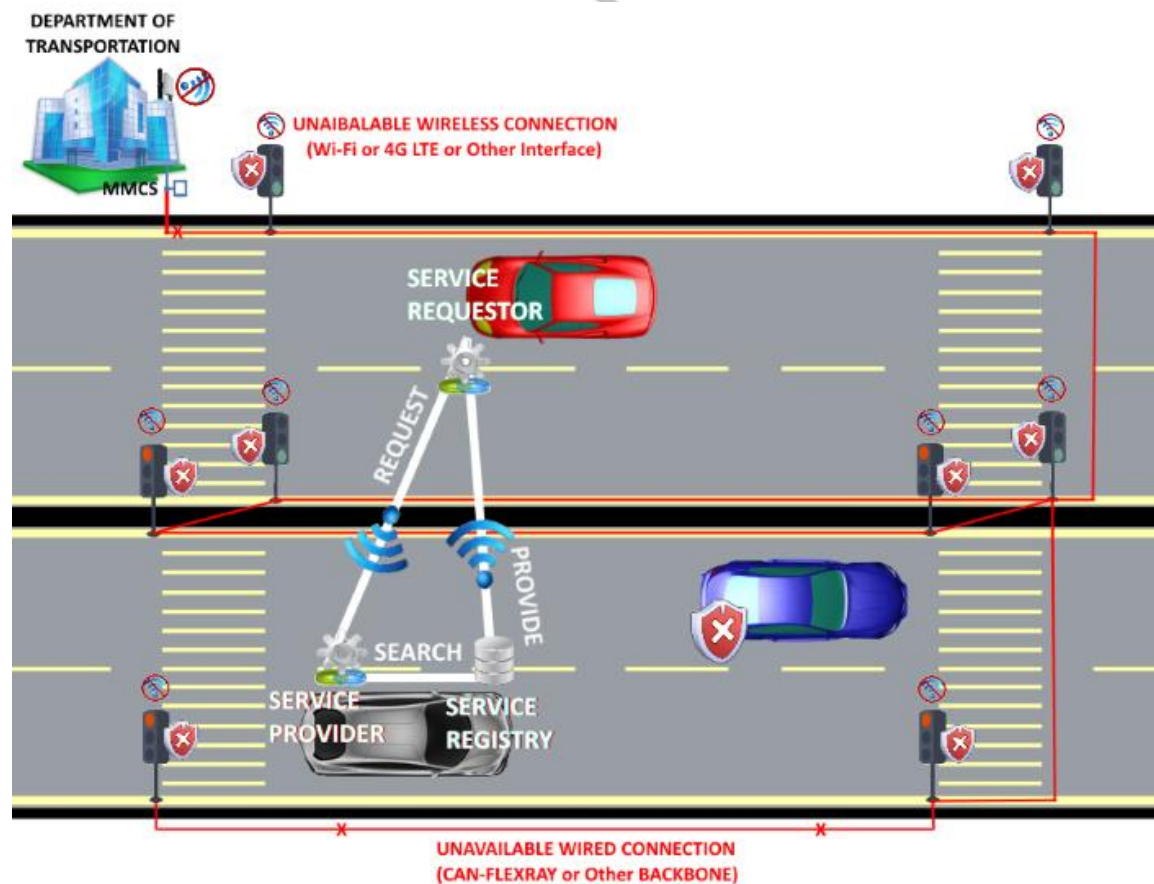
- A client node (Vehicle-Station) which requests for services starts searching for the existing connections among other available online nodes (Vehicle Stations, or nomadic-devices | personal-stations).
- This action is active until the client node finds another node capable of providing the required services.
- Every time a client node connects to another node the proposed operational model is enabled and SDM checks if the requested service is registered.
- If the service registry exists the Service-Requestor filters the provided/exposed service of interest from the Vehicle-Station service provider and consumes it.
- Furthermore, a periodic check of the connectivity status process can be utilized during all phases of the procedure of the established node for communication and exchange of data.

Based on the actual needs for service discovery and consumption over any possible communication medium and network interface, a number of scenarios can be deployed in order to retrieve the interoperable service of interest. These scenarios include the vehicle-to-vehicle (V2V) decentralized SDM and the vehicle-to-infrastructure (V2I) centralized SDM implementing a plethora of sub-scenarios (cases) concerning the methods of the interoperable service publication and consumption over the high mobility environment (i.e. highway). All these scenarios and cases, as presented in the next sections, highlight the requirements and the capabilities that need to be standardized in the proposed framework update to ensure interoperability, ease of integration, portability and robustness of the environment as the pre-step to establish a sustainable transportation domain.

The V2V Decentralized SMD can be applied in a transportation environment where no other centralized ITS-stations exist or the entire infrastructure is not operational for security or maintenance reasons. More specifically, during the progress of the decentralized SDM scenario, two cases of the SDM procedures can occur between two vehicles or between more than two vehicles with a random selected leader hosting the Service Registry.

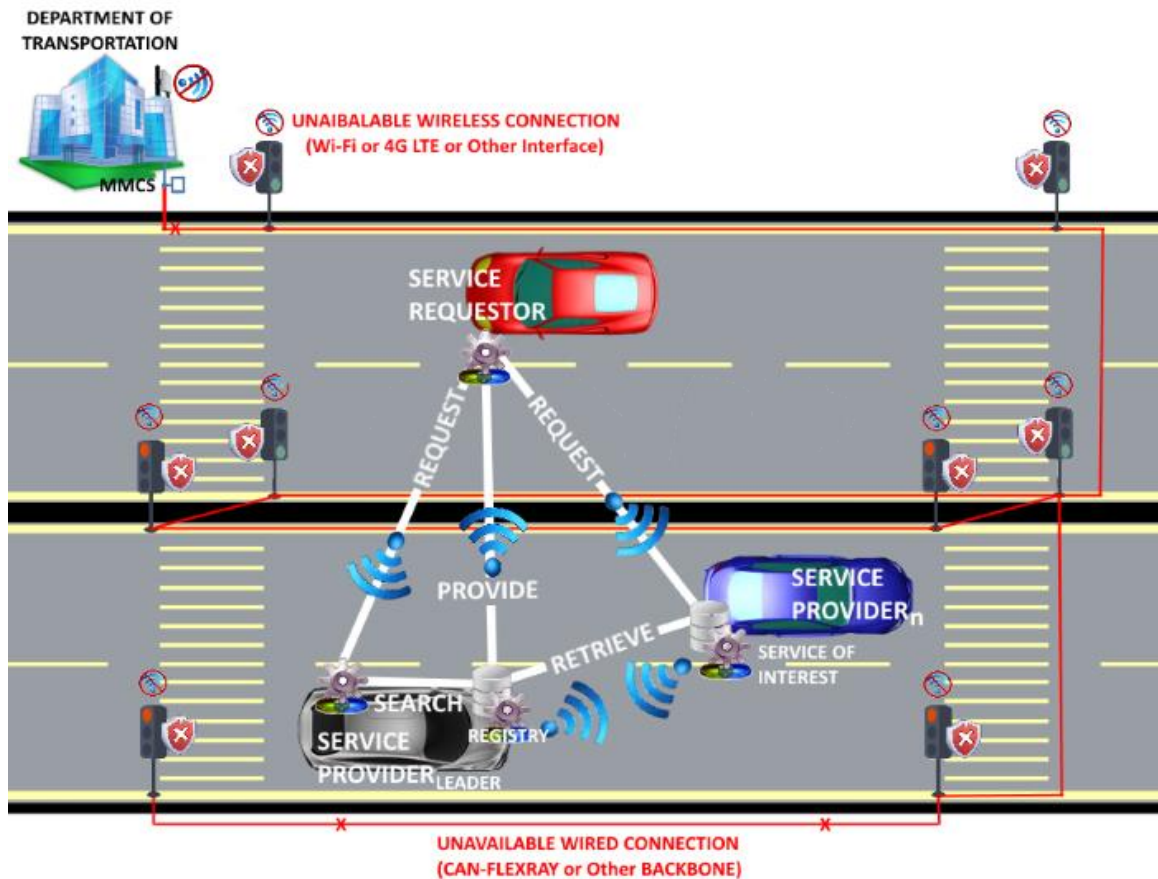
- Case I: In the first case of the decentralized SDM procedure (Figure 11), two secured vehicles exchange services based only on the up-to-that moment updated Service Registries. This means that an interoperable service of interest cannot be obtained unless a vehicle is already equipped with it (e.g. factory-default installation, already retrieved version from the trusted authority's repository) and responds to that specific request. In addition, during this process utilizing the available network bandwidth, protocols can be applied for the peer-to-peer data sharing to distribute the interoperable-services (e.g. similar to bit-torrent or µtorrent). Thus the interoperable service can be efficiently obtained from more than one vehicle if the previous state is true (applied).

FIGURE 11: CASE I - V2V DECENTRALIZED SDM SCENARIO A



- Case II: In the second case (Figure 12) a randomly selected vehicle from a group of vehicles undertakes the leading role of the road-side modules to hold the Service Registry. In this case, the group leader of the process retrieves and temporarily stores the service of interest from another vehicle or from a nearby personal station node (V2V advanced efficiency and performance case). The previous mechanism of P2P data sharing can be applied as an optimized method for retrieving the interoperable service.

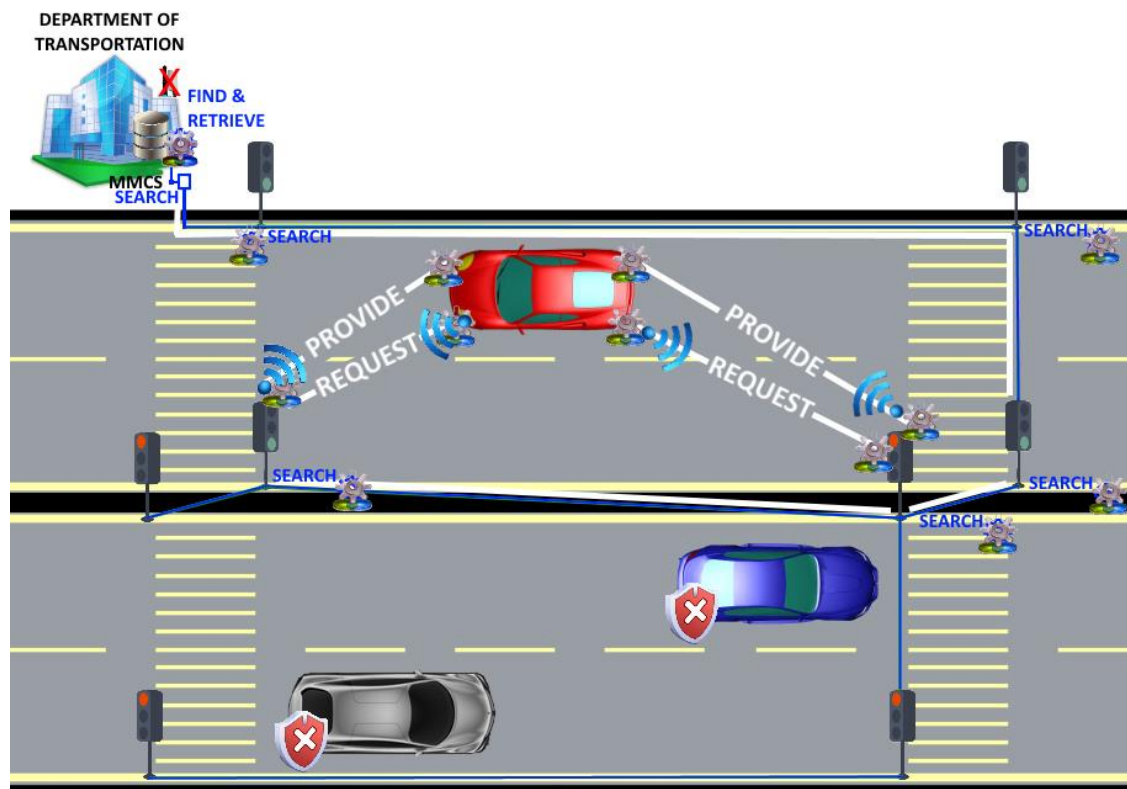
FIGURE 12: CASE II - V2V DECENTRALIZED SDM SCENARIO A



The V2I Decentralized SDM takes place between vehicles, road-side units (RSU) and nomadic devices.

- Scenario B – Case I: The first case of the V2I scenario (Figure 13) takes place between a vehicle (SREQ) and the RSU (SPRO) hosting the Service Registry (SREG) in a specific region of interest. All the services are retrieved from the TRA repository utilizing exclusively the hardwired backbone of the infrastructure. The rest of the SDM procedure between the SREQ and SPRO operated in wireless mode. This case states that the entire wired backbone structure is properly operating but the wireless backbone mode (from the TRA portal) is unavailable for security or maintenance reasons.

FIGURE 13: CASE I - V2V CENTRALIZED SDM SCENARIO B



- Case II: The second case of the V2I scenario (Figure 14) takes place between a vehicle (S_{REQ}) and the RSU (S_{PRO}) hosting the Service Registry (S_{REG}) and a group of other vehicles which have already stored the service of interest. In this case, S_{PRO} retrieves the service of interest in order to publish the service to S_{REQ} taking advantage both wired and wireless connections for an optimized and efficient SDM procedure.
- Case III: The third case (Figure 15) of the V2I scenario takes place, between a vehicle (S_{REQ}), the RSU (S_{PRO}) hosting the Service Registry (S_{REG}) and a group of other vehicles (S_{PRO}) which have already stored the service of interest. In this case the S_{PRO} retrieves the service of interest in order to publish it to the RSU taking advantage only of the wireless backbone of the ITS infrastructure. This case takes place when the wired backbone is unavailable for security or maintenance reasons.

In addition, in both cases II and III of scenario-B where a support group of vehicles participates, the nomadic devices (Personal Stations) can also be added to the proposed model supporting the SDM procedures. Furthermore, a periodic check of the connectivity status process can be utilized during the process for establishing the node for communication and exchange of data. The protocol utilizing the available network bandwidth is applied for the optimized peer-to-peer data sharing to distribute the interoperable-services. The nomadic devices are considered as personal-stations with roles similar to the ones of vehicle-stations.

FIGURE 14: CASE II - V2V CENTRALIZED SDM SCENARIO B

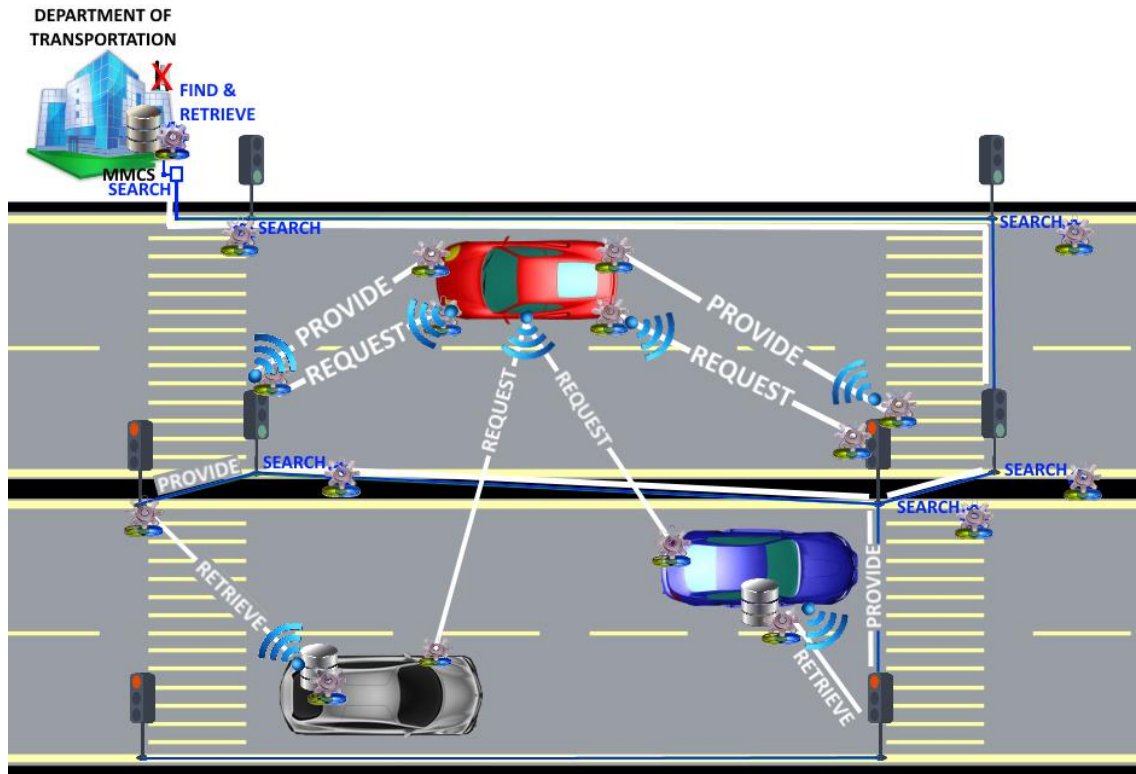
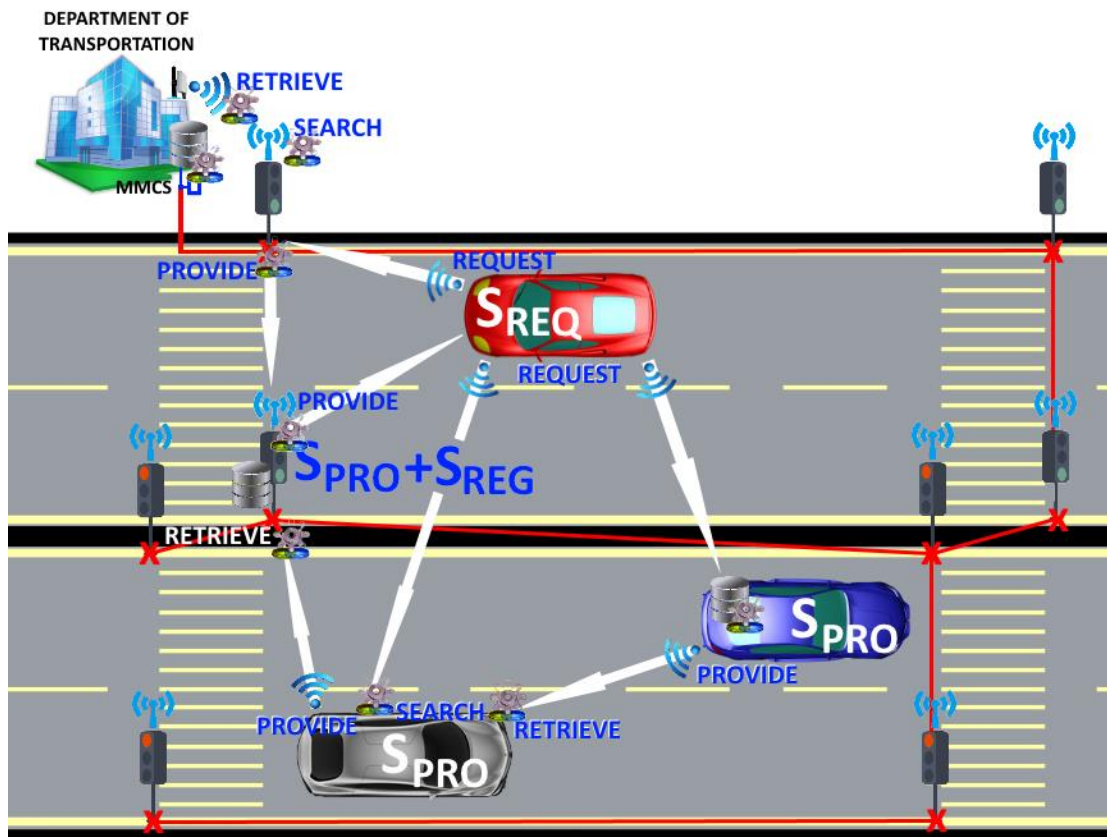


FIGURE 15: CASE III - V2V CENTRALIZED SDM SCENARIO B



5.5 CONCLUSIONS

Existing technological trends were used to establish communication between a source and a target entity [37][38]. In this chapter, an interoperable but still cooperative ITS framework upgrade with the form of a patch was presented. The proposed operational model enabled the search-discover-provide process of SOA in real-time ITS applications. The proposed framework [15][16] introduces the use of an embedded Module Management Control System that is able to undertake the management control of the entire ITS platform (elements and infrastructure) and thus to improve the quality of the provided services. Nevertheless, because security must not be neglected, a modified version of MASC [35][36] is proposed to be implemented in the updated framework. All of the MASC procedures and interoperable and cooperative ITS scenarios of the SDM are described in detail. Thus, the proposed solution is transformed into a functional approach of a service finding model for searching, finding and publishing services offering security and interoperability between the already defined cooperative ITS-entities and ensuring that the transportation cyberspace is equipped with the capability to share and deliver efficiently information, applications and services.

Any type of implementation of the proposed dynamic operational model, including the presented SDM, may vary on the level of technical design or operation, so that more than one of the already presented cases of scenarios can be added. This kind of utility computing based on the service provisioning model could be easily available on demand, transforming vehicles into autonomous networking nodes.

REFERENCES

- [1] World Commission on Environment and Development (1987), *Our Common Future*, Oxford University Press, ISBN 019282080X
- [2] Homeland Security, Transportation Systems Sector [Online] <http://www.dhs.gov/transportation-systems-sector>
- [3] ETSI, Cooperative ITS, [Online] <http://www.etsi.org/technologies-clusters/technologies/intelligent-transport/cooperative-its>
- [4] ETSI/TR | 101-607, ITS, C-ITS, release 1, [Online] http://www.etsi.org/deliver/etsi_tr/
- [5] ETSI/EN | 302-665 v1.1.1 European standard ITS [Online] http://www.etsi.org/deliver/etsi_tr/
- [6] E.C, Enterprise and Industry, Modernizing ICT standardization in the EU-the way forward, [Online] http://ec.europa.eu/enterprise/newsroom/inf/itemdetail.cfm?item_id=3263
- [7] CISCO, Internet of Everything [Online] <http://www.cisco.com/web/about/ac79/innov/IoE.html>
- [8] T. O'Reilly, J. Battelle, Web squared: Web 2.0 five years on (2009) [Online] http://assets.en.oreilly.com/1/event/28/web2009_websquared-whitepaper.pdf
- [9] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger and Dawn Leaf, NIST Cloud Computing Reference Architecture, 2011, Available: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909505
- [10] iMobility support, 3rd eSafety forum [Online] <http://www.imobilitysupport.eu>
- [11] ITU Webpage [Online], "The Fully Networked Car", International Motor Show WorkShop, 2005, 2007-2010. [Online] <http://www.itu.int/ITU-T/worksem/ict-auto/>
- [12] J. Jozczuk–Januszewska, *Development Trends in Intelligent Transport Systems in Respect to Environmental Protection*, Springer-Verlag Berlin Heidelberg, ISBN 978-3-642-16472-9, 2011
- [13] H. Fuhs, *Hybrid Vehicles and the Future of Personal Transportation*, CRC Press, 2009
- [14] Standardization Activities for Intelligent Transport Systems. ITU-T Technology Watch Report, 2008, [Online] http://www.itu.int/dms_pub/itu-t/oth/23/01/T2301000080002PDFE.pdf
- [15] K. Dellios, A. Chronakis, D. Polemi, Transforming Vehicles into e-Government Cloud Computing Nodes, *Global Security, Safety and Sustainability*, Springer Link, LNICST Vol. 99, 2012, pp.1-8.
- [16] K. Dellios, D. Papanikas, D. Polemi, A Service Discovery Mechanism for the Cooperative Intelligent Transport System (2014), *World Review of Intermodal Transportation Research Journal*, vol 4, pp. 259-279.
- [17] K. Dellios, D. Papanikas, Information Security Compliance over the Intelligent Transport Systems: Is IT Possible, *IEEE Security & Privacy*, 2014 (accepted for publication)
- [18] Java™ Platform, Standard Edition 6 API Specification, [Online] <http://docs.oracle.com/javase/6/docs/api/>
- [19] IBM, Transaction Strategies: The API Layer Strategy, [Online] <http://download.boulder.ibm.com/ibmdl/pub/software/dw/java/j-ts3-pdf.pdf>
- [20] SOA, Service Oriented Architecture [Online] <http://www.w3.org/TR/ws-arch /SOA>
- [21] W3C, Web of services, [Online] <http://www.w3.org/standards/webofservices/>
- [22] XML schema specifications, [Online] <http://www.w3.org/TR/xmlschema-0/>
- [23] WSDL specifications, [Online] <http://www.w3.org/TR/wsdl>
- [24] SOAP specifications, [Online] <http://www.w3.org/TR/soap/>
- [25] UDDI specifications, [Online] <http://uddi.xml.org/>

- [26] Graham, Davis, (2005) Building Web Services with Java: Making Sense of XML, SOAP, WSDL and UDDI, Sams Publishing
- [27] K. Kurbel, (2008) The Making of Information Systems; Software Engineering and Management in a Globalized World, Springer
- [28] Hirsch, Kemp, (2006) Mobile Web Services: Architecture and Implementation, John Wiley and Sons
- [29] W3C, Internationalization of web service, [Online] http://www.w3.org/standards/techs/i18nwebofservices#w3c_all
- [30] IBM UDDI4J specifications, [Online] <http://uddi4j.sourceforge.net/>
- [31] Apache jUDDI specifications, [Online] <http://juddi.apache.org/>
- [32] Python UDDI4Py Specifications, [Online] <http://www.ibm.com/developerworks/library/ws-uddi4py/index.html>
- [33] Perl UDDI Lite RPM resource, [Online] <http://rpmfind.net/linux/rpm2html/>
- [34] Ruby UDDI4R specification, [Online] <http://uddi4r.rubyforge.org/>
- [35] C. Patsakis, K. Dellios, Securing in-vehicle communication and redefining the role of automotive immobilizer. International Conference on Security and Cryptography (SECRYPT), 2012, pp 221-227
- [36] C. Patsakis, K. Dellios, M. Bourouche, Towards a distributed secure in-vehicle communication architecture for modern vehicles, Computer and Security, Elsevier, vol. 40, Feb. 2014, pp 60-74
- [37] ITS results from the Transport Research Programme, [Online] http://www.transport-research.info/Upload/Documents/200406/20040617_110730_48976_its.pdf
- [38] E. Curry, B. Guyon, et al, Developing a sustainable IT capability: Lessons from Intel's Journey, 2012, [Online] http://www.edwardcurry.org/publications/MISQE_SustainableIT_Intel_2012.pdf
- [39] B. Vlastic, Smart Cars Get a Connection Test in Michigan The New York Times, (2012) [Online] http://www.nytimes.com/2012/08/22/business/a-test-of-smart-cars-gets-under-way.html?_r=0

6. A SUSTAINABLE 'TRANSPORT CLOUD' SYSTEM

A step beyond the vision of autonomous networking vehicles that provide interoperable and cooperative ITS services and applications is the need of a sustainable form of computing capable to host the entire transportation domain. Recent ICT advances allow modern forms of computing to provide a sustainable environment not only for the automobiles or the decentralized, heterogeneous Intelligent Transport Systems but for the entire Transportation Domain. In this chapter a cloud system specifically to interact with the rest of the cyberspace designed for the transport environment is presented. The architectural design of the proposed legacy transport system is based on a cloud computing model capable of hosting the interoperable and cooperative ITS services and the entire transportation domain.

6.1 MOTIVATION AND CONTRIBUTION

The transportation domain is linked with the sub-sectors of highway, railway, maritime (seaports) and aviation (airport) and provides to all citizens secure and safe transports. Furthermore, the transportation domain is also linked with the communication, emergency services, information technology, government and commercial facilities, energy and critical manufacturing sectors. Therefore, the transportation domain is not only one of the most important sources of revenue inflows and nationwide strategies development, for both the automotive industries and global economy, but also it is placed among the Critical Infrastructures [1].

In addition, modern ITS development strategies as presented in [2][3] recognize the critical role of Information and Communication Technology (ICT) for productivity and innovation and the influence they have on other domains. Current Intelligent Transport Systems (ITS) and Information and Communication Systems (ICS), including network, hardware, software and human resources, are characterized by growing complexity and a plethora of electronic services distributed in various locations (i.e. rooms, buildings, cities). All of these systems interact and interwork with numerous cyber-entities, have a large number of users (i.e. internal, external administrators, users and providers), and host 'Big Data' related to all types and kinds of provided and exchanged transportation services. In addition, the automotive industries are still trying to fully adopt the vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications, driving business development in demand for interoperable and cooperative automotive and ITS services and applications. However, any kind of degradation, interruption or impairment of the ICSs has serious consequences on business continuity, on loss of reputation and services, on financial profits and on safety and security management.

Unfortunately, the automotive industries have overlooked two important considerations: a) the need of IT reference architectures and business models in the transportation domain as without these in place, the vehicle and b) the ITS as a ubiquitous form of computing. In addition, there is also the trend where the driver and the passengers need to access the features (applications and services) of their smart devices within their vehicles, generating very strong consumer forces that drive the automotive industries to respond. Therefore, a vehicle to everything (V2X) communication model or any other model capable of implementing the standards and the functionality of the cyber nature of the transportation domain needs to be introduced, integrating all the existing systems (such as the Advanced Driver Assist Systems- ADAS and Cooperative Adaptive Cruise Control - CACC). Unfortunately, the automotive industries have paid little attention to confront the numerous integration and implementation issues and now they are forced to face the challenge of a highly dynamic and constantly transformed environment. Simultaneously, the various constraints of interoperability, compatibility, cooperativeness, security and safety, presented in the previous chapters, generates the need for a 'legacy transportation system' [4] capable of hosting and providing sensitive data and interacting securely with other complex and heterogeneous systems.

Driven by this motivation a perspective beyond the traditional ICSs' utilization needs to be adopted. The 'legacy system' related with the transportation domain must be a reliable, efficient and sustainable ICS [5], delivering the new levels of interoperable and cooperative services and applications to drivers, passengers and vehicles in secure ways (Chapters 4 & 5). The contribution of this chapter; the 'iTransport Cloud', lies in the effort to establish a cloud ontology [9] and deep understanding of how to approach very large-scale environments with evolving computing forms and design efficient systems with interactive portals for both ITS services and applications. This task states that all transportation related elements depend on the deployment of a main server-side system and the roadside-client communication mechanisms in order to pervade every aspect of the 'networking vehicle' over a harmonized cloud architecture model [6][7][8]. The digital frontiers of the cyberspace and the strategic approach for the creation of the cloud environment are also defined.

6.2 CLOUD PRINCIPLES AND FUNDAMENTALS

As already mentioned in previous chapters, the new emerging technologies have changed the way communications between the ITS entities is established and data are exchanged. Through time numerous solutions for the IT service delivery have been proposed including:

- i. The virtualization technology [10], which is the creation of virtual resources in two main areas, storage and server virtualization. Storage virtualization refers to the pooling of physical storage from multiple network storage devices into a single one

known as a Storage Area Network (SAN) [11] and the server virtualization handles the resource sharing, utilization and future storage expansion of server.

- ii. Grid Computing [12] has been proposed for sharing unused processing cycles of networking terminals into a single network for the solution of individual problems or for intensive and complex projects over any geographical area or distance.
- iii. Lately, Cloud Computing, a hybrid technology of virtualization and grid computing [13] is already embraced by enterprises, industries, IT professionals and expertise. Cloud Computing provides hardware resources, platforms and software as services in order to be consumed by anyone anytime. It is the model for enabling ubiquitous, convenient, on-demand network access and provision to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) with minimal management effort or service provider interaction [14][15].

On Gartner's 2012 Hype Cycle of Emerging Technologies [24], Nerval Lobster mentioned that cloud computing will grow the next years and it will be serious important to consider whether or not to transit into a 'Cloud'. Nowadays, cloud computing has already transformed the traditional way that most of the computational tasks, the ICS and the services are developed, delivered and managed.

The main delivery (service) models currently used and commonly referred as defined by NIST [13] are:

- i. Infrastructure as a Service (IaaS) is the basis platform virtualization environment with storage and networking capabilities, where the cloud infrastructure services deliver the computer infrastructure. It is defined by NIST as “the capability provided to the consumer to provide processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications”.
- ii. Platform as a Service (PaaS) facilitates the deployment of applications, enabling the developers to create applications inside the cloud. It is defined by NIST as “the ability to provide a computing environment and the related development and deployment stack needed to deliver a solution to the consuming customer”.
- iii. Software as a Service (SaaS) is the front-end model that delivers software over the Internet, eliminating the need to install the application. It is defined by NIST as “the capability provided to the consumer to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser”.

The above CC delivery models offer the following important features:

- i. On-demand self-service: The users can obtain direct computing resources via any secure network-capable terminal. It is the ability to provision computing capabilities, such as server time and network storage as needed, automatically without requiring human interaction with each service's provider.
- ii. Flexible broad network access: Capabilities are available whenever accessed through standard internetworking mechanisms, supporting the main objective of interoperability based on the principle of plug-n-play.
- iii. Resource Pooling: Computer resources (e.g. storage, memory, network bandwidth and VMs) are used to serve multiple users dynamically and they are assigned on demand. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demands.
- iv. Virtualization: Virtual system grouping and sharing resources with multi-tenancy techniques.
- v. Rapid elasticity: The capabilities available can be rapidly and elastically provisioned to quickly scale out, rapidly released to quickly scale in and can be purchased in any quantity at any time.
- vi. Scaling: either horizontal scaling - referring to the increasing computational resources in order to fulfill the loading (data) requirements (virtual servers), or vertical scaling - referring to the adding of resources in the existing server (e.g. upgrading, replacing unit parts or the whole unit).
- vii. Dynamic Scalability: It is separated into proactive and reactive scalability; proactive scalability deals with scheduled changes of infrastructure based on the needs and requirements of an organization expected, while reactive scalability balances the infrastructure needs under current situation demands.
- viii. Measured Service: Cloud computing systems incorporate capabilities for measuring storage, processing power, bandwidth, and user account activity in order to automatically control, adjust and optimize the use of system resources by leveraging a metering capability. Therefore, resources can be monitored, controlled, and evaluated providing transparency for both the provider and the consumer of the utilized service.

The following deployment models are currently used:

- i. Private Cloud: Exclusively used by multiple users within the digital limits of a single environment. Private clouds are not considered as part of cloud computing by some authors and academic institutes (i.e. Reese, O'Reilly, Berkley)

- ii. Community Cloud: Exclusive use for a specific community of users, enterprises and/or organizations sharing common interest.
- iii. Public Cloud: For open use by the general public; owned by business, academic, governmental organizations or enterprises or even a combination of the above.
- iv. Hybrid Cloud: A composition of two or more distinct cloud infrastructures (private, community, or public), enabling information (data) and service (software/application) portability (e.g. cloud bursting between clouds).

All of the above presented dynamic properties can help overcome the existing limitations of the traditional ICS [16][17][18] and interact with cloud-enabled services (i.e. e-mail, social media, on-line gaming and mobile applications) while reducing the financial costs, the energy consumption and the carbon footprints [6][7][8] and improving the total ICS agility. Therefore, cloud computing can be utilized for the creation and the design of an “iTransport Cloud” system, exploiting all the technological resources from land, marine and aerial, dynamic, static and collaborative infrastructures, systems and resources.

FIGURE 16: OPEN CLOUD PROJECTS



Furthermore, there exist many open cloud projects [19] (Figure 16) that could be used in the design of the ‘iTransport Cloud’ system. For instance, the Ubuntu OpenStack [20][21] is an open project for large scale deployments, under any existing IT infrastructure of automatically provisioned virtual computing and delivery services. Eucalyptus [22] is used for deploying Infrastructure as a Service (IaaS) layers with scalable cloud resources for networking and storing. OpenNebula [23] is an open toolkit for constructing any type of cloud environments for managing complex services.

6.3 THE ‘ITRANSPORT CLOUD’ SYSTEM

Beside the motivation as previously presented, the author’s original vision of the ‘iTransport Cloud’ system derives from the concept of the sustainable development report ‘Our Common Future’ [5]. The report proposes that in order ‘to meet the needs of the present you must not

compromising the ability of future generations to meet their own needs'. It also proposes that 'any kind of sustainable development must emphasize the need to create the conditions for better quality of life for everyone, now and for future generations' and highlights three main components to sustainable development; the social equity, the environmental protection and the economic growth. These three components can be translated into three sophisticated principles and mandate a development process, a technological orientation, asset interaction and the generation of conditions for better satisfaction of human needs and aspirations now and in the future.

Adopting new forms of synchronous and emerging computing due to the need of utilizing intelligent, cost-saving and energy-efficient multi-modeling systems in order to facilitate complex and heterogeneous ITS is the application of the principles. In specific, cloud computing is the collaborative model capable to provide on-demand resources and utilities via an independent distributed network and over any type of technological platform. It is the new cloak of the cyberspace deployed to deliver 'iTransport' services, while collecting, storing and analyzing data that allow the research community to develop and implement such a sustainable framework. In addition, the interoperable and cooperative-ITS services and applications can be hosted or created, deployed, delivered and consumed in a cost-effective manner overcoming a global economic and financial crisis.

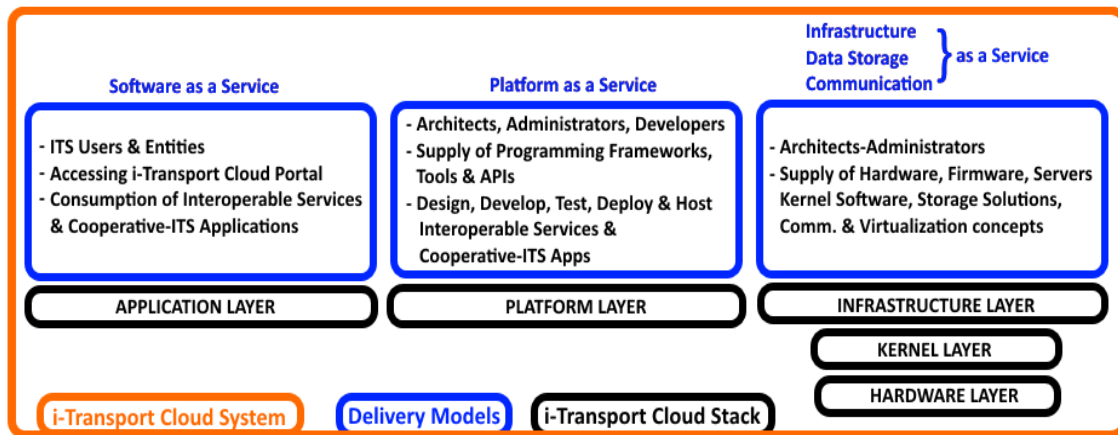
The proposed 'iTransport Cloud' Stack and Reference Architecture [53][54][55] are presented as follows.

6.3.1 'iTRANSPORT CLOUD' STACK ANALYSIS

This section describes the stack layers of the 'iTransport Cloud' in terms of application, software and platform environments and hardware infrastructure. The proposed 'iTransport Cloud' stack and reference architecture model (Figures 17 & 18) are presented and illustrated in detail.

The architecture analysis includes the main components that the IT architects need to utilize for building the 'iTransport Cloud' system. The bottom layer of the stack is consisted of the hardware layer which is the physical component of the 'iTransport Cloud' stack. The top layer of the 'iTransport Cloud' stack is consisted by the Application layer. The Application layer is the interface and interconnection of the proposed system with other systems, services and applications (interoperable and cooperative) acting as the digital frontier to the rest of the transportation cyberspace.

FIGURE 17: THE 'ITRANSPORT CLOUD' ARCHITECTURE MODEL



The five stack layers of the proposed i-Transport Cloud reference architecture [53][54][55] are described in details:

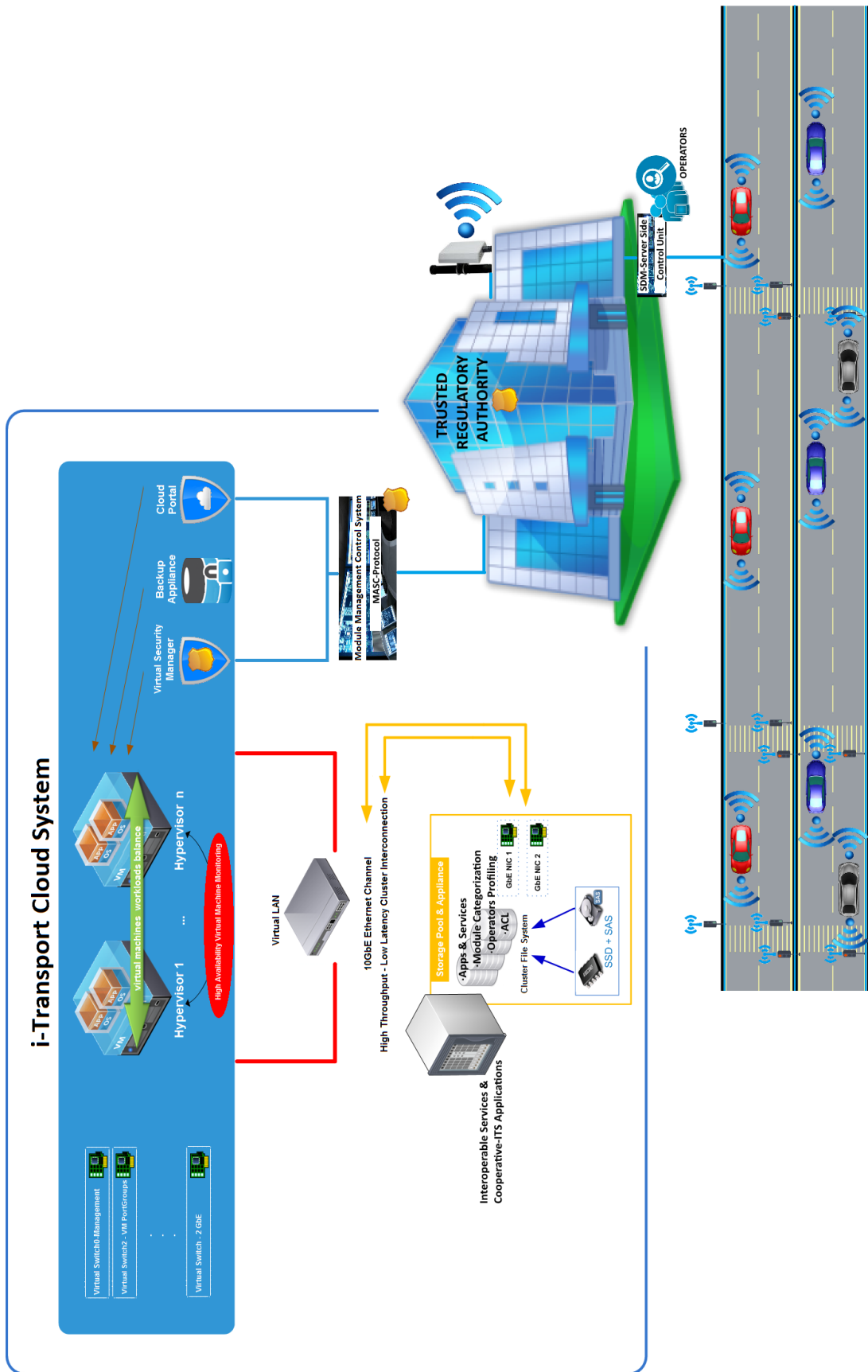
- I. 'iTransport Cloud' Hardware (5th) Layer: It is the physical hardware/firmware including the ITS, the physical infrastructures and the facilities. This layer forms the backbone of the stack including both server(s) and storage solutions used in cases governments, organizations or ministries are investing in data-centers and IT infrastructure. The storage solution consists of Solid State Drives (SSDs) [25] which provide reliable, high performance Serial Attached SCSI [26] (SAS) [27] storage solution. The SAS interface with SSDs is used as it is designed for I/O-intensive demanding environments, such as the transportation domain, for high performance computing (HPC) [28][29][30] and video on demand (VOD), even in cases of large-scale data-centers for mission-critical applications [31][31]. A virtual switch is also included in the hardware layer. The Virtual Switch [32][33][34][35] is a crucial component of the server firmware. The hardware layer also includes the data center management and the power consumption optimizations [36].
- II. 'iTransport Cloud' Kernel (4th) Layer: The kernel layer provides the software kernel to be implemented as an OS Kernel, the hypervisor, the Virtual Machine (VM) monitoring and the cluster middleware. It is responsible for memory management, process management, task scheduling and disk management [37][38][39][40]. The Kernel Layer includes the software interface for hosting three major components; the hardware, the guest systems and the console operating system. It also adds a management interface for the interaction of the core server system and the VMs running on the server.
- III. 'iTransport Cloud' Infrastructure (3rd) Layer: It is the layer that provides resources to the other layers of the cloud stack for the construction and the generation of new

transportation cyber-environments. The ‘Transport Cloud’ services of this third layer can be categorized into:

- computational resources (IaaS), that include virtualization hardware-assisted virtualization concepts as a form for providing the users and the entities’ computational resources;
- data storage as a service (DaaS), that allows users and entities to store their data and access them anytime from any place;
- scheduled and reliable communication capability as a service (CaaS), that includes traffic isolation, dedicated bandwidth, communication encryption and network monitoring.

In specific, the data-storage helps the administrators to develop a virtualization deployment of storage choosing proper storage protocols for achieving better throughput to meet the storage requirements [40][41][42]. The distributed storage manager is based on storage I/O and capacity within a cluster virtual machine and enables VM load balancing of the workloads based on CPU and memory resource utilization. The Virtualized cluster system is a high-performance cluster system that provides storage virtualization. It is optimized for virtual machines and for efficiently storing the entire virtual machine state in a central location. The VM is defined as a host machine and a software-based virtual datacenter for delivery, provision and consumption of storage services with automated control. Therefore, it can support virtualization-based distributed infrastructure services. The Tiered Storage [43] allows you to consolidate and deploy different types of storage within the same network-attached storage (NAS)-based system [44]. The Communication Capability includes the network interface controller (NIC) [45] which acts as the basic standard for a full network protocol stack. NIC allows communication of the physical and data link layers between groups of the same LAN and large-scale network communications through routable protocols (i.e. IP) [46]. Furthermore, the NIC virtualization provides information on the NIC functionality for the virtual LAN (e.g. 10Gb Ethernet channel) [47][48] that allow the sharing of a single 10 GbE network port and owns a virtual MAC that provide statistics per server on Transmitted/Received (Tx/Rx) traffic. The Link Aggregation Control Protocol (LACP) [48][49] for Gigabit Interfaces configures the Gigabit Ethernet port channels [50] and it allows the bundling of multiple Gigabit Ethernet links into a single logical interface on a router. It is defined by the IEEE 802.3ad [51] specification aggregation of multiple link segments standard. In addition, the virtual switch is the software service that allows one virtual machine to communicate with another. It forwards data packets and communicates directly by inspecting these packets before passing them forward. The Hypervisor (virtual machine monitor) is a piece of computer software, firmware or hardware that can generate and host other virtual machines [52].

FIGURE 18: THE 'TRANSPORT CLOUD' SYSTEM



- IV. 'iTransport Cloud' Platform (2nd) Layer: The Platform layer includes the tools to integrate service provisioning and to allow administrators and architects to develop complex automation tasks. This layer is responsible for delivering also the Service Level Agreements (SLAs) to all the applications. Software developers of the second layer are supplied with programming framework environments and APIs to develop and deploy the 'iTransport Cloud'-enabled interactive and scalable applications and services.
- V. i-Transport Cloud Application (1st) Layer: The Application Layer is the top layer of the proposed Stack. It provides the end-users access to the deployed services through the exclusive i-Transport Cloud Portal.

6.3.2 'iTRANSPORT CLOUD' DELIVERY MODELS

The above presented 'iTransport Cloud' Stack Layers (hardware, kernel, infrastructure, platform and software) as seen in Figure 17, are utilized in the design of the 'iTransport Cloud' System (Figure 18). For the delivery of any type of the i-Transport Cloud Services, the delivery models must be defined and implemented in the initial design of the i-Transport Cloud stack and architecture. This section includes the detailed description and definition of the three delivery models in order to provide and deliver to end-users/entities interoperable and cooperative-ITS services and applications. In addition, the term "services" in a i-Transport Cloud environment describes how a vehicle or any other network-capable electronic device can use on demand computation assets provided by other vehicles or from the original legacy system in the continued effort to transform automotive vehicles into fully autonomous cloud nodes. The 'iTransport Cloud' delivery models include:

- I. 'iTransport Cloud' Infrastructure as a Service: The 'iTransport Cloud' Infrastructure is the bare hardware deployed in the i-Transport Cloud facilities|infrastructures. More specifically, it is deployed in the hardware, kernel and infrastructure layers of the 'iTransport Cloud' Stack and it is responsible for providing server, storage, networking and load balancing services and system management of a regionally-defined ITS environment. The 'iTransport Cloud' infrastructure and the hardware can also derive from the already used infrastructure of the domain and they can be refurbished, reconfigured and reused. The Utilization or the collaboration of other sectors related to the transportation domain (e.g. aviation, maritime, rail) must not be excluded. In addition, it is the type of service that can offer the hardware infrastructure of a vehicle (e.g. on-board memory, GPS receiver) to users that do not have the same hardware capabilities in their vehicles.

- II. 'iTransport Cloud' Platform as a Service: It is the backplane platform where all the 'iTransport Cloud' applications are developed. It provides the tools for application design, development, testing, deployment and hosting of the 'iTransport Cloud' application solutions and the integration of existing systems. Known business models/standards can be followed for the creation of a fully customizable platform enabling the database integration, security, scalability, storage and management. Even the fully networked vehicle could deliver an integrated set of software and hardware that a developer needs in order to build an application for both software development and runtime. Some of the i-Transport Cloud platform essential modules are: operating system(s)/platform(s), databases, development tools (e.g. Java runtimes and web servers).
- III. 'iTransport Cloud' Software as a Service: While vehicle applications are stand-alone applications, companies who want to offer a portfolio of next generation vehicle applications will increasingly rely on shared services between vehicles (e.g. governance, account management, workflow, single-sign-on, social networking). The 'iTransport Cloud' software is the delivery model where the software and the applications are deployed and provided to users and vehicles on demand. The 'iTransport Cloud' Software delivery model related with the stack as seen in Figure 17 is the top layer, leading to the creation of new generation cross-border and trustworthy 'iTransport Cloud' services as described below:
- Communication services with all the ITS entities; e-information and status, administrative procedures, communication with authorities, authentication and monitoring, navigation and management services;
 - Logistics services that provide logistics operations such as e-orders, e-invoicing, e-payment, e-tracing, e-reservation;
 - Integration services that deliver customs declarations to borders, controls integration with ITS or other government authorities;
 - e-health and e-tourism services.
- IV. 'iTransport Cloud' Communication as a Service: Automotive vehicles with internet access can be used by vehicle users to obtain internet service (e.g. e-mail, RSS feeds) or even act as the gateways for users to gain access to any other network or the Transportation Domain. Treating traditional vehicle services and cooperative-ITS applications (e.g. navigation, traffic, warning and weather information), as 'iTransport Cloud' services, an enhancement in terms of functionality, interoperability and cost effectiveness can be achieved. Specifically, this innovative point of view can enable e-government to offer and provide innovative traffic information and management (cooperative traffic information & forecasting, dynamic

free parking space information, location based information and warning), safety and security (e.g. hazard warning, theft recovery, tracking and trace, emergency calls) or comfort (e.g. future adaptive cruise control systems and infotainment systems with music/video on demand or business information) 'iTransport Cloud' services.

6.3.3 'iTRANSPORT CLOUD' DEPLOYMENT MODELS

The Cloud Computing can be exploited for building various types of 'iTransport Cloud' Models and deliver the 'iTransport Cloud'-based services. The four deployment models, as described below, can motivate the automotive and scientific community to further research the 'iTransport Cloud' System.

- I. Private 'iTransport Cloud': A private 'iTransport Cloud' must be limited within the boundaries of an organization serving at a regional level the architects, the developers and the end-users-entities of the 'iTransport Cloud' Platform.
- II. Community 'iTransport Cloud': Apart from private clouds, a community 'iTransport Cloud' may also be created by expanding the use of the private cloud capabilities to other parties of similar interests, target groups and policies (i.e. security, privacy, certification and accreditation). A community model can be deployed at national, regional or worldwide level, offering cross-border 'iTransport Cloud'-based services, accessed by anyone within the limits of the specific community.
- III. Public 'iTransport Cloud': Because the general public needs to access certain services without any limitation, a public 'iTransport Cloud' is designed containing public portals to provide the required services and applications. A public 'iTransport Cloud' is deployed at national, regional or worldwide level offering cross-border services accessed by clients, customers, end-users and ITS entities.
- IV. Hybrid 'iTransport Cloud': A Hybrid 'iTransport Cloud' is the combination of the previous types of cloud deployment models. It is deployed to offer 'iTransport Cloud'-based services to the general public but it also consolidates legacy applications and data. It is designed for servicing all the sides of the 'iTransport Cloud' spectrum.

Finally, it must be mentioned that IT architects, administrators and developers may also parameterize the 'iTransport Cloud' architecture and stack and the delivery and deployment models upon the specific needs of the transportation domain they might want to serve.

6.4 'iTRANSPORT CLOUD' SYSTEM INTEROPERABILITY

In order for the proposed 'iTransport Cloud' Model to be fully activated and controlled by the authorized operators of the Trusted Regulatory Authority (TRA), the entire scheme of the proposed interoperable and cooperative-ITS framework will be placed inside the database repository (storage pool and applications block as found in Figure 18) of the 'iTransport Cloud'. This will give the advantage to treat and provide all of the interoperable and cooperative-ITS services similarly to the cloud services. The Operators Profiling, Module Categorization and ACL can adopt the same security methods that the cloud provides concerning the data storage, and the i-Transport Cloud Portal will exclusively deliver the interoperable and cooperative-ITS services to the entire transportation domain in a local, national or international region and in private, public or community mode.

- The ITS Central Station (Trusted Regulatory Authority block found in Figure 18) hosts the entire infrastructure of the 'iTransport Cloud' System which includes the Interoperable and Cooperative Applications and provides the environment for the deployment and operation of the Service Registry over the MMCS.
- The 'iTransport Cloud' Repository hosts the entire set of interoperable and cooperative-ITS services and applications.
- The 'iTransport Cloud' Portal and the MMCS are configured to host the Service Registry and publishes them via the SDM (server-side) interconnected and the wireless and wired virtual ports of the MMCS.

The rest of the security process is similar to the updated interoperable and cooperative ITS-framework as described in the previous Chapter 5.

6.5 'iTRANSPORT CLOUD' TRANSITION PLAN

The transportation environment as already have been described is quite complex and involves the interaction of numerous entities and elements that can be influenced by a member of social, political and economic factors reflecting the trends of the global market. Any kind of degradation, interruption or impairment of the transportation structure can cause serious consequences for the "business continuity of the entire domain. Therefore, before adopting the cloud technology a transition plan [55] is required. Current proposed Transition Plan consists of three basic steps; the implementation and integration model that includes the preparation, strategic and tactical approach; Each of these approaches of the Implementation and Integration Model include a number of 'tasks' and each task a 'set of actions' to be taken. Table 15 gives an analytical guide of the transition plan.

The 'implementation and integration model' guide is designed to provide a detailed description of the proposed tasks and actions related to the generation of the 'iTransport Cloud' system. The 'iTransport Cloud' system must provide access to the greater

Transportation environment via any network access with reduced management effort. It will also deliver mobile and e-services providing access to ITS data, enhancing the operational capabilities and improving the way Information and Telecommunication (IT) technology supports the cyberspace. For these reasons, several numerous issues must be taken under consideration during all the phases of the transition. In the follows the most important considerations are highlighted:

- The need to ensure that guaranteed service levels are achieved and performance instances with monitoring and reporting exist in all the services provided and consumed.
- The application design must not accommodate latency³⁵ errors as there might not be any opportunity for application and service customization, thus increasing the complexity level of integrating cloud services into the Intelligent Transport domain.
- The business opportunities to plan actions associated with the business planning process lifecycle of the architecture modeling.
- In both cases of application design and architecture modeling, the transition plan must eliminate the failing impact on business processes or any other existing technical barriers.
- Because of the dynamic nature of the cloud, information may not be immediately located in the event of a disaster, therefore business continuity and disaster recovery plans must be well-documented, monitored, optimized and tested.
- Legal regulatory frameworks and practices may become a key concern for data stored in the cloud and located within the ITS and the Transportation environments. The ‘iTransport Cloud’ system must also meet the requirements of Privacy Act 1988. Therefore the need to be aware of legislative and regulatory requirements in other geographic regions in order for compliance to be maintained is vital.

TABLE 15: ‘iTRANSPORT CLOUD’ TRANSITION PLAN

| Implementation & Integration Model | Tasks Steps | Set of Actions (i.e.) |
|------------------------------------|---|---|
| Preparation Approach | Cloud Computing Theory Adoption (Current task includes the deeper understanding of the Cloud Computing Theory and the ITS) | <ul style="list-style-type: none"> ▪ Monitoring Regional and Worldwide Cloud Activity. ▪ Adoption of Cloud Principles ▪ Adoption of Cloud Policies ▪ Monitoring Regional and Worldwide Cloud Guidance |
| | Cloud Computing Management Guidance | <ul style="list-style-type: none"> ▪ Deployment model guide ▪ Delivery model guide |

³⁵ A engineering latency is a time delay between the cause and the effect of some physical changes in the system being observed

| | | |
|---------------------------|---|---|
| | (current task includes the decision of which Cloud practices and guides will be adopted in order to generate the Cloud-ITS Framework Guidance) | <ul style="list-style-type: none"> ▪ Portability best practice guide ▪ Privacy best practice guide ▪ Security best practice guide ▪ Service Provider Certification Requirements guide ▪ Risk Management guide |
| | <p>Cloud Computing Theory Application</p> <p>(current task includes the decision of which Cloud Terminology, Framework, Services etc. will be applied)</p> | <ul style="list-style-type: none"> ▪ Information Knowledge Sharing ▪ Cloud Framework ▪ Cloud Services ▪ Service Provider Certification ▪ Terms of Reference |
| Strategic Approach | <p>Cloud Computing Solution Adoption</p> <p>(current task includes the study of the chosen Cloud Computing Solution that will be adapted for the needs of the ITS)</p> | <ul style="list-style-type: none"> ▪ Proof of Concept ▪ Commercially Available Clouds Solutions ▪ Cloud Service Provider Panel Cloud Solution Maturity Level |
| | <p>Implementation Transition</p> <p>(current task includes the design of the interoperable deployment strategy to drive the transition of the existing ITS & ICS into the iTransport Cloud)</p> | <ul style="list-style-type: none"> ▪ Sourcing model ▪ Applications - collaboration tools, developer/testing tools ▪ Open data and Mashups ▪ Channels and portals ▪ Financial Maturity Level Analysis of the establish Cloud Model |
| | <p>Strategy Preparation Review</p> <p>(current task includes the review of the preparation approach and implementation to highlight existing transition and service mitigation issues)</p> | <ul style="list-style-type: none"> ▪ Number of Service Levels related to Cloud Services require careful consideration, ▪ Portability of Data; ▪ Business Reporting and Continuity ▪ Data Security and Logging ▪ Disaster Recovery |
| | <p>Strategy Integration Evaluation</p> <p>(current task includes the evaluation of the cloud services approved for implementation and the first financial risk analysis.)</p> | <ul style="list-style-type: none"> ▪ Investigate opportunities of Concepts and Pilots ▪ Consider opportunity dependencies on the sensitivity of the data and the services (security classification). ▪ Evaluate with other mitigation strategies to discover further opportunities. ▪ Financial Risk Analysis |
| | | |
| Tactical Approach | <p>iTransport Cloud Architecture Design</p> <p>(current task includes the design of the cloud RA utilizing the ITS)</p> | <ul style="list-style-type: none"> ▪ Design and Create the iTransport Cloud Service Platform. ▪ Incorporate the ITS ▪ Service Platform into the existing ITS Base Station Infrastructure. ▪ Requirements for a service catalogue |
| | <p>Optimization of the data-centers and the legacy applications.</p> <p>(current task includes the</p> | <ul style="list-style-type: none"> ▪ Cloud technologies assessment for the provision of transport (ITS) data and ITS solutions. ▪ Securely drive the information/data into |

| | | |
|--|--|--|
| | optimization of the i-Transport Cloud and the Data-Centers) | <p>the iTransport Cloud data-centers.</p> <ul style="list-style-type: none"> ▪ Testing and Optimization of the iTransport Cloud services. ▪ Reform the financial policies and practices in order to reduce costs and energy consumption. |
| | <p>Deployment & Delivery of the iTransport Cloud and delivery of the Cloud-ITS services.</p> <p>(current task includes deployment, delivery models and portfolios opportunities to utilize further the iTransport Cloud)</p> | <ul style="list-style-type: none"> ▪ Exploitation and extension of provided iTransport Cloud services ▪ Expanding beyond a private iTransport Cloud environment. ▪ Use advanced virtualization techniques for reduced cost and energy. ▪ Risk Analysis-Assessment and Monitoring benefits. |

Other actions of the proposed transition plan may include:

- regulatory and policy framework improvements,
- collaboration with national and international research projects,
- the development of a minimum set of references, standards, measures, guidelines,
- the development of certification schemes for products and test assessments.

6.6 CONCLUSIONS

This chapter used the ‘iTransport Cloud’ conceptual system for addressing the open issue of the lack of sustainability over the transportation domain. The ‘iTransport Cloud’ architecture and stack were described in detail. The proposed ‘iTransport Cloud’ refocuses the perception of transportation sustainability and allows a look beyond the customized role of providing vehicular mobility to the broader impact of the transportation on cyberspace, the society and the economy. In addition, the proposed contribution of this chapter goes beyond the high-throughput, capacity, or scalability of a cloud-based computing system. The ‘iTransport Cloud’ theory (fundamentals and principles) and the transition guide plan are promoting the theoretical concept of sustainability and the technological transformation of the Transportation domain into a modern ‘high performance computing’ system.

REFERENCES

- [1] Homeland Security, Transportation Systems Sector, 2013,
Available: <http://www.dhs.gov/transportation-systems-sector>
- [2] E.C, Enterprise and Industry, Modernizing ICT standardization in the EU - the way forward,
Available: http://ec.europa.eu/enterprise/newsroom/ef/itemdetail.cfm?item_id=3263
- [3] Standardization Activities for Intelligent Transport Systems. ITU-T Technology 2008 Report,
Available: http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000080002PDFE.pdf
- [4] E. Curry, et al, Developing a sustainable IT capability: Lessons from Intel's Journey, 2012,
Available: http://www.edwardcurry.org/publications/MISQE_SustainableIT_Intel_2012.pdf
- [5] World Commission on Environment and Development (1987), Our Common Future, Oxford University Press, ISBN 019282080X
- [6] D. Kondo, B. Javadi, P. Malecot, F. Cappello, and D. P. Anderson, Cost-benefit analysis of Cloud Computing versus desktop grids, IEEE International Symposium on Parallel and Distributed Processing, 2009, pp 1-12
- [7] A. Berl, E. Gelenbe, M.d. Girolam et al, Energy-Ecient Cloud Computing, The Computer Journal,
Available: <http://comjnl.oxfordjournals.org/content/53/7/1045.full.pdf+html>
- [8] Smart 2020 Repor, Enabling the Low Carbon Economy In the Information Age,
Available: http://www.smart2020.org/_assets/files/02_Smart2020Report.pdf
- [9] L. Youseff, M. Butrico, D. Da Sivla, Toward a Unified Ontology of Cloud Computing, IEEE, Grid Computing Environments Workshop, 2008, pp 1-10.
- [10] VMware, Virtualization Overview, Whitepaper,
Available: <http://www.vmware.com/pdf/virtualization.pdf>
- [11] IBM Redbooks, Introduction to SAN and System Networking, chap 1 & 6
Available: <http://www.redbooks.ibm.com/redbooks/pdfs/sg245470.pdf>
- [12] IBM Redbooks, Introduction to Grid Computing with Globus, chap 1 & 4,
Available: <http://www.redbooks.ibm.com/redbooks/pdfs/sg246895.pdf>
- [13] F. Liu, J. Tong, J. Mao, et al, NIST Cloud Computing Reference Architecture, 2011,
Available: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909505
- [14] I. Foster, Y. Zhao, I. Raicu, S. Lu, Cloud Computing and Grid Computing 360-degree Compared, Grid Computing Environments Workshop, 2008, pp 1-10
- [15] G. Reese, Cloud Application Architectures, O'Reilly publications, 2009, chap 1 & 2.
- [16] J. Halscott, Desktop Virtualization & Evolving Strategies for IT Service Delivery, Realtime Publishers, Available: <http://nexus.realtimepublishers.com/>
- [17] J. Jozczuk–Januszewska, Development Trends in Intelligent Transport Systems in Respect to Environmental Protection, Springer-Verlag Berlin Heidelberg, ISBN 978-3-642-16472-9, 2011
- [18] H. Fuhs, Hybrid Vehicles and the Future of Personal Transportation, CRC Press, 2009
- [19] Ogrizović, D. Sviličić, B. ; Tijan, E., Open source science clouds, MIPRO, 2010 Proceedings of the 33rd International Convention May 2010, pp. 1189 - 1192
- [20] Ubuntu, Available: <http://www.ubuntu.com>
- [21] OpenStack Cloud Software, Available: <http://openstack.org/>
- [22] Eucalyptus Open Source Cloud Platform, Available: <http://open.eucalyptus.com/>
- [23] OpenNebula Open Source Solution, Available: <http://www.opennebula.org>

- [24] Gartner, Hype Cycle for Emerging Technologies, 2012-2013 Reports,
Available: <http://www.gartner.com/technology/research/hype-cycles/>
- [25] Micron, SSDs for Big Data – Fast Processing Requires High-Performance Storage, Technical Report,
Available: <http://www.micron.com/products/solid-state-storage/enterprise-sas-ssd> Technical Marketing Brief
- [26] T10 SCSI Architecture, Available: http://www.t10.org/drafts.htm#SCSI3_ARCH
- [27] T10 Technical Committee, Serial Attached SCSI, http://www.t10.org/drafts.htm#SCSI3_SAS
- [28] National Science Foundation, Advisory Committee for Cyber-infrastructure on HPC, Report, 2011,
Available: http://www.nsf.gov/od/oci/taskforces/TaskForceReport_HPC.pdf.
- [29] HPC-SIG:UK HPC Special Interest Group, HPC-SIG Report, 2010,
Available: http://www.hpc-sig.org/Publications?action=AttachFile&do=get&target=HPC-SIG_Report2010.pdf.
- [30] NC State University: Office of Information, Technology High Performance Computing (HPC), 2011,
Available: http://www.ncsu.edu/itd/hpc/Documents/Annual_Reports/2011/fy2011.php
- [31] H. Liu, H. Dezhi, The Study and Design on secure-cloud storage system, International Conference on ICECE, 2011, DOI: 10.1109/ICECENG.2011.6057171
- [32] Open vSwitch, Available: <http://openvswitch.org/>
- [33] TechNet, Hyper-V Virtual Switch Overview, Available: <http://technet.microsoft.com/en-us/library/hh831823.aspx>
- [34] Big Switch Networks, Big Virtual Switch, Available: <http://www.bigswitch.com/products/big-virtual-switch-network-virtualization>
- [35] Cisco, Configuring Virtual Switching Systems, Technical Guide, chapter 4,
Available: <http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/configuration/guide/vss.pdf>
- [36] US Department of Energy, Best Practices Guide for Energy-Efficient Data Center Design, 2011,
Available: <http://www1.eere.energy.gov/femp/pdfs/eedatacenterbestpractices.pdf>
- [37] Kernel Newbies, Linux Kernel, Available: <http://kernelnewbies.org/Documents>
- [38] M. Tim Jones, Anatomy of the Linux Kernel, IBM, 2007,
Available: <http://www.ibm.com/developerworks/linux/library/l-linux-kernel/>
- [39] W. Mauerer, Professional Linux Kernel Architecture, Wiley Publishing, Available: http://www.e-reading-lib.org/bookreader.php/142109/Professional_Linux_kernel_architecture.pdf
- [40] M. Rosenblum, The Reincarnation of Virtual Machines, ACM,
Available: <http://queue.acm.org/detail.cfm?id=1017000>
- [41] M. Eisen, Introduction to Virtualization, The Long Island Chapter of IEEE, 2011,
Available: http://www.ieee.li/pdf/viewgraphs/introduction_to_virtualization.pdf
- [42] VMware, “Understanding Full Virtualization, Paravirtualization and Hardware Assist”, Whitepaper, Available: http://www.vmware.com/files/pdf/VMware_paravirtualization.pdf
- [43] Hitachi, Tiered Storage Design Guide, Whitepaper, 2010,
Available: <http://www.hds.com/assets/pdf/hitachi-tiered-storage-options-design-guide.pdf>
- [44] Securing Data in Network Attached Storage (NAS) Environments: ServerProtect for NAS, 2001
Available: <http://support.trendmicro.com.cn/TM-product/HotSolutions/spnaswp.pdf>
- [45] IBM, Network Interface Card (NIC), Available: <http://publib.boulder.ibm.com/infocenter/zos/basics/>
- [46] Dell, “Enhancing Scalability Through Network Interface Card Switch Independent Partitioning”, Whitepaper, 2012, Available: <http://www.broadcom.com/collateral/wp/NIC-WP202-R.pdf>

- [47] Oracle, NIC Virtualization, Available: <http://docs.oracle.com/cd/E19530-01/html/821-0875/gjkfw.html>
- [48] Cisco, “Link Aggregation Control Protocol (LACP) (802.3ad) for Gigabit Interfaces”, 2012, Available: http://www.cisco.com/en/US/docs/ios/12_2sb/feature/guide/gigeth.pdf
- [49] IBM, “Link Aggregation Control Protocol (LACP)”, Available: <http://publib.boulder.ibm.com/infocenter/zvm/v5r4/index.jsp?topic=/com.ibm.zvm.v54.hcpa6/hcsc9b3169.htm>
- [50] Oracle, Ethernet Connections, Available: <http://docs.oracle.com/cd/E19530-01/html/821-0875/gjkfx.html#scrolltoc>
- [51] SysKonnect, Link Aggregation According to IEEE Standard 802.3ad, Whitepaper, Available: <http://cs.uccs.edu/~scold/doc/linkage%20aggregation.pdf>
- [52] M. Tulloch with Microsoft Virtualization Temas, “Understanding MS Virtualization Solutions 2nd edition”, Microsoft Press, Available: http://blogs.msdn.com/b/microsoft_press/archive/2010/02/16/free-ebook-understanding-microsoft-virtualization-r2-solutions.aspx
- [53] K. Dellios, D. Polemi, Maritime Clouds for the European Ports (2012), 16th Pan-Hellenic Conference on Informatics, Special Session – Secret_Didwe | PCI, IEEE, pp. 422-426.
- [54] K. Dellios, D. Papanikas, Deploying a Maritime Cloud (2014), IT Professional Magazine, IEEE, (September/October Issue)
- [55] K. Dellios, D. Papanikas, D. Polemi, Cyber Ocean: A Roadmap to Maritime Cloud (2014), International Journal of Business Innovation and Research (IJBIR), Inderscience, (in press).

7. CONCLUSIONS AND FUTURE DIRECTIONS

The research goals addressed in this doctoral dissertation were related to the cyber-security of the modern automotive-platform, the interoperability among the automotive-platform and the Intelligent Transport Systems (ITS) services and the sustainability of the global transportation systems. In the first part the automotive platform and the ITS were presented. In the second part the threat model for assessing the automotive platform was described and the MASC-Protocol solution for the automotive platform was proposed. In the third part the interoperable framework upgrade for the Cooperative-ITS and the sustainable “iTransport Cloud” system were analyzed.

All of the contributions and the applicability of the proposed solutions are studied within the spectrum of the relationship of the Information Security and the Transportation Domain. The following methodological approach was adopted for reaching the dissertation’s goals:

- Reformulate the modern automobile into an Information and Telecommunication (IT) platform (modern automotive-platform) by identifying its components and by correlating them with assets in IT systems.
- Describe the digital transportation cyber-system where a cluster of automotive platforms, nomadic devices, roadside units and base stations communicate with each other and provide cooperative (sensor-based) services.
- Identify the physical and cyber threats of the automotive platform leading to a detailed threat analysis.
- Perform a detailed vulnerability analysis for all the components (assets) of the automotive platform. Through the applied threat model not only the threats and vulnerabilities can be recognized, but also the entry points as well as the impact caused to the entire ITS can be identified.
- Characterize major design flaws (among the identified vulnerabilities) with high impact not only to the automotive platform but also to the most valuable functional elements and components of the ITS.
- Design and implement the MASC (Mutually Authenticated Secure Components – MASC) protocol which enhances the communication between the components of the automotive platform in order to implement security controls. MASC enhances the security of the automotive platform.
- Introduce the Service Oriented Architecture (SOA) design approach to enhance the ITS standardized reference architecture (ITS-RA).
- Integrate the Service Discovery Mechanism (SDM) in order to formulate a holistic upgraded ITS-RA framework, enabling the offering of not only the traditional (cooperative applications based on wireless sensor networks), but also a new set of interoperable automotive services.

- Design a parameterized MASC-protocol version to enhance the communication with the road side infrastructure in order to implement security controls. The latter enables the upgraded ITS-RA framework to offer interoperable and secure services.
- Provide specific use cases illustrating the functionality of the interoperable and secure enhanced ITS-RA framework.
- Propose a cloud computing architecture based on relevant principles and requirements.
- Design the 'Transport Cloud' system hosting the ITS-RA framework.
- Propose a transition strategy from a legacy system to a cloud system.

Mobility enables us to enjoy a high degree of freedom and quality of life; however it must be secured since it presents major challenges to road transport. Security measures implemented in the automotive platform, similar to the proposed MASC-Protocol, protect human lives, the network and communication interfaces and the confidentiality, integrity, availability and authenticity of the exchanged information, generating a trustworthy and robust ITS framework. In addition, the proposed enhanced interoperable and cooperative-ITS framework provides a contribution towards the security problems that the automotive industry and the research community have highly acknowledged. Furthermore, the global system of the current transportation domain evolves from an industrial and civil production (e.g. road-side infrastructures) context, to an ICT based innovative infrastructures where efficiency, quality, safety and security are major concerns.

Since, ITS one of the most cost-effective tools to improve all aspects of the transport chain. As a result, a wider deployment of ITS with optimum technical equipment for vehicles capable to provide cross border mobility is a major challenge addressing reliability, time-sensitivity, quality and continuity. The, sustainability of the entire transportation domain into the era of Internet of Anything is provided with the cloud computing technology where a Cloud-based Legacy System is designed and proposed to implement the entire structure of modern transportation. Although, the concept of "clouds" is not new, their commercial success over the recent years will play a major role in the ITS domain over the next years, as future global transportation systems will further exploit the capabilities of managed services and resource provisioning.

The Cloud Computing technology is of particular commercial interest for the ITS, not only with the growing tendency to outsource IT so as to reduce management overhead and to extend IT infrastructures, but even more importantly, to reduce the entrance barrier for new service providers to offer their respective capabilities to a wide market with minimum cost and infrastructure requirements. Cloud Computing also allows providers to experiment with

novel service types whilst reducing the risk of wasting resources. In the meanwhile, multiple opportunities arise from the cloud principles for the global transportation infrastructure and systems that will enable further types of interoperable and cooperative-ITS applications and services with reduced development and provisioning time, all of which imply a service-oriented architecture. Cloud Computing technologies and models have not yet reached their full potentials and capabilities related with the rest of the cyberspace, including ITS. Extended research within these guidelines allows using the 'cloud' and ITS to the fullest possible extent of scalability and heterogeneity of the underlying resources.

All of the above presented security, interoperability and sustainability challenges and the proposed solutions of the automotive-platform, intelligent transport systems and digital ecosystems have attracted considerable attention from the research community and the automotive industry in order to provide secure, interoperable and sustainable automotive systems and services. Therefore, the transition of the automotive and transportation domain from the ICT era to the "post-PC" era of cyberspace and the digital microcosm where each and every entity can be uniquely digitally identified and can be witnessed with the changing technological and business orientation that leading industries chose. The fact that these changes are now visible, makes the creation, the implementation and the utilization of new emerging technologies essentials for the transition to new forms of computing, services, applications, systems and final products or the optimization of already existing ones.

In a future vision, every transport movement is part of a fully connected and self-optimized sustainable digital ecosystem. Whatever the travelers' or vehicles' state is (e.g. road-trip, emergency, daily roots), future Internet and Internet of Things (IoT) can enable the information and the services exchanged and provided. The traveler through the automotive-platform will receive personalized and real-time solutions to support him to reach his destination safely and securely according to his personal preferences and constraints (e.g. real-time traffic data and status). The real-time and service oriented solutions utilize to high extend proactively updated information and data during the destination-root based on his effective progression (instant mobility and multimodality). Local authorities, public transport operators and professional drivers will all benefit from the solutions presented in this dissertation as they provide and publish services and information regarding immediate and near future mobility requests and events in all the means of transportation. Furthermore, by offering secure, interoperable and cooperative mobility services or ICT applications that involve vehicle-to-vehicle and vehicle-to-infrastructure communications, the potential to make road transport safer and more efficient is generated.

Currently designed and presented prototype solutions can take advantage of the wireless sensor networking or any other type of communication technologies, which means that the method and process related with their practical deployment is not anymore limited. New ways open how to optimize urban traffic with safety and privacy of the travelers data and promoting the car (or other vehicles) sharing and car-pooling on a new scale. Fleet operators' management and monitoring are two additional aspects of this dissertation's holistic vision concerning the near future of the automotive mobility evolution. Sustainable transportation mobility will become one of the greatest technological and societal challenges and a key topic for the automotive industries' agenda.

Of great research interest is the actual impact of the proposed technology on energy-efficiency data collected for evaluation from real-time environments. Implementing a service rather than a process oriented (event or time triggered) ECU-related architecture for Electrical Vehicles (EVs), a multi-system embedded automotive platform will be controlled easily and efficiently. The specification examples are described below:

- The establishment of a common multi-domain architecture and design platform for advanced multi-core hardware and middleware solutions for electrical vehicles. This can enable an even more flexible interoperability of systems, including the sensors, actuators, information systems, control systems across multiple domains (similar to AUTOSAR) and using a component-based design methodology.
- The establishment of heterogeneous multi-domain architectures to produce interoperable subsystems to support real-time data-processing and to achieve energy efficient HW/SW architectures.
- The development of design tools, associated libraries and runtime support to enable composability, predictability and management of systems according to a service driven or a data-centric approach.
- The energy modeling and performance analysis, verification and scalability of the EV-design should be adopted for gaining appropriate levels of safety.
- The development of multimodal-architectures in networked embedded systems for the heterogeneous automotive devices and advanced communication technologies generated in different dynamic domains, including system properties such as maintainability and survivability of the system and the vehicle.
- New approaches to safety and security, certification and qualification are required to accommodate the new embedded system technologies for the vehicles.
- Support for the ISO 26262 automotive safety standard, including a novel approach for the automatic allocation of safety requirements to components of an evolving architecture.

Moreover, we can identify technological aspects and non-technological issues related with the evolution of the global transportation systems. Related technological issues include:

- scaled interoperability and elastic scalability, which is currently restricted due to the inefficiently implemented resource capabilities;
- trust, security and privacy always pose issues in any provided service, but due to the specific nature of clouds and ITS, additional aspects related to multi-tenancy and control over data location arise;
- handling data both in clouds and ITS is still complicated due to the data size and the diversity, leading to consistency and efficiency issues;
- both trust-security-privacy and consistency-efficiency issues pose legalistic issues;
- most of the deployed models of the ITS are currently not aligned to the highly scalable applications or capable to exploit the capabilities of clouds;
- missing the design and development simplicity in the solutions provided.

Non-technological issues include:

- economic aspects which cover knowledge about when, why and how to use cloud computing systems and technology;
- unclear cloud legislative, intellectual property and data protection rights which come as a consequence of the dynamic handling of the cloud scalability process;
- aspects related to green IT and “green capabilities” by reducing unnecessary power consumption, given that behavioral models in scalability typically integrate insights from cloud-based economic models.

worldwide harmonized regulations of protecting the environment

Concluding this dissertation, all of the above future directions may improve transport efficiency, road safety, promote energy-efficient and IT secure-based modern vehicles. However, the generational shift from desktop to mobile, from software to services and interconnected devices, is in progress and today there are numerous ways for someone to access and search data. The rising cyber-threats and the possibility of numerous hacktivisms against the transportation domain cannot be overlooked. The fact that the mobile era is evolving must faster than the PC-era did, it reveals a social engineering challenge including actively the human factor but also there is no doubt that the information security will be challenged. Therefore, the embedded software used will also need to be adapted to the moving shape of the cyberspace. And just like Steve Jobs predicted some years ago at the ‘#codecon’ conference that nothing is inevitable in a digital world, the likelihood to fall into familiar patterns of technological needs is high, thus we should monetize the work of the past and deliver secure and sustainable innovation in the future.

APPENDIX I: LIST of ITS STANDARDIZATION ORGANIZATIONS

A. International Organization for Standardization (ISO)

ISO (International Organization for Standardization) is the world's largest developer of voluntary International Standards; a non-governmental organization that forms a bridge between the public and private sectors. ISO's are developed through global consensus and give the state of the art specifications for products, services and good practice, helping to make industry more efficient and effective. ISO/TC 204 is responsible for the overall system aspects and infrastructure aspects of intelligent transport systems (ITS), as well as the coordination of the overall ISO work programme in this field including the schedule for standards development, taking into account the work of existing international standardization bodies. The scope of ISO/TC 204 Standardization of information, communication and control systems in the field of urban and rural surface transportation, including intermodal and multimodal aspects thereof, traveler information, traffic management, public transport, commercial transport, emergency services and commercial services in the intelligent transport systems (ITS) field is summarized in Tables 16 and 17 :

TABLE 16: ISO/ITS RELATED STANDARDS

| Related Standard | Scope |
|-------------------------|--|
| ISO/TC 204/WG 1 | Architecture |
| ISO/TC 204/WG 3 | ITS database technology |
| ISO/TC 204/WG 4 | Automatic vehicle and equipment identification |
| ISO/TC 204/WG 5 | Fee and toll collection |
| ISO/TC 204/WG 7 | General fleet management and commercial/freight |
| ISO/TC 204/WG 8 | Public transport/emergency |
| ISO/TC 204/WG 9 | Integrated transport information, management and control |
| ISO/TC 204/WG 10 | Traveller information systems |
| ISO/TC 204/WG 11 | Route guidance and navigation systems |
| ISO/TC 204/WG 14 | Vehicle/roadway warning and control systems |
| ISO/TC 204/WG 16 | Wide area communications/protocols and interfaces |
| ISO/TC 204/WG 17 | Nomadic Devices in ITS Systems |
| ISO/TC 204/WG 18 | Cooperative systems |

TABLE 17: OTHER ITS RELATED STANDARDS

| Related Standard | Scope |
|-------------------------|--|
| ISO/IEC JTC 1 | Information technology |
| ISO/TC 8 | Ships and marine technology |
| ISO/TC 22 | Road vehicles |
| ISO/TC 184 | Automation systems and integration |
| ISO/TC 241 | Road traffic safety management systems |
| ISO/PC 286 | Collaborative business relationship management |

B. European Telecommunications Standards Institute (ETSI)

ETSI, the European Telecommunications Standards Institute, produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies. ETSI is a not-for-profit organization with more than 700 ETSI member organizations drawn from 62 countries across 5 continents world-wide. IT is officially recognized by the European Union as a European Standards Organization. ETSI/TC ITS scope includes communication media, and associated physical layer, transport layer, network layer, security, lawful intercept and the provision of generic web services. It has the responsibility for the development and maintenance of Standards. It is also responsible for the specifications and other deliverables to support the development and implementation of ITS Service provision across the network, for transport networks, vehicles and transport users, including interface aspects and multiple modes of transport and interoperability between systems, but not including ITS application standards, radio matters, and EMC. ETSI/TC ITS includes five (5) Working Groups (WG).

WG-1 develops ETSI deliverables on the application requirements and services including:

- The collection of requirements from Passenger (including accessibility), Automotive Industry, Road Network Operators, Freight and Logistics, Public Authorities
- On a harmonized requirements basis, the development of the application classification and specify a V2V / V2I-Communication Basic Set of Applications.
- Definition and specification of the functions, services and interfaces to support the V2V / V2I-C Basic Set of Applications.
- Specification of the application protocols and messages specification to support the Basic applications set & Specification of the operational requirements for the supporting system.
- Consideration of the conformance, interoperability testing procedures and test suites.
- Contribution to the harmonization and optimization of the overall system.

WG-2 develops the overall architecture and address cross (OSI) layer issues including: ITS Architecture; Communications Architecture; Cross Layer Issues; Separation of Service Provision from Medium provision; Methodology is to use different viewpoints or perspectives, e.g. user, standardization, network, security, operation, implementation.

WG-3 develops ETSI deliverables for the data transport and network protocol layers and management of these layers including:

- Development of a network architecture which covers existing and future wireless and wired technologies and various application services for any kind of ITS users, including vehicle drivers and passengers, railway users, pedestrians, bicyclists and other;
- Harmonization of the network architecture with the overall ITS system and protocol architecture; Development of novel networking protocols for ITS, such as ad hoc and multi-hop routing protocols, reliable transport protocols over multi-hop routing, and others;
- Integration of dedicated ITS network protocols and transport protocols with the Internet protocol suite and IP mobility extensions;
- Work out solutions for internetworking between access networks;
- Ensuring that the networking and data transport protocols and algorithms are efficient, scalable and reliable and protect the user's privacy and ensure security;

WG-4 encompasses ITS standardization on OSI model layers 1 and 2 including the management of these layers. WG-4 may have subgroups for each of the core subject areas ERM Liaison/participation with regard to ERM scoped issues. WG 4 is the responsible group inside TC ITS for the development of ETSI system reference documents for ITS

- 5 GHz, 60 GHz, Infra-red, CEN RTTT DSRC & ISO CALM (21212 and 21213) 2G / 3G

WG-5 is responsible for:

- Conducting studies leading to deliverables on Security & assuring ITS solutions conform to regulatory requirements for privacy, data protection, lawful interception and data retention;
- Management and co-ordination of the development of security specifications for ITS communication and data;
- Investigation of security services and mechanisms required for providing ITS services over the Internet;
- Development of security analyses of candidate protocols and network elements to be used within the ITS framework to implement capabilities e.g., ERMTEL aspects, IPv6 migration, keying strategies and methods;
- Tracking ongoing worldwide security activities of interest to ITS (notably in ISO TC204)

C. European Committee for Standardization (CEN)

The European Committee for Standardization (CEN) was officially created as an international non-profit association based in Brussels on 30 October 1975. Its mission is to foster the European economy in global trading, the welfare of European citizens and the environment. Through its services it provides a platform for the development of European Standards and other technical specifications. It provides the legal framework within which the European Standards Organizations (CEN, CENELEC, ETSI) will operate. The text of the new EU Regulation (1025/2012) is published in the Official Journal of the European Union (see Issue L316 of 14 November 2012). CEN/TC 278 is responsible for managing the preparation of standards in the field of Intelligent Transport Systems (ITS) in Europe. It serves as a platform for European stakeholder to exchange knowledge, information, best practices and experiences in ITS. The ITS topics covered by CEN/TC 278 are:

- WG-1 Electronic Fee Collection
- WG-2 Freight, Logistics and Commercial Vehicle Operations
- WG-3 Public Transport
- WG-4 Traffic and Travel Information (dormant)
- WG-5 Traffic Control Systems (dormant)
- WG-7 ITS spatial data
- WG-8 Road Traffic Data
- WG-9 DSRC (dormant)
- WG-10 Human-Machine Interfacing
- WG-12 Automatic Vehicle and Equip. Identification
- WG-13 Architecture and Terminology
- WG-14 Recovery of stolen vehicles
- WG-15 e-safety / eCall
- WG-16 Cooperative ITS

D. International Telecommunications Union (ITU)

The Study Groups of ITU's Telecommunication Standardization Sector (ITU-T) assemble experts from around the world to develop international standards known as ITU-T Recommendations which act as defining elements in the global infrastructure of information and communication technologies (ICTs). Standards are critical to the interoperability of ICTs and whether we exchange voice, video or data messages, standards enable global communications by ensuring that countries' ICT networks and devices are speaking the same language. From its inception in 1865, ITU-T has driven a contribution-led, consensus-based approach to standards development in which all countries and companies, no matter how large or small, are afforded equal rights to influence the development of ITU-T Recommendations. Standardization work is carried out by the technical Study Groups (SGs) in which representatives of the ITU-T membership develop Recommendations (standards) for the various fields of international telecommunications. The intent of the Collaboration is to provide a globally recognized forum for the creation of an internationally accepted, globally harmonized set of Intelligent Transportation Systems (ITS) communication standards of the highest quality in the most expeditious manner possible to enable the rapid deployment of fully interoperable ITS communication-related products and services in the global marketplace. Work Items include:

- Perform a study of identified ITS application requirements so that needed communication capabilities and performance can be properly defined. This study should identify and use existing sets of ITS application requirements from various global regions and supplement them to reflect recent application developments and direction. Requirements of individual applications or sets of applications should be combined to create communications capability needs and performance boundaries as required to support the full set of expected applications. All defined applications should be considered in the study, with particular attention being given to high priority applications such as:
 - Road safety applications
 - Traffic management/mobility applications
 - Applications affecting environmental needs, including those servicing electric/hybrid vehicles
 - Special attention needs to be given to the requirements of Developing Countries and Megacities
- Perform a gap analysis and quality assessment of current ITS communications standards and create an action plan to address identified needs. Gap analysis should compare the ITS communication standards that already exist or are in work with the standards that would be required with a 'best practices' communications standards scenario. If overlaps are found, the best elements of duplicative standards should be used in the study and the overlap should be clearly noted in the outcome of the study. The quality assessment should examine each existing standard to determine if it is clear to incorporate all the necessary ingredients to harmonize with its complementary standards and to create a complete communications solution. Throughout this study, the use of IPv6 should be assumed in all situations where it is viable.
- Create a complete, coherent and effective package of security frameworks and standards for use within ITS communications. This task should identify all existing and ongoing work in this area, leverage it to the greatest possible degree, and assure that modern communication security practices are embedded in the final product.
- Develop standards to govern the interaction of drivers with carry-in communication devices (such as smart phones brought into vehicles). The standards should require carry-in communication devices to determine if they are in a vehicle. If the carry-in communication device interacts with equipment in the vehicle, the standards should require the carry-in communication device to follow vehicle driver distraction rules. If the

carry-in communication device does not interact with equipment in the vehicle, the standards should require the carry-in communication device to not allow its use by the driver while the vehicle is moving.

- Investigate regulatory and legislative actions necessary to facilitate the deployment of ITS communication products and services based on the ITS communication standards being developed.
- Review mobility network services and ITS communications for their application as a 'last resort' supplement to other communication systems for emergency and disaster handling.

E. Internet Engineering Task Force (IETF)

The technologies related with Internet are discussed and standardized in the Internet Engineering Task Force (IETF). The organization is international and open for everyone such as network designers, operators and researchers. Different topics are discussed in working groups and any one can follow the discussion. ITS related working groups are illustrated in Mobile IP rfc6275, rfc5944 and mip6 WG discussing about Mobile IPv6.

The applicability of IETF protocols to Cooperative Intelligent Transport Systems (C-ITS) can be found in the analysis of IPv6 for ITS in deliverable D2.1 and D2.2 of the ITSSv6. ITSSv6 builds on existing standards from ETSI, ISO and IETF and IPv6 software available from the CVIS and GeoNet projects. The IPv6 ITS station stack provided by ITSSv6 supports at least 802.11p and 2G/3G media types and is configured differently according to the role played by the ITS station (roadside, vehicle, central). Implemented IPv6 features specific to the Vehicle ITS station include NEMO and MCoA to maintain Internet continuity over multiple medias and IPv6 GeoNetworking for multi-hop communications between Vehicle and Roadside ITS stations over 802.11p. The IPv6 ITS station stack will be tested in relevant EU or National Cooperative Intelligent Transport Systems' Field Operational Tests (Cooperative ITS FOTs) and projects. More information can be found in ISO 21210|CALM: IPv6 Networking and ISO 21217|CALM: Architecture.

F. Institute of Electrical and Electronics Engineers (IEEE)

The Institute of Electrical and Electronics Engineers (IEEE) is the leading professional association for advanced technologies. IEEE's core purpose is to foster technological innovation and excellence for the benefit of humanity. It is designed to serve professionals involved in all aspects of the electrical, electronic and computing fields and related areas of science and technology that underlie modern civilization. However, as the world's largest technical professional association, IEEE's membership has long been composed of engineers, scientists, and allied professionals. These include computer scientists, software developers, information technology professionals, physicists, medical doctors, and many others in addition to our electrical and electronics engineering core.

By the early 21st Century, IEEE served its members and their interests with 38 societies, 130 journals, transactions and magazines, more than 300 conferences annually and 900 active standards. The IEEE Intelligent Transportation Systems Society (ITSS) provides access to leading technical research in engineering and information technologies as applied to systems using synergistic technologies and systems engineering concepts. Major peer-reviewed publications and sponsored events include the IEEE Intelligent Transportation Systems Magazine and the International IEEE Conference on Intelligent Transportation Systems. The fields of interest vary from the theoretical, experimental and operational aspects of electrical and electronics engineering and information technologies as applied to Intelligent Transportation Systems (ITS) for example:

- IEEE 802.15 Bluetooth
- IEEE 802.11 Wireless LAN
- IEEE 802.11 p standard (WAVE-Wireless Access in Vehicular Environments)
- IEEE 802.16 standard (WiMAX-Worldwide Interoperability for Microwave Access)

APPENDIX II: LIST of ITS RESEARCH PROJECTS

A. ENERGY EFFICIENCY ITS-PROJECTS

[1]. HELIOS [Online] www.helios-eu.org

Battery reliability and safety are the key issues for the commercialization of Electric and Hybrid Electric Vehicles (HEV) for the private customers. For High Energy (HE) applications, requiring a large amount of energy stored on board, the lack of long-term visibility on the battery performances is limiting the commercial availability of Electric Vehicles and Plug-in HEV. The main goal of the project HELIOS is focused on improving dramatically the cells life and safety, while accepting a slight degradation in performances, in terms of energy and power density which should guarantee an excellent safety & performances.

[2]. EUROLIION [Online] www.eurolion.eu

Although the Li-ion cell appears to be the most appropriate technology to meet these goals, considerable research and development is required. The EUROLIION research described in this proposal aims to develop a new Li-ion cell for traction purposes with the following characteristics of high energy density and low costs improved safety.

[3]. HCV [Online] www.hcv-project.eu

Hybrid Commercial Vehicle (HCV) is a FP7 EU-funded project initiative for reducing the emission of climate gases and other emissions in urban areas. Commercial vehicles stand for a not insignificant part of pollution in today's city environments and hybridization of said applications can to a large degree decrease the emitted substances. The HCV project aims to enhance the further reduce fuel consumption and to decrease the cost of a hybrid system. Test methods, certification procedures and subsystems will be further developed and barriers for hybrid commercial vehicles will be evaluated in conjunction with commercial vehicle operators in a user forum.

[4]. CASTOR [Online] www.castor-project.eu

CASTOR is a STREP Project, co-funded by the European Commission FP7-ICT objective "ICT for the Fully Electric Vehicle". It addresses the distributed power train architecture proposed for electric vehicles (EVs) with the aim to reduce power ratings of the traction drive by partitioning of the power train into 2/4 driving wheels. CASTOR combines novel power electronic converter and storage system architectures interfacing batteries and super capacitors at module or cell level will be evaluated, implemented and demonstrated. CASTOR will explore architectures of the fully integrated power train electronics for distributed propulsion systems that enable future generations of EV's and personal propulsion systems.

[5]. SuperLIB [Online] www.superlib.eu

The project "Smart Battery Control System based on a Charge-equalization Circuit for an advanced Dual-Cell Battery for Electric Vehicles" (SuperLIB) addresses key objectives of the topic "ICT for fully electric vehicles" within the ICT work program of the European Commission's 7th Framework Program. SuperLIB focuses on smart control system solutions for batteries. Safety and control system relevant temperature sensors will be developed for an improved thermal management of the package and the whole system will be able to still provide the required usable energy content and power performance.

[6]. Motorbrain [Online] www.motorbrain.eu

The MotorBrain Project develops sustainable drive train technologies and control concepts/ platforms for inherent safe and highly efficient power-trains of the 3rd Electric Vehicle Generation. The project addresses the highly challenging research on power and high voltage electronic systems beyond state of the art. Smart miniaturized systems including subsystems, system layers and vehicle demonstrators will be derived. The envisaged EV-Power-trains shall enable significant steps ahead in terms of a) Overall energy efficiency and Smart failsafe electrical power-train concepts, b) Efficient smart motor management systems and intelligent integration concepts for passive components, sensors and power converters, c) Enhanced sustainability by improving recyclability and alleviating the dependency on rare-earth magnets.

[7]. ASTERICS [Online] www.asterics-project.eu

Overall performance of Fully Electric Vehicles (FEVs) has to be enhanced to meet customers' expectations therefore development time has to be cut drastically. The ASTERICS project will contribute to a huge leap forward, improving modeling and testing tools needed for the development of future FEVs all over Europe. ASTERICS will support the competitiveness of the automotive sector in all its aspects: basic components, integrated components, sub-systems, algorithms, systems and OEMs applications with efficient simulation & testing under real world conditions for innovative electric vehicle components and systems.

[8]. ENLIGHT [Online] www.project-enlight.eu

ENLIGHT Project strives to advance highly innovative lightweight material technologies for application in structural vehicle parts of future volume produced Electric Vehicles (EVs) along four axes: performance, manufacturability, cost effectiveness and lifecycle footprint. The main target is to develop viable, sustainable and energy efficient solutions for medium production volume EVs with lightweight materials such as carbon-fibre. Through the collaboration of EUCAR, CLEPA and EARPA, ENLIGHT will act as an open innovation platform, integrating valuable insights from other EU research projects with a holistic design approach. The demonstration and evaluation of the lightweight potential is supported virtually with a full vehicle model scenario.

[9]. ELVA [Online] www.elva-project.eu/

As electric vehicles, they have an electric motor and a battery instead of a combustion engine and a fuel tank. These modifications require extensive adaptations in order to integrate the battery in a safe manner. As a result, necessary reinforcement measures hinder to fully exploit the new freedom in design given by the electrification of the vehicle. In order to meet increasingly strict emission targets and growing traffic in urban areas, electro mobility is a promising way; the aim of the ELVA project was to bring in line technology options and customer expectations for the third generation of electric vehicles. ELVA developed innovative vehicle architectures that are fully exploiting the freedoms in design resulting from the electric drive-train.

[10]. COSMO [Online] www.cosmo-project.eu

COSMO project aims to install and run practical demonstrations of a range of these new services in realistic conditions, in order to produce quantified results of the impact of given cooperative systems on the environment with regards to fuel consumption and CO₂ emissions. The detailed specifications of the project are covering technical, legal and organizational issues involved in deployment of those systems, including indications on their procurement, installation, operation and maintenance linked with pilot cases.

[11]. CONVENIENT [Online] www.convenient-project.eu

The CONVENIENT project targets a 30% reduction of fuel consumption in vehicles for long-distance freight transport by developing an innovative heavy-truck archetype featuring a suite of innovative energy-saving technologies and solutions. Responding to this challenge, the objective of CONVENIENT is to achieve complete vehicle energy management by proposing highly innovative solutions for improved efficiency and enhanced integration of components (currently designed independently) which will be developed, integrated and evaluated directly on vehicles, including:

- Innovative energy efficient systems and hybrid transmission, HVAC Energy harvesting devices, like photovoltaic solar roof for truck and semitrailer;
- Advanced active and passive aerodynamics devices for the truck and for the semitrailer
- Holistic Energy Management system at vehicle level;
- A Predictive Driver Support to maximize the energy saving benefits;
- A novel Hybrid Kinetic Energy Recovery System for the semitrailer.

[12]. TRANSFORMERS [Online] www.transformers-project.eu

Today trucks and load carriers are designed and optimized towards a limited variance set of usage and for maximum payload. In the future there will be an increasing need for optimized load efficiency for each mission of a truck, and for optimizing the freight carried on a finite length of road. Configurable and adaptable trucks and trailers for optimal transport efficiency is a growing need. The overall objective of the TRANSFORMERS project is to develop and demonstrate innovative and energy efficient trucks and load carriers leading to an overall 25% less energy consumption on a t.km basis and a lower impact on the road infrastructure through the following key innovations:

- A distributed, modular, and mission adaptable Hybrid-on-Demand (HoD) driveline concept that will be applicable to both, existing and future truck-(semi)trailer vehicles
- Loading efficiency optimized trailer inside design (toolbox) and mission-based configurable aerodynamic overall truck-trailer design (toolbox)
- A pre-standard electric Hybrid-on-Demand Framework that supports a broad market introduction of hybrid commercial vehicles and provides planning certainty for future RTD activities;
- To agree on a common truck-trailer pre-standard energy management interface, enabling a 70% Hybrid-on-demand market penetration by 2040.

B. SAFETY & MOBILITY ITS-PROJECTS

[13]. interactiVE [Online] www.interactive-ip.eu

The interactiVE project vision was an accident-free traffic utilizing affordable integrated safety systems available for all vehicle classes and systems that continuously assist the driver and intervene if necessary. interactiVE was motivated by the wish to reduce the number and the severity of accidents and injuries on the roads. The predecessor project PReVENT had developed a vehicle surrounding safety zone. This zone is protecting the vulnerable road user not only by reacting to severe situations, but by actively intervening to prevent the accident and to mitigate the collision. The advanced driver assistance systems (ADAS) have been highly appreciated by most drivers testing them. So far, the system costs were perceived as an obstacle for application in day-to-day driving. interactiVE has taken the ADAS to the next level while paving the way for broad deployment of the system across all vehicle classes. At the Final Event results have been shown with presentations in Aachen and a Driving Demonstration at the Ford Lommel Proving Ground.

[14]. COMeSafety2 [Online] www.comesafety.org

COMeSafety2: The overall goal of COMeSafety2 is to support the realization and possible deployment of cooperative, communication based active safety systems. The project provides information to the European Commission about relevant technical and organizational matters. It is dedicated to foster wide agreement on technical issues on the one hand, but also wide agreements on deployment strategies on the other.

- Facilitating the preparation of a European set of standards to support European Community wide implementation and deployment of cooperative Intelligent Transport Systems and -Services (C-ITS)
- Effective EU-US and wider international cooperation
- Maximise the benefits of world-wide field operational testing outcomes shared in the C-ITS Community
- Promotion of objectives and prospects towards stakeholders, including industrial players and authorities.

[15]. DRIVE C2X [Online] www.drive-c2x.eu

DRIVE C2X focuses on communication among vehicles (C2C) and between vehicles, a roadside and backend infrastructure system (C2I). Previous projects such as PReVENT, CVIS, SAFESPOT, COOPERS, and PRE-DRIVE C2X have proven the feasibility of safety and traffic efficiency applications based on C2X communication. DRIVE C2X goes beyond the proof of concept and addresses large-scale field trials under real-world conditions at multiple national test sites across Europe. DRIVE C2X relies on results from the PRE-DRIVE C2X project in terms of specification, hardware and software prototypes, test environment and integrated simulation tool set developed. The basis comprises different technological components, namely the communication system (radio, communication protocols), facilities, human machine interface, applications and management.

[16]. DESERVE [Online] www.deserve-project.eu

DESERVE project aims at designing and developing a Tool Platform for embedded Advanced Driver Assistance Systems (ADAS) to exploit the benefits of cross-domain software reuse, standardized interfaces, and easy and safety-compliant integration of heterogeneous modules to cope with the expected increase of functions complexity and the impellent need of cost reduction. The DESERVE Platform will provide the environment for ADAS design, development and pre-validation and even pre-certification of software and hardware modules to be integrated in ADAS applications. Safety critical requirements will be considered in the design and systems development making integrated, trusted, interoperable tools and tool-chains available.

[17]. CRYSTAL [Online] www.crystal-artemis.eu

The ARTEMIS Joint Undertaking project CRYSTAL (CRITICAL sYSTEM engineering AccELeration) takes up the challenge to establish and push forward an Interoperability Specification (IOS) and a Reference Technology Platform (RTP) as a European standard for safety-critical systems. This standard will allow loosely coupled tools to share and interlink their data based on standardized and open Web technologies that enables common interoperability among various life cycle domains. This reduces the complexity of the entire integration process significantly. Compared to many other research projects, CRYSTAL is strongly industry-oriented and will provide ready-to-use integrated tool chains having a mature technology-readiness-level (up to TRL 7). In order to reach this goal, CRYSTAL is driven by real-world industrial use cases from the automotive, aerospace, rail and health sector and builds on the results of successful predecessor projects like CEASAR, SAFE, iFEST, MBAT on European and national level.

[18]. TEAM [Online] www.cooperative-team.eu

The TEAM project develops new collaborative transport solutions and thus addresses two challenges at the same time: the need to design an infrastructure for increasing traffic and the need to reduce environmental pollution. Therefore TEAM combines driving technologies with sophisticated telecommunication technologies and telematics. For the first time in this field of research, elements such as vehicle electronics and mobile devices, navigation systems, tablet computers and smartphones are integrated to focus on the road users' behavior. Road users will benefit from the new TEAM technologies through real time traffic recommendations balanced with global mobility and environmental aspects. In this way TEAM turns static into elastic mobility by joining drivers, travelers and infrastructure operators into one collaborative network. Collaboration is the key concept, which extends the cooperative concept of vehicle-2-x systems to include interaction and participation.

[19]. POLLUX [Online] www.artemis-pollux.eu

The POLLUX project considers both vertical integration and horizontal cooperation between OEMs, hardware/software/silicon providers to build a solid, embedded-systems European industry while establishing standard designs and distributed real-time embedded-systems platforms for EVs.

[20]. MAENAD [Online] www.maenad.eu

MAENAD is an FP7 project funded by the European Commission and a Model-based analysis & engineering of novel architectures for dependable electric vehicles is proposed in order for fully Electric Vehicles (FEV) systems will have more authority, share common components and rely less on mechanical backups. New complex power management and optimization algorithms are needed to ensure high performance, range of travel and low energy consumption. MAENAD will extend EAST-ADL2 with advanced capabilities to facilitate development of dependable, efficient and affordable FEV. In addition, MAENAD will propose an overall design methodology for FEV and evaluate its application via a realistic case study on an innovative FEV system which represents a current design challenge.

[21]. Know4Car [Online] www.know4car.eu

Current digital manufacturing ICT platforms have provided a series of useful tools to support engineers in a series of automotive activities. However today's ERP systems are often detached from the engineering knowledge, while current systems provide no link to actual performance indicators, such as cost, time, and quality parameters. Furthermore the engineering knowledge is often dispersed over many stakeholders and IT systems and they are often too complex and require much effort to follow. Know4Car IP project, will address the above challenges, by developing an agent-based collaborative platform for managing manufacturing process knowledge addressing the following objectives, utilizing a modern technical approach:

- Efficient knowledge management and collaboration, throughout the process lifecycle,;
- supporting the capture and systematic organization of knowledge across different stakeholders;
- Systematic analysis of data for process and product design specifications;
- Automatic extraction and representation of knowledge from history of design changes.

[22]. DELIVER [Online] www.deliver-project.org

The DELIVER project serves the purpose of exploring and identifying conceptual design options for fully electric light commercial vehicles in urban areas. The project partners make it their task to develop and build-up in hardware an innovative and sustainable vehicle concept that fulfils the demands of tomorrow. The DELIVER project, as part of the European Green Cars Initiative, aims to explore urban light commercial vehicle (LCV) concepts intended for larger scale production by executing a broad scope conceptual design study which will start by establishing initial design specifications and continue to a detailed prototype-based and virtual performance assessment as well as a running concept demonstrator vehicle. The project is focusing on the design rules of the design of fully electric LCVs to be launched by 2020. It will build upon the progress made and foreseen in each of the subsystems or main components that are to be integrated into the fully electric LCV through networking with complementary R&D projects.

C. STRATEGIC ITS-ACTIONS

[23]. AUTONET 2030 [Online] www.autonet2030.eu

AutoNet2030 shall develop and test a co-operative automated driving technology, based on a decentralized decision-making strategy which is enabled by mutual information sharing among nearby vehicles. The project is aiming for a 2020-2030 deployment time horizon, taking into account the expected preceding introduction of co-operative communication systems and sensor based lane-keeping/cruise-control technologies. By taking this approach, a strategy can be worked out for the gradual introduction of fully automated driving systems, which makes the best use of the widespread existence of co-operative systems in the near-term and makes the deployment of fully automated driving systems beneficial for all drivers already from its initial stages. Drivers shall receive maneuvering instructions on their HMI; the ergonomics and non-distraction of this new user interface shall be validated. This system shall be optimised to make safe, predictable, and efficient maneuvering decisions.

[24]. SATIE [Online] www.satie.eu

In order to accelerate the deployment of ICT for sustainable mobility and transport, the SATIE Support Action introduced in the 2009 EC Communication "A Strategy for ICT R&D and Innovation in Europe: Raising the Game". SATIE explored the key elements of a European Large Scale Action and provided assistance in the form of "Handbook" offering guidelines for the design, construction and operation. The SATIE approach was based on establishing a partnership of national, regional and local key stakeholders from both demand and supply sides to share in the implementation of ICT solutions for mobility and transport in Europe. The iterative process aims to specify an optimum model with regard to the added value for European innovation and Europe's economy.

[25]. ERTRAC [Online] www.ertrac.eu

Road Transport plays a vital role in the European economy and society. The Road Transport sector involves a wide range of industries and services from vehicle manufacturers and suppliers to infrastructure providers, mobility management, communication technologies, energy companies, and many others. Because of the importance of the role of Road Transport in Europe, an accelerated development of sustainable, integrated transport solutions is necessary. The European Road Transport Research Advisory Council (ERTRAC) is the European Technology Platform (ETP) for Road Transport. The mission of ERTRAC is to provide a framework through FOSTER-Road to focus coordination efforts of public and private resources on the necessary research activities.

APPENDIX III: PUBLICATIONS, DISSEMINATION ACTIONS & RESEARCH PROJECTS

| | |
|--|---|
| <p style="text-align: center;"><u>Journals</u></p> | <ul style="list-style-type: none"> ▪ K. Dellios, D. Papanikas, Information Security Compliance over the Intelligent Transport Systems: Is IT possible? (2015) Security & Privacy, IEEE, Vol.13, Issue 3 (to be published) ▪ C. Patsakis, K. Dellios, M. Bouroche, Towards a distributed secure in-vehicle communication architecture for modern vehicles (2014), Computer and Security, Elsevier, vol. 40, pp. 60-74. ▪ K. Dellios, D. Papanikas, D. Polemi, A Service Discovery Mechanism for the Cooperative Intelligent Transport System (2014), World Review of Intermodal Transportation Research Journal (WRITR), vol 4, pp. 259-279. ▪ K. Dellios, D. Papanikas, Deploying a Maritime Cloud (2014), IT Professional magazine, IEEE, Vol. 16, Issue 5, pp. 56-61 ▪ K. Dellios, D. Papanikas, D. Polemi, Cyber Ocean: A Roadmap to Maritime Cloud (2014), International Journal of Business Innovation and Research, Inderscience, (in press). |
| <p style="text-align: center;"><u>Conference Proceedings</u></p> | <ul style="list-style-type: none"> ▪ C. Patsakis, K. Dellios, Securing in-vehicle communication and redefining the role of automotive immobilizer (2012), International Conference in Security and Cryptography, SECRIPT, pp.221-226. ▪ K. Dellios, A. Chronakis, D. Polemi, Transforming Vehicles into e-Government Cloud Computing Nodes (2012), Global Security, Safety and Sustainability, Springer Link, LNICST Vol. 99, pp.1-8. ▪ K. Dellios, D. Polemi, Maritime Clouds for the European Ports (2012), 16th Pan-Hellenic Conference on Informatics, Special Session – Secret_Didwe PCI, IEEE, pp. 422-426. ▪ C. Patsakis, K. Dellios, Patching Vehicle Insecurity (2011), In-Depth Security Conference (Deep-Sec), (abstract) ▪ K. Dellios, D. Polemi, VBESS: Vehicular Biometric Embedded Security System (2010), Systemic Approaches in Social Structures, 6th National & International HSSS Conference, (abstract) |
| <p style="text-align: center;"><u>Dissemination Actions</u></p> | <ul style="list-style-type: none"> ▪ 2014, Can Android Security Protect the Connected Car? (Interview) [Online] http://news.dice.com/2014/01/17/can-android-security-protect-connected-car/ ▪ Hacker Unternehmen Das Steuer (Interview), Technology Review Magazine, Horizonte Report, pp. 46-49, [Online] http://www.heise.de/tr/artikel/Hacker-uebernehmen-das-Steuer-1764048.html ▪ 2011, Autos brauchen dringend eine Nutzerverwaltung, (Interview), IT News Fur Profis [Online] http://www.golem.de/1111/87942.html ▪ 2011, C. Patsakis, K. Dellios, Patching Vehicle Insecurity, Invited Talk - In-depth Security conference, Europe (Deep-Sec), The Imperial Riding School, Vienna, Austria [Online] https://www.youtube.com/watch?v=BA2J7O6cqzQ |
| <p style="text-align: center;"><u>Research Projects</u></p> | <ul style="list-style-type: none"> ▪ National Strategic Reference Framework SYNERGASIA, Bio-Identity: Secure and Revocable Biometric Identification for use in Disparate Intelligence Environments, (May 2011 – May 2014) ▪ National Strategic Reference Framework SYNERGASIA, S-PORT - A secure, collaborative environment for the security management of Port Information Systems, (January 2011 – December 2012) ▪ E.U. IST Programme, SWEB: Secure interoperable cross border m-services contributing towards a trustful European cooperation with the non-EU member Western Balkan countries, (September 2008 – March 2009) |