
Development Platform for Safe and Efficient Drive

# Regulatory Report

| | | | | |
|---|---|---|---|---|
| Deliverable n. | D7.2.3 Regulatory Report | | | |
| Sub Project | SP7 | Dissemination and Exploitation | | |
| Workpackage | WP72 | Exploitation, standardisation and regulatory issues | | |
| Task n. | T7.2.3 | Regulatory issues | | |
| Authors | Nereo Pallaro | | CRF | |
| File name | D723_Regulatory_Report_v8.doc | | | |
| Status | Final | | | |
| Distribution | Restricted (RE) | | | |
| Issue date | 29/08/2014 | Creation date | 09/04/2014 | |
| Project start and duration | 1st of September, 2012 – 36 months | | | |

## REVISION AND HISTORY CHART

| VER. | DATE | AUTHOR | REASON |
|---|---|---|---|
| 0.1 | 09/04/2014 | N. Pallaro (CRF) | Template |
| 0.2 | 11/06/2014 | N. Pallaro (CRF) | First draft, chapters 1-2-3 |
| 0.3 | 21/07/2014 | N. Pallaro (CRF) | Second draft, chapters 4-5 |
| 0.4 | 20/08/2014 | M. Kunert (Bosch) | Content update (ADAS standards and norms, table 6) and refinement |
| 0.5 | 22/08/2014 | D. Daurenjou (Continental) | Document review |
| 0.6 | 24/08/2014 | S. Fruttaldo (ICOOR) | Peer review |
| 0.7 | 27/08/2014 | F. Sommariva, L. Andreone, G. Zennaro (CRF)<br>J. Doorn (NXP) | Paragraph 2.4 |
| 0.8 | 29/08/2014 | N. Pallaro (CRF) | Final version for ARTEMIS submission |

# TABLE OF CONTENTS

## LIST OF FIGURES



## LIST OF TABLES



## LIST OF ACRONYMS

| ABBREVIATION | DESCRIPTION |
|---|---|
| ADAS | Advanced Driver Assistance Systems |
| APS | Assisted Parking Systems |
| ASIL | Automotive Safety Integrity Level |
| AUTOSAR | AUTomotive Open System ARchitecture |
| BSA | Basic Set of Applications |
| BTP | Basic Transport Protocol |
| CAM | Cooperative Awareness Messages |
| CIWS | Cooperative Intersection signal information and violation Warning Systems |
| CSWS | Curve Speed Warning Systems |
| DENM | Distributed Environmental Notification Message |
| DESERVE | DEvelopment platform for Safe and Efficient dRiVE |
| E/E | Electrical/Electronic |
| ERBA | Extended-range backing aid systems |
| EUC | Equipment Under Control |
| FMVSS | Federal Motor Vehicle Safety Standards |
| FSRA | Full speed range adaptive cruise control |
| HW | Hardware |
| ICRW | Intersection Collision Risk Warning |
| ID | Identification |

| | |
|---|---|
| IEC | International Electro-technical Commission |
| IEEE | Institute of Electrical and Electronics Engineers |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| ITS | Intelligent Transport Systems |
| IWI | Information Warning Intervention |
| JASO | Japanese Automotive Standards Organization |
| KPI | Key Performance Indicators |
| LCDAS | Lane change decision aid systems |
| LCRW | Longitudinal Collision Risk Warning |
| LDM | Local Dynamic Map |
| LDWS | Lane departure warning systems |
| LKAS | Lane keeping assistance systems |
| LSF | Low speed following systems |
| MALSO | Manoeuvring Aids for Low Speed Operation |
| n.a. | Not applicable |
| NHTSA | National Highway Traffic Safety Administration |
| OS | Operating System |
| RHS | Road Hazard Signaling |
| SAE | Society of Automotive Engineers |
| SoC | System on Chip |
| SPICE | Software Process Improvement and Capability determination |
| SW | Software |
| TIWS | Traffic Impediment Warning Systems |
| UNECE | United Nations Economic Commission for Europe |
| V2I | Vehicle-to-Infrastructure |
| V2V | Vehicle-to-Vehicle |
| WG | Working Group |

# 0. EXECUTIVE SUMMARY

The **purpose of D723 deliverable** (output of work package 7.2, dealing with the exploitation, standardisation and regulatory issues) is to compile a collection of European and national regulations regarding embedded systems and the research activities undertaken in DESERVE.

This collection will be preparatory to highlight any regulatory issue that will have any impact in fulfilling the dissemination and exploitation plan.

The Standards (or norms) and Regulations have been divided in five categories:

- **General**: referring to functional safety, process and architecture assessment, and quality management.
- **ADAS**: ISO standards for performance requirements and test procedures of ADAS systems;
- **Automation**: about the level of automation of vehicles.
- **Communication**: standards being proposed and finalized in ETSI and IEEE for cooperative applications.
- **ITS architecture reference**: the systems need to co-exist and operate within a known and supportive architectural framework.

The DESERVE framework addresses these standards and regulations with **different level of application**, having in mind what is mandatory for industrial use and what is planned to be implemented and demonstrated in the project on a prototype-level.

For instance, critical requirements like AUTOSAR compatibility, SPICE compliance and functional safety (ISO 26262) are mandatory for industrial use of the platform but they cannot be implemented in the DESERVE platform because not enough resources were allocated for that. Nevertheless all the work done for the "non-industrialized" DESERVE platform can be (partly) reused or carried over to the industrialized version, where possible and appropriate.

The major technical risks dealing with the general DESERVE platform requirements, which are affected by the selected standards and regulations, have been identified, and the countermeasures have been described for each risk in the **contingency plan**.

# 1. INTRODUCTION

## 1.1 Objectives and scope of the document

The **purpose of the D723 deliverable** (output of work package 7.2, dealing with the exploitation, standardisation and regulatory issues) is to compile a collection of European and national regulations regarding embedded systems and the research activities undertaken in DESERVE [1][2]. This list will be preparatory for the analysis of the information collected to highlight any regulatory issue to be addressed in order to fulfil the dissemination and exploitation plan. A contingency plan will be also defined to address the issues identified in the analysis.

There are several kinds of regulations according to different countries and continents. For example, in United States the National Highway Traffic Safety Administration (NHTSA) has been in charge of writing and enforcing the Federal Motor Vehicle Safety Standards (FMVSS) as well as regulations for motor vehicle theft resistance and fuel economy. Another example is World Forum for Harmonization of Vehicle Regulations from the UNECE (United Nations Economic Commission for Europe) and the Japanese Automotive Standards Organization (JASO) in Japan. In recent years, different automotive manufacturers have been cooperating through the International Organization for Standardization to develop a standard methodology for evaluating and establishing the functional safety requirements for their electronics systems [3].

The definition and design of the planned validation tests will be conducted alongside the best practice sharing principle for test space design (e.g. V-cycle process) and by considering and respecting the guidelines, standard and regulations that are currently in force in that domain.
However, full compliance with specific standards like AUTOSAR during the test validation setup and for the validation tests itself is not foreseen in the DESERVE project [6]. Emphasis is more pointed towards a sound and reliable determination of the KPI values for the different items that can be rated.
ASIL-related safety concepts pursuant to ISO26262 are not addressed within the DESERVE rapid prototyping development platform and only relevant for SoC implementation or industrialization components in a later stage [6].

## 1.2 Structure of the deliverable

The report is structured with the following chapters:

- Chapter 1 (current one) provides an overview with the scope of the document and the structure in chapters;
- Chapter 2 summarises the **Standard and Regulations** considered for the development of the DESERVE project;
- Chapter 3 describes how those norms are applied within the DESERVE project;
- Chapter 4 provides the possible **Risks and Technical Issues** that may arise during the operating conditions and the **Contingency plan** that has been defined.

# 2. STANDARDS AND REGULATIONS

## 2.1 Introduction

In this chapter the standards and the regulations that are applicable or relevant to the DESERVE project are listed.

**Standards** (or **norms**) have the following characteristics and impacts on (automotive) products:

- mostly of recommendation style, thus their use is voluntary;
- established by consensus of all parties concerned;
- based on consolidated results of science, technology and experience;
- providing the state-of-the-art in the domain addressed;
- approved and published by recognised standardisation body.

The main features of **regulations** are:

- legislative measures, thus their use is mandatory;
- developed by an authority under public observation;
- providing technical specifications either directly or by reference, e.g. to standards.

Both standards and regulations could be addressed in DESERVE framework, but some of those apply only for "Industrialized Platforms". Anyway, they can give a good starting point for the embedded systems and the software modules of the DESERVE platform that will be reused in the future. The use and the influence of the norms and regulation, listed here, on DESERVE project is described in the next chapter.

The Standards (or norms) and Regulations have been divided in five categories:

- **General**: referring to functional safety, process and architecture assessment, and quality management.
- **ADAS**: ISO standards for performance requirements and test procedures of ADAS systems;
- **Automation**: about the level of automation of vehicles.
- **Communication**: standards being proposed and finalized in ETSI and IEEE for cooperative applications.
- **ITS architecture reference**: the systems need to co-exist and operate within a known and supportive architectural framework.

## 2.2 General

The main general Standards and Regulations considered for DESERVE development are described in the current paragraph. They refer to functional safety, process and architecture assessment, and quality management. Some of the standards are common for many production activities, but most of them are specific for automotive industry.

**Table 1 - List of General Standards**

| Standard | Title | Description |
|---|---|---|
| ISO 26262:2011 | Road vehicles - Functional safety | ISO-26262 represents the state of the art regarding the safety processes with the related methods and the safety requirements for the development, production, maintenance and decommissioning of E/E systems installed in series production passenger cars (currently with a max gross weight up to 3.5 t).<br>The standard ISO-26262 is based on the Functional Safety standard for Automotive Electric/Electronic Systems (IEC 61508).<br>It covers safety aspects of the entire development process:<br>• Requirements specification<br>• Design<br>• Implementation<br>• Integration<br>• Verification<br>• Validation<br>• Configuration<br>The ISO-26262 provides an automotive-specific risk-based approach for determining risk classes (Automotive Safety Integrity Levels, ASILs). The ASILs refers to a classification of inherent safety risk in an automotive system or elements of different systems. These are used in ISO-26262 to express the level of risk reduction required to prevent a specific danger. ASIL **D** is the highest level and ASIL **A** the lowest. |
| ISO/IEC 15504 | Information technology - Process assessment | ISO/IEC-15504, also known as SPICE (Software Process Improvement and Capability Determination), is a set of technical standards documents for the computer software development process and related business management functions.<br>It is the reference model for the maturity models (consisting of capability levels which in turn consist of the process attributes and of generic practices) against which the assessors can place the evidence that they collect during their assessment, so that the assessors can give an overall determination of the organization's capabilities for delivering products (software, systems, and IT services). |
| Autosar V4.1 Specifications | AUTomotive Open System ARchitecture | The AUTOSAR development partnership was formed in 2003. Now, eleven years later, AUTOSAR is mastering the growing complexity of automotive electric/electronic (E/E) architecture and has become the standard for automotive software.<br>The objectives of AUTOSAR can be summarized in: |

| Standard | Title | Description |
|---|---|---|
| | | • paves the way for innovative electronic systems that further improve performance, safety and environmental friendliness;<br>• is a strong global partnership that creates one common standard: "Cooperate on standards, compete on implementations";<br>• is a key enabling technology to manage the growing electrics/electronics architecture and complexity.<br>• facilitates the exchange and update of software and hardware over the service life of the vehicle. |
| ISO/TS 16949 | Quality management systems | ISO/TS-16949 defines the particular requirements necessary to apply the ISO-9001 to automotive production cycles.<br>The goal of this Technical Specification is the development of a quality management system that provides for continual improvement, emphasizing defect prevention and the reduction of variation and waste in the supply chain.<br>This Technical Specification, coupled with applicable customer-specific requirements, defines the fundamental quality management system requirements for those subscribing to this Technical Specification.<br>This Technical Specification is intended to avoid multiple certification audits and provide a common approach to a quality management system for automotive production, and relevant service part organizations. |
| ISO/IEC 15939 | Systems and software engineering - Measurement process. | The ISO/IEC-15939 identifies the activities and tasks that are necessary to successfully identify, define, select, apply and improve measurement within an overall project or organizational measurement structure. It also provides definitions for measurement terms commonly used within the system and software industries.<br>This International Standard does not catalogue measures, nor does provide a recommended set of measures to apply on projects. It does identify a process that supports defining a suitable set of measures that address specific information needs. |
| IEC 61508 | Functional Safety standard for Automotive Electric/Electronic Systems | IEC-61508 is intended to be a basic functional safety standard applicable to all kinds of industry. It defines functional safety as: "part of the overall safety relating to the EUC (Equipment Under Control) and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities."<br>The standard covers the complete safety life cycle, and may need interpretation to develop sector specific |

| Standard | Title | Description |
|---|---|---|
| | | standards. It has its origins in the process control industry.<br>Central to the standard are the concepts of risk and safety function. The risk is a function of frequency (or likelihood) of the hazardous event and the event consequence severity. The risk is reduced to a tolerable level by applying safety functions which may consist of E/E/PES and/or other technologies. While other technologies may be employed in reducing the risk, only those safety functions relying on E/E/PES are covered by the detailed requirements of IEC 61508. |

## 2.3 ADAS standards and regulations

In this paragraph ISO standards for performance requirements and test procedures of ADAS systems are listed. These norms are very specific for different ADAS applications that can be developed using the DESERVE platform. The DESERVE platform allows to develop the applications targeting from the beginning the related requirements described by the ISO standards.
The ISO standards of table 2 are developed by the ISO/TC 204 WG14 group, that has the scope of enhancing the standardization of information, communication and control systems in the field of urban and rural surface transportation, including intermodal and multimodal aspects thereof, traveller information, traffic management, public transport, commercial transport, emergency services and commercial services in the Intelligent Transport Systems (ITS) field.

**Table 2 - List of ADAS standards and regulations**

| Standard | Title |
|---|---|
| ISO 15622 | Intelligent transport systems — Adaptive Cruise Control systems — Performance requirements and test procedures |
| ISO 22179 | Intelligent transport systems — Full speed range adaptive cruise control (FSRA) systems — Performance requirements and test procedures |
| ISO 15623 | Intelligent transport systems — Forward vehicle collision warning systems — Performance requirements and test procedures |
| ISO 22839 | Intelligent transport systems — Forward vehicle collision mitigation systems — Performance requirements and test procedures |
| EU regulation 347/2012 | Implementing Regulation (EC) No 661/2009 of the European Parliament and of the Council with respect to type-approval requirements for certain categories of motor vehicles with regard to advanced emergency braking systems |

| Standard | Title |
|---|---|
| ISO 17386 | Transport information and control systems — Manoeuvring Aids for Low Speed Operation (MALSO) — Performance requirements and test procedures |
| ISO 17387 | Intelligent transport systems — Lane change decision aid systems (LCDAS) — Performance requirements and test procedures |
| ISO 17361 | Intelligent transport systems — Lane departure warning systems (LDWS) — Performance requirements and test procedures |
| ISO 11270 | Intelligent transport systems — Lane keeping assistance systems (LKAS) — Performance requirements and test procedures |
| ISO 22840 | Intelligent transport systems — Devices to aid reverse manoeuvres — Extended-range backing aid systems (ERBA) |
| ISO 16787 | Intelligent Transport Systems — Assisted Parking Systems (APS) — Performance Requirements and Test Procedures (currently in committee draft stage) |
| ISO 26684 | Intelligent Transport Systems – Cooperative Intersection signal information and violation Warning Systems (CIWS) - Performance requirements and test procedures (currently in draft international standard stage) |
| ISO 11067 | Intelligent Transport Systems – Curve Speed Warning Systems (CSWS) (currently in draft international standard stage) |
| ISO 18682 | Intelligent transport systems — Basic requirements for hazard notification systems (currently in working draft stage) |
| ISO 22178 | Intelligent transport systems — Low speed following systems (LSF) |
| ISO 15624 | Transport information and control systems — Traffic Impediment Warning Systems (TIWS) (currently in working draft stage) |
| ISO 19237 | Intelligent Transport Systems – Pedestrian Collision Mitigation Systems – Operation, Performance, and Verification Requirements (currently in preliminary working item stage) |
| TS 101 539-1 | Road Hazard Signaling (RHS), Applications.<br>Road Hazard Signaling is one of the applications within the defined Basic Set of Applications (BSA). This document describes the application requirements of the application. Goal of the application is present a warning between 6 and 30 seconds before actual collision. |
| TS 101 539-2 | Intersection Collision Risk Warning (ICRW), Applications.<br>Intersection Collision Risk Warning is one of the applications within the defined Basic Set of Applications (BSA). This document describes the application requirements of the application. Goal of |

| Standard | Title |
|---|---|
| | the application is to present a warning between 2 and 6 seconds before actual collision. |
| TS 101 539-3 | Longitudinal Collision Risk Warning (LCRW), Applications.<br>Longitudinal Collision Risk Warning is one of the applications within the defined Basic Set of Applications (BSA). This document describes the application requirements of the application. Goal of the application is to present a warning between 2 and 6 seconds before actual collision. |

## 2.4 Automation norms

The level of automation of vehicles has been defined, with minor differences, by various standardization bodies. Operational definitions for advanced levels of automation and related terms are included in the standards considered. In particular detailed definitions for the highest three levels of automation: conditional, high and full automation, in the context of motor vehicles and their operation on public roadways are described in the following standards.

**Table 3 - List of Automation norms**

| Standard | Title |
|---|---|
| SAE J3016 | Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems. |
| NHTSA | National Highway Traffic Safety Administration (NHTSA) Levels of automation |
| BASt | Legal consequences of an increase in vehicle automation |

## 2.5 Communication norms

In this paragraph the communications norms and regulations are listed. The DESERVE platform will include also ADAS systems that require vehicle-to-vehicle and vehicle-to-infrastructure communication.

A wide variety of standards are being proposed and finalized in ETSI and IEEE [13]. They have various degree of maturity. A few are finalized, most are under development. Figure 1 provides an overview of the core ETSI standards. All standards are linked to the layers in the software platform. Whether or not the standard is being proposed or finalized can be derived from the name of the standard:

- If the name of the standard starts with EN then the standard is finalized.
- If the name of the standard starts with TS or TR then the standard is being proposed.

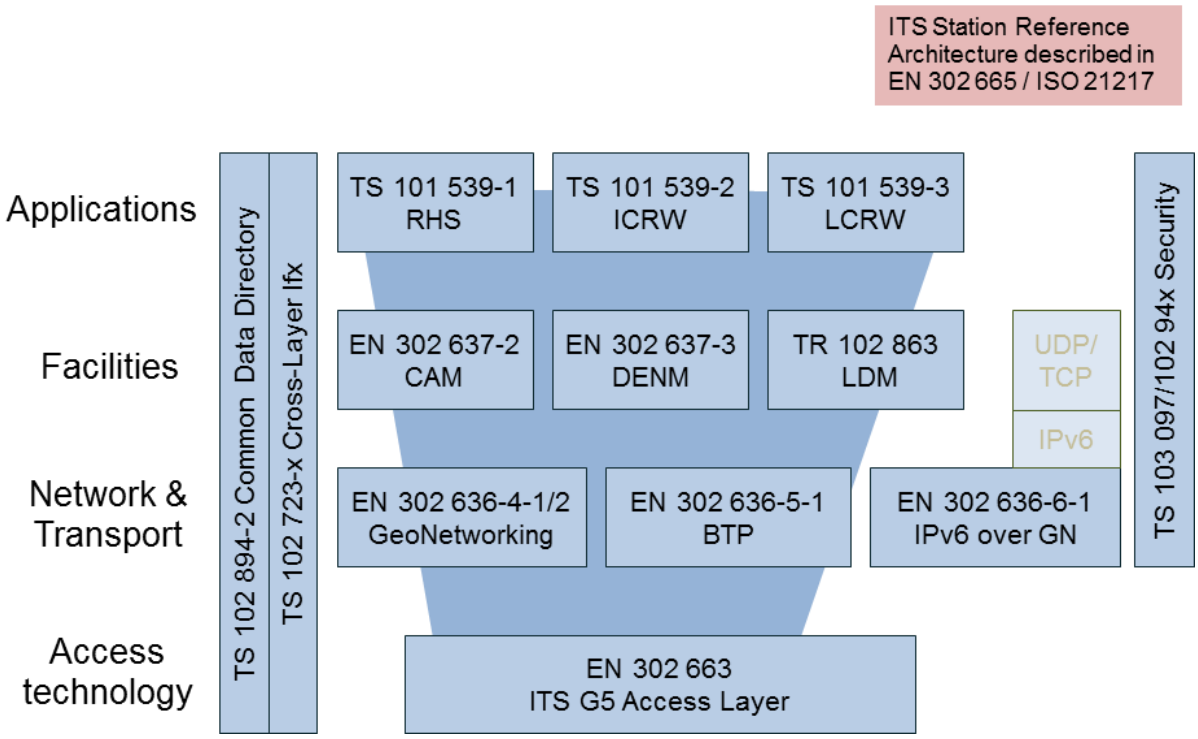


**Figure 1 - Core standards**

**Table 4 - List of Communication norms**

| Standard | Title |
|---|---|
| IEEE 802.11p | WAVE-Wireless Access for the Vehicular Environment |
| EN 302 637-2 | Cooperative Awareness Messages (CAM), Facilities.<br>This standard describes the format of the messages that are used to publish vehicle information. These messages contain current position, speed, direction etc. They are sent at a frequency from 2Hz to 10Hz, using a single-hop broadcast. |
| EN 302 637-3 | Distributed Environmental Notification Message (DENM), Facilities.<br>This standard describes the format of the messages that are used in case of special occasions, for example accidents and road condition warnings. These messages are sent based on events, using multi-hop or geonetworking broadcast. |
| EN 302 636-4-1/2 | GeoNetworking, Network & Transport.<br>This standard describes geographically bound communication, for example used to exchange information on road conditions. |
| EN 302 636-5-1 | Basic Transport Protocol (BTP), Network & Transport. |

| Standard | Title |
|---|---|
| | This standard describes the format of the low-level packets which are used as containers for the higher level messages. |
| EN 302 636-6-1 | IPv6 over GN, Network & Transport |
| EN 302 663 | ITS G5 Access Layer, Access technology.<br>This standard describes how the network is accessed. It is basically a mapping of IEEE802.11p incorporating European specific changes. |

## 2.6 ITS architecture reference norms

Intelligent transport systems (ITS) are systems deployed in transportation environments to improve both the driving experience and the safety and security of drivers, passengers and pedestrians. ITS can also assist in the labour, energy, environmental and cost efficiency of transportation systems. It is a feature of most ITS that their architecture involves the collection, use and exchange of information/data within and between software systems which affect or control the behaviour of physical equipment, providing a service to the actors involved in, or interacting with, the transport sector.
In order to maximize the efficiency of co-existing ITS, to obtain compatibility and/or interoperability and to eliminate contention, the systems need to co-exist and operate within a known and supportive architectural framework.
The ITS sector is still emerging and developing and is still close to the start of its evolution and application. The technology is developing and changing rapidly and ITS services have generally to make provisions not only for its interaction with other services, but with migration from one technology generation to later iterations.

**Table 5 - List of ITS architecture reference norms**

| Standard | Title |
|---|---|
| ISO 17356-3 | OSEK/VDX Operating System (OS) |
| ISO 14813 | Intelligent transport systems — Reference model architecture(s) for the ITS sector |
| ISO 28682 | Intelligent transport systems — Joint APEC-ISO study of progress to develop and deploy ITS standards |
| ISO 25102 | Intelligent transport systems — System architecture — 'Use Case' pro-forma template |
| ISO 25104 | Intelligent transport systems — System architecture, taxonomy, terminology and data modelling — Training requirements for ITS architecture |
| ISO 13185 | Intelligent transport systems — Vehicle interface for provisioning |

| Standard | Title |
|---|---|
| | and support of ITS services |
| EN 302605 / ISO21217 | Intelligent transport systems — Station reference architecture |
| TR 102 863 | Local Dynamic Map (LDM), Facilities.<br>This technical report describes the conceptual data store that is located within an ITS station. It contains information that is relevant to the safe and successful operation of ITS applications. Data can be received from a range of different sources such as vehicles, infrastructure units, traffic centers and on-board sensors. The data range from very static to highly dynamic data (road topography, static speed limit, signs and signals, road works, temporary speed limits, current information on vehicles or infrastructure nearby). |

# 3. APPLICATION OF STANDARDS AND REGULATIONS IN DESERVE FRAMEWORK

## 3.1 Norm Application

DESERVE development process has to adapt the actual **V-model cycle** in order to achieve the following main results:

- Provide a common environment for design, development and testing of ADAS functions;
- Provide a common environment for coexistence of ADAS functions;
- Allow reuse of pre-validated software components.

Within the DESERVE project the following **standards / regulations** have been considered in the definition process of requirements and specifications:

- The DESERVE development platform has been defined taking into account that general requirements such as AUTOSAR compatibility [6], SPICE compliance and functional safety (ISO 26262) [7][8][9][10][11] are mandatory for industrial use. But these requirements only apply for the "industrialized platform" and not for the prototype-style modules that are developed by the partners within the DESERVE project. Nevertheless all the work done for the "non-industrialized" DESERVE platform devices can be (partly) reused or carried over to the industrialized version.
- ISO performance requirements and test procedures for ADAS functions represent a necessary input for the V-model cycle development process; these standards have been taken into account for the ADAS applications addressed in DESERVE in order to guarantee that the minimum requirements are achieved in the DESERVE demonstrators.
- DESERVE platform will be validated considering also future introduction of cooperative solutions as Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications. The main communications and ITS architecture standards under definition will be addressed.

The norms considered for the development of the DESERVE project are summarised in the following table.

**Table 6 - Summary of norms and regulations used in DESERVE**

| Standard | Addressed Activity | Use |
|---|---|---|
| IEC 61508<br>ISO 26262:2011 | SP1 | For actuator and safety-critical task the spirit of ISO 26262 with the accompanying ASIL-levels will be considered but a full implementation of ISO 26262 is not foreseen in DESERVE. |
| ISO/IEC 15504 | SP1 | Full implementation of SPICE is not foreseen in DESERVE. |
| AUTOSAR 4.1 Specifications | SP1 | Module architecture, encapsulation and communication protocols from AUTOSAR V4.1 specifications are overtaken as far as possible. |

| | | |
|---|---|---|
| ADAS standards and regulations | SP4, SP5 | The vehicle demonstrators applications will be developed pursuant to the existing ADAS standards and ITS regulations. |
| Automation norms | SP4 | For automation the "iMobility WG automation group's" recommendations and guidelines will be applied. |
| Communication norms | SP5 | The EU cooperative applications are applicable in Deserve and the core ETSI standards are addressed. |
| ITS architecture reference norms | SP5 | Station reference architecture used for cooperative applications. |

## 3.2 Application software architecture

The baseline for DESERVE is represented by the results of past and on-going research projects [14][15], and in particular of interactIVe addressing the development of a **common perception framework** for multiple safety applications with unified output interface from the perception layer to the application layer [16].

In Figure 2 the DESERVE platform framework is shown, highlighting by a dashed line the different focus of DESERVE and interactIVe. The challenge of DESERVE is to go beyond interactIVe, targeting the **standardisation of a wider software architecture** including the Application and the Information Warning Intervention (IWI) platforms, in addition to the Perception platform already developed within interactIVe.

In this architecture the **Perception Platform** processes the data received from the sensors that are available on the ego vehicle and sends them to the **Application Platform** in order to develop control functions and to decide the actuation strategies. Finally, the output is sent to the **IWI Platform** informing the driver in case of warning conditions and activating the systems related to the longitudinal and/or lateral dynamics.

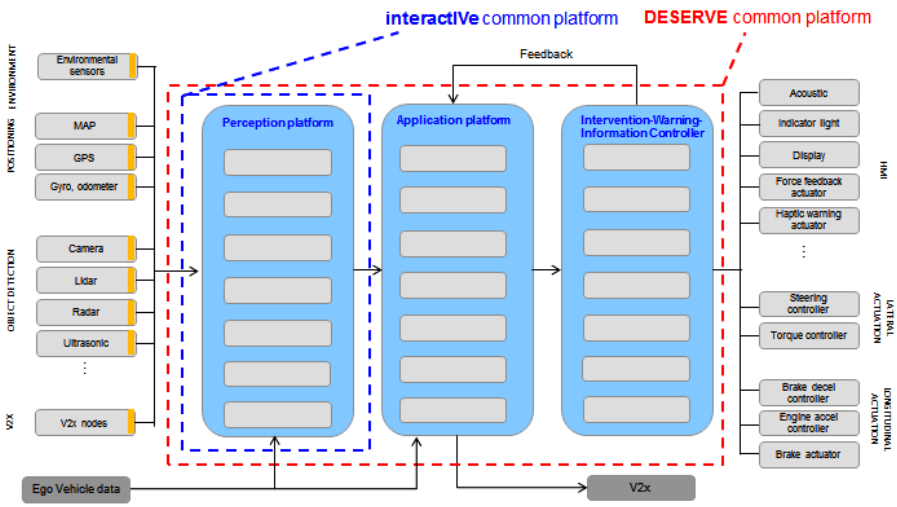


**Figure 2 - DESERVE Platform Framework**

# 4. RISK AND COUNTERMEASURES

## 4.1 Introduction

The main technical risks dealing with the general DESERVE platform requirements, affected by the standards and regulations described in chapter 3, are listed here. Below the tables 7 and 8 [12] describe respectively the identified risks (paragraph 4.2) and the related mitigation and contingency measures (paragraph 4.3).

## 4.2 Risk matrix

The technical risk matrix is presented in table 7 based on the following items:

- ID risk;
- risk definition;
- impact description;
- project activities at subproject level concerned by each risk;
- probability (High, Medium, Low) related to the risk occurrence;
- impact (High, Medium, Low) on the system if the risk occurs;
- global risk rating.

**Table 7 - Other Technical Risks**

| ID | Risk | Impact description | Addressed activities | **Probability** *How likely is to occur?* *[H, M, L]* | **Impact** *How bad will it be if it happens?* *[H, M, L]* | Rating |
|---|---|---|---|---|---|---|
| OthTecRi_1 | Lack of complete software modularity and reusability | - Less interoperability of SW modules<br>- Software cannot be partitioned (e.g. on separate processing units)<br>- The software application cannot be assigned to different SW developers<br>- The SW application cannot use standard libraries | SP1, SP2, SP3, SP4, SP5 | M | H | H |
| OthTecRi_2 | Software architecture not fully compatible with AUTOSAR standard | Limitations for the integration of applications from different suppliers inside a single processing unit and for the development of independent (hardware, operating system and communication technologies) software applications. | SP1, SP2, SP3, SP4, SP5 | H (in DESERVE) | L - fully implementation of AUTOSAR is not foreseen in DESERVE<br><br>H-beyond DESERVE | L - fully implementation of AUTOSAR is not foreseen in DESERVE<br><br>H-beyond DESERVE |
| OthTecRi_3 | Software development not fully compliant with ISO/IEC 15504 Information technology — Process assessment, also known as SPICE (Software Process Improvement and Capability Determination). | Higher efforts needed for the SW validation due to possible SW change request | SP2, SP3, SP4, SP5 | M (in DESERVE) | L-fully implementation of SPICE is not foreseen in DESERVE<br><br>H-beyond DESERVE | L-fully implementation of SPICE is not foreseen in DESERVE<br><br>H-beyond DESERVE |

| ID | Risk | Impact description | Addressed activities | **Probability** *How likely is to occur?* *[H, M, L]* | **Impact** *How bad will it be if it happens?* *[H, M, L]* | Rating |
|---|---|---|---|---|---|---|
| OthTecRi_4 | Software development not compliant to ISO26262 standard defining the "Functional Safety Assessment". | Safety requirements could not be completely implemented during the SW development with possible legal impacts. | SP2, SP3, SP4, SP5 | H (in DESERVE) | L-fully implement ation of ISO26262 is not foreseen in DESERVE<br><br>H-beyond DESERVE | L-fully implement ation of ISO26262 is not foreseen in DESERVE<br><br>H-beyond DESERVE |
| OthTecRi_5 | Application software not fully independent from hardware | Software code customisation for different HW targets | SP2, SP3, SP4, SP5 | M | M | M |
| OthTecRi_6 | The perception modules shall not be implemented in a programming language which is independent of the operating system | If the programming language depends on a dedicated operating system, it is very difficult to industrialize it later on | SP2, SP3, SP4, SP5 | M | M | M |

## 4.3 Countermeasures matrix

In this section the matrix with the major countermeasures related to each risk is provided:

- mitigation measures to reduce the probability that the risk will materialize;
- contingency measures to reduce the impact if a risk does materialize.

**Table 8 – Other Technical measures**

| ID | Risk | Impact description | Mitigation Measures<br>*How can you reduce the Probability* | Contingency Measures<br>*How can you reduce the Impact* |
|---|---|---|---|---|
| OthTecRi_1 | Lack of complete software modularity and reusability | - Less interoperability of SW modules<br>- Software cannot be partitioned (e.g. on separate processing units)<br>- The software application cannot be assigned to different SW developers<br>- The SW application cannot use standard libraries | To define common (a) software architecture, (b) software modules specifications, (c) software interfaces guidelines. To implement software code compliant with the specifications. | To identify not compliant software modules and to redefine the high level architecture (review of SW modules and/or addition of new SW modules) to reach modularity. |
| OthTecRi_2 | Software architecture not fully compatible with AUTOSAR standard | Limitations for the integration of applications from different suppliers inside a single processing unit and for the development of independent (hardware, operating system and communication technologies) | In order to mitigate the probability … beyond DESERVE it is needed to avoid the design of software modules already defined in AUTOSAR standard | Not addressed in DESERVE Review of software code after development (beyond DESERVE) |

| ID | Risk | Impact description | Mitigation Measures<br>*How can you reduce the Probability* | Contingency Measures<br>*How can you reduce the Impact* |
|---|---|---|---|---|
| | | software applications. | | |
| OthTecRi_3 | Software development not fully compliant with ISO/IEC 15504 Information technology — Process assessment, also known as SPICE (Software Process Improvement and Capability Determination). | Higher efforts needed for the SW validation due to possible SW change request | Implementation of ISO/IEC 15504 from the beginning | Not addressed in DESERVE Requalification of software code after development (beyond DESERVE) |
| OthTecRi_4 | Software development not compliant to ISO26262 standard defining the "Functional Safety Assessment". | Safety requirements could not be completely implemented during the SW development with possible legal impacts. | Implementation of software development framework consistent with ISO26262 from the concept phase. | Development of ADAS functionalities including software safety requirements based on the consortium skills for the addressed applications |
| OthTecRi_5 | Application software not fully independent from hardware | Software code customisation for different HW targets | Development of software layers allowing the separation between the physical layer and the application code | To identify hardware-dependent software modules in order to evaluate functional partitioning on HW targets and to define standard interfaces. |
| OthTecRi_6 | The perception modules shall not be implemented in a programming language which is independent of the operating system | If the programming language depends on a dedicated operating system, it is very difficult to industrialize it later on | Development of middleware allowing the separation between the operating system and the application code. | To identify OS-dependent software modules in order to evaluate functional partitioning on specific drivers to be implemented in standard modules. |

# 5. CONCLUSIONS

The present report has described the major European and national standards and regulations regarding embedded systems and the research activities undertaken in DESERVE.

The DESERVE framework addresses these standards and regulations with different level of application, having in mind what is mandatory for industrial use and what is planned to be implemented and demonstrated in the project on a prototype-level.

For instance, critical requirements like AUTOSAR compatibility, SPICE compliance and functional safety (ISO 26262) are mandatory for industrial use of the platform but they cannot be implemented in the DESERVE platform because not enough resources were allocated for that. Nevertheless all the work done for the "non-industrialized" DESERVE platform can be (partly) reused or carried over to the industrialized version, where possible and appropriate.

Besides the major technical risks dealing with the general DESERVE platform requirements, which are affected by the selected standards and regulations, have been identified, and the countermeasures have been described for each risk.

# REFERENCES

[1] www.deserve-project.eu

[2] DESERVE consortium, *DEvelopment platform for Safe and Efficient dRiVE*, Technical Annex Part B, 31.01.2013

[3] The safety Promise and challenge of Automotive electronics, Transportation Research Board SPECIAL REPORT 308, National Research Council of the national academies, USA, 2012.

[4] *D111 Application Database*, DESERVE

[5] *D121 Development Platform Requirements*, DESERVE

[6] AUTOSAR, www.autosar.org

[7] ISO 26262, Road vehicles - Functional safety (www.iso.org)

[8] Y. Papadopoulos, M. Walker, M.O. Reiser, M. Weber, D.J. Chen, M. Törngren, D. Servat, A. Abele, F. Stappert, H. Lönn, L. Berntsson, R. Johansson, F. Tagliabo, S. Torchiaro, A. Sandberg - *Automatic Allocation of Safety Integrity Levels*, 1st Workshop on Critical Automotive Applications: Robustness & Safety, CARS 2010 (EDCC Workshop), Valencia, Spain, 27 April 2010

[9] F. Tagliabo, S. Torchiaro, H. Lönn, R. Johansson, D.J. Chen, Y. Papadopoulos, M. Walker, A. Sandberg - *Modelling Support for the Automotive Functional Safety Standard*, IEEE Dependable Computing Systems (DEPCOS'11), Brunow Palace, Poland, June 27- July 1, 2011.

[10] D.J. Chen, R. Johansson, H. Lönn, H. Blom, M. Walker, Y. Papadopoulos, S. Torchiaro, F. Tagliabo, A. Sandberg - *Integrated Safety and Architecture Modeling for Automotive Embedded Systems*, e&i - elektrotechnik und informationstechnik, Volume 128, Number 6, Automotive Embedded Systems. Springer Verlag, 2011. ISSN 0932-383X / 1613-7620

[11] A. Sandberg, D.J. Chen, H. Lönn, R. Johansson, L. Feng, M. Törngren, S. Torchiaro, R. Tavakoli-Kolagari, A. Abele - *Model-based Safety Engineering of Interdependent Functions in Automotive Vehicles Using EAST-ADL2*, Lecture Notes in Computer Science, Volume 6351, Series: Computer Safety, Reliability, and Security (SAFECOMP), Pages 332-346. Springer Berlin / Heidelberg, 2011. ISSN 0302-9743

[12] *D822 Risk Managemenet and Contingency Plan*, DESERVE

[13] *D451 Cooperative systems functions,* DESERVE

[14] www.interactive-ip.eu

[15] www.haveit-eu.org

[16] S. Durekovic (NAVTEQ), Perception Horizon: Approach to Accident Avoidance by Active Intervention, Workshop "How can new sensor technologies impact next generation safety systems?" IEEE IV 2011, June 5 2011, Baden – Baden

# ANNEX

n.a.