SAFESPOT INTEGRATED PROJECT - IST-4-026963-IP

Core Architecture Requirements

SubProject No.	**SP7**	**SubProject Title**	**SCORE**
Workpackage No.	**WP2**	**Workpackage Title**	**Requirements Convergence**
Task No.	**-**	**Task Title**	**-**
Authors (per company, if more than one company provide it together)		**Main authors :** Abdel Kader Mokaddem, Renault Elena Balocco, CRF **Contributors:** Fulvio Tagliabò, CRF Achim Brakemeier, DC Dominique Vilain, Cofiroute Miguel Angel Guijarro, CETECOM Angela Spence, MIZAR	
Status (F: final; D: draft; RD: revised draft):		**RD**	
Version No:		**2.2**	
File Name:		**D7.2.1 Core Architecture Requirements v 2.2**	
Issue Date:		**8/5/2010**	
Project start date and duration		**01 February 2006, 48 Months**	

Revision Log

Version	Date	Reason	Name and Company
1.0	27/6/06	First Draft, table of contents Introduction of requirements: - Safety systems and applications requirements - Security requirements	Abdel Kader Mokaddem, Renault
1.1	11/7/06	Inputs: communication system requirements	Abdel Kader Mokaddem, Renault
1.2	13/7/06	Inputs: Quality of Service	Dominique Vilain, Cofiroute
1.3	17/7/06	-Minor changes -Addition of requirements	Abdel Kader Mokaddem, Renault
1.4	18/7/06	-Inputs: communication system requirements -Inputs: term and abbreviations -stakeholder definitions	-Achim Brakemeier, DC -Miguel Angel Guijarro, CETECOM -Angela Spence, MIZAR
1.5	18/8/06	-Inputs: modularity & other general requirements -Executive summary, introduction - EITSFA Methodology	-Fulvio Tagliabò, CRF -Abdel Kader Mokaddem, Renault
1.8	6/9/2006	-Requirements finalization -Update	-Elena Balocco, CRF -Abdel Kader Mokaddem, Renault
2.0	26/9/2006	Integration of review comments	-Abdel Kader Mokaddem, Renault -Elena Balocco, CRF
2.3	19/10/2006	Updated Requirements tables inclusion	-Elena Balocco, CRF

Note: 1.6, 1.7, 2.1 are intermediate vesions used by a single partner.

Table of contents

ANNEXES

Annex I - High level User needs

EXECUTIVE SUMMARY

This document provides high level requirements for the SAFESPOT System architecture, as a global system including key sub-systems, namely the vehicles/On Board Units (OBU), the Road Side Units (RSU), and operational centers.

The Core Architecture Requirements document is intended to identify and gather the architecture information that would support developing the priority needs for standardization process.

The emergence of a standard in the field of cooperative Vehicle-to-Vehicle and Vehicle-to-Infrastructure communications for road safety should start from a common high level architectural context.

As reference user needs a selection of the ones identified in the European ITS Framework Architecture were assumed. The SAFESPOT project decided to consider this architecture as a starting point to be extended using the same methodological approach.

In the document a process flow of the requirements collection for the whole Integrated Project is defined as well as the template to be used for the capture of the detailed requirements defined in the other subprojects related to technologies and applications.

The document is composed by four chapters including an introductory part, a methodology description, the activity flow, the SAFESPOT stakeholders, the list and description requirements and a glossary . As well a list and description of the user needs is included in the annex.

Considering the system complexity, the deliverable should be considered as a living document subject to further step of harmonization deriving from the input of the other subprojects or feedback in the specification phase.

1. Introduction

1.1. Intended Audience

This document is the first deliverable of the SP7. It delivers a first global view on what is expected from the SAFESPOT system. Following a well structured and agreed methodology, the document provides the system architecture requirements derived from identified high level users or stakeholders and their needs.

These architecture requirements are shared with all the subprojects which are defining the detailed low level requirements. It will be used by the developers of the SAFESPOT system to verify how the specification and the implementation respond to the expressed requirements.

The Core Architecture Requirements document is also an official deliverable to the EC.

1.2. Structure of this document

The structure of this document is the following:

There is an introduction part explaining what is intended by this document and how it will be used later in the SAFESPOT project. Then the first chapter is dedicated to explain the methodology followed to find out the architecture high level requirements. This methodology is based on the European ITS Framework Architecture developed in the former European projects CONVERGE, KAREN then FRAME. The chapter explains also how the SAFESPOT activity flow was (re-)organized to respect a coherent process of work during this phase.

The following chapters present the stakeholders and high level user and, of course, the architecture high level requirements which are the core of this document.

Finally, there is a glossary of terms and abbreviations used in this document and also in all the SAFESPOT subprojects.

2. Methodology for the definition of architecture requirements

2.1. SAFESPOT WP2 Objectives

The objectives of WP2 (Work Package 2), related to the different SPs, can be achieved following the activity flow with the following main steps:

- To identify the entities (vehicles, infrastructure, hardware modules, software modules, etc.) involved in each of the SPs of SAFESPOT and consolidate them at a global architecture level.
- To identify Use Cases at SP level based on the defined entities and using a common template.
- To formulate system requirements at SP level based on a common framework.
- To implement system level interactions when new entities are introduced during the definition of use cases and system requirements.
- To consolidate all the collected results at global architecture level to attain an overall project system view. The process includes the solution and harmonization of conflicts and incoherencies as well as links with similar projects like CVIS.

2.2. European ITS Framework Architecture

This sub-chapter is intended to provide a brief introduction to the European ITS Framework Architecture and to give some indications regarding how it was used to support the work within SAFESPOT project, by providing in particular:

- a ‘checklist’ for compiling the high level User Needs for SAFESPOT
- a common terminology and definitions for the whole IP
- a methodology which will help to ensure compatibility and interoperability of SAFESPOT systems at European level.

2.2.1. What is it and why was it created?

The European ITS Framework Architecture (EITSFA) was created by the EC project KAREN (Keystone Architecture Required for European Networks) and was first issued in October 2000. It was the result of an effort to create a minimum stable framework for the deployment of workable and compatible Intelligent Transport Systems (ITS) in the European Union until at least 2010. It focuses principally on telematics applications in the field of road transport.

Why is such a framework necessary? The growing use of advanced telematic technologies in modern transport systems, their increasing complexity and the importance of ensuring integration and interoperability between systems, has made it increasingly necessary to have an underlying framework or conceptual structure. The purpose of a high level architecture such as this is to provide guidelines for the planning, design and implementation of ITS applications. A Framework Architecture provides strategic decision guidance, and covers not only the technical elements, but also organizational, legal and business aspects.

2.2.2. What does it consist of?

Below is a diagram of the typical contents of a Framework Architecture.

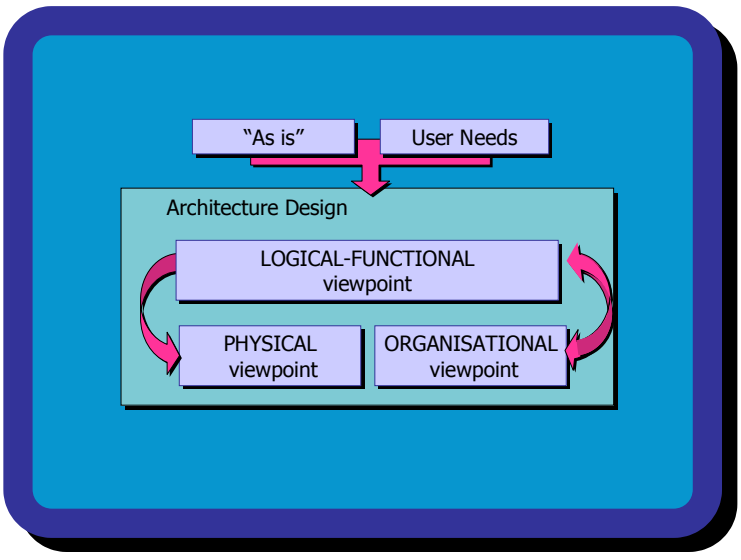

Figure 1 : Typical Contents of Framework Architecture

The elements related to SAFESPOT WP2 activity are described below.

2.2.3. User needs

The approach used by the Framework Architecture to proceed from the current state ("as is") to the definition of a new telematics-based system is a user-oriented process consisting of the following steps:

- Identify the Users (i.e. stakeholders)
- Define their expectations
- Organize these into categories to produce initial 'List of User Needs'
- Consult to gain endorsement, make modifications and improvements
- Produce a definitive List of User Needs (this list then serves as the basis for the definition of the System Requirements).

It is proposed that this process is adopted by SAFESPOT and that the European User Needs is used as a basis for defining these (in other words it can serve as a checklist). Those relevant to SAFESPOT would be selected and become the high level needs which would be the basis for more detailed User Needs for the individual subprojects.

The User Needs are divided into several categories (in bold the relevant categories for SAFESPOT) :

- **General**
- **Infrastructure Planning and Maintenance**
- Law Enforcement
- Financial Transactions
- **Emergency Services**
- **Travel Information and Guidance**
- **Traffic, Incidents and Demand Management**
- **Intelligent Vehicle Systems**
- Freight and Fleet Management
- Public Transport Management

When the high level SAFESPOT User Needs have been selected, they should be

listed in a table which shows which User is affected (see High Level User needs table in ANNEX).

It is also necessary first to identify the SAFESPOT Users or stakeholders. These will fall in various categories:

Road operators; Service Providers; Automobile Industry; System producers; Drivers and other road users; etc…..(see chapter 3) .

2.2.4. System Requirements

The System Requirements are directly derived from the user needs; it is the logical answer to the question “What should the developed system do to cover the expressed user needs?” or “What the future user of the system need this system to do?”

2.3. SAFESPOT WP2 Activity Flow

To define the SAFESPOT system requirements, it has been defined a common "activity flow" to be adopted to different subprojects SP1 SP2 SP3 SP4 SP5 and SP7. The activity flow describes the information or functions that are to be shared among the different SPs, highlights the Producer and the Consumer of that information. The WP2 Leader of each SP will verify the correct application in the respective SP. In the following picture it has been summarized the activity flow:

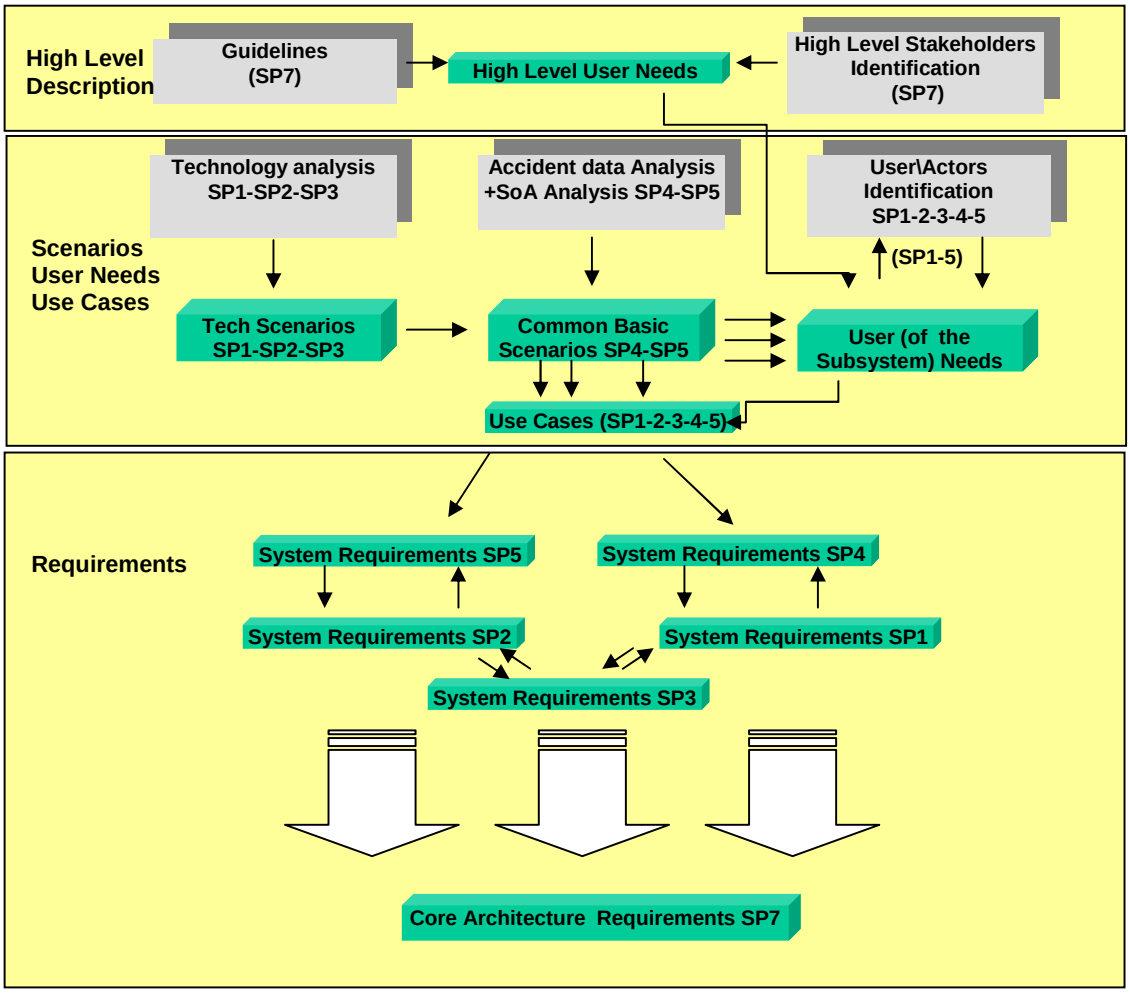

Figure 2: SAFESPOT WP2 Activity Flow

The activity flow selected is in line with the EITSFA approach [4].

The gray-boxes represent the "Tasks", the green-boxes represent the "Working-documents" to be shared among the different SPs.

It is important to highlight that these "Working-documents" aren't the "Official Deliverables" but a method to share information necessary to the different SPs to obtain the "Official Deliverables". If useful, it will be possible to include the "Working-documents" into the "Official Deliverables".

- **Guidelines (SP7):** to define the method to adopt to create the requirements, passing from user needs, scenarios, use cases. During this phase it will be defined a glossary and definition of terms (included at the end of this document) and the user needs.
- **High level Stakeholder (SP7)**: to identify the actors interested in the development of the whole system
  - **High level User Needs**: a working document will collect the user needs at system level, associated to the Stakeholders
- **Technology Analysis (SP1-SP2-SP3):**
  - **SP1:** to define a technological scenarios related to the sensors technology available on vehicle, considering traditional sensors and also innovative ones (like ADAS sensors).
  - **SP2**: to analyse the available technologies, to be adopted by the infrastructure, on the field of the vehicle dynamic positioning, sensors which will greatly improve the ability to detect safety-related events involving the driving environment and actuators.
  - **SP3**: to analyse the available technologies related to: accurate relative localization between vehicles (and, in some cases, also infrastructure), local dynamic maps and vehicular ad-hoc communication networking among vehicles.
- **Technology Scenarios (SP2-SP3)**: the technology analysis will allow to define working documents with technology scenarios.

- **Accident Data Analysis (SP5):** to analyze the main significant accidents data, that could occur, in order to identify a set of high safety-risk scenarios, i.e. accident black spots and safety-critical circumstances. This will take into consideration different road users (trucks, cars, motorbikes, bicycles and pedestrians), and conditions which may be specific to particular parts of Europe (risk of snow, ice, fog, etc). The aim is to describe clearly the combination of factors which lead to the safety risk.
- **State of the Art Analysis (SP4):** to define the state of the Art of the main applications available or developed in other European and Local Projects and technologies described in literature.
  - **Common Basic Scenario (SP4-SP5)**: the technology analysis, the accident analysis and the SoA analysis, will allow to define working documents for the common basic scenarios description.
- **User\Actors (SP1-SP2-SP3-SP4-SP5)**: to identify the user\actors relative at the different SP. These actors are different according to each SP point of view. Each SP defines a Subsystem with which an actor can interact. For example, the driver is an actor to the SP4 subsystem (application). This application is seen as an actor from the SP1 subsystem point of view.
  - **User Needs(SP1-SP2-SP3-SP4-SP5)**: starting from the different scenarios each SPs will provide a own user needs document
  - **Use Cases(SP1-SP2-SP3-SP4-SP5)**: starting from the different user needs each SPs will provide a own use case
  - **System Requirements (SP1-SP2-SP3-SP4-SP5)**: working documents where the system requirements are collected

3. High level users and Stakeholders

The stakeholders or high level users represent the actors interested in the development of the whole system. An actor is an external entity that represents the link between the SAFESPOT system and the outside World.

These users will be affected by, or have an effect on, the final system implementation. They are those who **want it**, those who **make it**, those who **use it** and those who **rule it**. They are defined in the EITSFA approach as follows:

Want it: These users want the system to solve (or diminish) traffic problems, or to provide travel information services to the public, e.g. city authorities, motorway operators, public transport operators, freight and fleet operators, police, etc.

Make it: Examples of this user category are system integrators, vehicle manufacturers, telecommunication operators, service providers, etc.

Use it: There are two categories of this class of user: primary and secondary. The primary users will benefit from the output of the systems, e.g. commuters, business users, leisure users, travellers with special needs, etc. The secondary users will control the system and provide the main input. Examples of this user category are traffic control operators and emergency services.

Rule it: The local and national authorities have the responsibility for issuing the regulations on how to implement and use the systems. The international authorities may also issue regulations, as well as standards and recommendations for international inter-operability. Examples of this user category are government ministries (transport, finance, etc.), European Union bodies, etc.

Name of Stakeholder	*Stakeholder description and aspirations*
Drivers : -Private Drivers -Commercial Drivers	End users of the On Board Unit system. A person driving any type of vehicle (equipped or not), including cars, commercial trucks, motorbikes, etc. In relation to the Infrastructure Platform, the driver is a receiver of the safety-related information generated. Will be concerned that the information arrives in time to prevent an incident, is easy and rapid to understand, is accurate, reliable and available at all times.
Road companies -Road Operators -Info Providers	Organisation responsible for maintaining the roads and managing the traffic on it.
Industry : -Car Makers -Suppliers	Manufacturers of the vehicle. Manufacturers, developers and suppliers of the OBU systems and the RSU systems
Public Authorities -Transport Ministries -Transport agencies	A public authority is a type of public benefit corporation that takes on a more bureaucratic role, such as the maintenance of public infrastructure that often has broad powers to regulate or maintain public property, laws and order. Will be concerned that the SAFESPOT system results in a substantial reduction in the number of accidents, injuries and deaths caused by road accidents (i.e. has low enough costs to permit widespread implementation) .It will also have a role in 'teaching' road users a new way of relating to (interpreting) the road infrastructure and will need to be informed of any modifications required in the Highway Code.

Exploitation : -Service providers -Infrastructure providers	Entity which is responsible for providing transport-related services which may include traveller information, emergency support for drivers, monitoring of hazardous goods, etc. Will be interested in being able to receive relevant safety-related data from the SAFESPOT systems (though the management of the services themselves are outside the scope of SAFESPOT).

Table 1 : Overview of high level users

4. Architecture Requirements

4.1. High level User Needs

For each of the high level user needs at system level, derived from EITSFA approach [4], the source of information of the collected data and their description should follow the format described in the following table.

Title	*explanation*
User need ID	Each user need has a unique ID number for traceability purposes. The format used is as follows: SP**X**_UN#ID_partnerID#_v1.#>
Definition of User Need	Each need must be written in a concise and precise manner, the meaning should be clear. The statements should start with “The user shall …”.
Rationale (optional)	Provide with a concise description of the reasons why this need should exist. If there is statistical data available, please make reference to it.
User need link to stakeholder	The user need shall be described with reference to an stakeholder. Whenever possible the agreed entity/actor definition to be used or another created. New entities should be communicated accordingly.

Table 2 : User Needs template table

The High Level User Needs are in **annex** to this document.

4.2. Presentation of Architecture Requirements

The overall system level requirements include system- and implementation-oriented details. They are described using (semi-) formal text techniques to capture all the requirements and might not be easy to read.

Primary requirements are governed by the user needs and use cases and include those derived by system engineers and system architects in order to give coherence and the operating characteristic to the complete system.

Following the system engineering formulation in EITSFA, the system requirements provide the information which is to be used for the formulation of the System Specifications and hence the definition of the system blueprint architecture, technologies, algorithms, etc. Within this context the types of system requirements identified following this approach are:

- **Functional requirements:** these specify the service(s) expected from the system, and/or the functions needed to provide a working system.
- **Non-functional requirements:** these specify the performance and/or quality attributes of a workable system.
- **Context requirements:** these specify the context within which the system is to operate, they include the constraints imposed by the environment and the effects that the system introduction might have on the operating environment. These include assumptions made on the environment, or statements as to what is needed for the system to work effectively under the agreed conditions.

In the following, some definitions will be used to identify the different roles of the SAFESPOT systems in a precise way:

- SAFESPOT Vehicle: a vehicle participating to the SAFESPOT system. A SAFESPOT vehicle may be a passive SAFESPOT vehicle or a SAFEPROBE vehicle
- Passive SAFESPOT vehicle: a passive SAFESPOT vehicle shall be able only to receive messages from the infrastructure or from other SAFEPROBE vehicles

- SAFEPROBE Vehicle: a SAFEPROBE vehicle shall participate actively to the SAFESPOT system. A SAFEPROBE vehicle shall be able at least to broadcast its own position to all other SAFESPOT Vehicles and to all RSU in a range of TBD meters
- RSU: the Road Side Unit is an infrastructure equipment able to exchange data with the SAFESPOT Vehicles and other infrastructure equipments

Title	***Explanation***
System requirement ID (Mandatory)	Each requirement has a unique ID number traceability purposes. The format used is as follows: SPX_REQ#ID_themeID#_partnerID#_v1.#> Where X is the Sub-Project Number The theme is related to the req classification (example_GEN related to a general requirement)
Name (Mandatory)	Denotes a unique name that complements the ID, but is easier to memorize.
System requirement Definition (Mandatory)	Each requirement supporting the implementation of a use case must be written in a precise and concise manner using the “shall” language (“The system shall” …). The use of formal methods in the form of modeling languages like UML 2.0 will facilitate the formulation of requirements.
System requirement Relevance (Mandatory)	This priority will help WP3 to prioritize the items to be developed during the system specifications. The value must either be: C – Critical, must be incorporated S – Significant, should be incorporated I – of Interest, may be incorporated.

Responsibility (Mandatory)	Specifies the organization and if possible the person responsible for implementing and maintaining a requirement.
Type of System requirement (Mandatory)	It can be Functional requirement, Non-functional requirement, or Context requirement.
Link to global architecture system requirement (Mandatory)	ID of the global architecture system requirement identified.
Conditions and Assumptions (Optional)	The conditions specify when the decision will be made and the criteria the decision will be based upon. The assumptions represent the facts we already know about the requirement or design decisions we already made.
Rationale (Optional)	Is an explanation why this requirement is necessary.
Originator (Optional)	When particular system requirements are included, the link with a given Sub-Project should be established. It should work as the *Client* to a particular requirement.

Table 3 : System Requirements template table

4.2.1. Modularity, Interoperability and other general aspects:

This group of requirements is partially derived from the “General” High Level User Needs (group1) and other ITS projects. It includes properties that either the SAFESPOT Architecture should possess, or that systems built in conformance to the SAFESPOT Architecture should possess.

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_001_MODUL_03_v1.0	System logic definition	The Safespot Architecture description shall include functional, information, physical and communication perspectives.	C	SP7	NF		general requirement needed for completeness	CRF
SP7_002_MODUL_01_v1.0	Reference models	The Safespot Architecture description shall include a number of reference models to describe the relationships between the services needed within the traffic and transport system.	C	SP7	NF			CRF
SP7_003_MODUL_01_v1.0	Glossary definition	The Safespot Architecture description shall include a glossary to explain all the main concepts described in the architecture.	C	SP7	NF			CRF
SP7_004_MODUL_01_v1.0	System update	The Safespot Architecture shall be provided in a form which enables it to be up-dated after delivery.	C	SP7	NF			CRF

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_005_MODUL_01_v1.0	Technology independence	The Safespot Architecture shall be technology independent.	C	SP7	NF			CRF
SP7_006_MODUL_01_v1.0	Modularity and scalability	The Safespot Architecture shall facilitate the creation of modular and flexible designs, so that manufacturers can produce their own versions of equipment and systems may be scaled to cover different range of functionality.	C	SP7	NF			CRF
SP7_007_MODUL_01_v1.0	Equivalent equipment	The Safespot Architecture shall allow equipment performing the same service to be provided by various suppliers.	C	SP7, SP1, SP2, SP3	NF		SAFESPOT shall be a standardised interoperable system	CRF
SP7_008_MODUL_01_v1.0	Function interoperability	The Safespot Architecture shall allow the same functions to be provided by various suppliers.	C	SP7, SP1-5	NF		Interaction should be possible between SAFESPOT & CVIS functions	CRF

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_009_MODUL_01_v1.0	Services interoperability	The Safespot Architecture shall support interaction between services provided by private and public bodies.	S	SP7,SP6	NF		Interaction should be possible between SAFESPOT & CVIS services	CRF
SP7_010_MODUL_01_v1.0	Responsibilities and liabilities	The Safespot Architecture shall allow current organisational responsibilities and legal liabilities to be retained.	C	SP7,SP6	NF			CRF
SP7_011_MODUL_01_v1.0	Migration from existing systems	The Safespot Architecture shall, where possible, describe migration path(s) that can be followed to enable architectures defined for existing traffic and transport management, as well as other ITS control and information systems, to become compliant.	S	SP7,SP6	NF			CRF
SP7_012_MODUL_01_v1.0	communication migration	The Safespot Architecture shall allow the use of existing and emerging communication infrastructures, or describe possible migration paths to explain how they can become compliant.	I	SP7,SP3	NF			CRF

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_013_MODUL_01_v1.0	Ontology	The Safespot Architecture shall provide a high level description of the message sets and data communication protocols to be used in data transfers.	C	SP7	NF			CRF
SP7_014_MODUL_01_v1.0	Data store and flow	The Safespot Architecture shall provide a high level description of data stores and data flows, and shall have a single data dictionary.	S	SP7	NF			CRF
SP7_015_MODUL_01_v1.0	System location communication	Systems that conform to the Safespot Architecture shall be able to locate a geographic area and exchange information about it in an unambiguous manner.	C	SP7, SP3	F			CRF
SP7_016_MODUL_01_v1.0	Road and traffic conditions	Systems that conform to the Safespot Architecture shall exchange information in a manner that permits road and traffic conditions to be understood by all parties.	C	SP7, SP4, SP5	F			CRF
SP7_017_MODUL_01_v1.0	High level message description	The Safespot Architecture shall provide a high level description of the message sets used to exchange data with external interfaces.	C	SP7	NF			CRF

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_018_MODUL_01_v1.0	Disabled and elderly people support	Systems that conform to the Safespot Architecture shall be able to provide facilities that accommodate the needs of disabled and elderly persons, when relevant.	C	SP4, SP5	F			CRF
SP7_019_MODUL_01_v1.0	Travel network data exchange	Systems that conform to the Safespot Architecture shall be able to provide facilities to enable data about the travel network to be entered and updated.	C	SP5	F			CRF
SP7_020_MODUL_01_v1.0	Global domain of application	The Safespot Architecture shall not constrain its functionality to be implemented in a single topographical domain, be it urban, inter-urban or rural, and by specific local organisations.	C	ALL	NF			CRF
SP7_021_MODUL_01_v1.0	Variety of user interfaces	The Safespot Architecture shall not constrain user interfaces to be of a particular type, or from a particular manufacturer.	C	SP7, SP4, SP5	NF			CRF
SP7_022_MODUL_01_v1.0	User interfaces operation	The Safespot Architecture shall not require that each of its user interfaces must operate on a specific item of equipment, unless it is for safety reasons.	S	SP7, SP4	NF			CRF

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_023_MODUL_01_v1.0	Compliance with privacy European law	The Safespot Architecture shall require all systems developed from it to comply with current European and National laws concerning data security, user anonymity and the protection of individual privacy.	C	SP7, SP3, SP6	NF			CRF
SP7_024_MODUL_01_v1.0	Traffic law compliance	The Safespot Architecture shall require all systems developed from it to comply with the traffic laws and regulations that apply in Europe.	C	SP7, SP6	NF			CRF
SP7_025_MODUL_01_v1.0	standardisation	The Safespot Architecture shall conform to relevant MoU, European directives and guidelines, and European (de facto-) standards.	C	SP7	NF			CRF
SP7_026_MODUL_01_v1.0	Quality and consistence of information	The Safespot Architecture shall provide functionality such that the quality of information content is continuous and consistent, both in time and space (i.e. as the traveller moves).	C	SP7, SP3	NF			CRF
SP7_027_MODUL_01_v1.0	functionality robusteness	The Safespot Architecture shall provide functionality that can accommodate environmental stress and infrastructure failures.	C	SP7, SP1-SP5	NF			CRF

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_028_MODUL_01_v1.0	multiple use of common data	Whenever possible and practical, the Safespot Architecture shall use the same data as input to several parts of its functionality.	S	SP7, SP4, SP5	NF			CRF
SP7_029_MODUL_01_v1.0	avoiding unnecessary data redundancy	The Safespot Architecture shall avoid the need for unnecessary multiple data sources or redundant data management.	S	SP7, SP1-SP5	NF			CRF
SP7_030_MODUL_01_v1.0	Safety services free of charge	The Safespot Architecture shall require all systems developed from it provide safety functionalities free of charge.	C	SP7	NF			CRF
SP7_031_MODUL_01_v1.0	Continuous upgrading	The Safespot Architecture shall allow systems developed from it to have an evolutionary development strategy that enables their continuous upgrading.	S	SP7, SP1-SP5	NF			CRF
SP7_032_MODUL_01_v1.0	General geographic operation	The Safespot Architecture shall provide services that are not constrained to operate in a particular geographic region.	C	SP7, SP1-SP5	NF			CRF
SP7_033_MODUL_01_v1.0	System repairability	The Safespot Architecture shall require all systems developed from it to be capable of being repaired.	C	SP7, SP1,SP2	NF			CRF

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_034_MODUL_01_v1.0	System maintainability	The Safespot Architecture shall require all systems developed from it to be easily maintainable with minimum disturbance.	C	SP1, SP2	NF			CRF
SP7_035_MODUL_01_v1.0	data accuracy certification	The Safespot Architecture shall enable all information systems developed from it to provide data with a stated accuracy, either as additional information or as part of the documentation, at all times.	C	SP7, SP1-SP5	NF			CRF
SP7_036_MODUL_01_v1.0	Input data validation	The Safespot Architecture shall require all systems developed from it to check all input data for validity, whenever possible, and to report failures.	C	SP7, SP1-SP5	NF			CRF
SP7_037_MODUL_01_v1.0	Input data accuracy	The Safespot Architecture shall enable all systems developed from it to check data values by comparing different sources, when available, so as to ensure high-accuracy and completeness.	C	SP7, SP1-SP5	NF			CRF
SP7_038_MODUL_01_v1.0	databases consistency	The Safespot Architecture shall require all systems developed from it to manage local/regional/national databases in a consistent way.	C	SP7, SP1-SP5	NF			CRF

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_039_MODUL_01_v1.0	data integrity and error detection	The Safespot Architecture shall allow all systems developed from it to be able to detect errors in operation, when higher integrity is required, e.g. for financial, security or safety reasons.	C	SP7, SP1-SP5	NF			CRF
SP7_040_MODUL_01_v1.0	System diagnosis	Systems that conform to the Safespot Architecture shall be able to monitor each safety-related component (including software), warn the user in case of problems, and disable it, or reduce it to a safe state.	C	SP1-SP5	F			CRF
SP7_041_MODUL_01_v1.0	System reliability	The Safespot Architecture shall require all systems developed from it to be reliable with respect to the legal and/or quality requirements necessary for each application.	C	SP7	NF			CRF
SP7_042_MODUL_01_v1.0	Operation independency from climatic and traffic conditions	The Safespot Architecture shall require all systems developed from it to be able to operate in all potential climatic and traffic conditions.	C	SP7, SP1-SP3	NF			CRF

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_043_MODUL_01_v1.0	User safety	The Safespot Architecture shall provide functionality that operates in a manner that does not generate a safety hazard for its users.	C	SP7, SP4, SP5	NF			CRF
SP7_044_MODUL_01_v1.0	Unsafe behaviour prevention	The Safespot Architecture shall provide functionality that operates in a manner that does not encourage unsafe behaviour.	C	SP7, SP4, SP5	NF			CRF
SP7_045_MODUL_01_v1.0	Degraded operation possibility	The Safespot Architecture shall provide functionality that operates in a safe manner during degraded modes of operation.	C	SP7, SP4, SP5	NF		SAFESPOT shall never create unsafe situation, at least fail safe behaviour should be maintained	CRF
SP7_046_MODUL_01_v1.0	human overriding	The Safespot Architecture shall provide functionality that is ultimately under the control of the human operator.	C	SP7, SP4, SP5	NF		In any case the SAFESPOT system can take over the responsability of human drivers	CRF

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_047_MODUL_01_v1.0	Ease of use	The Safespot Architecture shall ensure that the safety and security of systems developed from it are not compromised by their ease of use.	C	SP7, SP1-SP5	NF			CRF
SP7_048_MODUL_01_v1.0	low-cost technologies	The technologies adopted by the SAFESPOT system shall be potentially low-cost to ensure future high level penetration of the SAFESPOT system	C	SP1-SP3	NF			CRF
SP7_049_MODUL_08_v1.0	Non equipped user	The system should be able to provide non equipped users by SAFESPOT elaborated information as much as possible	C	SP2, SP5	F		a very probable expolitation scenario is a gradual diffusion of the system	Cofiroute
SP7_050_MODUL_08_v1.0	Open interface	The system architecture shall permit other traffic management system, existing or future, to receive and to use information	C	SP7	NF		easy system upgradability	Cofiroute

4.2.2. Security and integrity

This group of requirements provides general aspects of the level of security required for SAFESPOT system to work properly. It is also a result of a common workshop with CVIS and SEVECOM projects.

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_001_SECUR_03_v1.0	Privacy	The system shall protect the privacy of users, this means that their personal sensitive data are not transmitted	C	SP3,SP7 (sevecom)	F, NF			Renault
SP7_002_SECUR_03_v1.0	Traceability of user behaviour	The system shall not be used to trace the user/driver behavior (location, speed...)	C	SP3,SP7 (sevecom)	NF			Renault
SP7_003_SECUR_03_v1.0	Anonyme Identification	The system shall let the identification requirements be consistent with privacy requirements, which may require the anonymity of the driver.	C	SP3,SP7 (sevecom)	F, NF			Renault
SP7_004_SECUR_03_v1.0	Special vehicles Identification	The system shall allow identification (messages from) special vehicles (police, emergency...)	S	SP3,SP7 (sevecom)	F, NF		Privacy is less required with non personal vehicles.	Renault

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_005_SECUR_03_v1.0	Authentication architecture	The system shall use authentication security architecture mechanisms to simultaneously implement both identification and authentication requirements.	I	SP3,SP7 (sevecom)	F, NF			Renault
SP7_006_SECUR_03_v1.0	Authentication of RSU	The system shall allow distinguishing a public road infrastructure from a private (hacker's?) infrastructure.	C	SP3,SP7 (sevecom)	F, NF			Renault
SP7_007_SECUR_03_v1.0	Authorization	The system shall allow authorization mechanisms	S	SP3,SP7 (sevecom)	F, NF		e.g. Road clearance application is reserved for emergency and intervention vehicles even if the same system is used in the vehicle.	Renault

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_008_SECUR_03_v1.0	Integrity of the system	The system shall be able to prevent any undesirable means of destroying or damaging data and applications	S	SP1,SP2	F, NF			Renault
SP7_009_SECUR_03_v1.0	Integrity of data and communications	The system shall be able to ensure that communications and data can be trusted by checking that no unauthorized modification/creation/deletion was done.	C	SP3,SP7, sevecom)	F, NF			Renault
SP7_010_SECUR_03_v1.0	Intrusion alert	The system shall notify the user (driver, road operator...) in case of any intrusion to the system attempts.	S	SP3, SP7,(sevecom)	F, NF			Renault
SP7_011_SECUR_03_v1.0	tamper-proof device	The devices in vehicle and road side infrastructure should be tamper-proof.	I	SP3,SP7,(sevecom)	F, NF			Renault

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_012_SECUR_03_v1.0	Non-repudiation	A tamper-proof storing of all interactions/exchanges shall be possible.	I	SP1,SP2	NF		In case of accident it must be possible to make a reconstitution with all relevant elements (involved vehicles/RSUs, timestamps,...)	Renault
SP7_013_SECUR_03_v1.0	Degraded mode	The system shall detect if it is not working correctly by notifying the user in such case and switching to degraded mode with a minimum set of functions.	C	SP1,SP2	F		The degraded mode is intermediate state beween normal and failure mode.	TNO/Renault
SP7_014_SECUR_03_v1.0	Failure mode	The system shall detect if it is not working correctly by notifying the user in such case and switching to failure mode.	C	SP1,SP2	F			Renault

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_015_SECUR_03_v1.0	Survivability after failure	The system must be robust and able to survive accidental and intentional attacks on his integrity	I	SP1,SP2	F			Renault
SP7_016_SECUR_03_v1.0	Redundancy	The system should take into account redundancy mechanisms.	I	SP1,SP2	F			Renault

4.2.3. Performance

This group of requirements provides general aspects on the required performance of the SAFESPOT system in term of delay, accuracy, reliability and other criteria.

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_001_PERF_08_v1.0	Priority	The system shall assign priority to information to be transmitted to the users in accordance with their level of urgency	C	SP1-SP5	F		priority classification is needed for the best use of the available capacity	Cofiroute
SP7_002_PERF_08_v1.0	Latency	For each priority level, system shall be able to guarantee that the latency between originating event time and the information reception time by the user is lower a certain value defined for each priority level	C	SP1-SP5	F			Cofiroute
SP7_003_PERF_08_v1.0	Data Accuracy	The information provided in SafeSpot Architecture will be as accurate as achievable on the sensing/interpretation side and the uncertainty properties will be propagated together with the data itself. The applications should also process the uncertainty data and decide themselves about the proper actions under given circumstances.	C	SP1-SP5	F			Cofiroute

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_004_PERF_08_v1.0	False Alarm	The failure probability shall be given later in the project	C	SP1-SP5	NF			Cofiroute
SP7_005_PERF_08_v1.0	Reliability	The global reliability of the system shall be given later in the project	S	SP1-SP5	NF			Cofiroute
SP7_006_PERF_08_v1.0	Equity	All SAFESPOT vehicles with the same level of equipment shall benefit of the same service quality level	S	SP1-SP5	NF			Cofiroute
SP7_007_PERF_08_v1.0	Capacity	Communication capacity of the system shall guarantee that all high priority information shall be transmitted within the specified delay for the maximum possible vehicle density of the concerned section of road	C	SP3	NF		congestion control, preserving the mandatory messages	Cofiroute
SP7_008_PERF_08_v1.0	Message loss	The probability for the system user for not receiving information shall be given later in the project	S	SP1-SP5	NF			Cofiroute
SP7_009_PERF_08_v1.0	Minimum disturbance	The user disturbance due to display of information shall be as limited as possible	S	SP4	NF		avoiding user distraction and do not create habitude to unuseful messages that may lower attention to important messages	Cofiroute
SP7_010_PERF_08_v1.0	Event non-detection	The probability for the system not to detect an event shall be given later in the project	S	SP1-SP5	NF		Quality of service must be quantified	Cofiroute

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_011_PERF_01_v1.0	timely system response	Systems developed from the Safespot Architecture shall produce their output within a time that is sufficient to be useful, and within normal expectations,	C	SP1-SP5	NF			CRF
SP7_012_PERF_01_v1.0	information repetition	The Safespot Architecture shall require systems developed from it to be able to repeat information on request, in particular for those with special needs, where relevant.	C	SP4	F		to cover situations when an information is catched by the driver when firstly presented	CRF
SP7_013_PERF_01_v1.0	Positioning accuracy	All the SAFESPOT vehicles shall be able to compute their own location. The required accuracy will depend on the specific applications running on the vehicle	C	SP3	F			CRF
SP7_014_PERF_03_v1.0	Minimum Communication Range	The system shall support a minimum communication range in the order of ten meters (10m).	C	SP3	NF		exact range will be defined later	Renault
SP7_015_PERF_03_v1.0	Maximum Communication Range	The system shall support a maximum communication range in the order of one thousand meters (1000 m).	C	SP3	NF		exact range will be defined later	Renault
SP7_016_PERF_03_v1.0	Maximum Vehicle velocity	The system shall be able to operate with a traffic maximum speed of 200 km/h	C	SP3	NF			Renault

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_017_PERF_03_v1.0	Minimum density of mobile nodes	The system shall include a minimum density of OBUs.	C	SP3	NF		Minimum density for deployment of an operational system.	Renault
SP7_018_PERF_03_v1.0	Maximum density of mobile nodes	The system shall include a maximum density of OBUs.	C	SP3	NF		Maximum density to reduce packets collisions.	Renault
SP7_019_PERF_03_v1.0	Minimum density of static nodes	The system shall include a minimum density of RSUs	C	SP3	NF		Minimum density for deployment of an operational system.	Renault
SP7_020_PERF_03_v1.0	Maximum density of static nodes	The system shall include a maximum density of RSUs	C	SP3	NF		Maximum density to reduce packets collisions.	Renault
SP7_021_PERF_01_v1.0	user interface	All the information should be readable or audible in any climatic condition (rain, sun rays,…)	C	SP4	NF			CRF
SP7_022_PERF_01_v1.0	user interface customisation	The Safespot Architecture shall require systems developed from it to be able to have adaptable user interfaces that may be customised by the traveller, in particular those with special needs, where relevant.	C	SP4	F			CRF

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_023_PERF_01_v1.0	multiple user interfaces 1 (input)	The Safespot Architecture shall require systems developed from it to be able to take their input from a variety of alternative devices (e.g. keys, voice, buttons, touch-screen, smart card, etc.) to suit travellers with special needs, where relevant.	C	SP4	F			CRF
SP7_024_PERF_01_v1.0	multiple user interfaces 2 (output)	The Safespot Architecture shall require systems developed from it to be able to provide output in a variety of alternative modes (e.g. (enlarged) text, symbols, graphics, speech, tactile, HUD, etc.) to suit travellers with special needs, where relevant.	C	SP4	F			CRF
SP7_025_PERF_01_v1.0	user friendliness	The Safespot Architecture shall require all interactive systems developed from it to have a user interface syntax that is easy to learn and to remember (especially for users with specific needs).	C	SP4	F			CRF
SP7_026_PERF_01_v1.0	support for impaired users	The Safespot Architecture shall require systems developed from it to accommodate those users with one or more impairments (e.g. of upper/lower limbs/body, stature, coordination or power, vision, hearing, speech, cognition, epilepsy, etc.) where relevant.	S	SP4	F		Could have a very strong impact in addition to road safety.	CRF

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_027_PERF_01_v1.0	Common "look and feel"	The Safespot Architecture shall require all systems developed from it to have user interfaces with similar "look and feel" and similar end user assistance.	S	SP4	F			CRF
SP7_028_PERF_01_v1.0	system understandability	The Safespot Architecture shall require all systems developed from it to be simple and efficient for travellers to use, and easy to understand.	C	SP4-SP5	F			CRF
SP7_029_PERF_03_v1.0	Safe HMI	The vehicle shall present information to the driver in audible, visual or haptic form without impairing the driver's ability to control the vehicle in a safe manner.	C	SP4	F		The driver should not be disturbed by the system	Renault
SP7_030_PERF_03_v1.0	Speed limits	The system shall be able to display continuously to the driver the current mandatory speed limit.	C	SP4, SP5	F			Renault

4.2.4. Safety Systems and applications

This group of requirements is partially derived from the “Intelligent Vehicle Systems” High Level User Needs (group8) and other ITS projects. It includes the important functions required from a SAFESPOT system like collision detection, warning and support to the driver, and other applications that are to be specified.

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_001_APPLIC_03_v1.0	Position detection	All the SAFESPOT vehicles shall be able to receive the position of all neighboring SAFEPROBE vehicles and safety relevant objects	C	SP1, SP3	F		this information is fundamental in order to define the internal local dynamic map	Renault
SP7_002_APPLIC_01_v1.0	Position computation and transmission	All the SAFESPOT vehicles shall be able to compute their own location. All the SAFEPROBE vehicles shall be able to transmit their location to neighboring SAFESPOT vehicles and infrastructure.	C	SP3	F		as previous	CRF

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_003_APPLIC_03_v1.0	Driver impairment detection	The system shall be able to detect impairment of the driver, e.g. alcohol/drug abuse, drowsiness, sudden health problems, prolonged inattention, etc.	I	SP1,SP2, SP5	F		Interesting, considering the cooperative aspect of SAFESPOT	Renault
SP7_004_APPLIC_03_v1.0	Driver impairment warning	A SAFESPOT vehicle shall be able to warn the driver when a lack of alertness is detected.	I	SP1	F			Renault
SP7_005_APPLIC_03_v1.0	Driver impairment forwarding	A SAFEPROBE vehicle shall be able to warn surrounding drivers that this driver has a problem.	C	SP1, SP3	F		for cooperation,	Renault
SP7_006_APPLIC_03_v1.0	Road status detection	A sensor equipped SAFEPROBE vehicle able to decetct anomalous road surface condition (e.g.ice presence) through sensor fusion together with the vehicle dynamic characteristics, shall alert the driver (e.g. recommend an appropriate speed) and shall broadcast the warning to neighboring vehicles and RSU.	S	SP1, SP2	F		vehicle used as mobile sensor	Renault

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_007_APPLIC_01_v1.0	VRU detection	A sensor equipped SAFEPROBE vehicle/RSU detecting the presence of vulnerable road users (VRU), e.g. pedestrians, cyclists, animals, etc shall geo-broadcast this information to neighboring SAFESPOT vehicles	C	SP1, SP2	F			CRF
SP7_008_APPLIC_03_v1.0	Accident Data storage	A SAFEPROBE vehicle shall be able to record data about an accident and the journey immediately before (black box).	I	SP1, SP2	F	Can be used for accident data analysis.		Renault
SP7_009_APPLIC_03_v1.0	Virtual signals	A RSU able to detect the presence of traffic signs or information about the local traffic that may be useful to receive in advance (i.e. sudden traffic jam) shall broadcast this information to neighboring SAFESPOT vehicles	C	SP4, SP5	F	Traffic signs can be missed if the driver does not pay attention.		Renault
SP7_010_APPLIC_03_v1.0	Forwarding Virtual signals	A SAFEPROBE vehicle able to receive traffic signs and traffic information from RSU that are relevant to the current section of the road shall broadcast this information to neighboring SAFESPOT vehicles	S	SP3, SP4	F			Renault

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_011_APPLIC_03_v1.0	Obstacle detection	A RSU/SAFEPROBE vehicle shall monitor the area surrounding the vehicle to determine the proximity of other objects to the vehicle and detect the imminence of a collision. It shall broadcast this information to neighboring SAFESPOT vehicles	C	SP1, SP2, SP4	F			
SP7_012_APPLIC_03_v1.0	Vehicle tracking	A RSU/SAFEPROBE vehicle shall be able to monitor the course of the host vehicle		SP1, SP2, SP4, SP5				Renault
SP7_013_APPLIC_03_v1.0	RSU warning	The SAFESPOT vehicle shall receive warnings and collision avoidance data (intersection congestion, approaching vehicles, potential collision hazards, etc.) from the RSU or SAFEPROBE vehicles	C	SP1, SP2, SP4	F	The vehicles that are not equipped with detection sensors should benefit from those equipping the RSU		Renault

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_014_APPLIC_03_v1.0	Intersection collision warning	The SAFEPROBE vehicle shall provide intersection collision warnings to the driver about the presence of potentially hazardous situations and need for immediate collision avoidance action.	C	SP1, SP4	F			Renault
SP7_015_APPLIC_03_v1.0	Reduced visibility detection	The RSU/SAFEPROBE vehicle shall be able to measure the visibility distance and detect reductions caused by adverse weather and pollution conditions(but not darkness) of the view seen by driver	C	SP1, SP2	F			Renault
SP7_016_APPLIC_01_v1.0	Reduced visibility support	The system shall be able to support the driver in adverse visibility conditions, e.g. in fog, dakness etc	C	SP4, SP5	F			CRF
SP7_017_APPLIC_03_v1.0	Collision alarm	The RSU/SAFEPORBE vehicles shall be able to inform another vehicle when the host vehicle has detected that a collision is imminent.	C	SP4, SP5	F			Renault
SP7_018_APPLIC_03_v1.0	Lane warning	The system shall be able to provide support to the driver with information, to assist him/her to keep within the current lane of the carriageway.	S	SP1, SP2, SP4	F			Renault

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_019_APPLIC_01_v1.0	Speed limits	The SAFESPOT vehicle shall be able to receive mandatory speed limits from RSU and store them within the vehicle.	C	SP4, SP5				CRF
SP7_020_APPLIC_03_v1.0	Road information	The RSU/SAFEPROBE vehicles shall be able to provide information to SAFESPOT vehicles about various aspects of the road network, e.g. default speed limits, road hazards, junctions etc.	C	SP4, SP5	F			Renault
SP7_021_APPLIC_03_v1.0	Safety margins	The system shall be able to support a database of safety margins for distances between the vehicle and all other adjacent objects	C	SP4, SP5	F			Renault
SP7_022_APPLIC_01_v1.0	Lateral support	The RSU/SAFEPROBE vehicle shall be able to provide support to detect the position of all SAFESPOT vehicles relative to lane boundaries and/or roadway shoulders to determine safe trajectory.	C	SP1, SP2, SP4, SP5	F			CRF

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_023_APPLIC_08_v1.0	Data fusion	The SAFEPROBE vehicle shall be able to run applications that take into account information provided by on board sensors, other SAFEPROBE vehicles, RSU. The SAFEPROBE vehicle will merge all this information through proper data fusion strategies	C	SP1	F			Cofiroute

4.2.5. Communication system

This group of requirements is based on the functionalities expressed within the C2C-CC to specify vehicular ad-hoc communication systems for road safety.

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_001_COMM_03_v1.0	V2R Unicast	The system shall support two-way roadside-to-vehicle communication (point-to-point)	C	SP1, SP2, SP3	F		This requirements and the following ones are finalized to setup a dynamic network including SAFESPOT vehciles and RSU	Renault
SP7_002_COMM_03_v1.0	V2V Unicast	The system shall support two-way vehicle-to-vehicle communication (point-to-point)	C	SP1, SP2, SP3	F			Renault
SP7_003_COMM_03_v1.0	R2V geo-broadcast	The system shall support one-way roadside-to-vehicle communication (point-to-multi-point) by broadcasting to a specific area (geo-broadcast).	C	SP1, SP2, SP3	F			Renault
SP7_004_COMM_03_v1.0	V2V geo-broadcast	The system shall support one-way vehicle-to-vehicle communication (point-to-multi-point) by broadcasting to a specific area (geo-broadcast).	C	SP1, SP2, SP3	F			Renault

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_005_COMM_02_v1.0	Geo-anycast	The system shall be able to transport a message into a specific area (geo-anycast)	C	SP1, SP2, SP3	F			DC
SP7_006_COMM_02_v1.0	Multihop with geo-broadcat	The system shall be able to use multihop communication for geo-broadcast	C	SP3	NF			DC
SP7_007_COMM_02_v1.0	Congestion Control	The system shall use congestion control mechanisms	C	SP1, SP2, SP3	F		When a high density of node is reached the network need clear rules to maintain the best level of service	DC
SP7_008_COMM_02_v1.0	Power Control	The system shall use power control mechanisms to support the congestion control	C	SP1, SP2, SP3	F			DC
SP7_009_COMM_02_v1.0	Beaconing	The system shall use network layer beaconing with a period in the order of one second (1s)	C	SP3	F			DC
SP7_010_COMM_02_v1.0	Beacon Fields	The NL beacons shall contain at least the fields: identifier, position, timestamp, speed, heading	C	SP3	F			DC
SP7_011_COMM_02_v1.0	Routing	The routing for multihop shall be based on the NL beacons.	C	SP3	NF			DC

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_012_COMM_02_v1.0	Multi Channel Operation	The system shall support multi-channel operation, in case that several channels are designated for critical safety messages	C	SP3	F			DC
SP7_013_COMM_02_v1.0	Neighbor Table	The system shall maintain a neighbor table derived from received NL beacons	C	SP3	F			DC
SP7_014_COMM_01_v1.0	Integrity	The SAFESPOT system communication requires a high reliability frequency band to ensure reliable communication of safety inromation	C	SP7,SP3, COMeSafety	NF			CRF

4.2.6. Integration of safety centres

This group of requirements is partially derived from the “Emergency services” High Level User Needs (group5) and other ITS projects (GST, CVIS). It describes the required links to distant centers allowing a certain complementarity between the SAFESPOT system and what is developed within the other ITS projects.

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_001_SERV_02_v1.0	Emergency call support	The system shall provide informations to enhance the Minimum Set of Data used by May Day Call Application (eCall).	C	SP1, SP2, SP5	F			DC, Connexis
SP7_002_SERV_03_v1.1	GST Service support	The system shall be able to interface and to use the services provided by the GST infrastructure	C	SP1, SP2, SP5	F		e.g : On-board SAFESPOT system will have the ability to upgrade software by making a provisionning from a control center via an RSU.	Renault

ID	Name	Requirement Definition	Requirement Relevance	Responsibility	Type of Requirement	Conditions&Assumptions	Rationale	Originator
SP7_003_SERV_03_v1.1	CVIS Service support	The system shall be able to interface and to use the services provided by the CVIS infrastructure	C	SP1, SP2, SP5	F		e.g : On-board SAFESPOT system will have the ability to use data from traffic and travel informations centers via an RSU.	Renault

Conclusions and Next Steps

The methodology exposed in this document is following a global top down approach, starting from the identification of the users and actors of the SAFESPOT system as an innovative ITS system. It was considered in the analysis of the user needs all the relevant previous projects under the umbrella of the European ITS Framework Architecture initiative, but for the definition of the SAFESPOT core architecture requirements it was necessary to consider also a more Cooperative Safety System oriented initiatives and projects such as PReVENT, GST, CVIS and the C2C-CC results.

The core architecture requirements are also based on preliminary results expressed in other SAFESPOT sub projects, but give only a general overview of what the system should do. The more detailed requirements are defined in each sub projects and are linked to the general requirements defined in this document.

After the definition of the core architecture requirements, the architecture itself will be built based on the functional requirements. Functional modules will be mainly derived from the functional requirements as well as the data flows between these functional modules and also the actors of the systems.

This work will be performed during the WP3 phase and will require an iterative activity flow, similar to the one followed during the WP2, and involving all the SAFESPOT sub projects, to reach a consolidated architecture.

A closer cooperation will still continue with CVIS project to define the interfaces for an interoperable architecture and reach the objective of a common high level architecture.

Terms and abbreviations

List of acronyms

ADAS	Advanced Driver Assistance System
API	Application Programming Interface
ASN.1	Abstract Syntax Notation
ATCRF	Automobile Telematics Certification Reference Framework
ATSO	Automobile Telematic Stakeholders Organization (ATSO)
CA	Certification Authority
CALM	Continuous Air Interface, Long and Medium range
CAN	Controller Area Network
Car OEM	Car Original Equipment Manufacturer
CEN	Comité Européen de Normalisation
C2C – CC	Car to Car Communication Consortium
CVIS	Co-operative Vehicle-Infrastructure Systems (IP project, IST 027 293)
DSRC	Dedicated Short Range Communications
EC	European Commission
EITSFA	European Intelligent Transport Systems Framework Architecture
ETSI	European Telecommunications Standards Institute
EUCAR	European Council for Automotive R & D
FP6	Framework Programme 6
GPS	Global Positioning System
GST	Global System for Telematics (IP project)
HMI	Human Machine Interface
IEC	International Electrotechnical Commission
IEE	Institution of Electrical Engineers
IEEE	Institute of Electrical and Electronics Engineers
IP	Integrated Project
ISM	Industrial, Scientific and Medical
ISO	International Organization for Standardization
ISO/TC204	ISO Standardization of Transport Information and Control Systems (TICS)
ITS	Intelligent Transportation Systems
ITU	International Telecommunication Union
IUT	Implementation Under Test

KAREN	Keystone Architecture Required for European Networks
LDM	Local Dynamic Map
OBU	On Board Unit
OSCP	On-line Certificate Status Protocol
OSGi	Open Services Gateway initiative
OSI	Open System Interconnection
PKI	Public Key Infrastructure
QE	Qualified Equipment
QOS	Quality of Service
QP	Quality Plan
RFID	Radio Frequency IDentification
RSU	Road Side Unit
SCORE	SAFESPOT CORE architecture
SEVECOM	Secure Vehicle Communication
SLA	Service Level Agreement
SLS	System Level Specification
SMA	Safety Margin Assistance
SoA	State of Art
SP	Sub Project
TB	
TBC	To be confirmed
TBD	To be determined
TELCO	TELecommunication COmpany
TTL	
TS	Test Site
UML	Unified Modelling Language
UWB	Ultra Wide Band
VANET	Vehicle Ad Hoc Network
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
WAVE	Wireless Access in Vehicular Environments
WLAN	Wireless Local Area Network
WP	Work Package

Significant Terms within SCORE activities:

Term	Definition	Additional Explanation / Example
Actor	Is an external entity that represents the link between the SAFESPOT system and the outside World.	
Accreditation Body	Body that performs accreditations	One European accreditation Body may be responsible for the accreditation of Test Laboratories, Inspection Bodies and Certification Bodies. It has accepted the responsibility to carry out an additional evaluation of any certification body, any inspection body and/or any testing laboratory applying for accreditation based on the Frameworks for Competence in the Telematic Field, issued by the ECTA Committee It agrees to conduct an assessment of a potential certification body's, and/ or a potential Testing Laboratory's and/or a potential Inspection Body's ability to meet the requirement of the competence in the telematic field issued by the ECTA as well as assessment under the EN 45000 series Source: EN 45020:1998
Approval	Permission for a product, process or service to be marketed or used for stated purposes or under stated conditions	Source: EN 45020:1998
Body	Body that conducts Tests, Inspections, certification or Accreditation	Source: EN 45020:1998
Broadcast / Multicast Communication	When broadcasting, the message is sent simultaneously to all the users in the area. In Multicast, the message is transmitted to selected multiple recipients who have joined the appropriate multicast group. Multicast can be useful for those services which must be paid, like the dynamical navigation maps or some updates of the client system	
Certificate	Document issued under the rules of a certification system, providing confidence that a duly identified product, process, or service is in conformity with a specific standard or other normative document.	
Certification	Procedure by which a third party (also known as Certification Body) gives written assurance that a	The procedure includes a programme of verifications and

	product, process or service conforms to specified requirements	tests, which are designed to assess the conformity of a given manufacture's product with its SLA/SLS or technical specification
Conceptual Model	Top-level diagram that shows the whole system and explains how it works.	
Conformance Testing	Testing the extent to which an IUT is a conforming implementation.	Conformance Testing checks whether an implementation is implemented correctly with respect to the requirements stated in the relevant standard or specification. The purpose of Conformance testing is to determine to what extent a single implementation of a particular standard conforms to the individual requirements of that standard. Conformance testing establishes whether or not the implementation under test meets all of the requirements specified for the protocol itself.
Data Owner	Hold the rights of the raw data. For example in SAFESPOT, the data that makes the dynamical logic maps.	
Entity	An element which is part of the SAFESPOT system. Some entities can be decomposed in others.	For example: Hardware & Software Modules RoadSide Infrastructure
End User	Is an actor using SAFESPOT services (on a software/hardware platform installed into the car)	
FCD	Floating Car Data, is a method to determine the traffic speed on the road network. It is based on the collection of localisation data, speed, direction of travel and time information from driving vehicles. This data can be used as a source for traffic information	
Gentlemen Agreement	It is an informal agreement between parties, it can be either written or verbal.	
IEEE 802.11xx	IEEE 802.11 or Wi-Fi denotes a set of Wireless LAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802). The term is also used to refer to the original 802.11	The "xx" distinguishes between the different versions of the standard, being "p" the one for the ITS, currently under development.
Inspection Body	Body that performs inspections	Accreditation will be achieved by a recognized accreditation Body Source: EN 45020:1998
Interoperability	Ability of two systems to interoperate using the same communication protocol.	Source: ETSI TS 102 237-1
Mutual Recognition	Recognition agreement that covers the acceptance of one's party assessment results on the basis of a Certification Report by two or more parties.	
Risk Analysis	Examining potential problems, e.g., reliability of	

	technologies, uncertainty about sources and volume of revenue, potential stakeholder conflicts	
Road Operator	Organization responsible for maintaining the roads and managing the traffic on it.	
Role	Is a (set of) function(s) or task(s) that can be performed by an Entity or an Actor in a particular situation or use case. Each Entity or Actor can have more than one Role	
Road Side Unit / Infrastructure	Entity inside SAFESPOT architecture that interacts among others entities with the vehicles, content centre, control centre (TBC)	
Security	Preservation of confidentiality, integrity and availability of data.	Availability: meaning that authorized users have access to information and associated assets when required Confidentiality: Ensuring that information is accessible only to those authorized to have access Integrity: Safeguarding the accuracy and completeness of information and processing methods.
Stakeholder	Those interested in the development of the project. Each actor is also a stakeholder, but a stakeholder is not per definition an actor in the true meaning.	Those who: want it make it use it rule it
Stakeholder Aspirations	These consist of high-level objectives and requirements of all those Stakeholders involved in the ITS deployment, i.e., the users, operators, regulators and providers	
System Characteristics	All the features, properties and inherent difficulties that may have relevance for any of the stages in system realization	
System Concept	The basic description of the system as integrated from the perspectives from all contributing expertise domains.	
System Requirements	Provide information which is to be used for the formulation of the System Specifications and hence the definition of the system blueprint architecture.	
Template	A pattern used to create documents.	
Test	Technical operation that consists of determination of one or more characteristics of a given product, process or service according to a specified procedure.	
Test Body	The sequences of test steps that achieve the test purpose.	Source: ISO 9646
Test Case	Is the detailed set of instructions (or steps) that need to be taken in order to perform the test.	Source: ETSI TS 102 237-1
Test Laboratory	The laboratory where the compliance with the Service Level Agreement and the Service Level Specification is tested.	
UML	Unified Modeling Language can be used for	For further information and

	modeling the architecture of the system. It allows to analyze the requirements a design a solution to meet them. Although it is not a mandatory condition, the use of UML Use Case, Activity and Diagram is recommended, because that Diagrams would be useful in future phases of the project.	downloads, click on www.uml.org, including tools for using UML
Use Cases	From the User Needs, the Use Cases define a subset of the functionality of the system. They are used in a first approach to describe the behavior of a system without specifying its internal structure. An explanatory picture can be included, for example in JPEG format.	For formal presentation UML can be used.
User Needs / User Requirements	Statement in a natural language, of what services the system is expected to provide and the constraints under which it must operate.	
Validation Process	Final process for assuring the fulfillment of the initial objectives of the system.	
Viewpoint	When setting the Architecture of the System, different viewpoints can be selected, so the global architecture is defined through their definition.	For the RM-ODP approach, the viewpoints are: Enterprise Information Computational Engineering Technology Find More in http://www.rm-odp.net

References

[1] Cockburn A. Resources for writing use cases available at http://alistair.cockburn.us/usecases/usecases.html as of March 2006

[2] Ertico, Brussels, 6th EU Framework Programme, Global System for Telematics, GST Project, http://www.gstproject.org

[3] Jesty P.H at al "Guidance for the Development and Assessment of Intelligent Transport System Architecture, Framework IV Transport Telematics Project CONVERGE (TR1101, Deliverable 2.3, 1998)

[4] EITSFA approach, http://www.frame-online.net/library.htm

European ITS Framework Architecture: Overview, D3.6 Issue 1, Aug 2000 (KAREN) European Communities (2000)

European ITS Framework Architecture: List of User Needs, D2.02 Issue 1 Aug 2000 (KAREN) European Communities (2000)

[5] SAFESPOT SCORE Guidelines document: SCORE_SP7_Guidelines_for_UN_UC_Req_v2.0.doc

[6] Car 2 Car Communication Consortium, http://www.car-2-car.org