Deliverable

D31 European ITS Communication Architecture
Overall Framework
Proof of Concept Implementation

Version number 2.0
Lead contractor BMW Forschung und Technik GmbH
Confidentiality status PU
Due date of deliverable 31.10.2008
Actual submission date 05.03.2009

File name COMeSafety_DEL_D31_EuropeanITSCommunicationArchitecture_v2.0.doc
Authors

Richard Bossom, Siemens Traffic Controls
Roberto Brignolo, CRF
Thierry Ernst, INRIA
Knut Evensen, Q-Free
Alexander Frötscher, Austria Tech
Wolfgang Höfs, European Commission
Juhani Jääskeläinen, European Commission
Zeljko Jeftic, ERTICO
Paul Kompfner, ERTICO
Timo Kosch, BMW Forschung und Technik GmbH
Ilse Kulp, BMW Forschung und Technik GmbH
Antonio Kung, Trialog
Abdel-Kader Mokaddem, Renault
Andreas Schalk, Efkon
Elisabeth Uhlemann, Volvo Technology
Christian Wewetzer, Volkswagen
General Secretary
Rudolf Mietzner
cirquent
Zamdorfer Straße 120
81677 München / Germany
Phone +49 89 / 9936 1216
E-mail Rudolf.Mietzner@cirquent.de

Project Coordinator
Dr. Timo Kosch
BMW Forschung und Technik GmbH
Hanauer Straße 46
80992 München / Germany
Phone +49-89-382-41107
Fax +49-89-382-7044991
E-mail Timo.Kosch@bmw.de
## Revision chart and history log

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>05.03.2007</td>
<td>First draft</td>
</tr>
<tr>
<td>0.2</td>
<td>14.03.2007</td>
<td>Second draft, integration of comments</td>
</tr>
<tr>
<td>0.3</td>
<td>08.02.2008</td>
<td>Integration of project, workshops and standardisation results</td>
</tr>
<tr>
<td>0.4</td>
<td>22.02.2008</td>
<td>Refinement of overall structure</td>
</tr>
<tr>
<td>0.5</td>
<td>23.04.2008</td>
<td>New chapter policies</td>
</tr>
<tr>
<td>0.6</td>
<td>29.05.2008</td>
<td>Integration of contribution of chapter editors</td>
</tr>
<tr>
<td>0.7</td>
<td>05.06.2008</td>
<td>New chapter “Services and Application” and integration of missing contributions</td>
</tr>
<tr>
<td>0.8</td>
<td>10.06.2008</td>
<td>Integration of missing contributions</td>
</tr>
<tr>
<td>0.9</td>
<td>17.06.2008</td>
<td>Integration of missing contributions, new format and version for first review</td>
</tr>
<tr>
<td>0.95</td>
<td>26.06.2008</td>
<td>Integration of missing contributions</td>
</tr>
<tr>
<td>0.96</td>
<td>01.07.2008</td>
<td>Integration of missing contributions and some updates</td>
</tr>
<tr>
<td>0.98</td>
<td>08.07.2008</td>
<td>Final status before document workshop</td>
</tr>
<tr>
<td>1.0</td>
<td>05.08.2008</td>
<td>Final after review workshop, first delivery for overall review</td>
</tr>
<tr>
<td>1.1</td>
<td>18.09.2008</td>
<td>First work paper after second review workshop, restructuring and preparation for next review round</td>
</tr>
<tr>
<td>1.2</td>
<td>07.10.2008</td>
<td>Integration of updates chapter 1, 3, 6, 9, 10 and 13</td>
</tr>
<tr>
<td>1.3</td>
<td>08.10.2008</td>
<td>Editorial review, terminology harmonisation, introduction</td>
</tr>
<tr>
<td>1.4</td>
<td>16.10.2008</td>
<td>Integration of review comments</td>
</tr>
<tr>
<td>1.5</td>
<td>20.10.2008</td>
<td>Integration of further review comments, formatting, editorial changes</td>
</tr>
<tr>
<td>2.0</td>
<td>22.10.2008</td>
<td>Final first version for delivery</td>
</tr>
</tbody>
</table>
# Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal Disclaimer</td>
<td>11</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>12</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>13</td>
</tr>
<tr>
<td>1.1 Goal and purpose of the document</td>
<td>13</td>
</tr>
<tr>
<td>1.2 Document Structure</td>
<td>14</td>
</tr>
<tr>
<td>1.3 Intended audience and use of document</td>
<td>16</td>
</tr>
<tr>
<td>1.4 Related Projects and Organisations</td>
<td>16</td>
</tr>
<tr>
<td>1.4.1 COMeSafety</td>
<td>16</td>
</tr>
<tr>
<td>1.4.2 COOPERS</td>
<td>17</td>
</tr>
<tr>
<td>1.4.3 CVIS</td>
<td>18</td>
</tr>
<tr>
<td>1.4.4 SAFESPOT</td>
<td>20</td>
</tr>
<tr>
<td>1.4.5 SEVECOM</td>
<td>21</td>
</tr>
<tr>
<td>1.4.6 GeoNet</td>
<td>21</td>
</tr>
<tr>
<td>1.4.7 FRAME, E-FRAME</td>
<td>22</td>
</tr>
<tr>
<td>1.4.8 C2C Communication Consortium</td>
<td>23</td>
</tr>
<tr>
<td>1.4.9 ISO</td>
<td>23</td>
</tr>
<tr>
<td>1.4.10 ETSI</td>
<td>24</td>
</tr>
<tr>
<td>1.4.11 IEEE</td>
<td>24</td>
</tr>
<tr>
<td>1.4.12 IETF</td>
<td>24</td>
</tr>
<tr>
<td>2 Policies</td>
<td>25</td>
</tr>
<tr>
<td>2.1 In-vehicle Devices</td>
<td>25</td>
</tr>
<tr>
<td>2.2 Radio Spectrum</td>
<td>27</td>
</tr>
<tr>
<td>2.2.1 About the Radio Spectrum Policy</td>
<td>27</td>
</tr>
<tr>
<td>2.2.2 Commission Decision on harmonized use of the 5875 – 5905 MHz frequency band for ITS</td>
<td>28</td>
</tr>
<tr>
<td>2.2.3 Other Communications Technologies</td>
<td>29</td>
</tr>
<tr>
<td>2.3 Roadside equipment – additional issues</td>
<td>29</td>
</tr>
<tr>
<td>2.4 Liability</td>
<td>29</td>
</tr>
<tr>
<td>2.5 Security</td>
<td>30</td>
</tr>
<tr>
<td>2.6 Privacy</td>
<td>31</td>
</tr>
<tr>
<td>Part I: Architecture</td>
<td>32</td>
</tr>
<tr>
<td>3 ITS Communication Architecture - Description</td>
<td>32</td>
</tr>
<tr>
<td>3.1 Communication Architecture Terminology</td>
<td>32</td>
</tr>
<tr>
<td>3.2 European ITS Communication Architecture components</td>
<td>33</td>
</tr>
<tr>
<td>3.3 The ITS Station</td>
<td>34</td>
</tr>
<tr>
<td>3.4 Communication Scenarios</td>
<td>34</td>
</tr>
<tr>
<td>3.5 IPv6-based Communication Network</td>
<td>35</td>
</tr>
<tr>
<td>4 Scenarios, Applications, Use Cases</td>
<td>37</td>
</tr>
<tr>
<td>4.1 Basic Scenarios</td>
<td>37</td>
</tr>
<tr>
<td>4.2 Applications</td>
<td>39</td>
</tr>
</tbody>
</table>
8.3.3 GPS 80
8.4 Carrier Performance Summary 81
8.5 ITS Spectrum 83

9 Networking and Transport 84
9.1 Media-specific Communication Protocols 85
9.2 CALM 86
9.2.1 Architecture 87
9.2.2 Management 88
9.2.3 Groupcasting 89
9.2.4 Frame flow 91
9.3 Infrastructure controlled protocols 92
9.3.1 GPRS Communication Scenario 92
9.3.2 CALM-IR Communication Scenario 93
9.4 The VANET message frame structure 93
9.4.1 Lower layer frame structure 94
9.4.2 Networking Mechanism for the VANET Communication 96
9.4.3 Geobroadcast 97
9.4.4 Congestion Control 98
9.4.5 A design example: the SAFESPOT Router 99

10 Facilities 101
10.1 Local Dynamic Map (LDM) 104
10.2 The VANET messages 105
10.3 The common relevant information exchanged through the VANET 106
10.4 The Transport Protocol Data Unit (TPDU) 109
10.5 Protocol Data Unit 110
10.5.1 The “Cooperative Awareness Message” 111
10.6 Decentralized Environmental Notification Message 112
10.7 The Service TPDU 114
10.7.1 ServiceInit TPDU 114
10.7.2 ServiceAck TPDU 115
10.7.3 ServiceRq and ServiceRs TPDU 116
10.8 TPEG 116

11 Security 118
11.1 Introduction 118
11.2 Threats 120
11.3 Security Baseline Concepts 121
11.4 Security Architecture 122
11.4.1 Security Architecture Principles 122
11.4.2 Abstract Architecture: Conceptual View 123
11.5 Abstract Architecture: Other Views 126
11.5.1 Deployment View 126
11.5.2 Administration View 127
11.5.3 Integration View 127
## 12 System Management

### 12.1 Challenges

### 12.2 Implementation

### 12.3 Components

## Part III: Implementation

### 13 Organisational Topics

#### 13.1 CVIS

##### 13.1.1 General Concept

##### 13.1.2 The value network

##### 13.1.3 A value network example

##### 13.1.4 Central organisations

##### 13.1.5 Organisational configurations

#### 13.2 COOPERS

##### 13.2.1 General concept

##### 13.2.2 Identification of a basic Value Chain for Coopers Services

##### 13.2.3 Value chain example for COOPERS

#### 13.3 SAFESPOT

##### 13.3.1 Methodology: the six steps of the Organizational Architecture

## 14 Implemented Software Frameworks and Components

### 14.1 Overview table on available hardware and software

### 14.2 System Platforms

### 14.3 Communication Platforms

### 14.4 Software Frameworks & Modules

#### 14.5 Software Abstraction

##### 14.5.1 Roadside Gateway

##### 14.5.2 Roadside Station

## 15 Common Demonstration

### 15.1 Common test sites

### 15.2 Common demonstration at ITS World Congress Stockholm

### 15.3 Cooperative systems showcase event, spring 2010

## Annex 1 List of References used in each of the chapters

## Annex 2 Acronyms

## Annex 3 List of Annexes in separate documents

## Annex 4 Chapters and Chapter Editors
Table of figures

Figure 1: Scenarios for Cooperative Systems................................................................................. 13
Figure 2: European ITS Communication Architecture - Components...................................................... 14
Figure 3: Structure of Document and Correlation of Chapters .................................................................. 15
Figure 4: COMeSafety Overview Diagram.............................................................................................. 17
Figure 5: COOPERS Overview Diagram................................................................................................ 18
Figure 6: CVIS Overview Diagram......................................................................................................... 19
Figure 7: SAFESPOT Overview Diagram................................................................................................. 20
Figure 8: European ITS Communication Architecture – Ad-hoc Type of Communication......................... 33
Figure 9: European ITS Communication Architecture – Internet-based Type of Communication.............. 35
Figure 10: ITS Station Reference Architecture .......................................................................................... 37
Figure 11: C2C-CC Scenario Overview.................................................................................................... 38
Figure 12: ISO CALM Scenario Overview............................................................................................... 38
Figure 13: The Information Processing Cycle .......................................................................................... 46
Figure 14: System Views............................................................................................................................. 58
Figure 15: Overview of Cooperative Systems Technical Elements and Sub-systems................................. 61
Figure 16: Draft Reference Architecture of the Car2Car Communication Consortium................................. 62
Figure 17: Detail of the Access Technologies Block in the ITS Station Reference Architecture..................... 64
Figure 18: ITS Spectrum Overview........................................................................................................... 83
Figure 19: Details of the Network and Transport Block in the ITS Station Reference Architecture............... 84
Figure 20: CALM Layers............................................................................................................................ 87
Figure 21: CALM Communications Kernel............................................................................................... 88
Figure 22: Route Selection by CALM Management .................................................................................. 89
Figure 23: CALM Groupcasting................................................................................................................ 90
Figure 24: Service Provision using SAF and SCF..................................................................................... 91
Figure 25: Service Provision without SCF................................................................................................. 92
Figure 26: TCC to Vehicle Link via GPRS............................................................................................... 92
Figure 27: TCC to Vehicle Link via CALM............................................................................................. 93
Figure 28: PHY Frame............................................................................................................................... 94
Figure 29: MAC Frame............................................................................................................................... 95
Figure 30: LLC PDU.................................................................................................................................. 95
Figure 31: LSDU......................................................................................................................................... 95
Figure 32: Network Header......................................................................................................................... 95
Figure 33: ITS Station Reference Architecture: Facilities............................................................................ 101
Figure 34: Examples of Road Safety Scenarios........................................................................................ 103
Figure 35: General Connection Scheme................................................................................................ 104
Figure 36: LDM Concepts Illustration...................................................................................................... 104
Figure 37: Network Header and Transport Protocol Data Unit Structure.................................................. 110
Figure 38: General Structure of the Decentralized Environmental Message Payload
Figure 39: TPDU - ServiceInit A: only message identifiers
Figure 40: TPDU - ServiceInit B: message identifiers and local addresses
Figure 41: TPDU - ServiceInit C: message identifiers, local addresses and channel information
Figure 42: TPDU - ServiceInit D: broadcast data
Figure 43: TPDU - ServiceInit E: broadcast message with local addresses for reply
Figure 44: TPDU - ServiceInit F: broadcast message with local addresses for reply on a service channel
Figure 45: TPDU - ServiceAck A: acknowledgement of a service without enabling a session
Figure 46: TPDU - ServiceAck B: acknowledgement of a service with subsequent session
Figure 47: TPDU - ServiceRequest
Figure 48: TPDU - ServiceResponse
Figure 49: TPEG - Content and Delivery Segment
Figure 50: ITS Station Reference Architecture
Figure 51: Security Discussion Areas
Figure 52: Detail of the Security Block from the ITS Station Reference Architecture
Figure 53: Deployment View
Figure 54: Administration View
Figure 55: Integration View
Figure 56: ITS Station Reference Architecture: System Management
Figure 57: Typical Interference Paths
Figure 58: Conceptual Business Modeller
Figure 59: Value Network of Dangerous Goods / Cooperative Route Guidance Service
Figure 60: CVIS Organisational Example – Service Download
Figure 61: COOPERS Basic Value Chain
Figure 62: COOPERS Value Chain, TCC Operator as Integration
Figure 63: Demonstration Sites COOPERS, CVIS and SAFESPOT
Legal Disclaimer

The information in this document is provided "as is", and no guarantee or warranty is given that the
information is fit for any particular purpose. The above referenced authors shall have no liability for
damages of any kind including without limitation direct, special, indirect, or consequential damages that
may result from the use of these materials subject to any liability which is mandatory due to applicable
law.

Copyright 2008 by COMeSafety architecture task force.
Executive Summary

This document describes the baseline for a European ITS communications architecture for cooperative systems. It has been developed within the scope of the EC funded specific support action COMeSafety. It has been developed as a joint effort together with the EC funded projects COOPERS, CVIS and SAFESPOT and in cooperation with the Car2Car Communication Consortium, ETSI, IETF and ISO and with input from IEEE and SAE.

The document consists of three main parts. The first part takes on the overall architectural aspects, the second part concerns communication technologies and their specific use for the addressed application scenarios and the third part describes certain aspects of the communications network implementation.

This document will provide a basis for complementary work that will be done in liaison with the EC funded project PRE-DRIVE C2X to further prepare and support implementation and exploitation.

As the development of a European ITS communications architecture for cooperative systems is currently an ongoing process, the document will be continuously adapted and updated. For the time being, the COMeSafety project will act as a “host” for this communications architecture document. Later on the document ownership may be passed to a dedicated consortium.
1 Introduction

This document describes a baseline European ITS communications architecture for cooperative systems. It has been developed by the EC funded specific support action COMeSafety. Within this project an architecture task force with participants from other EC funded projects has been established. This document is one main result of this architecture task force.

1.1 Goal and purpose of the document

The goal of this document is to enable and facilitate conceptualization and specification of flexible, interoperable cooperative traffic and safety solutions based on agreed standards. From an implementation perspective this is illustrated in the following Figure 1, which shows the scenarios for cooperative systems in the road transport domain.

![Figure 1: Scenarios for Cooperative Systems](image)

Cooperation among road traffic participants and road traffic infrastructure requires communication capabilities. Figure 1 shows the actors in the transportation domain and ways for them to exchange information.

V2X is the acronym used to cover all types of communication to and from the vehicle. This includes vehicle to vehicle communication (V2V), vehicle to roadside communication (V2R and R2V) and vehicle to infrastructure communication (V2I and I2V).

From an architectural perspective the contents of the previous illustration is structured as the European cooperative ITS architecture view in Figure 2. This architecture is laid out in this document and comprises the four system parts Personal Station, Central Station, Vehicle Station and Roadside Station.

This document will expand on and discuss the elements of this diagram. It will include a discussion of the requirements on which it is based and provide the rational behind design principles. A certain architectural communication framework builds the core for the cooperative behaviour and the basis for all system stations. The components of this framework and how they are applied to the different stations will be expanded upon in the course of this document.
1.2 Document Structure

Besides the introductory part with introduction to the document and a discussion of policies the document has three main parts:

- Architecture: description of architectural aspects in a high level and general way
- Technology: description of communication technology in use
- Implementation: description of implemented prototypes and a first common demonstration of particular projects involved

The particular chapters are correlated as shown in Figure 3.
Figure 3: Structure of Document and Correlation of Chapters
The appendices provide a common terminology for communication technology for European cooperative systems and many additional information and documents to the particular chapters.

1.3 Intended audience and use of document

In order to achieve a common understanding of a basic V2X architecture the document is intended to be read, discussed, updated and maintained by all members of the architecture task force, the related projects as well as the COMeSafety Project Officer of the European Commission and subsequent projects.

The document may be a basis for the developer work of stakeholders in the safety solutions area (e.g. OEMs, authorities, telecommunication industries) as well as for IT-architects and developers of related research projects and the standardisation bodies.

The document itself is meant to give an overview of

- the scope of architecture in terms of goals, requirements and functionality (mandatory and optional)
- involved actors and entities
- required data (mandatory and optional).

On the other side, the document will not serve a fully fledged specification with respect to functionality and dynamic behaviour ready for an implementation project. The baseline architecture is independent from used technologies and describes a baseline European ITS communications architecture for cooperative systems in a very high-level and theoretical way. It will not provide technical solutions and a construction manual for cooperative systems.

After reading this document it should be possible to proceed in a concrete project.

1.4 Related Projects and Organisations

This section provides a brief overview of the projects and organisations involved in this document.

1.4.1 COMeSafety

Webpage: [http://www.comesafety.org](http://www.comesafety.org)
Start: January 2006
Duration: 4 years

The COMeSafety Project supports the eSafety Forum with respect to all issues related to vehicle-to-vehicle and vehicle-to-infrastructure communications as the basis for cooperative intelligent road transport systems.

COMeSafety provides a platform for both the exchange of information and the presentation of results. Regular electronic newsletters and publications at major conferences and press events complement the dissemination efforts. For European and worldwide harmonization, liaisons are established and workshops are organized to bring together the eSafety Forum and
all stakeholders. COMeSafety provides an open integrating platform, aiming for the interests of all public and private stakeholders to be represented.

Consolidated results and interests are submitted to the European and worldwide standardisation bodies. Especially the European frequency allocation process is being actively supported by participating in ETSI and CEPT technical groups. Relevant ISO and IEEE work will also be considered. With liaisons to all relevant stakeholders, the provision of information and preparation of strategic guidelines COMeSafety supports directly the eSafety Forum on the items of cooperative systems for road safety and traffic efficiency, which will speed up the system deployment.

COMeSafety actively supports the process of spectrum allocation for cooperative ITS systems as a common concern of all the related projects and as a basic requirement for a successful operation providing the expected impact on road safety.

**1.4.2 COOPERS**

[Image: COOPERS Overview Diagram]

**Webpage:** [http://www.coopers-ip.eu](http://www.coopers-ip.eu)

**Start:** February 2006

**Duration:** 4 years

COOPERS stands for COOPerative SystEms for Intelligent Road Safety and is a European research and development (R&D) and innovation activity within the Call 4 (Cooperative Systems and in vehicle integrated safety systems) of the 6th Framework Programme by the European Commission - Information Society and Media.

Hereby COOPERS focuses on the development of innovative telematics applications on the road infrastructure with the long term goal of a “Cooperative Traffic Management” between...
vehicle and infrastructure, to reduce the self opening gap of the development of telematics applications between car industry and infrastructure operators.

The goal of the project is the enhancement of road safety by direct and up to date traffic information communication between infrastructure and motorised vehicles on a motorway section.

The validation and test drives of the COOPERS system concept will be performed on public motorway sections in France, Belgium/Netherlands, Germany (Berlin and Bavaria), Austria and Italy.

1.4.3 CVIS

CVIS (Cooperative Vehicle-Infrastructure Systems) is a major new European research and development project aiming to design, develop and test the technologies needed to allow cars to communicate with each other and with the nearby roadside infrastructure.

Based on such real-time road and traffic information, many novel applications can be produced. The consequence will be increased road safety and efficiency, and reduced environmental impact. The project’s ambition is to begin a revolution in mobility for travellers and goods, completely re-engineering how drivers, their vehicles, the goods they carry and the transport infrastructure interact.
With CVIS, drivers will influence the traffic control system directly, and get guidance to the quickest route to their destination. Information shown on road signs will be available wirelessly and be shown on a display in the vehicle. Such displays can also warn drivers of approaching emergency vehicles, allowing emergency personnel to reach accidents faster with less danger for themselves and for cars along their path. In the same way, hazardous goods shipments can be tracked at all times and have priority along a pre-selected safe route.

Other key innovations include high-precision positioning and local dynamic maps, a secure and open application framework for access to online services and a system for gathering and integrating monitoring data from moving vehicles and from roadside detectors and sensors.

All this, however, can only happen if there is full interoperability in the communication between different car-makers and between vehicles and different types of roadside systems. CVIS will therefore develop a communication architecture inspired from the CALM standard where IPv6 is serving as a convergence layer between different communication media and different types of applications. It will allow a mobile router using a wide range of communication media, including cellular networks and wireless local area networks (M5), short-range microwave or infra-red, to link vehicles continuously with roadside equipment and servers, either using IPv6 or a fast dedicated communication protocol. The project will apply and validate the ISO “CALM” standards for continuous mobile communication, and will provide input to standards development in European and global standardisation bodies.

To validate the project’s results, all CVIS technologies and applications will be tested at test sites in six European countries: France, Germany, Italy, Netherlands/Belgium, Sweden and the UK.
However, technology is not the only stumbling block on the road to a reality where every car, every traffic light, every road sign and every kilometre of roadway is equipped with CVIS-like technology. A number of non-technical obstacles will also have to be overcome. The CVIS project is therefore creating a toolkit to address key “deployment enablers” such as user acceptance, data privacy and security, system openness and interoperability, risk and liability, public policy needs, cost/benefit and business models, and roll-out plans for implementation.

### 1.4.4 SAFESPOT

SAFESPOT is an integrated research project co-funded by the European Commission Information Society and Media among the initiatives of the 6th Framework Program.

The objective is to understand how intelligent vehicles and intelligent roads can cooperate to produce a breakthrough for road safety.

The aim is to prevent road accidents developing a Safety Margin Assistant that detects in advance potentially dangerous situations and that extends in space and time drivers’ awareness of the surrounding environment.

The Safety Margin Assistant is an Intelligent Cooperative System based on vehicle to vehicle) and vehicle to infrastructure communication. It uses the safety-related information provided by the network properly fused with the on board sensor and it provides the proper advises or warnings to the driver.

The technical development includes applications as well as the key enabling technologies:

- Communication through ad-hoc networks whose nodes are vehicles and road side units.
- An accurate relative positioning
- Local dynamic maps.
- Wireless sensor networks to be used at infrastructure level.

Moreover a dedicated Subproject (BLADE) is dealing with legal, business and deployment organizational aspects. These aspects are very important for the real exploitation of the system.

SAFESPOT applications and technologies will be validated in Test Sites located in France, Germany, Italy, Netherland, Spain and Sweden.

**Figure 7: SAFESPOT Overview Diagram**
1.4.5 SEVECOM

SeVeCom (Secure Vehicular Communication) is an EU-funded project that focuses on providing a full definition and implementation of security requirements for vehicular communications.

The Sevecom vision is that future vehicle-to-vehicle and vehicle-to-infrastructure communication will be widely deployed in order to keep the promise of improved road safety and optimised road traffic.

Sevecom addresses security of the future vehicle communication networks, including both the security and privacy of vehicle-to-vehicle communication and of the vehicle-to-infrastructure communication. Its objective is to define the security architecture of such networks, as well as to propose a roadmap for integration of security functions in these networks.

With the goal of enhancing the immunity of future road safety applications against a wide range of security threats, Sevecom focuses on communications specific to road traffic. Three major aspects will be examined.

- Threats, such as bogus information, denial of service or identity cheating.
- Requirements, like authentication, availability, and privacy.
- Operational properties, including network scale, privacy, cost and trust.

1.4.6 GeoNet

Next-generation vehicles are expected to be able to exchange information (beyond their immediate surroundings and line-of-sight) with other vehicles as well as with the road infrastructure and Internet peers. This will enable trajectories to be forecast, and the coordination of merging maneuvers between sideways neighbors. It would allow vehicles to be notified instantly of the braking action of vehicles in front of them and to warn oncoming traffic of icy patches. Road traffic conditions could be reported and parking lots located. It could also simply provide entertainment for passengers. In this context, the transmission of information shall target vehicles in a particular geographic area.

The exchange of information with vehicles in a particular geographic area - potentially far away from the information source - requires reliable and scalable communication capabilities. We refer to these capabilities as geographic addressing and routing (geonetworking).

The TCP/IP protocol suite provides a unifying layer between various physical communication technologies and various types of applications used in different contexts and environments. A wide deployment of in-vehicle onboard Internet access and services to millions of vehicles
certainly will only be possible with IPv6, the latest version of the Internet Protocol. However, geonetworking is still lacking in IPv6.

GeoNet is thus committed to address this gap by combining geonetworking and IPv6 into a single communication architecture, that is referred to as IPv6 geonetworking. The combination of geonetworking and IPv6 will allow for both IPv6 and non-IPv6 communications. This will, effectively, open the door for the development of new applications that require data to be transmitted to explicit geographical areas.

GeoNet is specifying, implementing, validating and standardizing the necessary functional blocks in coordination with European projects, ETSI and the Car-to-Car Communication Consortium.

1.4.7 FRAME, E-FRAME

FRAME is the generic name given to a series of projects funded by the European Commission. The first two of these projects (FRAME-S and FRAME-NET) further developed and promoted the European ITS Framework Architecture originally produced by the earlier KAREN project. The Framework Architecture comprises a set of User Needs and their supporting functionality.

As a result of the work done by the two FRAME projects, tools and other aids are available to encourage and assist with the use of the Framework Architecture. A by-product from the work is that the Framework Architecture has become known to many simply as “FRAME”.

Since the end of the FRAME projects in October 2004, support for the Framework Architecture has been provided by the FRAME Forum. Membership of the Forum comprises many of the initial users of the Architecture and has enabled the Framework Architecture to be given further limited promotion and support.

More recently, the E-FRAME project has been launched. This European Commission funded project will expand the Framework Architecture to include support for the deployment of Cooperative Systems in European implementations of ITS. The work of the project will enable FRAME to be used as a “tool” that those implementing ITS can use to produce information for use in their procurement processes.

E-FRAME has the objective to extend the European ITS Framework Architecture to include cooperative systems and provide advice for the development and operational issues for a given ITS architecture.

Webpage: http://www.frame-online.net

Start FRAME: July 2001   E-FRAME: May 2008

Duration FRAME: 3 ¼ years   E-FRAME: 3 years
1.4.8 C2C Communication Consortium

The CAR 2 CAR Communication Consortium (C2C-CC) is a non-profit organisation initiated by European vehicle manufacturers, which is open for suppliers, research organisations and other partners. The CAR 2 CAR Communication Consortium is dedicated to the objective of further increasing road traffic safety and efficiency by means of inter-vehicle communications.

1.4.9 ISO

ISO (International Organization for Standardization) is the world's largest developer and publisher of International Standards.

ISO is a network of the national standards institutes of 157 countries, one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system.

ISO is a non-governmental organization that forms a bridge between the public and private sectors. On the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government. On the other hand, other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations.

The ISO TC204 WG16 (International Organization for Standardization Technical Committee 204 Working Group 16) is defining and ITS communication architecture which is better known as the CALM Architecture (Communication Architecture for Land Mobile). This architecture covers all OSI layers, from the physical layer up to the application layer and covers all types of communication scenarios (direct and multihop vehicle-to-vehicle, vehicle-to-infrastructure, vehicle-to-Internet) and scopes (unicast, multicast and geocast). The architecture effectively supports any physical communication medium (cellular, long-range; medium-range and short-range communication networks) - to be used simultaneously - and all types of applications (ITS safety applications, IST non-safety applications, and all legacy Internet applications). The networking layer is designed to support IP (IPv6) and non-IP (FAST) types of communications.
1.4.10 ETSI

Webpage: http://www.etsi.org

The European Telecommunications Standards Institute (ETSI) produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies.

ETSI is officially recognized by the European Commission as a European Standards Organization. ETSI is a not-for-profit organization with almost 700 ETSI member organizations drawn from 60 countries world-wide.

1.4.11 IEEE

Webpage: http://www.ieee.org

A non-profit organization, IEEE is the world's leading professional association for the advancement of technology. The IEEE name was originally an acronym for the Institute of Electrical and Electronics Engineers, Inc. Today, the organization's scope of interest has expanded into so many related fields, that it is simply referred to by the letters I-E-E-E.

The IEEE Standards Association (IEEE-SA) is a leading developer of industry standards in a broad-range of industries. Globally recognized, the IEEE-SA has strategic relationships with the IEC, ISO, and the ITU and satisfies all SDO requirements set by the World Trade Organization, offering more paths to international standardization.

1.4.12 IETF

Webpage: http://www.ietf.org

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas (e.g., routing, transport, security, etc.). Much of the work is handled via mailing lists. The IETF holds meetings three times per year.
2 Policies

Intelligent Cooperative Systems that are based on vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications hold the promise of great improvements both in the efficiency of the transport systems and in the safety of all road users:

- Cooperative systems increase the “time horizon”, the quality and the reliability of information available to the driver about his/her driving environment, the other vehicles and all other road users, enabling improved driving conditions leading to better safety and more efficient and comfortable mobility.
- Cooperative systems offer increased information about the vehicles, their location and the road conditions in the whole road network to the road operators and infrastructure owners, allowing optimized and safer use of the capacity of the available road network, and better response to incidents and hazards.

Cooperative systems build and expand on the functionality of the autonomous and stand-alone in-vehicle and infrastructure-based systems, such as Intelligent Vehicle Safety Systems, including Advanced Driver Assistance Systems (ADAS), traffic control and management systems and motorway management systems. On the contrary to the stand-alone and autonomous systems, many of these benefits require a minimum level of penetration. The initial deployment of the Cooperative systems is a huge technical, legal and economic challenge, requiring cooperation of all public and private stakeholders.

Europe, as the largest producer and largest automotive market should take a leading position in the development, standardisation and market introduction of Intelligent Cooperative Systems. The European Commission will use the instruments in its disposal, in particular the support to research and technological development and standardisation, and policy measures including regulation to:

- Ensure the competitiveness and technological leadership of our automotive industry on the world markets
- Assure that the developed solutions fulfil the European needs as comes to EU’s transport and environmental policies (safety, efficiency and sustainability)
- Assure that the developed systems take into account Europe’s existing and future physical and information communications and infrastructures and the regulations in this area, as well as the characteristics of our road networks
- To assure that the developed applications and services are economically viable and fulfil the needs of Europe’s citizens, and comply with requirements as regards to security and privacy

2.1 In-vehicle Devices

Like any embedded in-vehicle system, cooperative systems must comply with the relevant directives under the European motor vehicle type approval system. In the case of cooperative systems, at least the directives on radio reference/electromagnetic compatibility (72/245/EEC with amendments) and interior fittings (identification of controls, tell-tales and indicators) (directive 78/316/EEC) would be relevant. For mopeds and motorbikes, the equivalent provisions under directive 97/24/EEC would be applicable. Further directives could be relevant, depending on the system.

Alternatively, the equivalent regulations of United Nations Economic Commission for Europe (UNECE) can be used, see the list below.

- For personal stations, the vehicle type approval legislation does not apply.
• For components or separate technical units of a vehicle, the Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity, also applies. As stated in the directive, the apparatus shall be governed by this directive without prejudice to the application of Directive 72/245/EEC or of Directive 92/61/EEC respectively (92/61/EEC is the old type approval directive for two- or three wheel motor vehicles, which is repealed by directive 2002/24/EC).

Furthermore, the European Statement of Principles (ESoP) must be taken into account. Also the results of the HASTE, HUMANIST and AIDE projects should be considered. Whenever the vehicle driver is supposed to interact with communication equipment, the Commission recommendation of 22 December 2006 on safe and efficient in-vehicle information and communication systems: Update of the European Statement of Principles (ESoP) on Human Machine Interface (HMI) should be respected. Besides the principles themselves the recommendations for safe use should be applied.

In addition, a Code of Practise (CoP) for designing of ADAS has been developed under the PREVENT Response 3 project. The CoP "comprises a suitable ADAS description concept including ADAS specific requirements for system development. It summarises best practices and proposes methods for risk assessment and controllability evaluation", as stated in the foreword of the Response 3 report. (add reference)

Under the UNECE World Forum for the Harmonisation of Vehicle Regulations (WP29), common understandings with regard to in-vehicle ITS applications have been developed. The basic principle is the concept of "the driver in the loop". This implies that in-vehicle systems should be designed in a way that the driver is always in control of the vehicle under normal conditions. The WP29 informal group on ITS suggests the following principles for designing in-vehicle ITS systems:

Systems should be designed in a way that the driver is always held responsible for his/her driving. For this purpose the following rule applies:

• Auditory or visual announcement devices providing information on the system functioning should be installed.

Control systems activated under normal driving condition should be designed based on the “Driver in the loop” principle, where driver should be involved in driving in one way or another. For this purpose following rules apply:

• Announcement should be made when the driving initiative is transferred from system to driver.
• Driver should be kept involved in the driving operation. For example, initiative for starting an action should not be given to the system.
• System should allow switching on or off by the driver.
• System should allow overriding by the driver.

As for Control systems to reduce collision speed activated under precrash conditions:

In conditions where collision is no longer avoidable, there is no room or necessity of overriding.

The progress in UNECE WP29 should be monitored with regard to common understandings and regulations affecting the design of cooperative systems. For more information about the ITS informal group under the UNECE WP29, please see their website:

2.2 Radio Spectrum

2.2.1 About the Radio Spectrum Policy

In the EU, the allocation of radio spectrum is in the hands of Member States who have regulatory authority. However, they are also bound by EU law and international radio spectrum agreements.

The development of radio spectrum policy in the Community is based on the Radio Spectrum Decision 676/2002/EC and contributes to the implementation of the EU regulatory framework for electronic communications. It includes coordinating and supporting the radio spectrum needs of EU policies and initiatives in such sectors as communications, R&D and broadcasting. The EU regulatory framework for electronic communications comprises a series of legal texts and associated measures that apply throughout the 27 EU Member States. The goals of the new framework are to encourage competition in the electronic communications markets, to improve the functioning of the internal market and to guarantee basic user interests that would not be guaranteed by market forces. The framework provides a set of rules that are simple, aimed at deregulation, technology neutral and sufficiently flexible to deal with fast changing markets in the electronic communications sector.

The **Radio Spectrum Decision 676/2002/EC** adopted by the European Parliament and the Council on 7 March 2002 has laid the foundation for a general Community radio spectrum policy. The objective of radio spectrum policy is to ensure coordination of radio spectrum policy approaches, harmonized conditions for the availability and efficient use of radio spectrum in particular to support specific Community policies, the provision of relevant information on spectrum usage and the coordination of Community interest in international negotiations in relation to existing EU policies such as in electronic communications, transport, R&D or broadcasting.

Under the Radio Spectrum Decision, the Commission relies on the assistance of specific structures and in addition takes into account through direct contacts the views of Member States, Community institutions, industry, radio spectrum users and other interested parties on technological, market and regulatory development related to the use of radio spectrum.

To help developing general radio spectrum policy at Community level a **Radio Spectrum Policy Group** has been set up in 2002 gathering high-level governmental experts from Member States. This strategic group assists and advises the Commission on spectrum-related issues such as availability, harmonization and allocation, information on allocation, availability and use of radio spectrum, methods for granting rights of use, reframing, relocation, valuation and efficient use and protection of human health.

The requirements of general policy principles identified at Community level are used to be reflected in radio spectrum technical management. This includes the harmonization and allocation of radio spectrum. Where a Community policy dependent on radio spectrum usage has been agreed, the Commission can adopt accompanying technical implementing measures with the assistance of the **Radio Spectrum Committee** which has been created under the Radio Spectrum Decision. Such technical implementing measures in general address harmonized conditions relating to the availability and efficient use of radio spectrum and the availability of information on the use of radio spectrum. Actions and measures in the context of the Radio Spectrum Decision are subject to public consultations and workshops and rely on studies completed by external consultancies for the Commission.
2.2.2 Commission Decision on harmonized use of the 5875 – 5905 MHz frequency band for ITS

A Commission Decision is in preparation with the objective of harmonizing the use of the 5875 - 5905 MHz band for Intelligent Transport Systems. ITS include cooperative systems based on vehicle-to-vehicle, vehicle–to-infrastructure and infrastructure-to-vehicle communications for the real time transfer of information. Given the mobility of vehicles and the need to ensure the achievement of the internal market and the increase in road safety throughout Europe, spectrum used by ITS cooperative systems should be made available in a harmonised way throughout the European Union.

Pursuant to Article 4(2) of Decision No 676/2002/EC, on 5 July 2006 the Commission has issued a mandate to the European Conference of Postal and Telecommunications Administrations (CEPT) to verify the spectrum requirements for safety-critical applications in the context of ITS and Cooperative systems and to undertake technical compatibility studies between safety-critical ITS applications and potentially affected radio services in the frequency ranges under consideration. CEPT was also requested to develop optimal channel plans for the bands identified for ITS.

The relevant results of the work carried out by CEPT constitute the technical basis for this Decision.

- CEPT has concluded in its report of 21 December 2007 (CEPT Report 20) that the 5 GHz band, in particular the range 5875 - 5905 MHz, is appropriate for safety-related ITS applications, which improve road safety by increasing the information to the driver and the vehicle on the environment, other vehicles and other road users.
- Furthermore, ITS are compatible with all the services studied in that band, and with all other existing services studied below 5850 MHz and above 5925 MHz, as long as they comply with certain emission limits as defined in the CEPT Report. The selection of this band would also be in line with spectrum use in other regions of the world and thus foster global harmonisation.
- Moreover, ITS could not claim protection from fixed-satellite service (FSS) earth stations and unwanted emissions from ITS equipment need to be limited in order to protect Radiolocation, RTTT and FS.

Harmonisation under this Decision should not exclude the possibility for a Member State to apply, where justified, transitional periods or radio spectrum-sharing arrangements.

It is expected that Member States will make the spectrum available for vehicle-to-vehicle ITS communications within the six-months period during which they have to designate the frequency band 5875 - 5905 MHz according to this Decision. However, for infrastructure-to-vehicle and vehicle-to-infrastructure ITS communications, it may prove difficult for some Member States to finalise an appropriate licensing framework or a coordination mechanism for roadside infrastructure installation of different ITS operators within this timeframe. Any delays in making the spectrum available beyond this period may impact negatively on the wide take-up of safety-related ITS applications in the European Union and should therefore be limited and duly justified.

Considering the market developments and evolution of technologies, the scope and application of this Decision may need to be reviewed in the future, based in particular on information on such developments and evolution provided by the Member States.

Harmonised standard EN 302 571 is being finalised by European Telecommunications Standard Institute (ETSI) in line with the CEPT compatibility studies in order to give presumption of conformity to Article 3(2) of Directive 1999/5/EC of the European Parliament and the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity, thus ensuring that compliant ITS
equipment avoids causing harmful interference. ITS transmitters are expected to maximise the use of the spectrum and control their transmitted power to the minimum level to use the spectrum allocated to ITS effectively so as to avoid harmful interference.

For the above reason, the standard foresees that a transmitter power control (TPC) is implemented with a range of at least 30 dB with regard to the maximum total transmit power of 33 dBm mean e.i.r.p. If some manufacturers choose not to use the techniques identified in this standard, any alternative methods would be required to provide at least an equivalent level of interference mitigation as that provided by the standard.

### 2.2.3 Other Communications Technologies

The Cooperative Systems will also use a wide range of other communications technologies, normally using already deployed technologies (such as cellular systems), and using potentially both licensed and in non-licensed bands. In Annex 2-1 is an overview of the regulatory status of these technologies.

### 2.3 Roadside equipment – additional issues

Up to now the relevant regulation on European level only addresses mobile equipment for ITS. As a general rule, for the roadside equipment the same rules and procedures should apply with respect to the use of frequency bands, provision of services etc. as for mobile equipment, but at present this is left to the discretion of the Member States. In the Member States rather different policies on licensing are applied.

In the recent research projects the national network authorities in Austria, France, Germany and Sweden have accepted notification on the use of the relevant bands for ITS without imposing specific regulations or restrictions on roadside equipment. In Austria the same frequency bands are used by the public TV broadcaster (ORF) to link outside cameras to the central control room during transmission of major sport events. No interferences are expected during the test operations, but coordination with ORF is required in Austria at present.

The certification of devices and services is discussed in CEPT/ETSI at present, and it remains an open issue. Self-certification of devices by its manufacturer might be sufficient in some cases, where no ETSI certification is required, but certification of services needs to be obtained from the relevant authorities.

To ease the deployment of cooperative systems a coordinated approach on European level for certification, but also for licensing of roadside equipment is strongly recommendable. For 5.9 GHz roadside stations like vehicle stations should not have licensing restrictions. Furthermore a clear and useful definition of mobile and roadside equipment is needed, as for the time being some systems (i.e. in road construction or police cars) might change their regulatory defined status depending on the current situation (driving on the road vs. standing at a construction / accident scene).

### 2.4 Liability

These Directives cover a wide range of products and thus provide a rather generic framework for the safety of products. Despite the fact that the Member States have implemented the requirements set out in the Directives in their national legislation, the laws are often complex and open to interpretation, and also in certain aspects different between the Member States.

Another group of relevant laws are the safety standards for vehicles and the vehicle type approval directives, which are also carried out on EU level, however traffic rules and traffic liability is a full competence of the Member States and thus not harmonised within EU.

The RESPONSE 3 project developed the Code of Practice mainly for the development of autonomous in-vehicle systems, addressing liability and product safety among other issues. The further challenge with cooperative systems is that there are more different parties involved, each responsible for a component or a function, which is dependent on other components of a complex system. The complexity and interdependencies - not only between the system’s components, but also between vehicles and the infrastructure – can make it very difficult to find the liable party in case the system fails. **Further work is needed in identifying the legal consequences of the proposed technical solutions**, which can have a direct impact on development and design process.

One major element of legislation which currently restricts the functionality of Intelligent Vehicle Systems is the UNECE Convention on Road Traffic (‘the Vienna Convention’), signed in November 1968, stipulating that the driver must control his/her vehicle at all times. However major developments in technologies used in vehicles and infrastructure make today’s cars and driving environment totally different from those of 1968. Moreover, the traffic has become more and more complex, making the driver's task increasingly difficult. Current technologies could be much more efficiently used in supporting the driver, if vehicle systems would be allowed to intervene in controlling the vehicle. Many systems currently on the market are also bordering a “grey zone”, where the way the driver controls the vehicle is fundamentally different from earlier systems, and open to different interpretations. **Revising the Vienna Convention in this respect should be considered in the near future**; otherwise the safety potential of many current and emerging technologies and applications is lost, and the liability issue remains problematic.

### 2.5 Security

Cooperative systems will exchange information which might be relevant for (automated) decisions upon which the safety of human lives depends. Therefore, it is mandatory to ensure that no malign intervention can threaten the health of road users and other traffic participants. One part of the safeguarding of critical communication might be the introduction of legal measures along the lines of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

Related to the i2010 EU policy framework for the information society and media, the following legal act has to be taken into account: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). According to it, providers of a publicly available electronic communications service are obliged to take appropriate technical and organisational measures to safeguard security of its services.

2.6 Privacy

The introduction of cooperative systems will imply the creation, storage and exchange over wireless communications links of personal data. In particular, it is expected that cooperative systems will generate a huge amount of location data, which may be considered as personal data, as they can lead to tracking the movements of individuals.

The results of the Eurobarometer survey carried out on 2006 regarding the perception of the use of the intelligent systems in vehicle showed privacy concerns vary. For the eCall, for a great majority, privacy is not a major concern, or it is considered to be only a minor inconvenience as compared with the usefulness of the system. However regarding real time traffic and travel information systems there is real concern: significantly more respondents considered this system as an intrusion and would not like to have it in their car. This is especially the case for the French (26%) and the German (25%) respondents. The introduction of some innovative insurance schemes which imply tracking of the vehicles and exchange of data between vehicles and infrastructure (such as the Pay as You Drive systems) have induced a debate in the media, and some national Data Protections Offices have rejected the introduction of these applications and considered them too intrusive regarding citizens’ privacy.

Therefore it is important to generate users’ confidence. The design of the cooperative systems has to take into consideration the appropriate measures to ensure protection of the privacy and personal data.


The European Commission has organised two workshops on the security and privacy implication of in-vehicle telematics and cooperative systems, bringing together experts from industry, research centres and data protection authorities. The main conclusion of the workshops is that it is necessary to incorporate security and privacy issues from the early stages of the design of cooperative systems, in order to develop the appropriate mechanisms to protect the privacy rights of the users and to generate the necessary trust.

The eSafety Forum (the eSecurity Working Group) is elaborating in collaboration with experts from the Data Protection Offices of the art. 29 Working Party on Data Protection a Code of Practice with recommendations on how to deal with privacy and data protection issues in the design of in-vehicle telematics and cooperative systems.

It is also important to consider, when designing the cooperative systems services and applications, the opinion of the art. 29 Working Party on Data Protection regarding the use of location data with a view to providing value-added services (25 November 2005) and the working document on data protection and privacy implications in the eCall initiative, adopted by the art. 29 Working Party on 26 September 2006. These documents contain recommendations applicable also to the cooperative systems.

Some European projects are researching on issues related to privacy protection on the vehicle-to-vehicle and vehicle-to-infrastructure communications environment. FP6 SeVeCom project addresses security of future vehicle communications networks, including both the security and privacy of inter-vehicle and vehicle-infrastructure communication. Its objective is to define the security architecture of such networks, as well as to propose a roadmap for progressive deployment of security functions in these networks. The FP7 project PRECIOUSA, is aiming at defining an approach for privacy evaluation of cooperative systems, with a focus on both communication privacy and data storage privacy, for the protection of location oriented information; defining a privacy aware architecture for cooperative systems; defining and validating guidelines for privacy aware cooperative systems around a concrete system and investigating specific challenges for privacy.
Part I: Architecture

3 ITS Communication Architecture - Description

3.1 Communication Architecture Terminology

The following is a list of terms commonly used to describe the various network entities that would be involved in a typical communication system. This list is not exhaustive and serves the purpose of easing the description of the ITS Communication Architecture in the sections that are immediately following this list of terms. As such, the list does not include new terms that are defined within this document:

- **Node**: a computer that has an address in the communication network.
- **Router**: a node that forwards to another node in the communication network packets not explicitly addressed to itself.
- **Host**: any node that is not a router.
- **Gateway**: a node (host or router) able to transfer information in one or both directions between the communication network and a dedicated ITS-specific local network (e.g. a CAN). The gateway may implement security and translations services as part of this role.
- **Mobile Node**: a node that can change its point of attachment from one link to another while maintaining sessions.
- **Access Network**: a network located on the edge of the communication network and providing access to mobile nodes.
- **Border Router**: a router residing on the edge of a local network (e.g. an access network) and connecting this network to the backbone of the communication network.
- **Access Router**: a router residing on the edge of an access network and connecting one or more access points. An access router offers network access to mobile routers, acting as a default router to the mobile routers it is currently serving.
- **Mobile Router**: a router capable of changing its point of attachment to the communication network, moving from one access router to another access router belonging either to the same access network or distinct access networks. The mobile router has an ingress interface to which an in-vehicle network and one or more egress interfaces are attached. The mobile router acts as a border router between an in-vehicle network and an access network and is capable of forwarding packets between these two.
- **Roadside Host**: a host located in the roadside subsystem component
- **Vehicle Host**: a host located in the vehicle subsystem component
- **Central Host**: a host located in the central subsystem component
- **Roadside Gateway**: a host acting as a gateway between the ITS communication system and legacy systems on a roadside.
- **Vehicle Gateway**: a host acting as a gateway between the ITS communication system and legacy systems in a vehicle.
• **Central Gateway**: a host acting as a gateway between the ITS communication system and legacy systems in a vehicle.

### 3.2 European ITS Communication Architecture components

The European ITS Communication Architecture (see Figure 8) is a communication system designed for ITS and made of four physically separated subsystem components:

- The vehicle subsystem component
- The roadside subsystem component
- The central subsystem component
- The mobile subsystem component

These components are inter-linked by a communication network. The communication network is typically made of a backbone network and a number of edge networks and access networks. Communications are performed over a wide range of wireless or wired communication media. Any number of instances in each of the subsystems can be connected through the communication network. This means that there can be as many vehicles, mobile hand-held devices, roadside and central servers as needed for any specific purpose. Thus, the architecture allows both for direct vehicle-to-vehicle ad-hoc networks as well as infrastructure-based systems or any combination thereof.

![Figure 8: European ITS Communication Architecture – Ad-hoc Type of Communication](image)
3.3 The ITS Station

Each of the four components described in Figure 2 contains an ITS Station (respectively Vehicle Station, Roadside Station, Central Station and Personal Station) and usually a gateway connecting the ITS Station to legacy systems (respectively Vehicle Gateway, Roadside Gateway and Central Gateway).

An ITS Station comprises a number of ITS-specific functions and a set of devices implementing these functions (by ITS-specific we mean the necessary functions in order to communicate with other ITS communication architecture components).

For the sake of clarity and referring to the bottom-left part of Figure 2 showing an example of an implementation of the ITS Station on-board the vehicle: the functions of a Vehicle Station may in one implementation be split onto several physically separated nodes communicating over a local area network (LAN) such as e.g. Ethernet. The communication function would be supported by a communication node (a mobile router) in charge of communication with outside the vehicle whereas applications may be supported by a number of other dedicated nodes (vehicle hosts). In another implementation instance, a unique node may support both the communication functions and the applications.

The decision for how to implement the necessary set of functions of an ITS Station is out of scope of this present document and is left out to stakeholders who will deploy this ITS Communication Architecture.

3.4 Communication Scenarios

The communication network allows for any subsystem component to communicate with any other subsystem component (in theory; in practice some scenarios wouldn't make sense with today’s know-how). The communication could be performed directly between two subsystem component instances or indirectly multi-hopping via intermediate subsystem component instances. For instance, in one specific instance, vehicles could communicate with one another without involving any of the other components (ad-hoc type of communication as illustrated in Figure 2); in another more general instance, vehicles could communicate with servers either directly reachable through the communication network or reachable through the roadside or even another vehicle (Internet-based type of communication as illustrated in Figure 9).

Each component has to obey to a number of rules in order to communicate with other components in a particular communication scenario. In the specific ad-hoc type of communication mentioned earlier and illustrated in Figure 8, all vehicles are communicating over the air using the same communication media in the 5.9 GHz frequency band.

Whereas the ad-hoc type of communication (see Figure 8) and other specific scenarios do not involve servers in the central subsystem at the particular point in time when this type of communication is under progress, all subsystem components must be able to talk to one another at some point in time in their lifetime in order to exchange some information, such as identifiers, credentials, security key, map update, toll payment, etc. For doing so, it is necessary that all subsystem components are inter-linked by a communication network using the same communication language, what is referred to as a protocol. This protocol must be of a wide-spread reach and use and must be independent from any of the wireless or wired access network technologies and must also accommodate all types of applications. The Internet Protocol (IP) serves this purpose. This is illustrated in Figure 9.
3.5 **IPv6-based Communication Network**

Using IP (Internet Protocol) for the European ITS Communication Architecture brings a number of benefits, including the possibility to interoperate ITS subsystem components with the legacy Internet. By decreasing costs and increasing revenue, it would ease the deployment of the ITS architecture.

There currently exist two versions of this protocol, IPv4 (Internet Protocol version 4) the currently deployed version, and IPv6 (Internet Protocol version 6), its successor currently under deployment.

Many reasons drive to the selection of IPv6:

- The number of subsystem components that shall be supported: the far-end objective is to support all vehicles, i.e. 200 millions vehicles in Europe, not to mention the mobile hand-held devices (more than one per citizen).
- IPv4 address depletion: in 2011 according to converging studies, there will not be any IPv4 address block left to be allocated to regional registries which subsequently provide address space to Internet Service Providers and big companies.
- IPv6 enhanced features: IPv6 provides new features such as network mobility, auto-configuration, Quality-of-Service, multiple interface management etc. that are key to meet ITS requirements.
European recommendations: in May 2008 and following a study of the impact of IPv6 on vertical sectors, the European Commission has published an IPv6 action plan setting up 2010 as a target to deploy IPv6 at a wide scale in Europe.

OECD: the Organisation for Economic Co-operation and Development has issued a report urging governments to facilitate IPv6 deployment.

ITS standardisation under progress: the ISO TC204 WG16, for example, is specifying the CALM architecture and uses IPv6.

The deployment of an IPv6-based ITS communication architecture is thus driven by both:

- operational and technical reasons (IPv6 provide the features that meet ITS requirements),
- economical reasons (interoperability with other communication systems; relatively few currently deployed systems operating in IPv4; off the shelves equipment available in IPv6 and wide-spread know-how in internet technologies as compared to a dedicated ITS network relying on another technology),
- political reasons (incentives to deploy IPv6 in order to boost European competitiveness), and
- societal reasons (the internet is deployed everywhere and there is no reason why the ITS communication network would not be part of the overall internet. It will ultimately simplify the living of everyone as it would allow the interoperability of the ITS communication system with other communication systems such as for example healthcare and emergencies).
4 Scenarios, Applications, Use Cases

This chapter introduces the basic scenarios and applications as well as a collection of user needs and use cases with a focus on the Applications block in the ITS Station Reference Architecture below. The other parts of this reference architecture will be explained in the further course of this document. This chapter sets the terminology used in this document and summarizes the prerequisites and constraints for cooperative systems.

4.1 Basic Scenarios

The scenarios addressed by the European ITS communication architecture are from the following main fields of application:

- Traffic safety
- Traffic efficiency
- Value-added services

Additionally, the architecture may allow other services to be implemented and offered in order to facilitate system introduction and provide sustainable business and operation models.

A number of graphical illustrations provide an overview on the system idea: connecting vehicles, roadside (traffic) infrastructure and backend (traffic) infrastructure to improve safety and traffic efficiency on European roads. Figure 11 is a sketch from C2C-CC.
The traffic safety field of applications will support services such as lane departure warning, speed management, headway management, ghost driver management, hazard detection and several other similar services. Traffic efficiency applications will support services such as urban traffic management, lane management, traffic flow optimisation, priority for selected vehicle types, e.g. busses, emergency vehicles etc. Applications providing value added services will include such things as journey planning, both pre-trip and on-trip, travel information and location based services. Applications for road user charging will fit into one or more of these fields depending on the policy behind their implementation.

A communication perspective according to ISO is provided by the picture in Figure 12.
4.2 Applications

The three basic scenario fields are supported by a number of application classes. For each of the three fields these classes are as follows:

- Traffic Safety
  - Cooperative Awareness Applications, e.g. head way management, lane departure warning, speed management, under road user detection, etc.
  - Hazard Warning Applications, e.g. road condition detection, hazard detection, traffic queue detection, adverse weather detection (like fog), etc.

- Traffic Efficiency
  - Inter-Urban Traffic Efficiency
    - Adaptive Electronic Traffic Signs, e.g. incident detection and management, variable message sign display management, lane use management, speed management, ghost driver management, etc.
    - Route Guidance and Navigation, e.g. on-trip guidance using real-time traffic data with special routes for particular vehicle types, road condition advice, etc.
  - Urban Traffic Efficiency
    - Traffic Flow Optimization, e.g. incident detection and management, minimising traffic delays and queues at intersections, priority for busses and emergency vehicles, speed management, etc.
    - Route Guidance and Navigation, e.g. on-trip guidance using real-time traffic data with special routes for particular vehicle types, parking availability advice, etc.
  - Freight and Fleet Applications, e.g. booking of delivery slots, management of hazardous goods vehicles, etc.

- Value-added services
  - Local connection access, e.g. service applications by car to car or car to roadside connections to provide traffic trouble and road condition information, etc.
  - High speed internet access, e.g. service applications by wireless connections to provide journey planning and other information from service providers like hotel, restaurant, cinema etc.

4.3 User Needs and Use Cases

4.3.1 Introduction

We follow here the same understanding of User Needs, Use Cases and System Requirements as used in some of the projects:

- User Needs emanate from the users and are entirely user-oriented. They will not necessarily be consistent, and are likely to be expressed in plain text, with informal diagrams if necessary to be more comprehensive. In the FRAME ITS Architecture methodology they are represented by FRAME Stakeholder Aspirations.
• Use Cases define a subset of the functionality of a system. They are primarily used to define the behaviour of a system without specifying its internal structure. In the FRAME ITS Architecture methodology the nearest equivalent are the contents of the FRAME Function Specifications. However the Specifications are created from the FRAME User Needs.

• System Requirements are system- and implementation-oriented, and will use (semi-) formal text techniques to capture all the requirements; they will not necessarily be easy to read by the users. The primary requirements will come from the Use Cases, but in addition the system engineers and system architect(s) will add derived requirements to provide the working characteristics of the system. System requirements for the main cooperative system projects are provided in the annex to chapter 5. In the FRAME ITS Architecture methodology the nearest equivalent is the FRAME User Needs. However they are derived from the FRAME Stakeholder Aspirations and therefore do not contain any description of the functionality. They will contain requirements about what the functionality must do.

Some of the projects have used a common template for Use Case and User Needs specifications.

There are hundreds of different use cases considered and developed within the different projects. They can all be mapped to one of the application classes listed in the previous section. These are shown by the tables in the following sections.

### 4.3.2 Traffic Safety applications

<table>
<thead>
<tr>
<th>Cooperative Awareness Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cooperative Warning</td>
</tr>
<tr>
<td>Approaching Emergency Vehicle (V2V/V2I)*</td>
</tr>
<tr>
<td>Emergency Electronic Brake Lights</td>
</tr>
<tr>
<td>Post Crash Warning (V2V/V2I)</td>
</tr>
<tr>
<td><strong>Highway / Rail Collision Warning</strong></td>
</tr>
<tr>
<td><strong>Car Breakdown Warning</strong></td>
</tr>
<tr>
<td><strong>Overtaking Vehicle</strong></td>
</tr>
<tr>
<td><strong>Merging Assistance</strong></td>
</tr>
<tr>
<td><strong>Lane Change Assistance</strong></td>
</tr>
<tr>
<td><strong>Precrash Sensing Warning</strong></td>
</tr>
<tr>
<td><strong>Cooperative Glare reduction</strong></td>
</tr>
<tr>
<td><strong>Cooperative Adaptative Cruise Control</strong></td>
</tr>
<tr>
<td><strong>Cooperative Vehicle-Highway Automation System (Platooning)</strong></td>
</tr>
<tr>
<td><strong>Cooperative Flexible Lane Allocation</strong></td>
</tr>
</tbody>
</table>
### Decentralized Floating Car Data

- **Traffic jam**
- **Road Works**
- **Slippery Road** *
- **Fog**
- **Rain**
- **Wind**

**Consists** for any vehicle to detect and signal to other vehicles such events on the road. Such information can be propagated until a certain distance by crossing vehicles in opposite direction using geocasting capabilities.

### Legal and Contextual Speed Limit

The road side unit sends the legal speed limit and also speed limit depending on the context (bad visibility, weather, accident...)

### Hazard Warning Applications

- **Wrong Way Driving Warning**
  - Consists for any vehicle detecting that it is engaged in a wrong way (forbidden heading) to signal to other vehicles arriving in opposite this dangerous situation.

- **Safety Function out of Normal Condition Warning**
  - Consists from any vehicle detecting a safety function (steering, braking,...) being out of its normal condition to signal this state to other vehicles and road side units.

- **Slow Vehicle Warning**
  - Consists from any slow vehicle being to signal its presence (vehicle type) to other vehicles.

### 4.3.3 Traffic Efficiency applications

**Route Guidance and Navigation**

- **Greenlight Optimal Speed Advisory**
  - Case consists for a traffic light to broadcast timing data associated to its current state (e.g. time remaining before switching to orange, red). When receiving this information, a speed advice can be given to the driver according to its relative distance to the traffic light and to its current speed.

- **Traffic Information and Recommended Itinerary**
  - Informs the approaching vehicles of traffic conditions and issues recommendations in case of traffic jam. May provide some map elements to avoid the traffic jam.
**Enhanced Route Guidance and Navigation**

Consists of road side units with capability to access to global network and enable any passing by vehicle or parked vehicle to access to an internet server to request the downloading of an optimized itinerary according to personal requirements. This interaction between a vehicle and an internet server may include a content purchasing transaction and Digital Rights management.

**Traffic Light Optimization**

<table>
<thead>
<tr>
<th><strong>Green Wave Assistant</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Consists of road side unit (e.g. traffic light or stop) with capability to warn a vehicle driver that he will be in violation of the stop according to its current speed and position. However, if it is a priority vehicle, this one can issue a preemptive message to request the infrastructure to facilitate its transit.</td>
</tr>
</tbody>
</table>

**Intersection Management**

Consider all the V2V and V2I cooperation possibilities to reduce the risk of vehicles’ collisions at a road intersection. In most of the case, such objective will be achieved through a combination of basic services.

**Cooperative Electronic Traffic Signs**

<table>
<thead>
<tr>
<th><strong>Road Side Unit Capabilities and Status</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The road side unit provides its capabilities and status permanently using I2V Cooperative Awareness Messages. When a vehicle receives this information, it can establish a unicats liaison to exchange more information with this RSU.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Road Restricted Access, Detour Notification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Warn the approaching vehicles of road restricted access (provides the reason for restriction). May provide some advice / map elements to avoid the restricted area.</td>
</tr>
</tbody>
</table>

### 4.3.4 Value added services

<table>
<thead>
<tr>
<th><strong>Local connection access</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Point of Interest Notification</strong></td>
</tr>
<tr>
<td>Informs about the presence of a local based service or Point of Interest. Can provide some dynamic information such as the opening hours, prices, waiting time, available room, promotions….etc.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Local Electronic Commerce</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>A road side unit signalling some POI / LBS may have the capability to process the local payment for service reservation or / and some good purchasing.</td>
</tr>
<tr>
<td>Car Rental / Sharing Assignment / Reporting</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>Automatic Access Control / Parking Management</td>
</tr>
<tr>
<td>Electronic Toll Collect</td>
</tr>
<tr>
<td>Stolen Vehicle Alert</td>
</tr>
<tr>
<td>High Speed Internet Access</td>
</tr>
<tr>
<td>Remote Diagnosis and Just in Time Repair Notification</td>
</tr>
<tr>
<td>Media Downloading</td>
</tr>
<tr>
<td>Map Download and update</td>
</tr>
<tr>
<td>Fleet Management</td>
</tr>
<tr>
<td>ECO Driving</td>
</tr>
<tr>
<td>Instant Messaging</td>
</tr>
</tbody>
</table>
service can be achieved using an RSU (V2I) connected to Global network.

**Vehicle Software Provisioning and update***

A road side unit which has global network access capabilities shall be able to insure the transparent software and associated data downloading through some exchanges between vehicles (passing by or parked) and a relevant software provisioning centre.

**Personal Synchronization at Home**

A road side unit which has global network access capabilities shall be able to insure the transparent data exchange between vehicles (passing by or parked) and their driver / travellers home computer(s).

* These applications are selected as common scenarios between SAFESPOT, CVIS and COOPERS.

From the user needs and use cases, requirements can be derived. For cooperative systems, this has been done in a joint effort of the projects COMeSafety, COOPERS, CVIS and SAFESPOT. These are provided in the annexes to chapter 5.

### 4.4 Terminology

This section provides definitions of some of the terms used in this document that have so far not been defined. Other definitions will be provided in the most appropriate parts of the document.

**ACTOR**

An Actor is defined as a human or as an organisational entity that interacts with the cooperative systems.

**APPLICATION**

An Application is a closed system, needed to provide a specific service, such as those defined earlier in this chapter. The procedure of executing this specific service is a use case.

**COOPERATION**

According to the Control Loop (Figure 13), an actor is conceived of as running through one or more control cycles, each of which successively consists of the following phases:

1. Observation – observation of the surroundings, the own performance and the performance of related stakeholders;

2. (Information) Evaluation – evaluation of the observations and extraction of the (actual or foreseen) bottlenecks and the moments where interaction or cooperation with other stakeholders is necessary;

3. Decision (making) – decision on the nature of the interaction or cooperation and/or the necessary changes or adaptations in the own performance (and thereby behaviour) and/or in the performance of related stakeholders;
4. (Legislative) action – take action and interact, cooperate and/or change, adapt the own behaviour, or adjust and communicate the expectations of the performance of related stakeholders.

Cooperation emerges when actors start to collaborate while running through their business control cycles. Collaborating by sharing information, by

- Mutually informing: the actors exchange information, but may adapt their actions separately;
- Negotiating: there is a set of rules for the mutual exchange of goals, preferences, feasible actions and restrictions of the interurban road network. These rules allow for an exchange of data by the actors, such that the actors adapt their actions after the negotiations;
- Instructing: a certain actor is authorized to give instructions to other actors given the evolving situation.

Once collaboration is in place the information flow follows the four steps in the control loop, as well as the iteration following from the observation-evaluation-decision-action loop.

![Figure 13: The Information Processing Cycle](image)

**ENTITY**

An Entity is defined as an element of the cooperative systems world. An Entity can either exist inside or outside the system. Often it can be further decomposed in other entities. Definitions of external entities are provided in chapter 6.

**FEATURE**

A feature is a specific name for a core component development unit.
ROLE
A 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. Roles can be assigned to Entities inside and outside of cooperative systems. Each Entity or Actor can therefore have more than one Role.

SPECIFICATION
A Specification is a detailed description of a feature as baseline for development. It is a description of HOW the development unit is designed in order to fulfil the requirements. A specification maybe used in the process of procuring components and systems for ITS implementations.

4.5 Prerequisites and Constraints
There are several prerequisites and constraints that need to be fulfilled to the design of applications to implement the use cases. In many cases they pose questions that have to be answered before the design of the applications can be completed. These are summarised in the following bullet points.

• Technical Prerequisites
  o System Capabilities: These are questions concerning the overall system capabilities which are required to support the considered use cases. This includes application, communication Quality of Service (QoS), vehicle electronics, anonymity and data security.
  o System Performances: These are questions concerning the system performances which are required to support the considered use cases. This includes scalability of communication system, positioning accuracy, robustness / reliability of the system etc.

• Legal Prerequisites
  These are questions already mentioned in chapter 2, especially concerning
  o effectively protected frequency band as a major requirement for robustness
  o respect of European privacy rules.

• Strategic Prerequisites
  o Time to Value (Strategic): The deployment time which is necessary for customers to obtain a minimum service value. This time to value is very related to the deployment strategy (time to reach a critical mass).
  o Part of the European Union Policy (Strategic): Questions here will rely to the EU policies as discussed in chapter 2.

• Economic Prerequisites
  o Societal value (Economical): These are questions concerning the societal value of the considered use cases and whether they enhance road safety, mobility efficiency (traffic management) and environmental efficiency.
- **Business value (Economical):** These are questions concerning the business and customer values of the considered use cases.

- **Return on Investment (ROI: Economical):** These are questions concerning the length of time it will take to obtain a return on investments and get some operational margin. This is of course related to the deployment strategy.

- **Adoption Factors**
  - The effectiveness of cooperative systems will depend on the real world penetration.
5 Stakeholder Aspirations, User Needs, Requirements

In this chapter combining the “Requirements” produced by the Cooperative Systems project is discussed. The discussion uses the term “User Needs” according to its definition within the FRAME methodology. It also makes reference to the results of work done to produce a set of combined requirements for cooperative systems, expressed as a set of FRAME User Needs.

5.1 Background and Methodology

As described in chapter 4, some (but not all) of the Cooperative Systems projects have created “Use Cases”, “Requirements” and “User Needs”. Where this occurs, the “Requirements” appear to be between the “User Needs” and the creation of the functionality in the projects’ architectures that is expressed in their “Use Cases”. Most of the “Requirements” are classified into “functional” and “non-functional”.

In order to produce a coherent set of combined requirements that includes all of the services that are being developed and explored by the cooperative systems projects it was decided to use the concept of User Needs from the FRAME methodology. This would also enable them to be used in an expanded version of the European ITS Framework Architecture and thus contribute towards the promotion of the use of cooperative systems in ITS implementations.

In the FRAME methodology, its User Needs fulfil the role of the “Requirements” in the architecture work carried out by some of the Cooperative Systems projects. In FRAME there is no division of its User Needs into “functional” and “non-functional” types but it is recognised that some are concerned with functionality and some are concerned with other architectural aspects such as the physical implementation, or the communications that will be needed between different parts of the architecture’s overall functionality.

Two “clusters” of FRAME User Needs have been created. The first contains those of the existing FRAME User Needs that can be mapped directly to the “Requirements” produced by the Cooperative Systems projects. In the second “cluster” are new FRAME User Needs that have been created for “Requirements” where no mapping to existing User Needs was possible.

5.2 Structure of the information in the annex to chapter 5

The results of the work to map the “Requirements” from each of the Cooperative Systems projects and produce the two “clusters” of FRAME User Needs are presented as a series of documents in the annex to this chapter (5) – see section 0. They comprise the following:

- Annex 5-1 Main Document: this provides a description of the methodology that was used to create the combined “Requirements” for the Cooperative Systems projects as a set of new and mapped FRAME User Needs. It also contains details of the sources of the “Requirements” from each of the projects and an overview of the results.
- Annex 5-2: CVIS Requirements – this Annex contains the requirements shown in this annex are taken from its project documentation and are shown as a series of tables, one for each of the four non-technology sub-projects.
- Annex 5-3: SAFESPOT Requirements – this Annex contains the requirements shown in this annex are taken from its project documentation and are shown as a series of tables, one for each of the five sub-projects.
- Annex 5-4: COOPERS Requirements – the contents of this Annex are taken from its project documentation and are shown in two tables. Unlike the other two projects, the
COOPERS project used the FRAME methodology for the creation of its architecture. Thus the first table contains a list of the existing FRAME User Needs that the COOPERS project could directly map to its Services. The second table contains the list of new FRAME User Needs, that the COOPERS project created for those parts of the Services for which no mapping was possible.

- Annex 5-5: FRAME User Needs – this Annex contains the complete list of the existing FRAME User Needs, which can be downloaded from the FRAME web-site – see chapter 1. This is provided as a reference for the following two annexes (5 & 6) because later work on the European ITS Framework Architecture may lead to changes in the structure and content of the User Needs that will make the mapping inaccurate.

- Annex 5-6: New FRAME User Needs for the Cooperative Systems projects – this Annex contains a table that provides a list of the new FRAME User Needs that have been created where no mapping of the Cooperative Systems projects’ “Requirements” could be made to the existing FRAME User Needs. The contents of the table are arranged so that the FRAME User Needs are shown in numerical order, together with the identity number of the “Requirements” to which they have been mapped.

- Annex 5-7: Mapped FRAME User Needs for the Cooperative Systems projects – this Annex contains a table that provides a list of the existing FRAME User Needs to which the Cooperative Systems projects’ “Requirements” could be mapped. The contents of the table are again arranged so that the FRAME User Needs are shown in numerical order, together with the identity number of the “Requirements” to which they have been mapped.

Although a large number of the existing FRAME User Needs have been mapped to the “Requirements”, there are also a substantial number of new User Needs. The reasons why there are so many new FRAME User Needs are as follows:

1. Cooperative Systems have “Requirements” that are new and represent an expansion of the scope and content of the services that can be provided by ITS.

2. It was considered a good idea to provide some flexibility for users when making choices about which User Needs will fit their particular ITS implementation requirements.

### 5.3 Using the combined requirements

The combined “Requirements” that have been created as FRAME User Needs are intended to be used in the implementation of ITS. Their direct use is of course with the FRAME methodology, which includes tools that will enable a set of specifications to be produced for the “building blocks” that will be required by any ITS implementations.

However if the use of an alternative methodology is preferred the FRAME User Needs can be seen as “Requirements” in the sense this term is defined in chapter 4. The FRAME functionality that fulfils them can then be used to create the corresponding “User Cases”.

The end result of using either methodology should be a description of what is needed to create any ITS implementation that uses cooperative systems. This description should include a definition of the communications requirements, which should be directly supported by the communications architecture described in the later chapters of this document.
6 Overall Framework: Actors, Terminators and Entities

6.1 Classification of Stakeholders and Actors

The CONVERGE\(^1\) project identified four main categories of stakeholders who will be affected by, or have an effect on, the final ITS implementation. They are those who want it, those who make it, those who use it and those who rule it. They are defined 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.

6.2 Operator Organisations

**Road Operator**

This Actor represents an organisation that is responsible for maintaining a road network and managing the traffic on it. It can be a private company, or an organisation belonging to central government or a local authority.

**Public Transport Provider**

This Actor represents an organisation that provides Public Transport services. It can use its own fleet of vehicles and/or vehicles hired from third parties. The vehicles themselves can be buses (including coaches), trolley buses, trams and mini-buses, i.e. any vehicle that carries passengers for which the driver requires a specific licence. Services can be provided in the urban and/or inter-urban environments.

**Emergency Service Provider**

This Actor represents an organisation that provides Emergency Services. The content of the Services may vary from one organisation to another and can comprise any combination of

---

\(^1\) CONVERGE was a EC funded project in the late 1990s. To see the results of its work on architectures for ITS, please, see the CONVERGE document which can be obtained from the “library” page of the FRAME website.
Ambulance, Fire, Police, and Vehicle Recovery. It is also for each organisation to have a different geographic scope, some of which may overlap where different Services are provide.

**Service Provider**

This Actor represents the legal organisation that provides services including the corresponding content. It may also operate a Service Centre or use a Centre that is provided and/or managed by another organisation. The Service Provider supplies the necessary means to provide the business related support of a specific service application. He is also responsible for delegating the task of service deployment. The Service Provider is in this case a commercial entity, because he acts in a commercial way with buying different services (without having the technical background for them) and then repackage them into new more complex services according to the special needs of his customers. This is so to speak a business layer between the technical provision of different services and the final distribution of them. Depending on the situation, this actor may take on various roles.

**Service Developer**

This Actor represents an organisation which is building or selling services and its necessary equipment to consume it. It can interact with the Development Centre and the Certification Centre in order to develop compliant service applications. Depending on the situation, this Actor may take on various roles.

**Fleet Provider**

This Actor represents an organisation that owns and/or operates a fleet of freight carrying vehicles that are licensed to operate on the road network. The Fleet Provider may also be a Freight Service Provider, or an organisation that provides transport services to Freight Service Provider. There may be one or more Fleet Providers operating on all or part of a geographic area.

**Freight Service Provider**

This Actor represents an organisation that provides services that enable the transportation of freight. It can also be a Fleet Provider, owning its own vehicles, or it may hire vehicles from one or more Fleet Providers. There may be one or more Fleet Providers operating on all or part of a geographic area.

**Network Operators and Providers**

This Actor represents organisations that offer wireless and wired connectivity to make devices able to communicate and exchange required data and information.

### 6.3 System Users

**End User**

This Actor represents a human entity that is using system services on a Client Device. A “Client Device” may be a PC (or Laptop), PDA, mobile phone or navigation device, or something that is a combination of all three. It can also be permanently located in the vehicle. An End User may therefore be an Operator, a vehicle Driver, a Pedestrian, a Passenger or any other form of Traveller who is either on a journey, or planning a journey to be carried out at some point in the
future. Vehicle Drivers may be using their own vehicles, or those belonging to a Public Transport or Fleet Provider.

Public Transport Operator
This Actor represents a human entity that uses the facilities of the system to manage the provision of Public Transport services on behalf of a Public Transport Provider. The system may be in communication with more than one human entity that is a Public Transport Operator. Each entity may all belong to the same Public Transport Provider, or to different Providers.

Emergency Operator
This Actor represents a human entity that uses the facilities of the system to manage some of the activities carried out by the Emergency Services Providers in response to incidents. The scope of activities shall be limited to the management of vehicles belonging to the Emergency Services Providers, plus the provision and receipt of information about the incidents. The system may be in communication with more than one human entity that is an Emergency Operator. Each entity may belong to the same Emergency Service Provider, or to different Providers.

Service Centre Operator
This Actor represents a human entity that uses the facilities of the system to manage some of the Services provided by a Service Provider. This Actor will manage the way that the Services are provided including their content and may respond to requests from Services users. The system may be in communication with more than one human entity that is a Service Centre Operator.

Application Management Centre Operator
This actor represents a human entity that uses the facility of the system to manage the operation of applications delivering services to end users.

Road Network Operator
This actor represents a human entity that uses the facilities of the system to actively manage the traffic flows in the road network.

Fleet Operator
This Actor represents a human entity that uses the facilities of the system to manage a fleet of freight carrying vehicles on behalf of a Fleet Provider. It shall be possible for the human entity that is the Fleet Operator to also fulfil the role of a Freight Operator if the Fleet Provider is also a Freight Services Provider. The system may be in communication with more than one human entity that is a Fleet and/or Freight Operator. Each entity may belong to the same Fleet and/or Freight Service Provider, or to different Providers.

Freight Operator
This Actor represents a human entity that uses the facilities of the system to manage the transportation of freight on behalf of a Freight Services Provider. It shall be possible for the human entity that is the Freight Operator to also fulfil the role of a Fleet Operator if the Freight
Services Provider is also a Fleet Provider. The system may be in communication with more than one human entity that is a Freight and/or Fleet Operator. Each entity may belong to the same Freight Services and/or Fleet Provider, or to different Providers.

6.4 Manufacturers/Suppliers

System Supplier
This Actor represents an organisation that is concerned with the development, production and distribution of the system or system components. The System Supplier is interested in providing systems that will enable the Services included in Cooperative Systems to be available to End Users. The Actor may be used to represent the following: OEM, Vehicle Manufacturer, Roadside Equipment Manufacturer, Traffic Management System Supplier

Original Equipment Manufacturer (OEM)
The OEM definition in the automobile industry constitutes a federally-licensed entity required to warrant and/or guarantee their products, unlike "aftermarket" which is not legally bound to a government-dictated level of liability. OEM's are the industry's brand name auto manufacturers, such as General Motors, Ford, Toyota, Volkswagen, etc.

Vehicle manufacturer
This Actor represents an organisation that manufactures the vehicles for use in the road network.

Roadside Equipment Supplier
This Actor represents an organisation that provides equipment that is for use at the roadside. The equipment may provide End Users with instructions and/or information that will assist in their use of the road network, or it may detect the presence of vehicles, End Users, local weather conditions, or atmospheric pollution.

Traffic Management Equipment Supplier
This Actor represents an organisation that provides equipment that is used to manage the use of the road network. The equipment may provide instructions and/or information that will assist End Users in their use of the road network, or it may detect the presence of vehicles, End Users, local weather conditions, or atmospheric pollution, or it may act as the “central” part of a systems to which other equipment, e.g. Roadside Equipment, is connected.

6.5 Authorities

Certification Authority
This Actor represents an organisation which issues digital certificates for use by other parties. The certificates figure as approval for the certified item is valid (i.e. it complies with an assured characteristic).
Public Authority
This Actor represents an organisation that legally obliged to take care and maintain public infrastructures in the most cost efficient way for overall public benefits. It often has broad powers to regulate or maintain public property.

Road authority
This Actor represents an organisation that is responsible for the policy making, enforcement, and rescue operations in road transport. It will want to reduce the negative effects of the use of the road network by End Users.

6.6 Driver
This Actor is a special form of End User. It represents the human entity that controls a licensed vehicle that is on the road network. It represents Drivers of all types of vehicle, but if required the following sub-types of this Actor are used:

Private Vehicle Driver
a person driving a private car, or a light van.

Freight Vehicle Driver
a person driving a vehicle that is designed and licensed for purpose of carrying fright of any kind.

Emergency Vehicle Driver
a person driving a vehicle belonging to one of the Emergency Service Providers.

Hazardous Freight Vehicle Driver
a person driving a vehicle that is designed and licensed for purpose of carrying hazardous freight.

Public Transport Vehicle Driver
a person driving a vehicle that is licensed to carry fare-paying passengers.

The system may be in communication with more than one human entity each of which is a Driver, either as a generic actor, or as a Driver of a particular vehicle type.

6.7 Traveller
This Actor is a special form of End User. It represents the human entity that is using the Services to make a journey. There are two types of traveller:
Dynamic Traveller
a human entity that is currently using the facilities of the system to help them complete his/her journey but is not a Driver.

Static Traveller
a human entity that is currently using the facilities of the system to plan a journey.

The system may be in communication with more than one human entity each of which is a Dynamic or Static Traveller.

6.8 Others

Association of Motorists
This Actor represents an organisation that serves the interests of private car drivers. It will want to strengthen their position by offering them value through defending their interests.

Insurance Company
This Actor represents a private company assuring vehicle owners against damage to their vehicles. It may wish to offer to the vehicle owners new policies based on Cooperative Systems.

Health Services
This Actor represents a public entity (typically a hospital) that needs to know the details of an accident in order to prepare for suitable care for people involved. The accident details are particularly important when one or more vehicles that are involved are carrying dangerous goods. The Emergency Rescue Operator may be a sub-actor or function at the Health Service.

Incident Manager
This Actor represents the legal organisation responsible for managing incidents and keeping up the road safety standards along the incident location.

Town Supervisor
This Actor represents the organisation that is responsible for traffic management at the town level. It will usually have the responsibility for creating a smooth, accident-free optimal traffic flow in towns.

Traffic Managers
This Actor represents the human entities that are responsible for traffic management at the road network level. They have the responsibility of creating smooth, accident-free optimal traffic flows on road networks.
**Transport Providers**

This Actor represents the organisations that want their vehicles to travel from A to B in a fast, safe and efficient and effective way so that they can provide a “transport service” to Travellers. They are in effect another form of Public Transport Service Provider but are unlikely to provide regular services that operate to schedules. This type of organisation will be interested in intelligent travel assistance and new services as long as it improves the performance of their businesses.
7 Architectural Views

This chapter describes the possible approaches and process steps for the definition, setup of subsystems and validation for a future EU ITS Architecture. Hereby the top down approach from a European perspective and methodology point of view is complemented by the bottom up approach of several parallel running projects and their validated results of subsystems and components. The related organisational models of the projects are drafted briefly. This leads to the used communication technologies in the following chapter.

The overall process to define the necessary viewpoints in this European ITS architecture can briefly be described as follows and combines two approaches which are currently performed in parallel: A top-down approach for an Overall High Level Framework of a European ITS architecture, in short called FRAME, and a parallel technical proof of concept for single system definitions of that framework within the currently running EU research and development projects COOPERS, CVIS and SAFESPOT.

These projects are collaborative efforts of project consortia and therefore include varying levels of functionalities, depending on the partners which work together. For this reason the technical and functional definitions have a “centre of gravity” for each of the projects. Apart from these centres of gravity, there is also in future space for further functionalities and elements of the system definition. The architecture allows for both other (e.g. non-communication related) system elements and future extensions of functionalities that they can be included in the overall EU ITS framework architecture.

Figure 14: System Views

Just as it is possible to deal with different parts or segments of the overall framework, both the combined and harmonized picture provided with this document as well as certain specific segments (e.g. as addressed by different projects or stakeholder groups) can also be viewed from changing perspectives to understand the implications of single system aspects for the overall layout. This is illustrated in Figure 14 that shows how one can both deal technically with
different system parts e.g in vehicle integration of systems as well as view the system from different angles, e.g user reaction to used communication technology.

The viewpoints provided in the following section are those recommended by the FRAME approach, the functional, communication and physical viewpoint which later need to be complemented by additional ones for full system deployment. The first part of this chapter provides harmonized views on the overall system following the FRAME methodology. The second part of the chapter provides views as generated by individual projects or initiatives. They are providing certain interpretations of the overall system. Using examples, it is explained how they relate to the extracted common viewpoints.

7.1 Top down Approach: European ITS Framework architecture

7.1.1 Introduction, History, Contents and Tools

The European ITS Framework Architecture (often called "FRAME" for short) provides guidelines and an approach to the planning, development and implementation of ITS. The first version was developed in the European Commission funded KAREN project with the focus on road-based ITS applications with eight major functional areas.

The KAREN project was followed by the FRAME projects (Framework Architecture made for Europe) which were funded by the European Commission. The linked projects (FRAME-NET and FRAME-S) promoted the use of the Framework Architecture and give support to the users. It is from these projects that the Framework Architecture got its short name of "FRAME".

7.1.2 Contents

FRAME consists of a set of User Needs and a Functional Viewpoint containing the functionality needed to support them. The Functional Viewpoint is divided into eight areas which comprise: Electronic Payment, Safety and Emergency Facilities, Traffic Management, Public Transport Management, Advanced Driver Assistance Systems, Traveller Journey Assistance, Support for Law Enforcement and Freight and Fleet Management. Each area contains functionality for its particular part of ITS.

7.1.3 Tools

FRAME provides two tools that can be used for creating subsets of the European ITS Framework Architecture to suit particular ITS implementations: These tools are the FRAME Browsing Tool and the FRAME Selection Tool. Together they provide two principal features:

- The opportunity to browse through the European ITS Framework Architecture with the related elements and their definitions.
- The opportunity to select a sub-set of the European ITS Functional Viewpoint that complies a sub-set of the European ITS User Needs for creating a Physical Viewpoint of that sub-set.

The FRAME Selection Tool enables users to select the elements – User Needs, Functions, Functional Data Flows, Data Stores – for their own project related requirements. For further details on the process of ITS architecture creation and update please see at [FRAME1] and [FRAME2] in section 0.
7.2 Use with Cooperative Systems

The FRAME User Needs and the status of the current mapping to existing definitions which are the basis for the COOPERS, CVIS and SAFESPOT architectures are described in chapter 5. The steps of this definition work for a common European ITS Framework Architecture that will in the future support cooperative systems are as follows.

- Definition of a common requirements document, showing the new and mapped FRAME User Needs that are based on the defined requirements of the 3 mentioned projects. This work has been completed and is described in Chapter 5.
- Elaboration of an extended version of the Functional Viewpoint to support the additional User Needs created in the first step.
- The next step is the definition of the Physical Viewpoint of the project related systems with the assignment of functions or functional blocks to physical locations and system elements. From this work the main hardware parameters and descriptions will be extracted and it can be expected to generate a first consistent overall system description including the subsystems necessary for single projects or initiatives and their proofs of concept for technology elements.
- The final step is the determination of the Communication Viewpoint of the ITS Architecture which defines the necessary communication infrastructure specifications to serve all user needs taken into account in the previous phases, but also the respective revisions necessary in the course of the system definition and specification.

For a new overall picture of the European ITS Framework Architecture with a combination of all the steps mentioned previously at single project level, the EC has contracted in FP7 the E-FRAME project. This has the mission to extend FRAME with the functionalities of cooperative systems. E-FRAME has started in June 2008 with duration of 36 months, and will make all the deliverables as well as functional extensions of FRAME in their respective data bases publicly available.

7.3 Technical Proof of Concept

To complement this process with a bottom up approach in the technical work the projects COOPERS, CVIS and SAFESPOT have started in the first quarter of 2006 in parallel to collect their own system requirements, as well as the C2C communication consortium which has published them on 28th August 2007 in the so called Manifesto of the CAR 2 CAR communication consortium. [Car2Car1].

Hereby the projects have their main focus of work or “center of gravity” in different areas of cooperative systems and therefore define the ITS architecture for the single project according to the partnership of the project consortia, but cooperate with the respective other project in several areas were common interest and work items exist.

The “centre of gravity” for the project activities or main areas of work for each project are as follows:

- COOPERS – traffic management and road safety relevant information for drivers
- CVIS – communication technology development, CALM standardisation and developement of applications
- SAFESPOT – vehicle ad hoc networks, VANET for critical safety applications

These subsystems are the basis for the validation and demonstration phases of the projects.
As these systems interact in a future deployment scenario of cooperative systems it is not defined now how the common functional blocks and the integration of them at sub system level will take place in the different domains. But together with the experiences made in the validation and demonstration phases of the projects in the year 2009 the next steps can be planed, defined and tested accordingly.

Figure 15: Overview of Cooperative Systems Technical Elements and Sub-systems

In Figure 15 an overview of the several systems involved is presented as a graphical representation for all the system domains from the drivers' point of view: in vehicle systems, car2car communication systems, road side units and communication networks, and central systems e.g traffic control centres for infrastructure management purposes. Hereby the scale on the right side indicates reaction times from the user, but also time horizons of the involved systems as well as their geographic area of reach and interaction with the user. For the single technical elements and the functional breakdown in sub-systems, modules, etc. it is refered to the references of the single projects in section 16.4

An overview of the communication viewpoint of the draft reference architecture of the C2C communication system elaborated in the EU project COMeSafety for C2C and C2I communication is shown in the following Figure 16

It comprises 3 different domains: in-vehicle, ad hoc, and infra-structure domain and has the objective to enable a communication between vehicles from all European manufacturers, possibly from all manufacturers. For details see the reference in section 0
After the discussion between the projects involved it seems not possible for various reasons to include an organisational viewpoint of the overall ITS system architecture at this point in time, but rather several models that have been defined in the single research projects and which could lead to different organisational settings in the future ITS deployment of cooperative systems. Hereby the starting point for the organisational setting is the technical solution of the various systems and networks developed in COOPERS, CVIS and SAFESPOT projects with the following main aspects of organisations and entities involved.

COOPERS – bidirectional data network with strong centralized functionality – Operator of the data network (and road infrastructure network) has the main responsibility for collecting, processing, coding and distribution of high quality traffic information for road safety relevant information to the travellers. Therefore he assures service quality, continuity and improvements with the data network built and operated for this purpose and extended to be able to communicate traffic management information in the best and direct way to the driver.

CVIS – generally a peer to peer type of network with changing characteristics of responsibility and roles between partners involved. System responsibilities for setup, service operation and improvement will be defined according to business and deployment models developed in the coming phases of the project.

SAFESPOT – a vehicular ad-hoc network (VANET) based on accidental meetings between network nodes which have roles in the data communication depending on the specific scenario. Hereby the main responsibilities will generally not be defined for long periods but rather for short time frames related to a network session classified applications into two different categories.
Applications are classified as vehicle based applications and infrastructure based applications. In the first case the vehicle is able to elaborate and fuse raw data from infrastructure, other vehicles and own sensors and then to define the warning to the driver. This kind of application could be seen as extended ADAS applications (e.g. cooperative collision warning). In the second case the vehicles are providing raw data to the infrastructure that elaborates specific warnings to be provided to the drivers. This second class is conceptually close to the COOPERS viewpoint. A SAFESPOT vehicle is able to manage contemporarily the two class of applications. In case of multiple applications providing warnings at the same time it is the responsibility of the vehicle to present the highest priority messages according to a predefined classification.

For these aspects of project work the organisational setting has to be divided into two aspects: the starting projects demonstration phase and the future deployment phase of cooperative systems in Europe. In the currently running demonstration and validation phases of the projects the proposals for the organisational settings include all necessary stakeholders but are at the same time pragmatic decisions for facilitating technical project work without high additional burden from an organisational or legal point of view.

After a confirmation of the main technical elements and as a preparation for a deployment phase additional regulatory and legal aspects will need to be addressed. Some of them are mentioned in chapter 2, the main topics for implementation in chapter 14.
Part II: Technology

8 Access Technologies

This Chapter provides details of the contents of the Access Technologies block in the ITS Station Reference Architecture shown in Figure 17. When reading it, the list of references in Annex 1 should be consulted. Note that while most of the contents of this document are subject to constant evolution, the issues described in this chapter can be expected to evolve and change particularly fast.

The detail of the Access Technologies block is provided by Figure 17. Both wired and wireless access technologies are depicted for both station-external and station-internal use, however, this chapter only describes wireless access technologies, i.e. different types of radio systems.

The following wireless systems are assessed in this chapter:

- Short range and ad-hoc systems:
  - CEN DSRC
  - European 5.9 GHz ITS
  - WLAN 5 GHz
  - IR

- Cellular systems:
  - WiFi
  - WiMAX
  - GSM/GPRS
- UMTS
- Digital broadcast systems:
  - DAB and DMB
  - DVB and DVB-H
  - GPS

Wired technologies are mainly used as Station-Internal Interfaces, whereas wireless technologies are primarily used as Station-External Interfaces. The purpose of the Access Technologies block is to handle the interfaces to the different communication technologies. An access technology typically contains only the two lowest layers in the ISO OSI stack, namely the physical (PHY) and the data link layers (DLL). However, for some of the access technologies, e.g., 2G/3G, or BlueTooth, the entire communication protocol stack is used. The Access Technologies block is managed via the MI-SAP, through which a list of physical interfaces (outputs) is provided such that a particular access technology can be selected for communication (input). SI-SAP deals with the security issues and will typically contain dynamic MAC addresses to protect privacy, as well as special restrictions on medium access rights. Finally, the IN-SAP is the interface towards the Networking and Transport block.

The same way as the word “traffic” has an ambiguous meaning in the context of vehicular communication (i.e., it can relate either to data traffic or vehicle traffic) the word “infrastructure” can refer either to communication infrastructure (e.g., access points and base stations used by a communication technology) or road infrastructure (e.g., road signs or toll stations). The former is most important in the lower protocol layers whereas the latter is more important in the application layer. Since this chapter deals with access technologies and especially the DLL and PHY layers, no real distinction is made if communication takes place in-between vehicle stations or between a vehicle station and a roadside station. On the contrary, even though the communication infrastructure is typically found in the network layer, it affects e.g., the latency and the choice of MAC method in the DLL and PHY. Consequently, there is a vast difference between access technologies that uses communication infrastructure and those that do not, and thus in this chapter the notation infrastructure refers to communication infrastructure. In the non-ITS context, communication infrastructure is referred to either as access points (typically in data communication networks such as WLANs) or base stations (typically in telecommunication networks such as GSM). In a network containing access points or base stations, all communication must take place via the access point or base station. This implies that no peer-to-peer or direct vehicle-to-vehicle communication is possible and that the minimum delay/latency consequently is longer. A network without access points or base stations is referred to as an ad-hoc system. Communication in an ad-hoc system can take place using peer-to-peer communications or master-slave communications (where a master is temporarily appointed and after a while goes back to being a regular peer).

In the Section “Short range and ad-hoc systems”, two-way communication systems without cellular structure are treated. Short range systems often use a (temporary) master and therefore typically require a setup procedure. However, communication generally takes place between the master and its slaves rather than the master transferring information between slaves. Ad-hoc systems employ direct peer-to-peer communications. Next, Section “Cellular systems” treats the data communication systems WiFi and WiMAX which includes access points and the telecommunication systems GSM and UMTS which include base stations. Communication primarily takes place between vehicle/roadside/personal stations via the access points or base stations (two-way asymmetric communication: up-link and down-link), but the access point or base station can also be used to broadcast information, although most cellular standards have only limited support for this. Finally, in the Section “Digital broadcast systems” communication primarily takes place by the base station broadcasting information in a one-way fashion (only down-link). In some systems a smaller up-link is also available but this is less common.
The radio systems are examined with respect to a number of parameters that are considered important for cooperating vehicular systems, namely:

**Standard**
If the radio system is based on or using a particular standard this is stated here.

**Antenna**
If only one antenna that can be placed anywhere is needed, this is indicated here by the word “rooftop”. If more than one antenna in specific locations are needed this is stated here.

**Frequency band**
The frequency band used/reserved/planned in Europe is stated here. If different bands are used in America or Asia, this is also stated.

**Channels** (number, size and separation, control channels, data channels)
The way the frequency spectrum is used is stated here, i.e., how the spectrum is divided among users and between control/signalling and data/payload traffic.

**Output power** (including possible power control)
Maximum allowed output power, spectrum masks and any potential power control is stated here.

**Data rate** (including range and latency)
The data rate mentioned here implies transmitted data rate in bits per second (bps) and says nothing about the quality of the received information. Data rate defined this way depends primarily on the type of coding and modulation schemes used. Therefore a lower data rate often has the ability of providing a higher data reliability. Range, on the other hand, is related to received data quality, presumed radio channel, carrier frequency as well as allowed output power. The measure provided here, when present, is the value stated in the different standards, which typically assumes that the allowed output power and data rate are used. Further it assumes that a particular received data quality is called for and a specific radio channel is used, which is directly related to the requirements imposed by its intended application (e.g., voice or data) and its intended context of use (e.g., stationary or mobile).

Latency (or communication delay) for an access technology is strictly defined here as the time from the start of packet transmission to the start of packet reception at the end node (possibly after relaying via an access point or a base station). This definition of latency is independent of the throughput and the packet size and is the absolute minimum delay possible. Latency obviously depends on the distance between transmitter and receiver, so here the intended use of the radio system again comes into play. The measure latency will thus here relate to the typical distance used by the particular radio system (e.g., short range or long range). In some cases the latency is implementation dependent, and this will then be stated. Finally, in many cases an exact value of the latency is not possible to give, and then an indication such as if the communication takes place via a base station or not is given.

The measure throughput is usually defined as the number of messages (successfully) delivered per unit time. Since it depends on several network parameters (e.g., queueing, two-way latency, available bandwidth, radio channel quality and potential retransmissions) it is instead treated in the next chapter. Finally the important measure data reliability is not treated in this chapter either as it depends on too many parameters including data rate, output power, frequency band, the particular radio channel and instantaneous interference. The reliability values listed in the standards are typically voice call drop percentage or measures including the TCP protocol (i.e., connection oriented). For time-critical data applications these measures are of little importance. For IEEE 802.11p for example, a target reliability measure is a packet error rate (PER) of less than 10% for vehicles driving in the same direction at the same speed of 140 km/h. However, depending on the distribution of these 10% it could potentially be devastating for some applications. Therefore reliability measures are better provided on a protocol level where some application requirements and intended mode of usage are known.
**MAC** (including real-time support, scalability, priority support, QoS)
The MAC protocol decides who is allowed to transmit when on the shared wireless channel. MAC methods can be distributed (typically for ad-hoc systems) or centralized (typically when base stations or access points are used). A centrally controlled MAC method is almost always predictable such that channel access is deterministically guaranteed within a certain maximum time (max delay). This implies that real-time traffic can be supported (given that the maximum delay is suitable for the application in question). The behaviour of the MAC method as traffic density increases (either due to increased data traffic by each vehicle or due to increased vehicle traffic) is referred to as scalability. Finally the ability of the MAC protocol to support traffic with different priorities (e.g. safety and efficiency) as well as different QoS classes (a more advanced way of expressing priority which may be expressed as high requirement on low delay, but moderate requirement on reliability) is treated. Note that QoS and real-time support is not synonymous since a protocol may provide improved quality of service in the form of reduced average delay – while the maximum delay remains unbounded. Of course, real-time traffic can still be transmitted using non-deterministic MAC methods with QoS support, but then the radio system often needs to be over-dimensioned. This, in turn, implies that the support for scalability is reduced.

**Transmission modes** (directed, one- or two-way, broadcast, peer-to-peer)
The radio signal can be directed (aimed in one direction only) or omni-directional (aiming in all directions).
Communication can take place using one-way communications (typically in master/slave systems or broadcast systems) or two-way communications (typically in ad-hoc or cellular systems).
The radio system may support broadcast or not (either in a one- or a two-way fashion).
The radio system may support direct peer-to-peer communications (without using an access point or a base station) or not.

**Requirements** (prerequisites or constraints, i.e., relies on GPS or communication infrastructure)
If something other than station and antennas are needed it is stated here.

**Interference** (intra- and inter-system)
System internal limiting factors are termed intra-system interference (also called co-channel interference), whereas when two different radio systems interfere this is termed inter-system interference, also called adjacent or neighbour channel interference.

Each radio system is typically developed for a particular purpose and as such they are best if used for this purpose. Data communication networks such as WiFi are developed for high rate internet applications and therefore usually provide high rate and high reliability but no real-time support. Telecommunication networks such as GSM are developed for voice applications and consequently provide low delay real-time support at the expense of reduced reliability. Note however, that the reduced reliability can be tolerated for voice applications whereas this is not the case for most applications carrying data traffic. Other radio systems such as CEN DSRC are even more application specific and thus if used in the intended context they provide high performance. Few, if any, current radio system can support high reliability, low latency/delay real-time communications since typically reliability is increased with increased delay (e.g. using retransmissions).

### 8.1 Short Range and Ad-Hoc

This section treats the short range systems “CEN DSRC 5.8 GHz” and “IR” and the ad-hoc systems “European 5.9 GHz ITS” and “WLAN 5 GHz”.

8.1.1 CEN DSRC 5.8 GHz

This is a radio system with focus on short range communication. It is intended for ETC systems and thus a roadside station is needed which acts as a master and the vehicle and personal stations as slaves. This is a good radio system for collecting information from passing vehicles or for informing passing vehicles about local conditions around the roadside station. The roadside station may or may not be further connected to a server or to the internet.

**Standard**
Must support European standards: EN12253-2004 (DSRC L1), EN12795 (DSRC L2), EN12834 (DSRC Application Support), EN13372 (DSRC Profiles).

**Antenna**
Rooftop (according to EN12253).

**Frequency band**
ECC/DEC(02)01 and CEPT/ERC REC 70-03:
(a) 10 MHz at 5.795-5.805 GHz and (b) another 10 MHz on a national basis with individual licence in the adjacent band at 5.805-5.815 GHz (see Figure 18)

**Channels** (number, size and separation, control channels, data channels)
The 20 MHz at 5.795-5.815 GHz is divided into 4 channels with the recommended 5 MHz channel spacing, where the centre frequencies are 5.7975 GHz, 5.8025 GHz, 5.8075 GHz and 5.8125 GHz respectively. Note that some countries only allow channels 1 and 2. For 10 MHz channel spacing systems the centre frequencies are 5.800 GHz and 5.810 GHz.

**Output power** (including possible power control)
Max output power: 33 dBm EIRP.
The use of 8 W EIRP allows for 1 Mbps in accordance with ETSI standard ES 200 674-1. 2 W EIRP allows for 500 kbps downlink and 250 kbps uplink in accordance with EN 300 674-1 and for low data rates (31 kbps) in accordance with EN 300 674-2.

**Data rate** (including range and latency)
Applying EN 300 674-2, downlink 500 kbps, uplink 250 kbps.
Range: 3-15 m
Short connection set-up time: 5-12 ms.
To support low delay communications a reduced protocol stack is used (physical, link and application layers).
Latency: 10 ms. No system-determined latency (i.e., direct master-slave communications). Random latency due to MAC method (see MAC below).

**MAC** (including real-time support, scalability, priority support, QoS)
TDMA, roadside station is master, vehicle and personal stations are slaves. Roadside station broadcasts a beacon, and vehicle stations randomly pick slots after this.
The roadside station determines the number of vehicle station slots to follow the beacon and thus also the scalability.
Normally TDMA supports real-time (the time before channel access can be determined deterministically), but since slots are picked at random by the vehicle stations, collisions may occur and thus real-time cannot be guaranteed.
No priority or QoS differentiation.

**Transmission modes** (directed, one- or two-way, broadcast, peer-to-peer)
Directed (omni-directional also exist).
Two-way communications (asymmetric).
Broadcast from roadside station to multiple vehicle stations (one-way broadcast), point-to-point as well as point-to-multipoint
Not intended for inter-vehicle communications since roadside station is master (no peer-to-peer).
Requirements (prerequisites or constraints, i.e., relies on GPS or communication infrastructure)
Requires a roadside station.

Interference (intra- and inter-system)

Intra-system interference:
Since the system is based on roadside stations being masters, the intra-system interference from other masters can be controlled by careful placement of roadside stations. However, vehicle stations may collide when randomly picking a time slot. A larger number of allowed time slots will reduce this probability (the profile standard that is mandatory in Europe does, however, fix this to three public slots).

Inter-system interference:
See Terms of Reference of ERM TG37, Intelligent Transport Systems.
It appears that CEN DSRC roadside station reception can be interfered by ITS communication equipment at 5.9 GHz. Depending on the antenna beams alignment, ITS communication equipment at 5.9 GHz may also be interfered by DSRC in the communication zone of the DSRC roadside station. CEN DSRC is a Short Range Device (SRD), listed in the CEPT/ERC REC 70-03 and in general SRDs cannot claim protection from other radio services. Nevertheless according to the ECC/DEC/(08)01, safety related ITS applications at 5.9 GHz has to protect existing services in its band and in adjacent bands, i.e., the ITS out of band emission is for now limited to – 65 dBm in the CEN DSRC band.

8.1.2 European 5.9 GHz ITS

This is a radio system based on the WLAN standard, but with focus on low delay ad-hoc data communication between vehicle stations and between vehicle and roadside stations, i.e., no access points are needed. This is a good radio system for traffic safety applications and inter-vehicle communications as long as the system load is reasonable (see MAC method below).

Standard
Will be based on the upcoming standard IEEE 802.11p.

Antenna
Rooftop

Frequency band
Below are the frequency bands that are currently reserved (EC decision on March 2008) in the EU and thus can be used for testing for now. Evaluation will follow.
ECC/DEC/(08)01: designation of 5875-5905 MHz on a non-exclusive basis for ITS road safety applications, and consideration of the frequency sub-band 5905-5925 MHz for future extension noting that protection of ITS cannot be ensured in this band extension. (see Figure 18).
ECC/REC/(08)01: assignment of 5855-5875 MHz for non-safety ITS applications to be deployed on a non-protected and non-interference basis.
(USA uses 75 MHz of spectrum within the band 5850-5925 MHz.)
(Japan uses 80 MHz within the band 5770-5850 MHz.)

Channels (number, size and separation, control channels, data channels)
The 30 MHz at 5875-5905 MHz are for now divided into 3 sub-channels of 10 MHz each, where the first one, SCH 1, is the main service channel for safety and efficiency messages (optimized for high throughput, safety messages with medium priority, multihop and geocast messages at the second hop), the second one, SCH 2, is a service channel used only with low transmission power for very short range communications, mainly between vehicles and roadside stations (optimized for peer-to-peer communication), and the last one at 5895-5905 MHz is a control channel, CCH, which also can be used for time critical messages (optimized for low latency, cyclic network layer packets, high priority safety messages, multihop and geocast messages at
the first hop). While this control channel for now is common for all applications, efficiency and other services will often use its own data channel of 20 MHz in the 5.5 GHz band, as described below. Note that testing to prove the optimum use of the available band may result in different configurations. Such testing is going on in US projects and in European projects.

**Output power** (including possible power control)
The maximum spectral power density for ITS stations should be limited to 23 dBm/MHz EIRP. The total power shall not exceed 33 dBm EIRP with a Transmit Power Control (TPC) range of 30 dB.

Unwanted emissions to be kept below (see Figure 18):

- 65dBm/MHz below 5815 MHz
- 55dBm/MHz below 5850 MHz
- 65dBm/MHz above 5925 MHz

**Data rate** (including range and latency)
IEEE 802.11p uses the IEEE 802.11a physical layer with adaptations to support higher vehicular speeds. The rates 3, 4.5, 6, 9, 12, 18, 24 and 27 Mbps in 10 MHz channels are currently available in the standard. Most likely a low rate (e.g. 6 Mbps) will be chosen since traffic safety applications require a high reliability.

Range: 500 m at maximum power and minimum data rate.

No connection set-up time is required due to the ad-hoc mode (although authentication etc will be required at start-up).

The IEEE 802.11 5.9 GHZ related communication stack is designed with the aim of supporting low delay data communications.

Latency: Implementation dependent. No system-determined latency (i.e., direct peer-to-peer communications). Random latency due to MAC method (see MAC below).

**MAC** (including real-time support, scalability, priority support, QoS)
IEEE 802.11p is based on IEEE 802.11 which uses CSMA. Since collisions may occur indefinitely with CSMA, IEEE 802.11p does not support real-time communications. The probability of collisions occurring may however be reduced if the load of the network is kept low (i.e., if the data traffic is low), but channel access can still not be deterministically guaranteed. This also implies that CSMA does not scale well. Above a certain network load (depends on the number of transmitting vehicles, the number of data packets, the length of data packets, etc) collisions are frequent and the usability of IEEE 802.11p rapidly decreases. Congestion control by upper layers could be a way of preventing this.

The MAC layer of IEEE 802.11p is enhanced with EDCA from IEEE 802.11e to support priority and QoS differentiation. Four different queues corresponding to four different service classes are provided.

As an example, SAFESPOT for now defines five priority levels: PRI\textsubscript{Emergency}, PRI\textsubscript{VANET}, PRI\textsubscript{High}, PRI\textsubscript{MID} and PRI\textsubscript{Low}. It is assumed that these priority levels are associated with the different application classes, but when communicating in geocast or multihop mode it describes the communication priority on the first hop only, i.e., multihop and geocast communication allows only the 1\textsuperscript{st} hop priority PRI\textsubscript{Emergency}. The priorities can be enforced by using the different channels SSH 1, SSH 2 and CCH as described above.

**Transmission modes** (directed, one- or two-way, broadcast, peer-to-peer)
Omni-directional (with some roadside stations using directional antennas).

Two-way communications (symmetric).

Broadcast, point-to-point as well as point-to-multipoint should be supported (two-way broadcast, i.e., any station can broadcast).

Peer-to-peer (not intended to use communication infrastructure).

**Requirements** (prerequisites or constraints, i.e., relies on GPS or communication infrastructure)
Can use GPS to synchronize slotted aloha, but not needed. No communication infrastructure is required.
Interference (intra- and inter-system)

Intra-system interference:
The MAC method CSMA may cause system internal interference by collisions. For this reason the network load needs to be controlled.

Inter-system interference:
Interference with CEN DSRC as described above.
In the band 5.855-5.875 GHz considered for non-safety applications, ITS may suffer from interference from several different applications.
There is a probability of interference from Fixed Satellite Services (FSS) in the vicinity of earth stations, but these are very limited in number and the impact depends very much on the real terrain shielding.
ITS applications within the band 5.905-5.925 GHz considered for future extensions may suffer from interference by Fixed Services (FS) operated above 5.925 GHz.
While the spectrum mask and other regulations for the use of 5,9GHz frequency takes care that system interference is kept to a minimum, there may be cases that will need additional technical adaptations or usage rules. If that will turn out for certain instances, these will be stated here in future updates of this document.

8.1.3 WLAN 5 GHz

This is a radio system based on the WLAN standard, but with focus on low delay ad-hoc data communication between vehicles. It is intended for use similar to European 5.9 GHz ITS but using a different frequency channel. This is a good radio system for traffic efficiency applications and inter-vehicle communications as long as the system load is reasonable (see MAC method).

Standard
Will be based on the upcoming IEEE 802.11p standard.

Antenna
Rooftop

Frequency band
5 GHz band: 5.47 GHz – 5.725 GHz, (see Figure 18)

Channels (number, size and separation, control channels, data channels)
One 20 MHz data channel for efficiency ITS applications and other services is used to complement European 5.9 GHz ITS for now, see above.

Output power (including possible power control)
The maximum spectral power density for ITS stations should be limited to 17 dBm/MHz EIRP.

Data rate (including range and latency)
IEEE 802.11p uses the IEEE 802.11a physical layer with adaptations to support higher vehicular speeds. The rates 3, 4.5, 6, 9, 12, 18, 24 and 27 Mbps in 10 MHz channels are available in the standard. Most likely a low rate (e.g. 6 Mbps) will be chosen since traffic safety applications require a high reliability.
Range: 500 m at maximum power and minimum data rate.
No connection set-up time is required due to the ad-hoc mode (although authentication etc will be required at start-up).
The IEEE 5,9 GHz related communication stack is designed with the aim of supporting low delay data communications.
Latency: Implementation dependent. No system-determined latency (i.e., direct peer-to-peer communications). Random latency due to MAC method (see MAC below).

MAC (including real-time support, scalability, priority support, QoS)
IEEE 802.11p is based on IEEE 802.11 which uses CSMA. Since collisions may occur indefinitely with CSMA, IEEE 802.11p does not support real-time communications. The
probability of collisions occurring may however be reduced if the load of the network is kept low (i.e., if the data traffic is low), but channel access can still not be deterministically guaranteed. This also implies that CSMA does not scale well. Above a certain network load (depends on the number of transmitting vehicles, the number of data packets, the length of data packets, etc) collisions are frequent and the usability of IEEE 802.11p rapidly decreases. Congestion control by upper layers could be a way of preventing this. The MAC layer of IEEE 802.11p is enhanced with EDCA from IEEE 802.11e to support priority and QoS differentiation. Four different queues corresponding to four different service classes are provided.

**Transmission modes** (directed, one- or two-way, broadcast, peer-to-peer)
Omni-directional (with some roadside stations using directional antennas).
Two-way communications (symmetric).
Broadcast, point-to-point as well as point-to-multipoint should be supported (two-way broadcast, i.e., any station can broadcast).
Peer-to-peer (not intended to use communication infrastructure).

**Requirements** (prerequisites or constraints, i.e., relies on GPS or communication infrastructure)
Can use GPS to synchronize slotted aloha, but not needed. No communication infrastructure is required.

**Interference** (intra- and inter-system)
Intra-system interference:
The MAC method CSMA may cause system internal interference by collisions. For this reason the network load need to be controlled.
Inter-system interference:
Interference with IEEE 802.11a.

### 8.1.4 Infrared

This is a radio system that can provide directed communications. It is good for very short range inter-vehicle communications as well as short range communications between roadside stations and vehicle stations. Especially, vehicles in a particular lane can be targeted.

**Standard**

**Antenna**
Mounted at front or rear (where communication is intended).

**Frequency band**
800 to 1000 nm wavelength.

**Channels** (number, size and separation, control channels, data channels)
4 independent infrared channels.

**Output power** (including possible power control)

**Data rate** (including range and latency)
Data rate: 1Mbps (and 2Mbps in CALM IR)
Range: 1 – 100 m (typical 7 m)
Connection set-up time: 10 ms
To support low delay communications a reduced protocol stack is available (physical, link and application layers).
Latency: 10 ms. No system-determined latency (i.e., direct master-slave communications). Random latency due to process of selecting a master (see MAC below).

**MAC** (including real-time support, scalability, priority support, QoS)
ISO 21214 defines TDMA for synchronized communications between multiple peers. However, one of the peers will temporarily be a dedicated master and organize the TDMA slots. A master organizing TDMA slots suggests deterministic channel access as long as the process to select a master is successful. Scalability is often a problem for TDMA protocols, but if the range is limited so is the number of potential network members.

CALM-IR supports 8 different priorities and a lower priority task will be interrupted if a higher priority task enters the system.

**Transmission modes** (directed, one- or two-way, broadcast, peer-to-peer)
- Directed communication.
- Two-way communications (symmetric).
- Broadcast point-to-point, directed broadcast, point-to-multipoint (several different communication zones can be defined). Different beams can provide different communication zones implying that different range and throughput can be used for different types of applications.
- Peer-to-peer (a peer temporarily becomes master).

**Requirements** (prerequisites or constraints, i.e., relies on GPS or communication infrastructure)
- One antenna for each intended direction is required, since IR communication relies on line of sight conditions.

**Interference** (intra- and inter-system)
- Intra-system interference: due to the high frequency IR may have problems with sun, rain and snow.
- Inter-system interference: None.

### 8.2 Cellular

This section treats the data communication standards WiFi and WiMAX and the 2G telecommunications standard dominant in Europe: GSM and its packet based extension: GPRS as well as the 3G standard dominant in Europe: UMTS which is packet based. The network topologies of these radio systems are cellular, containing a base station or an access point that controls the medium access within the cell and a handover process that works seamlessly to the end user (note however, that WiFi has limited support for handover). Mobile WiMAX networks work much the same way as cellular phone systems, where a user pays for subscription and get access to the Internet as long as there is coverage.

#### 8.2.1 WiFi

This is a radio system based on WLAN with focus on high rate data communication. This is a good radio system for internet access and high speed data communications when vehicle speeds are moderate.

**Standard**
- Must support IEEE 802.11a/b/g.

**Antenna**
- Rooftop

**Frequency band**
- 5 GHz band: IEEE 802.11a, (see Figure 18)
- 2.4 GHz: IEEE 802.11a/g

**Channels** (number, size and separation, control channels, data channels)
- Originally 12/13 non-overlapping channels
Output power (including possible power control)
17 dBm/MHz EIRP, 30 dBm max EIRP.
- TPC with a mitigation factor of at least 3 dB or general power reduction by 3 dB.
- Dynamic Frequency Selection (DFS) to protect military radio location applications including channel load distribution.

Data rate (including range and latency)
Max 54 Mbps (IEEE 802.11a/g)
- Range: needs coverage by access points.
  - All communication takes place via the infrastructure (access point) and as such the minimum delay is increased. Further, a connection set-up phase is required such that the access point recognize the presence of a new vehicle station.
  - Latency: Implementation dependent. System-determined latency (i.e., communication takes place via infrastructure). Random latency due to MAC method (see MAC below).

MAC (including real-time support, scalability, priority support, QoS)
Since IEEE 802.11a/b/g are based on IEEE 802.11 the MAC method CSMA is supported.
- When access points are included an additional MAC method is available, where the access point will poll each vehicle or roadside station and give them permission to transmit. Using this MAC method, IEEE 802.11a/b/g would be able to support real-time communication. The protocol would also scale well even if the minimum delay will increase for each node that joins the network. However, polling is optional in the standard (whereas CSMA is mandatory) and therefore this feature is not used. Since the CSMA method suffers from unbounded delay due to multiple collisions, real-time communications is not supported with IEEE 802.11a.
  - Prioritisation is defined in IEEE 802.11 Rev. of version 1999. QoS support is not provided.

Transmission modes (directed, duplex, broadcast, peer-to-peer)
- Omni-directional.
- Two-way communication (symmetric).
- Broadcast.
- No peer-to-peer (needs access points).

Requirements (prerequisites or constraints, i.e., relies on GPS or communication infrastructure)
- Infrastructure (access points) is required.

Interference (intra- and inter-system)
- Intra-system interference: the CSMA MAC method may cause system internal interference by collisions. For this reason the network load need to be controlled.
- Inter-system interference: WLAN 5 GHz (the ITS traffic efficiency data channel of 20 MHz for now placed in the 5.5 GHz band).

8.2.2 WiMAX

WiMAX belongs to the group of networks termed metropolitan area networks (MAN) typically spanning a larger geographic area such as a city. From a historical perspective, a MAN connects several LANs. WiMAX is a cellular system based on WMAN with focus on high rate data communication. This is a good radio system for internet access and high speed data communications when vehicle speeds are moderate.

Standard
WiMAX is not a single technology but rather a family of interoperable technologies. The original specification, IEEE 802.16 from 2001, was intended primarily for MANs and “the last mile” connections using spectrum in the 10 to 66 GHz range. In 2004 the extension 802.16-2004 added additional physical layer specifications (including OFDM-256 and OFDMA) for the 2-11 GHz range and in 2005 a mobile version (including handovers between base stations and handovers between operators at vehicular speeds of up to 120 km/h), 802.16e, was released.
Antenna
Rooftop (MIMO)

Frequency band
The 802.16 family of standards does not target specific frequency bands like the IEEE 802.11 does, but instead it is up to the user to apply for dedicated bands in their home frequency regulatory domains. Thus vendors can design equipment for either licensed or unlicensed bands.

Channels (number, size and separation, control channels, data channels)
The IEEE 802.16 standardizes several PHY layers: single-carrier, OFDM and OFDM access (OFDMA).

Output power (including possible power control)
Depends on the frequency band used. See Frequency band above.
Power control is provided.

Data rate (including range and latency)
Downlink 70 Mbps, uplink 70 Mbps – but only at close range and low vehicular speed (practically 10 Mbps at 10 km distance to the access point.
Range: needs coverage by access points. Max range of base station: 50 km (but then data rate is low).
WiMAX access points are highly scalable from "femto"-scale to multi-sector “maxi” scale. All communication takes place via the access point and as such the minimum delay is increased. No new connection set-up phase is required when a vehicle or personal station leaves access point coverage area, since access points support hand-over.
Latency: Implementation dependent. System-determined latency (i.e., communication takes place via infrastructure). No random latency.

MAC (including real-time support, scalability, priority support, QoS)
OFDMA centrally controlled by the access point implies real-time support. WiMAX is very spectrally efficient so it has reasonable scalability, but when all sub-carriers are filled no more nodes can join. However, since access can be added, this problem can be addressed by adding hardware.
QoS and priority is supported, but is relative between packets or flows rather than guaranteed.

Transmission modes (directed, one- or two-way, broadcast, peer-to-peer]
Omnidirectional
Two-way communication (asymmetric, i.e., uplink and downlink).
Limited support for broadcast.
No peer-to-peer communication support.

Requirements (prerequisites or constraints, i.e., relies on GPS or communication infrastructure)
Communication infrastructure in the form of access points is required.

Interference (intra- and inter-system)
Intra-system interference: Limited. Very spectrally efficient.
Inter-system interference: Depends on the selected frequency band.

8.2.3 GSM/GPRS

Since GSM is designed for voice applications it is circuit switched, whereas its extension GPRS is packet switched and is intended for data communications. However, voice still has priority over data in most GSM based networks (this is a parameter that can be altered by the operator, but since no request to change has been noted, the priority assignment remains). A voice application has requirements on low delay, real-time communications but is relatively
error tolerant. This means that it is better to drop a few packets with a temporarily lowered quality as a result, than to introduce longer and longer delays. Data traffic, especially when carrying traffic safety information, have different requirements and needs low delay real-time communication, but not at the expense of the data reliability being too low. This is a feasible radio system for moderate delay, low rate communications in-between vehicle stations as well as between vehicle, mobile and roadside stations (note though that the communication always takes place via a base station), and low speed data communications including internet browsing when vehicle speeds are high.

**Standard**
Must follow the GSM Standard.

**Antenna**
Rooftop

**Frequency band**
900 MHz (uplink: 890-915 MHz, downlink: 935-960 MHz) 1800 MHz (uplink: 1710–1785 MHz, downlink: 1805–1880 MHz)
(US: 850 MHz and 1900 MHz)
Some countries (e.g. Scandinavia) also use 400 and 450 MHz frequency bands

**Channels** (number, size and separation, control channels, data channels)
The 25 MHz bandwidth in the 900 MHz band is subdivided into 124 channels, each spaced 200 kHz apart.
Time division multiplexing allows eight users per channel.

**Output power** (including possible power control)
The transmission power in the handset is limited to a maximum of 2 watts in GSM850/900 and 1 watt in GSM1800/1900.

**Data rate** (including range and latency)
Downlink 60-80 kbps, uplink 20-40 kbps.
Range: needs coverage by base stations. Max range of base station: 35 km.
Initial set-up connection time: 10 s
All communication takes place via the base station and as such the minimum delay is increased.
No new connection set-up phase is required when a vehicle station leaves the base station coverage area, since base stations support hand-over at vehicular speed.
Latency: 500–700 ms. System-determined latency (i.e., communication takes place via infrastructure). No random latency.

**MAC** (including real-time support, scalability, priority support, QoS)
TDMA centrally controlled by the base station implies real-time support – however, this is only true for voice applications and GPRS data is a best effort service.
Limited scalability (when all timeslots are filled no more nodes can join) but since base stations can be added, this problem can be addressed by adding hardware.
Data is best effort, i.e. no QoS support.

**Transmission modes** (directed, one- or two-way, broadcast, peer-to-peer)
Omni-directional
Two-way (asymmetric, i.e., uplink and downlink).
Basically no broadcast ability
No peer-to-peer communication support.

**Requirements** (prerequisites or constraints, i.e., relies on GPS or communication infrastructure)
Requires a base station. Generally, also an agreement with an operator.

**Interference** (intra- and inter-system)
Reserved frequencies. Coordination (roaming agreements) between countries required.
8.2.4 UMTS

UMTS is a packet based network with support for different QoS classes. As such it is more suited for traffic safety applications than GSM/GPRS, but since many of the requirements from a traffic safety application are not called for by a typical cellphone user, support for these are still lacking. For example, the data rate is constantly improved (e.g., HSPA) since this is important to a cellphone user wishing to watch TV on the phone. However, the latency is of less importance so no real effort is made to reduce the minimum delay. In future LTE systems, however, this is expected to change. This is a good radio system for moderate delay, moderate rate communications in-between vehicle stations as well as between vehicle, mobile and roadside stations (note though that the communication always takes place via a base station), and moderate speed data communications including internet browsing when vehicle speeds are high.

Standard
Must follow the 3GPP Standard.

Antenna
Rooftop

Frequency band
900 MHz (uplink: 880-915 MHz and downlink: 925-960 MHz) and 2100 MHz (uplink: 1920-1980 MHz and downlink: 2110-2170 MHz).
(US: 850MHz, 1700 MHz and 1900 MHz.)

Channels (number, size and separation, control channels, data channels)
Channels are 5MHz wide. Frequency division duplex (time division duplex also supported).

Output power (including possible power control)
Power control.

Data rate (including range and latency)
Downlink 384 kbps, uplink 384 kbps (depends on cell breathing, see MAC below).
(HSPA downlink 14400 kbps, uplink 5760 kbps)
Range: needs coverage by base stations. Max range of base station: 2 km.
Initial set-up connection time: 2.12 s
All communication takes place via the base station and as such the minimum delay is increased.
No new connection set-up phase is required when a vehicle station leaves the base station coverage area, since base stations support hand-over at vehicular speed.
Latency: 200 – 300 ms (HSDPA: 100 ms). System-determined latency (i.e., communication takes place via infrastructure). No random latency.

MAC (including real-time support, scalability, priority support, QoS)
CDMA, centrally controlled by the base station implies real-time support.
Reasonable scalability (when all orthogonal CDMA codes are used, non-orthogonal CDMA codes are selected causing cell breathing with reduced performance but graceful degradation) but since base stations can be added, this problem can be addressed by adding hardware.
Priority and QoS support. Although, the service provided depends very much on the proximity to the base station and the vehicle speed.

Transmission modes (directed, one- or two-way, broadcast, peer-to-peer)
Omni-directional
Two-way (asymmetric, i.e., uplink and downlink).
Limited broadcast ability
No peer-to-peer communication support.
Requirements (prerequisites or constraints, i.e., relies on GPS or communication infrastructure)
Requires a base station. Generally, also an agreement with an operator.

Interference (intra- and inter-system)
Intra-system: cell breathing reduces reliability or data rate.
Inter-system: Reserved frequencies. Coordination (roaming agreements) between countries required.

8.3 Digital Broadcast

This section includes two competing standards for mobile digital TV, namely DMB and DVB-H. Since TV is broadcasted these standards have limited support for two-way communication, i.e., basically only downlink communication exists. They do however have very good coverage and digital broadcast is thus best for informing multiple vehicles about events. The benefit is that all vehicles will receive the same event information at the same time and can then act accordingly. GPS has also been included in this section even though it is not an access technology as such, albeit it does broadcast information. However, since GPS receives are needed on vehicle, mobile and roadside stations wishing to use the positioning application it is important to take GPS into account when attempting to minimize interference between different wireless technologies.

8.3.1 DAB and DMB

DAB (Digital Audio Broadcasting) is also known as Digital Radio or Eureka 147. Digital Multimedia Broadcasting (DMB) is based on the DAB standard and has some similarities with the main competing mobile TV standard: DVB-H. It is a digital radio transmission system for sending multimedia (radio, TV, and datacasting) to mobile devices such as mobile phones. DMB was developed in South Korea under the national IT project, originally as the next generation digital technology to replace the FM radio.

Standard
DMB is an ETSI standard (TS 102 427 and TS 102 428).

Antenna
Rooftop

Frequency band
Eureka 147 DAB uses a wide-bandwidth broadcast technology and typically spectra have been allocated for it in Band III (174–240 MHz) and the L-band (1452–1492 MHz), although the scheme allows for operation almost anywhere above 30 MHz. The US military has reserved the L-band, blocking its use for other purposes and therefore both DAB and DMB are unavailable in the USA. It is used mainly in Europe, Canada, China, India and Australia.

Channels (number, size and separation, control channels, data channels)
A main service channel and a fast information channel. The main service channel can be divided into several audio and data sub-channels.

Output power (including possible power control)
Power control not applicable.

Data rate (including range and latency)
Downlink 2.4 Mbps, no uplink
Range: >35 km
Set-up connection time: 2 s
Latency: < 100 ms. No system-determined latency (i.e., direct communications). No random latency.

**MAC** (including real-time support, scalability, priority support, QoS)
Not applicable. Only one transmitter.

**Transmission modes** (directed, one- or two-way, broadcast, peer-to-peer)
Omni-directional
One-way (only downlink).
Broadcast
No peer-to-peer

**Requirements** (prerequisites or constraints, i.e., relies on GPS or communication infrastructure)
None, except the receiver.

**Interference** (intra- and inter-system)
Reserved frequencies. Coordination between countries required.

### 8.3.2 DVB-T and DVB-H

DVB-T is an abbreviation for Digital Video Broadcasting – Terrestrial. It is the DVB European-based consortium standard for the broadcast transmission of digital terrestrial television. This system transmits compressed digital audio, video and other data in an MPEG transport stream. DVB-T has been further developed into newer standards such as DVB-H (Personal Stations), with additional features to meet the specific requirements of personal stations, battery-powered receivers.

**Standard**
DVB-H was formally adopted as ETSI standard EN 302 304 in November 2004.

**Antenna**
Rooftop

**Frequency band**
DVB-H is designed to work in the following bands:
- VHF-III (170-230 MHz, or a portion of it)
- UHF-IV/V (470-862 MHz, or a portion of it)
- L (1.452-1.492 GHz)
DVB-H can coexist with DVB-T in the same multiplex.

**Channels** (number, size and separation, control channels, data channels)
A main service channel and a fast information channel. The main service channel can be divided into several audio and data sub-channels. Time-slicing is used.

**Output power** (including possible power control)
Power control not applicable.

**Data rate** (including range and latency)
Downlink 6750- 39270 Mbps, no uplink
Range: 16 – 67km
Set-up connection time:
Latency: 6 s. No system-determined latency (i.e., direct communications). No random latency.

**MAC** (including real-time support, scalability, priority support, QoS)
Not applicable. Only one transmitter.

**Transmission modes** (directed, one- or two-way, broadcast, peer-to-peer)
Omni-directional
Generally a one-way communication system – however DVB has standardized a number of return channels that work together with DVB-T to create bi-directional communication. RCS is
short for Return Channel Satellite, and specifies return channels with return bandwidth of up to 2 Mbps. DVB-RCT is short for Return Channel Terrestrial, specified by ETSI EN 301958.

**Broadcast**
No peer-to-peer

**Requirements** (prerequisites or constraints, i.e., relies on GPS or communication infrastructure)
None, except the receiver.

**Interference** (inter- and intra-system)
Reserved frequencies. Coordination between countries required.

### 8.3.3 GPS

The Global Positioning System (GPS) is the only fully functional Global Navigation Satellite System (GNSS) in the world. GPS uses a constellation of satellites that transmit precise microwave signals, which enable GPS receivers to determine their current location, the time, and their velocity (including direction). GPS was developed by the United States Department of Defense.

**Standard**
GPS standard.

**Antenna**
Rooftop

**Frequency band**
All satellites broadcast at the same two frequencies, 1.57542 GHz (L1 signal) and 1.2276 GHz (L2 signal).

**Channels** (number, size and separation, control channels, data channels)
Two frequency bands where transmitting satellites are distinguished using CDMA.

**Output power** (including possible power control)
Power control not applicable.

**Data rate** (including range and latency)
The data message is transmitted at 50 bits per second.

**MAC** (including real-time support, scalability, priority support, QoS)
CDMA. The receiver can distinguish the signals from different satellites because GPS uses a CDMA spread-spectrum technique where each satellite uses a different CDMA code. The receiver knows the codes for each satellite and can use this to reconstruct the actual data message.

**Transmission modes** (directed, one- or two-way, broadcast, peer-to-peer)
Omni-directional (from satellites)
One-way transmission system.
Broadcast
No peer-to-peer

**Requirements** (prerequisites or constraints, i.e., relies on GPS or communication infrastructure)
None, except the receiver.

**Interference** (inter- and intra-system)
Intra-system interference: Solar flares, metallic features in windshields such as defrosters, or car window tinting will reduce the GPS signal strength. Electromagnetic interference can also disrupt, or jam, GPS signals.
Inter-system: Reserved frequencies.
## 8.4 Carrier Performance Summary

<table>
<thead>
<tr>
<th>Standard</th>
<th>CEN DSRC</th>
<th>European 5.9 GHz ITS</th>
<th>WiFi</th>
<th>Infrared</th>
<th>WiMAX</th>
<th>GSM/GPRS</th>
<th>UMTS</th>
<th>DAB</th>
<th>DVB-T</th>
<th>DVB-H</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CEN EN 12253-2004</td>
<td>IEEE 802.11p</td>
<td>IEEE 802.11a/b/g</td>
<td>ISO21214</td>
<td>IEEE 802.16</td>
<td>GMS</td>
<td>3GPP</td>
<td>TS 102 427</td>
<td>TS 102 428</td>
<td>EN 302 304</td>
</tr>
<tr>
<td>Antenna</td>
<td>Rooftop</td>
<td>Rooftop</td>
<td>Rooftop</td>
<td>Directed</td>
<td>Rooftop MIMO</td>
<td>Rooftop</td>
<td>Rooftop</td>
<td>Rooftop</td>
<td>Rooftop</td>
<td>Rooftop</td>
</tr>
<tr>
<td>Range (m)</td>
<td>3-15</td>
<td>500</td>
<td>Access point coverage</td>
<td>1-100 (typical 7 m)</td>
<td>Access point coverage max 50k</td>
<td>Base station coverage</td>
<td>Base station coverage</td>
<td>&gt;35 km</td>
<td>16 – 67km</td>
<td></td>
</tr>
<tr>
<td>Latency (ms)</td>
<td>&lt;5 ms</td>
<td>5-12 ms</td>
<td>Implementation dependent</td>
<td>Ad-hoc</td>
<td>Implementation dependent</td>
<td>10 0.01</td>
<td>Implementation dependent</td>
<td>Hand-over</td>
<td>500-700 Hand-over</td>
<td>200-300 2.12 Hand-over</td>
</tr>
<tr>
<td>Priority QoS RT support</td>
<td>No</td>
<td>4 QoS classes. No real-time support.</td>
<td>Priority support No QoS or RT support</td>
<td>Once set-up RT is supported. 8 priority levels.</td>
<td>Yes. Although QoS depends on proximity to access point.</td>
<td>No</td>
<td>Yes. Although QoS depends on proximity to base station.</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Transmission modes: Directed, One-or two-way, Broadcast, Peer-to-peer</td>
<td>CEN DSRC</td>
<td>European 5.9 GHz ITS</td>
<td>WiFi</td>
<td>Infrared</td>
<td>WiMAX</td>
<td>GSM/GPRS</td>
<td>UMTS</td>
<td>DAB</td>
<td>DMB</td>
<td>DVB-T</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Requirements</td>
<td>RSU</td>
<td>None</td>
<td>Access point</td>
<td>Directed antenna</td>
<td>Access point</td>
<td>Base station</td>
<td>Base station</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Interference</td>
<td>European 5.9 GHz ITS WiFi 5 GHz</td>
<td>European 5.9 GHz ITS</td>
<td>Sun, rain, snow</td>
<td>Depends on frequency</td>
<td>Reserved frequencies</td>
<td>Reserved frequencies</td>
<td>Reserved frequencies</td>
<td>Reserved frequencies</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Within the ITS field, many applications of a diverse nature are considered and thus their communication requirements differ significantly. This makes it difficult for one wireless access technology to support all or even most of these applications. Traffic safety applications for example typically have requirements like high reliability, low latency, and real-time communications. Efficiency and comfort applications have more relaxed requirements on latency whereas ITS applications involving voice or video have lower requirements on reliability. Further, some applications may need more than one wireless access technology to fulfill their full functionality, whereas for other applications, more than one suitable technology could be recommended. Each access technology is typically developed for a particular purpose and as such they are best if used for this purpose. Data communication networks such as WiFi and WiMAX are developed for high rate internet applications and therefore usually provide high rate and high reliability but no real-time support. Telecommunication networks such as GSM/GPRS and UMTS are developed for voice applications and consequently provide low delay real-time support at the expense of reduced reliability. Digital broadcast systems such as DAB/DMB and DVB-T/DVB-H are developed to broadcast radio, TV or video and therefore have excellent support for broadcast, but limited or no support for two-way communications. Other radio systems such as CEN DSRC, the European 5.9 GHz ITS and Infrared are more application specific and thus if used in their intended context they provide high performance.

Few, if any of the current wireless access technologies can support high reliability, low latency real-time communications since typically reliability is increased with increased delay (e.g. using retransmissions).
8.5 **ITS Spectrum**

**Figure 18: ITS Spectrum Overview**

- **Common Control Channel, Broadcast data, 10MHz@5900 (ch180) (Used by all)**
- **Service Channel: GeoRoute multihopping, 10MHz@5880 (ch176) (Safespot/C2C-CC)**
- **Aux Channel for roadside initiated data, 20MHz @5480+ (ch96) (CVIS/COOPERS)**
- **Vehicle-Roadside data, 10MHz@5890 (ch178) (Safespot/C2C-CC, not used initially)**

**Blue line represent European spectrum mask for BRAN (conditional use for ITS)**

**Red line represents European spectrum mask for ITS 5.9**

83 of 165
9 Networking and Transport

This chapter introduces the communication protocols with a focus on Network and Transport block in the ITS Station Reference Architecture. This and the detail of the Network and Transport block are shown in figure 30.

First some media specific communication protocols are described, and then CALM (Communications Architecture for Land Mobiles) is explained. CALM is a set of international standards for ITS communication developed by ISO TC204 (ITS) WG16. Finally some central functions for safety communications are addressed in some detail.

Further details are shown in Figure 19.

The main function blocks are as follows:

- TCP/UDP is the classical set of Internet Transport Protocols for acknowledged and unacknowledged communication. These protocols are standardised by Internet Engineering Task Force (IETF).

- IPv6 is the new Internet Protocol that needs to be used for ITS. This will facilitate Internet connectivity also in highly mobile environments. To help on that, certain new additions from the IETF working groups NEMO and MONAMI has been standardised and collated by the new IETF group for mobility extensions MEXT.

- ITS Transport is being defined to support integrity of data transfers in the hostile environment of fast moving cars. This work is underway in several groups and organisations at time of writing this document.

- ITS Network is a catch-all grouping for many ITS functions that will use ITS-specific media, in particular 5.9 GHz operation that to a large extent will be broadcast based. Some of the main tasks will be related to bundling and unbundling broadcast/multicasts, and congestion reduction on a frame-by-frame basis.
• GeoRouting is a specific ITS protocols to create mobile networks based on geolocations. More details will follow later in this chapter and the standards are being developed in ETSI TC ITS.

• Other Protocols are explicitly mentioned. There are some that will be developed relatively soon: An intelligent handover service between multiple roadside stations (Homogenous Horizontal Handover). Also route optimized vertical handovers with heterogeneous medias will likely need new protocol development soon.

9.1 Media-specific Communication Protocols

DAB-specific communication: TPEG

DAB stands for Digital Audio Broadcast and was initially intended to supersede analogue FM/AM radio broadcasts. The protocol stack of DAB consists of a physical layer, which deals with the transmission of digital data over the air and an application layer which specifies the content encoding. The properties of the physical layer are described in chapter 8 and are not covered here.

In the DAB multiplex, several services are grouped together in a single ensemble, and each service may be composed of different service components. The essential component of a service is called the primary service component. This is typically audio, but may also be data, e.g. TPEG stream. In addition, the service may be augmented by optional secondary service components.

The DAB service structure allows for efficient and flexible use of resources by allowing components to be shared among several services. For example, traffic information in the traffic message channel or service information may be two secondary service components. This also allows for services to change the set of components at different program times.

In respect to its usage in ITS where DAB is used to broadcast messages from the TCC to the vehicle, it is important to note that DAB does not provide 100% reliable communication on application layer. This is where the TPEG protocol comes in. The TPEG binary format (used for over-the-air transmissions) has been designed such that it adds additional redundancy to allow for a reliable message transmission.

Note that DAB as a broadcast medium ideally supports transmission of the carousel of TPEG messages.

GSM-specific communication: GPRS and TCP/IP

GPRS is an overlay on top of the GSM physical layer and network entities. It extends data capabilities of GSM and provides connection to external packet data networks through the GSM infrastructure with short access time to the network for independent short packets. The properties of the physical layer are described in chapter 8 and are not covered here.

Compared to the regular GSM network for voice calls, the GPRS network needs some additional components. One of them is the GPRS Support Node (GSN). It is responsible for packet switching, acts as a gateway to the data networks and also handles mobility management (mobile handover). These functions are distributed on two sub-systems. The Gateway GPRS Support Node (GGSN) acts as the gateway. The Serving GPRS Support Node (SGSN) is responsible for mobility management. Every mobile user is dynamically assigned a temporary address, which allows the SGSN to identify the user during mobility management.

The external data network is usually a public data network (PDN) like the internet, access to which is provided by an ISP. This means the GPRS user has access to the internet.
Regarding the data flow in a GPRS network two types of information are distinguished: payload data and signalling. Payload data are transmitted directly between the Base Station Controller (BSC) and the GPRS Support Node (GSN). Signalling is transmitted via Mobile Switching Center (MSC).

GPRS networks are covered in detail in [GPRS01] and [GPRS02].

When TCP/IP is used, each phone can have one or more IP addresses allocated. GPRS will store and forward the IP packets to the phone during cell handover (when you move from one cell to another).

As GPRS is packet based, a radio noise induced pause can be interpreted by TCP as packet loss, and cause a temporary throttling in transmission speed.

There are some experimental implementations of IPv6 over GPRS, but this is not yet commercially available. To traverse GPRS with IPv6 the recommended solution is to use L2TP which is a tunnelling solution to transport any layer 2 protocol over an IPv4 service.

From the communication point of view, the main advantages of GPRS in a mobile environment are:

- bidirectional communication
- large coverage (temporal and spatial)
- comparative simple antenna design
- cheap and readily available components

A drawback of GPRS is that it is sensitive to data volume. That is bandwidth is quite small and additionally GPRS service is commonly charged by data volume.

### 9.2 CALM

It is clear that the CALM architecture has many similarities to the COMeSafety architecture. In many ways the CALM architecture is a precursor to the newer ETSI TC ITS/COMeSafety architecture. The new elements include security support, fully defined application and facility support, and much improved traffic safety communications.

It is strongly suggested to feed the results of the European process back into CALM again since this is a way to help the global marketplace function in a better way by bringing down technology barriers between the different regions. It will also help safety for travellers since the personal stations/nomadic devices could be used anywhere in the world in a similar fashion as RDS TMC is functioning in cars today. Note that it is very likely that such devices will be widespread within a few years from now.

Please also note that ISO TC204 WG16 has strong links to other standardisation bodies such as IEEE802.11, IETF, ETSI and others. This will hopefully facilitate a rapid take-up of the European concepts to the wider audience.

Some of the basic ideas are:

- seamless communication (cooperative concept)
- support of multiple media
- future proof (adaptable to latest communication technologies)
- applications are independent of communications
9.2.1 Architecture

An overall view of the CALM layer architecture is illustrated in Figure 20 below. It shows the CALM layers in relation to the OSI reference model together with the Service Access Points (SAPs).

There are four major blocks:

1. The Application block provides a common API to applications that want to communicate using CALM.
2. The Network block creates a relation between applications and communication media, isolating the upper OSI layers from the different technologies which actually perform communication.
3. The Physical/Link block contains the different physical interfaces. It can contain several native CALM interfaces (CALM-IR, CALM-M5) or physical interfaces which have not been specifically been developed for CALM..
4. Finally the CALM management block resides outside of the communication stack and provides management functions.

SAPs define the interfaces between the individual blocks of the CALM architecture.

Within the communication stack the T-SAP connects the Application layer with the Network layer. The T-SAP provides the Application layer with a unified interface which allows a CALM service to address a specific CALM service at a remote node. Using the T-SAP the following operations are supported:

- creation of a socket
- deletion of a socket
- transmission of a packet
- confirmation for a transmitted packet
- reception of a packet

At the heart of a CALM communication unit is the CALM communication kernel, which is shown in Figure 21.
A CALM unit which only implements the CALM Communications Kernel (without the CALM service layer block) is called a CALM router. A CALM host additionally implements the CALM service layer.

The CALM service layer can be used by CALM FAST, CALM IP-based and even Non-CALM-aware applications.

Figure 21 above shows that the CALM network layer actually is not limited to a single protocol. It can be made up by one of the presented network protocols: CALM-FAST, Georouting, IPv6 or any other networking protocol.

The CALM CI layer comprises wireless and wired communication interfaces, which can be amongst others 2G/3G cellular, CALM-IR, CALM-M5, CALM-MM or for instance Ethernet.

### 9.2.2 Management

This section deals with some of the most important aspects of CALM management.

A key feature is the concept of virtual communication interfaces (VCIs). A VCI is an instance of a real CI. For each VCI CALM management maintains a set of parameters for physical layer and MAC layer of the corresponding CI. In regard to the direction of communication (transmission or reception) there are two kinds of VCIs: transmit VCIs (TX-VCI) and receive VCIs (RX-VCI). Each TX-VCI has its own set of parameters, whereas all RX-VCIs of a common CI share their receive parameters. VCIs can also be distinguished based on the mode of
communication. If applicable a Broadcast-VCI is always available. For communication with a single peer, a Unicast-VCI (UC-VCI), which creates a relation to exactly one peer station must be used. The remote peer is identified by its MAC address.

Another interesting facet of CALM is route selection management. CALM employs multiple media each of which has specific communication properties. “In order to decide which is the most appropriate communication interface to provide a communication service the route selection manager needs to know what the communication needs of the user application are, what communication interfaces are available, what the properties and statuses of these communication interfaces are, and what the requested policies are.” Figure 22 shows a schematic representation of route selection management.

![Route Selection by CALM Management](image)

The set of rules is partly pre-defined, partly configurable. It represents the part of the route selection process which is controllable by the user (human). CALM services (applications) access the CALM Management via A-SAP, which allows to request a certain communication functionality and performance. This process results in the “User application requirement list”. The third input for route selection comes from the CALM CIs via M-SAP. Through this interface the CI announces its communication functionality and performance. This process results in a CI/VCI status list. Output of the route selection process is the selected route respective CI/VCI. According to that selection the CALM forwarding tables in the network layer are updated. This is achieved via the N-SAP.

Route selection management is described in detail in ISO 24102 CALM management standard.

### 9.2.3 Groupcasting

Groupcast communications stands for

- Broadcast communications which is the distribution of information to all listeners
- Multicast communications which is the distribution of information to a predefined multicast group.
Three types of groupcasts can be differentiated: groupcasts that are periodic, event driven or repetitive event driven. There are several different sources of groupcast transmissions. They are described in the following.

A CALM service can initiate a groupcast to
- disseminate LDM (Local Dynamic Map) data
- advertise service information (as described in section 9.2.4)
- forward data

For this purpose the CALM Service uses the “Groupcasting Registration Handler” in the CALM Service Layer.
- A networking protocol can request a groupcast transmission to
  - forward data to a group of listeners
  - send out beacon data
  - disseminate other groupcast data specific to that networking protocol

CALM management can trigger a groupcast to
- transmit CI management data
- transmit CALM management data
- transmit beacon data

Figure 23: CALM Groupcasting
Finally the MAC layer of a CI can request a groupcast to publish medium specific MAC management data.

Before a request for a periodic groupcast transmission is submitted to the corresponding CALM CI, the ITS-MUX is used to process it.

ITS-MUX is a virtual network protocol which was designed to minimize the load in the wireless link by mapping as many as possible groupcast transmission requests onto a single frame.

If the implementation of the CCK (CALM Communication Kernel) consists of a single networking protocol, then the ITS-MUX simply forwards data packets between that networking protocol and the C-SAP. The overall groupcasting architecture is shown in Figure 23.

### 9.2.4 Frame flow

The following shows one example of signal sequence diagram showing service discovery and initialisation. Note that this example does not include the Cooperative Awareness Message concept. The frame flow in CALM-FAST communication takes place in two phases. Figure 24 and Figure 25 illustrate the communication flow.

![Figure 24: Service Provision using SAF and SCF](image)

In the service initialization phase the service provider (typically CALM master) announces to the service user which services are available. This is performed by so called Service Advertisement Frame (SAF).

From that point two scenarios have to be distinguished. In the first case the service initialization phase is concluded with the Service User subscribing to a list of services (typically a subset of available services). This is performed by so called Service Context Frame (SCF). Next the operation phase starts. Within operation phase communication takes place in pairs of request/response messages. The service provider sends out a request to the service user, which sends back a response. This process is repeated until service transmission is finished.

Alternatively it's possible to implement the communication flow such that the service announcement is not acknowledged by a SCF. In this case the service operation phase starts immediately after SAF. Now the direction of the request/response messages is inverted. The service user interested in a particular service sends out a request to which the Service Provider sends back a response in the context of the requested service. This process is repeated until all service transmissions are finished.

The service operation phase is optional.
9.3 **Infrastructure controlled protocols**

The main information flow is from the infrastructure to the vehicle. A central unit – the TCC (traffic control center) – deploys messages to vehicles using different communication media (DAB, GRPS, CALM-IR, CALM-M5, WiMax, DVB-H / DVB-T).

However some essential information is transmitted from the vehicle to the TCC. This is floating car data and a message acknowledgement for specific services. For this purpose communication media which support bidirectional communication are needed.

### 9.3.1 GPRS Communication Scenario

![GPRS Communication Scenario Diagram]

Figure 26: TCC to Vehicle Link via GPRS
Figure 26 illustrates the communications links which are involved when a service is transmitted via GPRS. The units GGSN, SGSN, BSC, BS are part of the providers 2.5G cellular network (GPRS network). Please refer to [GPRS1] for a detailed description of GPRS networks.

### 9.3.2 CALM-IR Communication Scenario

Figure 27 illustrates the communication link between TCC and vehicle.

![Diagram: TCC to Vehicle Link via CALM](image)

**Figure 27: TCC to Vehicle Link via CALM**

The TCC deploys TPEG-ML messages of the different services to the Communications Router (CCR). The CCR manages an internal message database of TPEG-ml messages and transforms the TPEG-ml messages to TPEG-rtm for transmission using the CALM-IR Transceiver (CIRT) to the vehicle. Once a vehicle enters an IR communication zone (passes a motorway gantry equipped with the CALM-IR Transceiver) the CIRT announces to the vehicle which services are available. The CALM Communication Gateway (CGW) in the vehicle can then subscribe to individual services. After that the CIRT transmits the requested service messages to the CGW. If the service requires a message acknowledgement from the receiver, the CGW immediately sends an acknowledgement. The CGW forwards the message to the Automotive PC, which is responsible to decode the TPEG-rtm message to TPEG-ML.

### 9.4 The VANET message frame structure

The goal for designing the frame structure for ITS communications is to comply with the European ITS communication reference architecture, which is based on the OSI model, and to find a harmonised solution for Europe and USA.

Applying the OSI model enables flexible usage of the communication facilities in an ITS station. At the same time, strictly speaking, ITS designs optimized for a single application / single communication medium need to be modified slightly in order to fit to the European ITS communication reference architecture. As a preliminary remark the ITS road Safety Channel usage is presented,

**ITS road safety Channel usage**

Road safety applications are designed to operate in the 5.9 GHz. range (see chapter 8 on Access Technologies). It is suggested to divide this frequency into 3 channels with 10 MHz bandwidth each and to use one channel as a control channel (CCH), one as a first service channel SCH1 and an additional channel as a second service channel SCH2.
Physical channels are automatically assigned based on the application class and priority of a message. It is assumed that messages on the CCH and SCH1 can be received in parallel, i.e. at least two receivers are required. If the channel load on the CCH is low, all messages could be redirected to the control channel. Five priority levels are defined: PRI\textsubscript{Emergency}, PRI\textsubscript{VANET}, PRI\textsubscript{High}, PRI\textsubscript{Mid} and PRI\textsubscript{Low}. Regarding Multihop and Geocast communication it is assumed that only the 1\textsuperscript{st} hop can have the priority PRI\textsubscript{Emergency}. It is assumed that these priority levels are associated with the application classes, but when communicating in geocast or multihop mode this describes only the communication priority on the first hop and the VANET router may reduce this priority on subsequent hops or repetitions.

The following channel usage scheme is proposed.

- **CCH**: optimized for low latency
  - Network layer beacons (PRI\textsubscript{VANET})
  - 1-hop broadcast high priority safety messages (PRI\textsubscript{Emergency})
  - 1st hop of high priority Multihop/Geocast Messages (PRI\textsubscript{High})

- **SCH1**: optimized for high throughput
  - Safety Messages (PRI\textsubscript{Mid}, PRI\textsubscript{Low})
  - Multihop Messages (≥ 2nd hop)
  - Geocast Messages (≥ 2nd hop)

- **SCH2**: optimized for peer-to-peer communication (PRI\textsubscript{High}, PRI\textsubscript{Mid}, PRI\textsubscript{Low})
  - reserved for short distance peer-to-peer communication at reduced power level (currently unused in SAFESPOT)

### 9.4.1 Lower layer frame structure

The physical layer (PHY) and medium access control sub-layer (MAC) functionality of the European 5GHz radio are standardised at ETSI ITS WG4. However this standard depends on the European ITS communication reference architecture and has to be built on some assumptions on the logical link control sub-layer (LLC) and upper layers specifications.

The format of a frame is illustrated with the sequence of the following figures.

The PHY frame consists of a PHY header, the MAC frame and an optional PHY trailer. The PHY header and the PHY trailer shall be as specified in IEEE 802.11 for "orthogonal frequency division multiplexing (OFDM) PHY specification for the 5 GHz band". Details of the MAC frame shall be as follows:

<table>
<thead>
<tr>
<th>PHY Header</th>
<th>MAC Frame</th>
<th>PHY Trailer</th>
</tr>
</thead>
</table>

**Figure 28: PHY Frame**

The MAC frame consists of a MAC header, an LLC protocol data unit (PDU) and a frame check sequence (FCS) used to detect transmission errors.
The LLC PDU consists of a one octet destination service access point (DSAP) address field and a one octet source service access point (SSAP) address field, an LLC header and a network protocol data unit (NPDU). The LLC header shall be compliant with IEEE 802.2, as required in the overall IEEE 5.9 GHz related protocol suite and ISO CALM. This choice is not restricting the implementation and operation of ITS applications in any way and does not add unnecessary complexity.

The NPDU consist of an optional ACT parameter (ACTP) header, a network header and the transport layer protocol data unit (TPDU). The optional presence of an ACTP header allows to set PHY, MAC and LLC parameters in the radio prior to transmission of the frame, and to report PHY, MAC and LLC parameter settings of the radio receiver related to the packet received. Presence of the ACTP header in the frame may be indicated in the LLC header, without restricting the functionality of 802.2.

The network header is characterized by a sequence of Protocol Elements partly mandatory and partly optional.

The mandatory part is the protocol identification and Net Header which includes the station identifier and the key geographical information of the station (position, speed).

The other protocol elements are optional and used for non all the non-broadcast addressing (Destination) and the multi-hop transmission (Forwarder). Moreover a security element may be added.

The Net Header also carries a number of conditionally optional information elements:

- The *Destination* information element is used to specify the network layer routing destination node. This element is not yet specified.
• The *Forwarding* information element is optionally used in case the station is forwarding a message and is used to specify the most recent network layer routing forwarder node. This element is not yet specified.

• The *Security* information element is used to specify routing security related information and credentials such as message signatures. This element is not yet specified in detail. The security technologies and strategies are explained in the dedicated Chapter 11.

Here in the following an introduction is reported and some networking mechanisms for multi-hop and geo-broadcasting, while the TPDU is described in section 10.4 in order to provide a unified view of the content.

### 9.4.2 Networking Mechanism for the VANET Communication

Decision was taken to make network layer (NL) beacons equivalent to the Cooperative Awareness Messages. According to current agreement, by default they are emitted twice per second. These NL beacons are transmitted in single hop mode, i.e. they are not forwarded.

The NL beacons can carry additional application data, but the applications are not allowed to change the time schedule of NL beacons. This can only be done according to the congestion control policies.

The beacon, sent by default at 2 Hz frequency, has the format defined in chapter 10.

The header contains node ID, position and speed and other fields that are relevant for the VANET functionality. The fixed payload depends on the role of the station and contains other node information, e.g. the vehicle size. The variable payload is inserted only if requested by the applications and if authorized by the congestion control. A further option is the addition of satellite raw data sent at the frequency of 1 Hz (every 2nd beacon) to support high accuracy relative positioning.

#### Generic Message Format

Other messages that are transmitted in single-hop mode will have a header, variable payload and a security field, e.g. certificate and signature.

![Network Header Table](image)

<table>
<thead>
<tr>
<th>Network Header</th>
<th>Destination Description</th>
<th>Originator Payload</th>
<th>Originator Security</th>
<th>Forwarder Header</th>
<th>Forwarder Payload</th>
<th>Forwarder Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geocast Section</td>
<td>Originator Section</td>
<td>Forwarder</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Forwarders of the message add or replace the forwarder section, such that only information of the originator and the last forwarder are visible to the recipients. Both sections are secured separately.

The messages different from the beacon could use geo-addressing or broadcast and could be single-shot or periodic with a period established by the applications. The period can be reduced in case of network congestion.

When receiving a geocast message a node determines if the message should be re-broadcasted (geo-broadcast, e.g. simple flooding) or transmitted to an appropriate next forwarder (geo-anycast, multihop). Very efficient routing algorithms for selecting the next forwarder, e.g. GPSR-MA (Greedy Forwarding) and MORA (Movement Based Routing Algorithm) have been specified and are under development.

It must be noted that all geocast retransmissions will compete with the other messages in the transmit message queue(s). They are part of the congestion control algorithms. The congestion control may lower the priority, delay a re-transmission or redirect the messages to another channel.
9.4.3 Geobroadcast

Communication Modes

Many applications rely on location based message distribution. For that purpose a message is distributed in single-hop mode or in geo-cast mode.

Only nodes in direct communication range receive a single-hop message. Single-hop communication is used to transmit Network Layer (NL) Beacons that establish the Cooperative Awareness. If the expected communication range in single-hop mode is too small to cover the destination area where a safety message is relevant, the applications may use the geo-broadcast functionalities.

A destination area is specified as an ellipse. In its simplest form the message originator’s position \(P_{\text{Orig}}\) and a destination point \(P_{\text{Dest}}\) form the focal points of the ellipse.

By default the small semi axis is selected as the expected communication range, but a more general ellipse can be specified using a shape factor \(\alpha\). A position relevance function \(\Gamma_{\text{Ellipse}}(x,y)\) defines a metric \(\Gamma_{\text{Ellipse}}\) for the destination area that is positive inside the destination area and negative outside. The maximum value 1.0 is achieved in the centre of the ellipse.

**Geo-Address and Geo-Broadcast**

A geo-address is equivalent to the destination area and the relevance function. It is specified with ~8 Bytes, having \(P_{\text{Dest}}\) relative to the originator’s position.

If the originator at \(P_{\text{Orig}}\) transmits a geo-broadcast message (having specified the geo-address) all vehicles inside the destination area that receives the message repeats this message exactly once. Vehicles outside the destination area simply drop the message. More advanced geo-broadcast functionalities will be available in future.

**Stored Geo-Broadcast**

In sparsely populated traffic scenarios not all vehicles will be reached by a single simple geo-broadcast transmission. With stored geo-broadcast the originator specifies a lifetime of that message and a message repetition is initiated.

Currently only the originator node itself or a directly addressed roadside unit are allowed to perform these repeated simple stored geo-broadcast transmissions.

---

\(^2\) If multiple geographic objects (road segments) should be used as the destination area the ellipse is specified as the convex hull and an additional filtering on application level is required.

\(^3\) Ellipse: Semi axes \(a\) (large) \(b\), focal value \(f\), shape \(\alpha = a/f\), relevance \(\Gamma_{\text{Ellipse}}(x,y) = 1-(x/a)^2-(x/b)^2\)
Line Forwarding
If the originator is outside the destination area, line forwarding mechanisms are used to transport the information into the destination area (Multihop)

9.4.4 Congestion Control

The objective of congestion control (CC) is to best exploit the available network resources while preventing sustained overloads of network nodes and links. Appropriate congestion control mechanisms are essential to maintain the efficient operation of a network system. The congestion indicators are the size of the neighbour table, the number of retransmissions "heard", the message transmission delay, the size of the messages stack, etc. Ensuring congestion control within vehicular ad hoc networks should address special challenges and issues, due to the characteristic and specificities of such environments (High dynamic and mobility of nodes, high rate of topology changes, high variability in nodes density and neighbourhood, broadcast/geocast communication nature ...).

The conception of a congestion control approach within VANETs should ensure the following objectives. First, the CC approach should be dynamically adaptable to the context of VANETs, while taking into account the required Quality of Service (QoS) metrics (in terms of reliability and delays). In addition, to take into account relay nodes, and in order to manipulate sending queues, CC should be a cross-layered hop-by-hop approach. And finally, no additional equipments are required, or bandwidth consumption due to communication overhead could be generated.

We present in the following the basic policies of the congestion control approach within VANETs, considered in the SAFESPOT project:

Priorities assignment
For each message a priority is evaluated. The priority is composed of 2 fields: the first is static, deduced from the application type, and the second is dynamic, obtained from the specific context of the VANET (vehicles density, variance of the mean speed of the neighbourhood,). The dynamic and the static fields are combined to obtain the overall priority indicator.

The Dynamic factor takes into account of:

- The node speed, according to the covered zone at each dt. The priority of a message increases when the speed of the sender increases.
- The utility of the sent message, according to the number of its retransmissions in the case of periodic or geocast messages.
- The message size. The priority of a message decreases when its size exceeds a defined threshold.
- The message validity (maximum duration of the message). As for the EDF scheduling approach (Earliest Deadline First), the message whose deadline is earliest, holds the biggest priority.

Messages scheduling and transmission
Each node schedules its messages stack, in order to send packets according to their priorities. Moreover, two messages queues are considered, one for each transmission channel (CCH and SCH1). Note that sending higher priorities packets (via the control channel) is pre-emptive, compared to lower priorities packets via control or service channels. Finally, the maximum duration of a transmission and the maximum number of transmissions per time interval are
defined, and could not be exceeded, except by \( \text{PRI}_{\text{Emergency}} \) messages that are emitted on an event basis.

### 9.4.5 A design example: the SAFESPOT Router

The SAFESPOT Router is designed in order to interact with the vehicle or RSU based Safety applications, the local dynamic map and other SAFESPOT nodes.

![Diagram of SAFESPOT Router](image)

The main specific router characteristics are periodical beacons, payload update and geocast functionalities.

The routers periodically send out beacons. The beacon transmission is functional to the maintenance of the network, due to the mobility of the nodes and therefore it is done automatically, without any request from the applications. A beacon can have additional application data piggy-back. The router is capable either to directly send the (static) payload or — if it is requested by the applications — to fill the content of the payload dynamically just before transmitting with updated data from the LDM. Otherwise a message that is delayed by the congestion control would contain old values. This update service is very useful for those vehicle physical parameters that are changing continuously, e.g., position and speed.

The router support geo-cast functionalities, mainly geo-broadcast, geo-anycast ang geo-unicast via multi-hop communication.

#### Communication Types

Two kinds of messages can be identified: messages exchanged with the applications and messages exchanged among the routers. The Message Manager is the instrument by means of which the applications drive the router providing the parameters of the message that must be sent. Mainly:

- The kind of message (Event, Emergency, Periodic, HMI)
- The priority of the message
- The addressing (Unicast, Broadcast, Geo-unicast, Geo-broadcast)
- The payload
  - Static payload \( \rightarrow \) treated as a black box by the router
  - Dynamic payload \( \rightarrow \) only the kind of data in the payload are specified: the router fills the payload, downloading updated values, just before the transmission of the message

Moreover all the application can add additional fields in the beacon through a tagged list. The router can send on the communication channels two kinds of messages:

- Beacon/extended beacon
- Generic message

#### Receiving a message

For most of the time the VANET router will be in Receive Mode. On message reception the router performs the following actions:

- Reception of a Beacon
  - The VANET neighbor table is updated. This table only contains the most recent beacon header information of the direct neighbors.
  - The satellite data (if available) is passed to the positioning subsystem
• The beacon information (without satellite data) is passed to the SAFESPOT platform such that after data fusion the objects of the LDM are also updated.

• Reception of a Single-Hop Message
  o same as for beacon reception, but update of the VANET neighbor table is optional

• Reception of a Multihop / Geocast Message (Generic Message Format)
  o Message duplicates are dropped
  o If the node is outside the destination area – this is detected by a relevance check based on the geo-address and the own position – the message is dropped
  o Otherwise the message is passed to the SAFESPOT platform (for updating the LDM objects) and the VANET router process this message according the multihop / geocast rules.
10 Facilities

The content of this chapter is devoted to outline the data Communication part related to facilities in the ITS Station Reference Architecture. It also includes a description of the data flow from applications and the structure of the main Message. The most important message is the "Cooperative Awareness Message" which is the heartbeat of the network and is the carrier of the basic information used by applications. The most significant data to be exchanged are described and a general Transport Protocol Data Unit structure is defined. This TPDU has been designed in order to allow to send in a single packet block of data related to different classes of applications (Safety, Efficiency, Value Added Services). Also the structure try to harmonize an existing standard (IEEE1609) and the structure proposed in European activities (C2C, SAFESPOT, ETSI WG). The facilities include a common geo-referenced repository named Local Dynamic Map (LDM) storing dynamic and static data and making them available through standard APIs to applications.

Figure 33: ITS Station Reference Architecture: Facilities

In a previous chapter applications examples were presented. Recalling the ITS Station Reference Architecture diagram, the focus of this chapter is to describe the fundamental data flowing from the relevant stations of the co-operative network. The stations of the network may be classified as moving (vehicles and/or personal stations) and static (road side Units and/or Central Units). Different communication channels may be available in order to exchange data. In this chapter we focus the VANET (Vehicle Ad Hoc NETwork) using as basic protocol IEEE802.11p in the 5.9GHz band.

The “user services / applications” decide which data and at what time they should be transmitted on the network based on the specific application scenario. The effective transmission is then regulated by the network management (NME) which should ensure the optimal congestion control of the network itself.

Certain critical data like time, position and ID are useful to the network maintenance and are consequently automatically sent by the networking layer in the beacon message header (see chapter 9). The heartbeat of the network is the “Network Layer Beacon Message”, transmitted by each station at a fixed frequency which can be only modified by the network “congestion control”. COMeSAFETY assumed according to the current proposal in C2C to use the
Cooperative Awareness Message (CAM) as replacement of the “Network Layer Beacon Message” for all the Stations participating to the Road Safety Application Data are organized according to a set of messages and formats which are described in the Annex 10-1 “Message Catalogue”.

Applications are classified as “Road Safety”, Traffic Efficiency” and “Other Applications”. These three categories have different requirements in terms of latency and geographical coverage. The main focuses of these three application areas are:

- Road safety, local area, low latency, Wireless 5.9 GHz.
- “Traffic efficiency”, Medium range and some latency acceptable, support to “Road Safety for long range coverage,”
- “Other applications” or “value added services”, medium – long latency accepted, all Wireless media + global network.

The Facilities function block is essential in the understanding of both how an ITS system works, and how an ITS Station is implemented.

The roles of these three functions are:

- **Application support** is the kernel of the middleware. This may consist of lifecycle management of the station, automatic discovery, download and initialisation of new services, HMI capabilities, and many others. For a more formal approach please see OSI reference model for Layer 7.

- **Information support** will manage data. In any ITS system, there will be an abundance of data sources; both mobile and static. This data will mostly be location specific and data elements should therefore be location referenced. In addition the data will be dynamic in nature: the information will change over time. Therefore the data needs to be time stamped and have some kind of validity attached to it. Finally the data will have a certain level of trust. This relates both to the accuracy, and reliability of the data. The data therefore needs to include both accuracy parameters and a cryptographic signature. Combining or Fusing data from different sources and keeping the information up to date is one of the challenges of Information Support, and very different solutions at implementation level are possible. Here in the following we will illustrate the Local Dynamic Map concept, that is a layered, geo-referenced data base containing all the relevant information needed by applications. Information Support takes on many of the OSI Presentation Layer functions.

- **Session support** will create and maintain a link between entities (Stations) that need a link. For some implementations focusing on low-latency applications like Road Safety, the session is pre-defined so that a link between the critical application and the used interface (5.9GHz) is established at power-on. For other scenarios e.g. in CVIS and COOPERS, the applications can require a link at any point, and the Session Support will establish a link through the best available physical interface. This function will also make sure that the link is kept available, or re-establish the link if all connectivity has been broken.

Note that these functions are always present in any station implementation, but they may be rudimentary and statically implemented depending on the usage scenario.

Figure 34 illustrates some typical SAFETY scenarios and the related data flow. **V1 is a sliding vehicle** which is able to send this information to **RSU1** placed there probably because that is a typical critical area for ice or other low friction situations. The information flows (Blue arrows) from the receiving station to a **variable message sign (VMS)**, to other near stations or even to a control center. The receiving RSUs are able to transmit the information to the vehicle running close to them. A selection may be done while transmitting in order to address only the vehicles which could be interested in the information. For this purpose the **geo-addressing**
mechanisms is available at communication level or filtering may be operated at application level.

Figure 34: Examples of Road Safety Scenarios

A similar path is followed by the information of a tilted motorbike. The information may be directly transmitted by the motorbike (if equipped with the cooperative system) and/or by a detecting vehicle (equipped with environmental perception devices – e.g. Laserscanners, cameras). Following the brown arrows it is possible to understand that V3 is not interested in the tilted motorbike info but it participates to the network forwarding the info to V2 which is interested. **V3 is operating as a router.** Finally a third situation, a traffic light equipped intersection, is represented. RSU3 is operating in synergy with RSU4 and may provide information and/or intervene on the traffic lights.

To completely cover the scenarios reported in Figure 34, both the wireless and the wired network are operating. The latency should be clearly low in order that the system information is usable with efficacy.

The relevant information are above all the position, dynamic parameters of the vehicles, the status of on-board equipments/sensors (e.g. Brake, ESC, tilt, sensor).

In order to extend the scenario to other applications/services it should be considered additional lower priority information, using the same network or parallel channel which provide contents for Traffic efficiency (e.g. traffic jam info or suggested route) and/or added value services (e.g. advertising or tourist info).

Figure 34 is a specific example of the more general connection scheme as represented in Figure 35. Vehicle and RSU contain basic elements (Router, Host, Gateway) which allow a connection to the global network.

The data flow from any element is clearly bi-directional.

For the Host computer an internal architecture including the Local Dynamic Map (LDM), a multilayered Data base containing all the relevant information provided by the on board sensors and the communication network has been developed and adopted. This LDM belongs...
to the Information Support function block, but is usually implemented very closely together with the applications because of the stringent performance requirements.

**10.1 Local Dynamic Map (LDM)**

Concept

![Figure 35: General Connection Scheme](image)

![Figure 36: LDM Concepts Illustration](image)
A cooperative system for safety critical applications will benefit from using a digital map. This map should include lane-specific information including curbs, pedestrian walking, bicycle paths and road furniture such as traffic signs and traffic lights. Furthermore all dynamic objects that are directly sensed or which presence is indicated by other road users (cooperative awareness) should have a reference to the digital map. As a consequence, large numbers of objects need to be stored and maintained in this Local Dynamic Map (LDM). This is shown in Figure 36.

Due to the physical nature of these objects, spatial queries are used to determine object dependencies and relationships. In order to determine whether a vehicle is in an area with ice on the road or aqua-planning, the request needs to be setup whether the vehicle is in that area or possibly approaching it. In order to get the information about pedestrians, animals or cyclists a query needs to be made in a bounding box area around the vehicle. Because of this, the Local Dynamic Map is considered as a spatial database that allows spatial queries.

Scenario Analyses

Scenario analyses based on the contents of the LDM figure out if the own vehicle takes part in specific driving scenario where some support can be given to the driver, e.g. the left/right turn assistant, safety margin assistant etc. In case of a potential dangerous situation a warning is issued to the driver. This scenario analyses target at the vehicle’s HMI.

But a potential dangerous situation for the own vehicle can be harmless or completely irrelevant for other vehicles. Therefore additional scenario analyses target at the communication to other stations. This cooperative part of the applications – the message manager – extracts the information of the LDM that has the highest relevance to other stations. When transmitting this information the other vehicles are enabled to complement their LDM and to improve the HMI scenario analyses.

LDM and Communication System

Predefined messages in particular the Beacons establish the cooperative awareness. The Beacon information is directly extracted from the LDM, including station information, position and speed. The LDM also decouples positioning sensor (GPS) rate from the NL Beacon rate by using interpolation or prediction, especially for the own vehicle, the EGO object.

Due to the restricted communication channel bandwidth the message manager may choose to communicate already aggregated information instead of raw sensor data.

In case that the cooperative scenario analyses detects a dangerous situation for another vehicle, an event message is generated that is transmitted with high priority and low latency.

10.2 The VANET messages

The data to be exchanged among stations have a double function:

- to maintain the communications network in an optimum way (facilitating routing and congestion control)
- to support the high level applications

For both needs the Cooperative Awareness Message (CAM) has been defined in order to ensure “the network survival and a minimum of information used by the applications, specifically providing the “cooperative awareness” to the stations participating to the network. Currently the repetition frequency has been set at 2 Hz.

COMeSAFETY defined also other messages to be exchanged on the VANET:
- Decentralized Environmental Notification Message (DENM)
10.3 The common relevant information exchanged through the VANET

For the cooperative systems the relevant data are the geographical position together with dynamic and status parameters. The mandatory header information has a part common to Vehicles and RSU and a part which is different for the two types of stations.

The Common part (header) includes

- **Identity** of the station for reference purposes. This identity may be static for e.g. RSU, or dynamic pseudonyms for vehicles to protect privacy.
- **Time Stamp** Identifies the UTC instant in which Position was measured in the transmitting station. It is a fundamental information for the Vehicle dynamics extrapolation.
- **Longitude**: the estimated Longitude of the geometrical centre of the station
- **Latitude**: the estimated Latitude of the Geometrical centre of the station
- **Elevation**: the estimated Geographical altitude of the station
- **Speed**: the estimated module of the speed of the station along the current direction. Clearly this data is set to zero for fixed stations.
- **Heading**: the estimated value of the angle of the vehicle trajectory with respect to North.
Speed and Heading together provide the speed vector, again set to zero for fixed stations

**Dynamic data accuracy**: a simple indicator of the Quality of the Positioning, Speed, Heading. Currently under discussion is the benefit if a covariance matrix of Position, speed, yaw-rate and acceleration of the vehicle is provided.

All the above mandatory information is contained in the header of each message.

These are the other mandatory vehicle data fields contained in the CAM:

- **Vehicle Type**: a parameter considering the type of vehicle (truck, bus, motorcycle, …)
- **Length**: the length of the vehicle
- **Width**: the width of the vehicle
- **Longitudinal Acceleration**: the acceleration in the heading direction
- **YawRate**: The vehicle’s yaw rate
- **Acceleration control**: a Boolean status (on/off) of the commands which controls the acceleration of the vehicle: Brake Pedal, Throttle Pedal, Cruise Control, Adaptive Cruise Control, Limiter
- **ExteriorLights**: the status of the exterior lights

For the RSU, the following set of mandatory data is to be provided in the CAM:

- **NearestRSU**: the position of the four nearest RSU
- **Road Link Type**: the type of road link (Intersection, motorway,…) associated to the RSU

There is a second set of data which is not transmitted by default but may be added according to the running applications and the specific operating scenarios. These data may be added as a variable payload to the CAM or using specific messages which may have different repetition rates.

Both the messages and the variable payload are structured in order to ensure the maximum flexibility for adding these data.

For this reason a **tagged list** is used. This concept allows adding a variable number of data elements and each added data is preceded by a tag that univocally identifies the data itself. In order to optimize this structure **data elements** may be grouped in **data frames** (e.g. **2D Position** is the sequence of Latitude and Longitude) which are identified by a single tag.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Identifier of the data element or data frame</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item</td>
<td>The effective data element or frame</td>
</tr>
</tbody>
</table>

The set of optional data is the following:

- **Airbag or Crash Sensor**: a signal informing that the vehicle had an accident
- **Brake Boost Applied**: a signal informing about an emergency brake
- **Friction Road Surface**: Estimation of the friction of the road surface
**Engine/Drivetrain Status:** Is the engine starting to overheat or otherwise malfunction (NOTE: This is needed in several CVIS applications – you do not want to give an overheating vehicle access to a critical tunnel for instance!)

**Gear Status:** Status of the gearbox (inserted speed)

**LightbarInUse:** For emergency or service vehicles

**Master Cylinder Pressure:** Estimation of the brake intensity

**Mean Steer Angle:** Information for trajectory prediction

**Position Covariance:** Information related to the quality of the estimation of the vehicle position and dynamics

**Programmed Speed Control Value:** Information for trajectory prediction

**Rain Sensor:** Environmental information

**Siren In Use:** For emergency vehicles

**Stability Control Status:** This information may be used to estimate a critical road condition (alternative/complementary to Friction road condition)

**Steering Wheel Angle:** Information for trajectory prediction

**Steering Wheel Angle Rate Of Change:** Information for trajectory prediction

**SunSensor:** Environmental information

**Tank Filling Level:** this information may be used to estimate a possible stop in critical areas (e.g. a tunnel)

**Tilt Sensor:** for motorcycles, alternative to Airbag

**Tire Pressure:** may help to estimate critical stability condition of a vehicle

**Type Of Goods:** for informing about dangerous goods transportation

**Vehicle Elevation:** additional position coordinate (useful where roads are overlapped)

**WindscreenWiper:** simpler alternative to rain sensor

**WiperRate:** related to rain intensity

**Obstacle parameters:** this data structure provides information about fixed or moving objects. The objects may be detected by the transmitting station using on board sensors or through VANET messages (e.g. a vehicle or an RSU may decide to forward the presence of a vehicle which may be hidden to other vehicles for propagation reasons).

**Satellite raw data:** this data can be transmitted as support for position accuracy improvement. Algorithms are under development based on the elaboration of these data in order to reduce the common mode errors bringing to a better accuracy of relative positioning.

The following data fields are optional for Road Side Units:

**Temperature:** the ambient temperature in the RSU area

**VisibilityRange:** the visibility range in the RSU area

**TrafficDensity:** the traffic density in the RSU area

**Weather:** the weather condition in the RSU area
10.4 The Transport Protocol Data Unit (TPDU)

Making reference to the frame structure introduced in section 9.4, in this section the structure of the Transport Protocol Data Unit (TPDU) is described.

The TPDU contains a Transport Header and the protocol data unit (PDU) of the facility layer as specified in the European ITS communications reference architecture.

The content of the TPDU has been defined taking into account the needs of European research activities (covered by COMeSafety), standardization done at IEEE 1609, standardization at ETSI ITS and standardization at ISO TC204 WG16.

Every broadcast communication, irrespective whether transmitted periodically, repetitive or in a single shoot, shall carry at least a single message identifier (ServiceID) which uniquely identifies the related service. In a generalized approach, there shall be a sequence of such identifiers allowing carrying several messages in a single packet.

Optionally there may be message data (ServiceData) connected to a message identifier. Note that a service specific sub-addressing may apply and being performed inside the message data.

Further on, connected to the message identifier, there may be information on local network / transport layer addresses (where is the local application) similar to IP address and port number (LocalAddress), allowing a peer station to reply to this message, and information on an optional service channel (ServiceChannel) to be used for subsequent communications. In case an optional request for a service channel is present, there has to be also the detailed information on this channel (ChannelInfo), e.g. medium, frequency, etc. carried in a service channel list element.

Such a broadcasted packet is of message type "ServiceInit". Dependent on the details of the packet, there may be a follow-up packet of type "ServiceAck" from recipients of this packet, which finally may end up in a unicast communication session with a sequence of packets of types "ServiceRq" and "ServiceRs". The various possibilities are illustrated in the following sub-clauses.

The approach also enables to select a networking protocol for the operation phase which is different to the networking protocol used during the service initialisation phase.

The Structure of the TPDU is defined by COMeSAFETY, based, as already remarked, on existing proposals of different projects and working groups. The basic Structure was defined in the C2C-CC and extended in order to support the three class of applications (Safety, Efficiency and Value Added Services).

Although this protocol is inherently cross-layered and includes the Transport part, it is nevertheless here reported as a facility in order to provide a unified view.

The TPDU structure is reported in Figure 37 and detailed in Annex 10-1 “Message Catalogue” using the ASN.1 syntax.

In Figure 37 also the Network header already described in section 9.4.1 has been reported in order to provide a global view of a message.

The Net Header information element contains some mandatory data as indicated in the previous section and unambiguously identifies the message originator node. It serves both network layer and application layer requirements. This element is derived from the current specification in C2C-CC.

The transport is formed by two 16 bit word (source and destination port).
The **PDU** carries application specific information and it has been structured in order to support all the classes of applications (Safety, Efficiency and Value Added Services). Three different information elements are possible (each dedicated to a single class of applications).

The **PDU** is described in the next section. It should be noted that some information used by a class of applications may also be used by other classes. This is generally true for Value Added Services or Efficiency applications which may use the information contained in the Safety unit. Generally in a message any combination of Information elements may be used but always a single Safety PDU element must be present. More than one V.A.Services information element may be present in a single frame. A filtering may be operated by the congestion control algorithm, based on priority of the different messages and type of applications requesting the transmission.

The **Forwarder Message** is a complete added on message that a forwarder station may add in case of forwarded message (that is the PDU content has been originated by another station). Using this strategy it is possible to send two messages in a single frame. It should be noticed, as described in a previous section, that the forwarder message is complete and may contain a separate security.

### 10.5 Protocol Data Unit

The general structure of each PDU element is characterized by a MessageType, Service Id field and ServiceData.

Message Type is used for discriminating situations like “ServiceInit” or “ServiceRequest” or “ServiceAcknowledge”.

For the Safety Messages the “ServiceInit” value is normally used.

The ServiceId (1 to 4 bytes) univocally identifies the Services.
The message identifier (ServiceID) value favourably is stored as an Integer variable with extendable size, i.e. in ASN.1 this is INTEGER (0..127,...) - using only 7 bits of each octet to represent the value. A viable and efficient compromise taking into account existing approaches with registered values is

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Service Id</th>
<th>Service data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message (service) identifier value</td>
<td>Size of identifier in octets</td>
<td>Description</td>
</tr>
<tr>
<td>0 - 31</td>
<td>1</td>
<td>Meaning of values shall be the same as specified in ISO 15628:2007 for DSRCApplicationEntityID. These numbers represent only classes of applications, thus a full cycle of “ServiceInit”, “ServiceAck” and one or several “ServiceRq” and “ServiceRs” are needed.</td>
</tr>
<tr>
<td>32 - 127</td>
<td>1</td>
<td>Reserved for road safety and traffic efficiency. To be controlled by a registration authority, e.g. a road administration. Could be BAST in Germany or the European / International equivalent, if existent.</td>
</tr>
<tr>
<td>128 - 2.097.151</td>
<td>2 / 3</td>
<td>Reserved for other services. This number range should be subject to a registration and may also reference specific applications, rather than application classes. The registration authority could be CEN TC278.</td>
</tr>
<tr>
<td>2.097.152 - 268.435.4555</td>
<td>4</td>
<td>Reserved for IEEE registration (ProviderServiceIdentifier). This is reasonable if IEEE accepts not to use the value range from 32 to 2.097.151 for ProviderServiceIdentifier, or follows the specifications of these values as done in Europe. Note that IEEE 1609 always is using a 4 octet representation, rather than a field with variable length.</td>
</tr>
</tbody>
</table>

The Service data is the Payload of the message. In Annex 10-1 The detail of the payload is defined for the SafetyPDU. For the Efficiency there is no specific definition and for V.A. Services a more detailed structure is described in a following section.

### 10.5.1 The “Cooperative Awareness Message”

CAM is the most important message as it has the role of a heartbeat of the network providing key information of the stations. It is issued continuously by any vehicle and roadside station with a repetition frequency currently established at 2Hz.

The complete TPDU of the CAM is
The Protocol and the Net Header are common for all the messages. The MessageType for CAM is always set to “ServiceInit” value. CAM Service Id is a specific 1 byte number. CAM Service data is the payload of the message which includes:

- **Header extension** (fixed) which contains a set of data which are mandatory for the safety applications, The list of the variables depends on the type of station (vehicle or RSU) and was already described in section 10.2.

- **Additional Payload** (optional) which is a variable part containing data available in the station and are sent as tagged list.

**Efficiency and A.V. Services PDU may be optionally added to CAM**

Any combination of payload is allowed. The combination is decided by the requests made by applications and eventually filtered by the congestion control according to applications priority criteria.

Normally only Header, Extended header, would be sent as a heartbeat (Neighbour discovery/safety radar map). Service Advertisement(s) can be sent when the network load is sufficiently low.

A complete message catalogue with full details and data format is reported in an Annex 10-1 using ASN.1 syntax. It should be underlined that the catalogue tried to reuse as much as possible the current version of SAE J2735 which specify the American DSRC standard.

Specifically, other kinds of messages are included which allow one-shot or periodic transmission with a period different from the beacon period (min. period 100 ms.). These messages are normally triggered by applications following the recognition of a specific event or scenario.

### 10.6 Decentralized Environmental Notification Message

The dezentralized environmental message provides information about a location based situation that is not necessarily connected to a communication node, e.g. black ice.

The existing situation can be detected by one or several vehicles as well as RSUs, and it will persist after the vehicle has passed on. The information is independent of the detecting vehicle. Typically, information persists for several minutes.

Information about the same situation might be issued from different originators. There are various types of originators: detecting vehicles, autonomous RSU with environmental sensors, or service centers connected to RSUs. The information is distributed by store and forward mechanisms within the C2C network without a central control unit.

Dezentralized environmental messages are created event based and periodically updated if the issuing node detects the persistence of the situation for a longer time. The sender node shall specify the destination area. Distribution mechanism shall ensure that the message is distributed within the latency requirement to all nodes that are or enter the destination area until the information expires. At receiver side, reasonable efforts should be taken to evaluate the relevance of the messages and the information.

The structure of the DENM is as follows:

<table>
<thead>
<tr>
<th>Transport Header</th>
<th>Protocol Id</th>
<th>Net Header</th>
<th>MessageType “ServiceInit”</th>
<th>DENM Service Id</th>
<th>DENM Service data</th>
<th>Other services (Option)</th>
</tr>
</thead>
</table>
The coding Protocol Id, NetHeader, MsgType and ServiceId follows the same rule of CAM. The “Service data” is composed by three fixed order components as shown in Figure 38.

**Message Management Container**

The message management container holds administrative information of the messages, e.g. the message ID, dataVersion, security etc. A cancel mechanism is also included in this container in order to cancel the detected situation. A situation can be canceled either when the detected situation has ended, or a detected situation has been judged as invalid.

**Situation Container**

The situation container includes the information describing the detected situation as well as its possible impact to the road safety.

**Location Container**

Location container consists mainly of three parts: event location, destination area and location referencing. Event location describes the position where the event is detected. This situation might be detected as a point on the road, a segment of road with certain length or an area. However, a reference position shall be used. The destination area describes the geographic area that the messages shall be sent. This area can be of different shape (rectangle, ellipse, circles) and different size. Location referencing is a means to provide information which allows a system to accurately interpret the location of the detected event. The location referencing method is necessary at both sender and receiver sides, this will help to improve the correlation precision.

![Figure 38: General Structure of the Decentralized Environmental Message Payload](image-url)
10.7 The Service TPDU

As already explained the TPDU has been designed in order to easily manage both one way messages and more complex protocols requiring the establishment of a session.

In the following the available features are described with some examples.

10.7.1 ServiceInit TPDU

Figure 39 shows the case that only a message identifier is sent which totally identifies a predefined message. The recipient knows the message just by reading the message identifier (ServiceID #1). A reply is not possible. There may be also several message identifiers in the packet.

![Figure 39: TPDU - ServiceInit A: only message identifiers](image)

Figure 40 shows the case that a message identifier and a local address are sent. The recipient either knows the message just by reading the message identifier (ServiceID #1) or knows the service class. A reply is prepared by providing the local address information (LocalAddress #1). A change to a service channel is not possible. There may be also several sets of message identifier and local address in the packet.

![Figure 40: TPDU - ServiceInit B: message identifiers and local addresses](image)

Figure 41 shows the case that a message identifier, a local address and channel information are send. The recipient either knows the message just by reading the message identifier (ServiceID #1) or knows the service class. A reply is prepared by providing the local address information (LocalAddress #1). A change to a specific service channel (ServiceChannel #1) with properties given in ChannelInfo is requested by providing the elements ServiceChannel and ChannelInfo. This approach basically also supports to use a completely different radio technology for the service channel. There may be also several sets of message identifier, local address and service channel in the packet. The element ChannelInfo appears only once and contains the information for all service channels.

![Figure 41: TPDU - ServiceInit C: message identifiers, local addresses and channel information](image)

Figure 42 shows the case that a message identifier together with message data is sent. The recipient is able to decode the message data (ServiceData #1) by evaluating the message identifier (ServiceID #1). A reply is not possible. There may be also several sets of message identifier and message data in the packet.

![Figure 42: TPDU - ServiceInit D: broadcast data](image)

Figure 43 shows the case that message identifier, message data and a local address are send. The recipient is able to decode the message data (ServiceData #1) by evaluating the message identifier (ServiceID #1). A reply is prepared by providing the local address information.
(LocalAddress #1). A change to a service channel is not possible. There may be also several sets of message identifier, message data and local address in the packet.

<table>
<thead>
<tr>
<th>Transport Header</th>
<th>MessageType</th>
<th>ServiceID #1</th>
<th>ServiceData #1</th>
<th>LocalAddress #1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&quot;ServiceInit&quot;</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 43: TPDU - ServiceInit E: broadcast message with local addresses for reply

Figure 44 shows the case that a message identifier, message data, a local address and channel information are send. The recipient is able to decode the message data (ServiceData #1) by evaluating the message identifier (ServiceID #1). A reply is prepared by providing the local address information (LocalAddress #1). A change to a specific service channel (ServiceChannel #1) with properties given in ChannelInfo is requested by providing the elements ServiceChannel and ChannelInfo. There may be also several sets of message identifier, message data, local address and service channel in the packet.

<table>
<thead>
<tr>
<th>Transport Header</th>
<th>MessageType</th>
<th>ServiceID #1</th>
<th>ServiceData #1</th>
<th>LocalAddress #1</th>
<th>ServiceChannel #1</th>
<th>ChannelInfo</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&quot;ServiceInit&quot;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 44: TPDU - ServiceInit F: broadcast message with local addresses for reply on a service channel

Any combinations of TPDU payload presented in figures 39, 40, 41, 42, 43, 44 are possible in a single packet. In case a reply is possible, this can be either of message type "ServiceAck" or "ServiceRq".

10.7.2 ServiceAck TPDUs

Figure 45 shows the case that the message type "ServiceAck" just confirms the message received previously in a MAC broadcast frame, by sending reply data (AckData #1). No subsequent session is enabled. If a service channel was requested, then this frame is transmitted in the service channel. Several replies may be contained in a single packet. Several replies may be contained in a single packet carried on a MAC unicast frame.

<table>
<thead>
<tr>
<th>Transport Header</th>
<th>MessageType</th>
<th>ServiceID #1</th>
<th>AckData #1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&quot;ServiceAck&quot;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 45: TPDU - ServiceAck A: acknowledgement of a service without enabling a session

Figure 46 shows the case that the message type "ServiceAck" confirms the message received previously in a MAC broadcast frame, by sending reply data (AckData #1), and enabling a subsequent session by providing local address information (LocalAddress #1). If a service channel was requested, then this frame is transmitted in the service channel. Several replies may be contained in a single packet carried on a MAC unicast frame.

<table>
<thead>
<tr>
<th>Transport Header</th>
<th>MessageType</th>
<th>ServiceID #1</th>
<th>AckData #1</th>
<th>LocalAddress #1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&quot;ServiceAck&quot;</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 46: TPDU - ServiceAck B: acknowledgement of a service with subsequent session
10.7.3 ServiceRq and ServiceRs TPDU

Figure 47 shows details for the message type "ServiceRq" carried in a MAC unicast frame. The information provided in the elements "LocalAddress" during initialisation is used in the transport header (and in the network header, depending on the networking protocol used).

Figure 47: TPDU - ServiceRequest

Figure 48 shows details for the message type "ServiceRs" carried in a MAC unicast frame. The information provided in the elements "LocalAddress" during initialisation is used in the transport header (and in the network header, depending on the networking protocol used).

Figure 48: TPDU - ServiceResponse

10.8 TPEG

TPEG is a bearer- and language-independent TTI (Traffic and Travel Information) service protocol that has a unidirectional and byte-oriented asynchronous framing structure. There are basically two formats for TPEG messages – tpegML and TPEG binary. The difference between tpegML and TPEG binary concerns only the format and not the content, as both variants are designed to map on onto each other precisely. Therefore the differences concern mainly the size of the data used and the accessibility. As there exist already a lot of software tools and libraries it is comparatively easy to handle messages in XML format as long as there are enough hardware resources and bandwidth. However, in an area of limited resources, one can save memory and/or bandwidth by using the binary format. For this reason the binary format is preferred for air transmission while on the internet it is possible to use both, the binary and the XML.

TPEG is a modular toolkit, standardised through CEN and ISO and consisting of the following applications:

- RTM - Road Traffic Message
- PTI - Public Transport Information
- Loc - Location referencing, used in conjunction with applications

Initially TPEG was imagined to be important in the so-called Delivery Segment and it was only later – when taking the whole information chain into account — that the Content Segment could also be seen to benefit from the development of tpegML.
The TPEG-RTM application is designed to allow the efficient and language independent delivery of road information directly from service provider to road users. The information provided relates to event and some status information on the road network and on associated infrastructure affecting a road journey. For example, limited information about abnormal operation of links in the network may be included, such as ferries, lifting-bridges, etc. The TPEG-RTM Application has the broad objective to allow the generation of TTI messages, for delivery to the end-user by one or more bearers. A hierarchical methodology has been developed to allow the creation of messages from a set of TPEG-RTM tables, which are essentially word oriented and cover most needs. These TPEG-RTM tables (essentially word oriented data object dictionaries) comprise a wide ranging ability to describe a TTI event and some status information, introducing new precision in a number of areas such as 'Vehicle types', 'Positional information on the carriageway' and 'Diversion routing advice'.

Considering, TPEG make reference to all categories of applications and it is suitable for communication technologies like DAB or Wi-Fi. Also some of the events considered in VANET messages catalogue use the coding of TPEG.

However, the existing TPEG-RTM tables do not describe all events and status information required for the implementation of the services for cooperative systems. Some of the specified services prescribe an acknowledgement to announce the successful transmission of traffic information. All these special requirements are currently not implemented in TPEG, because the initial idea was to use TPEG only for the coding of broadcast messages. An extension of these messages was proposed and tested in the COOPERS project.
11 Security

The communication technologies laid out in this document and their use for safety, traffic and other applications open up possibilities to attack parts or the overall system. It is viable to the system that these attacks are prevented and should an attack be tried that it is detected and countermeasures are taken. In addition to ensure a stable and reliable system operation that is effectively defendable, certain security mechanisms are needed to ensure certain desirable system features as privacy of information and the possibility to allow certain users only partly access to system functionality.

In the overall ITS Station Reference Architecture shown in Figure 50, this chapter describes the block “Security” and its interfaces to “user services/applications”, “facilities”, “networking” and “access technologies”.

11.1 Introduction

Securing V2X is an indispensable prerequisite for its deployment and real-world use. Three major goals need to be achieved:

- All information communicated in the network must be correct and trustworthy.
- The V2X system must be extremely robust and must not fail to work.
- The V2X system participants’ privacy must be ensured.4

---

4 In many cases, VANET applications communicate personal data, such as current location or current speed, which could be used for vehicle / driver profiling.
Besides this technical work considers various further discussion areas (see Figure 51):

- The goal of the security mechanisms is to ensure acceptance and credibility of the system by the end user, who trusts the system.
- Current standards are to be considered and properly applied to the system design. Where necessary, standards need to be extended or new ones created.
- In addition to pure ad hoc communication, the integration of communication infrastructures and telecommunication platforms into the overall system architecture are to be properly set.
- Thereby, the discussions are driven by commercial requirements conveying business models and operational concepts, partnerships and regulations.
- Legislation aspects need to address privacy, law enforcement and liability questions.

![Figure 51: Security Discussion Areas](image)

From a technical point of view, in order to achieve the first two of the major goals, i.e. trustworthy dissemination of information and robustness, the Car2X network must be protected against different kinds of attacks. Analyzing the threats for this special kind of network, Denial of Service attacks, generating fake messages or tampering with messages need special consideration.

For the assistance and collision avoidance types of applications, the security solution must still allow low latency communication. This is an important requirement since applying cryptographic methods can create considerable computing overhead. Hence, it is not possible to adopt security protocols involving strenuous verification or interaction processes.

Security mechanisms should normally not surface at the application layer. Of critical importance however is that applications receive from other vehicles or from infrastructure entities information with a certain level of trustability. This, besides integrity (knowing that the message had not been tampered with in an unauthorized way, see above), requires receiving it from a trusted source. While strong sender identification and authentication is not the goal here, it might still be somewhat required and is competing against the goal of driver/vehicle privacy. An anonymized authentication of messages should ideally be possible.

Notably, to establish trust, basically cryptographic measures can be applied as well as means of plausibility checking and cross-verification. It remains to be established, how cryptographic means can be balanced against application algorithms such as plausibility checking. Issues
such as radio resource consumption, processing power, hard-ware mechanisms enhancing security need to be considered here, as well.

Moreover, applications must not assume that individual vehicles can always be identified by some unique code that is openly communicated. To protect privacy and prevent recording of movement patterns etc. it should rather be assumed, that means for vehicles to assume dynamic identities and even dynamic certificates for regular over-the-air communication are established.

11.2 Threats

In the following, a short overview of potential threats on a the system is given:

**Extraction/modification of secret material**

The attacker extracts or modifies the vehicle's secret information, e.g. from the on-board equipment. Then, the attacker is able to perform identity spoofing by sending messages which will appear as sent by the unaware victim vehicle. The vehicle's secret information must be secured against such attack, aimed to steal the vehicle's private key, and also digital signature breaking must be computationally difficult to perform.

**Tampering with vehicle's platform**

A way to perform this attack, without any knowledge about the network protocols and the security enforcements, is to change the sensors' input values. The detection of such an attack is challenging. As one countermeasure, plausibility checks can be performed on the received message's content.

**Network jamming**

An attacker can jam the network, e.g. by sending thousands of packets, reducing the availability of nodes within the network or even breaking it down completely. In this way, lots of vehicles' resources could be consumed as well, since they may have to process a huge number of messages.

**Alteration attack**

A VANET applying multi-hop routing mechanisms, a malicious node may delay the relaying of important messages, as well as rejecting them. Node selfishness can be considered as a sub-part of this attack. Assuming that the majority part of nodes is honest, the success likelihood of this attack can be reduced by exploiting the multi-path nature of VANETs. An important message can be forwarded by several nodes in order to follow different paths.

**Fake message injection**

This attack consists in the injection of messages, e.g. advertising fake events by malicious nodes, influencing the behaviour of the system. Message replay can be classified as belonging to this kind of attack. Messages sent by honest vehicles can be caught and sent out again, in future, without any further modification.
Sybil attack
When speaking about security in VANETs, it is usually assumed that the majority part of nodes in the network is honest. This is true when a node is considered as a physical entity. The Sybil attack neutralizes the one-to-one relation between physical and logical entity. A malicious node can try to obtain many different identities in order to control a consistent part of the network (e.g. by owning different pseudonyms at the same time and then claiming to be many vehicles).

Privacy violation
Privacy can be violated by associating the vehicle identifier, contained in a message, to a precise vehicle and that again to a user profile. In this way the vehicle and user can be easily tracked. Such attack could have only temporary effects if some countermeasures were adopted. Usually, it is not a standalone attack since it can be used to track a vehicle position and performing other attacks on it.

11.3 Security Baseline Concepts
On the technology side, some baseline concepts have been drafted, that are currently being actively discussed within different consortia:

- As vehicles equipped with a Car2Car system will be periodically geo-broadcasting their position and send beaconing information for network layer purposes, the real identity of the vehicle will be concealed to protect privacy against both, malicious and casual observation or tracking. This means, that permanent identifiers and addresses must not be communicated in clear over the air.

  To the contrary, at all layers from physical to IP/network to application, in-vehicle systems will be using temporarily assigned identifiers. Fixed identifiers should only be used in the occasional situation, where mutual system authentication is necessary, e.g. when obtaining a new set of temporary identifiers.

  The real identity is not to be revealed over the air, but has to be concealed accordingly.

- To ensure trust in messages, they have to be signed. Signing of messages again has to happen with dynamically assigned, temporary pseudonyms. It is currently under investigation, how frequently pseudonyms will be updated and what the technical mechanisms will be for this procedure.

- Moreover, it is yet to be decided, which crypto-technology to actually use for these pseudonym signatures. In this choice, a number of factors have to be balanced, such as security level, size of signature and bandwidth constraints, processing time and real-time requirements of e.g. safety applications. Currently, RSA and ECC are candidates under investigation, where ECC is the favourite.

Note, that all these assumptions are still work in progress. A clear favourable solution has not been identified yet and some questions are yet under discussion. The C2C-CC is in liaison with various security activities and open to discussions with and proposals from projects such as SEVECOM\(^5\) or the data security working group of the project NoW – Network on Wheels\(^6\) as well as the HIDENETS project (Highly Dependable ip-based NETworks and Services, \texttt{http://www.hidenets.aau.de}).

\(^5\) \texttt{http://www.sevecom.org} \\
\(^6\) \texttt{http://www.network-on-wheels.de}
11.4 Security Architecture

The rationale for the security architecture part presented here is the following:

- Deployment of Car2X in the future is based on communication standards that are not finalised yet. This means that a clear separation must be made between the architecture and technologies below.

Consequently, the approach proposed is the following:

- Definition of an abstract security architecture which is future proof, i.e. the abstract security architecture does not change, even though some technology standards will change, or stronger crypto systems will be included. The abstract architecture is based on a number of founding principles.

- The abstract architecture can then be mapped to specific technology solutions.

As in other parts of this document, the resulting baseline architecture therefore consists of:

- The abstract architecture

- Specific implementation solutions that can be considered as proof-of-concept implementation

11.4.1 Security Architecture Principles

This section identifies the principles of the future-proof architecture for a secure vehicular communication system. In the following table, we describe each principle and explain the rationale for it. Besides conceptual principles, the table conveys implementation concepts in order to provide an extensible security implementation.

<table>
<thead>
<tr>
<th>Category</th>
<th>Principle</th>
<th>Description</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication management</td>
<td>Layered based security</td>
<td>Assuming that the communication system will be divided into different layers, the security system will consist of different components that connect to these layers and address the security aspects of each individual layer.</td>
<td>Separation of concern between application and security Technology independence</td>
</tr>
<tr>
<td></td>
<td>Configurable security level</td>
<td>Applications can configure their security level based on individual security needs (insecure, integrity, confidentiality, privacy …)</td>
<td>Adaptation to application needs</td>
</tr>
<tr>
<td>Identity management</td>
<td>Resolvable Pseudonymity</td>
<td>Digital actor identity can be replaced by a pseudonym. This is mandatory for vehicles. Higher jurisdiction may allow for transcript access.</td>
<td>Ensures privacy as digital actor identity is not revealed.</td>
</tr>
<tr>
<td></td>
<td>Protocol identities control</td>
<td>Pseudonym system has full control of changing the underlying protocol stack’s identities. Any other identifications (e.g. application identities, upper layer protocol identities) are not transmitted in the clear</td>
<td>Prerequisite for effective pseudonym change and privacy support</td>
</tr>
<tr>
<td>Category</td>
<td>Principle</td>
<td>Description</td>
<td>Rationale</td>
</tr>
<tr>
<td>----------</td>
<td>-----------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td>Actors have a long term identity</td>
<td>Actors possess a life-long unique identity which is never revealed over the air.</td>
<td>The unique digital identity can be used to authenticate and authorize the actor to a Car2X system, when required.</td>
</tr>
<tr>
<td></td>
<td>Configurability of pseudonym system</td>
<td>Possibility to parameterize the pseudonym system (e.g. in a region, during a period)</td>
<td>Specific policies, Infrastructure scale up, Individual privacy requirements</td>
</tr>
<tr>
<td></td>
<td>Openness to multiple credential sources</td>
<td>Possibility to have independent set of pseudonyms</td>
<td>Takes into account existence of multiple authorities (multiple business stakeholders, multiple countries, …).</td>
</tr>
<tr>
<td></td>
<td>Eviction of nodes</td>
<td>Management of nodes with unauthorised credentials</td>
<td>Takes care of broken credentials or attackers</td>
</tr>
<tr>
<td></td>
<td>Upgrade-e-ability of security system</td>
<td>Possibility to upgrade the security system.</td>
<td>Update of security component, e.g. in case of detected flaws</td>
</tr>
<tr>
<td></td>
<td>Hardware security module</td>
<td>Optional: Dedicated security hardware</td>
<td>Enhancement of protection of vehicle cryptographic material and safeguard data usable for liability implication</td>
</tr>
<tr>
<td></td>
<td>Platform</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 11.4.2 Abstract Architecture: Conceptual View

This section explains the security baseline abstract architecture from a conceptual view. It first provides an overview of this conceptual view. It then further describes the four modules it is comprised of:

- Firewall and Intrusion Management
- Authentication, Authorization, Confidentiality, Profile Management
- Security Information Base
- Hardware security module
Figure 52: Detail of the Security Block from the ITS Station Reference ARchitecture

11.4.2.1 Overview

Figure 52 shows the security architecture in an abstract and deployment-independent view. The security modules are logical containers that group components that fall within their domain. These security components then realize specific security functions.

The five security modules and their components are described below.

1. The **Authentication, Authorization, Confidentiality, Profile Management Module** addresses secure communications in Car2X networks. There are dedicated security components for different communication patterns. Currently envisioned secure communication components include:
   - Establishment of secure channels to infrastructure services providing integrity, authenticity and confidentiality
   - *Secure Beaconing* provides the means for the receiver to verify the authenticity and integrity of beacons.
   - *Secure Geocast* assures the reliability and security of Geocast.
   - *Secure Georouting* assures the authenticity and integrity of the route messages, and protects routing against routing attacks (e.g. rerouting, replay, dropping, forging etc.)

2. The **Security Information Base Module** provides and manages identities and certificates of all entities directly involved in vehicular communications, i.e. vehicles,
road-side units and infrastructure components and leverages on pseudonyms (i.e. certified public keys) to assure a certain level of privacy to individual vehicles in vehicular networks.

- **Identity Management** manages the long-term identifier,
- **Trust Management** describes a system that provides services like public key management and revocation services.
- **Reasoning about trustworthiness of data, e.g. by checking authenticity, and using plausibility checks**
- **Pseudonym Management** generates, stores, and refills the pseudonyms.
- **Pseudonym Application** provides pseudonyms used in secure communication and decides when to change pseudonyms.

3. The **Firewall and Intrusion Management Module** assures the security of the in-car Car2X system and prevents unauthorized access to critical in-vehicle systems. This module contains the following components:

- **Gateway/Firewall** protects critical in-vehicle systems from attacks through vehicular communications. It monitors and checks the consistency of data flow between the communication system and in-car systems.
- **Intrusion Detection/Attestation** detects tampering (intrusion) with in-car systems.

4. The **Hardware Security Module** provides hardware for storage and processing of cryptographic material and safeguard data:

- **Key/Certificate Storage** stores the private keys and the vehicle’s long-term certificate.
- **Protected Functionality** stores functions which has high secure priority, e.g. signature creation.

The logic links depict the information flow and cooperation among the security modules. A brief description of the links is given below.

- **Identification & Trust Management** – **Hardware Security**: Parts of the identification credentials and necessary operations will be stored or implemented in hardware, so there is a connection to the hardware security module.
- **Identification & Trust Management** – **In-car Security**: The in-car security module relies on the secure identification & trust management module for making access decisions based on actors’ identities and attributes.
- **Secure Communication** – **In-car Security**: The in-car security module cooperates with the secure communication mechanisms in cases of communication of external nodes with internal systems. E.g. protects in-car systems from attack through communications channels.
- **Secure Communication** – **Identification & Trust Management**: The secure communication module relies on secure identification & trust management, e.g. in order to verify the identity information received from other parties or for accessing the own key material for purpose of signature creation.
- **Secure Communication** – **Privacy Management**: The Privacy Management Module provides pseudonyms to the Secure Communication Module and also decides when to change pseudonyms.
- **Privacy Management** – **Identification & Trust Management**: The Privacy Management Module can be seen as an extension to the identification & trust management module as it extends the creation and application of identifiers.
11.5 Abstract Architecture: Other Views

11.5.1 Deployment View

Figure 53 shows a deployment view of the architecture, showing how the conceptual view is mapped on a physical structure made up of three types of entities, vehicles, roadside units (RSUs) and the service infrastructure:

- Vehicle entities include all five modules of the conceptual view.
- RSUs do not need two of these modules: the in-car security module (in charge to protect the vehicle against intrusion), and the privacy management module as it is assumed that RSU identities are public.
- The service infrastructure includes the trust management infrastructure as well as secure communication capability with RSUs, and possibly directly with vehicles.

![Deployment View Diagram]

Figure 53: Deployment View

Vehicles, RSUs and the Service infrastructure interact as follows:

- Vehicles interact with other vehicles (not showed in figure) and with RSUs through a wireless medium.
- RSUs interacts with the service infrastructure though a communication backbone (e.g. Internet based).
- Vehicles interact directly with the service infrastructure through direct communication capability

Figure 53 also shows other details of deployment:
- In vehicles and RSUs, conceptual modules are grouped into an overall system called the security and policy manager
- The security and policy manager internally interacts with the following entities as follows:
  - In the vehicle, the application interacts with the in-car security module, the communication stack interacts with the secure communication module and the privacy management module.
  - In the RSU, the communication stack interacts with the secure communication module.

11.5.2 Administration View

Administration capabilities are needed in order to allow the upgrade-ability of the security system. Figure 54 shows an administration view explaining how upgrades take place. Vehicles and RSUs are equipped with a local administration system which interacts with a master administration system available in the service infrastructure. Several types of updates are possible:
- Parameters (e.g. pseudonym change parameters, keys …)
- Code (e.g. an updated security system)

![Figure 54: Administration View](image)

The administration view is not elaborated further.

11.5.3 Integration View

Software integration features are needed in order to allow the integration of security mechanisms into existing implementations. Figure 55 shows an integration view depicting the
integration of security and policy manager. It consists in having a hook system which allows security and policy manager to be integrated with applications and/or communication stacks.

![Integration View Diagram](image)

**Figure 55: Integration View**
This chapter is focused on the System Management block in the ITS Stations Reference Architecture – see Fehler! Verweisquelle konnte nicht gefunden werden.

The System Management role is to amalgamate applications, networks and interfaces in a specific implementation. This implementation may range from a simple stand-alone unit in a vehicle (Vehicle Station), to a complex router-host interaction in large roadside network.

The central system manager tasks are:

- Manage policy setting and maintenance for each logical functions block in a Station
- Manage (dynamic) interface selection per application. Criteria based on policies, application requirements and interface performance/availability
- Manage transmit permissions and synchronisation based on physical cross-interference between air interfaces combined with information priorities
- Manage security and privacy functions depending on application type and interface used.

The following drawing shows a typical scenario where there are multiple interfaces that need coordination. The scenario may involve different interfaces implemented in separate physical units, in which case the T-SAP must also be used.
12.1 Challenges

The main challenge is to combine the contrasting requirements from safety applications with requirements from other applications.

The characteristics of safety critical applications are

- Low latency
- Interference free environment
- Application is linked to one specific interface
- Security preference is stand-alone implementation in a separate box.

The characteristics of most other applications are:

- Latency is often less important than guaranteed delivery
- Can accept interference if communication succeeds in the end
- Can usually utilize any interface
- Must be network connected – Internet is central to the operation

There is an extensive amount of research going on world-wide to determine the theoretical basis for these systems related to everything from channel models to human response and behaviour. To support this theoretical work, there are many implementations to verify and validate the various findings. It is too early to draw all conclusions at the time of writing this, but it seems to be clear that

a) it is possible to combine the contrasting requirements

b) careful considerations for the implementation is needed to avoid overloading the scarce spectrum that has been allocated in the 5.9GHz range.

Note that some experiments are still underway before the absolute conclusion can be drawn on optimum spectrum usage, but it is clear that the management functions from the application level down to how the radio channel is used is absolutely essential.

12.2 Implementation

System Management is a central architectural function since it controls the entire ITS Station. All the other elements have been described in the previous chapters.

All management and control functions in an ITS Station is per definition collected in the Management plane. This makes for a relatively complex and rigorous definition order to reflect the multitude of potential implementations both in the test/validation and in the full deployment phase.

A real implementation will be very different. Once the overall requirements are determined on a system level, the implementation will usually be much more optimized and monolithic than the strongly layered and block-separated architecture. The implementation depends on the wanted system scenario and the architecture should be seen as a guideline. This means that only elements that are relevant should be considered, and that embedded interfaces are not relevant.

As an obvious example: If there is only one physical interface, all mechanisms related to interface selection and cross-interference management are redundant.

Another example: If all functions are implemented inside one box as a monolithic station, all cross-coordination between Routers and Hosts are not exposed on any interfaces and need not be implemented.
The implications are important:

- Formal description methods using layered architecture can also be applied to Road Safety systems without any impact on performance.

- In a real implementation, the HW and SW of a Road Safety system and a Traffic Efficiency/Value Added Services system may look very similar. The Common Cooperative Platform (CoCoP) will implement a combined solution with Road Safety given a higher priority. It is expected to validate the performance reduction of combining such systems, but note that in the end optimization of implementations will be much more important than benchmarking prototypes.

- Interoperability is only relevant for the observable interfaces. This means that the air interface is the only common interface to describe accurately for functional and technical parameters. Other interfaces will usually exist and needs to be specified in detail as well, but from a system interoperability viewpoint they are less central.

- When a certain management function is required over an exposed open interface, the architecture advice should be followed to achieve interoperability.

- In other cases there is intentionally no interoperability, for instance in a vehicle station consisting of several physical devices with OEM-proprietary interconnections with no 3rd party access. Still the functions described in this document could be used to simplify the implementation.

### 12.3 Components

The architectural components of system management are shown in Fehler! Verweisquelle konnte nicht gefunden werden. More details on management functions can be found in chapter 9.2.1 Architecture, 9.2.2 Management, 9.2.3 Group Casting and 9.2.4 Frame Flow.

There are four sub-function blocks shown:

- **Station Management** is the high-level management of a station. In other words this management will handle:
  - Internal control over multiple Hosts and Routers that belong to one Station
  - External control and communication between Stations as far as needed for management purposes
  - Initialisation and Configuration of (parts of) a Station
  - Decision making on what Application shall use what Interface, including dynamic configuration of all involved layers

- Networking Management will handle aspects of various network functions such as:
  - Routing table updates for IPv6 as defined in ISO 21210
  - General GeoNet management and medium specific GeoRouting as being defined in ETSI TC ITS
  - Optimised non-routing networking for low-latency single-hop scenarios. Mostly medium specific functionality as defined in ISO29281 and under study in ETSI TC ITS

- Cross-Interface Management will handle:
  - Initialisation as well as dynamic configuration and status reporting from each available interface. Configuration parameters may be changed depending on cross-border differences in regulatory domains.
Interference mitigation between multiple interfaces within the same Station, see example in Figure 57

Interference mitigation and load reduction between nearby Stations.

- The MIB is a (virtual) data store inside the management. The purpose of this is to define some important variables and data sets that typically need to be present in the management box. A set of definitions can be found in ISO29281.

There are five main access points to the management functionality that may or may not be relevant depending on the overall system configuration. These interfaces are described as Service Access Points or SAPs.

The five SAPs starting from the lower end are:

- MI-SAP: This is the Management-to-Interface SAP that transfers status information from the actual interface to the management, and returns commands from the management to control the interface operation. The definition of this SAP can be found in ISO 21218.

- MN-SAP: The Management-to-Network SAP will handle routing updating and media selection. Also neighbour tables and similar information will logically be transferred across this SAP. The functionality is partly defined in ISO 29281 and ISO 21210.

- MF-SAP: The Management-to-Facilities SAP will manage link setup and also facilitate transfer between Management entities in different devices. Depending on configuration, there may be several Routers and Hosts in a specific Station. If there are multiple units, there is also a need to transfer coordination and initialisation information between the different physical devices. This involves e.g. priorities and internal handovers when a radio pointing forward hands over a session to a radio pointing backwards because the vehicle is moving, see Figure 57 “Typical Interference Path”.

- MA-SAP: Application information will transfer via this interface. This is typically quality-of-service requirements from the applications to aid selection of the optimum interface. Station configuration, status reporting and policy settings are also transferred via this SAP. Definition can be found in ISO29281.

- MS-SAP: Management-to-Security-SAP. Most of the Management functions will require a high level of security. As long as critical functions are performed outside of a trusted environment, there is a need to protect against threats. This includes configuration and initialisation protocols on a global level such as new channel usage rules from national spectrum authorities, and down to local station-internal protocols between routers and hosts. It is up to the responsible system integrator to decide at the level of trust and protection need. These functions are currently under (joint) development in ISO TC204/WG16 and in ETSI TC ITS WG5.
Part III: Implementation
13 Organisational Topics

This chapter presents organisational aspects as viewed by the three IP’s. For successful deployment of any system not only technological but also organisational aspects need to be considered. A value chain identifying flows of money, information, goods and services needs to be identified. In addition, questions such as “What entities are needed?” and “Who will operate these?” must be answered before the specification of a system can be seen as finalised.

13.1 CVIS

The CVIS project seeks to create a unified technical solution that will allow all vehicles, and infrastructure elements to communicate with each other in a continuous and transparent way using a variety of media, with enhanced localization, and that will enable a wide range of potential cooperative services to run on an open application framework in the vehicle and in roadside equipment. The business modeling approach is mainly based on the experiences in e- and m-Business.

13.1.1 General Concept

In the CVIS project new services are developed with high added value through combining new and existing functionalities. The combination of these functionalities is supported by intelligent use of current and new technologies within a complex organizational framework. Representative for the CVIS kind of services (m-Business) is the pressure of a short time to market. Because of the short product/service life cycles there is only a limited amount of time to collect the necessary resources and to return the investments. Based on e-/m-Business market research only the first service provider on the market will be able to conquer most of the market and thereby to earn back most likely the investments made. This limited time to market forces the multiple participants to cooperate within a network of organisations to combine resources and develop and deliver the services in time. The intelligence behind the architecture of the value network and supporting organisation is perceived as a major competitive factor for the provider of the service.

13.1.2 The value network

To make the inventory based on the 16 services in scope and to determine the different types of cooperation’s within the network a conceptual business modeller is used (see Figure 58).

This basic model is divided in five area’s containing the different actors:

- Actors that buy and consume the service.
- Actors that are supporting the underlying service technology.
- Actors that deliver the functionality through content or service components.
- Actors that supervise and regulate the delivery of the certain service.
- Actors that finance the service.
- And in the centre the actor responsible for the providing service

All these actors can be private or public organisations.
13.1.3 A value network example

As an example of a value network the Dangerous Goods / Cooperative Route guidance service is presented below. This service supports a truck driver and fleet operator to transport dangerous goods safely. Sensitive areas are provided by the (local) government to the service provider, which uses this information to guide the trucks.

Figure 59: Value Network of Dangerous Goods / Cooperative Route Guidance Service.
In the centre of network the service provider is presented. The service provider is the owner of the contractual relationship with the customer. The supporting technology, the content and other service components are delivered through the service provider or directly to the customer. The regulation of the service is demonstrated by the enforcement of regulations and the supervision on the compliance. Next to the actors the value network represents the architecture of the flows of money, information, services and goods within the network.

Only a balanced architecture of value distribution will lead to a sustainable value network and service. The value network is not a fixed situation but has to be optimized for a balanced value distribution by applying sensitivity analysis for different scenarios.

For most of the 16 investigated services there are more than one optional architectures applicable. One differentiator is the extent wherein the service provider is willing or capable to deliver the supporting technology or the embedded content and service components. A specific choice for a certain architecture should be driven by the availability of resources, the return of the value network and the sustainability of the service that is delivered by this network.

### 13.1.4 Central organisations

In addition to looking into value network for one specific service application (example above), the CVIS project is looking also into another type of functionality. Dangerous Goods / Cooperative Route Guidance, as an example of one service application is very interesting today, however, what happens if there is a new service application reaching market in two or ten years from now? Do we need to buy a new cooperative systems unit for that functionality?

Based on these thoughts a need to enable scalability and life cycle management, while ensuring interoperability has been put in focus in CVIS. In order to enable this functionality certain central organisations (organisation types) are crucial for realistic deployment of interoperable cooperative systems. Such organisations would handle the following tasks:

- Govern minimum set of basic technology (e.g. Application/Services/Models)
- Govern Cooperative Systems “community” rules (e.g. how different players interact)
- Govern the operation of the Cooperative Systems world (Publish/exchange of data models & interface definitions)
- Govern security (issue Keys, Certificates, etc)

Furthermore, it is important to mention that there will be no special “Cooperative Systems network organisation”. This is because the Cooperative Systems will run on global IPv6 network, which itself will have certain governing organisations or create peer-to-peer network arrangements.

### 13.1.5 Organisational configurations

Cooperative systems need to allow for scalability and life-cycle management, thus reliable download of new services and applications onto the cooperative units is seen as necessary. The Cooperative Systems could allow both open and restricted download and configuration of applications and services. Depending on implementation strategies one organisation (e.g. vehicle manufacturer X or fleet operator Y) might choose to allow full or partial software download access to their “cooperative systems units”, leaving it up to the end user (e.g. driver) to download those applications and services he would like, from any supplier. At the same time another organisation might want to restrict this access, e.g. due to safety and security issues. Both scenarios, from fully open to fully restricted software download access are supported by the CVIS architecture and its technology platform.
Each CVIS host (part of the cooperative systems unit) will “belong” to only one Host Management Centre. A service can be downloaded from an “in-house” software supplier. However, it can also be downloaded from an external service centre, as long as that host has agreement with the responsible Host Management Centre. This agreement could be realised in a form of certificate.

Figure 60: CVIS Organisational Example – Service Download

Figure 60 presents an example of organisational architecture for service download use case. Simplified, this means that there could be e.g. a Volvo Host Management Centre providing services and applications for their customers. However, even other service centres could offer services or applications thus when a Volvo driver drives to a new country there could be a new service that the driver can choose to download to it’s Volvo vehicle’s cooperative unit from a local Service centre in the new country.

13.2 COOPERS

In the COOPERS project (see http://www.coopers-ip.eu) the organisational aspects are described in following way: The organisational setting for a value chain in the area of cooperative systems or more specific of real time traffic information services to enhance road safety and traffic efficiency in a motorway network, which will be expanded to further areas in the future. It will include additional actors end entities as well as companies, stakeholders and interested parties.

13.2.1 General concept

The general outline of the value chain is related to business activities for an information services product, which will be delivered to final customers, or end users via different means and contracts. At a later stage also the bundling of certain services in one package which is attractive for the customer can also be analysed but is not the core interest in the basic outline of the organisational setting.
13.2.2 Identification of a basic Value Chain for Coopers Services

The activities necessary to provide a real-time traffic information service in the context of a large transport network are data acquisition, data processing, data distribution and data customizing. Data acquisition steps are done with the inclusion of external data sources but also with the help of external service providers, e.g., for a detailed weather forecast of a single geographic area of the network. Data processing is the main activity and will be done in a semi-automated way for the amounts of data which need to be processed and which are also needed to support and assist the highly specialized staff in the traffic control centers best in their efforts. Data distribution is completed with the support of various data network types ranging from broadcast (DAB, DVB-H) via cell based (GPRS/UMTS, WiMAX) to short and medium range networks on the road infrastructure (CALM IR and CALM M5). Hereby the network provider can be a service provider in a B2B context or also be the partner responsible for customization of the data to the end user. Data customization and servicing is the last activity in the value chain and will for most of the road safety relevant activities be in the responsibility of the infrastructure network operator and his service obligation or as a public authority or as a concessionaire operator.

13.2.3 Value Chain example for COOPERS

As one of the COOPERS examples of a value chain, which will be setup and tested from an organisational point also in the demonstrations includes: External service providers for FCD Data and weather information, TCC operator as service integrator (including all steps of the value chain: data acquisition, data processing, data distribution and data customizing).

Hereby the central role of the TCC operator reflects also his responsibility for data processing from all the different sources for a provision of correct and accurate information to the final user.
users or travellers. The data customisation is a complex task because the relevance of the
generated information is rather limited in geographic coverage and timing with the higher
customer requirements. The TCC operator needs to take care of the data network setup,
operation and maintenance as well as for service quality and enhancements. An additional
challenge for the operator is the end user expectation of a seamless service even if the legal
situation and background in the various EU member states for providing these services is
different. And there has to be made a differentiation between advanced content providers with
an already established link to road network operators and the content providers just
establishing themselves in countries which start to invest in ITS with traffic monitoring.

There are a number of other types of companies, organisations and entities which can
contribute to a value chain in the traffic information domain, and which are mentioned in the
figures, be aware that these are examples and not an exhaustive list.

13.3 SAFESPOT

BLADE sub-project has performed an in-depth analysis of organisational aspects for the
SAFESPOT cooperative system. The study produced a methodology for deriving the
Organizational Architecture for each particular configuration of the service. The Organizational
Architecture worked out within the project is currently at a preliminary stage and will be
finalized during the next months, therefore the main result so far is the setup of the
methodology, while the actual roles and their inter relations may be subject to further changes
and developments.

The Organizational Architecture design is focused on the activities belonging to the functional
area of the system and derives from a structured process during which the elementary
activities are mapped on the value chain of the service, together with the roles of the involved
actors and their responsibilities and means. The methodology, that is derived from the Italian
reference ITS architecture (ARTIST) and adapted for the SAFESPOT environment, is made of
six steps of analysis.

Instead of focusing directly on the overall SAFESPOT service, the methodology starts
considering a collection of single selected Applications; in the following step the Global System
Organizational Architecture is built as the union, or “overlap” of the single applications
structures; this approach is thought to ensure the consistency with the modular structure of
SAFESPOT, where different combinations of applications may be implemented on a single site
or vehicle, according to particular conditions of location, driving environment, morphology, or
business evaluations.

The final result of the analysis is an overall flowchart representing the system in terms of
sequence of the activities to be performed in order to supply the service, mapped on the roles
of the identified actors; a deep analysis of the single roles in terms of responsibilities, levers
and criticalities completes the work.

The Organizational Architecture scheme for the whole system shows two predominant roles,
the Infrastructure Service Provider and the Vehicle Service Provider, in charge of a significant
part of the system functionalities. The introduction of two separated units providing the
SAFESPOT service was needed in order to take into consideration different possible
scenarios; in fact the information needed by the cooperative system comes from the
infrastructure sensors and from the probe vehicles and, in the real implementation of the
system, the two parts may be managed by different entities.

The “bottom-up” approach (from the single Applications to the Global System), moreover, lead
to other significant findings: the comparison between the single Applications Organizational
schemes showed that the functionalities that are in common among the different applications
are the majority. This implies that the representation of a Global System made of a certain
group of applications actually does not differ radically from a theoretical global system
including all the developed SAFESPOT V2V and V2I applications or, which is more interesting,
from a different SAFESPOT system including a different subset of applications. In fact, in order to put in place even a small number of functionalities, the basic logical functions block would be required, and this represents a relevant part of the total available system functions. This leads to conclude that the Global System worked out in the present research, may be considered as sufficiently representative of any different "multi-application" SAFESPOT system.

The Organizational Architecture scheme shows the way these two main roles interact with the other roles during the system operations: the Public Authority, with its main institutional/regulatory responsibility, the Infrastructure Manager/Owner, with the significant responsibilities deriving from the ownership of the roadside devices, the Map Provider, in charge of the LDM static layer, and possible Value Added Service Providers. The interactions between the different actors are mainly represented by data flows from an entity to the next one along the value chain; in general, these will be ruled by dedicated contracts or agreements formalized under the needed guidelines of the local contract law.

13.3.1 Methodology: the six steps of the Organizational Architecture

The methodology for the Organizational Architecture definition defined for the SAFESPOT environment consists of six activities: two preliminary steps regard the whole system (steps 1. and 2.), while the following four specific steps regard the single applications (3. to 6.).

1. **Roles preliminary definition.** The set of roles involved in the operations of the SAFESPOT system is preliminarily determined, based on an initial analysis of the service. The difference between the concepts of “role” and “actor” used in this study is underlined here. While the role is the general function within the service (e.g. Road Manager), the actor is the actual entity, organization, company etc. covering the role (e.g. ANAS SpA). This important distinction brings some significant implications: the same actor, for example, can cover more roles (e.g. ANAS SpA is the Road Manager for a portion of road network and also the Service Provider for a certain ITS application). On the other hand, the same role can be filled by more entities (e.g. two different companies act as Content Provider for a certain service).

2. **Definition of the global SAFESPOT system Value Chain** (macro-process), applying the traditional arrow diagram to represent the high-level processes involved in service delivery. Breaking down the business unit into its main strategic activities makes it possible to distinguish the behaviour of costs and the associated generated value. In this context, the general concepts are transposed in order to reach the prefixed objective: providing a general vision on how the telematic services are supplied, and to detect the path of the value generation, thus evaluating the real feasibility and possibility to supply the service. The following picture shows the value chain of the macro-process with the typical arrow-diagram.

![The SAFESPOT system Value Chain](image)
3. **Identifying the set of functions**, derived from the Functional Architecture of the single applications, which form the sequence of operations needed to run the service. This step is the first performed separately for every single application, and consists of splitting every single chain mail (the processes) into sub-processes/activities (or functions of the Logical Architecture).

Each macro activity of the macro process value chain, can be divided into sub-processes/activities, corresponding to what is set by the Logical Architecture. This partition is needed for the correct assignment of the activities to a certain chain mail and thus to a certain role. Within SAFESPOT, this step started from the analysis of the single applications Functional Architecture logical functions.

The functional architecture diagrams, provided by the applications developers, show the basic functionalities of the system and the way they are related to each other in terms of input and output, via the proper data exchanges. The Data Flow Diagrams, that represent these relations, are composed of functional blocks (square boxes) and data flows (arrows). In practice, in order to simplify the graphical representation (see step number 5) and to make the Organizational Architecture schemes uniform in view of being overlapped for the global architecture, some adaptations are made. The set of functional blocks used to build the Organizational Architecture was adapted also in order to be compliant with the overall architecture defined at IP level.

4. **Mapping the sub-processes on the macro-process** activities identified in the preliminary steps. After the simplification and “harmonization” process is performed on the logical functions of the applications, the detected sub-processes/activities are positioned on the value chain, to build what is called “sub-processes diagram”.

The diagram depicts the value chain and all the activities or sub-activities positioned on the single rings of the chain.
### The value chain for the SAFESPOT system with the sub-processes mapped on the single rings

<table>
<thead>
<tr>
<th>Service Provider</th>
<th>Detection</th>
<th>Processing</th>
<th>Alert</th>
<th>Driver</th>
</tr>
</thead>
<tbody>
<tr>
<td>SF.01_Update circulation rules</td>
<td>SF.16_Query LDM-RSU info</td>
<td>SF.27_Verify SF TLC actuation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SF.22_Update static map</td>
<td>SF.15_Query LDM-VEH info</td>
<td>SF.28_Actuate TLC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SF.02_Provide circulation rules</td>
<td>SF.13_Data fusion &amp; update LDM-RSU</td>
<td>SF.20_Send msg to VANET from roadside</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SF.03_Provide vehicle dynamics from infrastructure</td>
<td>SF.14_Data fusion &amp; update LDM-VEH</td>
<td>SF.23_Alert driver on board</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SF.11_Detect road status roadside</td>
<td>SF.17_Generate msg for VANET roadside</td>
<td>SF.25_Valculate warning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SF.12_Detect weather info roadside</td>
<td>SF.20_Send msg to VANET from roadside</td>
<td>SF.24_Display warning on VMS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SF.30_Detect visibility roadside</td>
<td>SF.18_Generate message for VANET on board</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SF.31_Detect traffic roadside</td>
<td>SF.21_Send msg to VANET from veh</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SF.04_Provide vehicle dynamics from vehicle</td>
<td>SF.19_In-vehicle SP5 application client</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SF.05_Provide vehicle other info from vehicle</td>
<td>SF.60_Determine Safety Margin I2V</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SF.06_Provide static road geometry &amp; ITS devices</td>
<td>SF.61_Determine Safety Margin V2V</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SF.07_Provide events info</td>
<td>SF.26_Provide TLC planning info</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SF.29_Provide TLC status</td>
<td>SF.08_Provide external safety-related info</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SF.22_Update static map</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. **Designing the overall process flowchart.** Once the functionalities to be supplied and the involved roles are defined (respectively at steps 1 and 3), the flow of activities needed for the service supply at the single application level is designed, grouping the functionalities by roles, hence putting in evidence the pertinences. This vision is a deepening of the concept of value chain. A dedicated diagram, where for each role the corresponding Value Activities are assigned, is built in order to make the relationship between Roles and Value Activities immediately usable; this activity represents a basis for the definition of the levers and responsibilities.

The diagram contains the activity flows with the exchange of the macro-data that are related to the corresponding macro-functions, as a guide for the correct sequence of the activities.
The SAFESPOT organizational scheme
6. **Describing the roles and their means/responsibilities.**

In this step the roles needed for the implementation of the activities inside the chain mails (i.e. the single elements of the value chain) are better defined, considering the inter-relationships that have emerged in step 5 and the different functionalities in charge of each one.

The responsibilities are detected such that each role has to implement its own activities, and the levers to make his job operationally effective. The possible criticalities to physically fulfil these responsibilities are also searched.

In this context the term “responsibility” is used in its widest meaning, that is as the moral or legal duty of a person or company to answer for the harmful effects of his or others’ actions; specifically the term responsibility is used to refer to the commitments of a service supply to the next role of the chain or the final user.

The responsibilities are grouped according to the following views:

- **Institutional normative responsibility;** attaining to the responsibilities deriving from the definition of the normative/procedural frame that rules the service/role field
- **Management Responsibility (Governance);** attaining to the responsibilities in terms of correct management of the business levers determining the expected value.
- **Commercial Responsibility;** attaining to the responsibilities to supply the services/products required by the market according to the user needs.
- **Delivery Responsibility;** attaining the responsibilities in terms of services/products supply in line with the service and quality levels determined at a contractual stage.

This kind of approach allows to evaluate the crossover between activities (functions) and responsibilities and to define consequently the corresponding roles, which are the basis of the following definition of the levers.

The detected levers can be of economic, politic, legal, technological nature, but also professional skills and workforce.

Moreover, in the analysis of the whole value chain it is clear that some activities depend on data and information (inputs) coming from terminators that are external to the chain itself.

The complete list of the identified roles is reported below.

- **Public Authority.** This role has the responsibility for the transport network and an interest in the safety of the traveling public as a whole (e.g. Ministry of Transports).

- **Infrastructure SAFESPOT Service Provider.** This role has the task of managing the SAFESPOT system on a certain portion of road network, and possibly, but not necessarily, is covered by the same entity acting as the infrastructure manager/owner. This includes running the infrastructure platform system operations and ensuring its functionality.

- **Vehicle SAFESPOT Service Provider.** The actor covering this role will be responsible for managing the data coming from the vehicles, including taking in charge the on-board vehicle system and the communications with the rest of the system. At this stage of the project, it is still not clear what possible entity will likely be covering this role; this will depend on several factors, for example regarding the sale/installation of the on-board equipment (by the vehicle producer only or also as a retrofit product?). The possibility that this role may be covered by the Infrastructure SAFESPOT Service Provider, should also be discussed. This may be an issue given that, in the long term,
the vehicle on board units are supposed to comply with different SAFESPOT-infrastructureroad networks along Europe.

- **Infrastructure Manager/Owner.** Body or organization (public or private) responsible for managing the road infrastructure, i.e. motorway operator, road authority, etc.

- **Map Provider.** An organization responsible for collecting, processing, certificating and providing Geo-referenced Data. The Map Provider is the supplier of the static LDM layer.

- **Value Added Service Provider.** An organization responsible for providing transport-related services, which are external to SAFESPOT, to road users. These can include the safety-related services as well as general information, emergency support for drivers, monitoring services, weather information, etc.

In the following paragraphs some examples of roles definition are reported.

**Infrastructure SF Service Provider**

**Functionalities**

The functionalities in charge of the Infrastructure SF Service Provider include:

- SF.03_Provide vehicle dynamics from infrastructure
- SF.11_Detect road status roadside
- SF.12_Detect weather info roadside
- SF.30_Detect visibility roadside
- SF.31_Detect traffic roadside
- SF.13_Data fusion & update LDM-RSU
- SF.16_Query LDM-RSU info
- SF.60_Determine Safety Margin – I2V
- SF.17_Generate message for VANET roadside
- SF.20_Send message to VANET from roadside

The first functionalities are dedicated to the detection of the measures needed by the system from the road sensors (road status and weather, vehicle dynamics from the Laserscanner system or the camera-based object detection module). The next functions are dedicated to the interaction with the RSU LDM (processing, upload and extraction). The last two functional blocks regard the transmission of the information about the danger to the VANET, as to send the message to the single vehicles on-board HMI.

The Infrastructure Service Provider role will be covered by any entity taking in charge the management of the SAFESPOT road-based part of the system on a certain portion of road network. In most cases this entity would likely be the Infrastructure Manager, but there may also be the option it is a different organization, for example a company managing the ITS systems in a city area.

**Responsibilities**

This role shares with the SF Vehicle Service Provider the fundamental responsibility of Delivery of the service (red prolongation, safety alert on board) to the final user (driver); in fact a significant part of real-time information feeding the application (the vehicle dynamics, the road status, the weather information), is detected via the roadside sensors, processed by the Road Side Unit, and sent to the VANET from the RSU router. The responsibility Delivery of safety information to the driver can be seen as decomposed into the single steps from one single ring of the system chain to the following one: the detection system to the RSU, the RSU
to the router or to the respective platform alert system or actuators, the router to the vehicles. In
general the Delivery responsibility is a delicate issue, since timing plays a fundamental role in
the safety related alert provision. An average and maximum delay will need to be defined from
the moment the safety related event happens to the moment the driver is alerted. Also, the
Infrastructure Service Provider shall be able to quantify the delivery timing of the critical
information provided to the following steps within the system information flow sequence, in
order to monitor its compliance to the limit delays. Two particular critical steps under the timing
point of view are the query mechanism to extract the needed data from the RSU and the
process of dispatching-validating-displaying the alerts on the VMSs for the applications where
this is required. In this latest case the role of Infrastructure Manager/Owner is involved as well
(see OA diagram).

Since input data may come not only from the SAFESPOT sensors but also be communicated
by external organizations, the way this exchange of information is ruled is also very important.
The RSU receives information (that may also be real-time) from the VASP role, therefore
proper agreements will be needed for this data transfer; a periodic update needs to be
provided also by the Map Provider, from which the Infrastructure Service Provider will need
prompt update in case of static road geometry changes. More information may come from the
Infrastructure Manager as well; this would imply extra agreements on this information
exchange.

Another important aspect to be taken into account for the Delivery responsibility is data
reliability; the information should comply defined limits of precision and accuracy when
delivered from detection systems to the RSU, from the RSU to the VANET.

The Infrastructure Service Provider, finally, is charged of a major Management responsibility of
the system, since some of the physical devices and external organizations upon which the
system relies are under its control.

Levers

The main levers for the Delivery responsibility are technical-related. The timing and reliability of
data will strongly depend upon the efficiency of the technological supports, the processing
techniques, the communication devices.

The other important lever for the Delivery responsibility, both in terms of timing and data
reliability, are the contracts set up between this role and those acting as information suppliers
(VASP, Map Provider, Infrastructure Manager, Vehicle Service Provider) and information
clients (Vehicle Service Provider through the VANET and Infrastructure Manager for the alert
visualization via the roadside alert equipment or actuation). Any synergies with other safety
systems installed on the same platform (e.g. CVIS) would significantly decrease the costs and
therefore improve the value.

Criticalities

The critical aspects for this role are those involving the supply well-timed and reliable
information to the driver. The Infrastructure Service Provider, together with the Vehicle Service
Provider, is the interface between the system and the user; moreover, the SAFESPOT system
will be successful inasmuch as the driver will modify its behaviour according to the alert
messages. Since this will happen proportionally to the confidence that the he will have in the
reliability of the messages he will receive, it is easy to understand that a major focus has to be
given at all levels, included the organizational one, in order to reach the highest possible level
of trust of the driver towards the system. Several aspects will be involved in this goal other than
the timing and the reliability of the alerts: the homogeneity of the warning in time and space, the
information on the current functioning status of the system; on the other hand, the risk of over
compliance of the driver towards the system may have dangerous effects as well.
**Infrastructure Manager/Owner**

**Functionalities**

Functional blocks in charge of the Infrastructure Manager:

- SF.02_Provide circulation rules
- SF.06_Provide static road geometry & ITS devices
- SF.07_Provide events info
- SF.24_Display warning on VMS
- SF.25_Validate warning
- SF.26_Provide TLC planning info
- SF.27_Validate SF TLC actuation
- SF.28_Actuate TLC
- SF.29_Provide TLC status

The role of Infrastructure Manager includes a series of functions for the data supply, either quasi-static (updates on circulation rules from the Public Authority, updates on road geometry) or dynamic (traffic lights status, events or measures detected by safety systems installed on the infrastructure other than the SAFESPOT system).

The other group of functions is related to the warning display on the road based devices (VMS) and the management of the red prolongation at the TLC system level.

**Responsibilities**

As the supplier of part of the data needed to run the application (SF.06, SF.07, SF.26), the Infrastructure Manager holds the responsibility to deliver data in the required time and with the required reliability (Delivery responsibility). The same responsibility is assigned to this role when the warning message to reduce speed is delivered to the driver through the VMSs or the red prolongation is implemented. In fact, in case other TLC control or warning systems are operating on the same portion of network, the Infrastructure Manager will use automated procedures in order to verify if the SAFESPOT alerts or traffic lights controls are compliant with possible other actions on the same area, and, if needed, set the proper priorities. However, for the “pure” V2V applications (i.e. where no roadside alert or actuation is planned) the Infrastructure Manager has no responsibility on the delivery of the alert to the driver.

Moreover, as pointed out in D6.4.2 (Legal Aspects of SAFESPOT Systems), the Road Manager may be, within the boundaries set by the national legislator (and international treaties) responsible for setting speed limits for the roads within its jurisdiction (Speed Alert Consortium, 2004). In this case this role will detain as well a Normative responsibility.

**Lever**

As for the information detection side (first three functions), the main lever at disposal of the Infrastructure Manager in order to fulfil its Delivery responsibility is the ownership of the original data, allowing the control on the information timing and reliability. As for the red-phase prolongation and the warning displaying on the VMSs, the Infrastructure manager role holds the last “filter” before the control or warning is put in place, therefore he can adjust the level of “impact” of the SAFESPOT system according to the situations.

**Criticalities**

An important critical point has to be considered for this role. Introducing a new system for road safety on a certain portion of network may be regarded with some distrust by a road manager correspondingly to the responsibility that would be imputed to him in case of malfunctioning of the system, possibly causing any damage to drivers. Although this issue is deeply dealt within the legal aspects analysis, it shall be considered as a major concern also for its implications on
some organizational aspects, in particular on the contracts regulating the exchange of information between this role and the other actors.

It remains to be seen whether the chosen methodology is flexible enough in practice to deal with the fact that there are many motivations for stakeholders to invest (or not) in cooperative systems such as SAFESPOT and the assumption that the possible benefits of the system are largely macroscopic in nature. The latter implies that the tangible benefits could be lower and this could influence investment decisions.
## 14 Implemented Software Frameworks and Components

### 14.1 Overview table on available hardware and software

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Project</th>
<th>Company</th>
<th>Contact</th>
<th>Information Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Platforms</td>
<td>On Board Unit Prototype</td>
<td>CVIS (EU)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Road Side Unit Prototype</td>
<td>Aktiv (German)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OBU (Car PC and Software)</td>
<td>COOPERS (EU)</td>
<td>ARS T&amp;TT</td>
<td>Jan Linssen</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication Platforms</td>
<td>Gateway Prototype</td>
<td>COOPERS (EU)</td>
<td>Efkon</td>
<td>Andreas Schalk</td>
<td></td>
</tr>
<tr>
<td>IEEE802.11p/1609</td>
<td>VII (US)</td>
<td>DENSO</td>
<td>Dr. Bert Böddeker</td>
<td></td>
<td>Pre-commercial, samples for testing available</td>
</tr>
<tr>
<td>IEEE802.11p/1609</td>
<td></td>
<td>Renesas</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEEE802.11p</td>
<td></td>
<td>Siemens</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEEE802.11p</td>
<td></td>
<td>Mira</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Development Frameworks</td>
<td>Open WAVE Engine</td>
<td>Aktiv (German)</td>
<td>BMW Group</td>
<td>Dr. Peter Zahn</td>
<td>“Community License”, Flyer and Usage Rules available from contact person, NDA required</td>
</tr>
<tr>
<td>Viilab</td>
<td>Commercial</td>
<td>Carhs</td>
<td>Dr. Alois Mauthofer</td>
<td></td>
<td>Commercial</td>
</tr>
<tr>
<td>Software Network Protocols</td>
<td>Car2X SDK (<a href="http://c2x-sdk.neclab.eu/">http://c2x-sdk.neclab.eu/</a>)</td>
<td>NOW</td>
<td>NEC</td>
<td>Dr. Andreas Festag</td>
<td></td>
</tr>
<tr>
<td>Roadside gateway</td>
<td>CVIS (EU)</td>
<td>Peek, Siemens</td>
<td>Eric Koenders</td>
<td></td>
<td>API under BSD license</td>
</tr>
<tr>
<td>Roadside Unit</td>
<td>COOPERS (EU)</td>
<td>SWARCO/ Mizar</td>
<td>Gino Franco</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
14.2 System Platforms

On-board unit prototype (CVIS)

The CVIS ITS Vehicle Station: Application Host and Gateway

Hard- and Software Configuration (COOPERS)
14.3 Communication Platforms

A COOPERS vehicle station: Gateway prototype (COOPERS / Efkon)

Prototypes of vehicle station mobile routers from Renesas and DENSO:

IEEE802.11p / 1609 (Renesas)
14.4 Software Frameworks & Modules

ACUp Open WAVE Engine

The ACUp has been developed as an evaluation and test framework for c2x – communication concepts, strategies and ideas. It considers the current standards from the C2C-CC and the Network on Wheels Project. The main focus of this framework is:

- Flexibility,
- Extensibility,
- Scalability,
- Ready for future usage.

This means that fast prototyping of safety and traffic efficiency applications and c2x communication stack concepts has been enabled. The ACUp framework has been designed to expedite the standardisation process by fast evaluation of ideas.
14.5 Software Abstraction

14.5.1 Roadside Gateway

The Roadside Gateway defines an interface which connects traffic controllers to cooperative applications in CVIS and SAFESPOT.

Data describing the current state of an intersection (Signal head states, detectors, pushbuttons etc.) is provided to the cooperative system through a well known API (Application Programming Interface).

Requests from applications for specific traffic control functions (for example a priority request) are also sent through the API towards the traffic controller, and replies are sent back.

The API is developed in a joint effort by Peek Traffic and Siemens. It is available as a Java interface which can be accessed locally or through SOAP.

Information from a traffic controller is passed to the Gateway API in an OEM specific way (for example via a proprietary interface, or through a network via SOAP). Before entering the Gateway API the information must be translated into the format prescribed by the API.

At the other side of the API (the cooperative implementation of the interface) the information is handed over to the data fusion components and finally to the LDM, or to the applications directly, dependant on the type of information.

By defining a general API, traffic controllers of various brands and models can all be connected to a cooperative system. The way a traffic controller is connected to the cooperative system is intentionally undefined. This leaves room for differences in implementation and capabilities of the various traffic controllers. For example the Peek EC-2 traffic controller is connected via a proprietary TCP/IP/IPV4 based protocol. This protocol is translated into the Gateway API by a Java program in the cooperative host. The Siemens traffic controller is connected by means of a separate processor which translates a proprietary protocol into SOAP Gateway API messages.
14.5.2 Roadside Station

The roadside station developed in COOPERS by Swarco connects existing motorway controllers to Traffic Control Centers and enhances their functionalities with an I2V communication link based on CALM and several communication technologies and channels.
15 Common Demonstration

To round off this common architecture document, we discuss the organisation of possible events to demonstrate interoperability amongst the various solutions emerging from both nationally and EU-funded research projects as well as from industry initiatives such as Car-to-Car Communication Consortium. These events aim at showcasing the achievements of the above projects and related products and services, and to raise awareness amongst both professional and general public audiences.

The importance of interoperability for future market development is underlined by the risks of not achieving interoperability: in case different brands of vehicle could not communicate with each other, or if a driver’s vehicle could not identify and access services provided in another city than his home town, or in another country, the local cooperative services would simply never spread out across the country, or across Europe, leading to fully mature deployment.

We discuss here three main opportunities for common demonstration events that arise in the next few years. These are:

1. Coordinated demonstrations at common EU project test sites;
2. Coordinated demonstrations and other activities at the ITS World Congress in Stockholm, in September 2009;
3. A dedicated European Showcase for Cooperative Systems to be held in the first half of 2010, at a location to be selected.

15.1 Common test sites

To plan for possible coordinated activities at projects’ test sites it is necessary first to establish which projects will test which applications at which physical location, and with which roadside infrastructure, vehicles and communication means.

It will also be necessary to plan a coordinated test campaign at any site(s) selected for common demonstration. This should be built up on the basis of agreed test use cases and scenarios. As of today three common use cases have been selected and described by the three projects CVIS, SAFESPOT and COOPERS:

- Slippery road warning
- Component download
- Emergency vehicle priority.

It appears that there is potential to test interoperability at at least the single test site (Netherlands-Belgium) common to all three projects. Further analysis is being carried out to establish to a deeper level just what can (and cannot) be compared, allowing for the technology implemented by each project. Figure 63 shows the planned demonstration sites of the projects COOPERS, CVIS and SAFESPOT.
Figure 63: Demonstration Sites COOPERS, CVIS and SAFESPO
The following table shows possible interoperability between CVIS applications and other projects in different CVIS test sites.

<table>
<thead>
<tr>
<th>Test site country</th>
<th>Application</th>
<th>Location &amp; site description</th>
<th>Vehicles / to be shared</th>
<th>Equipment / to be shared</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVIS</td>
<td>SAFESPOT</td>
<td>COOPERS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>France</td>
<td>?</td>
<td></td>
<td></td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>Germany</td>
<td>COMO Data?</td>
<td>Dynamic black spot</td>
<td>Dortmund / ?</td>
<td>No</td>
<td>?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>It will be demonstrated in CVIS test sites</td>
</tr>
<tr>
<td>NL-B</td>
<td>CURB Priority</td>
<td>Intersection application</td>
<td>?</td>
<td>Helmond / ?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The SAFESPOT and CVIS test location lie in the same place</td>
</tr>
<tr>
<td>Italy</td>
<td>?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sweden</td>
<td>COMO data</td>
<td>Slippery Road</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>UK</td>
<td></td>
<td>London</td>
<td></td>
<td></td>
<td>No plans</td>
</tr>
</tbody>
</table>
15.2 Common demonstration at ITS World Congress Stockholm

The next ITS World Congress to be held in Europe will be in Stockholm from 21-25 September 2009. This is soon after the trials should be completed at each of the project’s test sites, and when technical developments should have been both completed and even revised in the light of the trials in each project.

The Congress will provide facilities for normal conference sessions, for both static displays and also some innovative dynamic activities in the exhibition hall, and for a variety of demonstrations both indoors and outdoors at the conference centre, and also at some test facilities reachable on a technical tour. All these features are still to be finalised, but their potential is already clear.

It appears that the following possibilities will be offered:

- Large video screens in the exhibition area on which live relays from test sites across Europe could be shown, in real time. This could be based on a coordinated programme from more than one project, e.g. to feature specific common technical issues or applications;
- An indoor “ITS Theatre” where scripted scenarios could be brought to life using professional help, as part of a sort of theatrical programme. This too could be arranged to show a coordinated set of scenarios, such as those mentioned above for the test site demonstrations;
- Individual exhibitors’ stands may feature each project’s results, or also grouped displays based on more than one project. This might work best on the stands of exhibitors present in multiple projects. The EC is expected also to provide a stand where EU funded projects could show off their results – this might feature a “cooperative systems corner” grouping these projects together;
- In a covered demonstration area outside the congress centre there will be a small but realistic roadway with basic traffic management features and where small electric vehicles can be demonstrated interacting with the infrastructure. The different IPs could arrange for a common demonstrator to show off the common scenarios or some other achievements;
- Going further a field, there will be technical tours to surrounding test tracks, e.g. at Scania. Here it will be possible to bring vehicles from the three IPs and to show off a number of scenarios, perhaps including the core three interoperability case studies.

The next task is for each project to put forward its plan for Stockholm, and to see if there is interest and potential for any common activities to highlight the common benefits and value of the applications shown, or for demonstrations of hardware and software interoperability.

15.3 Cooperative systems showcase event, spring 2010

Plans are underway to hold a major European event on the theme of cooperative system technologies, applications and services, as well as issues such as deployment.

This should be a world-class demonstration event, combined with an exhibition and symposium, and should feature the achievements of the EU-supported R&D projects such as CVIS, SAFESPOT and COOPERS, and other recent, current and planned national R&D programmes such as AKTIV, SIM-TD, IVSS, and also the Car-to-Car Communication Consortium.

The demonstrations will aim to convince the event’s participants (professionals, politicians, general public) by hands-on experience of the potential benefits and value of cooperative systems, and their utility as tools for public policies. A high political profile is needed.

The event should focus on vehicle-to-vehicle and vehicle-to-infrastructure communications, and their applications/services for urban, interurban and commercial and public transport domains.
Elements to be demonstrated should include roadside infrastructure and interfaces, in-vehicle hardware and HMI, control and service centre hardware and software, etc. Trial vehicles should operate on express and urban roads as well as in an off-road test track.

The event should include an international symposium, an extensive exhibition and vehicle demonstrations. Target timing is spring 2010, a period relatively free of overlaps with other ITS events such as the European congress in Thessaloniki (June 2010) and the TRA European Research Arena in Brussels (June 2010).

The location should be selected by an open competition, according to criteria of accessibility, suitability & quality of facilities, local support and finance, possible synergies etc. Cost is likely to be at least €2M, with revenue expected from EU and local support, EC project budgets, sponsorship and exhibition sales.

The organisation of this Showcase will be the responsibility of a project team, guided by a steering board drawn from key actors involved in current R&D projects, cooperative system industries, and public bodies (e.g. EC).
Annex 1  List of References used in each of the chapters

Chapter 2: Policies


2. Directives under the European Type Approval Framework:


5. Commission Recommendation for HMI:
   Commission Recommendation of 22 December 2006 on safe and efficient in-vehicle information and communication systems

6. Standard ETSI EN 302571
   Intelligent Transport Systems (ITS); Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive

7. Code of Practise, PREVENT Response 3:

8. UN/ECE Regulations:
   Regulation 10: Uniform provisions concerning the approval of vehicles with regard to electromagnetic compatibility.
   Regulation 60: Uniform provisions concerning the approval of two-wheeled motorcycles and mopeds with regard to driver-operated controls including the identification of controls, tell-tales and indicators
   Regulation 121: Uniform provisions concerning the approval of vehicles with regard to the location and identification of hand controls, tell-tales and indicators.

Chapter 5: Stakeholder Aspirations, User Needs, Requirements

The documents referred to in this chapter are provided separately. Their details can be found in Annex 2 to this document.
Chapter 6: Overall Framework, Actors, Terminators and Entities

The following documents contain details of the abbreviations used by CVIS:
9. D.CVIS.3.2 – High Level Architecture
10. D.CVIS.2.2 – Use Cases and System Requirements
11. D.COMM.2.1– Use Cases and System Requirements
12. D.FOMA.2.1– Use Cases and System Requirements
13. D.POMA.2.1– Use Cases and System Requirements
14. D.COMO.2.1– Use Cases and System Requirements
15. D.CURB.2.1– Use Cases and System Requirements
16. D.CINT.2.1– Use Cases and System Requirements
17. D.CF&F.2.1– Use Cases and System Requirements

Terminology
21. D.CVIS.2.2 – Use Cases and System Requirements

Stakeholders and actors
26. D.CVIS.2.2 – Use Cases and System Requirements

Chapter 7: Architectural Views

27. [FRAME1]: European ITS Framework Architecture, FRAME Selection Tool, User Handbook, Version 1, April 2004
29. [COOPERS1]: COOPERS_D13-B-IR3100-2 Report on ITS Reference Architecture
30. [CVIS] D.COMM.3.1 Architecture and System Specifications
31. [SAFESPOT] D7.2.1 Core Architecture Requirements v2.2
32. [CAR2CAR1]: CAR 2 CAR Communication Consortium Manifesto
Chapter 8: Access Technologies

33. ECC Report 101: Compatibility studies in the band 5855–5925 MHz between Intelligent Transport Systems (ITS) and other systems
34. ECC/DEC/(08)01: ITS in 5 GHz band ECC Decision of 14 March 2008 on the harmonised use of the 5875-5925 MHz frequency band for Intelligent Transport Systems (ITS)
35. ECC/REC/(08)01: Use of the band 5855-5875 MHz for Intelligent Transport
37. ETSI prEN 302 571: Intelligent Transport Systems (ITS); Radio communications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive
39. Draft ETSI EN 302 571 V1.1.1 (2008-05) Harmonized European Standard (Telecommunications series) Intelligent Transport Systems (ITS); Radio communications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive
40. www.wikipedia.org
41. CVIS COMM Architecture D.COMM.3.x
42. COOPERS internal report: “Analysis of impact on communication links”, version 4.7
43. C2C-CC manifesto

Chapter 11: Security

## Annex 2 Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C2C-CC</td>
<td>Car to Car Communication Consortium</td>
</tr>
<tr>
<td>CEN</td>
<td>European Committee for standardisation</td>
</tr>
<tr>
<td>CEPT</td>
<td>Conference of European Postal &amp; Telecommunications</td>
</tr>
<tr>
<td>DAB</td>
<td>Digital Audio Broadcast</td>
</tr>
<tr>
<td>DEC</td>
<td>A DECision made by ECC</td>
</tr>
<tr>
<td>DFS</td>
<td>Dynamic Frequency Selection</td>
</tr>
<tr>
<td>DLL</td>
<td>Data Link Layer</td>
</tr>
<tr>
<td>DMB</td>
<td>Digital Multimedia Broadcast</td>
</tr>
<tr>
<td>DSRC</td>
<td>Dedicated Short Range Communications</td>
</tr>
<tr>
<td>DVB-H</td>
<td>Digital Video Broadcast – Personal Station</td>
</tr>
<tr>
<td>DVB-T</td>
<td>DVB-T Digital Video Broadcast - Terrestrial</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>ECC</td>
<td>Electronic Communications Committee (European)</td>
</tr>
<tr>
<td>EIRP</td>
<td>Equivalent Isotropic Radiated Power</td>
</tr>
<tr>
<td>ERM</td>
<td>Electromagnetic compatibility and Radio spectrum Matters</td>
</tr>
<tr>
<td>ETC</td>
<td>Electronic Toll Collection</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standards Institute</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>FWA</td>
<td>Fixed Wireless Access</td>
</tr>
<tr>
<td>GPRS</td>
<td>General Packet Radio Service</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile Communications</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers (American standardisation body)</td>
</tr>
<tr>
<td>IR</td>
<td>Infrared</td>
</tr>
<tr>
<td>IRIS</td>
<td>Intelligent coopeRative Intersection Safety</td>
</tr>
<tr>
<td>ISM Band</td>
<td>Industrial, Scientific and Medical Band</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>ITS</td>
<td>Intelligent Transport Systems</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>IVC</td>
<td>Inter Vehicle Communications</td>
</tr>
<tr>
<td>MAC</td>
<td>Medium Access Control</td>
</tr>
<tr>
<td>MAN</td>
<td>Metropolitan Area Networks</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnection Basic Reference Model</td>
</tr>
<tr>
<td>PHY</td>
<td>Physical Layer</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RSU</td>
<td>Roadside Unit</td>
</tr>
<tr>
<td>R2V</td>
<td>Roadside to Vehicle Communications</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>SRD</td>
<td>Short Range Device</td>
</tr>
<tr>
<td>SRD-MG</td>
<td>Short Range Device Maintenance Group</td>
</tr>
<tr>
<td>SRDoc</td>
<td>System Reference Document</td>
</tr>
<tr>
<td>TC</td>
<td>Technical Committee</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmitter Power Control</td>
</tr>
<tr>
<td>TG</td>
<td>Technical Group</td>
</tr>
<tr>
<td>TPC</td>
<td>Transmit Power Control</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunications System</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
</tbody>
</table>
Annex 3  List of Annexes in separate documents

[Annex 2-1]  Communications Technologies for Cooperative Systems
  → COMeSafety_COM_ARCH_FRAME_Annex_2-1.doc

  → COMeSafety_COM_ARCH_FRAME_Annex_5-1 Combined Requirements Specification.doc

[Annex 5-2]  CVIS Requirements
  → COMeSafety_COM_ARCH_FRAME_Annex_5-2 CVIS Req.doc

[Annex 5-3]  SAFESPOT Requirements
  → COMeSafety_COM_ARCH_FRAME_Annex_5-3 SAFESPOT Req.doc

[Annex 5-4]  COOPERS Requirements
  → COMeSafety_COM_ARCH_FRAME_Annex_5-4 COOPERS Serv.doc

  → COMeSafety_COM_ARCH_FRAME_Annex_5-5 Fame UN Req.doc

  → COMeSafety_COM_ARCH_FRAME_Annex_5-6 New Fame UN Req.doc

  → COMeSafety_COM_ARCH_FRAME_Annex_5-7 Mapped Fame UN Req.doc

[Annex 10-1]  Data and Messages Descriptions (Messages Catalogue)
  → COMeSafety_COM_ARCH_FRAME_Annex_10-1.doc

[Annex 10-2]  Covariance Matrix
  → COMeSafety_COM_ARCH_FRAME_Annex_10-2.doc
# Annex 4  Chapters and Chapter Editors

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Editor/Editors</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  Introduction</td>
<td>Ilse Kulp, All</td>
</tr>
<tr>
<td>2  Policies</td>
<td>European Commission</td>
</tr>
<tr>
<td>3  Architectural Description</td>
<td>Thierry Ernst</td>
</tr>
<tr>
<td>4  Scenarios, Applications, Use Cases</td>
<td>Abdel-Kader Mokkadem</td>
</tr>
<tr>
<td>5  Stakeholder Aspirations, User Needs, Requirements</td>
<td>Richard Bossom, Ilse Kulp</td>
</tr>
<tr>
<td>6  Overall Framework: Actors, Terminators and Entities</td>
<td>Zeljko Jeftic</td>
</tr>
<tr>
<td>7  Architectural Views</td>
<td>Alexander Frötscher</td>
</tr>
<tr>
<td>8  Access Technologies</td>
<td>Elisabeth Uhlemann</td>
</tr>
<tr>
<td>9  Networking and Transport</td>
<td>Andreas Schalk</td>
</tr>
<tr>
<td>10 Facilities</td>
<td>Roberto Brignolo</td>
</tr>
<tr>
<td>11 Security</td>
<td>Antonio Kung</td>
</tr>
<tr>
<td>12 System Management</td>
<td>Knut Evensen</td>
</tr>
<tr>
<td>13 Organisational Topics</td>
<td>Zeljko Jeftic</td>
</tr>
<tr>
<td>14 Implemented Software Frameworks and Components</td>
<td>Timo Kosch</td>
</tr>
<tr>
<td>15 Common Demonstration</td>
<td>Paul Kompfner</td>
</tr>
</tbody>
</table>