Communication Technologies for Cybercars and Advanced City Vehicles

<table>
<thead>
<tr>
<th>Deliverable no.</th>
<th>3.4.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dissemination level</td>
<td>Public</td>
</tr>
<tr>
<td>Work Package</td>
<td>3.4 Cooperative vehicles and navigation</td>
</tr>
<tr>
<td>Author(s)</td>
<td>Michel Parent</td>
</tr>
<tr>
<td>Co-author(s)</td>
<td>Hamada Alshaer, Matteo Viarengo, Joseph Canou, Jennie Lioris</td>
</tr>
<tr>
<td>Status (F: final, D: draft)</td>
<td>F1_01.11.2007</td>
</tr>
<tr>
<td>File Name</td>
<td>D3.4.2-PU-Comm_Technologies_Cybercars&amp;ACV-FINAL-Parent-30-08-08.doc</td>
</tr>
<tr>
<td>Project Start Date and Duration</td>
<td>01 May 2006 - 30 April 2011</td>
</tr>
</tbody>
</table>
### TABLE OF CONTENTS

1. Executive Summary .................................................. 4
2. Introduction ............................................................ 4
3. Requirements For Vehicular Communication .................. 5
   3.1 Vehicular Traffic Classification ............................... 5
      3.1.1 Static and Dynamic Data ................................. 5
      3.1.2 Elastic and Non-Elastic Traffic ......................... 5
   3.2 Communication Technologies .................................. 6
      3.2.1 Wireless Communication Technologies .................. 6
      3.2.2 Radio Communication Technologies ..................... 7
   3.3 Vehicular Message Propagation ............................... 8
      3.3.1 Rules Based Forwarding Algorithms ..................... 9
   3.4 Vehicle Ad hoc Network Protocols .......................... 9
      3.4.1 Mobility Sensibility .................................... 10
      3.4.2 QoS Provision ........................................... 10
      3.4.3 Topology Based Routing Protocols ...................... 10
      3.4.4 Geocast Routing Protocols .............................. 10
      3.4.5 Network Clustering Based Routing Protocols ............ 11
      3.4.6 Broadcast Protocols .................................... 11
   3.5 Vehicle to Infrastructure Communication ................... 12
      3.5.1 IP unified Network ...................................... 12
      3.5.2 Mobile IPv6 .............................................. 13
      3.5.3 Mobile Network Protocols ............................... 13
      3.5.4 V2I and V2V Integration ................................ 14
      3.5.5 Continuous Air-Interface for Long and Medium Range Communication (CALM) ............................... 14
      3.5.6 Vehicle Connection to Internet ......................... 14
4. Requirements for communication technologies according to scenarios .................................................. 16
   4.1 Town centre ..................................................... 16
      4.1.1 Data types ............................................... 16
      4.1.2 Priority and network propagation area .................. 16
      4.1.3 Reliability and probability of reception ............... 17
      4.1.4 Communication security .................................. 18
   4.2 Principal urban roads with an equipped lane (called “e-lane”) ......................................................... 18
   4.3 Inner city centre ............................................... 18
   4.4 Shared traffic space with automated buses and dual mode vehicles ..................................................... 19
5. Evaluation of maximum throughputs ............................. 21
   5.1 Deterministic Model ........................................... 21
   5.2 Stochastic Model ................................................ 22
   5.3 Fundamental graphs for a system of two circular roads-one crossing ......................................................... 23
      5.3.1 Control and design of crossings ......................... 26
      5.3.2 Improving the crossing design .......................... 27
   5.4 Reservation algorithm for crossroads ....................... 28
6. Communication tests for certification ........................... 30
   6.1 Certification procedures ...................................... 30
6.2 Communication test procedure
   6.2.1 V2V communication
   6.2.2 V2I communication
6.3 Communication test for the different scenarios
6.4 Remarks test procedure

7 References

TABLES
Table 1: Matching relation between communicated data and communication networks........ 5
Table 2: Wireless Network Standards ........................................................................... 7
Table 3: Wireless Mobility Data Through Radio Technologies and Standards [4] .......... 8
Table 4: Network characteristics ................................................................................. 17
Table 5: Latency and reception .................................................................................. 17
Table 6: Performance of the reservation algorithm [22] ................................................ 29

FIGURES
Figure 1: Wireless Communication Networks ............................................................. 6
Figure 2: Two values of the security distance .............................................................. 22
Figure 3: Flow as a function of the density in the non anticipated stochastic case for a
continuation of $\lambda$ when $v=3s$ ................................................................................ 23
Figure 4: Flow as a function of the density in the anticipated stochastic case for a
continuation of $\lambda$ when $v=s$ ................................................................................ 23
Figure 5: Two one-way circular roads with one crossing [9] ......................................... 24
Figure 6: ................................................................................................................... 24
Figure 7: Four roads with two crossings [9] ................................................................. 25
Figure 8: Dependence of the global graph on the ratio between the sum of the sizes of the
priority roads and the sum of the sizes of the non-priority roads [9] .......................... 25
Figure 9: Fundamental graph for two roads with one crossing and four roads with two
crossings [9] ............................................................................................................... 26
Figure 10: Fundamental graphs for three policies [9] .................................................. 26
Figure 11: Fundamental Graph with buffer of size 1 and 2 at crossing [9] .................... 27
Figure 12: Attainable two-dimensional traces [22] ...................................................... 28
Figure 13: Steps of the reservation algorithm [22] ...................................................... 29
Figure 14: Test course ................................................................................................. 32
Figure 15: Test protocols for CityMobil scenarios ...................................................... 33
1 Executive Summary

This report presents the various technologies available on the market or close to the market, which are available for communication, needs for cybercars, automated buses or advanced city vehicles. Communication between vehicles and between vehicles and infrastructure is a key issue for the deployment of automated vehicles in the urban environment. This deliverable has been elaborated to give some information to the developers of such systems. It introduces the state of the art of the various techniques now in the market and those which might soon be and tries to match these techniques with the requirements of the various scenarios which have been elaborated in CityMobil SP2. The impact of these communication technologies on the vehicle throughput is studied, and finally, test procedures for the certification of the communication techniques of the vehicles are proposed.

2 Introduction

In sub-project 3 of CityMobil the technological issues of advanced urban transport systems are addressed. The main objective of this sub-project is to remove technological barriers in order to introduce advanced urban transport systems on a large-scale. Advanced vehicle architectures are developed and the basic subsystems for cybercars, automated buses and advanced city cars are defined to achieve this objective within the sub-project. A dual-mode platform is also developed within SP3 and optimum solutions for human-machine interfaces and information systems are proposed. Furthermore specific obstacle detection systems and navigation techniques, focusing on wireless communication for high throughput are evaluated.

In order to study the described technological issues, working scenarios are developed, which represent different transport areas in modern city life and provide possible solutions for future penetration of innovative transport systems and integration in urban areas under the consideration of the already existing infrastructure. The scenarios offer a good level of generality and potentiality for the CityMobil sub-project. Functions, such as automatically moving in dedicated lanes, entering and exiting a parking area automatically and joining and leaving a formation of Cybercars, have to be considered within those scenarios. The defined working scenarios are the town centre, principal urban roads with an equipped lane (called “e-lane”), Inner city centre and shared traffic space with automated buses and dual-mode vehicles.

The selected working scenarios are described in detail to understand the boundary conditions. Considering those scenario descriptions the definition of system requirements are derived for each scenario. The requirements are based on reliable sources such as simulations, experience from previous projects or calculations. Based on the derived requirements, the main technological challenges for the realisation of these scenarios are identified, which allow the subproject to address them in WP3.2 – Human factors, WP 3.3 - Obstacle detection and avoidance and WP3.4 – Cooperative vehicles and navigation. As a result of the deliverable preliminary system definitions are given in form of a description of the vehicles and their components with the necessary additional infrastructure belonging to the system in different scenarios.

This deliverable deals specifically with the technologies and the requirements for communication in cybercars, advanced city buses and advanced city vehicles. Its objective is
to give to the developers of the systems, recommendations for the introduction of these technologies accordingly with the sites selected.

3 Requirements For Vehicular Communication

To realize guaranteed and safe vehicular communication, one among other issues that must be taken in consideration is the matching relation between the deployed wireless communication networks and data exchanged in Vehicle-to-Vehicle (V2V) case, or traffic destined to or generated by a vehicle in case of Vehicle-to-Infrastructure (V2I) Communication. The main characteristics of this relation are summarized in Table 1.

Table 1: Matching relation between communicated data and communication networks

<table>
<thead>
<tr>
<th>Communicated Data</th>
<th>Communication Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data size</td>
<td>Throughput</td>
</tr>
<tr>
<td>Data protection</td>
<td>Security support</td>
</tr>
<tr>
<td>Data sensibility</td>
<td>E2E QoS support</td>
</tr>
<tr>
<td>Vehicle Mobility</td>
<td>Mobility Support</td>
</tr>
</tbody>
</table>

3.1 Vehicular Traffic Classification

Although data exchanged in V2V case could be considered as traffic, in this deliverable traffic will indicate to that destined to or generated by vehicles in case of V2I communication; on the other hand, data will indicate to that exchanged in V2V case. This will better clarify the different requirements for these two types of vehicular communication. In case of V2V, it is supposed that there is no continuous communication between vehicles, but it must be guaranteed whenever it is needed, since most of the V2V applications are safety related. In case of V2I communication, however, multimedia and other types of traffic circulate between the vehicles and communication infrastructure is assumed to be continuous. Nevertheless, this traffic could go through V2V phase to reach a gateway or an access router installed somewhere on the communication infrastructure. In what follows, we discuss the different types of data that could be communicated in V2V.

3.1.1 Static and Dynamic Data

Before vehicles can communicate, they must be authorized to do so. Static data, hence, related to vehicles is collected and stored in a server configured somewhere in the communication infrastructure. This data is used to identify the registered vehicles and ensure safe and guaranteed V2V; it includes a vehicle’s identifier, colour, radio modem number, type and embedded equipments like GPS, camera, radar, WLAN cards. This data might be considered as part of the traffic in V2I communication. The remaining data that might be exchanged in V2V could be classified into two types [2]:

- **Dynamic data**: this includes vehicle’s direction, speed, position and zone (road sector), which change continuously as long as the vehicle is moving.
- **Conclusion**: this represents the result of vehicles cooperation, which can be obstacle detection, an emergency notification or any other control information.

3.1.2 Elastic and Non-Elastic Traffic

Advanced city vehicles and buses could become information centres and mobile Internet. They could send regularly their dynamic data to transport traffic centres for communication, traffic management and control purposes. Users who connect to Internet can generate and receive different types of traffic: video, mail or voice traffic. This is divided into real-time traffic (non-elastic traffic), which requires rigorous End-to-End (e2e) Quality-of-Service (QoS) and
non real-time traffic (elastic traffic), which tolerates some of e2e QoS violation. QoS is explained in section 3.4.2.

Here are a few examples about traffic generated by a vehicle or destined to it. Priority vehicles or even ambulances might need extra space for security and safety purposes. To this end, these could be equipped with GPS and cameras to enable private or public transportation centres to track and monitor it. Video and trajectory information transmission to these centres, hence, must be guaranteed with high quality. Consequently, vehicles receive updated route planning to find the shortest and less congested route to its destinations. Another example, vehicles transporting money, dangerous materials or products should be monitored by security transportation traffic centres, which require reliable V2I communication with rigorous e2e QoS. In what follows, we will discuss the different wireless communication technologies that could be deployed to transport vehicular traffic, and that could be used to maximize vehicle throughput.

### 3.2 Communication Technologies

Different wireless and radio communication networks and equipments have been developed to cope with different mobility and e2e QoS requirements.

#### 3.2.1 Wireless Communication Technologies

Wireless networks evolve in terms of bandwidth, QoS provisioning and transmission range as shown in Figure 3.1 and Table 3.2. They could be categorized into [4]:

- WPAN (Wireless Personal Area Network)
- WLAN (Wireless Local Area Network)
- WMAN (Wireless Metropolitan Area Network)
- WRAN (Wireless Regional Area Network)

**Figure 1: Wireless Communication Networks**

The different usages of wireless network standards are clarified in Table 2. Note, however, WLAN has been mostly tested and deployed in vehicular communication, though it suffers from interference and security problems, and doesn’t support efficiently mobility nodes.
Table 2: Wireless Network Standards

<table>
<thead>
<tr>
<th>PAN</th>
<th>WLAN</th>
<th>WMAN</th>
<th>WRAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.15-WiMedia</td>
<td>IEEE 802.11 (Wi-Fi)</td>
<td></td>
<td>IEEE 802.22 (Wi-RAN)</td>
</tr>
<tr>
<td>IEEE 802.15.1 – Bluetooth</td>
<td>IEEE 802.11b, a, g</td>
<td>IEEE 802.16-2004</td>
<td></td>
</tr>
<tr>
<td>IEEE 802.15.3 – UWB (Ultra Wide Band)</td>
<td>IEEE 802.11n</td>
<td></td>
<td>IEEE 802.16e/IEEE 802.20 (Wi-Mobile)</td>
</tr>
<tr>
<td>IEEE 802.15.4 – ZigBee</td>
<td>IEEE 802.11p - WAVE - Wireless Access for the Ability in Vehicular Environments</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IEE 802.11r - Fast roaming</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IEEE 802.11s – Wireless mesh networking</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IEEE 802.11t - Wireless Performance Prediction (WPP)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IEEE 802.11u - Interworking with non-802 networks (e.g., cellular)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IEEE 802.11v - Wireless network management</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3.2.2 Radio Communication Technologies

The foundation of a wireless system whether it is mobile, fixed, or a hybrid is the Radio Access Network (RAN). Regardless of the particular RAN protocol used, there are several common issues that transcend technology: Radio system, modulation, propagation, antennae and link budget. The fundamental underpinning of any successful design and network adjustment is based on the existence of engineering guidelines. Table 3 shows us that an important concept, especially when using multiple RANs, is that there can be several link budgets in any system based on the operating frequency, spectrum allocated, link reliability, physical components for the system, differences in up and down stream modulation methods or protocols and rain fade issues to maintain some of the elements that need to be considered. The biggest issue with wireless data is that the network engineer needs to ensure that there is sufficient bandwidth to support the various applications and services offered and correct CPU processing and memory to support the required additional services.
Table 3: Wireless Mobility Data Through Radio Technologies and Standards [4]

<table>
<thead>
<tr>
<th>Technology</th>
<th>Data Capability</th>
<th>Spectrum Required</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSM</td>
<td>9.6Kbps or 14kbps</td>
<td>200 kHz</td>
<td>Circuit switched data</td>
</tr>
<tr>
<td>CDMA</td>
<td>9.6 kbps/14.4 kbps</td>
<td>1.25 MHz</td>
<td>Circuit switched data</td>
</tr>
<tr>
<td>2.5G Technology</td>
<td>Data Capability</td>
<td>Spectrum Required</td>
<td>Comment</td>
</tr>
<tr>
<td>GPRS</td>
<td>128 kbps</td>
<td>200 kHz</td>
<td>Circuit/Packet data</td>
</tr>
<tr>
<td>Edge</td>
<td>384 Kbps</td>
<td>200 kHz</td>
<td>Circuit/Packet data</td>
</tr>
<tr>
<td>3G Technology</td>
<td>Data Capability</td>
<td>Spectrum Required</td>
<td>Comment</td>
</tr>
<tr>
<td>WCDMA/UMTS</td>
<td>144 kbps vehicular 384 kbps outdoor 2 Mbps indoors</td>
<td>5 MHz</td>
<td>Packet data</td>
</tr>
<tr>
<td>CDMA 2000/EVDO/EVDB</td>
<td>144 kbps vehicular 384 kbps outdoor 2 Mbps indoors</td>
<td>1.25 MHz</td>
<td>Packet data</td>
</tr>
</tbody>
</table>

The delivery of IP data and associated benefits of these exciting transport methods are available with all 2.5G and 3G RAN as well as WLAN. The key difference is how they deliver the IP data defined by its latency and throughput (QoS provisioning). For example, in CDMA 2000 network, the system uses a Point-to-Point Protocol (PPP) between the mobile and the Packet Data Serving Node (PDSN) for every type of packet data session that is transported. It is very similar to a dial-up Internet connections used by many people over standard landline facilities. Simple IP is where a PPP session is established between the mobile and PDSN. The PDSN basically routes packets to and from the mobile in order to provide e2e connectivity between the mobile and Internet.

So far, vehicular traffic, wireless and radio communication technologies have been explained. In what follows, we will first discuss the main challenges of vehicular messages propagation. Afterwards, we will clarify the different Mobile Ad hoc NETworks (MANET) protocols that could be used to realize V2V. Some vehicular applications, mostly safety related will be discussed in this context. The performance of these protocols evolves in terms of its capacity to cope with vehicle mobility and vehicular applications requirements in terms of e2e QoS support. While vehicle ad hoc network protocols have been mostly developed to transmit alert or warning messages to avoid an accident or execute complex manoeuvres in a platoon, complete communication architectures, in case of V2I communication, have been developed to enable vehicles to connect to Internet network and thus eases services provisioning to vehicles.

3.3 Vehicular Message Propagation

Message propagation enables each vehicle within a dangerous zone to be informed about any accident. Whenever a vehicle node receives this message, it decides whether to forward it or not, depending on the deployed forwarding algorithm. In all cases, warning messages must be received by all the vehicles approaching a dangerous zone, so that they can avoid the accident. Furthermore, message propagation within the zone might be required to continue until certain time, to inform new vehicles approaching this zone about the accident. Note, however, a vehicle involved in an accident might be in one of the following situations [11]:

- The vehicle might be destroyed in the accident, resulting in the destruction of the transmitter, before it can send any emergency message.
- The vehicle sent only one emergency message before its transmitter is destroyed
- The vehicle's transmitter can keep sending periodically emergency messages, since it isn't destroyed in the accident.

The most dangerous situation is when the vehicle is destroyed completely or when it could send only one message, since the message could be lost leading to warning absence in the accident zone. In such situation, different vehicle groups could be involved in the forwarding process:

- Only vehicles belonging to the Hazardous zone are involved in the forwarding process
- Only vehicles belonging to the opposite zone are involved in the forwarding process.
- Vehicles belonging to both zones are involved in the forwarding process.

The deployed VANET protocol will decide which vehicle group will be involved in the forwarding process. In any case of vehicle accident, abnormal vehicle must be able to send at least one message, and VANET protocol must correctly forward the message using the radio or wireless networks to all concerned vehicles approaching the accident zone. In what follows, forwarding strategies will be explained.

### 3.3.1 Rules Based Forwarding Algorithms

There is a difference between transmission range and information range. The transmission range of a vehicle depends on its antenna's transmission power, antenna's height and on the propagation channel characteristics. The area space covered by a radio system depends on these factors. Most of the antennas are omni-directional antennas, so its radio coverage area extends homogenously in a circle whose centre the vehicle transmitting the message. Under normal condition, when a vehicle sends a packet, all vehicles in its transmission range receive simultaneously this packet. Information range, however, shows how far message reaches from the message source. Multi-hopping communication strategy enables vehicles beyond the source's transmission range to receive the message. But, due to interference level or other channel characteristics deterioration, some vehicle nodes cannot decode the messages, hence information range could be less than the transmission range.

There is a trade off between information range and to what extent message should be propagated to avoid infinite message forwarding. There are different ways to discard or stop message propagations: One-Way is to define a hop count in a packet, so it can be discarded based on this hop count. Rejection or forwarding message could depend on its content importance and its distance from the source. Here, different messages could be circulated in a zone: one is generated by an abnormal vehicle and another forwarded by a vehicle involved in the dissemination process. In what follows we will discuss the different protocols that could forward messages in VANET.

### 3.4 Vehicle Ad hoc Network Protocols

Vehicle Ad hoc NETworks (VANET) protocols contribute in increasing mainly safety and could be used to increase comfort on the roads. These protocols control and manage the way to transmit warning messages in inter-vehicle communication using the deployed wireless or radio network. Consequently, autonomous vehicles could be informed about an obstacle or an accident so they can avoid it, as well as drivers could be assisted to drive safely. Thereby, the range of awareness of autonomous vehicles and drivers is extended from current line-of-sight to the radio range of a deployed wireless transceiver. Furthermore, with multi-hop warning packet forwarding, each vehicle on the road can benefit from the locally sensed or gathered data about surrounding vehicles. Unfortunately, vehicular network topology changes continuously which complicates warning messages transmission and delivery to destinations. In what follows, different Mobile Ad hoc NETwork (MANET)
protocols will be discussed in the context of inter-vehicle communication to see how they could be adapted to VANET environment for safety purposes.

### 3.4.1 Mobility Sensibility

Vehicles change continuously their positions so VANET protocols must cope with this dynamic change and guarantee permanently a routing path between sources and destinations, especially those approaching dangerous zones or an accident point. Furthermore, VANET protocols must cope with high dynamic of vehicular topology, which changes continuously and randomly.

### 3.4.2 QoS Provision

In inter-vehicle communication, end-to-end QoS provisioning is crucial, particularly for safety applications where real-time messages (warning messages) delivery to destinations and concerned vehicles is important. Wireless and radio communication networks are limited by their network resources, namely bandwidth, thus VANET protocols must avoid sending unnecessary message. Whatever inter-vehicle application is running, VANET protocols must efficiently make use of the scarce bandwidth resource. Therefore, efficient and effective medium access control, routing and data forwarding can have a direct impact on QoS that could be provided by VANET protocols, like message delay, loss and jitter. VANET protocols must manage efficiently vehicles mobility and guarantee QoS provisioning. In what follows, we classify and discuss the main MANET protocols and see how could be deployed in vehicular communication environments.

### 3.4.3 Topology Based Routing Protocols

The functionality of these protocols is based on network topology status information, namely network nodes and links status. They are classified as proactive or reactive routing. Optimized Link Status Routing (OLSR) \cite{13} is an example of proactive routing protocols, in which all routing tables are built in advance at the different nodes constituting the network. Meanwhile, reactive protocols like Ad Hoc On Demand Vector (AODV) protocol \cite{5}, a routing path is built based on request. The OLSR protocol uses HELLO packets to gather status information about network nodes and links, which enable vehicle nodes to get the subset of one-hop list and second two hop list. These hops are called Multipoint Relays (MPRs), since they relay messages from a vehicle to others. In AODV, routes are discovered on demand by using broadcast messages called Route REQuest (RREQ). The destination replies by a unicast routing message to the source along the discovered route, and when the route is broken, it is re-established using control messages.

In OLSR protocol, control and HELLO messages are used to maintain routing tables at each node, which waste in turn some of network resources. On the other hand, AODV protocol requires some delay before each communication for routes discovery. In proactive routing protocols, like OLSR, routing overhead increases based on network dynamicity. In reactive routing, to cope with network dynamic control messages increase to find a dynamic routing connecting source and destination. In \cite{3}, the authors proposed an approach to improve HELLO messages frequency to better cope with network dynamicity. In \cite{24}, the authors proposed to improve AODV by adding some geographical information into packet requests to adapt for changing networking topology information.

IMARA team, at the INRIA Rocquencourt has deployed the OLSR protocol to realize inter-vehicle communication. Note, however, that research work is still undergoing to adapt it to vehicle topology dynamicity and to make it more efficient.

### 3.4.4 Geocast Routing Protocols

These protocols depend on position information, which could be computed easily by vehicles as far as most of these are equipped by a GPS. Here, we have to distinguish between two
types of protocols: Geocast and position-based routing protocols. Geocast routing protocols transmit data to a geographical area; meanwhile, position based routing protocols transmit data to a position. Location Based Multicast (LBM) [19] and Geocast Adaptive Mesh Environment for Routing (GAMER) are examples of Geocast routing protocols. Location-Aided Routing (LAR), Distance Routing Effect Algorithm for Mobility (DREAM) and Greedy Perimeter Stateless Routing (GPSR) [21] are examples of position based routing protocols.

The LBM routing protocol reduces flooding by transmitting messages to a zone that includes at least one destination, and then it establishes at least one routing path between the source and a destination in this zone. In [20], the authors proposed a stored Geocast routing protocol that adapts to VANET environment. The source first sends a message to a zone using the normal Geocast routing protocol. Afterwards, all vehicle nodes inside this zone agree on one node to receive the next messages and periodically send it in the zone or based on a request.

In [10], the authors conducted some studies showing that the routing algorithms relying on position information are likely to be appropriate for messages routing in VANET. When VANET dynamic increases, the position information becomes inaccurate, thus the receiver position in a zone will no longer be valid, leading to message delivery failure to the whole zone. Although Geocast routing protocols could be deployed in VANET, they depend mainly on computation accuracy of the receiver’s position. In such situation, it is clear that this protocol, as others, is very sensitive to vehicle nodes mobility. To deal with this problem, a geographical area including the destination can be enlarged, but this increases the number of involved vehicle nodes resulting in bandwidth waste. Further solutions have been proposed for this problem by anticipating the node’s positions based on vehicle nodes direction.

This protocol could be deployed whenever there are two platoons and there is a distance separating them.

3.4.5 Network Clustering Based Routing Protocols

The network is arranged into a number of clusters. A cluster is a group of nodes that share the same communication and mobility characteristics. A platoon of vehicles could form a cluster. The message is propagated from a cluster to another through relay nodes, called gateways, existing in the transmission range of cluster heads.

In Zone-Based Hierarchical Link State Routing (Z HLS) [14] and GeoGRID [19] protocols, the authors adapted this protocol to operate with geographical routing protocols. In [31], [15], the authors get benefit of and take in account the cluster traffic road characteristics to increase the lifetime of the clusters. This protocol might contribute in optimizing network radio resources.

Control messages are sent within and between clusters to keep reliable and stable connections between gateways, which causes overhead problem for these routing protocols. This protocol could be used to establish communication between manually driven and autonomous cars, or between two Platoons of cybercars and manually driven cars.

3.4.6 Broadcast Protocols

This approach might be the easiest one and could be deployed for message routing in VANET. Each vehicle node receives a message, and retransmits it to other vehicle nodes in its zone; however, this creates the storming problem, well known in broadcast protocols, due
to the redundant message retransmission. In [1], the authors implemented and evaluated a broadcast protocol in VANET environment; it optimizes the number of vehicle nodes re-forwarding messages. Upon receiving the messages by a vehicle node, it computes the broadcast probability, which enables it to decide whether to forward it, or not. In OLSR routing protocol, forwarding vehicle nodes are previously determined and connected through mesh network. An optimized broadcast protocol reduces the number of vehicle nodes forwarding these messages while guaranteeing message delivery.

In [23], the authors proposed a location-based broadcast algorithm, which enables a node to decide about forwarding messages based on its position and retransmission coverage. A node adds its own location in the transmitted messages. When a node receives the message, it computes the additional coverage area it can cover by retransmitting this message. Similarly, in the direction-based broadcast algorithm, the broadcasting decision is improved by using the nodes trajectory or a digital map. In network clusters [16], only cluster head retransmits the messages. The nodes can also estimate the message utility to decide which message should be retransmitted first [30], in order to minimize the bandwidth consumption. Nevertheless, optimized broadcast routing protocols might suffer from overhead problem and bandwidth consumption, since these depend on exchanging control messages to get information about neighbourhood nodes. This problem becomes more complicated as network gets more dynamic and mobile.

In what follows, we discuss the second major part of vehicular communication and analyze the different ways to realize V2I communication.

### 3.5 Vehicle to Infrastructure Communication

This part of vehicular communication enables vehicles to connect to Internet network, which ease different service provision to vehicles. Passengers can surf on Internet, download films and communicate with others through the Internet network. Furthermore, vehicles could be monitored, managed and controlled by a server configured in Internet network, for security purposes and billed intelligent transport services. In what follows, the different mechanisms required to realize V2I communication will be discussed.

#### 3.5.1 IP unified Network

Different wireless access technologies are required to enable vehicles to keep communicating with each other, and to realize seamless multimedia and Internet service provisioning to vehicles. These wireless technologies have different characteristics, which complicate service provisioning to traffic flows destined to or transmitted by vehicles. Furthermore, the performance of vehicular applications is easily impacted due to the heterogeneity of these wireless access networks. However, networks are changing and growing more complex than the data network of the 1990s. The Internet Protocol (IP) is shaping the future of unified network systems. IP technology can federate together protocols selected from a loose collection, so IP layer always keeps transparent communication with mobile networks, for example with vehicles. This means that IP can run on top of any link layer technology and that any service can run on top of IP layer. This also decouples the network layer very clearly from the service and application.

If vehicular applications require real time service support, a reliable technology must be installed underneath the IP to guarantee that packets arrive within a certain maximum delay. IP is however fundamentally unsuited to delivering packets within a time [8], especially for mobile IP users. With e2e QoS provision and policy based management mechanisms, today’s IP networks are expected to be more intelligent and sophisticated. Now more and
more than ever before, the heterogeneous wireless access networks and wired network are required to be unified into a single, more efficient, network infrastructure. However, this might lead to fattening the hourglass and losing some of the simplicity of IP networks. IP networks also rely on the principle of global addressing, and this IP address is attached to every packet. Unfortunately, there are not enough IP addresses to go round- since the address field IP is limited to 32 bits. To this end, a new version of the IP protocol (IPv6)- is being introduced to extend the address space to 128 bits [7]. In what follows, the IPv6 technology will be discussed.

3.5.2 Mobile IPv6

The proliferation of mobile computing devices inside vehicles and wireless networks connecting it to Internet require mobility support, to guarantee seamless and persistent vehicular communication. The IPv6 technology procedure could be explained through three steps: address registration, address resolution and tracking. When a vehicle is in the transmission range of its home network, it registers its IPv6, called Home Address (HoA), in a home agent which will be responsible for all the different services that could be provided to it.

As vehicle moves out of its home network, the IPv6 technology will enable it to connect to a foreign network, by resolving a new IPv6 called care-of-address (CoA). The vehicle sends this CoA to its home agent to bind it with it HoA. This will enable the home agent to offer a ubiquitous service to the vehicle, which allows it to keep the same internet address anywhere, and allows applications using that address to maintain transport and upper-layer connections despite of changing locations and networks. Consequently, this guarantees transparent mobility across homogenous and heterogeneous media.

In this Reference [7], the authors summarize the advantages of the technology IPv6 in the following points:

- The ability to maintain Internet connectivity while vehicles are changing their point-of-attachment to Internet network.
- The ability to deploy several IPv6 nodes interconnected through an in-vehicle network (Network mobility support)
- The ability to use multiple access technologies simultaneously (multihoming)
- The ability to communicate with the neighbouring vehicles as ad-hoc networking vehicle-to-vehicle (V2V) communications.

3.5.3 Mobile Network Protocols

Vehicles as other mobile networks could contain different mobile computing devices and multimedia networks. These protocols enable mobile networks to manage its mobility and mobile network nodes inside it. The MObility NEtwork Basic Support (NEMO-BS) [6], based on MIPv6, has been standardized to manage the entire mobility of mobile networks. One or more mobile routers are added inside a mobile network, depending on its size, to manage upstream traffic generated by mobile network or downstream traffic destined to it. These mobile routers have different interfaces to enable mobile network to connect to Internet through different wireless and radio networks. The NEMO-BS protocol creates a bi-directional tunnel with the mobile network’s home agent, which guarantees transparent communication to all the mobile network nodes (MNNs) inside it, consequently they will be unaware of mobility. MNNs could be sensors transmitting critical data to another NEtwork that is MObile (NEMO) or a server somewhere to analyze it for safety purposes and fleet management. MNNs could be simple users surfing on Internet or sending emails and communicating through their PDAs with other external users. MNNs might be a group of doctors performing a surgical operation and getting assistance from others in a hospital while they are in an ambulance driving them to the hospital. MNNs might be travellers listening to music and watching video in a bus or train.
3.5.4 V2I and V2V Integration

Integrating different communication approaches in an Inter-vehicle communication platform to guarantee a continuous and reliable communication between the communicating vehicles is very crucial, though it is an inherently challenging task. It requires very good functionality of each communication approach, transition mechanisms between these approaches and adaptation between their communicating functions. In this [2], the authors developed an integrated and reliable inter-vehicle communication platform. The V2I approach has been realized by implementing client/server communication module using GSM network, meanwhile the V2V (VANET) approach has been realized by implementing simple broadcast protocol using Wi-Fi (802.11b).

In [25], the authors could integrate V2I approach realized by NEMO-BS protocol and V2V approach realized by OLSR VANET (MANET) protocol in one platform. The integration of both MANET and NEMO approaches is called MANEMO; this gives the possibility to use route optimization and multihoming possibilities.

3.5.5 Continuous Air-Interface for Long and Medium Range Communication (CALM)

Mobile networks require ubiquitous and seamless communication; however, due to the heterogeneity of wireless technologies enabling vehicles to connect to Internet, these experience vertical handover when they swap wireless technologies to maintain their Internet connection, which impacts negatively the communication quality. The Continuous Air-interface Long and Medium range (CALM) architecture [12] is being standardized to enable vehicles to handle vertical handover problem. CALM architecture is a related set of communication protocols and management techniques; it provides a layered solution that enables continuous communications between vehicles and infrastructure, using wireless telecommunications media that are available in any particular location.

It provides a standardized set of air interface protocols and parameters for medium and long range, high speed ITS communication using one or more of several media, with multi-point and networking protocols within each media, and upper layer protocols to enable transfer between media. It is expected therefore to support multiple media and types of application such as support of Internet services and traditional ITS applications. CALM is based on IPv6, which means it is fully compatible with Internet services, while at the same time not being restricted by the addressing shortcomings of the current IPv4 protocols. It defines five communication scenarios: V2I non-IPv6, V2I/V2V using local IPv6, V2I using MIPv6, V2I using NEMO and V2V non-IPv6. Furthermore, CALM defines smooth transition protocols between the different radio M5 technologies ((microwave 5.9 GHz), IR/MM-wave (directional),GSM/3G (cellular)). CALM enabled router is expected to have different interfaces working at a particular frequency and offering high communication performance. Some of the protocol functionalities that CALM supports are: mobile IPv6 routing, geographically mapped IPv6 addressing, fast location addressing, real-time data exchange and CALM management entities. In addition, it defines and open channel communication with those equipments installed on roadside infrastructure. CALM is conceived to appear in a vehicle in the form of a box, it is just likely to be incorporated into one of the in-car computing functions.

3.5.6 Vehicle Connection to Internet

Wireless and radio technologies enable a vehicle to request services from stationary servers configured in Internet network or other vehicles through a multi-hop communication. One of the different problems is to determine the best wireless access network that can offer the required service. Another one is to cope with the overlapping of multiple wireless access
networks. Furthermore, in case of multi-hop communication, how the optimal route could be determined to a gateway, regarding network resource utilization and connection lifetime. Vehicle Internet connection requires the following:

- Access networks scalability, offered services and mobility protocol.
- Fast services discovery, registration and de-registration.
- End-to-End QoS provisioning
- End-to-end security issues
- Intelligent resource control and management.

In multi-hop packet forwarding, packet loss, delay and delay variation depend on the total hop count required to reach the destinations. Traffic destined to Internet and that for safety purposes like emergency packets should be given their corresponding priority when other traffic is sent through VANET. Security issues must be respected in this case, because flows characteristics could be changed when they pass through multiple nodes. Furthermore, IP mobility support enables a seamless communication. In a platform where connection to Internet passes through multi-hop, this requires a support for IP-mobility in wireless networks.
4 Requirements for communication technologies according to scenarios

In the following section the communication requirements for the various scenarios elaborated in the deliverable D3.1 are discussed. The first scenario deals with partly automated dual mode vehicles/advanced city cars in a historical town centre, the second with a combination of both fully automated cybercars and partly automated dual mode vehicles/advanced city cars (mixed traffic) on dedicated lanes and the third scenario with cybercars in inner city centre. The last scenario describes automated BRT (Bus Rapid Transit) systems on dedicated lanes, which are shared with dual mode vehicles and cybercars.

4.1 Town centre

This scenario deals with a historical city centre inside the city structure, which is not well connected to surrounding districts, consists of a network of small roads and limiting vehicle access and parking places. The environment is therefore rather complex. The assisted vehicles will be parked around the zone and allowed to drive in a dedicated network of roads. The dual mode vehicles provide assisted driving, especially in difficult or narrow passages, in order to follow a fixed trajectory (e.g. in a right angle curve) or to stop at precisely defined places.

Obstacle detection for increased safety of the other road users, especially pedestrians and cyclists is a key element of those vehicles. The capability of use in platoon, where the first vehicle is manually driven and a second one is linked automatically, for instance in order to pick up a vehicle or bring it to users is considered in this scenario.

4.1.1 Data types

In this scenario, a wireless V2V and V2I communication system is required for information exchange about:

- Traffic network status;
- Fleet management;
- Missions assignment;
- Platooning management;
- User identification and payment;
- Vehicle status;
- Emergency and assistance services;
- Traffic lights management;
- Path crossing and merging management;
- Internet services employment.

4.1.2 Priority and network propagation area

Information are characterized by priority and propagation:

- Priority: each type of information requires suitable priority, i.e. data regarding safety issues must be shared in real-time while generic traffic management can be delayed without any risk.
- Propagation: Information can be useful for the entire vehicle present in the network, or only for vehicles located in a particular area.

The following table summarizes requirements for any kind of information which the communication system must satisfy in terms of priority and in terms of propagation.

**Table 4: Network characteristics**

<table>
<thead>
<tr>
<th>Information</th>
<th>Priority</th>
<th>Network propagation area</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2I communication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traffic network status</td>
<td>Medium</td>
<td>5 Km</td>
</tr>
<tr>
<td>Fleet management</td>
<td>Low</td>
<td>Whole network</td>
</tr>
<tr>
<td>Mission assignment</td>
<td>Low</td>
<td>Whole network</td>
</tr>
<tr>
<td>User Identification</td>
<td>Medium</td>
<td>Whole network</td>
</tr>
<tr>
<td>Vehicle status</td>
<td>High</td>
<td>Whole network</td>
</tr>
<tr>
<td>Emergency services</td>
<td>High</td>
<td>Whole network</td>
</tr>
<tr>
<td>Traffic lights management</td>
<td>Real-time</td>
<td>100 m</td>
</tr>
<tr>
<td>Internet services</td>
<td>Low</td>
<td>Whole network</td>
</tr>
<tr>
<td>V2V communication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Platooning management</td>
<td>Real-time</td>
<td>100 m</td>
</tr>
<tr>
<td>Crossing and merging path management</td>
<td>Real-time</td>
<td>100 m</td>
</tr>
</tbody>
</table>

**4.1.3 Reliability and probability of reception**

The probability of reception per packet is affected by the particular scenario topology, consisting of tall and tight buildings; this implies a probability of perception well below 100%.

For this reason, the communication system must provide a robust routing protocol (with multi-hop techniques) and redundancy strategies in order to improve data delivery reliability.

Different priority levels determine specific constraints regarding latency time and corresponding probability of reception. The following table set the correspondences between these parameters.

**Table 5: Latency and reception**

<table>
<thead>
<tr>
<th>Priority level</th>
<th>Latency</th>
<th>Probability of reception</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>10 s</td>
<td>70 %</td>
</tr>
<tr>
<td>Medium</td>
<td>5 s</td>
<td>90 %</td>
</tr>
<tr>
<td>High</td>
<td>1 s</td>
<td>95 %</td>
</tr>
<tr>
<td>Real-time</td>
<td>100 ms</td>
<td>99.99%</td>
</tr>
</tbody>
</table>

The communication protocol should be compliant with these parameters, in order to guarantee communication reliability and overall system safety. For example, multi-channel and/or multi-path communication, or message repetition strategies, should be provided in order to favour high priority messages over low priority ones without causing network congestion.

Particular strategies must be provided for real-time messages, which are in charge of guarantee safety-critical tasks. If a real-time message, regarding for example traffic lights or vehicle crossing management, is not properly transmitted, severe consequences might occur: for this reason, specific strategies must be adopted in order to detect any lack of communication in real-time messages delivery and then automatically prevent possible dangerous situations (i.e. polling strategies).
4.1.4 Communication security

The presence of sensitive information sharing, e.g. vehicle control commands and user’s identification data, requires the implementation of appropriate security mechanisms (e.g. data encryption, firewalls, gateways…), in order to guarantee vehicles safety and users privacy.

4.2 Principal urban roads with an equipped lane (called "e-lane")

This scenario deals with a migration step towards autonomous driving by utilising a so-called “e-lane”. Hereby defined roads signposts indicate the possibility of driving autonomously on an e-lane. This e-lane is exclusively reserved for higher automated traffic. With a dual mode vehicle, which is specially equipped and certified, the e-lane can be used. Once the vehicle is on the e-lane the guidance of the vehicle is conducted autonomously.

The driver can focus on other activities (e.g. read newspaper, office work etc.). The driver can intervene and take over the responsibility and leave the e-lane, whenever he wants to. The vehicles drive up to a velocity of 120 km/h on protected lanes, so that there is no interaction with pedestrians, cyclists etc. Longitudinal control of all the vehicles is implemented in order to smooth and improve the maximum capacity of the traffic flow.

The requirements for the communication in this scenario are not very different than those of the advanced city vehicles described previously with the most difficult requirement to be placed on the platooning application which calls for real-time data exchange for the proper control of acceleration and deceleration. However, this information should be backed up by a distance sensor to increase reliability.

4.3 Inner city centre

In the “inner City” scenario a limited fleet of automated vehicles drive fully autonomously in the city centre at low speed. The user can enter the vehicles at defined access points and then has the possibilities to choose the destination on pre-defined tracks. The Cybercars have to interact with pedestrian and cyclists on one side and with other Cybercars and low speed vehicles (cleaning machines etc.) on the other side. For user pick-up and maintenance parking places are reserved. A fleet management system optimises the displacement of the vehicles in real time.

Like for the town centre scenario, this inner city scenario requires, a wireless V2V and V2I communication system. This communication system should allow exchange for:

- Traffic network status;
- Fleet management;
- Missions assignment;
- Platooning management;
- User identification and payment;
- Vehicle status;
- Emergency and assistance services;
- Path crossing and merging management;

From a communication priority point of view the requirement for the inner city scenario is as follow (based on the table presented for the town centre scenario):

<table>
<thead>
<tr>
<th>Information</th>
<th>Priority</th>
<th>Network propagation area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic network status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fleet management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Missions assignment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Platooning management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User identification and payment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vehicle status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency and assistance services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Path crossing and merging management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>V2I communication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Traffic network status</td>
<td>Low</td>
<td>5 Km</td>
</tr>
<tr>
<td>Fleet management</td>
<td>Low</td>
<td>Whole network</td>
</tr>
<tr>
<td>Mission assignment</td>
<td>Medium</td>
<td>Whole network</td>
</tr>
<tr>
<td>User Identification</td>
<td>Medium</td>
<td>Whole network</td>
</tr>
<tr>
<td>Vehicle status</td>
<td>Medium</td>
<td>Whole network</td>
</tr>
<tr>
<td>Emergency services</td>
<td>High</td>
<td>Whole network</td>
</tr>
<tr>
<td>V2V communication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Platooning management</td>
<td>Real-time</td>
<td>100 m</td>
</tr>
<tr>
<td>Crossing and merging path management</td>
<td>Real-time</td>
<td>100 m</td>
</tr>
</tbody>
</table>

The meaning of priority used for the previous table and defined in the town centre scenario are as follows (previously defined in Reliability and probability of reception section of town centre scenario):

<table>
<thead>
<tr>
<th>Priority level</th>
<th>Latency</th>
<th>Probability of reception</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>10 s</td>
<td>70 %</td>
</tr>
<tr>
<td>Medium</td>
<td>5 s</td>
<td>90 %</td>
</tr>
<tr>
<td>High</td>
<td>1 s</td>
<td>95 %</td>
</tr>
<tr>
<td>Real-time</td>
<td>100 ms</td>
<td>99.99%</td>
</tr>
</tbody>
</table>

4.4 Shared traffic space with automated buses and dual mode vehicles

The fourth scenario consists of dedicated lanes for automated busses and dual mode vehicles/Cybercars. It is based on infrastructure, which is already available in some European cities today. A well-organised, automated public transport system alone can help to improve the increasing traffic congestions in European cities. The combination of automated busses and other types of automated vehicles provides an even more efficient saturation of valuable space for traffic on one side and intensifies the deployment of advanced innovative transport systems on the other side, because only minor modifications of the already existing infrastructure are needed.

In this scenario a cooperative control system in form of the traffic management system can improve the handling of traffic. Mixed automated vehicles share one driving lane, whereas dual mode vehicles can leave the dedicated lanes at any exit. The dual mode vehicles and Cybercars are integrated into existing infrastructure.

In this scenario the communication is a very critical aspect. Indeed, if the V2I will be used for supervision, fleet management and navigation, the V2V will allow the safe sharing of traffic space between automated vehicles (buses and cybercars) and entering or leaving dual mode vehicles.

Concerning the communication needs they are more or less the same as communication needs for town centre and inner city scenario:

- Traffic network status;
- Fleet management;
- Missions assignment;
- Platooning management;
- User identification and payment;
- Vehicle status;
• Emergency and assistance services;
• Path crossing and merging management;
• Traffic light management
• Management of entering or leaving the dedicated lane

From a communication priority point of view the requirement for this scenario is as follow (based on the table presented for the town centre scenario):

<table>
<thead>
<tr>
<th>Information</th>
<th>Priority</th>
<th>Network propagation area</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>V2I communication</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traffic network status</td>
<td>Low</td>
<td>5 Km</td>
</tr>
<tr>
<td>Fleet management</td>
<td>Low</td>
<td>Whole network</td>
</tr>
<tr>
<td>Mission assignment</td>
<td>Medium</td>
<td>Whole network</td>
</tr>
<tr>
<td>User Identification</td>
<td>Medium</td>
<td>Whole network</td>
</tr>
<tr>
<td>Vehicle status</td>
<td>Medium</td>
<td>Whole network</td>
</tr>
<tr>
<td>Emergency services</td>
<td>High</td>
<td>Whole network</td>
</tr>
<tr>
<td>Dual mode vehicle entering or leaving dedicated lane</td>
<td>High</td>
<td>Whole network</td>
</tr>
<tr>
<td><strong>V2V communication</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Platooning management</td>
<td>Real-time</td>
<td>100 m</td>
</tr>
<tr>
<td>Crossing and merging path management</td>
<td>Real-time</td>
<td>100 m</td>
</tr>
<tr>
<td>Dual mode vehicle entering or leaving dedicated lane</td>
<td>Real-time</td>
<td>100 m</td>
</tr>
</tbody>
</table>

The meaning of priority used for the previous table and defined in the town centre scenario are as follows (previously defined in Reliability and probability of reception section of town centre scenario):

<table>
<thead>
<tr>
<th>Priority level</th>
<th>Latency</th>
<th>Probability of reception</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>10 s</td>
<td>70 %</td>
</tr>
<tr>
<td>Medium</td>
<td>5 s</td>
<td>90 %</td>
</tr>
<tr>
<td>High</td>
<td>1 s</td>
<td>95 %</td>
</tr>
<tr>
<td>Real-time</td>
<td>100 ms</td>
<td>99.99%</td>
</tr>
</tbody>
</table>
5 Evaluation of maximum throughputs

Longitudinal control of vehicles inserted into a platoon can lead to headways as small as 0.3s, which has to be compared to the mandatory 2s “human” headway. This represents the time needed by the platooning system to react to a change in speed.

Typical vehicle flows for passenger cars are on the order of 2,000 to 2,200 cars per hour per lane in the best cases. Using platooning technologies with headways of 0.5 seconds, the maximum flow could reach as much as 7,200 vehicles per hour. Of course, this is only theoretical and one must allow for gaps for safety and merging or crossing of flows. However, it is considered as feasible to reach throughputs at least twice as large as with manual vehicles with a higher safety and this on a much narrower lane (typically less than 2 meters instead of 3.5).

Traffic research engineers describe in a precise mathematical manner the interactions between vehicles and infrastructure. Various traffic flow models have been developed to characterise the relationship between the traffic stream variables: speed, flow and concentration.

5.1 Evaluation of maximum throughputs with the Fundamental Traffic Law

The Fundamental Traffic Law is a well-known relation between traffic flow (f) and density (d). [17] analysed deterministic and stochastic traffic models, succeeding to obtain a typical hat-shaped fundamental traffic law for each one. Below, each model is described briefly and the derived conclusions are applied to the case of a platoon of driverless automated vehicles.

5.1.1 Deterministic Model

We consider \( n \) vehicles, moving on a one-way circular road of length \( m \).

Each vehicle has a desired speed \( v \) and must respect a security distance \( s \) such that \( n*s<=m \).

At each unitary time step \( t \), each car is to cover distance \( v \) taking into consideration that it cannot overtake the car ahead.

Two cases can be considered:

The actions of the car ahead are not anticipated

If we denote the car density by \( d \ (d=n/m) \) then the Fundamental Traffic Law is given by:

\[
f = \min(vd, 1 - sd)
\]

Figure 2 depicts the implication of the Fundamental Law for two values of the security distance. The required security distance for a platoon of automated vehicles is inferior to the one required for manual cars.

We can see that the maximum flow (B) corresponds with the shortest safety distance and therefore a greater traffic density value.
The actions of the car ahead are anticipated.
In this case, at time $t$ car $i$ knows the position of car $i+1$ at time $t+1$.
In this case, the fundamental traffic law is given by $f = vd$.
Note in addition, that the result can be guessed intuitively, indeed, it is obvious that now all the cars can move at speed $v$.
To begin with all cars must respect the security distance so they can all move together at the desired speed complying with that safe following distance.
In this case, one can easily see that since the condition $ns \leq m$ must be respected, if $n_1$ denotes the number of automated vehicles and $n_2$ the number of manual ones then $n_1 > n_2$ and consequently we conclude that $f_1 > f_2$.

5.1.2 Stochastic Model
As the name suggests, we suppose now that at each unitary time step $t$, each car $i$, for $i=1,...,n$, chooses his desired speed $v_{n_i}$ independently and randomly between $\{h,k\}$ with probabilities $\{p1,p2\}$.
As noted earlier, two cases can be identified, the first where at time $t$ car $i$ (for $i=1,...,n$) anticipates the position of the vehicle ahead at time $t+1$ and the second where the position of the vehicle ahead at time $t+1$ is not anticipated. By applying simulations (using [18]) is possible to plot the fundamental traffic law. The following graphs show that we still obtain the same typical hat-shaped form.
Figure 3: Flow as a function of the density in the non anticipated stochastic case for a continuation of $\lambda$ when $v=3s$

Figure 4: Flow as a function of the density in the anticipated stochastic case for a continuation of $\lambda$ when $v=s$

5.1.3 Fundamental graphs for a system of two circular roads-one crossing

Up to this point we have studied traffic models involving one-way circular roads. [9] examines a more complex situation where two one-way circular roads cross and vehicles move without overtaking. More precisely, they consider a system of two one-way circular roads with one junction as depicted in Figure 5.
The crossing circulation rule adapted here is "priority to the right", (or its equivalently "priority to the left") loosely speaking to give way to traffic approaching from the right (eq. left).

The following model concerns a vehicle's movement. The roads are cut into sections, and each vehicle occupies one. If the occupied position is not the crossing cell and if the section ahead is empty then the vehicle can advance. A vehicle in a section connected to a crossing, enters if the crossing is free and if it is on the priority road. If the vehicle is on a non-priority road, it enters only if the crossing is free and if no other vehicle on the priority road wants to enter.

Figure 6 indicates the Fundamental Graph for different ratios between the section numbers of each road. As Figure 6 points out, the maximum flow is obtained for a higher car density when the number of sections for the non-priority road is increased.

**Figure 6:**

*Four roads with two crossings*

With the previous results, the authors now focus attention on the case of four roads with two crossings as shown on Figure 7.
As in the case of two roads and one crossing, we study the relation between the average flow and car density for different ratios between the road sizes. Simulations show that for a fixed size of system, the fundamental traffic diagram depends only on the ratio between the sum of sizes of the priority roads and the sum of sizes of the non-priority roads.

Figure 8: Dependence of the global graph on the ratio between the sum of the sizes of the priority roads and the sum of the sizes of the non-priority roads [9]

Figure 9 shows the comparison of the fundamental graph for two roads (20 sections each) with one crossing, and fundamental graph for four roads (10 sections each) with two crossings. One can remark that a system of four roads with two crossings behaves like a system of two roads with one crossing.
Control and design of crossings

In an attempt to avoid congestion and in order to improve the traffic flow, we can overcome limitations, by the use of open loop traffic lights altering the control strategy of traffic lights (the length of the light phases do not depend on the traffic) or feedback control (lengths of the phases depend on the vehicle numbers in the controlled streets, case of local feedback, or more generally on all vehicle numbers on the different streets).

Going deeper into numerical applications, it can be shown that even with a simple local feedback, we are able to reach the maximal possible flow. Figure 10 depicts experiments that have been done using:

Right priority (1), open loop light control (2), feedback light control (3).

Figure 10 highlights the fact that traffic lights improve the flow only at a medium and large density and do not reduce the flow of a small density. Furthermore, feedback policy strongly improves the state of the system especially at high density. In addition, a feedback light control dissolves jams faster than an open loop traffic light system.

This central conclusion has an important impact for the case of cybercars.

Exploiting further the properties of automated driverless vehicles, the necessary feedback for the crossing control policy, can be easily obtained since communication can be established
amongst vehicles and vehicles with the infrastructure (for instance, real-time detection of the presence of traffic waiting at lights, or along the road in general, warning for an accident or other obstacles limiting the access of a road or other special circumstances-events causing an unusual demand at a road-intersection...)

Likewise a more sophisticated dynamic control of the traffic flow, well adapted to circumstances, can be provided.

As long as the exchange of information is constant, giving current, stable and reliable information, the necessary feedback will be correctly guaranteed, and so once again in the case of the crossroads we can have the optimal policy concerning the vehicle flow according to the Fundamental Traffic Law.

It is important to use the information obtained correctly and crucial that the messages exchanged between the vehicles and the infrastructure be robust and the treatment of the collected information reliable. This will ensure that the feedback on the state of the system is current and adequate to control the crossing properly.

**Improving the crossing design**

Throughout the analysis [9] have used crossroad models where only one vehicle can stay in the crossing section. They also consider the case of a larger road where there can be two vehicles at the crossing. Figure 11 illustrates this situation.

**Figure 11: Fundamental Graph with buffer of size 1 and 2 at crossing [9]**

We can see that during the average density phase, the improvement is impressive, with a maximum flow rate matching the maximum flow reached on a circular road with no junctions. Unfortunately, during the high-density phase when the number of vehicles exceeds the capacity of the non-priority road, a deadlock can occur. Dynamic traffic control using feedback can provide excellent results, constituting an important alternative approach to controlling traffic jams. Consequently even in this case, the fundamental traffic diagram can obtain the same form as in a unique circular road.

By making some minor assumptions it is reasonable to say that a pool of automated vehicles as described in the previous model will behave in an optimum manner. The smooth flow of traffic is maintained from a constant exchange of information as the situation changes.

The fundamental traffic diagram of a system of four roads with two crossings presents the same phases as the model of two roads with one crossing.
When the density is low, vehicles move freely. For medium densities, vehicles on the roads with priority move freely whilst the others have to wait at crossings. The high-density phase starts as soon as traffic volume is sufficient to form a circuit of full non-priority roads. In the latter case there are almost always deadlocks.

**Traffic light control to avoid bottling-up**

With feedback traffic light control combined with speed reduction, [9] achieve the best possible control of traffic and by buffering the crossing it is possible to match the flow rate diagram of a unique circular road without a crossing and without speed reduction. Furthermore, the knowledge of modelling circular roads and crossroads leads to the possibility of modelling an entire town.

The use of platoon of automated cars, can provide one of the best environments to apply the above results and by establishing various communication technologies to each car, messages are transmitted and received, providing the necessary feedback for traffic control.

### 5.2 Reservation algorithm for crossroads

Another promising idea concerning the case of crossroads is a "Reservation Algorithm" described in [22]. This algorithm allows each vehicle to cross an intersection once its request is authorized based on acceptance at a time $t$ according to its direction, speed and vehicle dimensions.

The key principle is to attribute parts of the crossroads to each vehicle for a given period and distribute this common resource (intersection) in the most efficient way in order not to block the path of other vehicles or force excessive speed reductions.

Each vehicle must pass the crossroad as fast and safely as possible, avoiding all risk of collisions.

Given the dynamics of vehicles, attainable two-dimensional traces on the road can be determined, as the figure below illustrates. Each vehicle following one of these traces reaches its target-outgoing lane. Only parts of the 2D traces are collision-prone. The authors consider that the risk points are where at least two traces intersect.

**Figure 12: Attainable two-dimensional traces [22]**

The following figure depicts the three steps of the reservation algorithm.
When a vehicle is reaching the vicinity of a crossroads, it asks the infrastructure (supervisor) for the crossroads geometry.

To conformably maintain its speed, it sends a reservation request to the infrastructure.

A message is communicated back to the vehicle indicating the acceptance or refusal of the vehicle's request.

In principle, a reservation request will be accepted if all the critical points required are free to be reserved during the requested period. This must hold true for all critical points, otherwise the reservation is rejected.

For a specific vehicle:

If a reservation is accepted the vehicle either maintains a constant speed or asks for a new reservation at a higher speed. If a reservation is refused the vehicle reduces its speed so as to stop if required before approaching the first critical point.

The simulation results point out the efficiency of the algorithm. Table 6 illustrates the performances of the following two policies compared to the reservation algorithm:

- None, allowing every vehicle to pass the intersection at full speed disregarding the danger of possible collisions;
- Polling, allowing only one vehicle to pass the crossroads.

<table>
<thead>
<tr>
<th></th>
<th>Time (s)</th>
<th>Collisions</th>
<th>Vehicles</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>min</td>
<td>max</td>
<td>average</td>
</tr>
<tr>
<td>None</td>
<td>5.28</td>
<td>10.80</td>
<td>6.21</td>
</tr>
<tr>
<td>Polling</td>
<td>5.28</td>
<td>92.02</td>
<td>47.37</td>
</tr>
</tbody>
</table>
It is worth highlighting too that the reservation algorithm prevents collisions (a vehicle is required to have reserved a critical point before passing it) while authorising a satisfactory number of cars to go through it.

The central conclusion here is that within this framework an intelligently administrated scheme is developed, improving crossroads management, perfectly adapted for fully automated vehicles (where the exchange of all necessary information is feasible and multiple tasks necessary for the computational/decisional parts of this algorithm are effectively realised).

6 Communication tests for certification

The aim of this chapter is to define test protocols for communication evaluation, which can be used in the certification process of cybercars and dual mode vehicles. Within CityMobil D3.3.1 and D3.4.1 test protocols for the functions of respectively obstacle detection and navigation control are described which can be used in the certification process of cybercars and dual mode vehicles. Both obstacle detection and navigation control have specific requirements for vehicles such as cybercars and dual mode vehicles. For the vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communication of cybercars and dual mode vehicles the requirements are less specific. Several EU projects like Prevent/Willwarn, GST, Safespot, CVIS and Coopers are or have been investigating applications that make use of v2v and v2i applications. Most of the safety related applications developed within these projects have similar communication requirements as the requirements for the different CityMobil scenarios. For cybercar developments it is therefore important to join the certification activities of these developments. Especially the car2car and comesafety consortia drive standardisation processes. Especially the CERTECS subproject of the EU project GST has made a significant effort to develop a certification framework for telematics components. Consistent with the before mentioned deliverables, section 6.1 contains a short summary of the different steps needed to reach certification of a cybercar system. After this a proposal of a test procedure is shown and explained in more detail in section 6.2. Section 6.3 contains links between the test procedure and the different defined CityMobil scenarios.

6.1 Certification procedures

In sub-project 2 of CityMobil future scenarios are addressed. As part of this subproject, WP 2.5 –Legal and administrative issues has made a brief survey of existing legislation, legal traditions and cultural differences in Europe. Deliverable 2.5.3 [29] the existing standards and guidelines that could be relevant for the future certification of cybercars. The information in that deliverable is primarily based on the work documented in D6.1 [26] and D6.2 [28] of the EU project CyberCars. A short summary:

Traditional vehicles that use public roads have to meet a large number of requirements laid down in standards and regulations. The sheer number of standards limits the car developers in their innovations. But the standards also give the developers guidance on how to create safe and reliable vehicles. When they develop new vehicles the manufacturers know the limits within which they have to stay in order to have their vehicle certified for use on public roads.
In contrast to the extensive set of certification standards for traditional vehicles, there are hardly any rules for vehicles that use private grounds or for vehicles that do not fit into the categories of the European Directive 70/156/EEC. This means on one hand that manufacturers have a large amount of freedom in designing their systems, which creates room for innovative solutions. On the other hand, however, manufacturers and operators run great liability risks in case something goes wrong with their systems. Operators and authorities will be reluctant to introduce innovative systems if there is no objective judgment possible on the safety of such systems. An objective judgment is only possible if it can be proven that a system meets generally accepted standards.

Traditional road vehicles are meant for use on public roads. These public roads represent a system to which a very strict set of rules, that we call traffic regulations applies. When a car is certified the environment in which it is to operate is not explicitly considered. That is not necessary because it is an implicit part of the vehicle design that the vehicle will operate in: the very rigid environment of our public road system. This however is different for Cybernetic Transport Systems.

To reach certification for a cybercar system in a certain environment ideally the following is needed:

- A comprehensive safety assessment of the vehicle in its surrounding. CityMobil deliverable D 2.5.3 contains the theory of both the risk reduction methodology and safety assessment analysis. It is not sufficient to certify the vehicle and vehicle related systems because of the interaction of the vehicles with the environment. The risk reduction methodology is a first step aiming at reducing the safety risks associated with the environment. After that a safety assessment analysis aims at reducing the safety risks associated with the system as a whole.

- A set of standards, which the cybercar system or subsystem or certain functions of the system should meet.

The three main functions that drivers carry out are observing; analysing/deciding and transferring the decision to the vehicle systems. In a cybercar the sensors, the obstacle detection system, the vehicle controller and the different actuators take over these functions. Input for the vehicle controller can be information received through V2V or V2I communication. For traditional vehicles standards on component level exist. For these 'new' components such standards do not exist. In the following sections an attempt is therefore made to define a test protocol to evaluate the communication function of a cybercar or dual mode vehicle.

6.2 Communication test procedure

The base of the communication in a cybercar or dual mode vehicle system will be existing serial-production systems like the ones discussed in section 3. For these available techniques (e.g. WiFi) standards are available, which means that for cybercar applications no extra conformance testing is needed. Communication testing can therefore be limited to interoperability testing which will be used to prove the end-to-end functionality between two communicating systems. This end-to-end functionality is rather basic: send data in a certain time period, with a certain maximal latency time. The evaluation of this functionality is therefore really straightforward. The requirements mentioned in CityMobil deliverable D3.1.1 and in chapter 4 of the current deliverable strongly depend on the specific application but remain rather general. The V2V and V2I communication should be reliable and fast (enough). Both these requirements are more stringent when vehicles are closer to each other.
6.2.1 V2V communication
This procedure is only valid for cybercar or dual mode vehicle systems in which the different vehicles should communicate with each other. The V2V procedure is really straightforward. The interoperability between the communication systems in two vehicles will be evaluated. The vehicles will drive towards each other, both at the maximal velocity at which these vehicles are allowed to operate in their operational environment. If in the operational environment no communication is envisioned with vehicles travelling in the opposite direction than one of the vehicles should have zero velocity.

**Figure 14: Test course**

![Test course diagram](image)

The criterion at which the communication system is judged is the ability to send data and receive this data within a certain latency time. This communication should be possible when the vehicles are within the maximal communication distance needed in their operational environment (with a maximum of 500m). Since the latency time and maximal communication distance strongly depend on the application and communication system, no specific limits are set.

**The following procedural steps should be taken:**
Two vehicles have to drive in a straight line. The distance D2 between the vehicles should be set at 5m. Vehicle 1 should have the possibility to send a message through its communication system at a specific accurate time. Vehicle 2 should have the possibility to show the message and the accurate time of receipt. The time measurement in both vehicles should be synchronized. The communication will be checked by a confirmation of the receipt of the message and the latency time should be lower than the maximal latency time needed in the operational environment.

Perform the tests under the following conditions:

1.1 The distance between the vehicles at the moment of transmittal of the message should be the maximal communication distance needed in their operational environment.

6.2.2 V2I communication
This procedure is only valid for cybercar or dual mode vehicle systems in which there is communication between the vehicle and the control centre. The procedure is identical to the V2V procedure in which one vehicle is replaced by a static control post. If the vehicle is able to communicate to the control post than vehicle 2 is replaced by the control post. If the control post is able to communicate with the vehicle than vehicle 1 is replaced by the control post. If communication is bidirectional than the test has to be performed twice, switching the control post from sending to receiving. The communication will be checked by a confirmation
of the receipt of the message in the control post or in the vehicle and the latency time should be lower than the maximal latency time needed in the operational environment.

### 6.3 Communication test for the different scenarios

The following table contains the four CityMobil scenarios as described in chapter 4. For each scenario the most important characteristics are shown. On base of these characteristics the communication tests that are most suited to evaluate the communication performance are marked and when needed, additional remarks are made.

**Figure 15: Test protocols for CityMobil scenarios**

<table>
<thead>
<tr>
<th>Scenario</th>
<th>1. V2V communication</th>
<th>2. V2I communication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Town centre</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dual mode vehicles</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication with a control centre</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Principal road with an equipped e-lane</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dual mode vehicles</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication with infrastructure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to obtain clearance</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Inner city centre</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cybertcars</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication for fleet management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>with fleet manager and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>possibly between vehicles</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Shared traffic space</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cybertcars</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dual mode vehicles</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automated high tech buses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication with traffic manager</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Within the requirements described in D3.1.1 and in chapter 4 of the current deliverable no specific requirements for the latency time and communication distance are mentioned.

### 6.4 Remarks test procedure

In the section above an attempt is made to define a test protocol for the communication system of a cybercar or dual mode vehicle, which could be a base for a future standard. The following is noted:

1. Critical in communication systems is their reliability. The test procedure only contains a very limited number of possible test configurations, the effect of surrounding objects etc are not taken into account. Since a certification test protocol is described which could become used in the standardized certification process of a cybercar vehicle it is not feasible to include a large range of measurements under different environments. These tests should be part of the development of the communication systems. The risk and the effect of possible malfunctioning of the communication systems of a particular cybercar under certain (environmental) conditions has to be evaluated in an extended safety assessment of the vehicle in its surrounding.
2. The description of the test procedure is not fully-determined. I.e. not all dimensions and locations are explicitly mentioned. This would go in to too many details, more than needed at the moment of writing.

3. Since the latency time and maximal communication distance strongly depend on the application and communication system, no specific limits are set yet.

4. Again it must be noted that to reach certification of an entire automatic guided vehicle system, the certification test of e.g. the function of communication is only part of the process. A comprehensive safety assessment of the vehicle in its surrounding is required. The safety analysis should give indications of the risk of malfunctioning of the navigation control function in non standard situations.

7 References


