EUROPEAN COMMISSION

DG RESEARCH

SIXTH FRAMEWORK PROGRAMME

THEMATIC PRIORITY 1.6

SUSTAINABLE DEVELOPMENT, GLOBAL CHANGE & ECOSYSTEMS

INTEGRATED PROJECT – CONTRACT N. 031315

CityMobil

Towards advanced transport for the urban environment

Deliverable no.	D. 2.5.3
Dissemination level	Public
Work Package	2.5 Legal and administrative issues
Author(s)	WP 2.5 partners: IKA, SINTEF, TNO
Co-author(s)	
Status (F: final, D: draft)	F : Version 3.0, 10-05-2010
File Name	Guidelines for safety, security and privacy; barriers to implementation
Project Start Date and Duration	01 May 2006 - 30 April 2011

SIXTH FRAMEWORK PROGRAMME

TABLE OF CONTENTS

Abstract

CityMobil is an Integrated Project in the 6th Framework Programme of the European Union. The project aims at achieving a more effective organization of urban transport, resulting in a more rational use of motorized traffic with less congestion and pollution, safer driving, a higher quality of living and an enhanced integration with spatial development. The project is divided in 6 sub-projects. Sub-project 2 deals with future scenarios. Work package 2.5 of sub-project 2 focuses on legal and administrative issues. The results of WP 2.5 are presented in two deliverables: D.2.5.2: Certification guidelines for advanced transport systems and the present deliverable D.2.5.3.

Deliverable D.2.5.3 focuses on two main subjects: 1) The definition of a number of guidelines for safety security and privacy in automated transport systems and 2) An overview of barriers that are still in the way of the large scale introduction of automated transport systems and strategies to remove these barriers. The deliverable is meant to be used as a tool to assist stakeholders in making their decisions concerning the implementation of an advanced transport system. Therefore the deliverable only contains the final results of the work. Further details of the work on barriers, safety, security and privacy, intermediate steps and a report of the work that was done in the first phases of the project are included in deliverable D.2.5.1.

1 Introduction

The CityMobil project "*Towards advanced transport for the urban environment*" aims at achieving a more effective organisation of urban transport, resulting in a more rational use of motorised traffic with less congestion and pollution, safer driving, a higher quality of living and an enhanced integration with spatial development. This will be achieved by promoting the introducing of advanced technologies into the transport environment. The concepts, methods and tools developed in CityMobil will be validated and demonstrated in a number of different European cities under different circumstances. The three main demonstrators will take place in Heathrow, Rome and Castellón. These will be real implementations of innovative new concepts, and represent the first stages of automated transport systems that are really integrated in an urban environment. A number of smaller events will take place in different locations all over Europe.

CityMobil is divided in 6 sub-projects. Sub-project 2 "Future scenarios" investigates how automated road transport systems fit into the expected scenarios for advanced transport in the future. Work Package 2.5 "Legal and administrative issues" within this sub-project aims at identifying legal and administrative barriers that are in the way of large scale introduction of advanced transport systems, to take them away where possible and to define strategies for the removal of the remaining barriers.

For the purpose of a good understanding the following definitions are used:

- Safety: The level of protection in case of malfunctions of the system.
- Security: The protection against unfriendly actions of other people
- Privacy: The level of protection of personal information

Work Package 2.5 consists of two parts. In the first part from month 1 (the project started in May 2006) to month 18 (November 2007) certification procedures and recommendations for safety, security and privacy have been developed. The results of part 1 were laid down in CityMobil deliverable D.2.5.1. This deliverable thus represents an intermediate state in the work of WP 2.5.

In the second part, from month 19 (December 2007) to month 44 (January 2010) the draft certification procedures were evaluated by applying them to the new transport system for the Fiera di Roma, the subject of one of the 3 large scale CityMobil demonstrations. The results of the evaluation and the final procedures can be found in CityMobil deliverable D.2.5.2.

The recommendations on safety, security and privacy and the results of the discussions on barriers, were further discussed in a workshop in Brussels in November 2009. During the workshop the WP 2.5 partners were supported by two experts: Mr. T.M. Gasser from BAST in Germany, who also provided the draft text for paragraph 5.1 and Dr. Jørn Vatn, from SINTEF in Norway. Their contribution was highly appreciated. The results, a series of guidelines on security and privacy and strategies to address the remaining barriers are included in the present document: CityMobil deliverable D.2.5.3.

2 Safety

Safety, in this case is defined as "The level of protection in case of malfunctioning of the system". Robustness, the resistance a system should offer against incorrect use is also considered a part of safety. The safety issue is extensively covered in CityMobil Deliverable 2.5.2 [1], where the newly developed certification procedures for advanced transport systems are described. Therefore this chapter on safety will only contain a brief description of the process that must be followed to come to a safe system.

A 4-step procedure is defined that could in future cover safety and certification of automated transport systems.

1. Preliminary risk reduction
2. Determine which safety regulations apply
3. Production and implementation of the system
4. Certification

1. Preliminary risk reduction

In the first step the Risk Reduction Method [3] is used to roughly analyse a number of issues that have influence on the safety of the transport system in its environment. The basis of the analysis is a series of checklists that take into account a number of actors present in the environment and estimate their influence on the safety of the system. The analysis is carried out by the authorities, the operator and the evaluation organization. The result is a series of recommendations that can be applied in the first planning phase. By following the recommendations, fewer corrections will need to be made in the later stages. The Risk Reduction Method is a ‘quick and dirty’ method that is also suitable as an instrument to evaluate the safety of showcases and demonstrators, where a comprehensive safety analysis is impractical or too expensive.

2. Determine which safety regulations apply

In the second step it is established which existing safety regulations the system should meet. In addition to the safety evaluation and certification procedure, most systems will have to meet particular requirements, related to the environment they are being used in. For instance, requirements concerning the applicability for disabled people or local fire regulations. The second step is carried out by the authorities and the evaluation organization.

3. Production and implementation of the system

In the third step for which the manufacturer of the system is responsible, in combination with the operator, the system is produced and implemented on site. For the production phase it is highly advisable to follow the Code of Practice for the design and evaluation of ADA systems, as developed in the Response projects [4]. Although the recommendations in the Code of Practice are meant for standard cars with drivers, most of the recommendations are directly applicable to fully automated systems and can greatly improve the safety of a system if applied correctly. For the safety evaluations the analysis method described in step 4 should be used.

Depending on the size and complexity of the system the principles of life cycle safety should be followed. According to these principles safety is a part of all the process steps during the design, development and building of a product. Safety should be a constant issue of attention during the period in which the product is operational and even the safety implications of the final dismantling of the system should be taken into account. Applying the principles of life cycle safety in the period of production and implementation means that safety analysis should be carried out in a number of phases of the design/development process, ending with the last safety analysis that will be the basis for certification. The procedures for carrying out these safety analyses in principle is the same as described in CityMobil deliverable D.2.5.2 [2] for the certification.

4. Certification

In the final step the system is certified, using the certification procedures described in CityMobil Deliverable 2.5.2 [2]. An independent evaluator should carry out the procedure, until, after formal acceptance of the procedures by the European authorities a notified body will take over this task.

If these four steps have been followed with a positive result, the system can be considered safe enough to be introduced.

Table 2-1 : Procedures for automatic modes

Step	Procedure	Responsible
1	Risk Reduction Method	Authorities, operator and evaluation organization
2	Safety regulations	Authorities and evaluation organization
3	Production and implementation	Manufacturer
4	Certification	independent evaluation organization

3 Privacy

This chapter concerns privacy which is defined here as "the level of protection of personal information". The most important standards for the protection of privacy in Europe are the following two documents:

- Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Chapter 4 concerns security, defined here as "the protection against unfriendly actions of other people". It is clear that there is a sensitive balance between the requirements of privacy and security. More security often means less privacy and more privacy often results in less security. Most of the measures described in chapter 4 to enhance security have negative privacy implications. Therefore it was decided to treat privacy not separately in detail in chapter 3, but make it part of the security discussion. Which issue, privacy or security should have the most weight depends on a number of parameters, for instance: the type of transport system, its location, whether it is isolated or part of a busy environment and also on privacy laws that can be different from one European country to the other.

4 Security

4.1 Personal security

Security is defined here as "the protection against unfriendly actions of other people". There is a difference in the perception of personal security for passengers of an automated public transport system and a traditional transport system. In traditional transport systems there usually is a driver or other official persons present. The presence of people who are obviously there for professional reasons enhances the security and the feeling of security. In automated transport systems there often is nobody physically present. Therefore some measures are advisable in addition to those measures that are also taken in traditional systems. The guidelines described in this chapter are such additional measures meant to increase the security and the feeling of security of the passengers.

*e*Safety is a joint industry-public sector initiative driven by the European Commission and co-chaired by ERTICO – ITS Europe and ACEA (European Automobile Manufacturers Association), with the aim to promote the development, deployment, and use of Intelligent Vehicle Safety Systems to enhance road safety throughout Europe. The eSafety Forum Steering Group (SG) decided to establish the eSafety Security WG at its meeting on 15 January 2007. The objectives of this WG are to investigate eSecurity needs, which address the vulnerability of Road Transport introduced by the misuse of networked and co-operative systems, integrate existing and emerging RTD initiatives and provide a communication platform of all major stakeholders in order to support the introduction of eSecurity technologies in parallel to the technical progress and compatible to legal and certification aspects. The draft report of the eSafety Security WG can be found on the web. [5]

The following personal security issues (often combined with privacy issues) will be treated here:

- Access control
- Monitoring
- Communication
- Emergency procedures
- Identification
- Lighting
- Information systems

Guidelines for access control

The goals of access control are the following:

- To only allow people that are authorized to use the system (holders of a valid ticket)
- To enable people to enter the vehicle in a safe way
- To prevent people from entering if the maximum number of persons allowed is reached
- To prevent people from entering in case it concerns a private vehicle

Systems that can pick people up at any location are comparable to private cars. Access control issues will be less important, because usually there will not be other persons present when the vehicle is entered. Therefore only systems that use designated stops are treated here. Furthermore it is important to distinguish between public vehicles and private vehicles.

Guideline 1

In case of public vehicles everybody who has a valid ticket is authorized to use the vehicle. To check whether all users have a valid ticket is one way of increasing security in public vehicles. The gateway systems that are widely used in metros could also be used at designated stops of driverless systems. This will increase the costs of stops, but it will also allow checking the maximum number of persons using a vehicle. Furthermore, safety and orderly access is further improved if these gates are combined with a system that helps people to make orderly queues.

Guideline 2

The feeling of security will be greatly enhanced when people have the possibility to reserve a private vehicle. Making private vehicles available, possibly against a higher fee, is therefore an option to be considered where possible. When someone has ordered a private vehicle, or when the system only consists of private vehicles, access can also be controlled by gates as mentioned above. A key card system that only gives access to the dedicated vehicle would provide additional security. The possibility to lock the vehicle from the inside, like in standard cars would also further enhance security.

Unless ticketing systems allow identification of individual passengers there are no serious objections against these access control systems from a privacy point of view. The possibility to identify passengers does improve the personal security. Whether or not ticketing systems allow such identification is a matter of local law. In this respect, there is no difference between driverless systems and traditional public transport.

Guidelines for monitoring the inside and outside areas with cameras and television systems

In contrast with the access control systems mentioned above there are significant privacy aspects related to monitoring with Closed Circuit Television systems (CCTV). The legal regulation of CCTV varies greatly across Europe. Its employment is regulated by federal and state data protection acts, by police laws and codes of criminal procedure, by specific laws on video surveillance and by special regulations for locations such as banks or sport stadiums. Also copyrights provisions influence the usage of CCTV.

In some countries strict regulations exist with regard to private CCTV systems. In other countries only public systems are legally regulated. As a general rule, different acts govern the employment of CCTV for purposes of public security and the prevention of disorder or crime. The employment is regulated by specific laws as police acts. Some countries such as Spain have explicit laws for CCTV surveillance by the police in the public realm. In Denmark the “Law on the ban against TV-surveillance”, which came into force on July 1st 1982 forbids the private use of CCTV in public areas. In other countries such as Germany explicit sections on CCTV can be found in the data protection acts. From case to case this variety causes major differences, for example, in regard to the demand of transparency as required by data protection regulations. In Great Britain there is no explicit CCTV law and there is also no explicit regulation of video surveillance in the British Data Protection Act. But meanwhile there is a "Code of Practice" issued by the British Information Commissioner that sets a framework on how the Data Protection Act of 1998 should be put into practice in regard to CCTV. As this code does not have any independent legal character it is unknown how effective it is. Nevertheless, besides this formal diversity of legal regulations there are different regulatory tools such as the registration of systems as it is known from France, Norway and Sweden or the notification in order to guarantee transparency. [6]

Taking into account the privacy requirements the following guidelines are recommended:

Guideline 3

At designated stops and stations there should be camera systems monitoring the areas where people are present. Permanent surveillance is important for 2 reasons: protection against misuse and vandalism and protection against terrorism. Protection against terrorism will be more important in case of an area where many people can be present. To guard people's privacy the recordings should not be saved for more than a certain time period. Access to the data should be restricted to the police and bound to strict rules. In areas where there is permanent camera surveillance people should be informed by means of clear signs.

Guideline 4

For privacy reasons, permanent video monitoring of the inside of the vehicles is not recommended. However, in case of emergency a passenger should be able to press a button that switches on a camera that covers the inside of the vehicle. This will allow the operator to take action if needed. In case of private vehicles there are no privacy issues, since the passenger has willingly switched on the camera. It must be made clear, however, for instance by means of a sign, that pushing the button switches on a camera. In case of public vehicles the same restrictions with regard to the time recordings are kept and the access to recordings as mentioned above for the designated stops should be observed.

Guideline 5

Cameras outside the vehicle, that monitor the area around the vehicle, can be important for security reasons. In order to protect privacy of people being recorded, these cameras should not record situations permanently, but they should be switched on by the operator, in case the operator is notified of a special situation requiring monitoring. The same restrictions with regard to the time recordings are kept and the access to recordings as mentioned above for the designated stops should be observed.

Guidelines for communication systems connecting the passengers with the operator

The personal security and the feeling of security will be greatly enhanced if passengers of driverless systems have a possibility to speak one on one with an official person, for instance at the operators desk. The contact should be initiated by the passenger, for instance by pressing a button. For privacy reasons the communication system should only be switched on when the passenger initiates contact. Such a communication system is not necessary in high tech buses, where a driver is present. In driverless vehicles for private use, which are comparable to standard cars a communication system is not necessary for security reasons, but could be helpful in case of emergencies.

Guideline 6

In driverless vehicles for public use and on designated stops a two-way communication system that guarantees immediate contact with a person at the operator's desk should be installed. The person at the operator desk must be able to make quick decisions and take necessary measures. Guidelines for an acceptable response time should be established. The communication language is of importance. In cosmopolitan areas, like big cities the operator should be able to speak at least two different languages (the native language and a wide-spread language like English). For privacy reasons, restrictions for the period that recordings are saved and the access to such recordings should be in place.

Guidelines for emergency procedures

For Cybercars an emergency button to stop the vehicle is required. Whether or not that same button will allow the doors to be opened depends on the local situation. Information on how to behave in case of emergencies is to be provided in visible and comprehendible form. Communication with the operator must be possible in case of an emergency. PRT-systems also need to have an emergency button to stop the vehicle and a mechanism for opening the doors (similar to trains).

Guideline 7

Each driverless vehicle for public use should have a clearly marked emergency button. Whether or not the vehicle stops when the button is pushed depends on the local situation. The vehicle should always go to a fail-safe state. This could mean that in some cases the vehicle stops, so that the passenger can leave the vehicle and in other cases the vehicle continues on its way for a certain distance. In all cases the emergency button should trigger the vehicles cameras and initiate contact with the operator's desk, so that the operator can take action, if required.

Guideline 8

Each vehicle should have a door open button that will enable passengers to leave the vehicles in case of an emergency. The button should only operate when the vehicle is at a standstill and should only open the doors in a situation where that does not cause immediate danger for passengers that leave the vehicle. In all cases the emergency button should trigger the vehicles cameras and initiate contact with the operator's desk, so that the operator can take action, if required.

Guidelines for lighting

Vehicle lighting is to be divided into inside and outside lighting. The purpose of outside lighting is to be seen and recognized, in case vehicles share the roads with conventional traffic or other traffic participants such as pedestrians and cyclists. The purpose of inside lighting is to be able to see inside a cabin.

Guideline 9

Cybercars, high-tech busses and advanced city vehicles require standard outside vehicle lighting, as they can share the road with other traffic. PRT-systems do require outside lighting only at PRT-stops as they drive on dedicated tracks. In public vehicles, the inside lighting should be on when the daylight situation requires it. In private vehicles the inside lighting should be off, with a possibility for the passenger to switch it on, as required.

Guidelines for information systems

Having adequate information available about the status of the vehicle, emergency procedures and instructions increases the personal security of passengers. Other information can be given as well, but such information is not immediately important for security reasons.

Guideline 10

An information system to provide information on status, emergency procedures and instructions, should be installed in every vehicle. The HMI should be easy to understand, even for non-skilled users and foreigners.

4.2 Protection against terrorism

The terrorist attacks in New York in September 2001 and later events like the Madrid and London attacks have shown that transport systems can be terrorist targets. The efforts to protect passengers and equipment can become barriers against use of a transport system, because they can increases the travel time and the cost of using the system. Nevertheless it is important to consider the terrorist threat and arrange sufficient protection.

It is not possible to protect transport systems entirely from the risk of terrorism. Most transport systems are meant to be open to any potential user, and it is hard to know who has terrorist intentions and who has not. Driverless systems introduce particular risks, because a terrorist could place a bomb into a driverless vehicle and send it into a busy area without immediate danger to him- or herself.

For reasons of privacy identification of passengers is not an acceptable option.

Guideline 11

There should be camera systems inside the vehicle to check that empty vehicles that are requested to go to a certain station are really empty. For instance by means of cameras with AID (automatic incident detection) and alarm systems. The camera should only be switched on if there is no person present in the vehicle. If there are unidentified objects in the vehicle, the control system should redirect the vehicles to a safe place, or prevent them vehicles from driving at all.

Guideline 12

It is important to ensure that the data systems are protected against hacking.

4.3 Protection against vandalism and misuse

Vandalism is a problem in public transport systems in many places. There are some measures that will reduce the effects of vandalism. Misuse of the system can either be misuse on purpose or misuse because the users are not aware how the system works. One of the most likely cases of misuse is misuse of the alarm system. This is also one of the cases against which protection is most difficult, because the alarm system should always be accessible and consequently is very visible. A driverless vehicle could be a tempting shelter for homeless people or playing children. To avoid this kind of misuse the access control measures as mentioned above can help.

Guideline 13

Damage to the equipment due to vandalism can be avoided partly by choosing a vandalism-proof design. For instance: objects that are not fastened properly can be easily broken off or damaged and weak materials could be too easy to destroy. It is recommended to use materials with surfaces which can easily be washed or cleaned.

Guideline 14

In order to avoid damage to the equipment because passengers are unaware of how the system works, it is important to keep all instruments and information as simple and self-explanatory as possible.

4.4 Freight security

An important application for driverless systems is the possibility to transport goods instead of people. For freight transports dedicated vehicles can be used, but it is also possible to use the same vehicles that are used for people transport in dual-mode use. In principle, systems for transporting goods are closed systems, where only authorized personnel will be allowed to load and unload the system. It is not allowed for people who are not authorized for freight transport to send goods in a passenger vehicle to a certain location without a person present. In this case the system described in guideline 11 will detect this and appropriate action will be taken.

Guideline 15

Since only authorized personnel are allowed to load and unload the system for freight purposes, privacy is a less important matter. The identity of the handlers of the system is

known. Cameras inside the vehicles can be switched on at all times. Only authorized personnel should be allowed to open vehicles.

Guideline 16

If vehicles are used for dual-mode purposes, the vehicles should be checked for unidentified objects before entering or re-entering passenger mode.

Guideline 17

Dangerous goods as well as goods of high value (for instance money) should not be allowed in automated transport systems in order to minimize the danger of terrorism and theft and on the other hand increase the safety of the transport system. Therefore the transport of freight should be in accordance with the multilateral agreement of the United Nations (see ADR 2007 Accord Européen sur le transport des marchandises dangéreuses par route, part 3).

5 Barriers

In addition to the barriers related to security, safety and privacy there are other barriers that are in the way of the large scale implementation of automated transport systems. These barriers are treated here as follows:

- Legal barriers
- Political barriers
- Organisational barriers
- Financial barriers
- Social barriers

In the paragraphs below, these barriers will be addressed and actions or strategies to remove them will be defined. The European Conference of Ministers of Transport (ECMT) is an inter-governmental organisation established in 1953 to provide a forum in which Ministers responsible for transport, and more specifically the inland transport sector, can cooperate on policy. Four different ECMT reports presented at a ministerial meeting in Dublin in May 2006 address different policy objectives and policy instruments, they all highlight key barriers to the effective implementation of policies to promote sustainable transport [7]. The work done within the ECMT initiative addresses most of the barriers described but from another viewpoint i.e. from a superior transport political view. In CityMobil the basis is to look into solutions on local level for single towns. CityMobil Deliverable D.2.2.4 City Application Manual [8], also has a section on implementation barriers.

5.1 Legislation

The legal issues of automation can only be outlined according to today's legal situation for road traffic. At least full automation in open traffic is, from a legal point of view, a completely new field. The legal grounds for such applications remain unsolved to a very high extent as the legal situation is specific to manually driven vehicles. However, to gain an overview, it is best to start from the (most likely permissible) applications very close to ADAS today:

Automation as “Assistance” for the driver:

As far as a driver is still available in the vehicle and (only) a certain driving-function has been automated (e.g. steering), the legal issues indeed remain very close to those of driver assistance systems today: This might be considered the case for advanced high-tech buses that offer full automation of steering. If this automation remains at any time fully overrideable (which is assumed in the following, otherwise see below “Vienna Convention on Road Traffic”), the driver has the possibility to take control whenever necessary. It is, however, depending on the design, important to understand the following differentiation between professional drivers and other motorists:

As long as only professional drivers are entrusted with vehicle-guidance (e.g. high-tech buses), it can be assumed that they will have been specially trained for the use of an unusual high-degree automation of functions. Their understanding of system limits can therefore be supposed to be in so far comprehensive. It can also be assumed that these drivers know about their obligation to always pay full attention to other road users, pedestrians crossing the street, etc. and react – by taking control – accordingly (whenever a danger occurs that system limits will not allow detecting). Apart from this, these drivers are continually monitored by passengers and aware of their responsibility for safe vehicle guidance. The full attention of a professional driver at any time can therefore be assumed without a substantial risk of overreliance or system-misuse.

This can be very different in case such systems would be made available in Road traffic to regular motorists. As soon as there is a possibility to turn away from the driving task, it must be assumed that there is a threat that this will happen in some cases, regardless of contrary warnings (e.g. in an instruction manual). It must therefore be assumed that – for the reason of a lack in understanding of system limits or by purpose – the misuse of such automatic steering would be immanent (especially in case longitudinal automation is available in combination with automatic steering, i.e. a combination with systems like Adaptive Cruise Control, ACC).

Yet, at this point it is decisive to point out the difference to “Lane-Keep-Assistance”-Systems already on the market: These systems already offer automation of steering to a certain extent, however, this is very limited: On the one hand there is an automatic “Hands-off” detection that will make the driver take over control after a very short period of hands-free steering (e.g. after 10 seconds) and thus avoid misuse. Another reason lies in system characteristics: low steering torque and the lane keeping layout that will intervene at a very late stage (when lane markings are about to be traversed), make it necessary for the driver to correct the steering angle fairly often. Overreliance and inattentiveness are thus countered.

To summon up for the application the high-tech buses provide: As long as professional and specially trained drivers are in the focus of such a system – that will in most cases offer full automation of a certain function – and the driver can manually take over control whenever necessary, such an amount of automation will usually be considered to remain below the threshold of legally critical design. A proof of this finding according to the national legal situation is nevertheless recommended as this cannot be assessed to full extent for all countries within the EU.

Automation in areas with restricted public access:

All Road-Traffic-Codes, Vehicle-Licensing-Requirements, etc. only take effect on grounds accessible to the public (property may not be decisive, e.g. in Germany). These legal regulations all take their origin in the idea of danger-prevention in case of multiple road-use by the public. If these issues are not applicable, because public access is excluded, safety can be ensured otherwise than via a driver as the legal regulations will not apply. This will most easily be achieved by means of segregation of automated traffic from other subjects. Liability will, however, remain with the operator of such vehicles in case an accident nevertheless occurs and this can be led back to a danger originating in an automated vehicle.

Automation in areas with unrestricted public access:

Up to now it is unclear how to assess which amount of automation will lead to a conflict with laws, regulations, etc. However, different legal issues have already been identified in the past for ADAS. In the following they shall be described as well as those that will apply only in case of automation.

The Vienna Convention on Road Traffic (1968) and national Road Traffic Codes:

The Vienna Convention on Road Traffic is an international treaty on Road Traffic Law between the contracting parties (over 60 countries worldwide). It entitles the contracting (national) country to claim for admission of its citizens to the other countries' traffic under the conditions stated in the convention. The effect the Vienna Convention takes is therefore limited to cross-border traffic and the respective vehicles. The Vienna Convention has strongly influenced many road traffic codes especially in terms of behavioural aspects. The same is true for licensing requirements partially still in place on a national level, even though EU-harmonisation has led to an at least parallel permissibility according to ECE-Regulations within the EU. The Vienna Convention on Road Traffic defines the Driver as "... any person who drives a motor vehicle... [...]" (Art. 1 lit. v Vienna Convention on Road Traffic) and further rules that "every moving vehicle or combination of vehicles shall have a driver" (Art. 8 No. 1 Vienna Convention on Road Traffic). According to Art. 8 No. 5 Vienna Convention on Road Traffic "Every driver shall at all times be able to control his vehicle... [...]" and Art. 13 states more clearly that "Every driver of a vehicle shall under all circumstances have his vehicle under control ... [...]".

This wording is not very surprising considering the fact that at the time the treaty was negotiated in 1968, naturally automation of road traffic was most certainly not foreseeable, and hence, there was no need to regulate this issue.

The strongest effect for the applications shown within CityMobil, however, lie in the fact that according to road traffic codes similar provisions might be in place that might bar the possibility to implement automated vehicles even in certain regions. In how far this is the case should be made subject to professional legal opinion in the country of the foreseen implementation-site.

Whereas the Vienna Convention on Road Traffic itself will in most cases have no direct influence on the permissibility of automation of vehicles used for public transport in certain regions: The reason lies within the negligible effect these vehicles take on cross-border-traffic: It is difficult to imagine that they will ever cross a border within their lifecycle. This would be different, however, in case of private vehicles used for long-distance trips (these are, however, not the focus of CityMobil).

Liabilities:

Road traffic liability will in some countries – as is e.g. the case in Germany – depend on negligence of the driver and depend mostly on the actions the driver takes. It might therefore well be the case that certain provisions no longer correctly mirror the legal situation in case of

automation. For Germany this is the case with Paragraph 18 of the “Strassenverkehrsgesetz (StVG)” – the German Road Traffic Law underlying inter alia the Road Traffic Code: Therein negligent behaviour of the driver is presumed in case of an accident – even though a driver might not be available in an automated vehicle at all or his reaction to a certain situation has no longer belonged to his “driving”-duties. Therefore, a solution for these liability issues might prove necessary as well, even though a solution will often be in reach on a single-case national basis accompanied by full insurance coverage.

Product Liability:

The manufacturer of automated vehicles will be subject to product liability just like the manufacturer of any other product. What must therefore be avoided is the defect of a product. This, however, can also result from the safety of automation applied. The importance of functional safety aspects for non-defectiveness can therefore only be highlighted.

Future assignment of duties in danger avoidance:

Presently the Road Traffic Codes assume the full availability of a driver in every moving vehicle to perform according to driver-duties. Due to sweeping clauses in national Road Traffic Regulations the final decision on and performance of danger avoiding acts is even in very complex situations not clearly ruled but left mostly to the driver. Road traffic codes therefore depend on the availability of a driver as an addressee of legal obligations. A solution to this situation is very difficult to foresee. Solutions on a single-case national basis are, however, possible.

Strategies to address legal barriers

Much depends on the degree of automation. At a low degree it will under certain circumstances prove possible to resort to the driver for safety and responsibility. The higher the degree of automation, however, the more complex the legal issues grow as they presently and generally will be found to recur to the driver’s responsibilities. In case of a high degree of automation this conflict will have to be solved legally, in case automation in areas with unrestricted public access is intended. Further research will be necessary on this aspect in future to achieve large-scale permissibility (i.e. to provide for legal certainty of implementation).

5.2 Political barriers

There can be many reasons for politicians to either adopt or oppose new initiatives on the field of automated transport systems. Reasons for opposition can include:

- Other priorities for available funding
- Change of the laws necessary to allow driverless vehicles can be politically sensitive
- Not enough information available to introduce automatic transport systems
- Election periods could intrude with the planning or implementation of new systems

Automatic transport systems have potentially many benefits. They are usually environmentally friendly, they are safe, they can provide improved transport possibilities for disabled people and the fact that no driver is needed can make the system cheaper than conventional systems and so forth. With such a wide variety of benefits, introducing

automated transport could be appealing to several political wings, even to people who are against public funding in principle.

When an automatic transport system is proposed, it should be completely clear which problem it is meant to solve. (The problems could both be local or regard a wider area). If the system is introduced merely because of the potential publicity it might get disliked, or if professionals are enthusiastic about a new exiting transport system, the system might be implemented in settings where it does not solve any transport problems or even be a burden on the environment. This could lead to too few passengers and economic losses, mistrust in automatic transport systems in general and lack of public funding and support in future projects.

Any demonstration carried out should be precise about what the motive of implementing a new system is. It is also important to measure and report how well new systems work in practice. Successfully implemented projects will improve the reputation of automated transport systems. Information campaigns and other forms of publication of results could become powerful tools in order to make decision-makers aware of gains to be expected by the introduction of automatic transport systems.

Some situations require a combination of means to make the automatic transport system work in association with the rest of the transport system. This might require politically unpopular actions, like extra parking fees, limited access to certain areas for some transport groups and so forth. In these cases information about how the transport system is meant to work as a united system and how the different instruments are fitting in the greater system is important. Also some patience might be needed until the system operates as intended, and until the potential passengers have altered their habits, or overcome personal objections, before they start using the system.

Strategies to address political barriers:

It is difficult to give general guidelines on how to address political barriers, since they can be of very different natures. However, there are two important instruments for the removal of political barriers that can be used almost everywhere: information and publication. Politicians will be more confident in making decisions if they have reliable and extensive information about the advantages an automated transport system could have in their particular situation. Extensive publicity campaigns have proven to be able to change the hearts and minds of people. The same instruments can be used to inform political bodies about the necessities to change the laws that are now in the way of the introduction of automated systems (see also 5.1).

Many of the political barriers are of a local nature, but in case certification or national laws are in play, careful consideration should be given to the political level on which decisions could be influenced. It seems logical to address certification issues and legal issues on a national or even European level, while economic issues often are better addressed locally.

5.3 Organisational barriers

Advanced transport systems are new and plans and strategies to introduce them do not exist. Therefore lack of information is the most severe organisational barrier. There is almost no history of implementation processes and there are no examples that stakeholders can use as a basis for their plans. If a new metro system needs to be introduced the builders can use the experience of many other metros built in cities everywhere in the world, but for automated transport systems no blueprints exist. The introduction of new transport systems therefore requires a good dialogue between stakeholders like politicians, planners and transport providers in order to identify objectives and define strategies. The lack of a concrete

plan can become a crucial barrier to implementation. It is also important to put the new transport system into the correct context; will the new system be complementary to existing systems or will it replace conventional solutions?

The implementation of a new transport system in an existing environment can also be ground for severe barriers. New systems will always intrude in an existing situation and whatever the advantages, there will always be protests by some group or other.

One other important issue is that of safety. Since certification standards for automated systems do not yet exist it is unclear to stakeholders how the safety of automated transport systems can be established. People must be convinced that automatic transport systems without a driver can be safer than more familiar systems with a driver present. Until this has become generally accepted it might be necessary to keep a driver and face the extra cost due to lack of public acceptance.

At the moment of publication of this deliverable there is only one existing automated system for people transport operating in scheduled public transport in the world (the Parkshuttle, operating in Capelle aan de IJssel in the Netherlands). Soon there will also be systems at Heathrow airport (UK) and Masdar City (Abu Dhabi). These examples should be used as much as possible to help convincing decision makers. Good relationships with the builders, operators and owners of these systems will make future implementations easier.

Strategies to address organisational barriers

An information and knowledge plan has to be made to reach the different stakeholders. Commercials, local television etc. can be used for this. Support groups can be established, which could do the lobbying and place pressure on the decision makers. Furthermore, more demonstrators are needed to convince people that automated system really work. It is also important to include these issues in teaching-programs at universities, because that is where the future stakeholders are. The City Application Manual, developed in CityMobil can be used as a basis for a teaching program.

Since the introduction of automated systems in existing environments always will cause problems, it could be advantageous to focus on applications in new cities or suburbs first. In a new city, it is relatively easy to take into account the requirements of a new advanced transport system and since sustainability is an important argument in present-day discussions this can help to convince city planners to consider the advantages of automated transport.

Within the framework of the CityMobil project new certification procedures for automated transport systems have been developed. The next step is to introduce these procedures on a European level and discuss the wider introduction of the procedures with the relevant authorities.

5.4 Financial barriers

Money is one of the main obstacles towards implementing automatic transport systems, especially in the initial phase (when the uncertainty is greatest). There is a great financial risk to be the first city to implement a new system. Later implementations have the advantage to avoid known pitfalls and learn from earlier experiences. Financial risks relate to robustness of cost/revenue forecasts and the likelihood of future financial viability and of obtaining funding for implementation. There may be difficulties in constructing robust forecasts for innovative systems. Additionally there may be problems of “credibility” even if it can be demonstrated that forecasts are robust. This may belong partly in the political category.

Strategies to address financial barriers:

Public-Private Partnerships might be a potential way to address financial barriers. A Public-Private Partnership is essentially a relationship between actors, which may be used in situations where the respective authorities lack the resources (e.g. financial, organisational, knowledge, skills) to overcome delaying and or hindering implementation. Cities in EU member states such as the UK where there is now a strong emphasis on Public-Private Partnerships may be more comfortable with such an approach than cities with a tradition of public sector ownership.

Another potential solution is to focus on cities that have a lot of money available. These could be new cities that are carrying out a major city development plan or cities where a major event takes place (for instance host cities of world championships, Olympic games, etc.) If such cities implement automatic transport solutions, it would also represent valuable PR for this kind of systems.

5.5 Social barriers

Both the authorities and the public can be sceptical about the introduction of advanced and innovative transport systems for various reasons. For instance:

Authorities

- Operational level scepticism
  - Is there someone who can operate and administrate, perhaps also finance, the system in a viable way?
  - Can the system coexist with other local transport systems and other traffic?
  - Is the system vulnerable for specific weather conditions?
- Strategic level scepticism
  - Will the system solve all or some of the problems they were intended to, for instance congestion problems, safety levels, pollution?
- Technological level scepticism
  - Will it work technically?
  - What are the consequences if the technology fails?

General Public

- Personal level scepticism
  - Would drivers and passengers feel uncomfortable using a system which replaces their full control of the vehicle?
  - Will all user groups, regardless of their cultural background, driving experience, etc., manage to use the systems as intended?
- Society level scepticism
  - Would the investment in new systems have a positive or negative impact on the growth of Gross Domestic Product?
  - Would the automatic system replace some of the existing workforce, leading to unemployment?

If the new systems replace or compete with existing transport systems, there is a risk that some of the staff might become redundant. It is therefore important to introduce the system along with a plan that covers such issues. One of the benefits of driverless systems is that they do not need drivers, and that saves costs. Redundant Staff should therefore, if possible,

be offered other positions, maybe as parking inspectors. This happened in Trondheim, when the tram service was stopped in 1987.

The impact of innovative transport systems on local businesses would largely depend on the success of the system. If they deliver all that is promised, it could have a huge positive impact for city and town centres and the businesses located there. It could also bring potential benefits in encouraging redevelopment and new buildings that would be positive for existing businesses. However, on the other side, the failure of a scheme would cast an extremely negative view on a town or city.

The system could potentially become aesthetically intrusive in a city environment. This must be considered when the system is designed. Installation of a new and advanced transport system might have negative impacts on the visual appearance of the city. This could be due to the system's degree of "futuristic appearance", consumption of space, mismatch with the architectonical style of a historical city centre, noise, etc. However, a city's image can be enhanced by a transport system, e.g. the cable tram in San Francisco. The design of vehicles and infrastructure should be complementary to the aesthetics of historic buildings, and help maintain the city's identity.

Even though jobs may disappear with the introduction of automatic systems, new job opportunities will be introduced in designing and operating the new systems. However, the new jobs will probably require more skills than the old ones. This could represent a social barrier.

Strategies to address social barriers:

The most important instrument to address social scepticism is information. People (authorities and the public) should be informed about a possible new system in a very early stage, using the knowledge and information plan as described above under organisational barriers. The CityMobil City Application Manual can also play an important role in taking away the scepticism with the authorities.

6 Conclusions

This report describes the results of the work on safety, security, privacy and barriers to implementation in CityMobil Work Package 2.5. The main result is a number of guidelines and strategies. Below is an overview of the guidelines and strategies.

Guideline 1

In case of public vehicles everybody who has a valid ticket is authorized to use the vehicle. To check whether all users have a valid ticket is one way of increasing security in public vehicles. The gateway systems that are widely used in metros could also be used at designated stops of driverless systems. This will increase the costs of stops, but it will also allow checking the maximum number of persons using a vehicle. Furthermore, safety and orderly access is further improved if these gates are combined with a system that helps people to make orderly queues

Guideline 2

The feeling of security will be greatly enhanced when people have the possibility to reserve a private vehicle. Making private vehicles available, possibly against a higher fee, is therefore an option to be considered where possible. When someone has ordered a private vehicle, or when the system only consists of private vehicles, access can also be controlled by gates as mentioned above. A key card system that only gives access to the dedicated vehicle would provide additional security. The possibility to lock the vehicle from the inside, like in standard cars would also further enhance security.

Guideline 3

At designated stops and stations there should be camera systems monitoring the areas where people are present. Permanent surveillance is important for 2 reasons: protection against misuse and vandalism and protection against terrorism. Protection against terrorism will be more important in case of an area where many people can be present. To guard people's privacy the recordings should not be saved for more than a certain time period. Access to the data should be restricted to the police and bound to strict rules. In areas where there is permanent camera surveillance people should be informed by means of clear signs.

Guideline 4

For privacy reasons, permanent video monitoring of the inside of the vehicles is not recommended. However, in case of emergency a passenger should be able to press a button that switches on a camera that covers the inside of the vehicle. This will allow the operator to take action if needed. In case of private vehicles there are no privacy issues, since the passenger has willingly switched on the camera. It must be made clear, however, for instance by means of a sign, that pushing the button switches on a camera. In case of public vehicles the same restrictions with regard to the time recordings are kept and the access to recordings as mentioned above for the designated stops should be observed.

Guideline 5

Cameras outside the vehicle, that monitor the area around the vehicle, can be important for security reasons. In order to protect privacy of people being recorded, these cameras should not record situations permanently, but they should be switched on by the operator, in case

the operator is notified of a special situation requiring monitoring. The same restrictions with regard to the time recordings are kept and the access to recordings as mentioned above for the designated stops should be observed.

Guideline 6

In driverless vehicles for public use and on designated stops a two-way communication system that guarantees immediate contact with a person at the operator's desk should be installed. The person at the operator desk must be able to make quick decisions and take necessary measures. Guidelines for an acceptable response time should be established. The communication language is of importance. In cosmopolitan areas, like big cities the operator should be able to speak at least two different languages (the native language and a wide-spread language like English). For privacy reasons, restrictions for the period that recordings are saved and the access to such recordings should be in place.

Guideline 7

Each driverless vehicle for public use should have a clearly marked emergency button. Whether or not the vehicle stops when the button is pushed depends on the local situation. The vehicle should always go to a fail-safe state. This could mean that in some cases the vehicle stops, so that the passenger can leave the vehicle and in other cases the vehicle continues on its way for a certain distance. In all cases the emergency button should trigger the vehicles cameras and initiate contact with the operator's desk, so that the operator can take action, if required.

Guideline 8

Each vehicle should have a door open button that will enable passengers to leave the vehicles in case of an emergency. The button should only operate when the vehicle is at a standstill and should only open the doors in a situation where that does not cause immediate danger for passengers that leave the vehicle. In all cases the emergency button should trigger the vehicles cameras and initiate contact with the operator's desk, so that the operator can take action, if required.

Guideline 9

Cybercars, high-tech busses and advanced city vehicles require standard outside vehicle lighting, as they can share the road with other traffic. PRT-systems do require outside lighting only at PRT-stops as they drive on dedicated tracks. In public vehicles, the inside lighting should be on when the daylight situation requires it. In private vehicles the inside lighting should be off, with a possibility for the passenger to switch it on, as required.

Guideline 10

An information system to provide information on status, emergency procedures and instructions, should be installed in every vehicle. The HMI should be easy to understand, even for non-skilled users and foreigners.

Guideline 11

There should be camera systems inside the vehicle to check that empty vehicles that are requested to go to a certain station are really empty. For instance by means of cameras with AID (automatic incident detection) and alarm systems. The camera should only be switched on if there is no person present in the vehicle. If there are unidentified objects in the vehicle,

the control system should redirect the vehicles to a safe place, or prevent them vehicles from driving at all.

Guideline 12

It is important to ensure that the data systems are protected against hacking.

Guideline 13

Damage to the equipment due to vandalism can be avoided partly by choosing a vandalism-proof design. For instance: objects that are not fastened properly can be easily broken off or damaged and weak materials could be too easy to destroy. Also it is recommended to use materials with surfaces which can easily be washed or cleaned.

Guideline 14

In order to avoid damage to the equipment because passengers are unaware of how the system works, it is important to keep all instruments and information as simple and self-explanatory as possible.

Guideline 15

Since only authorized personnel are allowed to use the system for freight purposes, privacy is a less important matter. The identity of the handlers of the system is known. Cameras inside the vehicles can be switched on at all times. Only authorized personnel should be allowed to open vehicles.

Guideline 16

If vehicles are used for dual mode purposes, the vehicles should be checked for unidentified objects before entering or re-entering passenger mode.

Guideline 17

Dangerous goods as well as goods of high value (for instance money) should not be allowed in automated transport systems in order to minimize the danger of terrorism and theft and on the other hand increase the safety of the transport system. Therefore the transport of freight should be in accordance with the multilateral agreement of the United Nations (see ADR 2007 Accord Européen sur le transport des marchandises dangéreuses par route, part 3).

Strategies to address legal barriers

Much depends on the degree of automation. At a low degree it will under certain circumstances prove possible to resort to the driver for safety and responsibility. The higher the degree of automation, however, the more complex the legal issues grow as they presently and generally will be found to recur to the driver's responsibilities. In case of a high degree of automation this conflict will have to be solved legally, in case automation in areas with unrestricted public access is intended. Further research will be necessary on this aspect in future to achieve large-scale permissibility (i.e. to provide for legal certainty of implementation).

Strategies to address political barriers:

It is difficult to give general guidelines on how to address political barriers, since they can be of very different natures. However, there are two important instruments for the removal of political barriers that can be used almost everywhere: information and publication. Politicians will be more confident in making decisions if they have reliable and extensive information about the advantages an automated transport system could have in their particular situation. Extensive publicity campaigns have proven to be able to change the hearts and minds of people. The same instruments can be used to inform political bodies about the necessities to change the laws that are now in the way of the introduction of automated systems (see also 5.1). Many of the political barriers are of a local nature, but in case certification or national laws are in play, careful consideration should be given to the political level on which decisions could be influenced. It seems logical to address certification issues and legal issues on a national or even European level, while economic issues often are better addressed locally.

Strategies to address organisational barriers

An information and knowledge plan has to be made to reach the different stakeholders. Commercials, local television etc. can be used for this. Support groups can be established, which could do the lobbying and place pressure on the decision makers. Furthermore, more demonstrators are needed to convince people that automated system really work. It is also important to include these issues in teaching-programs at universities, because that is where the future stakeholders are. The City Application Manual, developed in CityMobil can be used as a basis for a teaching program.

Since the introduction of automated systems in existing environments always will cause problems, it could be advantageous to focus on applications in new cities or suburbs first. In a new city, it is relatively easy to take into account the requirements of a new advanced transport system and since sustainability is an important argument in present-day discussions this can help to convince city planners to consider the advantages of automated transport.

Within the framework of the CityMobil project new certification procedures for automated transport systems have been developed. The next step is to introduce these procedures on a European level and discuss the wider introduction of the procedures with the relevant authorities.

Strategies to address financial barriers:

Public-Private Partnerships might be a potential way to address financial barriers. A Public-Private Partnership is essentially a relationship between actors, which may be used in situations where the respective authorities lack the resources (e.g. financial, organisational, knowledge, skills) to overcome delaying and or hindering implementation. Cities in EU member states such as the UK where there is now a strong emphasis on Public-Private Partnerships may be more comfortable with such an approach than cities with a tradition of public sector ownership.

Another potential solution is to focus on cities that have a lot of money available. These could be new cities that are carrying out a major city development plan or cities where a major event takes place (for instance host cities of world championships, Olympic games, etc.) If such cities implement automatic transport solutions, it would also represent valuable PR for this kind of systems.

Strategies to address social barriers:

The most important instrument to address social scepticism is information. People (authorities and the public) should be informed about a possible new system in a very early stage, using the knowledge and information plan as described above under organisational barriers. The CityMobil City Application Manual can also play an important role in taking away the scepticism with the authorities.

References

[1] CityMobil Deliverable 2.5.2: Certification procedures for advanced transport systems. CityMobil WP 2.5 partners, January 2010

[2] CityMobil Deliverable 2.5.1: Intermediate report on legal and administrative issues. CityMobil WP 2.5 partners, November 2007

[3] CyberMove project: Deliverable 3.2: Safe sites and systems: J.P. van Dijke and M.M. Janse. October 2004.

[4] Code of Practice for the design and evaluation of ADA systems. RESPONSE III project. October 2006

[5] eSecurity WG Report: Towards Recommendations; Internal Working Document, Version: v0.8. Authors: eSecurity WG, 20 May 2008 (www.esafetysupport.org)

[6] EU-project: Urbaneye, Final Report: CCTV in Europe

[7] A.D. May, M. Crass, Sustainability in Transport: Implication for policy makers, July 2006

[8] CityMobil Deliverable 2.2.4: City Application Manual. CityMobil WP 2.2 partners, April 2011.