# Certification of automated transport systems

Jan van Dijke, Margriet van Schijndel, Fawzi Nashashibi, Arnaud de La Fortelle

Transport Research Arena– Europe 2012

# Certification of automated transport systems

Jan van Dijke[a], Margriet van Schijndel[a,*] Fawzi Nashashibi[b], Arnaud de la Fortelle[b*]

[a]*TNO Integrated Vehicle Safety, Steenovenweg 1, Helmond, 5708 HN, the Netherlands*
[b]*INRIA, Domaine de Voluceau, Le Chesnay, F-78153, France*

**Abstract**

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 paper describes a certification procedure for automated transport systems, developed in various European research projects and completed in the CityMobil project. The paper also describes the first experiences with the procedure. Furthermore the paper describes experiences with certification processes of automated systems in various countries where systems have been introduced.



Automated guided vehicles; certification; safety; public transport

## 1. Introduction

The city of tomorrow is in need of integrated traffic solutions that provide the required mobility in an efficient, safe and economic manner. It is inevitable that automation, in all possible forms between providing information at one end of the spectrum and fully autonomous driving at the other, will play a major role. In the future fully automated transport systems will become a part of everyday life. However, before these systems can be introduced on any scale, a number of barriers need to be removed. One of these barriers is the absence of a dedicated certification system, to prove to stakeholders that the systems indeed are safe. For many different technical systems procedures and standards exist, that deal with the analysis of the safety and with the certification of these systems, but for automated transport systems such standards did not yet exist. This paper describes a certification procedure, developed in various European research projects and completed in the CityMobil project [1]. The paper also describes the first experiences with the procedure in two systems: The Masdar Personal Rapid Transport (PRT) system in Abu Dhabi and the CityMobil Rome demonstrator in Italy.
Furthermore the paper describes experiences with certification processes for automated systems in various countries where systems have been introduced. Transportation is a global matter and standards will certainly play a central role in certification. But which standards? There are several other paths that are currently independently explored in the world, from TÜV in Germany to Google in Nevada (USA). Taking these developments into account, the paper drafts a blueprint for the future steps in the standardization of certification of automated transport systems.

* Corresponding author. Tel.: +31 888665755 *E-mail address*: Margriet.vanschijndel@tno.nl

The CityMobil project was built on the results of recent European and national projects [2, 3] and has validated and demonstrated the capabilities of new mobility solutions in different European cities. In 5 horizontal sub-projects the issues that still prevent full scale implementation of innovative automated transport systems have been identified and investigated and solutions have been developed. At two sites large scale demonstrators were set up to supply proof of concept of innovative transport systems integrated in the urban environment. In a number of cities smaller demonstration activities have been organised to show to the public, authorities and operators what automated transport can look like. CityMobil started in May 2006 and was finished in December 2011. The project was carried out by a group of 29 partners from very different backgrounds like industry, R&D, universities, cities and operators of public transport and from 10 different countries. The consortium was led by TNO, the Netherlands Organisation for Applied Scientific Research. The total budget was roughly 40 million Euros, of which 11 million was funded by the EU.

## 2. The CityMobil certification procedures

### *2.1 The safety analysis process*

The draft certification procedures consist of four steps. If these steps have been followed with a positive result, the system is considered safe enough to be introduced. The four steps are:
:

a. Preliminary risk reduction
b. Determine which safety regulations apply
c. Production and implementation of the system
d. Certification

a. Preliminary risk reduction

In the first step the risk reduction method [4] is used to roughly analyse a number of variables 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.

b. 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.

c. Production and implementation of the system

In the third step, for which the manufacturer of the system in combination with the operator is responsible, 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 Advanced Driver Assistance (ADA) systems, as developed in the Response projects [5]. Although the recommendations in this 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.

d. Certification

In the final step the system is certified, using the certification procedures described in section 2.6. 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.

*2.2 Requirements*

Certification procedures need to meet a number of requirements in order to be truly considered certification procedures. Furthermore there are considerations, limitations and choices to be made, depending on the particular circumstances of the system that needs to be certified. The paragraphs below describe those requirements, choices and limitations.

- Certification procedures should be based on the system safety approach and the safety life cycle.
  Life cycle safety is one of the major topics in system safety analysis. The concept of life cycle safety is that safety is an issue during the whole design cycle of the product and that safety not only concerns the period the product is being used, but the complete period from the first concept until the end of the life of the system. The big advantage of the life cycle approach is that safety issues are raised and solved in an early stage of system development and in this way can avoid more radical and expensive changes further down the development path.
- Certification procedures should contain performance criteria instead of design criteria.
  In order to guarantee that innovations offer the maximum benefits, limitations to design choices by means of design criteria should be avoided. Performance criteria guarantee that a system meets the required performance without preventing the designer from making the most economic choices.
- Certification procedures should include a rating system so that a quantitative assessment is possible.
  Almost all present standards and regulations include quantitative requirements that components or complete systems must meet in order to be approved. When, like in the case of automated transport systems, the system to be assessed is a complicated integrated system with large software content, simple component testing of for instance a steering or braking system is not sufficient anymore. Since the braking and steering systems are part of a much larger integrated system everything influences everything and simple input-output testing does not give the required answers. Here system safety acceptance levels must be defined and an analysis method with which it is possible to establish whether or not a system meets the defined level must be used. In order to define system safety acceptance levels the question: "how safe is safe enough" should be answered.
- Certification procedures should define acceptance levels for different kinds of vehicles.
  The present motor vehicle regulations specify several categories of vehicles for which different requirements are defined. Parameters like mass and maximum speed of motor vehicles have a strong influence on safety. The safety requirements of, for instance cybercars should reflect the fact that they, because of their limited weight and speed are relatively safe in comparison with traditional cars.
- Certification procedures should use relevant existing standards and follow developments in standards for related vehicle types carefully.

Some automated transport systems will use the same road infrastructure as traditional cars and it would be preferable when all systems that are being used on public roads meet the same requirements. Therefore it is not only important to refer to existing standards, but also to carefully follow developments in relevant standards. In addition, a number of practical requirements can be defined that ensure that the analysis method is fit for use. The method has to fulfil the needs of several parties who are involved in the decisions concerning the safety of automated transport systems.

- User friendliness: The method must be easy to use, so that people from different backgrounds can use it with a minimum of training.

- Uniformity: The method must be suitable for analysis of almost every vehicle system, vehicle or vehicle component without the need for special adaptations.
- Reproducibility: The results should be the same, independent of the people that carry out the analysis.
- Acceptability: In order for a method to be acceptable, it should have a firm basis in existing standards.

*2.3 Relevant standards*

Although there are no standards immediately available for the system analysis of an automatic guided vehicle system, starting points can be found in existing standards. The most important one is IEC 61508: Functional Safety of electrical/electronic/ programmable electronic safety-related systems [6]. IEC 61508 is a generic standard in which amongst others Safety Integrity Levels are defined. A system meets the requirements of IEC 61508 if its Safety Integrity Level is in accordance with the level prescribed for that particular system. Another important standard that was used as a reference is the new ISO 26262: Functional safety. This ISO standard is an adaptation of IEC61508, particularly for use with Advanced Driver Assistance systems (ADAS) in road vehicles. Although ISO 26262 is meant for vehicles with drivers, it was of great benefit to the development of the present standard for driverless systems and care has been taken to make use of similarities between the standards where possible.

As the basis for the system safety analysis method the Failure Modes, Effects and Criticality Analysis (FMECA) was chosen. Literature describes many methods for system safety analysis. The System Safety Analysis Handbook [7] for instance, describes over a hundred methods. The FMECA has the advantage that it is extensively used in the vehicle industry and that most developers have either heard of it or have contributed to one. The FMECA is not the only analysis method that would be suitable. It was considered to add other methods to the method, for instance a Fault Tree Analysis. That would increase the accuracy of the result but it would have an adverse effect on the user-friendliness of the method and especially on the time consumed with an analysis. An important consideration to limit the method to the FMECA was that all traditional certification tests are in fact compromises. A product has to meet certain requirements when it is tested under well-defined standard conditions. When the conditions are slightly different, like in a real situation the product will not perform the same way and might not even meet the certification requirements. Since the method is a certification instrument and since the requirement of user friendliness is considered important it was decided not to include other methods. The FMECA is per definition a subjective analysis method. In a typical FMECA 4 - 5 people use their knowledge and experience to systematically list all possible failure modes of the system to be analysed. Then the causes and effects of these failure modes are established and severity and likelihood of the effects are rated. The reproducibility of the result depends on the knowledge of the participants but also strongly on the strictness with which the procedure is being followed. In order to guarantee an acceptable reproducibility, so that different groups of analysts reach the same conclusions, the analysis process is defined in detail and the process moderator has to monitor the process strictly in order to guarantee the procedure is being followed.

*2.4 References: "how safe is safe enough"*

Whether or not a transport system or any other system is safe enough depends on the risk that is accepted in a given context based on the current social criteria. For traditional road vehicles "safe enough" is made concrete by establishing limits that vehicles should meet under well described and realistic test conditions. For intelligent transport systems like cybercars this is not possible, since the number of variables that influences the results of a test is so high that testing would cost too much time and money. This means that "safe enough" for automated transport systems should be defined differently. The choice

made in this procedure is to base "safe enough" on the safety of comparable systems. For innovative systems, like automated transport systems it is possible to state that they should be safer than comparable traditional vehicles in the same class. Safety or the lack of safety can be expressed in various units. In statistics the number of casualties per traveller-kilometre is often used. Safety is thus expressed on the basis of the seriousness of an accident and the distance travelled. In this proposal we express safety as the number of casualties per travelled hour. Safety is expressed in terms of the seriousness of an accident and the time a person spends travelling. The risks connected with one hour walking or one hour flying an airplane is perceived as a more realistic means of comparison than the risks of travelling a certain distance.

When, for instance, we know that in Europe there are 6 casualties per billion travelled kilometres in passenger cars (Eurostat 1997) and when we assume that the average speed driven by passenger cars is 60 kph we can calculate that there will be $36 \times 10^{-8}$ casualties per hour travelled. Or expressed differently: the chance to die each hour as a result of an accident with a passenger car is 1 on 2.8 million.
Another consideration is the contrast between "as safe as possible" and "as safe as necessary" The last expression encompasses an accepted level of risks. The idea of this approach is that it is not possible to ban all the risks from the lives of people but the harm that a system can cause should be limited to a level that is generally deemed acceptable. This approach is also used in IEC 61508.

### *2.5 Limitations*

*Human Factors*
The guidelines, as presented in this report are not only meant for the analysis of technical systems. Human factors can play a role in the analysis. This is understandable if we realize that automated transport systems are not controlled by human drivers, but that humans nevertheless play a role, by being passengers or by controlling central systems, carrying out maintenance, repairs etc.

*Software*
Software is a difficult subject in any safety analysis. How can a judgement be made as to whether or not software is safe? Certainly in complicated control software like that in automated transport systems the number of possibilities for failure is very large. It is generally acknowledged that it is risky to make firm statements based on tests about the safety of complicated software. The more extensive and complex the software is the more tests are necessary to exclude all possible failure modes. A more realistic approach therefore is to follow generally accepted design rules during the design phase. By strictly following such design rules (for instance the IEEE Software Engineering Standards [8]) the risk of failure will be minimised. These standards give recipes for developing the software and also for documentation. When the design rules are followed and the software meets its functional specifications the chance of failure can be deemed to be small.

*Present laws*
In order to be approved for use on public roads, present laws require the presence of a driver in a motor vehicle. Since automated transport systems do not have a human driver, they cannot be approved under the present laws. This can be interpreted in two ways: 1: automated transport systems are not allowed to use public roads and 2: automated transport systems are not motor vehicles as defined by the law and as such do not have to meet this law. The 2$^{nd}$ interpretation would offer a window for the introduction of automated transport systems on public roads, but at present only the first interpretation is accepted.

### *2.6. The certification method*

A complete certification program for an automated transport system will consist of a combination of functional tests and evaluations and a series of FMECA analyses as described here. The functional tests

should prove that the system does what it is supposed to do according to its specifications. The FMECA analyses should prove that the risks involved in system failures are within the range of acceptance.

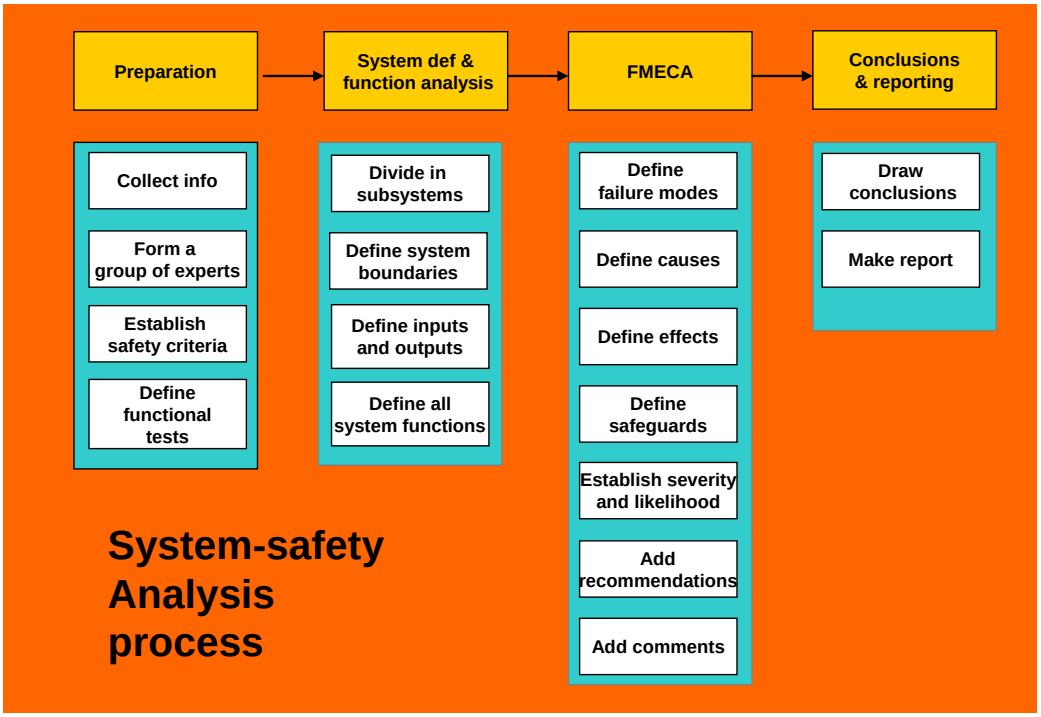


Fig. 1. The certification process

Such a certification process can be carried out when the development phase is concluded and the system is ready for introduction or it can start when the first concept is available and end with the final functional tests and analyses. The advantage of the last option is that it is very unlikely that in the last tests and analyses serious failures will be discovered. Such serious failures would have been detected in earlier phases and the design would have been adapted accordingly. If, however, a certification process starts when the design phase has been completed and the system is ready for introduction possible faults that are discovered could lead to expensive redesign and loss of time. It is therefore highly recommended to observe the safety life cycle and start the safety analysis process in the earliest design phases. On the basis of the considerations, choices and limitations described above, a basic structure for the certification process was designed. The structure consists of a number of process steps, each in its turn divided in sub-steps. Figure 1 shows a graphic overview of the structure. For reasons of reproducibility, it is essential to carry out all of the above steps in the order given.

## 3. Evaluation of the procedure

The certification method was evaluated by applying it to the CityMobil Rome demonstrator and the Masdar PRT system in Abu Dhabi.

*The CityMobil Rome demonstrator*

The certification procedure was evaluated by using it to analyse the safety of the people mover for the new Rome Exhibition centre. This exhibition centre is a huge new development which is located between the City of Rome and Fiumicino airport. It was built between 2005 and 2008 and part of the complex is a very large parking area. The distance between the far parking places of this parking area and the entrances of the exhibition complex is up to 500 meters and it was decided to implement a driverless system to bring people from the parking to the entrances. In order for the Italian Ministry of Transport to certify the transport system for use a safety analysis was carried out on the complete system, including sub-systems like the communication system, the remote maintenance system and the infrastructure. The analysis was carried out between April 2009 and July 2009. The Italian Ministry of Transport accepted the results of the analysis as the main basis for its decision to certify the system.

*The Masdar PRT system*
Masdar City is a new sustainable city built from scratch in Abu Dhabi. The Masdar PRT system was designed to be the main transport system for the city. The system consists of small fully automated cybercars that find their way in a separate transport infrastructure at the lower city level. After the analysis was completed, the Ministry of transport in Abu Dhabi required an additional analysis before the system was accepted.

In both cases a time consuming process of negotiations was necessary. These experiences show the importance of generally accepted procedures, which, by omitting the need for these discussions and extra requirements can speed up implementations significantly.

In general the attendants were satisfied with the procedure and the way it was carried out. There are, however, a number of points of attention. The most important ones follow below:

- The preparation process and the system definition take roughly half of the time needed for the complete analysis. Dividing the system in sub-systems and painstakingly defining all system functions is a tough and tiring job, but if it is done thoroughly it will prove to be advantageous in the further FMECA analysis.
- During the analysis of the Rome people mover three persons attended all of the sessions. Some sessions were attended by specialists in case a certain subject was treated that required additional knowledge, but more often a session had to be interrupted because the opinion of some expert was required. For reasons of efficiency it is recommended to have experts in the session when a certain subject is being treated.
- Developers that are involved in an FMECA analysis appear to have a strong tendency to start generating solutions when a safety flaw or something else that can be improved upon is discovered. It is the task of the moderator to keep the focus on the analysis of the present system. Development can be done in a later stage.

## 4. Experiences with other certification procedures

*The CityMobil Cybus service at La Rochelle*
The city of La Rochelle is known to be among the cities with the most deployed electro mobile systems in France. There is a bus system, an electric vehicles car sharing system and an electric boat shuttle system. The Cybus system is composed of 2 electric shuttles that have been deployed during 3 months (May to July 2011) in a city neighborhood located between the university campus and touristic area with its electric boat harbor. Deploying the on-demand Cybus system in this 1.2 km long area had the advantage of completing the transport chain and the challenge of operating the system in a mixed urban area where the driverless Cybus shuttles had to cope with vehicles and pedestrians (residents and tourists) and with some access barriers as well. There were five stations equipped with touch screens to allow the users to call a Cybus while the destination could be chosen or confirmed inside the Cybus. The system was

developed and operated by project partner INRIA within the CityMobil project and revealed many challenges of different nature beside the technical of which certification was one.
Since the maximum speed of a Cybus (25 kph) is less than the 30 kph that qualifies it as a vehicle from a juridical point of view, the Cybus system had to get a special authorization from the Mayor and the Municipality to operate. In fact, the certification process consisted of a safety evaluation to identify and take away possible safety risks and this authorization from the mayor. Nevertheless, because French regulations do not allow fully unmanned vehicles, it was necessary to keep a person inside each Cybus!
The tricky problem of insurance (the driver, the Cybus and others) has been solved thanks to an insurance company that accepted the challenge and even contributed in partially sponsoring the operation

The deployment of a wireless communication network has shown the necessity of having a certified and secure communication system operating in a crowded and "polluted" urban area with visibility issues and canyoning.The ground experiences revealed the necessity of having a remote Vehicle Monitoring System to solve conflict situations e.g. temporary road blockage, highly crowded situations, hazing, etc.
The operator in each vehicle, besides holding the traditional finger pointed on the emergency button, had to explain the system to the users and conduct surveys and collect statistics. This way more than 1000 passengers were surveyed with different ages, at different locations and different times of day. The feedback after 3 months of service revealed a great acceptability of the system (94%) with 73% of people feeling secure. Furthermore, 94% of the people were accepting the deployment of such a system in their city and think the system can be generalized [9][10].

*The CityVIP project*
This 3-years project has been sponsored by the French National Research Agency (ANR) and the PREDIT. The project objectives are the development of CityVIP methodological and technological advances in the management of urban transport mode driver assistance but also automatic driving mode. The project is organized around two main axes: the development of basic functions whose availability is a prerequisite to any deployment of new services; the second axis is devoted to experiments that will validate these functions under realistic conditions foreshadowing the actual operating conditions. The project ended in October 2011 with demonstrations using two kinds of platforms: Cycab-like small electric vehicles from Robosoft used by the parties INRIA, IRISA and LASMEA; and car-like vehicles used by the parties UTC, LCPCP and XLIM/DMI/CANSO. Although dedicated to demonstrations in cities, the systems have not been tested in the city centers and did not tackle specifically the certification or the standardization issues. Certification was recognized as an important issue, however, and INRIA and LASMEA are currently submitting a joint project dedicated to the certification of mobile autonomous vehicles in cities and urban environments.

Thanks to this experience the French company LIGIER and the LASMEA laboratory situated in Clermont-Ferrand have designed the VIPA (a French acronym that stands for Autonomous Individual Passenger Vehicle), a self-driving electric small vehicle that is being designed for use any place where people need a on-demand vehicle with a top speed of 20 kph (average speed it more like 10). Similar to the Cybus developed by INRIA the VIPA is an autonomous vehicle guided by its own sensors and reasoning capabilities.

## 5. Future steps

The certification procedure as described in Fig. 1 is a very general sketch that is recognized in the community. It has also shown its potential through two real examples of certification procedures leading to authorizations by transportation authorities. Therefore, CityMobil has shown fully automated

transportation systems indeed can be certified. This is a milestone for the development of this industry because everybody sees there is a maturing market and not only technical prowess. In order for the procedure itself to mature and gain acceptance, more examples of systems analysed with the procedure are needed

We identified at least two main challenges for future progress in certification:

- Diversity of assistance systems;
- Standardization of components.

The first point addresses the needs an automated system answers to, whatever the level of automation – partly, highly or fully automated. Automation is not a goal per se but is a means for problems such as assistance for difficult driving tasks, like automated steering for docking buses, or extended functionalities like automated valet parking. Even though first systems will go through a customized certification process (as in Rome or Masdar), a sustainable automation industry will need to offer faster and re-usable procedures. This means to go towards categorization of automated systems at the application level.
Moreover, industrialization requires a better definition of the type of systems considered, its sub-systems and interfaces between components. The experience of CityMobil shows that the definition of the level of acceptable risks is a difficult point: a single transportation authority cannot define it alone. It is finally a societal hence political issue. Since it is the basic starting point for declining the global risk into risks of subsystems, it is very important to precise the categorization of automated transportation systems (e.g. depending in the level of automation) and their decomposition (e.g. in perception-planning-control).

The second point – standardization of components – is a technical answer to the complexity raised by the needs, i.e. the first point. There are many techniques to answer technical problems (e.g. perception), some of them very mature, but the variety of systems you can create with such blocks is huge. One typical example is the Internet where the diversity is almost infinite but protocols are rather simple (TCP/IP, HTTP…). This shows the power of an appropriate set of standards; an evolving set of course, but compliant with a general architecture (for Internet Protocols the base view are the famous ISO layers). This approach has been pushed by Europe and is currently adopted globally for ITS systems. However the global architecture is not finalized even though parts of it are in a pretty good state (e.g. ITS communication stack). Terminology, components and interfaces are defined in standardization organizations (ISO TC204, ETSI TC ITS…) with a clear will of all regions to have a consistent set of standards all around the world.
This question raises also the link between cybercars and the rest of the transportation community. A few years ago, cybercars were considered as scientific toys. We believed there would be a convergence between fully automated vehicles that would increasingly be allowed to drive more and more on open roads until they can be allowed on public roads and between “normal” vehicles that would support more and more the driver until full automation is reached. Life went faster than expected and we see mixture instead of convergence. Specific automated functionalities are integrated into traditional cars (e.g. automated parking) using “cybercars technology”. This means automation arrives through partial applications taking subsystems from fully automated vehicles architecture. This is a great news but also a challenge: the cybercar community will have to speak the same language (AUTOSAR for electronics, IEC or ISO for safety, etc.).

Finally, a last challenge due to mixture of automation and human driving is the interface. In the 2011 Frankfort Motor Show, VALEO demonstrated its automated parking system supervised through a smartphone! Mines ParisTech and INRIA demonstrated with VALEO a prototype of “iPad Steer” where the steering wheel is replaced by an iPad (final demonstration of French AROS project). Interfaces are a key component in an automated system supervised by human; and such systems are highly desirable in an aging society but push further all questions around certification. The questions raised are then: Who is driving? What is automated? What is automated driving?

**Acknowledgements**

CityMobil was funded by the European Union as an Integrated Project in the 6th Framework Program.

**References**

[1] CityMobil website: www.citymobil-project.eu.
[2] Netmobil: New Transport System Concepts for Enhanced and Sustainable Personal Urban Mobility. European 5th Framework Program 2002-2005. www.netmobil.org.
[3] LUTR: Land Use and Transportation Research: Policies for the City of Tomorrow. European 5th Framework Program 2002-2005. www.lutr.net.
[4] CyberMove project: Deliverable 3.2: Safe sites and systems: J.P. van Dijke and M.M. Janse. October 2004.
[5] Code of Practice for the design and evaluation of ADA systems. RESPONSE III project. October 2006
[6] IEC 61508: Functional Safety of electrical/electronic/programmable electronic safety-related systems; IEC 1998
[7] System Safety Analysis Handbook; System Safety Society.
[8] IEEE Software Engineering Standards; IEEE 1999
[8] IEEE Software Engineering Standards; IEEE 1999
[9] An On-Demand Personal Automated Transport System: The Citymobil Demonstration in La Rochelle, L. Bouraoui, C. Boussard, F., Charlot, C. Holguin, F. Nashashibi, M. Parent, P. Resende, Proceedings of the 2010 IEEE Intelligent Vehicles Symposium, 5 - 9 June, 2011, Baden-Baden, Germany.
10] Advanced Transport Systems Showcased in La Rochelle, A. Alessandrini, M. Parent, C. Holguin Proceedings of the 2011 IEEE Intelligent Transoortation Systems Conference, 5 - 7 October, 2011, Washington DC, USA.