SAFETY STANDARDS FOR CYBERCARS

Part 2: Recommendations for certification procedures

Deliverable Type: Report
Number: D 6.2
Nature: Final version
Contractual Date of Delivery: 01/05/2004
Actual Date of Delivery: 22/06/2004
TaskWP:WP 6

Name of responsible: J.P. van Dijke
e-mail: vandijke@wt.tno.nl
J.J. Uwland
e-mail: uwland@wt.tno.nl

Name of the institute: TNO Automotive
Address: P.O. Box 756
5700 AT Helmond
The Netherlands

Abstract:

At present generally accepted certification procedures for Cybernetic Transport Systems (cybercars) do not exist. This makes the introduction of such systems difficult, because neither manufacturers nor operators nor authorities have guidance as to what is acceptable from a safety point of view. This report aims to make a contribution towards solving that problem by developing recommendations for safety requirements and by proposing a method to analyse and certify cybercars with respect to safety. The proposed method has been evaluated on two operational cybercar systems.

Keyword List:
Safety standards; safety guidelines; Cybernetic Transport Systems; Certification; Automatic guided vehicles; cybercars.

EXECUTIVE SUMMARY

The work that is described in this report was carried out within the framework of the CyberCars project, a project supported by the IST program of the European Union. Cybercars are Cybernetic Cars for a new transportation system in cities.

This report contains the second deliverable in Work Package 6: "Recommendations for certification procedures". In deliverable 1: "Existing standards and guidelines" [1], a survey of existing standards and guidelines was carried out, in order to establish which present standards are relevant for cybercars and what is still missing.

In the present report, the requirements for certification procedures are set out and a method is proposed to establish acceptable safety levels and to analyse a cybercar system in order to find out whether or not it meets the requirements. The basic idea for this method was developed by TNO for the analysis of automatic guided vehicles and was first evaluated on drive-by-wire systems. Within the framework of the CyberCars project the development was continued and adapted to the specific cybercar requirements.

The result was evaluated by analysing the safety of two cybercar systems: The 2nd Generation Rivium People Mover and the Floriade CyberCab. The method proved to provide very useful information that can be used to improve products in the concept and design phases. The method has also shown a potential to develop into a certification instrument, but additional research and additional test cases are necessary to improve the process of establishing safety criteria and to prove the reproducibility of the method.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Background

The work that is described in this report was carried out within the framework of the CyberCars project, a project supported by the IST program of the European Union. Cybercars (Cybernetic Cars for a new transportation system in cities) aim to improve mobility in cities by means of introducing automated vehicles for moving people and goods. The main characteristics of these systems are the use of small electric automated vehicles running on the existing urban infrastructure. The vehicles can be used for public transport but also for individual door to door transport.

The CyberCars project focuses on improvement of existing technologies, but also pays attention to existing legal constraints that could hamper the diffusion of cybercar systems in cities. Work Package 6 of the CyberCars project therefore addresses the certification guidelines that are needed to certify that systems are safe.

This report contains the second deliverable in Work Package 6: "Recommendations for certification procedures". In deliverable 1: "Existing standards and guidelines" [1], a survey of existing standards and guidelines was carried out, in order to establish which present standards are relevant for cybercars and what is still missing. In deliverable 2, the requirements for certification procedures are set out and a method is proposed to establish acceptable safety levels and to analyse a cybercar system in order to find out whether or not it meets the requirements. The basic idea for this method was developed by TNO for the analysis of automatic guided vehicles and was first evaluated on drive-by-wire systems. Within the framework of the CyberCars project the development was continued and adapted to the specific cybercar requirements.

The result was evaluated by analysing the safety of two cybercar systems: The 2nd Generation Rivium People Mover [2] and the Floriade CyberCab. The reports on these evaluations are confidential but the conclusions with respect to the method are included in this report.

1.2 Motivation

Traditional vehicles that use the public roads have to meet a large number of requirements, laid down in standards and regulations. Most of these standards and regulations are related to safety but there are also standards on pollution, recycling of material and many other subjects. The sheer number of standards limit the car developers in their innovations. But the standards also give the developers guidance on how to create safe and reliable vehicles. When they develop new vehicles the manufacturers know the limits within which they have to stay in order to have their vehicle certified for use on public roads.

In contrast to the extensive set of certification standards for traditional vehicles, there are hardly any rules for vehicles that use private grounds or for vehicles that do not fit into the categories of the European Directive 70/156/EEC. This means on one hand that manufacturers have a large amount of freedom in designing their systems, which creates room for innovative solutions. On the other hand, however, manufacturers and operators run great liability risks in case something goes wrong with their systems. Operators and authorities will be reluctant to introduce innovative systems if there is no objective judgement possible on the safety of such systems. An objective judgement is only possible if

it can be proven that a system meets generally accepted standards. Thus, the absence of generally accepted standards puts up barriers for the introduction of innovative transport concepts like cybercars.

So on the one hand there is a need for standards and regulations that offer guidance to manufacturers for the design of their systems and give authorities and operators certainty about safety of the system. On the other hand rules and directives should leave room for innovative concepts and limit the manufacturers as little as possible in making design decisions.

Cybercar systems are in the beginning stages of development. This development would be seriously hindered by prescribing standards that contain design criteria and thus would restrict manufacturers in the choices they want to make. Standards that only require products to meet certain performance criteria, but leave the way in which these criteria are met to be decided by the manufacturer are preferable.

In order to meet these needs an analysis method was developed that allows qualitative and quantitative judgements on the safety of cybercars and other innovative transport systems. The method is not design-restrictive, so it does not limit developers in the design-choices they make, as long as the result is that the system is safe. In order to make quantitative judgements an answer to the question: "how safe is safe enough" must be given. One possible approach towards answering that question is provided in this report.

1.3 Existing standards, laws and regulations

Deliverable 6.1 of CyberCars [1] provides an overview of existing standards and of topics that are missing in these standards and that are relevant for cybercars. In this paragraph the findings are summarised.

- The overview in deliverable 6.1 shows that there is a consistent and extensive set of standards for vehicles that make use of public roads. There is also an extensive number of standards for rail vehicles, although these standards are mainly nationally orientated, instead of being accepted on a European scale. For non-rail systems and systems that do not use public roads there is the Machinery Directive. This Directive, however, is not designed for means of transport and explicitly excludes some means of transport. The draft new Machinery Directive indeed excludes all means of transport
- The inventory shows that the existing standards and laws do not form a uniform and all-encompassing system, not even for traditional vehicles. For instance, in The Netherlands there are no safety requirements for streetcars that operate within city limits, although these streetcars are vehicles that make use of public roads and share that road with other road users. For other rail vehicles the formal rules have a limited reach.
- The existing cybercars and those that are being developed, depending on the environment they are used in, are subject to the same laws and standards as traditional vehicles. In addition to the limitations mentioned in par. 1.4 these existing laws and standards have another limitation. The present laws imply the presence of a human driver in the vehicle. The absence of a driver causes legal problems: who is accountable in case of an accident.
- The three main functions that human drivers carry out are observing; analysing/deciding and transferring the decision to the vehicle systems. In a cybercar the sensors, the obstacle detection system, the vehicle controller and the different actuators take over these functions. For traditional

vehicles standards on component level exist. For these 'new' components such standards do not exist.
- A cybercar system often includes a command post, from which several functions are centrally controlled. Also for such command posts no specific standards exist.
- Control software can be seen as part of these systems. The specific character of software makes it necessary to establish specific requirements. Although there are many standards in the field of software engineering and software development, these are at present not part of the current legislation.
- The existing standards not only list the requirements a product must meet, but they also supply binding guidelines for the construction of a product. They do not only contain performance criteria, bust also design criteria. For instance, the Directive for seatbelts has requirements that must be met by the seatbelt retractor, thus implicitly requiring a seatbelt retractor to be part of the seatbelt. Better solutions can perhaps be thought of, but the Regulation does not allow them.

1.4 Recent developments in safety standards

Developments in safety standards for automobiles with respect to electronic and computer controlled devices mainly focus on system analysis as a design and evaluation tool. At present there are three important developments in Europe where certification of electronic devices in cars and Advanced Driving Assistance Systems (ADAS) are concerned.

- Within the framework of RESPONSE I, II and III, [3] European projects initiated by the European Automotive industry, a Code of Practice for the development and testing of ADA systems is being developed. This Code of Practice should give manufacturers guidance with respect to the development and test of their systems and should give some protection in liability cases. However, it is accepted that liability remains an issue and that no Code of Practice or formal regulation will protect manufacturers against all claims. The work that is done in the Response projects can be of great value for cybercars. Although the scope of the Response projects is limited to ADA systems there are so many common factors with cybercars that the Code of Practice, maybe with some adjustments will be useful for cybercar systems also. Alternatively, the systems-approach that has been chosen for cybercars could be one of the building blocks for the Code of Practice.
- There is also a link with the FP6 project SPARC (Secure Propulsion using Advanced Redundant Control). In SPARC software and hardware interfaces of safety decision control systems are being developed. One of the main aims is to evaluate and describe harmonised homologation paths of complete vehicle safety relevant systems.
- Proposals are being under discussion concerning ECE Regulations 79 (Steering Systems) [4] and ECE 13 (Braking) [5] to allow steer-by-wire and brake-by-wire. The proposal is to add an annex to these regulations with special provisions. These special provisions mainly concern the presentation of a safety concept, correct documentation and a system safety analysis to identify possible failures of the system. The general idea is that such an annex in future should be added to all regulations where products with a significant software content are concerned.
- The German Automobile Manufacturers, within the framework of FAKRA are working on an adaptation of IEC 61508 (Functional Safety of electrical/electronic/programmable electronic safety-related systems) [6] to make it suitable for certification of ADA systems and other electronic systems.

These developments do not directly concern cybercars, but it is nevertheless of great importance to take notice of these developments and to incorporate them in certification guidelines for cybercars

where possible. Therefore it is important to monitor all developments of standards and regulations for road and rail vehicles and strive for harmonisation of developments in these different but related areas. Care has been taken to ensure that the solutions presented in this report stay as close as possible to the developments described in this paragraph.

2. RECOMMENDATIONS FOR STANDARDS

2.1 Requirements

Based on the results of the survey presented in deliverable 6.1 [1], the present developments in the field of regulations for traditional road vehicles and the issues identified in Chapter 1 of this report, a number of requirements for certification standards for cybercars can be defined.

Certification standards for cybercars 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 avoid more radical and expensive changes further down the development path. Another advantage is that decisions on the necessity of redundancy of systems can be taken on the basis of a well-structured and documented approach. By using the life cycle safety approach, developers can be more confident that the system will pass the tests before the system is up for its final certification test.
- 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.
- Include a ranking systems 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 cybercars, the system to be assessed is a complicated integrated system with a 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. In order to define system safety acceptance levels the question: "how safe is safe enough" should be answered.
- 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 for cybercars should reflect the fact that they, because of their limited weight and speed are relatively safe in comparison with cars.
- Use relevant existing standards and follow developments in standards for road vehicles carefully.
  cybercars 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 cybernetic transport systems.

- User friendliness: The tool must be easy to use, so that people from different backgrounds can use it with a minimum of training.
- Uniformity: The tool 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 tool to be acceptable, it should have a firm basis in existing standards.

2.2 Considerations and choices

Although there are no standards immediately available for a system analysis of an automatic guided vehicle system like cybercars, nevertheless 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. IEC 61508 is a very comprehensive set of documents. The Safety Integrity Levels are not specifically adapted for use with cybercars and the standard does not specify which analysis methods should be used. Therefore IEC 61508 does not meet the above requirements of user friendliness and reproducibility. The standard does, however, provide important guidance and it was used as a reference for further work.

Since there was no direct reference for a certification standard for cybercars, it was decided to develop one. The basic idea was to develop a simple and user friendly method for the safety analysis of cybercar systems that can be used during the complete design process of the system. The method can be applied to assess the first concept for a new system. After that the same method should be suited for the different phases of the design process and finally for the certification test of the completed system.

As the basis for the analysis method the Failure Modes, Effects and Criticality Analysis (FMECA) was chosen. Literature describes many methods for system safety analysis. For instance the System Safety Analysis Handbook [10] describes over a hundred methods. The FMECA, however, 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 almost always in a real situation the product will not perform the same and might well not meet the certification requirements. Since the method is a certification instrument and since the requirement of user friendliness is considered important it was decided to accept not to include other methods.

The FMECA is per definition a subjective analysis method. In a typical FMECA a group of 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 the severity and likelihood of the effects are rated. Whether or not the result is reproducible 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 described in detail and the process manager has to monitor the process strictly in order to guarantee that the procedure is being followed.

Essential in this respect is the system definition that precedes the actual FMECA. A complex system like a cybercar is divided in a number of systems that are analysed separately. It is essential that it is clear to all participants what the boundaries of a system are. When the systems to be analysed are clearly defined a function analysis should provide all possible functions that the system performs. These functions are the basis of the FMECA, where a failure is defined as a failure to perform a certain system function. In order to define the system functions the PASSPORT method [7] is used. This method will be described in more detail in chapter 3.

2.3 Limitations

2.3.1 Human Factors

The guidelines, as presented in this report are only meant for the analysis of technical systems. This means that human factors are not part of the equation. This is not so much a problem if we consider that cybercars are not controlled by human drivers, but nevertheless humans play a role in controlling central systems, maintenance, repairs etc. In the analysis of the Floriade People Mover an attempt has been made to also analyse the behaviour of the human system controllers, but more research and the contribution of human factors experts is needed in order to establish the limits of use of the method.

2.3.2 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 cybercars 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 about the safety of software is therefore 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. In assessing the safety of software controlled systems it is more and more common to look at the way in which the software is designed. In the world of aviation this is already common practice. The FAA uses DO-178B: "Software Considerations in Airborne Systems and Equipment Certification" [9], a standard that describes how software for use in aircraft should be developed, documented and tested. Here again is a reference to the safety lifecycle. In order to assess whether or not a product is safe, the development history is being assessed and not just the completed product.

2.3.3 Present laws

As already explained, in order to be approved for use on public roads, present laws require the presence of a driver in a motor vehicle. Since cybercars do not have a human driver, they cannot be approved under the present laws. This can be interpreted in two ways: 1: cybercars are not allowed to use public roads and 2: cybercars are not motor vehicles as defined by the law and as such do not have to meet this law. The 2nd interpretation would offer a window for the introduction of cybercars on public roads.

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 result is so high that testing would cost too much time and money. This means that "safe enough" for cybercars should be defined differently.

The choice made here is to base "safe enough" on the safety of comparable systems. For innovative systems, like cybercars it is for instance 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 aeroplane are percepted 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 (Eurostat 1977) and when we assume that the average speed driven by passenger cars is 60 km/hour we can calculate that there will be 36×10^{-8} casualties per hour travelled. Or expressed differently: the chance to die 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 when a system is used the harm that the system can cause should be limited to a level that is generally deemed acceptable. This approach is also used in IEC 61508.

3. PROPOSED CERTIFICATION METHOD

3.1 General

A complete certification program for a cybercar system will consist of a combination of functional tests and evaluations and a series of FMECA analyses. 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. 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 redesigns and loss of time. It is therefore highly recommended to observe the safety life cycle and start the certification process in the earliest design phases.

The certification process should result in a certificate that shows that the system meets the requirements. Since cybercars systems can differ from each other strongly and since a system may or may not include infrastructure and communication devices there is no standard set of requirements and thus there cannot be a standard certificate. The proposal therefore is to include a table stating what the requirements are, what the results of the tests and analyses are and a conclusion as to whether or not the system did meet the stated requirements. Annex 1 gives an example of such a cybercars certificate.

3.2 Overview

On the basis of the considerations, choices and limitations laid down in Chapter 2, 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.

1. Preparation of the safety evaluation
   - Collect information about the system
   - Form a group of experts
   - Agree on goals, safety criteria, planning and process
   - Set up a program for functional tests
2. System definition and function analysis
   - Define system boundaries
   - Divide into subsystems
   - Make Passport diagrams
   - Define all functions
3. FMECA
   - Establish failure modes
   - Establish causes
   - Establish effects
   - Identify possible safeguards
   - Establish severity and likelihood

- Add recommendations
- Add comments

4. Conclusions and reporting
   - Draw conclusions
   - Lay results down in a report

3.3 Preparation

The preparation phase is mainly meant to collect all information that is needed to carry out the analysis and to prepare all necessary requirements, so that the following steps in the process can be carried out without delays.

3.3.1 Collect information about the system

The purpose of collecting and documenting all information about the system is twofold. Firstly, it is important to establish the status of the system at the moment of the analysis. If the system to be analysed is a system in development and the status is not clear, design changes that are implemented during the analysis can cause confusion. Secondly, the collected and documented information is a reference for later, in case questions arise about the results of the analysis. All documentation is listed and provided with a unique number.

As a minimum, the following information is needed:

- The information about the use of the system and the circumstances in which the systems operate like climate, other users of the environment, etc. This information is in most cases already available in a system specification.
- Information about the system itself and the components of the system.
  - Functional specification
  - Specification of standards with which components possibly must comply.
  - Test results
  - Certificates of manufactures of sub-components
  - Track record of components with information about failures
  - Construction plans
  - Process descriptions

3.3.2 Form a group of experts

The next steps in the process, the system definition, the function analysis and the FMECA are carried out by a group of experts. In an FMECA the group is typically 4 - 5 people. The composition of this group is important and depends strongly on the system to be analysed. The composition of a group that analyses a cybercar vehicle should be such that expertise from the design side (mechanically; electronically and software), from the operator side and, if safety-critical sub-systems supplied by external suppliers are involved, from this supplier should be represented. An open communication on the safety issues is important, so in case external parties are present it is essential to agree on confidentiality and intellectual property issues. Not all detail knowledge has to be represented in the group. The members can consult other experts if detail knowledge is needed, but the group members should have a thorough overall knowledge of the system.

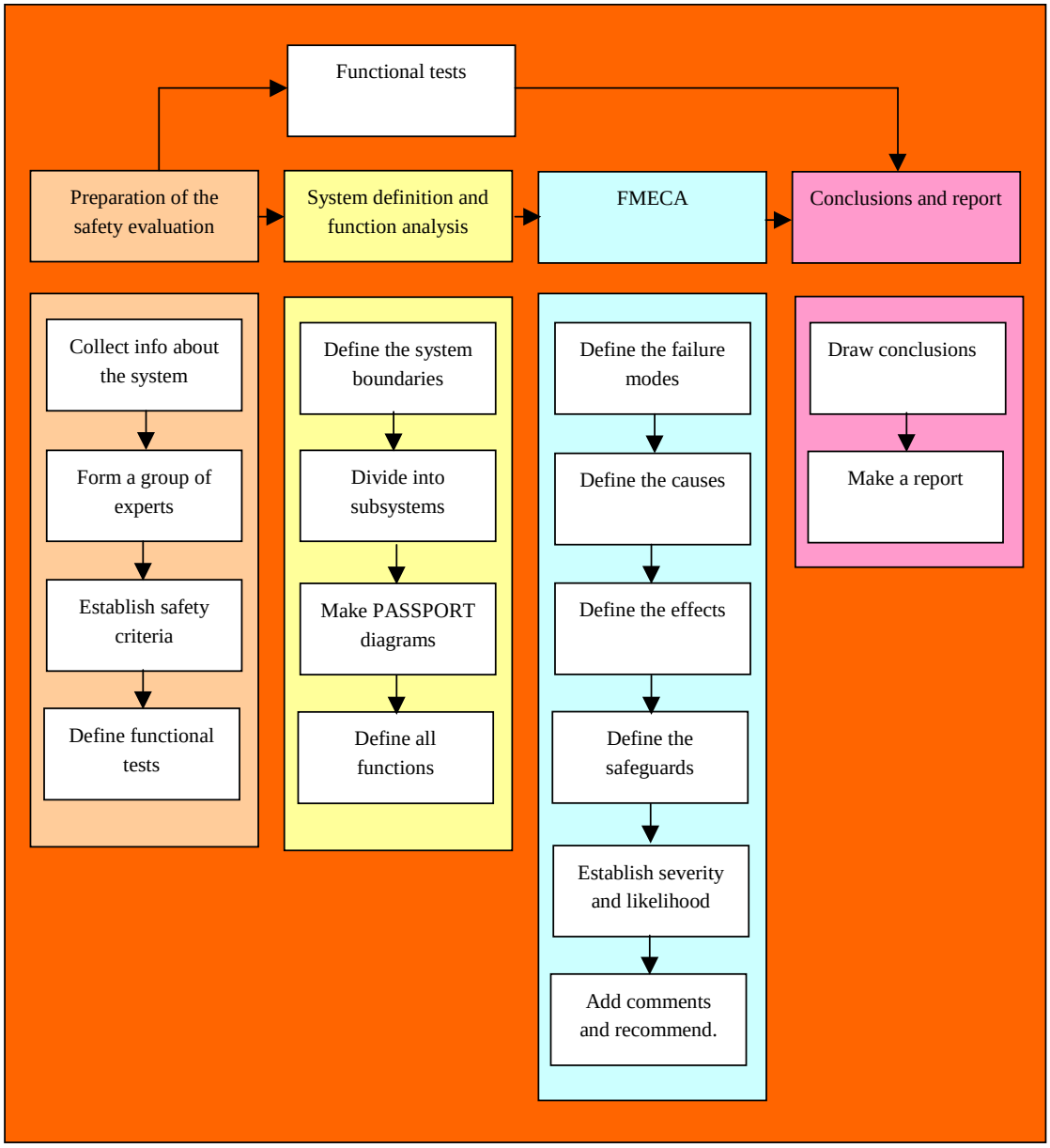

Figure 1 Overview of the structure.

It is important to work with the same group of people during the whole analysis. Changes in the group can disturb the process and the quality of the results. One of the group members performs the moderator function. His or her job is mainly to control the process and see to that all the process steps are properly taken.

3.3.3 Agreements on goals, safety criteria, planning and process

3.3.3.1 Goals

Before the actual analysis process starts a number of issues must be discussed, so that all parties involved agree on the basics of the analysis. Most important is the goal of the analysis. Is it a concept or design analysis, meant to identify safety issues, that have to be taken into account in following development phases, or is the goal certification, to establish that a system meets the given requirements. The system boundaries should be agreed upon so that it is clear which systems are part of the system to be analysed. In a cybercar system not only the vehicles, but also the central control system, the road infrastructure, the stops, possible energy supplies and garages could or could not be part of the analysis.

3.3.3.2 Safety criteria

In paragraph 2.4 a proposal is made for a manner in which a decision can be made as to what "safe enough" means. This proposal can give guidance and the resulting safety level can be chosen as the safety criterion for the cybercar system. However, until a generally agreed safety level for cybercars exists, it is important to decide on the safety criteria that are going to be used before the analysis starts.

3.3.3.3 Planning

The time needed for the safety evaluation depends of a number of aspects like the complexity of the system, how familiar the experts are with the system, experience with similar safety evaluation processes and the availability of results of former safety evaluations already done on the (sub)system. It is also important in what phase of the design process an analysis is carried out. A concept analysis, done in a phase when there is little or no detail information available will take considerably less time than a full analysis on a complete design.

It is therefore difficult to give reliable general estimates about the length of the analysis process and the time involved. Experience with FMECA sessions learns that individual sessions should be limited to 4 hours and that sessions should not be to close together. 2 - 3 sessions per week is a reasonable average. A really reliable estimate on the number of sessions needed can only be given after the completion of the preparation phase.

3.3.3.4 Process

It is important that the people who are going to be involved in the analysis are fully aware of the tasks that they are going to perform, of the type of questions that are going to be asked and of the process steps that are going to be taken. They also should be aware of what is going to be done with the results. This is generally guaranteed if the same people that are going to be involved in the preparation phase also will be involved in de following phases. Where this is not the case a clear explanation of goals, planning and process has to precede their involvement.

3.3.4 Functional tests

Cybercar systems are not standard devices like automobiles. It is therefore not possible to make a standard list of functional tests that should be carried out in each cybercar certification. For each cybercar system to be certified a dedicated list has to be made, based on the specifications of that particular system.

To illustrate this let us compare the 2 systems that have been analysed and are reported in Chapter .. . The Floriade Cybercab is a system that runs with a low speed (max. 12 km/h) on a dedicated infrastructure. The chances that a collision between a CyberCab, even if it drives at full speed, and a pedestrian would be fatal for the pedestrian is very small. Therefore there is only a limited obstacle detection system present in the shape of a bumper with emergency switches and a short distance ultrasonic device. The Rivium People Mover, on the other hand, is a much heavier vehicle driving with a higher speed (max. 40 km/h). A collision between this cybercar driving at full speed and a pedestrian could very well be fatal for the pedestrian. Therefore the Rivium People Mover has an extensive array of obstacle detection systems on board, for which a specific test cycle has been defined. The way in which the Floriade CyberCab is tested is completely different from the way the Rivium People Mover is tested.

The functional tests that are to be carried out strongly depend on the specification of the system. The main guideline in making the list of functional test therefore depends strongly on these specifications. Nevertheless, since the heart of the system always are a series of vehicles braking tests, tests of the steering system and acceleration and speed tests will almost always be included.

3.4 System definition and function analysis

3.4.1 General

The functions of the system to be analysed are the basis of the FMECA analysis. If not all functions have been identified certain failure modes can be overlooked. In order to be certain that all functions are being identified a strict procedure, as described below must be followed.

3.4.2 System definition

In order to avoid confusion about what is and what is not part of the system to be analysed a clear system definition is necessary. A simple method to help with this task is to define which (sub)systems are outside the system. Only those systems are listed that have interactions with the system.
In principle it is possible to perform an FMECA on the system thus defined. For analyses of very small systems this may be an option, but a complete cybercar system is much too complex for such an approach. Therefore the system is divided into subsystems that are analysed separately. The division in subsystem is done in a pragmatic way, so that systems to be analysed as much as possible coincide with actual subsystems in the vehicle. Experience with the procedure will be an advantage in choosing the optimum division.

Figure 2 shows a sheet that can be helpful in defining the various subsystems. For each separate subsystem that must be analysed a sheet should be made.

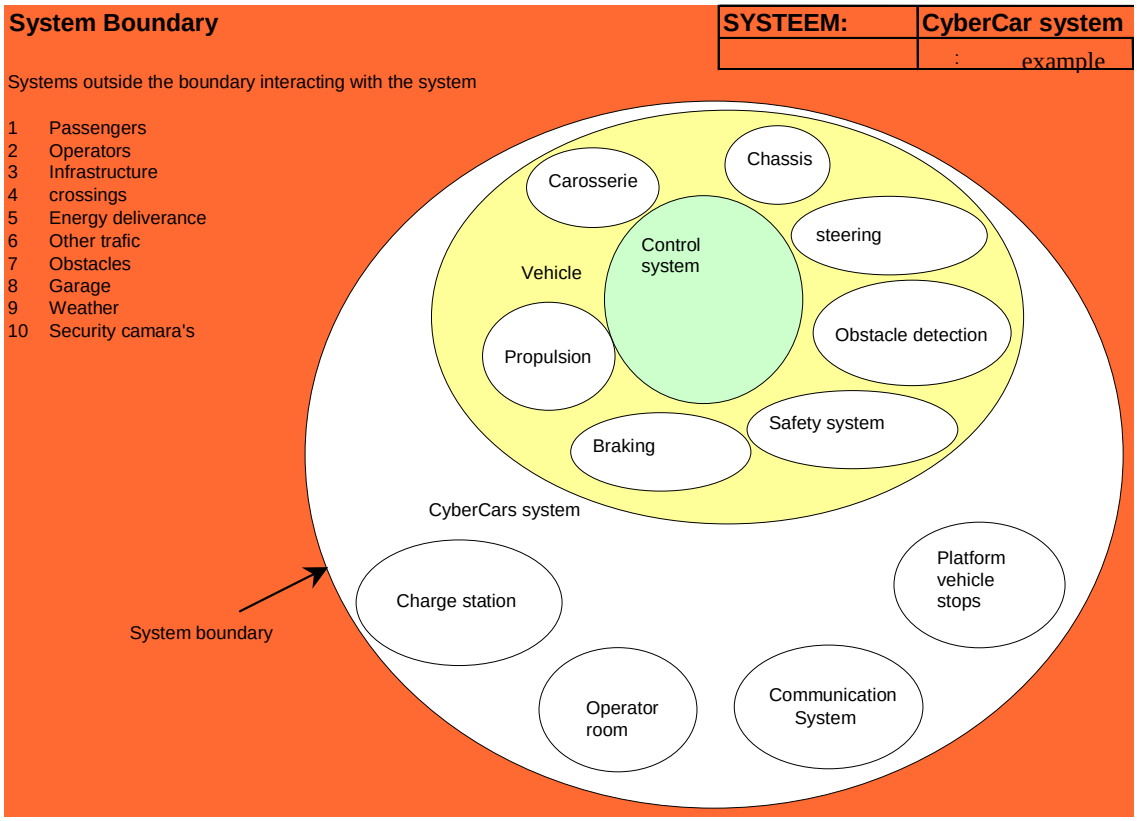

Figure 2 System boundaries

3.4.3. Function analysis

For each of the subsystems to be analysed the interactions between the subsystem and the subsystems outside the system boundary are listed. Interaction means that there is an exchange between the systems. These exchanges are always in the form of either information or matter or electric current. Although people strictly spoken are "matter" and radiation is "electric current", for practical reasons the division below is being used.
1. information
2. matter
3. people
4. electric current
5. radiation

All exchanges can be defined as either inputs or outputs of the system to be analysed and functions are defined as relationships between outputs and inputs. So if all the functions of a system have to be established it is sufficient to establish all relationships between outputs and inputs.

In order to establish all functions the PASSPORT method is used. The PASSPORT method is a result of the DRIVE-II project [7]. The goal of the project was to develop a systematic methodology for a hazard analysis of an advanced road transport telematic system. A PASSPORT diagram (see figure 3) is a graphical representation of the system.

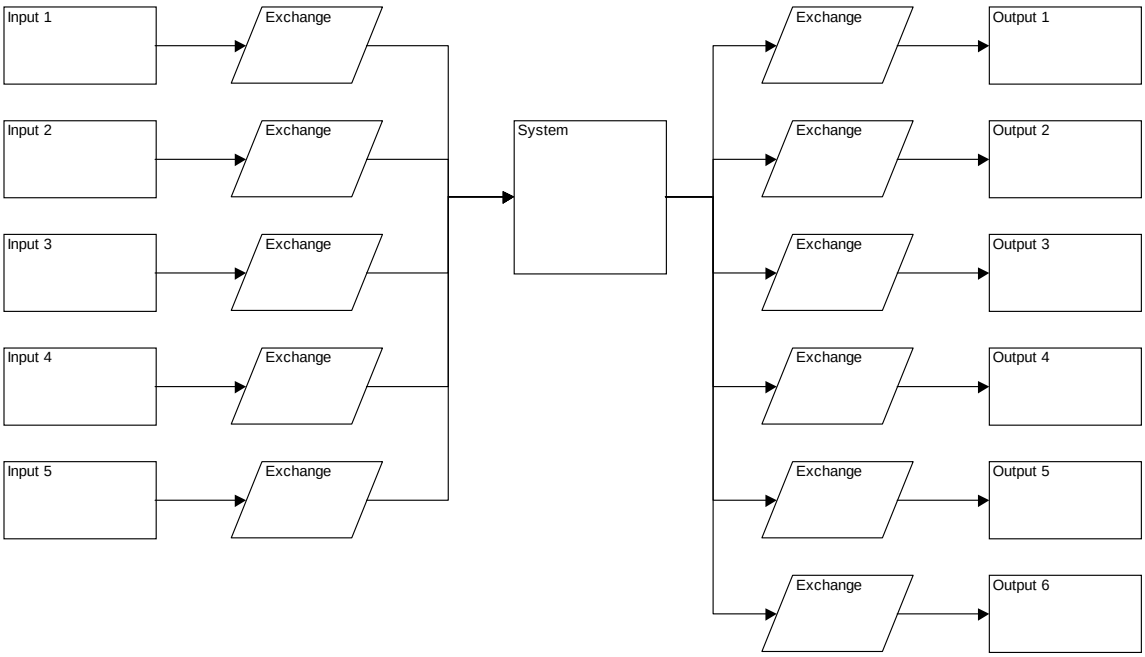

Figure 3: Example of a Passport diagram

The functions of a system are defined by the relationships between system outputs and system inputs. Therefore, in order to find all functions of the system for every output the inputs must be identified that have an influence on that output. The functions thus identified are the input for the FMECA analysis.

3.5 Failure Modes, Effects and Criticality Analysis (FMECA)

3.5.1 The FMECA process

The FMEA (Failure Modes and Effects Analysis) is an instrument that is used extensively in many industries to identify safety and reliability flaws in a design. In case it is not only important to identify flaws, but to also give them a certain value an FMEA becomes an FMECA (Failure Modes, Effects and Criticality Analysis). The basic principle is the same everywhere, but many variations in the execution of FMECA's are possible. For our purpose, where the FMECA must not only give a quantifiable result but also a reproducible one, it is important to follow a strict procedure.

FMECA sessions are carried out in a number of sessions by a group of 4 - 5 experts. The sessions are therefore very labour-intensive and a careful preparation as described in the paragraphs before is important. The steps in the analysis process are depicted in figure 4.

ID	FUNCTION	FAILURE MODES	CAUSES	EFFECTS	SAFEGUARDS	S	L	R	RECOMMEN-DATIONS	COMMENTS
1										
2										
3										
4										
5										
6										

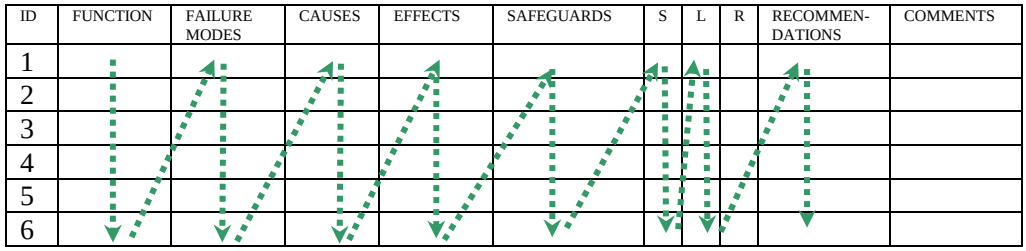

Figure 4. FMECA sheet

Function	In the column "Function" all functions are listed that have been identified in the function analysis.
Failure Modes	The column "Failure Modes" contains all modes in which the system can fail to perform each of the functions. As an aid in identifying failure modes checklists are available, but each system has its own characteristics and checklists will never be complete.
Causes	The column "Causes" lists all possible reasons for each failure mode. Often there is more than one cause for a failure mode. All of these possible causes are listed, even the most improbable.
Effects	In the column "Effects" the effects of each failure are listed per cause. In identifying effects it is important to have a thorough knowledge of the world outside the system boundary. When the system to be analysed is a cybercar, the effects can be totally different in a situation where the vehicles drive on a separate infrastructure where no other road users are present or when they make use of the public roads. In principle only those effects that threaten the safety of man, animals and material are listed. If the analysis not only concerns safety but for instance also reliability other effects, not directly related to safety can be considered.
Safeguards	The column "Safeguards" contains possibly built-in measures that can soften the effect of the failure. Safeguards are often included in users instructions, prohibiting the use of the system under certain risky conditions.
Severity	In the column "Severity" the seriousness of the effect is rated on a 5-point scale. The categories used are direct results of DRIVE II [7]. See paragraph 3.5.2
Likelihood	In the column "likelihood" the probability that an effect will occur is rated on a 5-point scale. See paragraph 3.5.2.
Safety Score	The safety score is a combination of the severity and likelihood score. It is a figure between 1 and 10 that gives an immediate rating for the risk that is related to the failure mode.
Recommendations	If the Safety Score is too low (below or near the safety criterion established in par. 3.3.3.2), recommendations can be included for actions that would raise the safety score to an acceptable level. Experience learns that during an FMECA the attendants often come up with ideas to improve the design. These improvements can also be included in the "Recommendations" column.

Comments — In the "Comments" column relevant remarks, like references to standards or reasons for a certain rating can be recorded, but also differences of opinion that emerged during the analysis or facts and events that came to light during the analysis.

3.5.2 Severity and likelihood tables

The table below shows the severity categories that were developed in the DRIVE II project [7]

	Category	Description
5	Uncontrollable	Failures whose effects are not controllable by the vehicle occupants, and which are most likely to lead to extremely severe outcomes. The outcome cannot be influenced by a human response.
4	Difficult to control	Failures whose effects are not normally controllable by the vehicle occupants but could, under favourable circumstances be influenced by a mature human response. They are likely to lead to very severe outcomes.
3	Debilitating	Failures whose effects are usually controllable by a sensible human response.
2	Distracting	Failures which produce operational limitations, but a normal human response will limit the outcome to no worse than minor.
1	Nuisance only	Failures where safety is not normally considered to be affected.

Table 1: Severity categories

In practice these categories appear to be easier to handle when they are interpreted in terms of harm to occupants and other road users:

	Category	Description
5	Uncontrollable	Failures that lead to many casualties. The outcome cannot be influenced by a human response.
4	Difficult to control	Failures that will result in severe injuries or even casualties. The outcome can be influenced by a mature human response.
3	Debilitating	Failures that will result in human injuries. The effects are usually controllable by a sensible human response.
2	Distracting	Failures which produce operational limitations, but no human injuries.
1	Nuisance only	Failures where safety is not normally considered to be affected. No human injuries; only operational loss.

The severity categories are easy to work with, but the likelihood ratings appear to be the most difficult and most critical part of the analysis. In practice it is difficult, even for experienced engineers to

establish whether a component will fail once in every 10 years, or once in every 100 year or even once in every 1000 years. Here more background information is needed, for instance in the form of tables with failure data for various components and other reference data based on practical experiences. The documentation collected at the beginning of the process should include all manufacturer information about failure data of critical components. For the likelihood of software failure the principles set out in paragraph 2.3.2 can be used.

	Likelihood
5	Once in 10 years
4	Once in 100 years
3	Once in 1000 years
2	Once in 10.000 years
1	Once in 100.000 years

Table 2: Likelihood categories

3.5.3 Safety score

The combination of the severity and likelihood scores leads to a safety score for the failure mode and its cause. Table 3 shows the combinations as they were used in the analysis performed until now. In this table the highest safety score is 10 and the lowest safety score is 1. The figures in the table are not based on a formula but are arbitrary figures that only have a practical basis. More discussion and more experiences with the method are necessary to establish a final table.

Safety score		Likelihood				
		1	2	3	4	5
Severity		1/100.000 years	1/10.000 years	1/1000 years	1/100 years	1/10 years
1	Nuisance only	10	10	9	7	5
2	Distracting	10	9	8	6	5
3	Debilitating	7	6	5	5	4
4	Difficult to control	6	5	4	3	2
5	Uncontrollable	5	4	3	2	1

Table 3 Safety score table

3.6 Conclusions

The result of the FMECA analysis is a table with a large number of safety scores and a number of recommendations. The safety level for the system or subsystem is equal to the lowest safety score in the table. That means that if one single failure mode results in a safety score that is lower than the safety requirement, than the complete system does not meet that requirement. The complete system is considered to be as safe as its weakest link.

The results are laid down in a report that contains as a minimum the following:
1. Agreements on goals, safety criteria, planning and process

2. System definition
3. Function analysis
4. FMECA sheets
5. Result of the functional tests
6. Conclusions
7. Certificate

4. EVALUATION

4.1 The CyberMove pilots

The value of an evaluation method can only be proven in practice, by carrying out evaluations on real systems. The CyberCars project with the focus on technology development, is strongly linked to the CyberMove project where the focus is on actual pilots, in which cybercar systems are evaluated in a real environment. The opportunity therefore presented itself to evaluate the method using real Cybernetic Transport Systems. From the various pilots in the CyberMove project 2 projects were selected: The 2nd generation Rivium People Mover and the Floriade CyberCab. The evaluation of the 2nd generation people mover largely took place within the framework of a separate project. In the present report only the results that concern the evaluation method are presented. The results of the actual safety analysis and the recommendations made to the developers of both systems are confidential and not relevant for the topic of this report.

With neither of the pilots it was possible to apply the analysis method to the complete development life cycle, as is recommended. The 2nd Generation Rivium People Mover was in an advanced state of development when the development started. The Floriade CyberCab pilot had already ended. Nevertheless both analysis supplied valuable results. During the analysis of the Rivium People Mover a lot was learned concerning the analysis of a developing product, in which the state of development changes during the analysis. The Floriade CyberCab analysis allowed a comparison between the results of the analysis and the actual recorded behaviour of the system.

4.2 The 2nd Generation Rivium People Mover

The 2nd generation Rivium People Mover is presented in deliverable 2.1 of Cybermove [2]. The system has a maximum transport capacity of 400 persons per hour per direction with 6 similar vehicles. The vehicles have a maximum capacity of 20 persons, a maximum speed of 32 km/hour, a mass of 3750 kg and have a obstacle detection system on board. The vehicles run on a separate road infrastructure with a number of secured crossings where traffic can cross the path of the people movers. There are a number of platforms where passengers can get in and out of the vehicles. The vehicles are guided by magnets placed at regular distances in the road surface. There is a central controller from where the information exchange between vehicles is being controlled.

The 2nd generation Rivium people mover was developed and built by a consortium of Dutch companies led by Frog Navigation Systems. The system will be operated by Connexxion, one of the largest Dutch public transport operators. The vehicle was largely based on the basis of coach technology and where possible subsystems were certified in accordance with the current regulations for buses. In addition to the evaluations according to the method described in this report a number of additional technical tests were carried out in order to check the performance of subsystems like the obstacle detection system. The safety evaluation took place in the second part of 2003. Because of financial and time constraints the number of subsystems that was analysed had to be limited, so the focus was on safety-critical subsystems and on those subsystems that are related to vehicle navigation and control.

Figure 5: 2nd Generation Rivium People Mover

4.3 The Floriade CyberCab

During the Floriade, a horticultural exhibition held in The Netherlands in 2002, people were transported from the foot of a hill to the top by so-called CyberCabs, small automatic guided vehicles that could carry 5 people with a maximum speed of 12 km/h. The CyberCab used a wire guided system, with navigation sensors on the vehicle and a wire embedded in the road surface. At specific locations magnets were placed in the road surface to provide location information to the CyberCabs. The track was a separated piece of road, 1200 meters long, where no other traffic was present and where pedestrians were not allowed. There were two stations, one at the foot and one at the top of the hill, where people could get in and out of the CyberCabs. The CyberCabs were built by Yamaha and operated by 2GetThere, both partners in the CyberCars project. The system was operated by a team, consisting of a site manager, a system operator and stewards to assist people at both stops. The pilot lasted about 6 months, during the whole period the exhibition was open.

In the system definition phase, the system was defined as the complete CyberCab system, including infrastructure, loading station and stops. As an experiment, the operators were defined as part of the system, while the passengers were not. In total 15 subsystems were defined and analysed. Because of time and financial constraints only 8 FMECA sessions were held. Although this total number of sessions was small, the relative simplicity of the system allowed a thorough analysis that provided a lot of information.

One of the most interesting conclusions was that the people, the operator and the stewards were the major causes of danger.

Figure 6: The Floriade CyberCab

4.4 Conclusions and recommendations

4.4.1 General

In general the method proved to be a useful instrument to identify safety critical issues in cybercar systems. The method proved useful for evaluation of the vehicles in such systems, but also for the infrastructure in which the systems operate.

Whether or not the method can also be used as a certification instrument strongly depends on the reproducibility of results. The limitations of the present project did not allow for an evaluation of one system by different groups of analysts.

Although the method described consumes a considerable amount of time, in the end the balance is positive, not only because it can be proved that the resulting system meets the applicable safety requirements, but also because the method helps in identifying and making design decisions in an very early stage, so that the number of feedback loops in the design process can be minimised.

4.4.2 System definition and function analysis

In all evaluations carried out until now, it appeared that a good preparation is extremely important. Collecting information and making a system definition and a function analysis takes at least as much time as the FMECA analysis itself.

It is important to choose a uniform terminology and to stick to it. In several cases confusion arose because analysts thought they were speaking about the same issue where they only used the same language. Terminology used in the system documentation should be uniform and during the analysis the terminology laid down in the documentation should be used.

4.4.3 FMECA

During the evaluation of the 2nd generation Rivium people mover the system was still under development. The same people that were taking part in the evaluations were also taking part in the development, which now and then caused confusion, because the developers had to discuss system-

components that at the time of discussion were not current anymore. In order to limit the confusion it is important to keep the time spent on the analysis of one particular subsystem as short as possible.

Taking into account design changes that have taken place after the system definition was made, must be avoided, because these design changes might have an adverse effect on the results of parts of the analysis that have already been completed.

In cases where it was not possible to establish a severity or likelihood figure, or in cases where a difference of opinion remains between analysts, always the least favourable option was selected. In some cases this could lead to a low safety figure. It is therefore important always to keep in mind that if a resulting safety figure for a system is so low that the requirement is not met, this does not always mean that the system is unsafe. It can also mean that safety could not be proven. This is especially the case with software.

The safety analysis of software is an item that requires attention. Often software has not been developed according to accepted software standards and very often it is also impossible to test such software in such a way that it can be satisfactorily proved that the software is safe.

4.4.4 Recommendations

One of the most important questions that remains is whether the reproducibility of the results is good enough for certification purposes. One of the next steps therefore is to carry out an analysis of one system with different independent teams of analysts and compare the results.

In order to identify all possible failure modes, it would be helpful to have a dedicated reference list for cybercars. Even more important is a reference list with failure data of critical components, to give guidance to analysts in establishing likelihoods.

The establishment of safety criteria also requires attention. The proposal done in this report is only one of many possibilities. Especially the development described in paragraph 1.4, where FAKRA is developing an adaptation of IEC 61508 for ADA systems could be important for cybercars.

In general it is recommended to very carefully monitor all developments in Europe, but also in the USA and Japan on related test and certification issues. It is considered of major importance that there is a harmonisation of standards.

Because it is important that the procedure is followed carefully it is recommended to develop a manual, that can help analysts to take the correct steps in the correct order. Although the method is certainly not difficult to use, the procedure is extensive and it is easy to forget or overlook things.

5. REFERENCES

1. Safety Standards for cybercars; deliverable 6.1: Existing Standards and Guidelines. J.J. Uwland and J.P. van Dijke; september 2002

2. CYBERMOVE deliverable D2.1, Site selection,2002,EESD EVK4-2001-00050

3. RESPONSE II European project IST-2001 37528

4. ECE-Regulation 79. Uniform provisions concerning the approval of vehicles of categories M,N and O with regard to steering equipment.

5. ECE-regulation 13: Uniform provisions concerning the approval of vehicles of categories M,N and O with regard to braking.

6. IEC 61508: Functional Safety of electrical/electronic/programmable electronic safety-related systems.; IEC 1998

7. Framework for Prospective System safety Analysis Volume 1; Preliminary Safety Analysis; Hobley, K.M. e.a. DRIVE-II project, V2058, Deliverable 9a. December 1995.

8. IEEE Software Engineering Standards; IEEE 1999

9. DO-178B: Software Considerations in Airborne Systems and Equipment Certification. RTCA, december 1992.

10. System Safety Analysis Handbook; System Safety Society.

ANNEX 1: Example of a certificate

The certification process should result in a certificate that shows that the system meets or does not meet the requirements. Since cybercar systems can differ from each other strongly and since a system may or may not include infrastructure and communication devices there is no standard set of requirements and thus there cannot be a standard certificate. The proposal therefore is to include a table stating what the requirements are, what the results of the tests and analyses are and a conclusion as to whether or not the system did meet the stated requirements. This Annex 1 gives an example of such a cybercars certificate.

CERTIFICATE

concerning the approval of a cybercar system with the following characteristics:

Manufacturer: _____
Type: _____

The system was tested in accordance with the provisions in the [safety Standards for cybercars] and did / did not meet all of the applicable requirements as set out in the table below.

Nr	Item	Requirement	Result	Passed/Failed
	Systems safety Analyses	safety level ≥ 4	4	Passed
Functional tests				
1	Braking	meets ECE -13	see report nr ..	Passed
	Additional requirements			
	Maximum deceleration	5.5 m/s^2	6.5 m/s^2	Passed
	Nominal deceleration (normal braking)	1.5 m/s^2	1.6 m/s^2	Passed
2	Obstacle detection			
	Detection of obstacle 1		detected	Passed
	Detection of obstacle 2		detected	Passed
	Detection of obstacle 3		detected	Passed
3	Acceleration			
	Nominal acceleration	1.0 m/s^2	1.1 m/s^2	Passed
4	.....			
5	.....			
6	.....			

Certifying authority date and stamp

_____