

EUROPEAN COMMISSION DG RESEARCH

SIXTH FRAMEWORK PROGRAMME
THEMATIC PRIORITY 1.6
SUSTAINABLE DEVELOPMENT, GLOBAL CHANGE & ECOSYSTEMS
INTEGRATED PROJECT – CONTRACT N. 031315



Towards advanced transport for the urban environment

Deliverable no.	D. 2.5.2
Dissemination level	Public
Work Package	2.5 Legal and administrative issues
Author(s)	WP 2.5 partners: IKA, SINTEF, TNO
Co-author(s)	
Status (F: final, D: draft)	F : Version 3.0, 01-04-2010
File Name	Certification procedures for automated transport systems
Project Start Date and Duration	01 May 2006 - 30 April 2011

TABLE OF CONTENTS

1	INTRODUCTION	4
2	SAFETY	5
2.1	HISTORY.....	5
2.2	SAFETY ANALYSIS PROCESS	5
2.3	REQUIREMENTS	6
2.4	CONSIDERATIONS AND CHOICES.....	8
2.4.1	<i>Relevant standards</i>	8
2.4.2	<i>References: "how safe is safe enough"</i>	9
2.4.3	<i>Limitations</i>	9
2.5	THE CERTIFICATION METHOD.....	10
2.5.1	<i>General</i>	10
2.5.2	<i>Overview</i>	11
2.5.3	<i>Preparation</i>	12
2.5.4	<i>System definition and function analysis</i>	14
2.5.5	<i>Failure Modes, Effects and Criticality Analysis (FMECA)</i>	16
2.6	EVALUATION OF THE PROCEDURE.....	21
2.6.1	<i>Introduction</i>	21
2.6.2	<i>Learning points and improvements</i>	23
3	CONCLUSIONS	25
4	REFERENCES	26
	ANNEXES	I
	Annex 1 : Flow diagram FMECA procedure	i
	Annex 2: Various sheets, used in the procedure	iv

Abstract

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

Deliverable 2.5.2 describes certification procedures for automated transport systems. The first version of these certification guidelines were developed in the framework of the CyberCars and CyberMove projects [1, 2, 3], which were carried out between 2000 and 2004. In the CityMobil project these draft procedures were updated to include the developments of the past 5 years and a full evaluation was carried out on the people mover for the CityMobil Rome demonstration. The result of the evaluation was that the Rome people mover met the requirements set out at the beginning of the analysis process. The evaluation provided a number of learning points, which have been included in the final procedure, as presented in the present deliverable.

1 Introduction

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

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

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

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

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

In the second part, from month 19 (December 2007) to month 44 (January 2010) the recommendations on safety, security and privacy and the results of the discussions on barriers, were further discussed in a workshop in Brussels in November 2009. During the workshop the WP 2.5 partners were supported by two experts: Mr. T.M. Gasser from BAST in Germany and Dr. Jørn Vatn, from SINTEF in Norway. Their contribution was highly appreciated. The results, a series of guidelines on security and privacy and strategies to address the remaining barriers are included in CityMobil deliverable D.2.5.3: Guidelines for safety, security and privacy; barriers to implementation.

The draft certification procedures were evaluated by applying them to the new transport system for the Fiera di Roma, the subject of one of the 3 large scale CityMobil demonstrations. The results of the evaluation and the final procedures can be found in the present deliverable D.2.5.2.

2 Safety

2.1 History

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. In the CyberCars and CyberMove projects [1, 2, 3], that were carried out between 2000 and 2004 the first version of what were called "Recommendations for certification procedures" for fully automated transport systems without mechanical guidance were described. Since then a lot of experience has been gained with these draft procedures. Several analyses of automated transport systems were carried out, among which the Floriade people mover and the Parkshuttle, that presently operates in Capelle a/d IJssel in the Netherlands. In the first years of the CityMobil project the draft procedures were updated to include the latest developments in regulations. In 2009 a full evaluation was carried out with the people mover for the CityMobil Rome demonstration as a subject. This evaluation provided a number of learning points, which have been included in the final procedure, as presented in this deliverable.

2.2 Safety analysis process

The draft procedures consist of a number of steps that together constitute the certification procedures. These steps are:

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

1. Preliminary risk reduction

In the first step the risk reduction method [3] is used to roughly analyse a number of 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. The Risk Reduction Method is a 'quick and dirty' method that is also suitable as an instrument to evaluate the safety of showcases and demonstrators, where a comprehensive safety analysis is impractical or too expensive.

2. Determine which safety regulations apply

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

3. Production and implementation of the system

In the third step, for which the manufacturer of the system 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 ADA systems, as developed in the Response projects [4]. 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.

For the safety evaluations the analysis method described in step 4 below should be used. It is important to realize that safety is not just ensured by a certification process. Certification is only the final step in a process to develop a safe product. Safety should be a main point of attention from the moment the first concept is developed and should remain to be a point of attention during the complete life cycle of the system. This is known as life cycle safety. The certification procedure described below can be used for the final certification, but also to carry out analyses throughout the design and development of the transport system. Each analysis step may result in improvements that either reduce the need for expensive design changes in a very late phase because of safety flaws that are discovered during certification or avoid the implementation of expensive redundancies that otherwise would have been installed "just to be sure".

4. Certification

In the final step the system is certified, using the certification procedures described in Chapter 2 of this deliverable and Annex 1. An independent evaluator should carry out the procedure, until, after formal acceptance of the procedures by the European authorities a notified body will take over this task.

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

2.3 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. 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 meet the requirements when the system is up for its final certification test.

- 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 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.

2.4 Considerations and choices

2.4.1 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 probably is IEC 61508: Functional Safety of electrical/electronic/programmable electronic safety-related systems [5]. 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 automated transport systems 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 the work described in this deliverable. 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 [6] 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 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 defined in much detail and the process moderator 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.

2.4.2 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 km/hour we can calculate that there will be 36×10^{-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.

2.4.3 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 [7]) 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 2nd interpretation would offer a window for the introduction of automated transport systems on public roads, but at present only the first interpretation is accepted.

2.5 The certification method

2.5.1 General

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. 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.

2.5.2 Overview

On the basis of the considerations, choices and limitations laid down in Paragraphs 2.2, 2.3 and 2.4, 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 2.1 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.

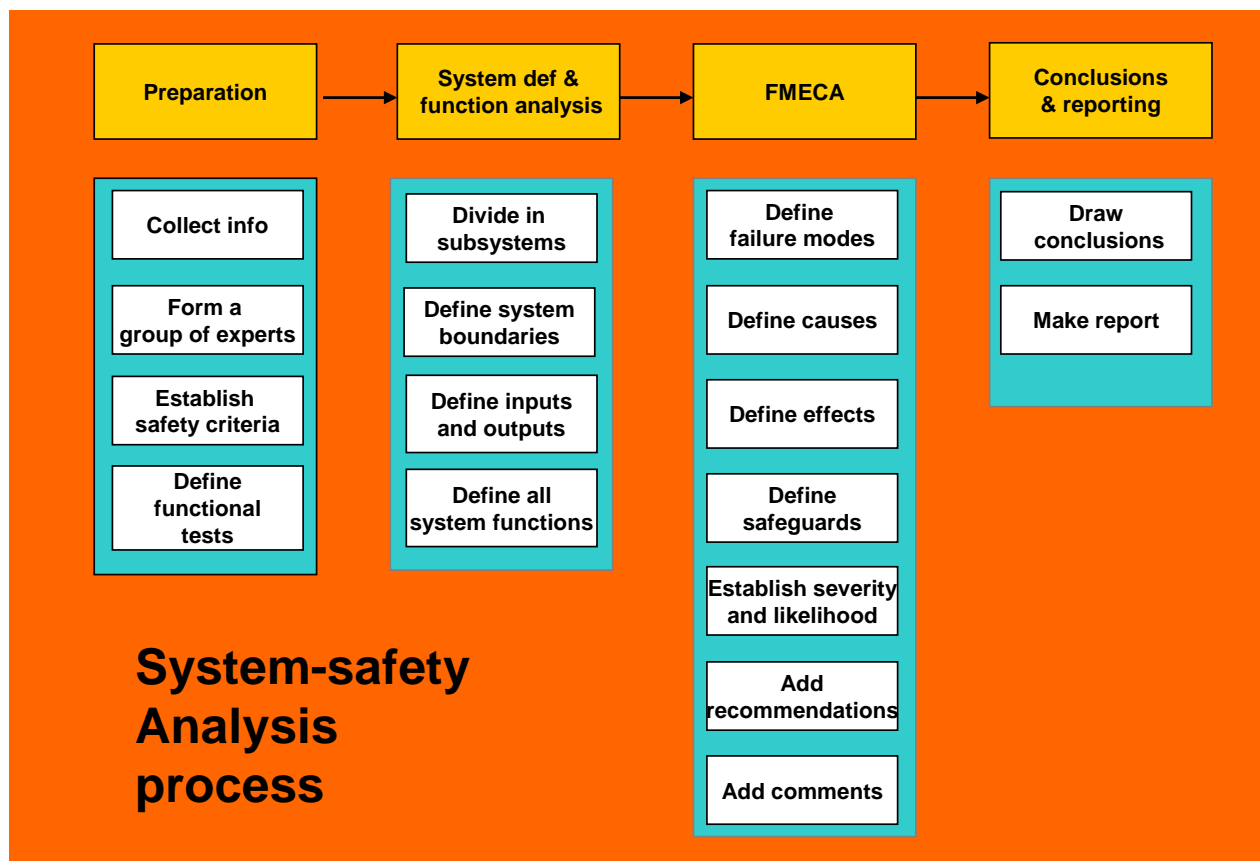


Figure 2-1: Overview of the structure

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
 - Divide into subsystems
 - Define system boundaries
 - Define inputs and outputs per sub-system
 - Define all system 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

2.5.3 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.

2.5.3.1 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 activities, 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

2.5.3.2 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 an automated transport system 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 such suppliers 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.

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.

2.5.3.3 Agreements on goals, safety criteria, planning and process

2.5.3.3.1 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 parts 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.

2.5.3.3.2 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 automated transport system. Until a generally agreed safety level for automated transport systems exists, it is essential to decide on the safety criteria that are going to be used before the analysis starts.

2.5.3.3.3 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 system.

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 too close together. Experience learns that after 4 hours of intensive analysis attendants are often not as clear and sharp anymore as is required. 2 - 3 sessions per week is a reasonable average. A really reliable estimate on the number of necessary sessions can only be made after the completion of the preparation phase.

2.5.3.3.4 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 the following phases. Where this is not the case a clear explanation of goals, planning and process has to precede their involvement.

2.5.3.4 Functional tests

Automated transport 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 automated transport system certification. For each 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 2 systems that have been analysed and are reported in [1] The Floriade Cybercab is a system that runs with a low speed (max. 12 km/h) on a dedicated infrastructure. The chance 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 types of functional test therefore depend strongly on these specifications. Nevertheless, since we are talking about vehicle systems, a series of braking tests, tests of the steering system and acceleration and speed tests will almost always be included.

2.5.4 System definition and function analysis

2.5.4.1 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.

2.5.4.2 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 to be analyzed. 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 indeed be an option, but a complete automated transport 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.

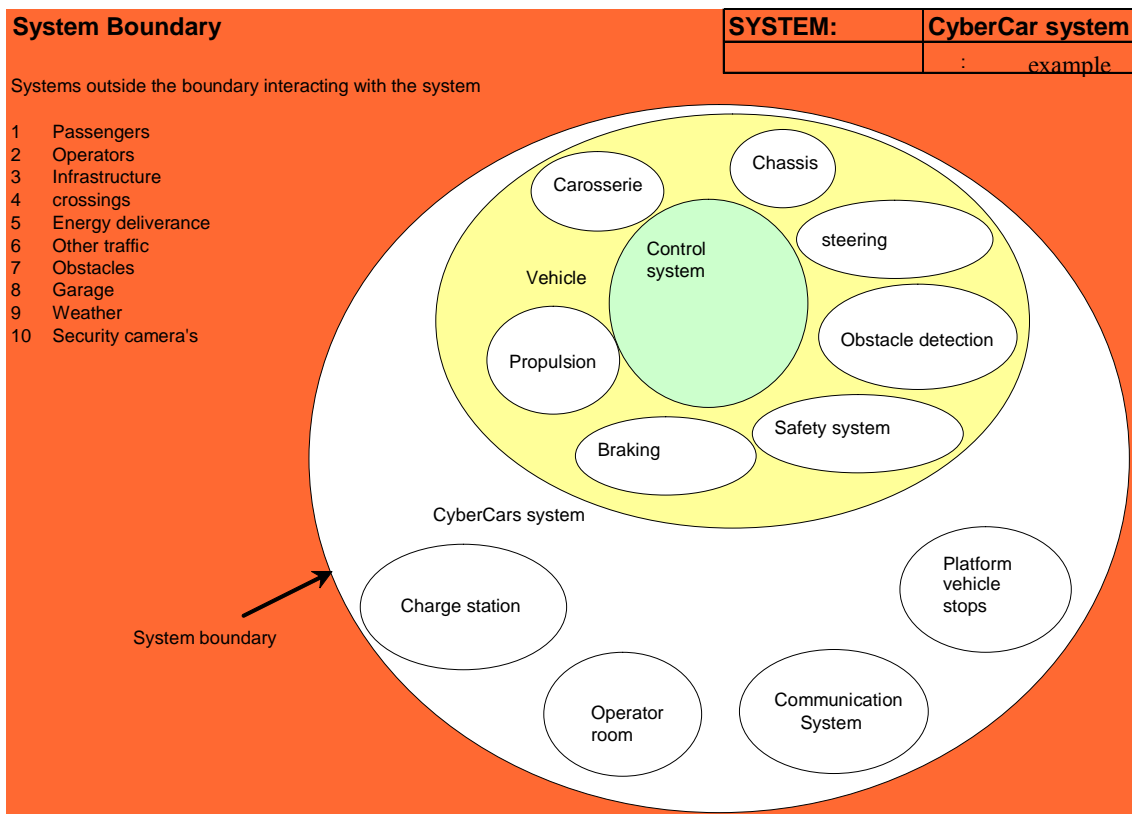


Figure 2-2: System boundaries

Figure 2.2 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. Within the circle describing the system boundary are the sub-systems that are part of the system to be analyzed. They can be divided in sub-systems also. In the left top corner are the sub-systems that are outside the system boundary and are not part of the system to be analyzed. Nevertheless, there are interactions between the sub-systems within the system boundary and those outside the boundary

2.5.4.3. Function analysis

For each of the subsystems to be analysed the interactions between the subsystem to be analyzed 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

Per definition 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 individual output the inputs must be identified that have an influence on that output. The functions thus identified are the input for the FMECA analysis.

2.5.5 Failure Modes, Effects and Criticality Analysis (FMECA)

2.5.5.1 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 the purpose described here, 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.

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 any of the functions. As an aid in identifying failure modes checklists can be made, 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 between situations 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 people are listed.
Safeguards	The column "Safeguards" contains built-in measures that can soften the effect of the failure or decrease the likelihood of occurrence.
Severity	In the column "Severity" the seriousness of the effect is rated on a 4-point scale. See par. 2.5.5.2
Likelihood	In the column "Likelihood" the probability that an effect will occur is rated on a 5-point scale. See paragraph 2.5.5.2.
Safety Score	The safety score is a combination of the severity and likelihood score. The safety score is a figure representing the risk that is related to the failure mode-effect combination.
Recommendations	If the Safety Score is too low (below or near the safety criterion established in accordance with par. 2.5.3.3.2), recommendations can be included for actions that will 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.

2.5.5.2 Severity categories

The table below shows the severity categories that are used for the analysis. They are based on the descriptions in ISO 26262: Road vehicles - Functional safety [8]

	Category	Description
S3	Fatal	Perilous injuries and fatalities
S2	Serious	Serious injuries, survival probable
S1	Moderate	Light and moderate injuries
S0	No injuries	No injuries, only operational losses

For each failure mode/cause/effect combination the severity is established. There can be many different effects of a failure mode/cause combination, but for the purpose of this

analysis only the most severe effects are chosen. These are typically the effects that result in harm to people involved. It is not always sufficient just to list and rate the worst case. It is always possible that an effect with a lower severity results in a higher risk than the worst case effect, because the likelihood of the less severe effect can be higher.

2.5.5.3 Likelihood categories

The likelihood that is used in the analysis is the likelihood that the failure mode/cause/effect combination occurs. The table below shows the 5 likelihood categories that are used. The severity categories are usually easy to work with, but the likelihood ratings are the most difficult and most critical part of the analysis.

	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

The likelihood concerns the likelihood that the cause occurs in combination with the likelihood that the effect will occur. The likelihood category therefore is often a combination of two figures.

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.

If such information is not available, a simple list with example likelihoods is used. This list is based on experience rather than on hard data and each time the list is used a consideration should be made as to whether or not the figure chosen is realistic in the particular situation.

LIKELIHOOD rules of thumb		
L5	1/10 years	Human activities. Software that is not developed in accordance with accepted software development guidelines
L4	1/100 years	-
L3	1/1000 years	mechanical subsystems; heavy stress; electrical subsystems own production; electronical consumer subsystems
L2	1/10000 years	mechanical subsystems; own production; electrical subsystems (shortcuts; cable breakage; loose contacts); electronical industrial subsystems
L1	1/100000 years	complete certified (mechanical) subsystems; failure rate available; software developed acc. Accepted software engineering standards

An example to show how a typical likelihood rating is made:

Failure mode: A machine suddenly starts operating when it should not

Cause: A shortcut in the wiring (electrical failure)

Effect: A maintenance worker is hurt and possibly killed by moving parts of the machine

The likelihood of this failure mode/cause/effect combination is the likelihood that a shortcut occurs in combination with the likelihood that some maintenance worker is working on the system and gets hurt:

The likelihood of the cause (L_{cause}), a shortcut, according to the table above is L2 (1/1000 years). For the likelihood of the effect an analysis should be made. If the machine is only switched off for maintenance purposes the chance that a maintenance worker is present is 100%. Depending on the type of machine and the type of maintenance work an estimation must be made of the chance that the maintenance worker really will be hurt. Suppose that that chance is 1 in ten times. That will result in a likelihood (L_{res} of 1/1000 years * 1/10 is 1/10000 years. The likelihood category is 2.

In order to understand this figure it is helpful to realize that if the chance of the failure mode/cause/effect combination is 1/10000 year and if there are 10000 machines like of this particular kind in the world, there will be a casualty because of this failure mode cause/effect combination every year.

Establishing the failure rate of software is even more difficult than establishing the failure rate of an electrical or mechanical system. Therefore a simple rule is used: If it can be demonstrated by means of written certificates that software has been developed in accordance with established software engineering standards (for instance the IEEE software engineering standards) the software is considered safe ($L=1$). If it cannot be shown that software is developed in accordance with such standards the software cannot be considered safe ($L=5$). This last qualification does not imply that the software is unsafe; it just means that safety cannot be proven.

2.5.5.4 Safety score

The combination of the severity and likelihood scores leads to a safety score for the failure mode and its cause. The table below is used to establish the safety scores. The highest score is 5 and the lowest score is 1.

Safety score R							
		Lres	1 / 100.000 years	1 / 10.000 years	1 / 1000 years	1 / 100 years	1 / 10 years
			Lres1	Lres2	Lres3	Lres4	Lres5
S0	No injuries		5	5	5	5	5
S1	Moderate		5	5	5	4	3
S2	Serious		5	5	4	3	2
S3	Fatal		5	4	3	2	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. In a number of analyses of automated vehicle systems carried out between 2003 and 2009 the safety criterion was that a safety score of 5 is the threshold. 5 is still acceptable. Everything below 5 is too low. This threshold was derived from European accident data as referred in par. 2.4.2.

2.5.5.5 Safeguards

The likelihoods established in accordance with par. 2.5.5.3 are usually established without taking into account that the system designers have built in safeguards. Safeguards are measures that can soften the effect of the failure (lower severity) or decrease the likelihood of occurrence. After establishing the safety score and only when the safety score is above the safety criterion that was established, it should be established whether there are safeguards present. If there are, a new rating of severity and likelihood, now with the safeguard included is made. The table in par. 2.5.5.4 gives the final score for the failure mode/cause/effect combination.

There again is a separate safeguard rating for software. The rating for software safeguards depends on the type of safeguard, according to the table below. The effects of the different safeguards must be considered as 'rules of thumb'. The values are not based on calculation or analysis, but are assumptions. Representative values will only be available after a long period of use of the method in practical situations.

	Category	Effect
C1	Hardware safeguard	$L_{failure} * L_{safeguard}$
C2	Software safeguard; part of the same software system	$L_{failure} / 10$
C3	Software safeguard; part of same type of software in a separated system	$L_{failure} / 1000$
C4	Software safeguard; different software in separated systems	$L_{failure} / 10000$

C1 Hardware Safeguards

A hardware safeguard is an independent system with its own likelihood of failure. If a hardware safeguard is built in to protect against a software failure, the likelihood of failure of the hardware safeguard is usually much lower than that of the software. The total likelihood is the likelihood system * likelihood safeguard.

C2 Software safeguard; part of the same system

The same software, with the same likelihood of failure, placed in the same housing and thus vulnerable to the same influences that caused the failure of the basic software. Basically we have two software modules in the same system that check each other. The value of the safeguard is limited. Decreases the total likelihood with one step (factor 10)

C3 Software safeguard; part of the same software in a mechanically separated system

Still the same software, vulnerable to the same influences, but placed in a different mechanical environment. Decreases the total likelihood with three steps (factor 1000)

C2 Software safeguard; different software in a mechanically separated system

The chances that different software, placed in a different housing fails at the same time as the basic software is very small. Decreases the total likelihood with 4 steps (factor 10000)

2.5.5.6 Final safety score

After the influence of the safeguards is taken into account the final safety score can be established based on the resulting severity and the resulting likelihood. For this the table as shown in par. 2.5.5.4 is used again. In this table a safety score of 5 means that the system is safe enough and that no further risk mitigation actions are needed with regard to that particular failure mode/cause/effect /safeguard combination. If the safety score is less than 5, usually a recommendation is included in the FMECA sheet, with remarks on the non-conformity and possible ways to improve the situation.

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 total 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, then the complete system does not meet the requirement. The complete system is considered to be as safe as its weakest link.

2.5.5.7 Report

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

2.6 Evaluation of the procedure

2.6.1 Introduction

The certification procedure was evaluated by using it to analyze 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. Figure 2.3 shows a lay-out of the parking area and figure 2.4 shows one of the vehicles that were developed for this system.

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, with representatives of ITR (Rome

demonstration project manager), Robosoft (producer of the system), ATAC (system operator) and TNO (safety analysis moderator) present. Part of the work was done in Biarritz, France, where Robosoft has its manufacturing plant and the remaining part was done in Rome.

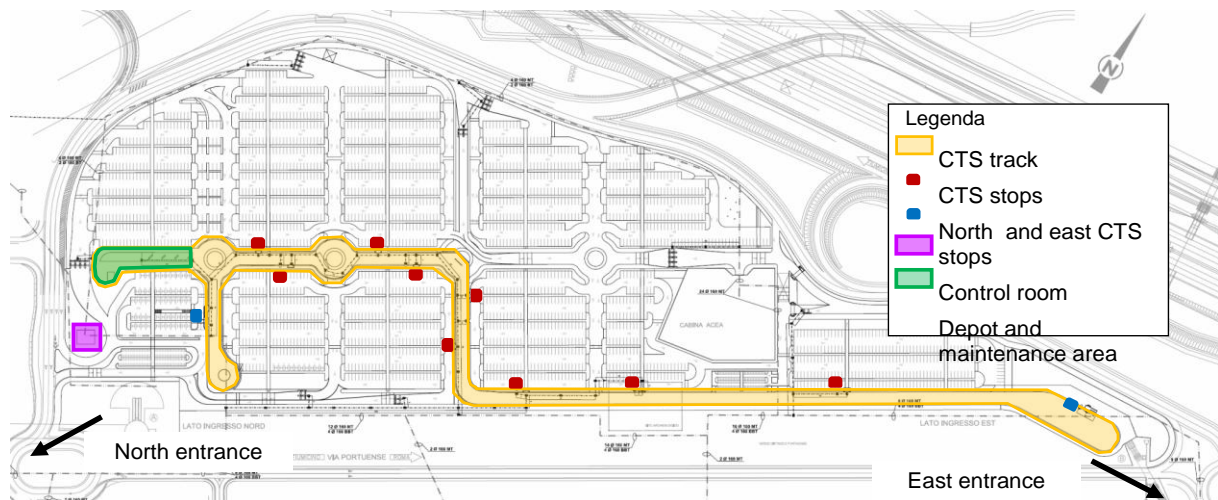


Figure 2-3: Rome Fiera parking

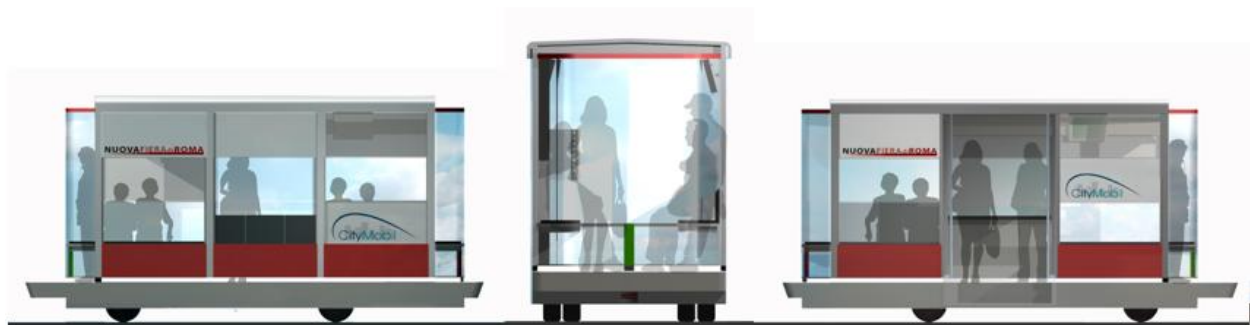


Figure 2-4: Vehicle for the Rome Fiera

The most important decision concerned the safety criteria, the acceptable safety level, expressed as the minimum safety score the system should meet. In order to determine a reasonable safety level it was decided to use existing accident statistics for road vehicles as a basis. It was agreed that the automatic guided vehicles on private roads should be at least twice as safe as cars on public roads. That decision led to a maximum number of fatalities per traveller-kilometre and that figure corresponds with a safety score of 5 in the FMECA table (2.5.5.4). For each failure mode/cause/effect combination a safety score is established.

All of these safety scores had to be above the threshold (5) for the system to be declared safe enough.

The analysis showed that for most of the failure mode/cause/effect combinations the system was safe enough. There were some exceptions, mainly concerning the vehicle doors. In the FMECA table a number of recommendations for improvements were made and if these will have been implemented the system will meet the safety requirements that were set out. The analysis will be presented to the Italian Ministry of Transport for further processing.

2.6.2 Learning points and improvements

In general the attendants were satisfied with the procedure and the way it was carried out. Although the procedure is time consuming (the total number of analysis sessions was 29. One session is typically 4 hours) it was thought to be thorough and complete.

Points of attention:

- 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.
- The analysis process is an intensive operation. Experience, also from earlier analyses shows that 4 hours is a maximum for an effective session. After 4 hours the average attendant tends to loose focus and sharpness.
- 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.
- It is recommended to ask attendants to switch off telephones and to concentrate fully on the analysis.
- 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.
- During the process the sheets that were used were improved to make them more practical. (see annex 2). A numbering system for inputs; outputs and functions was introduced, so that it became easier to make references.
- A coding and colouring method was introduced to clearly mark failure modes, issues that needed more attention and non compliances.
- The most difficult part of the analysis is establishing the likelihood that a failure will occur. Likelihoods are expressed as once in every 10, or 100, or 1000 years and it is difficult, when hard data about failure rates is missing to make reasonable decisions about failure rates. Therefore the single likelihood column that existed in the original procedure was split in one for the likelihood of the causes and one for the likelihood of the effects. In addition a simple system of rules of thumb was developed (see 2.5.5.3) for the likelihoods of the causes. The likelihoods of the effects appear to be easier to analyse. In all cases where an analysis of the likelihood of the effect was made, a report about the analysis was either included in the FMECA table or laid down in an appendix.

- Uniform terminology for causes and effects was introduced, so as to avoid confusion when the same effect is named differently throughout the analysis.

Most of the learning points described above are of a practical nature. The basis of the method remained unchanged. Further analyses in future will probably give rise to more improvements.

3 Conclusions

This report describes the work carried out in Work Package 2.5 as a part of Sub Project 2 of the CityMobil project. The report describes certification procedures for automated systems. These certification procedures are meant for 2 major purposes:

1. As a final certification instrument to establish whether or not an automated transport system meets the requirements that were established with respect to safety.
2. As a method to analyse the safety of a system during the development phases of an automated transport system, in order to be able to make modifications and take safety related issues into account in an early stage of the development process.

The method is based on well established analysis methods (FMECA) which were adapted to suit the purpose of this procedure. The procedure itself is based on recommendations that were formulated in other projects [1, 2, and 3] and which were updated in accordance with the latest developments in Europe. The procedure was evaluated using the people mover system developed for the CityMobil Rome demonstration as a case. Some improvements were made to the method based on the experiences gained during the evaluation, but these were all minor adaptations of a practical nature. The evaluation was successful and the Rome people mover met the requirements set out in the beginning of the analysis process. The next step is that the results of the analysis will be presented to the Italian Ministry of Transport. The Ministry will make a decision whether the system can be approved on the basis of the evaluation report.

4 References

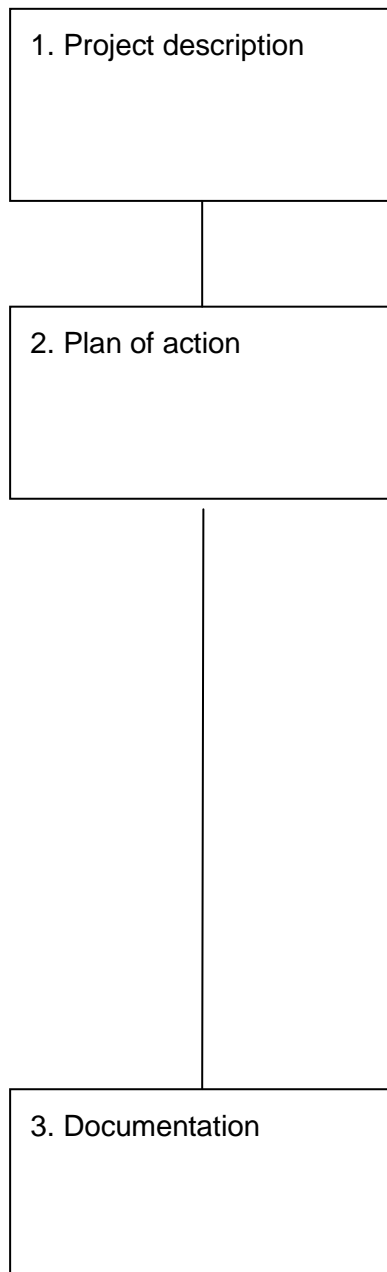
- [1] CyberCars project: Deliverable D.6.1: Safety standards for Cybercars Part 1: Existing standards and guidelines. J.J. Uwland and J.P. van Dijke. September 2002
- [2] CyberCars project: Deliverable D.6.2: Safety standards for Cybercars Part 2: Recommendations for certification procedures. J.P. van Dijke and J.J. Uwland. June 2004
- [3] CyberMove project: Deliverable 3.2: Safe sites and systems: J.P. van Dijke and M.M. Janse. October 2004.
- [4] Code of Practice for the design and evaluation of ADA systems. RESPONSE III project. October 2006
- [5] IEC 61508: Functional Safety of electrical/electronic/programmable electronic safety-related systems; IEC 1998
- [6] System Safety Analysis Handbook; System Safety Society.
- [7] EEE Software Engineering Standards; IEEE 1999
- [8] ISO 26262: Road vehicles - Functional Safety

Annexes

Annex 1 : Flow diagram FMECA procedure

Discuss and complete steps 1, 2 and 3 in a preparatory conversation with the principal
Carry out step 4 in close cooperation with the principal.

A. General preparation



Discuss with the principal and register:

1. Name of the project
2. Description (maximum 10 lines)
3. Name of the principal
4. Date of the analysis
5. Name of the project leader
6. Name of the project leader/contact of the principal

Discuss and register the action plan with the principal:

1. Overall system borders
Which systems are considered (what is inside and what is outside the system boundaries)
 2. System definition and function analysis
Describe the method in 10 lines
 3. Description FMECA analysis Type of FMECA (is it a concept, design or certification analysis.
Estimate the number of subsystems;
Estimate the number of sessions; timing; names of the participants
 4. Documentation Which documents are going to be used How to register documents
 5. Provisional planning
 6. Accepted safety level
Discuss and agree on which accepted safety level will be used
 7. Agree on and sign off on the plan of action
1. List of available documentation and drawings;
Give each document a unique number
Register doc. number, date of receipt and source
The list is a controlled document.
Organize version control
 2. Only registered documents are used in the analysis
 3. All new information is numbered and registered also sketches and notes

4. Verbal information from the principal is put on paper, authorized, numbered and added to the list
5. In case of software: register which design rules/principles have been applied
6. Assess whether or not there is sufficient information to carry out an analysis. If not the principal is asked to provide additional documentation

B. Execution: Go through the steps for every separate sub-system that is analysed

4. System definition &
function analysis

1. Name the system to be analysed and establish the system boundaries. Do this by establishing which components/subsystems are inside the system boundaries and which are outside but do have interactions with the system inside the system boundaries.
2. Subdivide the systems within the system boundaries further on the basis of pragmatic choices and repeat step 1 for each of these sub-systems. Choose the subsystems in such a way that they will probably coincide with the subsystems on which an FMECA will be carried out.
3. Indicate which interactions exist between the (sub)system to be analysed and the outside world (everything outside the system boundary).
4. Establish on practical grounds on which (sub)systems analyses will be performed and which systems need to be subdivided further.
5. Establish the inputs and outputs entering and exiting each (sub)system. Distinguish between the following categories: information; matter; people; electric currents; radiation.
6. Establish the terminator (input/output point) through which the media named under 5 enter or exit the (sub)system.
7. Carry out a function analysis. Functions are defined as every relation between an output and an input and in some cases between output and internal sources.
8. Each system has one or more functions. The failure modes on which the FMECA is based are defined as deviations from those functions

5. FMECA sessions

1. All Information that becomes available during the analysis is registered and added to the list of documents.
2. In preparation of the FMECA sessions the list with functions as established above is included in the Excel file.
3. To be carried out for each (sub)system:
 1. Establish the failure modes for each function
 2. Determine all causes of each failure mode
 3. Establish the most serious effect for each failure mode/cause combination
 4. Establish the severity [S] for each combination
 5. Establish the likelihood of the cause [Lcause] for each combination
 6. Establish the likelihood of the effect (Leffect) for each combination
 7. Establish the resulting likelihood and establish the safety score for that failure mode/cause/effect combination using the table. If the safety score is equal to or lower than the safety criterion, no further analysis is needed.
 8. Establish whether or not safeguards exist. Safeguards are functions that come into action when other systems fail. Safeguards decrease the likelihood of a failure or decrease the effect.
 9. Establish the resulting severity and likelihood
 10. Establish the final safety score for the combination
 11. Add recommendations if necessary
 12. Add relevant comments.

6. Reporting

The report includes:

1. A summary
2. Contents
3. Introduction
4. The project description
5. An action plan
6. The system definition
7. The relevant results
(safe scores below the accepted safety level)
8. Conclusions
9. Recommendations

Appendices:

- a. List of documents
- b. All session reports
- b. All of the sheets made during the procedure

Annex 2: Various sheets, used in the procedure
REPORT FMECA SESSION

Principal	
Date	
Session no.	

Contributors

Name	Company	Remarks

Work done during the session

Activity

Homework

Name	Action

Documents

Number	Name

Remarks

Company			
Name			
Date			
Signature			

SYSTEM BOUNDARIES

SYSTEM:	
----------------	--

Sub-systems and components outside the system boundary that interact with the system

1
2
3
4
5
6
7
8
9
10
11
12

