SAFETY STANDARDS FOR CYBERCARS

Part 1: Existing standards and guidelines

Deliverable Type: Report
Number: D 6.1
Nature: Final version
Contractual Date of Delivery: 01/07/2002
Actual Date of Delivery:15/09/2002
Task WP: WP 6

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

Name of the institute: TNO Automotive
Address: P.O. Box 6033
2600 JA Delft
The Netherlands

Abstract:

This report contains the results of a survey of existing safety standards and guidelines that could be relevant for the future safety standards and guidelines that will govern the approval of Cybernetic Transport Systems (CyberCars). The report focuses on the certification requirements for the vehicles as such. Requirements for the environment in which the vehicles will have to operate are subject of the CyberMove project. The results of the survey will be analysed in the second task of WP 6 of the CyberCars project and will serve as a basis for a proposal for certification procedures for Cybercars.

2 Annexes contain an overview of the relevant standards found and descriptions of the most relevant standards and guidelines.

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 the cities.

The report contains the first deliverable in Workpackage 6: Report on existing guidelines. It describes the results of a survey of existing standards and guidelines that could be relevant for the future certification of CyberCars. The report focuses on the certification requirements for the vehicles as such. Requirements for the environment in which the vehicles will have to operate are subject of an alternative project CyberMove.

The first step was an inventory of relevant existing standards, guidelines and developments. In the second step attention was paid to the differences in the various European countries. The partners were requested to give information on the current practises for approval of CyberCars.

The results of the work are included in 3 annexes to the report. Annex 1 is a schematic overview of relevant existing guidelines. Annex 2 describes the current practises for the approval of CyberCar systems and annex 3 contains characterisations of a number of relevant standards and guidelines.

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 are Cybernetic Cars for a new transportation system in the cities. CyberCar systems aim to improve mobility in the 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 CyberCar project focuses on the testing, analysis and improvement of existing techniques, but also pays attention to existing legal constraints that could hamper the diffusion of CyberCar systems in the cities. Workpackage 6 of the CyberCar project therefore addresses the certification guidelines that are needed to certify that systems are safe.

This report contains the first deliverable in Workpackage 6: Report on existing guidelines. It describes the results of a survey of existing standards and guidelines that could be relevant for the future certification of CyberCars. The report focuses on the certification requirements for the vehicles as such. Requirements for the environment in which the vehicles will have to operate are subject of an alternative project CyberMove.

In the next phase in Workpackage 6, the results of the survey will be analysed and will serve as a basis for a proposal for certification procedures for CyberCars

1.2 Objectives

The objectives for this deliverable are to obtain insight in the standards and guidelines that govern the use of CyberCars today. The report should give an overview into the requirements based on present formal standards and guidelines that authorities in Europe could require system operators to meet.

1.3 Method

1.3.1 Inventory of standards

The first step was an inventory of relevant existing standards, guidelines and developments. The search concentrated on five relevant areas:

- Specific standards for automatic guided vehicles
- Standards for road transport
- Standards for rail transport
- Systems safety standards
- Software standards

Rail transport was included because of the possible comparison between rail vehicles (mechanically guided vehicles) and CyberCars (non-mechanically guided vehicles). Systems safety standards were included because of the similarity between complex electronic and computer controlled systems and CyberCars. Software standards are included because software is one of the most important 'component' in each CyberCar system and the safety of CyberCars therefore depends heavily on the reliability of the software.

This report does not contain an analysis of the standards that were found, nor a viewpoint on whether or not the standards could be applicable. That all will be part of the second step, that will result in recommendations for certification procedures for CyberCars.

In this survey a number of restrictions has been observed and a number of subjects received particular attention.
The standards and guidelines that have been studied mainly focus on safety requirements. Requirements for the use and maintainability of systems have not been made part of the work. Furthermore only standards for vehicles that move on wheels were part of the survey. This means that we have not looked at automatic guided vehicles for water and air transport, although sometimes, where appropriate reference is made to standards in these fields.

Standards can be international standards, recognised and observed in more than one country or they can be national standards, only important at national level. In this report national standards have only been included when they are especially relevant to the subject. National standards that are only available in the language of the country concerned, will have been missed in this work, unless such a standard was brought to our attention by a representative of that country.

The world of automatic guided vehicles extends far beyond that of CyberCars. Where CyberCars are vehicles for personalised transport in urban environments, automatic guided vehicles also have uses in mass and intermediate mass transport (metro's and people movers) and furthermore in the transport of goods over shorter and longer distances. In this report attention is also paid to the standards that concern these applications.

1.3.2 Inventory of current practises

In the second step attention was paid to the differences in the various European countries. The partners were requested to give information on the current practises for approval of CyberCars.

1.4 Standards, guidelines and laws.

In principle everybody is free to follow the requirements set out in standards and guidelines. In principle there is no obligation to meet these requirements. Standards and guidelines only become obligatory when laws refer to those standards and guidelines.

Basically standards and guidelines are documents in which requirements for products and processes are given, for instance with maintaining a certain quality or safety level as the objective. Standards are being published by organisations that have a certain interest in maintaining quality of safety standards. These organisations can be authorities, societies of producers or groups of experts in the same discipline.

Laws are usually made on a national level. This means that in different countries different requirements for the same product can be valid. In recent years a lot of effort has been invested in harmonising standards throughout Europe and even on a world-wide scale. Taking away trade barriers is an important driving factor for harmonisation of standards and guidelines. Harmonised standards ease the comparison of products and enable a fair comparison of products with regard to quality and safety.

In the European Union harmonisation is making rapid progress in some fields, while it is still in its infant stage on other fields. For instance, in the whole of the Union the requirements for road vehicles are the same and a road vehicle that is approved for use on the public roads in one of the countries of the Union, is automatically approved for use in all of the countries. The requirements for road vehicles are laid down in European Directives. On the basis of European treaties these Directives are part of the national laws of all of the countries of the union.

In rail traffic matters have not progressed that far. At present there is only one Directive, with requirements for high speed trains (that are often border crossing). With the exception of this directive, there are no international agreements about harmonised requirements for rail vehicles. This means that each country in the Union can and does make its own laws and standards. However, there are certain standards that are being observed on a voluntary basis by a growing number of countries.

2. STANDARDS AND GUIDELINES

2.1 General

In the search for relevant standards, at first a definition of what is relevant needed to be made. For the purpose of this work CyberCars were described as follows:

CyberCars are:

- Automatic Guided Vehicles
- Surface vehicles on wheels
- Complex electronic and computer controlled systems

Because CyberCars fall into that category, special attention has been paid to fully automatic guided vehicles. However, systems that are partially guided, like the so-called ADA (Advanced Driver Assistance) systems are much closer to large scale market introduction. Examples are 'adaptive cruise control' and 'lane departure warning systems'. The most important difference between these systems and CyberCars is that in the ADA systems there always is a driver present who will take responsibility of the vehicle. When, in future, these systems evolve into systems where no active contribution of a driver is required anymore, the systems and also the standards and requirements will come very close to those for fully automatic guided vehicles.

2.2 Specific standards for automatic guided vehicles

The search resulted in only a few existing dedicated standards for fully automatic guided vehicles. When no dedicated standards are available vehicles are subject to the requirements of more general standards, like the Machinery Directive or the Directives for road vehicles.

CEN EN 1525 — In Europe CEN EN 1525 is used. This standard contains safety guidelines for industrial driverless trucks and their systems.

APM standards	In the US the Automated People Mover Standards (ASCE 21-96; ASCE 21-98 and ASCE 21-00) exist. These standards establish the minimum set of requirements necessary to achieve an acceptable level of safety and performance for an Automated People Mover (APM) system. The standards consist of three parts: Part 1: Operating Environment; Safety; System dependability; ATC; Audio and Video Part 2: Vehicles; propulsion and braking Part 3: Electrical; stations; guideways The APM standards are based on the contents of MIL-STD-882C
BOStrab	In Germany the BOStrab standard with specific guidelines for streetcars is used. There is a separate annex that describes guidelines for operation without drivers. Although this standard is only available in the German Language it is widely used outside Germany.

2.3 Specific standards for surface vehicles on wheels

If we look at surface vehicles on wheels there are several sets of laws that can be relevant, depending on the application of the vehicle. An important distinction is whether the vehicle makes use of the public road, or whether it is driving on private property. It is also important to know whether the vehicle is mechanically guided. For the purpose of this investigation, surface vehicles on wheels can be divided in the following 4 categories:

- Vehicles for use on the public road
- Vehicles for use on private grounds
- Rail vehicles (mechanically guided surface vehicles) for use on public roads
- Rail vehicles for use on private grounds

2.3.1 Vehicles for use on public roads

Examples: Cars, motor cycles; trucks busses, trolley buses, etcetera

In Europe vehicles for the public road have to comply with the requirements of Directives 70/156/EEC and 92/61/EEC. These directives contain requirements for the approval of motor vehicles. The Directives each contain references to many detailed directives, that are all part of the approval system. There are different requirements for different categories of vehicles.
The Economic Commission for Europe (ECE), a body of the United Nations, issues ECE-standards. Many European countries that are not part of the European Union have included ECE-standards in their law systems. The ECE-regulations exist parallel to and sometimes additional to the EEC Directives. Contrary to the EEC Directives where all countries of the European Union are obliged by law to accept the requirements, ECE regulations can be accepted by all European countries on a voluntary basis.

CyberCars that are going to be used on private roads will eventually have to meet the requirements that all present road vehicles have to fulfil. The present requirements have to change, however, to allow CyberCars on public roads, for one of the implicit requirements of the present regulations is that a driver always has to be in control of the vehicle. This is not only important for safety reasons, but also from a liability point of view. In Europe, if a car is involved in an accident and the accident is not caused by gross negligence of the manufacturer, the driver is liable and the manufacturer is not held responsible. In case of CyberCars, where there is no driver, it is unclear where the liability lies. Fingers will point to the manufacturer or the operator when an accident occurs. This is a problem that could hamper the development of CyberCars, but also the development of ADA-systems (Advanced Driver Assistance) that take part of the control over the vehicle away from the driver. Since ADA systems from a technical point of view are very close to market introduction, this problem is addressed by the European automobile industry. In another European project: RESPONSE II, a code of practice for the development and manufacturing of ADA systems is being developed to enable ADA systems to be introduced.

2.3.2 Vehicles for use on private grounds

Examples: Cars; industrial vehicles

In this category we see a variety of vehicles that are used for transport of people and goods in factories; on industrial premises and in attraction parks. The people movers that are operational at Schiphol Airport and in Capelle aan de IJssel in The Netherlands also fall into this category. Both systems operate on private grounds, although the people mover in Capelle has one crossing with a public road.

There are no specific guidelines for this category of vehicles. Some of them are subject to the Machinery Directive (Directive 98/37/EEC), that contains fundamental requirements on the field of safety and health, and a list of more specific requirements for specific types of machines. The Machinery Directive, however, has a lot of exclusions:

- Means of transport, i.e. vehicles and their trailers intended solely for transporting passengers by air or on road, rail or water networks, as well as means of transport in so far as such means are designed for transporting goods by air, on public road or rail networks or on water. Vehicles used in the mineral extraction industry shall not be excluded.
- special equipment for use in fairgrounds and/or amusement parks.

Means of transport for people and goods on non-public roads are subject to the requirements of the Machinery Directive. This is also true for CyberCars running on private roads. Special (transport) equipment for use in fairgrounds is excluded, however. This is why the Floriade people mover was certified on the basis of a Dutch national Directive regarding the safety of attractions in an amusement park and not on the basis of the Machinery Directive.

For most machinery the Directive allows a system of self certification. The manufacturer declares that his machine complies with the requirements of the Machinery Directive and affixes the obligatory CE-sign to the equipment. For certain machines a government approved homologation service has to test and homologate the system. The Directive includes a list of such machinery. Means of transport, however, are not on this list.

2.3.3 Rail Vehicles for use on public roads

Examples: streetcars

Streetcars or trams are widely used in the inner cities in Europe. They often make use of the same infrastructure as other road traffic does and they do have to meet the traffic laws that govern the use of the public road.

There are no harmonised standards for streetcars and metro's. Since these systems are also excluded from the Machinery Directive, they are only subject to local requirements of local authorities. This certainly is in great contrast with the very detailed regulations that exist for cars, which in some cases use the same infrastructure as streetcars do. Only in Germany there is a specific regulation, BOStrab, that is mentioned in this report because it is also used outside Germany.

2.3.4 Rail Vehicles for use on private grounds

Examples: Trains; metro's

Most of the presently known Automatic Guided Vehicle systems fall into this category. In most cases they are automatic metro systems like those that operate in Paris, but also in Chicago and in several airports around the world. The Detroit People Mover also falls into this category. Strictly spoken, cable cars and elevators also fall into this category.

It is remarkable that in contradiction with other modes of transport, standards for rail traffic are hardly harmonised on a European level. The only European Directive is Directive 96/84/EEC, concerning high speed trains. For other rail traffic standards only exist on a national level. In spite of attempts to harmonise rail traffic there is still a large variety of voltages; track widths and safety systems.

The limitations that mechanical guidance offer make these systems explicitly suited for automatic guidance. The mechanical guidance decides on the route so that navigation is easy or superfluous and safety risks can be controlled rather easily.

2.4 Specific standards for electronic and computer controlled systems

One of the most important differences between CyberCars and traditional vehicles is the major role that electronics and software play in CyberCars. In and outside the world of transport the role of autonomous and non-autonomous electronic control systems is growing. This growth of importance leads to an increased impact on the safety of systems. In fully automatic guided vehicles the electronic control system and the software are important safety critical components. Because the electronic control system influences and is influenced by almost all subsystems (propulsion, braking, steering) it is increasingly difficult to see these subsystems as separate units. The subsystems are increasingly part of a complete system and, in safety assessments they must be seen as parts of complete systems. This means that in future, the focus will shift more and more from component safety to system safety.

Until now the transport world has not paid much attention to system safety and the safety of automated control systems. In the aircraft industry and the process industry system analysis is standard procedure. There are a number of standards in the field of system safety. These standards are not often referred to in binding laws, but they are gaining in importance. These standards are often based on the system life-cycle and classify systems in safety classes or safety integrity levels. The most relevant examples are:

IEC 61508: Functional safety of electrical/electronic/programmable electronic safety related systems. IEC 61508 is a generic standard, aiming at the whole width of application areas. Specific sector-oriented standards can be derived form this standard. The standard particularly addresses systems of which failures can have consequences for persons or the environment; it is less suited for establishing economic damage. IEC 61508 is a European standard and it is mainly used in Europe.

MIL-STD-882C
Safety Systems Program Requirements. Originally an American military standard that also found wide acceptance in the civil world. Comparable to IEC 61508. Both standards are often referenced in the literature.

EN 50126
Railway Applications: The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). A European standard, especially developed for the rail world. Defines safety integrity levels just like IEC 61508 and MIL-STD-882C

Software Standards
Electronic control systems are almost always dependent on software. In the future, CyberCars software will be an important, if not the most important safety-critical component.
The integrity of the software used shall be decisive for the safety of the complete system. Therefore software should be subject to high reliability and safety demands. A problem that immediately presents itself is that even software for simple control systems is already very complex, which makes the evaluation of software difficult. Evaluation of software safety can be carried out through tests only up to a certain limit In a complex system it is often impossible to check all possible failure modes through testing. In the existing standards for software, focus is therefore on the quality of software engineering, rather than on testing. This is based on the premises that the reliability of software will be higher, when this software is developed according to strict guidelines. Certification of software and software controlled systems will therefore probably be carried out more and more on a proven reliable and robust design and less on the basis of tests. The existing standards and guidelines are based on that principle and on the software lifecycle. This connects them with the system safety standards mentioned above.

IEEE standards
IEEE Software Engineering Standards consist of 4 volumes with about 50 different standards on the following fields:
- Customer and terminology standards
- Process standards
- Product Standards
- Resource and technique standards

MISRA Guidelines
Development guidelines for vehicle based software. The MISRA Guidelines are sector-specific guidelines for software development, in which reference is made to IEC 61508. They are not software engineering standards, like the IEEE standards, to which also reference is made.

DO 178-B
Software considerations in airborne systems and equipment certification. Is used by the FAA (Federal Aviation Authority) to certify software. The standard provides guidelines for the evaluation of the safety of software for aircraft and related equipment

For CyberCars especially the MISRA Guidelines and the IEEE standards seem important. The MISRA guidelines because they concern (road)vehicles and the IEEE standards because they are widely used generic guidelines.

2.5 Developments

The complexity of automatic guided systems forces lawmakers and developers of standards in the direction of system level. This is visible in various relevant sectors

2.5.1 Road traffic

Big steps are taken in the development of ADA systems. There are, however, two important restrictions for the approval of these systems:

- The law requires that the driver must be in control of the vehicle at all times. If a system takes over control of the vehicle partly or completely and an accident happens, it is unclear who is responsible. When a driver is in control this driver is responsible, unless the accident is caused by a technical failure that is caused by obvious negligence of the manufacturer or the authorities. However, when the driver is not in control, he cannot be held responsible and in present laws the responsibility shifts to the manufacturer. Until this liability issue is solved, the introduction of ADA systems that take over control from the driver is unlikely.
- Present standards do not allow electronic steering systems. This means that drive-by-wire and brake-by-wire systems cannot be used in cars for the public road. However, 'X-by-wire' systems are a precondition for advanced ADA systems, where the vehicle controller, by means of software influences the behaviour of the car. X-by-wire systems also offer other advantages. For instance the classic steering column, that is a source of danger in crashes, can be replaced by an electronic system, which does not have rigid components that can intrude into the occupant space in a crash. At present progress is being made in allowing X-by-wire systems in road vehicles. Changes to the present regulations have been proposed, that will allow X-by-wire systems, if these meet additional requirements. Among these requirements is a systems safety evaluation by means of FMEA or FTA methods.

Within the framework of a European project RESPONSE II, manufacturers, suppliers, lawyers and research institutes are presently looking for solutions. The goal is to present requirements for a code of practice for the development of ADA systems within a few years. Since the technical solutions that are being implemented in advanced ADA systems are expected to be much like those for CyberCars the developments in the CyberCar project can be interesting for RESPONSE II and vice versa.

There are also developments in the field of automatic guided vehicles for the public road. In Eindhoven, in The Netherlands, an experiment with a new segmented bus will soon start. The bus has a driver on board, but will in principle be able to drive automatically. In Clermont-Ferrand, in France a similar experiment has started in 2001. The French bus, called CIVIS, has been approved for automatic driving on the basis of a risk analysis and tests. At first, the bus had to meet the requirements for buses. Later the responsible authorities decided that the requirements for guided transport should be observed. Since there are no guidelines for guided transport on rubber tyres at this moment, the responsible authorities have decided to evaluate the vehicle on the basis of CEN EN 50126 and 50128.

2.5.2 Rail traffic

In the rail world the system approach is clearly gaining ground. The European standard CEN EN 50126 describes a system approach for the evaluation of Reliability, Availability, Maintainability and Safety (RAMS) of rail vehicles. In a policy document of the Dutch Government the government view on the field of rail traffic is given. The establishment of risk levels and the evaluation of the safety of systems on the basis of risk calculation is central in this document. The document will eventually lead to a new Dutch rail traffic law. As already mentioned; initiatives on a European level are mainly restricted to high speed trains.

2.5.3 Machinery Directive

In May 2001 a proposal for a modification of the Machinery Directive has been presented to the European parliament. The main modification, related to the contents of this report is that means of transport, including trailers are excluded from the guidelines. The consequence is that, when this modification is approved CyberCars will not be subject to the Machinery Directive any more.

An important development that is being confirmed by the results of the inventarisation, is the increasing importance of system analysis on system level instead of on component level. This development is mainly caused by the fact that components of vehicles and vehicle systems increasingly are part of an integrated unit. That makes it more difficult to see and test a component as a separate entity. The safety and reliability of such a component depends on a large number of factors outside the component itself.

2.5.4 System safety

Central in the analysis on system level is the life-cycle approach. Traditionally the safety of a product is evaluated by means of tests of the completed system. In the life cycle approach safety is considered in all phases of the product life-cycle; form the first concept stage through the design and development stages and the operational stage to the disassembly and scrapping of the product. When safety and reliability are issues already in the concept stage, so that responsible decisions can be made for the design and development phases, the chance that a product will be safe will increase. in principle it is possible to decide whether or not a product will be safe by evaluating its design process. In that case, safety is not any more an absolute factor, derived from intensive testing, but a relative factor, expressing the chance that a design might fail.

The increase of the importance of system analysis is evident in the growing importance of standards like IEC 61508 in Europe and MIL-STD-882C in the US, but also of the European Standard EN 50126 for rail traffic. The system approach also offers solutions for the safety evaluation of software. If software is developed according to certain rules, in which during the whole development and design process safety has been a factor, the chance will be smaller that software will have intrinsic safety problems.

In the field of ADA systems the same trend can be seen. In the European project RESPONSE II it is concluded that the component approach will increasingly fail to provide solutions and that a process or system approach is necessary. The industry meanwhile has also set the first steps toward a system approach. Delphi Automotive Systems works on drive-by-wire systems. The safety-evaluation of these systems is based on MIL-STD-882C.

2.6 Current practises

The results of the questions to the partners in the CyberCar project as to the current practises for approval of CyberCars did give varying results. The only constant was that it is unclear what exactly the legal requirements for CyberCar systems are. Authorities are wrestling with the matter as well as the manufacturers and other parties involved. This shows again that there is a real need for formal certification procedures and guidelines, that can provide a reference for all parties involved with CyberCar systems. Annex 2 has an overview of the response on the questions asked to the partners.

2.7 Discussion

2.7.1 Present standards and laws

Annex 1 contains a schematic overview of the inventory described in this chapter. The overviews shows once more 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 new Machine Directive indeed excludes all means of transport

2.7.2 What is missing in the present situation?

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 limited reach.

2.7.3 What is missing for Automatic guided Vehicles?

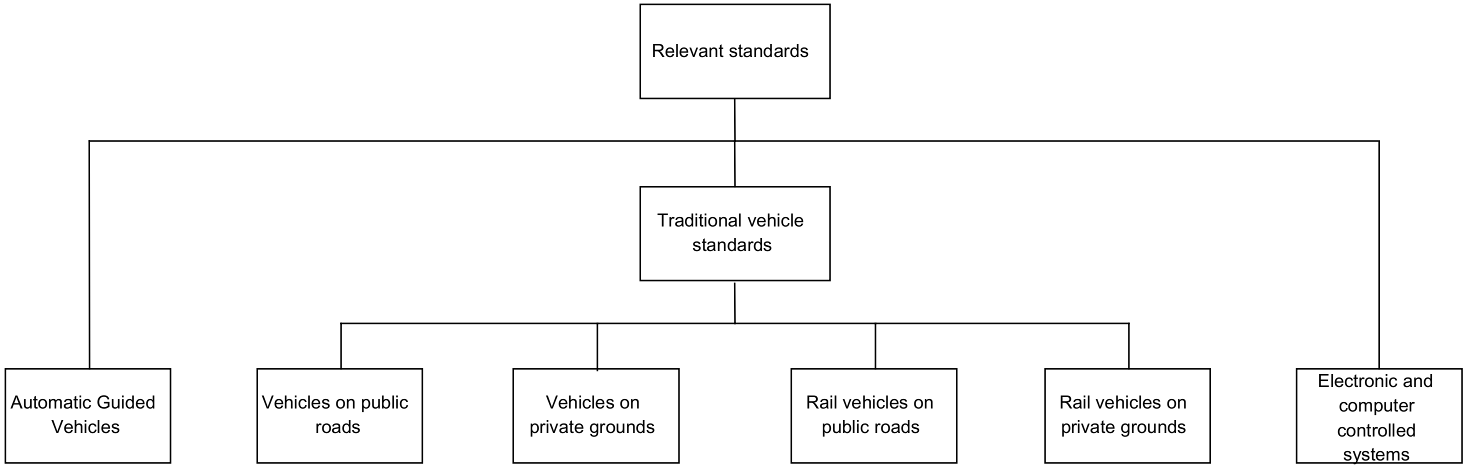
The existing CyberCars and those that are being developed, depending on the environment they are used in, are subject to the same laws and standards as traditional vehicles. In addition to the limitations mentioned in par. 1.4 these existing laws and standards have other limitations, with respect to CyberCars.

- 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 requirements for the safety of software. Although there are many standards

in the field of software engineering and software development, these are at present not part of the present 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. CyberCars 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 are able 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.

ANNEX 1: OVERVIEW OF STANDARDS


Relevant standards
Traditional vehicle standards
Automatic Guided Vehicles
Vehicles on public roads
Vehicles on private grounds
Rail vehicles on public roads
Rail vehicles on private grounds
Electronic and computer controlled systems

Examples of vehicles		Cars, motor cycles Trucks, buses	Cars, industrial vehicles	streetcars	trains, metro's	
Examples of standards						
European standards	CEN 1525	Directive 70/156/EEC Directive 92/61/EEC	Directive 98/37/EEC			IEC 61508 MISRA guidelines EN 50126 EN 1050
National standards	BOStrab operation without driver			BOStrab		
US standards	ASCE 21 APM standards	FMVSS standards				MIL-STD-882c IEEE software eng. standards DO-178b

ANNEX 2: CURRENT PRACTISES FOR THE APPROVAL OF CYBERCARS.

1. Rivium People Mover; The Netherlands

The certification of the first generation of people movers did not raise a special issue. The new track built for the project was declared 'private road', which meant that the vehicles did not have to meet the rules for vehicles on public roads. The company that operates the people mover applied for and received a special waiver under the Public Transport Law to have the system function as a public transport system. Since the law was declared applicable to the system liability was arranged in line with a 'normal' bus system

2. Serpentine; Lausanne, Switzerland

The Serpentine system should have been in operation in 2001. Already in 1990 a request for a licence to operate the system was made, at which time the system was classified as a 'railway' system. At the time the authorisation for the first experiments was applied for, the system was classified as a 'trolley bus'. The infrastructure (the patented magnetoglisseur system) is subject to the railway regulations and the vehicles are subject to road traffic regulations. This last requirement makes the system subject to the European Agreements (signed by Switzerland) that require a driver to be present in a vehicle.

3. Various Cycab systems; France

Drive-by-wire systems like CyberCars are not (yet) allowed on public roads in France (and elsewhere in the European Union). On private roads CyberCars are considered machines. Some CyberCar systems produced and supplied by Robosoft have been audited by an independent organisation (APAVE) to show compliance with the Machinery Directive (98/37/EEC) and the European EMC (Electromagnetic Compatibility) and low voltage requirements.

4. RUF system; Denmark

The developments are not yet such that formal approval has to be applied for. However, there are plans to contact the railway authorities in Denmark to discus the concept.

ANNEX 3: CHARACTERISTICS OF A NUMBER OF STANDARDS

The standards listed here are subject to periodic adaptations and modifications The characteristics represent the situation as it was at the time this report was written.

Directive 70/156/EEC; Approval of motor vehicles
Directive 92/61/EEC; Approval of 2- or 3-wheeled motor vehicles

Directive 98/37/EEC; Machinery
EN 1050; Principles for risk analysis

EN 50126; Railway applications. The specification and demonstration of RAMS
BOStrab; Strassenbahn Bau- und Betriebsordnung (Germany: Streetcar building and operating procedures)
BOStrab; Vorläufige Richtlinien für den Fahrbetrieb ohne Fahrzeugfahrer (Germany: Preliminary guidelines for operation without driver)

EN 1525; Safety of industrial trucks; Driverless trucks and their systems
ASCE 21-96 and 21-98; Automated People Mover Standards

IEC 61508; Functional safety of E/E/PE systems

MISRA; Development guidelines for vehicle based software
DO 178-B; Software considerations in airborne systems and equipment certification
IEE Guidelines for the documentation of computer software
IEEE Software Engineering Standards

Title	**Directive 70/156/EEC**
Type	European Directive
Issued	1970; with later changes
Status	Compulsory for all member states
Published by	European Community
Description	Council Directive 70/156/EEC of 6 February 1970 on the approximation of the laws of the Member States relating to the type-approval of motor vehicles and their trailers
Concerns	Motor vehicles intended for use on the road, with or without bodywork, having at least four wheels and a maximum design speed exceeding 25 km/h, and its trailers.
Exclusions	Vehicles which run on rails, agricultural tractors and machines
Related to	
Remarks	Contains an overview of the approval requirements for vehicles on 4 and more wheels, with references to EEC Directives with technical requirements.

Title	**Directive 92/61/EEC**
Type	European Directive
Issued	1992; with later changes
Status	Compulsory for all member states
Published by	European Community
Description	Council Directive 92/61/EEC of 30 June 1992 relating to the type-approval of two or three-wheel motor vehicles
Concerns	This Directive applies to all two or three-wheel motor vehicles, twin-wheeled or otherwise, intended to travel on the road, and to the components or separate technical units of such vehicles.
Exclusions	- vehicles with a maximum design speed not exceeding 6 km/h, - vehicles intended for pedestrian control, - vehicles intended for use by the physically handicapped, - vehicles intended for use in competitions, on roads or whatever the terrain, - vehicles already in use before the application date of this Directive, - tractors and machines, used for agricultural or similar purposes, - vehicles designed primarily for off-road leisure use having wheels arranged symmetrically with one wheel at the front of the vehicle and two at the rear.
Related to	
Remarks	Contains an overview of approval requirements for vehicles running on 2 and 3 wheels and for some vehicles running on 4 wheels (quadricycles), with reference to other EEC Directives with technical requirements.

Title	**Machinery Directive 98/37/EEC**
Type	European Directive
Issued	1998
Status	Compulsory for all member states
Published by	EEC
Description	Health and safety requirements for machinery
Concerns	Machinery an assembly of linked parts or components, at least one of which moves, with the appropriate actuators, control and power circuits, etc., joined together for a specific application, in particular for the processing, treatment, moving or packaging of a material, an assembly of machines which, in order to achieve the same end, are arranged and controlled so that they function as an integral whole, interchangeable equipment modifying the function of a machine, which is placed on the market for the purpose of being assembled with a machine or a series of different machines or with a tractor by the operator himself in so far as this equipment is not a spare part or a tool;
Exclusions	among others: means of transport, i.e. vehicles and their trailers intended solely for transporting passengers by air or on road, rail or water networks, as well as means of transport in so far as such means are designed for transporting goods by air, on public road or rail networks or on water. Vehicles used in the mineral extraction industry shall not be excluded, machinery whose only power source is directly applied manual effort, unless it is a machine used for lifting or lowering loads machinery for medical use used in direct contact with patients special equipment for use in fairgrounds and/or amusement parks
Related to	The Directive is a combination of the old Machinery Directive 89/392/EEC and a series of corrigendum's and addendum's. A new Directive is being developed.
Remarks	If a product complies with the requirements:

	• CE mark • EC declaration of compliance Obligations only apply in case the machinery is used in the manner that the manufacturer has intended The manufacturer is obliged to carry out a risk analysis and take account of the results.

Title	**NEN-EN 1050; Principles for risk assessment**
Type	European Standard
Issued	1996
Status	Voluntary standard
Published by	CEN
Description	General principles for the procedure known as risk assessment, to assess the risk during all the phases of the life of the machinery.
Concerns	Detailed instructions on how to comply with one of the requirements from the Machinery Directive
Exclusions	
Related to	98/37/EEC; Machinery Directive
Remarks	• Not a detailed account of methods for risk analysis • Gives a list of hazards, hazardous situations and hazardous events • Gives examples of risk analysis methods: Preliminary hazard analysis What if method FMEA Fault simulation for control systems MOSAR method FTA Delphi technique

Title	**NEN EN 50126**
Type	European Standard
Issued	1999
Status	Voluntary Standard
Published by	CENELEC
Description	Railway applications: The specification and demonstration of Reliability; Availability, Maintainability and Safety (RAMS)
Concerns	All railway applications and all levels of such an application in particular to: • new systems • new systems integrated into existing systems • modifications of existing systems At all relevant phases of the lifecycle of an application For use by railway authorities and the railway support industry
Exclusions	
Related to	• ISO 9000 series • EN 50128 (software; in preparation) • ENV 50129 (electronic systems for signalling • IEC 60500 (Vocabulary) • IEC 61508
Remarks	Reliability; availability, maintainability and safety (RAMS) RAMS is a characteristic of the system's long term operation and is achieved by the application of established engineering concepts, methods, tools and techniques throughout the lifecycle of the system. Technical concepts of safety are based on a knowledge of: • all possible hazards in the system • characteristics of each hazard in terms of its severity of consequences • safety related failures • maintainability of safety related parts • system operation and maintenance of safety related parts Classifies frequency and severity in categories and establishes risk by means of a matrix: conform FMECA principle. Acceptance of risk's via matrix based on 4 safety integrity criteria (intolerable; undesirable; tolerable; negligible)

Title	**BOStrab; Strassenbahn Bau- und Betriebsordnung (Building and operating instructions for streetcars)**
Type	German National Standard
Issued	1987
Status	Compulsory by law
Published by	
Description	Instructions for the construction and operation of streetcars systems according to par 4. of the German law for transport of people (PBeFG)
Concerns	Strassenbahnen (streetcar systems; not being railroads)
Exclusions	
Related to	
Remarks	Extensive traditional requirements for streetcars in the widest sense Also contains instructions for operation without driver (par. 16, 31, 43, 53 en 56) Further expanded on in BOStrab FOF

Title	**BOStrab; Preliminary guidelines for the operation without driver**
Type	German National Standard
Issued	1997
Status	Compulsory by law
Published by	
Description	Specific Instructions for the operation of streetcars without driver
Concerns	Operations when no driver is present On independent tracks (par. 1.2.2 BOStrab): • no crossings • safety space according to BOStrab par. 19 next to each platform • getting in and out of the vehicle on a level plane
Exclusions	
Related to	BOStrab; Strassenbahn Bau- und Betriebsordnung Par: 16, 23, 31, 38, 46, 52, 53, 56
Remarks	Alternative solutions than those incorporated in the guidelines are allowed if an equal level of safety is obtained. Requirements from Bostrab for operations without driver; Reference to BOStrab paragraphs: Par. 16: Unauthorised access to the tracks must be made difficult by the installation of fences or by other means. Fences should be at least 1.2 meter high. The fences or other means must be constructed such that people and articles carried by people cannot get on the track by negligence. Gross negligence or purposeful action is not taken into account. Par. 23: There must be an audio link that enables a priority connection between passengers and (manned) control room. Par. 31: Platforms must have special provisions that minimise the dangers for persons related to moving trains. This requirement is met when: a. For sections of track that can be accessed from the platform an independently operating device should be present that stops the train when persons are present on the track. b. For sections of track that can be accessed from the platform an independently operating device should be present that cuts of the power when there is danger that someone touches the parts that are under power.

	c. The sections of a platform where people may not be present when trains are moving are also recognisable for people with a visual handicap. d. There are emergency switches on platforms that can stop vehicles and switch off power. A, b en c do not have to be met when the platform is separated from the tracks by walls with doors . Furthermore: a. The doors and the open side of the platform should be supervised with video camera's. b. Loudspeakers should be present for messages to travellers form the control room c. There must be an audio link that enables a priority connection between passengers and (manned) control room. Par. 38: The braking system must be provided with sensors that check whether or not braking commands are being executed. Par. 46: See par. 23 Par. 52: Vehicles and autonomous functions should be checked for problemless operation. Par. 53: Regularly (at least once a day and after events) the tracks near platforms should be checked for obstacles. On dangerous locations permanent video control can be required. Par. 56: Along the track provisions should be made so that passengers, when a vehicle stops can be transferred to a safe location at all times. Transfer should start within half an hour after the event FOF3.1: Technical provisions that allow stopping the vehicles from the control room should be available. FOF3.2: Technical provisions that allow cutting off the power from the control room should be available. Furthermore there is a series of requirements relating to vehicle doors, obstacle detection through contact switches and stopping vehicles after derailment

Title	**EN 1525; Safety of industrial trucks; Driverless trucks and their systems**
Type	European Standard
Issued	1997
Status	Voluntary Standard
Published by	CEN
Description	Technical requirements to minimise the dangers related to automated functions of machinery.
Concerns	Self propelled trucks up to and including 10.000 kg capacity and tractors with a drawbar pull up o and including 20.000 N.
Exclusions	• Trucks that are mechanically guided • Trucks that operate in environments that are open to people who are not informed about the dangers Furthermore: • Operation under difficult circumst. (climate; magnetic fields, etc.) • Explosive atmospheres • EMC • Passenger transport • dangerous cargo • Parts that are controlled by hand during operation
Related to	89/392/EEG (old machinery Directive) 98/37/EC
Remarks	Meant to prove compliance with the relevant safety requirements of the Machinery Directive. Contains requirements for: • Braking system • Control during emergencies and maintenance • Speed control • Loading batteries • Stability and steering • Protective devices and warning systems • Emergency stopping • Obstacle detection • Instruction handbook • Markings Verification through: • design check • type testing routine testing

Title	**ASCE 21-96 and ASCE 21-98; Automated People Mover Standards**
Type	
Issued	1997/1999
Status	no legal authority in its own right
Published by	ASCE
Description	Minimum set of requirements necessary to achieve an acceptable level of safety and performance. Includes minimum requirements for the design, construction, operation and maintenance of APM systems. Three parts: Part 1: Operating Environment; Safety; System dependability; ATC; Audio and video. Part 2: Vehicles; propulsion and braking Part 3: Electrical; stations; guideways Part 3 is not (yet) available
Concerns	APM's; a guided transit mode with fully automated operation, featuring vehicles that operate on guideways with exclusive right of way
Exclusions	
Related to	MIL-STD-882C (System Safety)
Remarks	• Requires a System Safety Program and System Safety Plan during the design phase (according to MIL-STD-882C) • Defines safety principles • Fail-safe design Checked redundancy Parallel programming Self checking Numerical assurance (?) • ATC (automatic train control) system has a MTBHE of 10^8 operating hours • ATP (protection) functions Presence detection Separation detection Unintentional motion detection Overspeed protection Overtravel protection Coupling detection Lost signal protection Zero speed detection

	Unscheduled door opening protection Door control protection interlocks Departure interlocks Direction reversal interlocks Propulsion and braking interlocks Guideway switch interlocks • ATO (operation) functions Motion control Programmed station stop Door and dwell time control • ATS (supervision) functions Provides the interface between the system and the central control operator Where there is no operator physically located in the control room information must be transmitted to a person authorised to respond to situations. • Audio and video communication requirements PART 2: • Vehicle requirements Capacity; load; structural design; coupling; suspension and guidance; passenger comport; doors; windows; fire protection; lighting; electrical systems • Propulsion and braking requirements PART 3: • Electrical • Stations • Guideways

Title	**IEC 61508**
Type	European Standard
Issued	1998
Status	Voluntary Standard
Published by	IEC
Description	Functional safety of electrical/electronic/programmable electronic safety-related systems **Part 1**: General requirements Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems **Part 3**: Software requirements **Part 4**: Definitions and abbreviations **Part 5**: Examples of methods for the determination of safety integrity levels Part 6: Guidelines on the application of parts 2 and 3 Part 7: Overview of techniques and measures Parts 1, 3, 4 en 5 already exist; the others still have to follow
Concerns	Electrical/electronic/programmable electronic safety-related systems In particular, this standard • Applies to safety related systems, when one or more of such systems incorporates electric/electronic/programmable electronic devices • id generically based and applicable to all E/E/PE safety related systems irrespective of the application • covers possible hazards caused by failures of the safety functions to be performed by E/E/PE safety related systems, as distinct from hazards arising from the E/E/EP systems itself (for example electric shock) • does not cover E/E/EP systems where - a single E/E/EP system is capable of providing the necessary risk reduction - the required safety integrity of the E/E/EP system is less than that specified for safety integrity level 1 (the lowest safety integrity level in the standard) • is mainly concerned with the E/E/EP safety related systems whose failure could have an impact on the safety of persons and/or the environment; however, it is recognised that the consequences of failure could also have serious economic implications and in such cases this standard could be used to specify any E/E/EP system used for the protection of equipment or product. • uses an overall safety lifecycle model as the technical framework for dealing sytematically with the activities necessary for ensuring the

	functional safety of the E/E/EP safety related systems • does not specify the safety integrity levels required for sector applications (which must be based on detailed information and knowledge of the sector application) • provides general requirements for E/E/EP safety related systems where no application sector standards exist • does not cover the precautions necessary to prevent unauthorised persons damaging, and/or otherwise affecting the functional safety of E/E/EP safety related systems Parts 1, 2, 3 en 4 are basic safety publications, intended to be used by Technical committee's in the preparation of standards that are in agreement with the principles of IEC guide 104 (Guide to the drafting of safety standards) and ISO/IEC guide 51 (guidelines for the inclusion of safety aspects in standards.
Exclusions	
Related to	IEC guide 104 ISO/IEC guide 51
Remarks	

Title	**IEC 61508-1**
Type	European Standard
Issued	1998
Status	Voluntary standard
Published by	IEC
Description	Functional safety of electrical/electronic/programmable electronic safety-related systems **Part 1**: General requirements
Concerns	Electrical/electronic/programmable electronic safety-related systems
Exclusions	
Related to	
Remarks	**Par. 5. Documentation** Requirements for documentation in order to: • specify the necessary information to be documented in order that all phases of the overall E/E/EPS and software safety lifecycles can be effectively performed. • specify the necessary information to be documented in order that the management of functional safety, verification and the functional safety assessment activities can be effectively performed. **Par. 6. Management of functional safety** Requirements for the management of the safety lifecycle process, specifying the responsibilities of the persons, departments. and organisations involved in the process. **Par. 7. Overall safety lifecycle requirements** • Definition of an overall safety lifecycle as a technical framework **Par. 8 Functional safety assessment** Requirements to investigate and arrive at a judgement on the functional safety achieved by the E/E/EP safety related systems.

Title	**IEC 61508-3**
Type	European Standard
Issued	1998
Status	Voluntary standard
Published by	IEC
Description	Functional safety of electrical/electronic/programmable electronic safety-related systems **Part 3**: Software requirements
Concerns	Electrical/electronic/programmable electronic safety-related systems Applies to any software forming part of a safety related system or used to develop a safety related system within the scope of IEC 612508
Exclusions	
Related to	
Remarks	Requires that software safety functions and software SIL levels have been specified **Par. 5 Documentation** See IEC 61508-1, par. 5 **Par. 6. Software quality management system** See IEC 61508-1; par. 6.2 furthermore: • The functional safety planning shall define the strategy for the procurement, development, integration, verification validation and modification of the software, to the extent required by the safety integrity level of the system • Requirements for software configuration management **Par. 7. Software safety lifecycle requirements** Objective: Development of the software structures in well defined phases and activities **Par. 8. Functional safety assessment** See IEC 61508-1

Title	**IEC 61508-4**
Type	European Standard
Issued	1998
Status	Voluntary Standard
Published by	IEC
Description	Functional safety of electrical/electronic/programmable electronic safety-related systems **Part 4**: Definitions and abbreviations
Concerns	Electrical/electronic/programmable electronic safety-related systems
Exclusions	
Related to	
Remarks	

Title	**IEC 61508-5**
Type	European Standard
Issued	1998
Status	Voluntary Standard
Published by	IEC
Description	Functional safety of electrical/electronic/programmable electronic safety-related systems **Part 5**: Examples of methods for the determination of safety integrity levels
Concerns	Electrical/electronic/programmable electronic safety-related systems • Underlying concept of risk and the relation between risk en safety integrity • A number of methods to establish safety integrity levels
Exclusions	
Related to	
Remarks	Annex B: ALARP model Annex C: Determination of SIL: A quantitative method Annex D: Determination of SIL: A qualitative method; risk graph Annex E: Determination of SIL: A qualitative method; hazardous event severity matrix

Title	**MISRA; Development guidelines for vehicle based software**
Type	
Issued	1994
Status	
Published by	MIRA; The Motor Industry Research Association
Description	8 extensive reports and a set of guidelines. Sector-specific guidelines for software development. As such more specific interpretation of IEC 61508-3. The MISRA guidelines, however, are not guidelines for software engineering. For those reference is made to existing standards (IEE; IEEE) • Guidelines to draft contracts and specifications for software • Introduction to automotive software reliability issues • Basis for training requirements • Guidelines for company quality procedures • Basis for assessment • Basis for a future standard
Concerns	
Exclusions	
Related to	ISO 9001 IEC 61508 IEEE software engineering standards IEE documentation guidelines
Remarks	

Title	**DO 178-B, software considerations in airborne systems and equipment certification**
Type	Software standard
Issued	1992
Status	Consensus standard of the aviation community
Published by	RTCA Radio Technical Commission for Aeronautics
Description	'Provides guidance for determining, in a consistent manner and with an acceptable level of confidence, that the software aspects of airborne systems and equipment comply with airworthiness requirements' Is used by FAA to certify computer software
Concerns	Airborne systems
Exclusions	
Related to	EUROCAE ED12B (identical European version) ISO 9001 IEC 61508
Remarks	Defines 5 failure conditions A: Catastrophic failure condition B: Hazardous; severe/major C: Major D: Minor E: No effect Defines 5 software levels; A t/m E • Objectives for software lifecycle processes • Description of activities and design guidelines to reach those objectives • Documentation of the proof that the objectives have been met 3. Software lifecycle 4. Software planning 5. Software development 6. Integral processes software verification software configuration management software quality assurance certification liaison

Title	**IEEE Software Engineering Standards**
Type	IEEE standard
Issued	1999
Status	voluntary standard
Published by	IEEE
Description	
Concerns	Software engineering
Exclusions	
Related to	3 umbrella standards, used as a basis for integration of individual standards: ISO 9001/3 IEEE 1490; Guide to the project management body of knowledge ISO/IEC 12207 Software life cycle processes
Remarks	4 volumes; about 50 standards 1. Customer and terminology standards 2. Process standards 3. Product standards 4. Resource and technique standards Important standards with safety related aspects: IEEE 730 Software quality assurance plans IEEE 828 Software configuration management plans IEEE 829 Software tests documentation IEEE 1012 Software verification and validation IEEE 1228 Software safety plans