UC Berkeley
Research Reports

Title
Safety Assessment of Advanced Vehicle Control and Safety Systems (AVCSS): A Case Study

Permalink
https://escholarship.org/uc/item/3411889p

Authors
Chan, Ching-Yao
Zhang, Wei-Bin
El Koursi, El Miloudi
et al.

Publication Date
2001-10-01

eScholarship.org Powered by the California Digital Library
University of California

CALIFORNIA PATH PROGRAM
INSTITUTE OF TRANSPORTATION STUDIES
UNIVERSITY OF CALIFORNIA, BERKELEY

Safety Assessment of Advanced Vehicle Control and Safety Systems (AVCSS): A Case Study

**Ching-Yao Chan, Wei-Bin Zhang,
El Miloudi El Koursi, Etienne Lemaire**

California PATH Research Report
UCB-ITS-PRR-2001-30

This work was performed as part of the California PATH Program of the University of California, in cooperation with the State of California Business, Transportation, and Housing Agency, Department of Transportation; and the United States Department of Transportation, Federal Highway Administration.

The contents of this report reflect the views of the authors who are responsible for the facts and the accuracy of the data presented herein. The contents do not necessarily reflect the official views or policies of the State of California. This report does not constitute a standard, specification, or regulation.

Report for MOU 395

October 2001

ISSN 1055-1425

SAFETY ASSESSMENT OF ADVANCED VEHICLE CONTROL AND SAFETY SYSTEMS (AVCSS): A CASE STUDY

July 2001

MOU-395 Final Report

Ching-Yao Chan, Wei-Bin Zhang
California PATH Program

El Miloudi El Koursi, Etienne Lemaire
INREST-ESTAS

EXECUTIVE SUMMARY

Advanced Vehicle Control and Safety Systems (AVCSS) involve several safety critical functions such as vehicle longitudinal and lateral control. It is required that the system be able to prevent or mitigate hazardous conditions. The system must be capable of tolerating failures and, when failures are no longer tolerable, be fail-safe. In order to verify the safety of a system, an assessment or evaluation methodology must be developed and implemented prior to implementation of new technologies such that errors in the processes of specification, design, development, and integration can be revealed in order to prevent hazardous consequences. Since some AVCSS technologies will begin to be implemented widely in the next few years (such as adaptive cruise control), timely development of a sound safety assessment/evaluation method for AVCSS is crucial.

INRETS "French Institute of Research in the Transports and Their Safety " and California PATH (Partners for Advanced Transit and Highways) of University of California at Berkeley collaborate, by using a case study related to a significant part of the Advanced Vehicle Control and Safety of Systems (AVCSS), to set up a common approach for developing and validating a safe and operating system. The joint research project aims to create a synergy between INRETS' expertise in safety verification of automated transportation systems and PATH's knowledge in the implementation of AVCSS.

As one example of AVCSS, frontal collision avoidance systems (FCAS) for ground vehicles is used as the target of the current study. The approach to conduct safety assessment should follow the following steps:

(1) Identification of primary problems and safety goals
For example, the goals of FCAS are to minimize the number of frontal collisions and to reduce the severity of accidents.

(2) Identify solutions for the targeted problems
To achieve the safety goals, solutions may come from several approaches, such as increasing the headway of driving, installing collision mitigation devices, or increasing the reliability of vehicles and their parts.

(3) Conduct trade-off studies at the system level

While contemplating on the various solutions, there are usually conflicting demands or consequences that must be balanced. For example, while increasing headway will provide a safer environment for driving, it will lead to a reduced capacity of highways. Even though safety may be a primary objective, it can not be accomplished without sacrificing the operation efficiency. Therefore, trade-off studies must be conducted to determine the implications of adopting a certain design and the sensitivity of selecting operating parameters.

(4) Define safety requirements

Once the trade-off studies are carried out to understand the benefits and risks of various approaches at the system level, safety requirements should be established. These safety requirements are defined at certain acceptable levels, due to the balance of all considerations. For example, the allowable number of accidents for every hour of operation should be kept below a specified number. One complication regarding the definition of safety requirement is the balance of accident severity and frequency. The other is that often only estimates can be provided at this stage without a fully implemented design.

(5) Functional decomposition

In this task, the solution for the targeted problem is decomposed into finer granularity based on its functions. For instance, a FCAS is separated into sensing, processing, warning, and actuation. Each sub-function is then decomposed further into lower layers. The task can be carried out into the lowest physical representation, such as individual sensors or signal processing circuits.

(6) Conduct hazard analysis

With the safety requirements and functional decomposition in place, hazard analysis should be conducted. The contents of hazard analysis include the identification of hazard types, severity, frequency, risk levels, and safety integrity levels. To assist these analysis, probability modeling and analysis, fault tree models (FTM) and failure mode effect and criticality analysis (FMECA) are standard procedures.

(7) Establish safety criteria and safety measures

This step involves the determination of indicators or standards that can be compared to the measurements of the system to judge the safety performance of a prototype or operational system.

This report documents the efforts taken in the joint project and the methodology adopted with the consensus between the researchers at PATH and INRETS. The findings from this project serve as a foundation for conducting a systematic process for safety assessment and certification for AVCSS.

1.0 INTRODUCTION

In recent years, there have been significant developments in advanced vehicle control and safety systems. They range from commercial products, such as adaptive cruise control systems, and experimental programs, such as driver guidance systems for snow plows and studies of automated vehicles conducted by PATH.

AVCSS involves several safety critical functions such as vehicle longitudinal and lateral control. Because of the safety critical nature, it is required that the system be able to prevent or mitigate hazardous conditions that will be otherwise dealt with by human operators. This will require the system to be capable of tolerating failures and, when failures are no longer tolerable, to be fail-safe. In order to verify the safety of a system, an assessment or evaluation methodology must be developed and implemented prior to the implementation of new technologies such that errors in the process of specification, design, development, and integration can be revealed in order to prevent hazardous consequences. Since some AVCSS technologies, such as adaptive cruise control and IVI applications, will begin to be implemented in the next few years, timely development of a sound safety assessment/evaluation method for AVCSS is crucial.

PATH/Caltrans and INRETS have determined that safety analysis and evaluation of AVCSS is one of the critical area for AVCSS development and deployment and propose to conduct a collaborative research to assess safety of AVCSS system. PATH will contribute expertise in vehicle control and failure analysis of AVCSS system while INRETS will provide expertise in safety analysis and assessment. This proposed collaborative work is conducted under the Cooperative Agreement Between Caltrans/California PATH and French DOT/INRETS.

The first phase of the project lasted for 18 months from January 1999 to June 2000. Continual efforts in the second phase will start from July 2000 under a new MOU agreement.

1.1 Participating Organizations and Expertise

INRETS has world-leading expertise in safety verification and certification of operational transportatino ssytems. Although the operating environment are different for rail systems and AVCSS, failure modes and fail-safe modes for railroad control systems and AVCSS resemble. The safety requirements for AVCSS are similar to those for railroad control ssytems – fail-safe and fault tolerance. PATH is interested in learning from INRETS about safety certification methods and in applying them in current and future projects in the National Intelligent Vehcile Initiatives (IVI) program.

INRETS' ESTAS department located at Villeneuve d'Ascq is specializing in safety and operation of automated transport systems and methodologies for safety assessment. ESTAS has played important roles in numerous projects dealing with development of safety standards and safety assessment/certification method for European railways. In a recent project involving ESPRIT III program in the area of Information Processing

Systems supported by European Commission, ESTAS collaborated with several industrial partners (MATRA, Lloyd's Register, DSB Consult TACS and Rover) to develop a generalized assessment method for "Certification and Assessment of Safety-Critical Application Development." ESTAS is interested in collaborating with PATH to adapt these methodologies for safety evaluation of AVCSS.

INRETS LEOST department has been working on technology developments for advanced transportation systems. LEOST is currently involved in "Telematics Systems Dedicated to Improve Safety in Railway Transport and Development of New Exploitation Help (STATUE)," a project conducted by a dozen partners in Europe aiming to develop technologies for improving safety of light rail systems. Many of the aspects of this project are relevant to AVCSS work. One specific area LEOST would like to collaborate with PATH is to develop obstacle detection system using radar and video sensing.

California PATH program has devoted significant efforts in safety design and analysis of AVCSS. This work includes preliminary hazard analysis, tradeoff between safety and efficiency of AVCSS, safety operation strategies of AVCSS, fault tree analysis of AVCSS software, and failure detection and fault tolerance. Because of the potential near-term implementation of some AVCSS elements, including technologies developed by PATH, the safety evaluation/assessment issues need to be addressed. PATH contribute to the project with its accumulative knowledge in AVCSS design and experimental evaluation.

1.2 Areas of Studies

The primary objective of this study is to combine PATH's knowledge on Advanced Vehicle Control and Safety Systems (AVCSS) and INRETS' expertise in safety verification and certification to develop an approach for evaluating and verifying the safety of AVCSS systems. During the course of this project, active exchanges between INRETS and PATH have stimulated significant discussions and exchanges of ideas. Working meetings were held at INRETS (June 1999), at PATH (November, 1999), and then at INRETS again in June 2000. To date, progress was made in all areas defined by the scope of work for the current phase. Although this study references PATH's previous safety studies, it primarily focuses on approaches used by INRETS in developing safety certification methods for railway control systems. The current phase has achieved progress in the following areas:

(1) Preliminary hazard analysis (PHA) and failure mode analysis: INRETS and PATH focused a preliminary hazard analysis on an example AVCSS system. Through this analysis, PATH benefited by learning from INRETS the methods to quantitatively define safety level of the system. This is an important set of parameters for evaluating system safety and is an area in which INRETS has strong expertise.
(2) System architecture: PATH also worked with INRETS to decompose an example AVCSS system (a longitudinal control system) and to develop a digital

architecture for the longitudinal control system. This is another important step toward the development of a method for verification and validation of safety critical systems. PATH and INRETS are working on a method allowing an AVCSS system to be represented by both a logical and physical architecture. The AVCSS system can therefore be broken down into elements so that the safety level of each element can be verifiable through testing or evaluation.

(3) Sensor selection and assessment: PATH and INRETS are also working on sensor selection and assessment of a case study example (a longitudinal control system). For example, we are conducting analysis on ranging/obstacle detection sensors and are expecting to learn the safety characteristics of each type of sensor (laser, microwave) and how to verify them.

(4) Identification of human factor issues: This task is relevant to human factor studies but is conducted from a different angle. In this project, we focus on identification of issues on how to verify the safety level of a Human Machine Interface-HMI (as opposed to HMI design).

In this joint project, PATH and INRETS determined to conduct the analysis through an exemplar case study to understand how INRETS' safety verification and certification methods could be applied to AVCSS. This exercise was critical because of the difference between the railway control system and AVCSS. An example of such difference is the complexity of input and output (i.e., binary input/output for railway control system vs. mostly linear input/output of AVCSS system). One candidate system for such a case study was collision warning/avoidance systems, which possess many typical components of a longitudinal control system. The selected case study served to carry out the exercise of applying INRETS' expertise in safety verification.

During the course of the studies in the past year, it was found that certain tasks deserve further investigation beyond the scope that was defined in the previous proposal. Both organizations believe that it is important to expand the case study in a later phase to include more diversified system characteristics and level of complications. PATH and INRETS therefore will expand the research efforts for the next phase to focus on the following areas

(1) Extension of hazard analysis and system architecture studies to additional areas of AVCSS, including lateral control and other safety critical functions.
(2) Verification method of human-machine interface.
(3) Hardware and software assessment through experimental data collected from real-world operating environment.

1.3 Process of Safety Assessment and Verification

Advanced Vehicle Control and Safety Systems (AVCSS) involve several safety critical functions such as vehicle longitudinal and lateral control. It is required that the system be able to prevent or mitigate hazardous conditions. The system must be capable of tolerating failures and, when failures are no longer tolerable, be fail-safe. In order to verify the safety of a system, an assessment or evaluation methodology must be

developed and implemented prior to implementation of new technologies such that errors in the processes of specification, design, development, and integration can be revealed in order to prevent hazardous consequences.

As one example of AVCSS, frontal collision avoidance systems (FCAS) for ground vehicles is used as the target of the current study. The approach to conduct safety assessment should follow the following steps:

(1) Identification of primary problems and safety goals

For example, the goals of FCAS are to minimize the number of frontal collisions and to reduce the severity of accidents.

(2) Identify solutions for the targeted problems

To achieve the safety goals, solutions may come from several approaches, such as increasing the headway of driving, installing collision mitigation devices, or increasing the reliability of vehicles and their parts.

(3) Conduct trade-off studies at the system level

While contemplating on the various solutions, there are usually conflicting demands or consequences that must be balanced. For example, while increasing headway will provide a safer environment for driving, it will lead to a reduced capacity of highways. Even though safety may be a primary objective, it can not be accomplished without sacrificing the operation efficiency. Therefore, trade-off studies must be conducted to determine the implications of adopting a certain design and the sensitivity of selecting operating parameters.

(4) Define safety requirements

Once the trade-off studies are carried out to understand the benefits and risks of various approaches at the system level, safety requirements should be established. These safety requirements are defined at certain acceptable levels, due to the balance of all considerations. For example, the allowable number of accidents for every hour of operation should be kept below a specified number. One complication regarding the definition of safety requirement is the balance of accident severity and frequency. The other is that often only estimates can be provided at this stage without a fully implemented design.

(5) Functional decomposition

In this task, the solution for the targeted problem is decomposed into finer granularity based on its functions. For instance, a FCAS is separated into sensing, processing, warning, and actuation. Each sub-function is then decomposed further into lower layers. The task can be carried out into the lowest physical representation, such as individual sensors or signal processing circuits.

(6) Conduct hazard analysis

With the safety requirements and functional decomposition in place, hazard analysis should be conducted. The contents of hazard analysis include the identification of hazard types, severity, frequency, risk levels, and safety integrity levels. To assist these analysis, probability modeling and analysis, fault tree models (FTM) and failure mode effect and criticality analysis (FMECA) are standard procedures.

(7) Establish safety criteria and safety measures

This step involves the determination of indicators or standards that can be compared to the measurements of the system to judge the safety performance of a prototype or operational system.

In the following sections, individual areas and associated research efforts are further elaborated.

2.0 Safety Requirement Principles [1]

This section deals with safety requirements, which is the first step of safety evaluation. We have suggested the adaptation of safety principles in the railway (e.g. GAMAB, ALARP and MEM) to the AVCSS system, which serve as the guidelines for setting safety objectives at the global level. The approach widely preferred for modern safety regulations is described as "goal-setting", where the goal to be achieved is described, but not the detailed method of delivery. Hence it usually requires the operator or the manufacturer to assess the risk and then take proportionate action on the risk assessment. The way to formulate it is different from one country to another, but on the whole, the formulations are different facets of the same idea. Three of them are considered in the following: the French principle GAMAB, the English one ALARP and the German one MEM.

2.1 GAMAB principle

A comparison with other comparable systems that provide the equivalent services; This is equivalent to the viewpoint of GAMAB = Globalement Au Moins Aussi Bon [2,3,4] used in France. The complete formulation of this principle is as following :

"All new guided transport system must offer a level of risk globally at least as good as the one offered by any equivalent existing system".

This formulation [3,5,6] takes into account what has been done and requires implicitly a progress to be made in the projected system, by the requirement "at least". It does not consider a particular risk, by the requirement "globally".

This formulation may be translated in the following way:
(a) Let $t_{c.réf.}$ be the fraction (casualty/passenger) experimented for a certain number of transported passengers by a transport system in the last years of operation, casualties caused by a collision between 2 trains. This fraction should be extracted from the statistics for the existing system, and form the reference for the new system, of the same nature.
(b) Now consider the new (replacement) system. For this system let :

1. C = capacity of one train (passenger/train)
2. F = frenquency of trains (train/hour)
3. r = mean occupation coefficient (train not completly full)
4. n_c = number of casualties per collision in this new system
5. Dm = throughput (passenger/hour) = r.C.F

The number of collision actually seen by each passenger must be:

$$col. = \frac{\tau_{c.ref}}{n_c} \quad \frac{collision}{passenger}$$

Also the collision rate for the new system must be smaller than that of the existing system: $\lambda_c \le col. * D_m = \frac{\tau_{c.ref}}{n_c} * D_m = \tau_{c.ref} * \frac{rC}{n_c} * F \quad \frac{collision}{hour}$

It is assumed that the proportion of casualties among the passengers in the same train is the same for the existing system and the projected system:

$$\frac{n_c}{rC} = constant$$

The manufacturer of the system of transport is free to distribute allocation between the different risks inherent to the system. The designer is free to distribute l_c between roadside equipment and on-board equipment. For example, the tolerable number of accidents and fatalities on a train system is set at a level equal to the current numbers on a highway system. This type of measures often needs to be adjusted based on other benefits and drawbacks present as well as the public perception in the systems that are evaluated. For instance, convenience and flexibility of driving may allow a discrepancy in comparison for individual automobile from a public transit system.

2.2 ALARP (As Low As Reasonably Practicable)

The ALARP principle [3,5,6] can be represented by the following diagram:

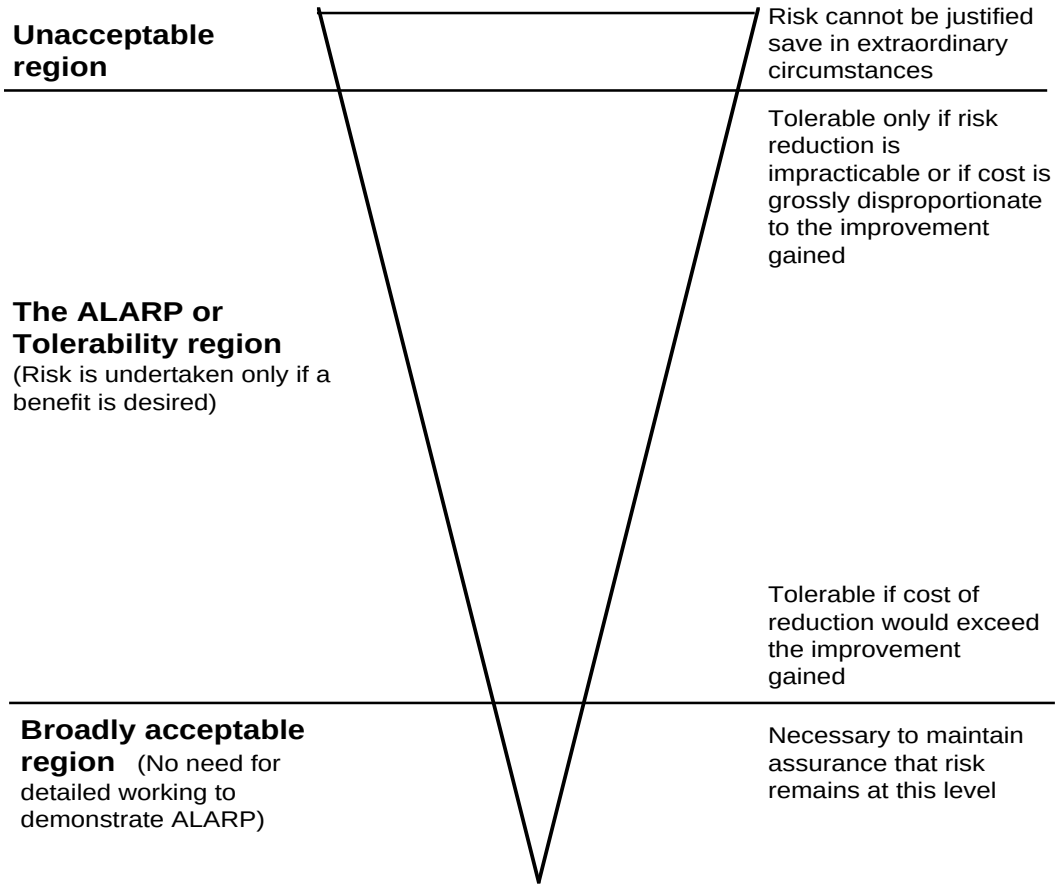

Figure 2.1. ALARP regions

(1) Some risks are so large and some outcomes so unacceptable that they are intolerable and cannot be justified on any grounds. The upper bound (Figure 2.1) defines levels of risks that are intolerable; if the risk of an operation cannot be reduced below this bound then the operation should not be carried out.

(2) The lower bound of the diagram (Figure 2.1) defines the broadly acceptable region where risks are considered to be so low that strenuous efforts to reduce them further would not be likely to be justified by any ALARP criteria. For people living in the vicinity of nuclear installation, the upper limit of this region is generally regarded as being an individual risk of 10^{-6} per annum, which is considered to be no greater than many day-to-day risks widely accepted by the public.
(3) The area (Figure.1) between the upper and the lower bounds is called the ALARP region [4,5,7]. It must be stressed that it is not sufficient to demonstrate that risks are in the ALARP region, they must be made as low as reasonably practicable. There are various ways to demonstrate ALARP. It may be sufficient to show that the best available current standards and practices are being applied. For novel operations, or where the adequacy of current standards or practices is in doubt, the concepts of cost benefit analysis and value of life can be introduced.

For a new system to be introduced, there may not be adequate measures or existing standards to evaluate the potential benefits or risks, therefore the goal is to search for a risk level as low as possible technically and socially. This is equivalent to the viewpoint of ALARP = As Low As Reasonably Practicable [4].

2.3 MEM (Minimum Endogenous Mortality)

This principle [3,5] has been derived in the following manner. Death will result from many different causes. One such cause is termed "technological facts":
(1) Entertainment and sport (surf, trial);
(2) Do-it-yourself (lawn mowing...);
(3) Work machines;
(4) Transport.
This group of causes results in a certain percentage of death per annum that varies according to the age of the population being considered. This risk is referred to as Endogenous Mortality "R". In well-developed countries, R is the lowest for the age group of 5 to 15 years. This lowest level of Endogenous Mortality, known as Minimum Endogenous Mortality (MEM), R_m, has been determined as:

$$Rm = 2.10^{-4} \text{ fatalities/person.year}$$

From the above, the following rule is formulated:
"Hazards due to a new system of transport would not significantly augment the figure Rm". For systems that may result in a large number of fatalities, "differential risk aversion" (DRA) is introduced by a decreasing slope as represented in the curve shown in Figure 2.

If a system is totally new and has no peers that provide similar services, then the targeted safety goals can be established by imposing a comparative standard that is perceived to be acceptable by the society. This is equivalent to the viewpoint of MEM = Minimum Endogenous Mortality [4]. For instance, the mortality rate of the targeted users for a certain type of activities is used as an equivalent measure when evaluating the reliability of a newly constructed system.

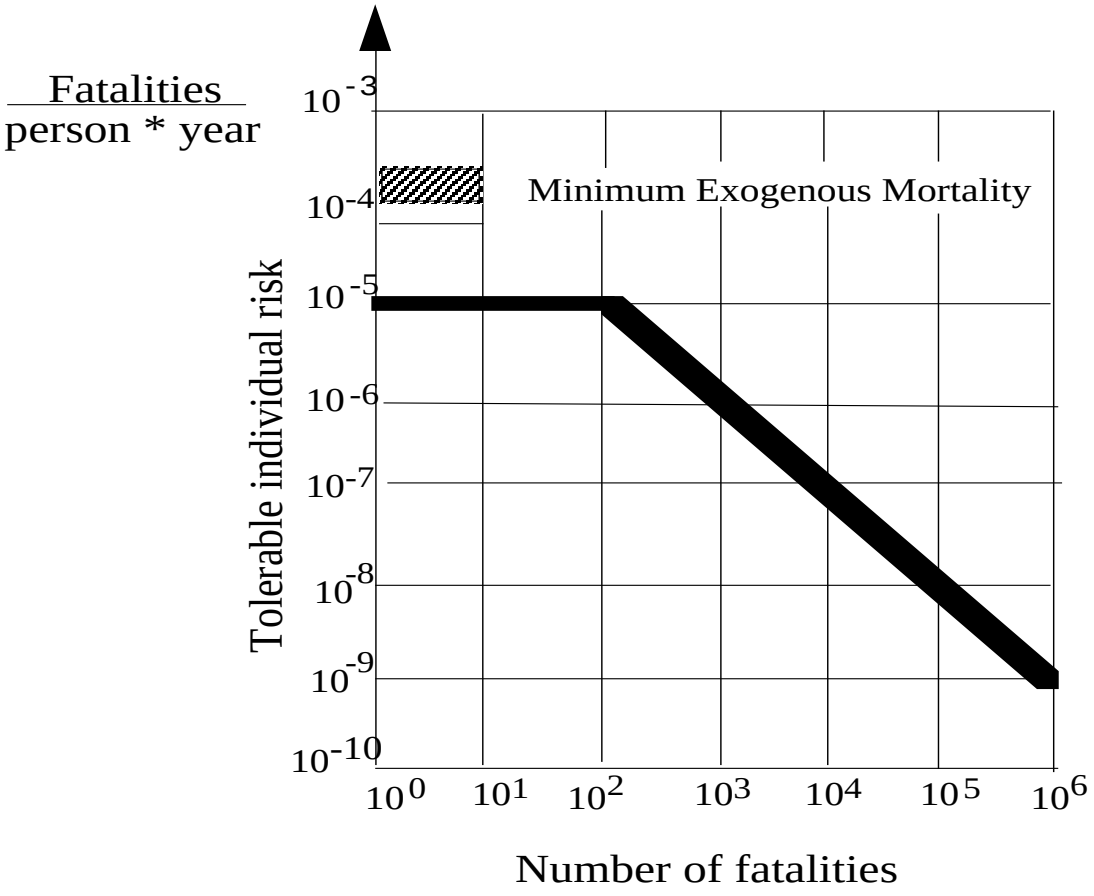

Figure 2.2. MEM principle

An evaluation on a newly established system should be studied thoroughly from the technical perspective; for example, the potential reduction of accidents when collision warning or avoidance systems are implemented on ground vehicles. This type of measures is based on targeted scenarios of the suggested systems. For instance, if a proposed frontal collision warning system is capable of generating a warning in 50% of all accidents and it is expected to be effective in eliminating an accident in 80% of accounted situations, then potentially it should reduce the total accidents by 40%. Therefore, the safety performances of the chosen groups can be clearly defined as a target for safety measures. The actual performance of such systems will depend on the market penetration rates and the complications of secondary effects generated in the deployment.

3.0 AVCSS ARCHITECTURE

In this section, we establish the architecture of general Advanced Vehicle Control and Safety Systems and analyze Frontal Collision Warning and Avoidance Systems (FCWS and FCAS) based on proposed architecture. Furthermore, we use a software tool, ASA, to construct a hierarchy module to indicate the information flows among functional blocks of AVCSS.

3.1 Logical Architecture

The suggested logical architecture of AVCSS is based on a PATH concept proposed for AVCS and ATMIS (Advanced Traffic Management and Information Systems) [1]. Of interest to us are the three layers: physical, regulation, and coordination, as shown in Figure 3.1 The physical layer represents the actual hardware, such as sensors, actuators, computers, etc. The regulation layer stands for the algorithms that are built upon the physical layer to exercise control or issue command to "regulate" the system into the desired states. The coordination layer is in charge of the control efforts above the level of regulation when coordinated maneuvers or actions are required between or among multiple systems.

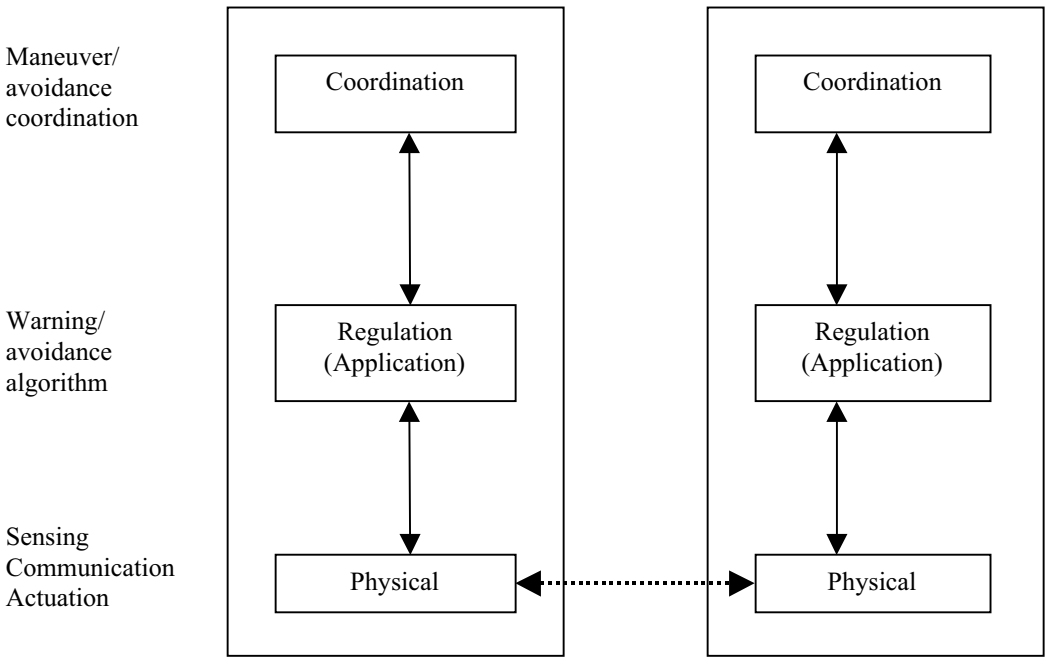

Figure 3.1. Logical Architecture of AVCSS

Under this architecture, each system builds its own layers of control structures. In between layers, information is passed to facilitate the designated functions. For example, the coordination layer receives from the regulation layer exchange vehicle state

information so that coordinated maneuvers can be planned. The regulation layer receives sensor measurements from the physical layer, while inputs actuator commands to the physical layer. Between two systems, if information exchange is required, it is channeled through communication or networking hardware and sent to the regulation or coordination layer for processing.

For the case studies of frontal collision warning or avoidance systems, the physical layer includes radar, lidar, camera, and warning display. The regulation layer contains the algorithms for obstacle detection, tracking, and threat assessment. The coordination layer involves coordinated vehicle control through the use of inter-vehicle or vehicle-infrastructure communication.

3.2 Physical Architecture

Figure 3.2 depicts a basic physical structure of AVCSS. When a vehicle is operating in its environment, sensors generate signals with interference from the background. The sensors outputs are provided to the algorithms or the processing unit for various purposes, such as diagnostics about the system states, or the tracking of a particular obstacle, or the threat assessment to determine the potential hazards presented by the obstacle. If equipped, a communication system will transit and receive information from other systems (vehicles or infrastructure) to the processing unit. The information from the processing unit is then fed into a human-machine interface to alert or indicate to a driver of the existing threats. Alternatively, the output can be fed into actuators to control the vehicle to minimize the determined threats. In either case, the actions taken by the actuators or the drivers will alter vehicle dynamics, which is further fed back into the loop for sensing and processing.

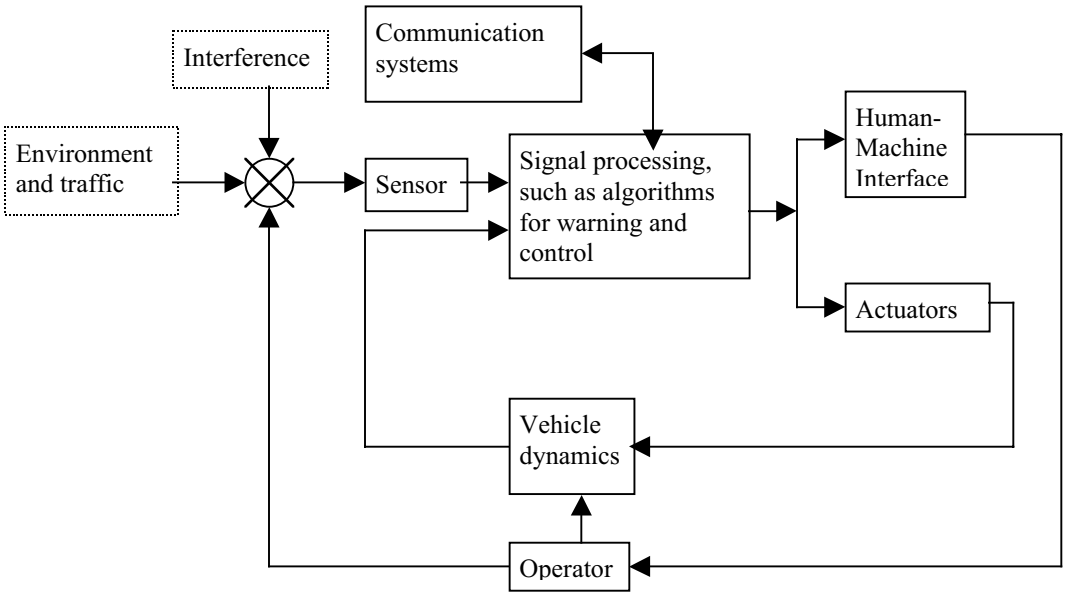

Figure 3.2. Physical Architecture of AVCSS

Abstractly, in terms of information flows among various sub-systems, the system contains the following types of elements:

(1) Information source, such as an obstacle
(2) Information transmission and reception (transducers), such as sensors
(3) Information processor, such as hardware and software for signal processing
(4) Information representation, such as human-machine displays
(5) Information executor, such as actuators or operators
(6) Information channel, such as interfaces between various elements

3.3 Functional Decomposition and ASA Modeling Tool

The functional decomposition is based on the modeling approach of the specification of the system (figure 3.3). The modeling technique enables one to evaluate that the system specification complies with the safety requirements of the equipment. To perform this task, the ASA (Automata and Structured Analysis) tool is used to describe both the static and dynamic aspects of the system. A brief description is given below. The ASA executable model of the functional specification provides:

(1) a way to check the adequacy between the requirements analysis phase and the User Needs,
(2) a clear identification of safety requirement at different levels.
(3) a way to produce a tests set dedicated to check the adequacy between the Functional specifications and the object code ,
(4) a common basis for all partners involved in the project (developer, operator, Regulatory Authority..)

The formalism used by ASA makes possible to apply automatic consistency and completeness on the model. So the quality of the functional specification obtained is greatly improved. Furthermore, the executable model can ensure the conformity between the Requirements and the functional specification.

The ASA technique is used for describing both the static and dynamic aspects of a system. The static description is a hierarchical top-down structured analysis approach . It identifies the set of elementary functions of the system and allows the identification of the data flow and the decomposition of the safety requirements.

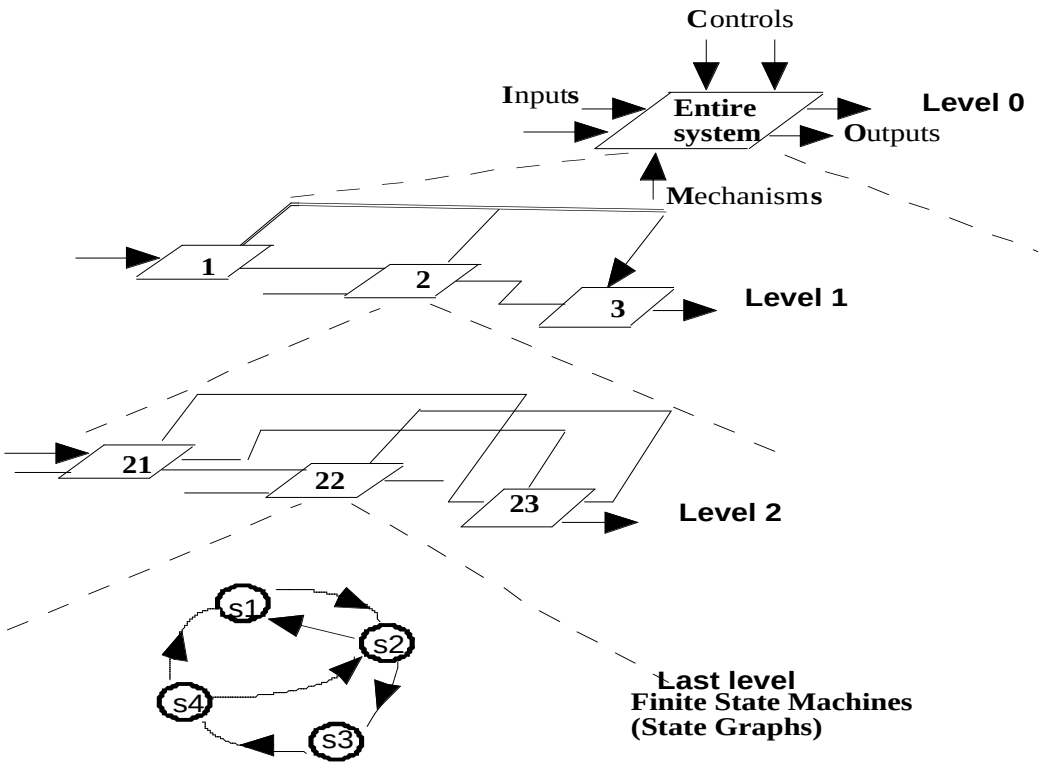

Figure 3.3. Hierarchical Top-down Analysis

The dynamic description (the last level) is given by communicating extended finite state machines concept (figure 3.4). This concept gives the behavior (or the transfers function) of each elementary functions according to the received stimulus (inputs/controls/mechanisms) added to the memory of past events.

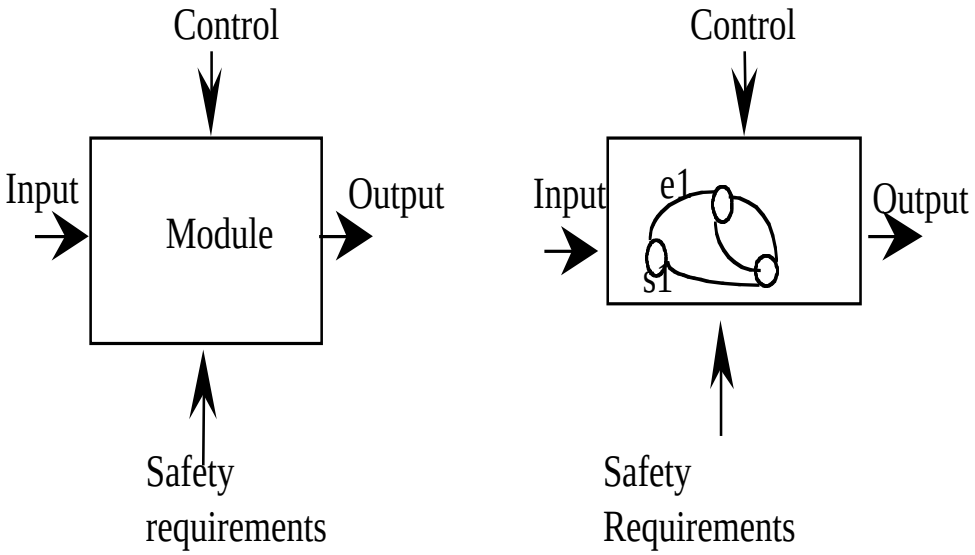

Figure 3.4. Static Description and Dynamic Description

A module creates output information by consuming input, control and mechanism (safety requirements) information.

3.4 Functional Decomposition for the Case Study

Depending on the design features and functional requirements of AVCSS, there can be significant variations in the selection of sub-systems and components. For the case studies of FCWS and FCAS, the main functioning blocks are:

(1) Sensing, which provides measurements of the vehicle states and the surrounding environment.
(2) Processing, which involves the calculation of sensing inputs and generation of outputs to warning or display, and actuation.
(3) HMI, which provides the monitoring information and the interface between the vehicle and the user or driver.
(4) Actuation, which receives the signal from the processing unit to control the vehicle. To maintain the discussions here to a limited scope, only the control in the longitudinal direction is included. In other words, actuation only involves acceleration (throttling) and deceleration (braking).
(5) Networking, which provides channels of communication or data exchange between all functioning blocks.

Each of the four blocks will be further decomposed by their functions.

Sensing can be separated into:
(1) Radar sensing
(2) Lidar sensing
(3) Computer vision sensing
(4) Speed sensing, the ground speed of the vehicle itself
(5) Acceleration sensing
(6) Yaw rate sensing
(7) Throttle position sensing
(8) Brake line pressure sensing
(9) Wheel torque sensing

Processing can be separated into:
(1) Obstacle detection processing
(2) Vehicle state and fault detection processing
(3) Warning and display signal processing
(4) Acceleration command processing
(5) Braking command processing

HMI can be separated into:
(1) Monitoring, indicating the state of vehicular systems

(2) Signal of impeding automated functions, indicating actions or problems with the control process
(3) Warning of hazardous situation
(4) Request for intervention by the driver

Actuation can be separated:
(1) Throttle control
(2) Braking control

Networking can be separation into:
(1) Networking between sensors and processor
(2) Networking between processor and display
(3) Networking between processor and actuator

4.0 PRELIMINARY HAZARD ANALYSIS [9]

This section deals with preliminary hazard analysis, which is the first step of safety evaluation. We have suggested the adaptation of safety principles in the railway (e.g. GAMAB, ALARP and MEM) to the AVCSS system, which is discussed in Section 2, which serve as the guidelines for setting safety objectives at the global level. In this section, the list of hazards related to the system and the safety objectives to be allocated to the system are presented. Hazard assessment and risk management issues are discussed. Hazards associated with exemplar safety functions are identified.

The methodologies for determining the safety integrity levels for safety-critical systems are covered in Section 4.1. Preliminary hazard analysis of selected AVCSS is given in Section 4.2.

4.1 Determination of Safety Integrity Level

The design of safety-critical systems involves a certain amount of work in conformance with the safety program to define the critical components. The primary work is related to identify and to determine the critical components. The determination of integrity level influences the development approaches and the assessment level to be performed in the process and the product itself. The safety integrity levels are allocated by identification and analysis of hazards, as well as by assessment and classification of risks. The process includes:

- Appoint out the qualified personnel,
- Allocate the development effort,
- Perform in the depth the V&V activities,
- Set up the required techniques, tools and languages
- Construct step by step the Safety Case
- Identify the assessment level to be performed.

4.1.1 Hazard Identification and Analysis

The hazard Identification and analysis aims to cover all system safety behavior by taking into account its environment conditions. This activity starts by identifying the system and safety boundaries, then performing a preliminary hazards analysis to identify the actual and potential hazards perceived within these limits. This analysis allocates to each hazard or group of hazards a severity category. Four categories of hazard severity are classified, in the qualitative terms, depending on the consequence of the system's reaction to failure risk assessment and classification. The four classes are catastrophic, critical, marginal, and trivial, as depicted in Figure 4.1.

The combination of the consequence of hazard or sequence of hazards and the probability of its occurrence determine the risk classification. Probabilities of accident occurrence are also classified into six categories: frequent, probable, occasional, remote, improbable, and incredible. The Risk Class Range cenelec pr EN 50126 (RC1 to 4) defines four groups to be:

- Eliminated by construction at different stages of the life-cycle development,
- Accepted when the reduction is impracticable with an agreement of safety authority,
- Acceptable with adequate control and the agreement of Safety Authority,
- Acceptable with agreement of safety authority.

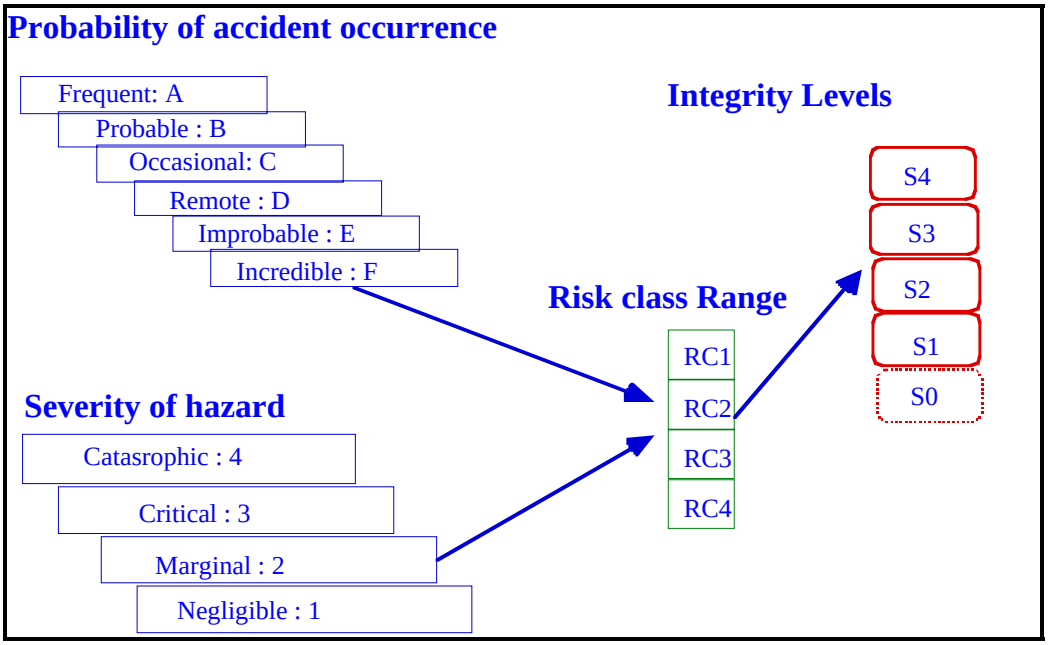

Figure 4.1. SIL determination

It is the responsibility of the developer to assign the safety integrity level on the basis of the level of risk associated with the system. The safety functions allocated to the system should be clearly identified and the integrity level determined (Figure 4.1). The safety integrity level requires compliance with the quality and safety management and technical safety. The way of determining the appropriate level needs to identify the safety requirements, specification and safety integrity level of subsystem, item and equipment. The level of software is deduced from the level of equipment in which the software is a component.

The cenelec standard prEN 50129 identifies two types of safety integrity:

- Systematic integrity, which is related to a non-quantifiable part such as systematic faults caused by human errors. This systematic integrity is achieved by the quality of the process.

- Hardware integrity, which is related to a quantifiable part such as hazardous random hardware failures.

The cenelec standard identify five integrity levels and prescribe techniques and measures to be used. The level 0 refers to non safety-related application. The levels 1 to 2 are safety-related. The levels 3 and 4 are related to the safety critical application. The techniques and measures required for level 1 are the same as for level 2. The techniques and measures associated to the level 3 are the same as for level 4. The required development and assessment can be categorized into 3 classes:

Categories	SIL	Grading Assessment
Non essential	0	Low level
Essential	1 & 2	Medium level
Critical	3 & 4	High level

The assessor should be independent from the developer. However, the independence between design, verification and validation activities can be summarized as follow:

- For the level 0, the designer, verifier and validator can be the same person
- For levels 1 and 2 the verifier and validator can be the same person and can not the designer
- For levels 3 and 4 the designer, verifier and validator must be the separate persons.

We collect and categorize the threats, which can appear in a safety-critical system. Assuming that all threats can be avoided by an appropriate safety system the reason for residual threats are failures of this safety system. Therefore we can concentrate on the term failure and on failure avoiding and failure controlling measures. The reasons for these failures are random failures in the hardware or faults in hardware or software that cause systematic failures.

- *Random failures* are the result of a variety of degradation mechanisms. The point to observe here is that nothing can be said about the moment the failure will occur. Only a probability can be given.
- *A systematic failure* is the result of a fault in the specification, design, construction or use of a system that causes it to fail every time under a particular set of conditions.

4.1.2 Hazard Assessment

Different measures have to be taken to avoid failures. The following list gives an overview of the main activities in the development and assessment of safety critical systems. The functional description of the system is the starting point for further considerations. The analysis of the risk leads to the System Integrity Level. The System Integrity Level determines a set of safety

measures, which have to satisfy the System Integrity Level. If the safety measures chosen from the standard are applied properly, then the system can be considered safe according to the standard used.

(1) Development process:
- *Functional description of the system*
- *Risk analysis*
- *Derivation of safety integrity level (SIL)*
- *Choose a set of safety measures*
- *Build the system to satisfy safety measures*

(2) Assessment Process:
- *Is the risk analysis done properly?*
- *Is SIL derived properly?*
- *Are the safety measures chosen properly?*
- Are the safety measures satisfied properly?

Applying the chosen safety measures in the system, the designer needs much more information about these measures than he can find in the standards. The knowledge of the state-of-the-art in safety technology of the application area in question, and the experience of the designer provide further important information. The assessment process is very similar to the development process.

4.1.3 Risk Management

Risk management can be defined as the systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating and controlling risk. Thus, risk management consists of four parts:

- Hazard Analysis,
- Risk estimation,
- Risk evaluation,
- Risk reduction and control.

These four parts have to be applied to a well-defined system with clearly defined intended function of the system. The main task of hazard analysis is the identification of hazards. This paper shall present methods of hazard identification within the context of hazard analysis.

4.1.3.1 Definition of the System

Before starting hazard identification in a system, the system has to be defined. The following aspects must be taken into account:

- Boundaries of the system,

- Intended function of the system,
- Working environment of the system,
- Hardware-software interaction within the system.

4.1.3.2 Hazard Identification

Hazard identification is a major part of risk management. A hazard is a source of potential harm or a situation with a potential harm. That means a hazard is not an event but a pre-condition, which under certain conditions can lead to a chain of events resulting in harm to human beings, the environment, or material values. Depending on the problem, a general list of hazards should be established. The easiest way to check which hazards are inherent in a system under study, a table or matrix can be established showing in their rows all hazards of the checklist and in their columns all components of the system. If a hazard occurs in a component the coinciding box is marked with a cross. A checklist of hazards or groups of hazards is an important tool. Nevertheless, hazard identification is an intelligent process performed by the analyst. The checklist can give hints as to which hazards have to be accounted for.

4.1.3.3 Risk Estimation and Evaluation

Risk estimation and evaluation has to be done based on the results of the hazard identification. The scope is to assess the risk connected with certain hazards. Methods such as Fault Tree Analysis can be used.

4.1.3.4 Risk Reduction and Control

Together with the identification of a hazard and the chain of events that may lead to damage, measures how to safeguard against the undesired consequences must be established. Two groups of measures can be identified:

- Hazard reduction or removal,
- Hazard control.

The first group of measures incorporates measures that are dedicated to remove or reduce the hazard. E.g. a toxic substance is replaced by another, nontoxic substance with the same function. If it is not possible to remove the hazard completely, it can be reduced. As an example the application of low voltage technique may serve. Here the dangerous high electric voltage is replaced by low voltage that is able to fulfill the same function but is less dangerous.

Especially in the second group of measures, i.e. measures for hazard control, computerized protection systems play an increasing role. Consequently, the focus must also be on software that is mostly the heart of such systems. Measures of hazard removal, reduction or control must be indicated. Using the results from risk analysis, a priority must be established and possible effects of these measures must be studied. A decision should be made as to which measures have to be taken and management methods must be implemented to trace the actions until they are fulfilled.

After having performed the risk reduction process, the hazard identification and risk analysis have to be updated. Measures of risk reduction must be taken into account and the analysis must be changed appropriately. In particular, it has to be ascertained whether the measures of risk reductions have been sufficient to bring risk to an acceptable level. If an acceptable level has not yet been reached, further measures of risk reduction have to be implemented and the process has to be continued repeatedly until the risk is reduced in a sufficient manner.

4.2 Preliminary Hazard Analysis of AVCSS

In this section, we'll identify hazards associated with each of the safety functions. Certain elements or phenomena of hazards are similar in different system functions, while others are unique in individual cases. Associated with each system function, there is a list of components and related failures that may result in those hazards. A table of components is developed for all targeted systems to show the linkage between component failures and external events that are related to hazards in AVCSS.

The functions of targeted AVCSS should be identified first. A selected list of AVCSS functions is given below:

- *Collision warning (frontal, side, rear)*
- *Lane departure warning*
- *Automated longitudinal control*
- *Automated lateral control*
- *Collision avoidance in frontal direction*
- *Safety impact of coordination layer and network layers*

For the case studies, we will examine the collision warning and avoidance systems (CWS/CAS), and the lane departure warning systems (LDWS).

4.2.1 Categories of Hazards in AVCSS

To analyze the criticality of hazards, the types of hazards must be identified first. Certain hazards are similar in various AVCSS, while others are distinct in their nature. Generally speaking, there are three major categories of hazards for AVCSS: environment, driver, equipment, passenger, and design-related. They are detailed further below.

(1) Environment factors – such as weather or infrastructure problems.
Environmental hazards most influential to AVCSS are foggy, rainy, and icy conditions. The direct effects on AVCSS operations are:

- *Performance of sensing devices deteriorates in these conditions,*

- *Uncertainty of vehicle control increases due to changes in vehicle-roadway interface, and*

- *External disturbance causing vehicle deviate from its course.*

(2) Driver actions – driver alertness or readiness or intervention.
Driver actions or in-actions can become causes of accidents. They may fail to take actions due to drowsiness, unconsciousness, or inattention. They may react improperly due to distraction, panicking, or wrong perception and misunderstanding. The last two items may be results of insufficient training or poor design of human-machine interface.

(3) Component or function failures
Equipment and functional failures can certainly lead to hazardous conditions. The types and causes of these failures will be discussed later with a functional decomposition of the candidate AVCSS.

(4) Passenger actions – behaviors, responses, or conditions that may affect operations.
Passenger actions are a concern in other transportation systems, but less relevant in AVCSS. However, due to the interaction between drivers and passengers, the actions of passenger may propagate into driver response that lead to accidents. For the purpose of discussions, we will neglect this category for now but group related concerns into those in the driver category.

(5) Design errors
Safety hazards can be created by specification or design errors. Specification errors and design errors may not present as a hazard until one or more of above described failures or errors occur.

4.2.2 Hazard Analysis for Lane Departure Warning Systems (LDWS)

Lane Departure warning systems provide warning functions to prevent vehicles from deviating into undesired or unsafe trajectories.

4.2.2.1 Hazard Identification
Common hazards for lane departure warning systems are:
(1) Environmental-related:
(a) Loss or deterioration of lateral positioning accuracy due to infrastructure: For example, this may be resulted from a computer-vision system with no visible lane markings, or a magnetic marker system interfered by background noises.
(b) Loss or deterioration of lateral positioning accuracy due to weather conditions For example, this may be arise from a computer-vision system in a foggy situation.
(c) Loss or deterioration of tire control due to weather conditions This can be caused by slippery or icy road surfaces.
(d) Intrusion of surrounding vehicles or unavoidable traffic hazards (system limitations)The movement of other vehicles may intrude into the path of the subject vehicle and result in a hazardous situation while the subject vehicle is functioning properly within its design requirements.
(2) Driver-related:

(e) Driver non-alert or inattentive: This refers to the situation when the driver fails to recognize the warning signal even if it is properly generated by LDWS

(f) Driver over-reacting or panicking: This situation occurs when the driver takes the wrong action, such as excessive steering for correcting vehicle maneuvers.

(g) Ignorance or intended destructive actions taken by the driver: This rare situation arises when the driver is intentionally destructive or suicidal.

(3) Equipment-related:

(h) No warning or alarm: This hazard occurs when the system does not generate a warning when it is warranted.

(i) Warning invisible or inaudible: This condition is caused by deficiencies of the human-machine interface.

(j) False alarm due to erroneous signal processing or HMI errors: The warning signal is incorrectly generated when it is unwarranted.

(k) Lateral positioning sensing errors due to sensor failure

(l) Vehicle state sensors information incorrect

(m) Computer hardware failure

(n) Computer software failure

(o) Communication network failure

A combination of the hazards (a)-(o) may result in collisions with other vehicles or obstacles or may cause unnecessary maneuvers, which lead to subsequent hazards to following or neighboring vehicles.

4.2.2.2 Functional Decomposition for LDWS

A lane departure warning system consists of the following blocks:

(i) Lateral positioning systems, such as magnetic markers or computer vision

(ii) Vehicle state sensors, such as speed, acceleration, yaw, yaw rate, steering angle, throttle position, and brake line pressure or wheel torque.

(iii) Processing, including computer hardware and software

(iv) Human-machine interface (HMI), which provides visual and/or audio signals to drivers

(v) Driver, who adjusts the vehicle speed based on the warning from HMI.

(vi) Communication network that allows data exchange between sub-systems.

(vii) Environmental interference or intervention, including the surrounding traffic, obstacles, and signal noises.

Hazards often can be associated with the failure of sub-systems (i)-(vii) mentioned. The following table shows how the cause and effect among the hazards H(a) through H(p) and the failures of sub-systems S(i) through S(vii). A cross mark in a table cell indicates that the sub-system is a potential contributing factor in the hazard.

	S(i)	S(ii)	S(iii)	S(iv)	S(v)	S(vi)	S(vii)
H(a)							X
H(b)							X
H(c)							X
H(d)							X
H(e)					X		
H(f)					X		
H(g)					X		
H(h)	X	X	X	X		X	
H(i)				X			
H(j)		X	X	X			
H(k)	X						
H(l)		X	X				
H(m)			X				
H(n)			X				
H(o)				X			

4.2.3 Hazard Analysis for Collision Warning System (CWS) and Collision Avoidance Systems (CAS)

Collision warning systems provide warning functions to prevent vehicles from collisions with neighboring vehicles. The difference between CWS and CAS is the brake actuation to be introduced for CAS. Hazard analysis of CWS and CWA can be derived using the similar method.

4.2.3.1 Hazard Identification

Common hazards for CWS/CAS are:

(1) Environmental-related:

(a) Loss or deterioration of accuracy of range and range rate measurements due to weather conditions: Examples of this category of failures include heavy rain fall, fog (for optical sensors), and dust (for ultrasonic sensors).

(b) Reduction of tire friction due to weather conditions: This can be caused by slippery or icy road surfaces.

(c) Intrusion of surrounding vehicles or unavoidable traffic hazards (system limitations): Vehicles or obstacles intrude into the path of the subject vehicle resulting in less reaction time than necessary for preventing collision.

(2) Driver-related:

(d) Driver non-alert or inattentive: This refers to the situation when the driver fails to recognize the warning signal even if it is properly generated by CWS.

(e) Driver over-reacting or panicking: Driver takes the more aggressive control action than necessary, such as emergency braking for correcting vehicle maneuvers.

(f) Ignorance or intended destructive actions taken by the driver: This rare situation arises when the driver is intentionally destructive or suicidal.

(3) Equipment-related:

(g) No warning or alarm: This hazard occurs when the system does not generate a warning or providing control when needed.

(h) Warning invisible or inaudible: This condition is caused by deficiencies of the human-machine interface.

(i) False alarm due to erroneous signal processing or HMI errors: The warning signal is incorrectly generated when it is unwarranted.

(j) Range or range sensing errors due to sensor failure

(k) Vehicle state sensors information incorrect

(l) Computer hardware failure

(m) Computer software failure

(n) Communication network failure

A combination of the hazards (a)-(n) may result in collisions with other vehicles or obstacles or may cause unnecessary maneuvers, which lead to subsequent hazards to following or neighboring vehicles.

4.2.3.2 Functional Decomposition for CWS/CAS

A collision warning/avoidance system consists of the following blocks:

(i) Range and/or range rate sensors, such as radar or ladar sensors

(ii) Vehicle state sensors, such as speed, acceleration, throttle position, and brake line pressure

(iii) Processing, including computer hardware and software

(iv) Human-machine interface (HMI), which provides visual and/or audio signals to drivers

(v) Brake actuator, which enables deceleration

(vi) Driver, who adjusts the vehicle speed based on the warning from HMI.

(vii) Communication network that allows data exchange between sub-systems.

(viii) Environmental interference or intervention, including the surrounding traffic, obstacles, and signal noises.

Hazards often can be associated with the failure of sub-systems (i)-(viii) mentioned. The following table shows how the cause and effect among the hazards H(a) through H(p) and the failures of sub-systems S(i) through S(viii). A cross mark in a table cell indicates that the sub-system is a potential contributing factor in the hazard.

	S(i)	S(ii)	S(iii)	S(iv)	S(v)	S(vi)	S(vii)	S(viii)
H(a)								X
H(b)								X
H(c)								X
H(d)					X			
H(e)					X			
H(f)					X			
H(g)	X	X	X	X				
H(h)				X		X		
H(i)				X				
H(j)	X		X					
H(k)		X	X					
H(l)			X					
H(m)			X					
H(n)							X	

4.2.4 Failure Mode Effect and Criticality Analysis

Risk analysis can be defined as the systematic application of management policies, procedures and practices to the tasks of analysis, evaluating and controlling risk. Hazard identification and the measures to cope with are a major part of safety analyses. The safety requirements attached to each function are used as mechanism to allow the module to operate.

Failure mode analysis has to be applied to a well-defined system with clearly defined inputs and intended outputs. The definition of the system is done by the functional decomposition and analysis. An example of the failure mode analysis for exemplar AVCSS is given in the Appendix. The last column gives the type of safety measures to be implemented to cope with the hazards.

5.0 ASSESSMENT AND CEERTIFICATION PROCESS

5.1 Safety Computer

5.1.1 Concepts

The safety design approach of computer based critical application can use the following concepts:

- the *information redundancy* concept which consists in detecting faults due to failures or perturbations by the very contents of information, is made as a basic technique. This involves mainly a single microprocessor computer using information redundancy like the coding techniques, the software diversity and the self-checking techniques.
- the *hardware redundancy* concept, based on several hardware running simultaneously, is adopted when the safe state is the end of the mission; this is the case particularly of air transport or space programs.

These approaches can be jointly used in a given architecture. We develop here after the main architectures related to these concepts. The distributed computer notion is also described.

5.1.1.1 Information redundancy

This redundancy can be integrated into the software or installed in the very processor. The principle consists in giving to the processed information a certain redundancy. Validation is made by controlling the information belonging to the chosen redundancy.

- The *signature microprocessors*: the partial signatures, collected during the processing, are bound to unveil the errors when the final signature is verified. The signature is independent of the type of microprocessor. This is the case, for instance, of the French *coded microprocessor* used in the train protection systems .

- The *software diversity* (N version programming) means that N independently developed functionally equivalent versions are executed in parallel. Their outputs are adjudicated by a voter.

- The *self checking processors* are designed and developed in order to facilitate tests of different processor blocks. They integrate into their computer the devices necessary for implementing operational tests. Special operations are added to the conventional instructions, in order to facilitate the testing of the microprocessor. These specialised processors are capable of detecting immediately their own faults.

5.1.1.2 Hardware redundancy

These architectures contain two, three and more distinct most often homogeneous processors (for reasons of maintenance costs) accompanied by their own environment equipment. These architectures differ by the nature of comparator and the techniques of its putting into safety. They often integrate internal functional tests for protecting themselves against latent failures. The difficulty inherent in these tests is the evaluation of the coverage rate of failures.

- The *Dual microprocessor* computercan be found in on-board automatic devices

- The *Triple Modular redundancy* architectures are based on the redundancy of three microprocessors to which a system of comparison and majority vote is associated. The result of each processor is compared with those of the other ones and the system output is the result of a "Two out of three" vote. The suspected processor can then either be put out of action (thus no longer a participating voter) or penalised and put out of action if its failure persists. The replacement of the failed part may be made without stopping the system. These architectures are well adapted to ground equipment.

5.1.1.3 Safety distributed architectures

In a distributed computer, the overall functionality is decomposed into sub-functions, which are allocated to logically or physically separate subsystems that communicate and collaborate to achieve the required functionality.

Distribution may result from different design considerations such as

- adaptation to a geographically distributed process
- increase of dependability (safety and/or reliability and availability) by redundancy or diversity
- functional partitioning or functional autonomy to obtain graceful degradation behavior and then to increase system dependability
- performance considerations (increase of system time response through local intelligence at peripheral levels, load sharing, etc.).

The dependability of any distributed system relies on the dependability of

- the separate subsystems,
- the computeritself and
- the communication.

Distribution also introduces additional complexity, might cause synchronization problems and requires sophisticated solutions for data storage and data management. Additionally there might be cost, weight and space problems. The benefits and drawbacks of distribution thus have to be carefully analyzed for each application.

5.1.2 Typology of faults and countermeasures

5.1.2.1 Type of Faults

Several kinds of fault are liable to happen in a computer controlled system. They originate from various circumstances. The origin of faults can be divided into two categories :

- *Human factors*. It is typically the wrong design, production, construction, operation, maintenance and illegal input from other systems,

- *Physical factors*. It is related to the deterioration of hardware elements, to environmental interference like electromagnetic noise and high or low temperature.

5.1.2.2 Measures and Techniques

The means to achieve the computer safety relates to controlling the factors, which influence the safety. This control requires the establishment of mechanisms and procedures to defend against sources of error being introduced during the realization and support of the system. Such defenses need to take account of both random and systematic failure.

The means used to achieve safety are based on the concept of taking precautions to minimize the possibility of an impairment occurring as a result of an error during the realization phases. Precaution is a combination of:

- Prevention: concerned with lowering the probability of the impairment;
- Protection: concerned with lowering the severity of the consequences of the impairment.

The primary approach to achieve the safety of an computer is to improve its reliability by *fault prevention* measures. The goal is to prevent failures by ensuring that all faults have been removed from the computer during its development. Fault avoidance and fault removal are the basic aspect of the prevention of faults:

- Fault avoidance is related to the design methodologies and the techniques and technologies which aim to avoid the introduction of faults during design and construction of an architecture.
- Fault removal is concerned with checking the implementation of an computerand removing any faults. It is mainly based on extensive test to reveal faults in the hardware and software before putting the system into service.

The second approach to achieve the safety of an computer is to improve its reliability by *fault tolerance* measures. The hardware can generate failures in the system due to components deterioration and environmental conditions. The fault tolerance is required at least to protect the operational system against such failure. Once identified, the consequences of failure could be anticipated. Appropriate fault tolerance measures could also be incorporated in the computer to detect when the failure occurred and to ensure that correct system operation is maintained.

So, the measures used against failures can be classified in the two following categories:

- Measures for fault prevention: these measures are used to avoid failures during the different phases of the safety life-cycle,
- Measures for fault tolerance: these measures are used to control failures during the operation.

5.2 ASSESSMENT AND CERTIFICATION

5.2.1 Process

The objective of a product assessment and certification process is to verify and confirm the fact that the product meets its safety requirements specification. Figure 5.1 shows the

ideal set of processes for development, assessment and certification. This is an ideal scheme but in some cases, the processes are overlapped: the assessment process can be concurrent or consecutive to the development process.

Figure 5.1. Certification process

The first stage of the process is the development, followed by the assessment and the certification stages. The main objective of the assessment phase is to prepare an impartial report giving enough information on the safety of the product, to obtain the confidence that the product reaches the safety requirements specification and to obtain the certification of the product. The certification is a formal declaration that confirms the results of the assessment. The next stage is the *approval* stage: the integration of the product in a system or the installation of the product in its real environment. The approval process is the mean to confirm that the use of a product in a particular environment and with a particular goal is acceptable. In a safe operational exploitation, a product is used according to agreed procedures. In this case, changes made to the environment of the product can involve modification of the product and influence the development process.

5.2.2 Phases of the assessment and certification process
The assessment and certification process is divided into three main phases : preparation, assessment and certification. These phases lead to the redaction of plans and reports including mainly the assessment plan, the assessment report and the certification report.

5.2.2.1 Phase I: Preparation of the assessment
The client (sponsor or supplier) must give a precise description of the product and defines the safety requirements specification and the boundaries of the assessment. When the sponsor is not the supplier, the participation of the supplier is strongly recommended.
The sponsor asks a notified body for an assessment of the product.
The notified body points out competent assessors. A preliminary analysis of the product description and the Safety requirement specification is made in order to control the completeness and the coherence of the two descriptions.

The assessor defines an assessment plan, containing a detailed assessment work plan. The plan has to be agreed by the client. The client prepares and transmits an assessment case to the notified body. This assessment case contains:

- the description and boundaries of the product,
- the safety requirements specification,
- the supplies delivery plan,
- the confidentiality clauses (delivery of supplies, etc.),
- the identification of the notified body and the identification of the assessors.

The assessment can be divided into work packages, shared or not between several assessors.

5.2.2.2 Phase II : Assessment

The client supplies the assessment inputs according to the assessment plan. The assessment inputs are delivered according to the delivery protocol established during the preparation phase of the assessment.

The assessors proceed the assessment tasks defined in the assessment plan. For each task, reports are regularly produced to control the progress of the assessment tasks. The assessment inputs are analyzed in conformance with a referential constituted of assessment criteria (examples are given in the document [10]).

During the assessment, non compliances can be detected (non delivery of an assessment input, design errors, etc.). In general, there are two categories of non compliances : the minor non compliances which can be easily corrected and the major non compliances which require further attention to be solved. Both types of non compliances are recorded in the assessment report. All non compliances must be solved at the end of the assessment and the decision of closing a non compliance must be taken with the agreement of all the partners involved in the assessment.

At the end of each assessment task, an *assessment report*, which contains the results of the assessment work, is written by the assessor. Each assessment report is examined and internally approved by the notified body. The assessment reports contain mainly:

- the objectives of the task, the inputs,
- the criteria applied,
- the description of the work achieved by the assessors,
- the techniques, methods and tools used for the assessment work,
- the results of the assessment,
- a proposal for the verdict of the assessment,
- a description of the non compliances detected,
- an estimation of the time and resources used for the task,
- a conclusion and recommendations.

A pass verdict is assigned if all applicable criteria are satisfied and, in particular, no risk of hazardous failure have been found. A fail verdict is assigned if any error is found and is not corrected, or if a risk of hazardous failure is found.

5.2.2.3 Phase III : Certification

In this phase, the technical assessment report is approved by the notified body. On the basis of the technical assessment report, the notified body summarizes the conclusion in the *certification report*. The certification report is a public document, accessible by end user that uses the product. In consequence, the certification report must contain all the observations, measures and recommendation necessary to have a safe use of the product. The notified body delivers a *Certificate* that attests that the assessment was achieved correctly, with impartiality, competencies, in accordance with the criteria and procedures.

The certificate is valid for the version and configuration of the product as it has been assessed.

5.2.3 Assessment procedure

Assessment is the evaluation of a process or a product against a set of criteria by a technically competent person who is independent from the designer. Such criteria are drawn from various sources : standards, state of the art, best practice and experience. The objective of an assessment method is to ensure that an assessed system meets its safety requirements.

The assessment shall begin with the formulation of an assessment plan, detailing the scope of assessment and its basis, such as the safety and reliability targets, integrity level and norms. The assessment plan and detailed criteria shall be produced by the assessor. The supplier of the computershall provide all the evidence required to demonstrate compliance with the criteria. The evidence should be organized in accordance with the Safety Case Structure [11], and shall be readily available for audit, walk-through, review and detailed examination.

The assessor shall make judgments about the evidence presented by the supplier. The detailed assessment criteria must cover all the techniques and procedures used by the developer to achieve the integrity of the architecture. The assessment should be focused, mainly, on the conformity and effectiveness of the techniques and measures, where:

- Conformity characterizes how accurately the techniques and measures are implemented and how well they are explained in the supplied documentation.
- Effectiveness characterizes how effectively the techniques and measures are in identifying and eliminating or mitigating the hazards.

Where necessary, single criteria can be broken down into several lower-level criteria in order to make the assessment. Each criterion shall be applied according to current best practice and experience. In addition, the assessor shall assess the design of the computer independently, for example, by carrying out as a minimum, an independent hazard analysis.

The assessor shall produce an assessment report which should provide detailed reasons why the elements of the computer passed or failed the criteria. This section provides information on the Assessment procedure It outlines how to conduct an assessment and references the minimum level of activities to be undertaken. The aim is to:

(a) Enable assessors to understand how to conduct an assessment,

(b) Enable repeatability between assessments when conducted by different assessment agencies and/or countries,

(c) Provide a framework around which the assessors can plan and perform assessments.

The assessment procedure [12,4,13] consists of five processes, each of which is discussed more fully in the rest of this chapter. Briefly the procedure consists of:

(a) Planning the Assessment,

(b) Specifying the Requirements of the Assessment,
(c) Assessing the Process used to develop the Product,
(d) Assessing the Product,
(e) Documenting the Findings in a Report.

The assessor will produce both the Assessment Plan and the Assessment Requirements Specification. The Assessment Requirements Specification will be produced in close consultation with the client and the client will be required to authorise the final document.

5.2.3.1 Assessment Plan

The Assessment Plan is produced by the assessor. It is likely that the planning of an assessment will be carried out partly in parallel with determining the requirements of the assessment and the production of the Assessment Requirements Specification.
The Assessment Plan will provide the following information:
(a) The products and processes to be assessed,
(b) The assessment activities to be undertaken,
(c) The team that will undertake the assessment,
(d) The responsibilities of the team,
(e) The assessment criteria which will form the basis of the assessment,
(f) The minimum level of documentation to be examined,
(g) A schedule of assessment activities, and for each activity;
(h) Procedure for dealing with appeals, complaints and disputes.
The Assessment Plan shall allow for presentations to be given by the design and production teams if required.

5.2.3.2 Assessment Requirements Specification

The requirements of the assessment will be produced by the assessor in close consultation with the client. The final version of the Assessment Requirements Specification must be authorised by the client.
The Assessment Requirements Specification will provide the following information:

- The scope of the system paying particular attention to the system boundaries
- The purpose of the assessment, e.g. whether it is for internal purposes or an integral part of a certification process
- The assessment basis, such as the standards, criteria, constraints, legal requirements etc.
- The depth of analysis required
- The level of details needed for the assessment

5.2.3.3 Process assessment

Process assessment ensures that the system development and supporting processes are appropriate for the standard being used and that the standards are maintained and followed.

The assessment of the process shall consider the following evidence as a minimum:

- Project lifecycle activities and associated documentation
- Standards
- Safety Integrity Level

As ISO 9001 certification is one of the minimum requirements for the development of safety-critical systems, the assessment must ensure that the quality system has been followed for the product and processes being assessed.

5.2.3.4 Product assessment
Product assessment ensures that there exists sufficient analytical evidence showing compliance with the standards and conformity with product criteria. Product assessment shall consider the following evidence as a minimum:
- Safety Requirements
- Hazard Identification and Analysis
- Risk Analysis
- The Product Safety Case

Appropriate product assessment criteria should be developed using the requirements for the assessment. The product should be assessed using the selected criteria. The results from the assessment and the evidence should be documented in the Assessment Report. The main activities of product assessment are to ensure that the safety requirements are complete and consistent with the system safety requirements, and that the safety integrity requirements for those functions are correctly assigned. The aim is also to ensure that the design meets the safety requirements the safety functions are correctly implemented and the implemented system is safe.

5.2.3.5 Assessment Report
The assessment report should provide detailed reasons why the product(s) and processes were accepted or rejected and is essentially an assessment results.

5.3 Assessment Criteria for Vital Computer

Various aspects of the computer validation require the implementation of an assessment activity in order to verify that all safety measures have been taken to ensure the safe operation of the digital architecture. Those aspects can be classified as follows: Life-cycle plans; Requirements; Design; Validation and Off-line Testing; Fault and Failure Analyses; Operation, Maintenance and Support.

5.3.1 Basic criteria
The basic criteria are presented in the form of process and product properties. They state the requirements for the life-cycle processes and products, where each requirement is devised to address a specific set of hazards. These requirements will in general be satisfied by using the relevant techniques and measures recommended by the safety critical standards. Therefore, with each set of basic criteria, a table of relevant techniques and measures is attached. These tables also identify the objects to which they apply. The

basic assessment criteria have been categorized by process and are presented in this document in the following sections:

- Section 2.4: Life-cycle plans;
- Section 2.5: Requirements;
- Section 2.6: Design;
- Section 2.7: Validation and Off-line Testing;
- Section 2.8: Fault and Failure Analyses;
- Section 2.9: Operation, Maintenance and Support.

5.3.1.1 Lifecycle Plans

A well-structured lifecycle plans are essential for ensuring the product integrity of digital architectures. Suitable lifecycle frameworks have been described in safety critical standards, EN50129 and IEC150. The structure and activities of the product lifecycle shall provide a systematic approach to the development, production, support and maintenance of the product. The activities required to identify, control or eliminate hazards at each lifecyle phase shall be described. A structured plan of these activities constitutes the safety plan.

5.3.1.1.1 Basic Criteria

(1) The lifecycle plans shall cover all development phases and describe the processes used to ensure the quality, reliability, maintainability and integrity of the products.

(2) The lifecycle plans shall identify all the resources to be used and their essential qualities, such as the designers and their competence, tools and their reliability, validation teams and their independence.

(3) Each development phase shall precisely specify:

- the inputs, information and resources required to carry-out the activity;
- summary of the processes;
- its successful termination conditions;
- its outputs.

(4) All development activities shall be covered by an appropriate safety plan. The safety plan should have the approval of the supplier's project manager and the supplier's internal independent safety organisation.

(5) In particular, the safety plan shall be compliant with the standards Safety Plan Requirements [11]. All lifecycle activities shall be audited for compliance with the safety plan.

(6) The supplier shall produce the safety case of the computer which shall be compliant with the standards [11].

(7) The life cycle plans should cover the following plans:

- Development plan,
- Safety plan,
- Quality plan including:
    - *Configuration and management plan,*
    - *Maintenance plan,*
    - *Manufacturing plan.*

(8) The techniques and measures, equivalent to those recommended by the standards, EN50129 and IEC1508 shall be used to prepare and implement a lifecycle plan. Variance from the recommendation of these standards should be fully described and justified.

The techniques and measures from the standards which are applicable to life-cycle processes and products, are listed in Table 5.1. This list is not complete. It is important to note that SIL 4 computer will need a combination of techniques and measures with which to provide a very high degree of protection against any identified hazard. For instance, a SIL 4 computer safety planning process procedure would need to use a combination of several techniques and measurers, such as checklist, audit and document review.

Activity and Object	Technique and Measure	Standard Reference
Safety Planning and Quality Assurance	• Checklist • Audit • Document Inspection and walk-through of the Specifications • Review after safety plan change • Review after each life cycle phase	EN50129, E.1
Resource Qualities	• Repetitive and regular Staff Training • Completely independent designers, validators and assessor • Highly qualified and experienced staff	EN50129, E.3
Project Management	• Definitions of tasks and responsibilities • consistency procedures after modification • configuration management • monitoring and control of project status.	IEC1508, I 7
Documentation	•Guidelines for organization scheme. • Checklists for contents, unique form, on-line documents, formalised revision, interface description, environment studies, modification and maintenance procedures, manufacturing and application documents.	IEC1508, I 7, G.2 EN50129, E.8
Construction	• Use well tried and approved components	IEC1508, I 7
Testing and Validation	• Black-box testing from cause-consequence diagram, boundary value cases • Statistical testing - realistic distribution of input data and assumed failure modes • Proven by use	IEC1508, I 7
Manufacturing	•Requirements, precautions and audit plan of actual manufacturing process by safety organization	EN50129, E.9
Installation and Maintenance	•Requirements, precautions and audit plan of actual installation and maintenance processes by safety organisation	EN50129, E.9

Table 5.1. Safety Life Cycle Techniques and Measures for SIL 4 Safety Critical Digital Architectures

5.3.2 Requirements

A systematic approach to requirements development is essential to ensure high integrity. The functionality and integrity, reliability and performance requirements of the computer are specified. The functionality and integrity, reliability and performance requirements of the computer are specified. The desired design features, such as protection against some

specific component faults or target time for fault detection, are regarded as an integral part of requirements.

5.3.2.1 BASIC CRITERIA

(1) The approach for identifying detailed requirements shall be described. This should include procedures for:

- decomposition of system level requirements to lower level requirements specifications;
- verifying the consistency of requirements;
- tracing their relationships to the design objects, components and code;
- providing traceability to test specification to enable testing of each requirements to validate the systems;
- change control.

(2) facility to install application programs. The safety critical digital computershall meet the SIL 4.

(3) The safety critical digital computer shall provide the following functionality:

- implementation of requirements derived from mitigation or elimination of hazard identified for the range of perceived applications of the architecture;
- execution of application programs;
- collection of inputs and delivery of outputs;
- detection and negation of faults;
- provision of timer and watchdog functions;
- fail-safe inputs and outputs.

(4) All credible failure modes for each hardware and software element of the computer shall be identified.

(5) The hardware components shall be able to perform the safety function in the presence of two faults [IEC1508 part 2 table 5.2].

(6) Faults shall be detected with on-line, high diagnostic coverage [IEC1508 part 2 table 5.2]. A fail-safe computer very much depends on the effectiveness of its fault detection measures, it may not need any on-line diagnostics. However, a fail-operational computer needs detailed on-line diagnostic coverage to achieve its integrity and reliability, because without this it is very difficult to implement any recovery mechanism.

(7) Undetected hazardous faults shall be detected by the (off-line) proof checks [IEC1508 part 2 table 5.2].

(8) The safety requirements shall consider Human factor issues, reliability of the operators, information overloading, operator errors, etc.

5.3.3 Design

Digital architectures are designed to reduce random and systematic credible faults to an acceptable level by using appropriate techniques and measures. The design describes all the elements of the architecture, their interrelationships and interfaces, and their role in fulfilling the requirements. The techniques and measures used to achieve the design goal are also explained.

5.3.3.1 BASIC CRITERIA

(1) The procedures used to derive the design from the requirements and to verify the design against the requirements shall be described.

(2) The computershall be designed to minimise the credible faults by using a combination of well tried and well defined fault avoidance and fault tolerant measures.

(3) The design specification shall identify the components and modules of the architecture, and describe their functional and other characteristics (such as their integrity levels, failure rates, performance). It shall also describe interfaces, internally and with external equipment.

(4) The failure modes of all the following components shall be identified along with the techniques and measures used to eliminate or mitigate the hazards arising from such failures:

- main processor, co-processors and micro-controllers;
- watchdog and clock;
- I/O cards, data path and field bus;
- communication network;
- operating system or executive program.

(5) A quantitative estimate of the reliability of the overall computer (for the worst case scenarios) shall be presented. The process, procedures and standards on which these are based shall form part of this presentation.

(6) The design of the computers hall ensure that higher integrity level modules are not affected by lower integrity level modules. Appropriate analyses shall be used to justify this.

(7) The design shall ensure that the computer operate correctly in all foreseeable environmental conditions, such as EMC, noise, heat, etc. The envelop for the environmental conditions and requirements shall be defined in the requirements specification.

(8) All software components of the computers hall conform to EN50128 norms and the relevant GAM principles [12,4,13]. The software shall be developed to SIL 4. The detailed software assessment criteria are given in [12].

Activity and Object	**Technique and Measure**	**Ref.**
Architectu re	• Dual digital channels based on composite fail-safety with fail-safe comparison • Single digital channel based on inherent fail-safety • Single digital channel based on reactive fail-safety • Diverse digital channels with fail-safe comparison • Justification of the computer by quantitative reliability analysis of the hardware	EN50129 E.4
Processin g Units	• Comparator • Majority voting • Self-test by software (single channel only) • Self-test by hardware (single channel only) • Coded processing (single channel only) • Reciprocal comparison by software	IEC1508 2B
Invariable memory ranges	• Signature of a double word (16 bit) • Block replication	IEC1508 2B
Variable memory ranges	• Galpat or transparent Galpat test • Abraham test Double RAM with hardware or software comparison and read/write test	IEC1508 2B
I/O units and interfaces	• Test pattern • Code protection • Multi-channelled parallel output • Monitored outputs • Input comparison	IEC1508 2B
Data paths	• Complete hardware redundancy • Inspection using test patterns • Transmission protocol • Transmission redundancy • Information redundancy	IEC1508 2B

Activity and Object	**Technique and Measure**	**Ref.**
Power supply	• Overvoltage protection with shut-off • Voltage control (secondary) • Power-down with shut-off • Graceful degradation	IEC1508 2B
Watchdog	• Separate time basis and time-window • Combination of temporal and logical monitoring of program sequence • Temporal monitoring with on-line check	IEC1508 2B
Clock	• Reciprocal comparison in redundant configuration • Dual frequency timer	
Communication	• Separation of electrical energy from communication lines • Spatial separation in redundant lines • Increase of interference immunity • Antivalent signal transmission	
Input and Output cards	• Idle current principle • Test pattern • Electrical interlocking • Cross-monitoring of redundant units	
Software Components	• Techniques and measures recommended by EN50128 and IEC1508 part 3	EN50128 IEC1508-3

Table 5.2. Design - Techniques and Measures for SIL 4 Safety Critical Digital Architectures

5.3.4 Validation and Off-Line Testing

Validation of architectures against their requirements and dynamic off-line testing of their elements and assemblies are essential to ensure their integrity and reliability. Validation and testing processes are also immensely valuable for fault detection and removal, and for fault forecasting. A well-structured validation and test plan is required. This plan shall describe all the activities from test environment set-up and test scenario selection to test execution and analysis of the test results. It also describes test organization, test processes and test documentation. The test specifications, acceptance criteria and test results form an essential part of evidence of safety.

5.3.4.1 BASIC CRITERIA

(1) The plan shall define the validation test process by:

- identifying the requirements specification against which the validation test is based;
- identifying the different test phases including unit, integration and requirements testing;
- specifying the test organisation and their responsibilities;
- describing the testing procedures, e.g. fault injection, statistical testing method, or regression testing;
- identifying the test environment and their required integrity and quality requirements.

(2) Procedures to ensure and demonstrate independence of test from the design and integration activities shall be defined. Such procedures shall describe, explicitly, requirements for independence of groups of personnel.

(3) Each test phase shall accompany a test specification describing the test objectives, test scenarios, configuration data, and acceptance criteria.

(4) The SIL 4 test techniques and measures (see Table 2.1), recommended by the standards, shall be used.

(5) The test results shall record the frequency of tests, fault detection success rate, coverage and mean detection times.

(6) The test results shall be analysed to give quantitative estimates of the hidden faults, and their effects on reliability estimates.

(7) The Assessor shall witness a representative sample of tests to ensure that the test procedures have been correctly implemented.

(8) The test specification shall cover all credible failure modes.

5.3.5 Fault and Failure Analysis

An independent fault and failure analysis of the digital computers hall show that the computer has been thoroughly analyzed to ensure that all credible faults are identified, the fault control methods are effective, and the residual faults are non-hazardous. The analyses should be carried out as detailed in the safety plan. Their application, procedures and scope of analysis should be explained. The main finding of the analysis should be available for examination.

5.3.5.1 BASIC CRITERIA

(1) The analyses shall be planned and performed in a timely manner, so that their findings are effectively used in the development process.

(2) Review and incorporation of the finding of the analyses shall be part of a formal implementation process.

(3) The analyses shall identify all credible failure modes, estimate their criticality and frequency of occurrence.

(4) The types of failures considered shall be specified. They shall cover as far as possible all static and intermittent failures, combination of failure modes, hazardous and safe failures, and latent and undisclosed failure modes.

(5) The results and findings of the analyses shall be integrated in the safety case of the architecture, they shall form the core of the safety argument, evidence to support functional and technical safety.

(6) The faults arising from the following sources shall be considered:

- hardware and software and their interactions;
- environmental factors, e.g. EMC;
- network elements and data and field buses;
- operators and operating conditions;
- critical operations including start up and close-down.

5.3.6 OPERATION, MAINTENANCE AND SUPPORT

A digital computer is a "product", primarily designed to be used as a platform for delivering safety critical applications. To fulfill this aim, it must be supported with an adequate, operation and maintenance program. The objective of the overall operation and maintenance is to operate and maintain the safety architecture, its control system and the total combination of safety-related systems and external risk reduction facilities such that the designed functional safety is maintained. User manual, maintenance manual, and user support must be provided.

5.3.6.1 BASIC CRITERIA

(1) There shall be a maintenance plan for the product which should include collection of field data. Inspection and off-line tests shall be performed at regular interval.
(2) A support service plan shall specify support organisation, its responsibilities and policies. The support procedure shall explain the mechanisms used for fault reporting and incorporating new releases.
(3) Safety operation procedures, inspection and maintenance procedures shall be formulated and defined in a way that ensures safety and minimises operator errors. All relevant issues from the hazard and safety analyses shall be addressed.
(4) The digital components shall be kept as simple as possible to respect the limits of the human capacity. Appropriate metrics may be used to assess the relative complexity of these components.
(5) Data-driven systems (including parametric or configurable systems) shall be protected against possible errors arising from entry of incorrect data.
(6) The control devices and means of surveillance shall be such that additional hazards due to operator error are remote.
(7) There shall be a well-specified procedure for collecting and analysing the product's history of use data.

6.0 Human-Machine Interface (HMI) Issues in AVCSS

In the scope of the project, there is a task that involves the evaluation of driver behaviors and the safety complications in the use of AVCSS, such as Frontal Collision Warning and Frontal Collision Avoidance Systems. The studies of human factors and related HMI issues are very far-reaching. They involve a wide range of aspects and a thorough evaluation for them all is beyond the scope of this project. The purpose of this section is to suggest a study plan and an outline for the task within the project, which will be used as guidelines in conducting the associated studies in the next phase.

Several areas deserve to be investigated with respect to driver behaviors and system safety.

6.1 Develop criteria and MOEs for evaluating the effectiveness of FCWS/FCAS on driver

Current development of FCWS/AC is being conducted separately by research and industrial entities. In the context of safety verification and certification, there is a need for a set of evaluation criteria and Measure of Effectiveness (MOE) for evaluating the FCWS. The criteria and MOEs will deal with specification and evaluation of key driving parameters such as driver reaction time, change for normal driving behavior and safety impacts.

6.2 Understand needs and impacts on drivers and on the system:

(1) Communication needs between a driver and the subject system: This refers to the exchange of information between a vehicle driver and FCWS or FCAS/AS. For example, a display or an interface is typically used to convey the state of or a signal generated by the system. Since the display dictates the effectiveness of communication, there ought to be guidelines for the design of such human-human-machine interfaces (HMI). The issues pertaining to FCWS or FCAS are:

- What information should be provided to the driver?
- In what formats should the information be presented?
- How effective are the presented information for the benefits of safety?
- What kinds of inputs can the driver feed into the system?
- Through what channels can the driver provide inputs to the system?
- Does the driver input affect the safety performance of the system?
- What are the methods or procedures can be established to provide answers to these questions?

(2) Behavior changes of the driver induced by the subject system: With the introduction of a device previously not existent in a vehicle, drivers' attention may be drawn or drivers' response to traffic conditions may be altered. The problems of interest are:

- To what degree does a driver depend on the judgment of the subject system? Will a driver tend to rely heavily on it or attempt to disable it?

- What changes in driving behaviors will develop, if a driver accepts and rely on the subject system?
- Can the change in driver behaviors result in feedback into the system, thus leading to safety issues?
- What are the methods or procedures can be established to evaluate these situations?

(3) Intervention by drivers in extraordinary or abnormal driving conditions: Since driver-assistance systems are in discussions here, it is reasonable to expect that there are situations when driver actions are expected. Furthermore, driver intervention can also occur when the system does not require it. Therefore, several questions arise:

- What conditions may lead to unsafe consequences when a driver intervenes?
- What types of safety guards can be implemented to discourage intervention from a driver if potential hazards exist?
- What conditions may lead to hazardous situations without timely response from a driver?
- What types of safety guards can be implemented to induce or enable a driver to react properly to intervene?
- What methods or procedures can be established to evaluate these issues?

(3) Impact due to False Alarm vs. miss: With an understanding of the fact that any FCWS/AS system will be designed with a tradeoff between false alarm and miss, there is a need for a general assessment of how the frequency of false alarm and miss will impact the normal driving behavior and the effectiveness of the collision warning/avoidance function. Furthermore, it is necessary to assess whether the impact on driving behavior and safety is related to the means for displaying the warning information (e.g., visual vs. audible).

6.3 Develop verification and certification approaches: The final product of this task in the context of the evaluation and certification of FCWS/AS.

We would like to develop verification/certification approached through which tests can be conducted by different developer/evaluator and the results can be compared and evaluated.

7.0 CONCLUSION

AVCSS are becoming popular with the introduction of driver-assistance functions, such as adaptive cruise control. AVCSS will also become increasingly important in the future as efforts are devoted toward further automation of driving functions for safety purposes.

The topic covered in this project is a critical element in the development and implementation of AVCSS. In this report, we gave a summary of the approach in conducting the preliminary safety analysis of a safety-critical system in order to identify the safety measures to be implemented in the system. Using frontal collision avoidance systems as a case study among AVCSS, the procedures and methodologies for pursuing a vigorous assessment of safety issues were presented. The functional description of the system is the starting point for further considerations. The analysis of the risk leads to a set of safety measures, which have to satisfy the safety requirements. If the safety measures chosen from the standard are applied properly, then the system can be considered safe according to the standard used. Applying the chosen safety measures in the system, the designer needs much more information about these measures than he can find in the standards. The knowledge of the state of the art in safety technology of the application area in question, and the experience of the designer provide further important information.

The assessment and certification of a safety-vital system requires a detailed and well-defined plan. The procedures must be strictly followed and the validation carefully executed. This report uses an example to describe the process involved in such assessment and the criteria and the rules that typically represent the types of safety measures to be investigated. The process can be complicated, since it involves the evaluation of various aspects and demands. However, the approach should be followed to ensure safety measures are met in the deployment of the subject system. INRETS and PATH expect to continue the endeavor for continual pursuits of AVCSS safety by combining the expertise in computerized modern systems and transportation research from both organizations.

REFERENCES

[1] E.M.El koursi, Ching-Yao Chan and Wei-bin Zhang “Preliminary Hazard analnyses : A case study of advanced Vehicle control and safety system”, IEEE, SMC’99, TOKYO, Japan, 12 –15, October 1999, Volume 1V, pp 558- 563.
[2] CENELEC prEN 50126, “Railway Applications Dependability for Guided Transport Systems”, June 1997.
[3] CENELEC prR009-004, “Railway applications, Systematic Allocation of Safety Integrity Requirements”, March 1999.
[4] El Koursi and al, “Generalised Assessment method (GAM) : Part 2 Guidelines”, - ESPRIT 9032 - CASCADE Project , 10 January 1997, INRETS-Lille.

[5] CENELEC prEN 50129, “Railway Applications - Safety related Electronic Systems for Signalling”, Version 1.0, January 1997.
[6] CENELEC prEN 50128, “Railway Applications - Software For Railway Control And Protection Systems” ,January 1997.
[7] AIC Conference, “Risk Management in Railway Environment”, Workshop, London, 15_16 October 1998.
[8] P. Varaiya, S. Shladover, “Sketch of an IVHS System Architecture, “ PATH Research Report, UCB-ITS-PRR-91-03, October 1990.
[9] E.M. El Koursi, C.Y.Chan and W.B Zhang, “Preliminary Safety Analysis of Frontal Collision Avoidance”, IEEE, Intelligent Transportation Systems, Dearborn, USA, October 1-3 2000.
[10] Deliverable 3: The proposed assessment and certification methodology for digital architectures. 12 June 1998. Doc. ID : ACRuDA/WP2/D3/V2.
[11] Deliverable 2: State of the Art - Method Synthesis. 29 September 1997. Doc. ID : ACRuDA/INRETS/PM-MK/WP1/D2/97.39/V3.
[12] S.Mitra and all, Generalised Assessment Method (GAM) - Part 1 : Rules - ESPRIT 9032 - CASCADE Project - version 1.0 - 17 January, 1997, INRETS-Lille.
[13] M. Elkoursi and all, Generalised Assessment method (GAM) : Part 3 Examples, - ESPRIT 9032 - CASCADE Project , 24 January 1997, INRETS-Lille.

APPENDIX

FAILURE MODE EFFECT AND CRITICALITY ANALYSIS FOR FCWS & FCAS

Sensing

Function	Output	Failure	Effects	Hazard (potential danger)	Necessary Condition	Severity	Dangerous Situation
Range Sensing	Distance between two vehicles	No detection	No automated control and Excessive delta V	Severe frontal collision, leading to chain accidents	Obstacle ahead, no driver action, and congested traffic	Catastrophic	No detection by range sensor
			No automated control	Moderate frontal collision	Obstacle ahead and driver action not in time	Critical	No detection by range sensor
			No automated control	Minor frontal collision	Obstacle very small	Marginal	No detection by range sensor
			No automated control	Near-miss frontal collision	Obstacle ahead and driver action in time	Marginal	No detection by range sensor
			No automated control	No collision	Obstacle moves away	Negligible	
		False detection	Automated controlled braking	Rear end collision	Vehicle following behind closely	Moderate	False detection by range sensor
			Automated controlled stops	No collision	No vehicle behind closely	Negligible	False detection by range sensor
			Driver braking due to warning	Rear end collision	Vehicle following behind closely	Moderate	False detection by range sensor
			Driver braking due to warning	No collision	No vehicle behind closely	Negligible	
		Inter-mediate detection, becoming no detection	No automated control	Moderate frontal collision	Obstacle ahead and driver action not in time	Critical	Intermediate detection, becoming no detection
			No automated	Minor frontal	Obstacle very small	Marginal	Intermediate detection,

			control	collision			becoming no detection
			No automated control	Near-miss frontal collision	Obstacle ahead and driver action in time	Marginal	Intermediate detection, becoming no detection
			No automated control	No collision	Obstacle moves away	Negligible	
		Inter-mediate detection, becoming false detection	Automated controlled braking	Rear end collision	Vehicle following behind closely	Moderate	Intermediate detection, becoming false detection
			Automated controlled stops	No collision	No vehicle behind closely	Negligible	Intermediate detection, becoming false detection
			Driver braking due to warning	Rear end collision	Vehicle following behind closely	Moderate	Intermediate detection, becoming false detection
			Driver braking due to warning	No collision	No vehicle behind closely	Negligible	
		Over-measuring range	No automated control	Moderate frontal collision	Obstacle ahead and driver action not in time	Critical	Over-measuring range
			No automated control	Minor frontal collision	Obstacle very small	Marginal	Over-measuring range
			No automated control	Near-miss frontal collision	Obstacle ahead and driver action in time	Marginal	Over-measuring range
			No automated control	No collision	Obstacle moves away	Negligible	
		Under-measuring range	Automated controlled braking	Rear end collision	Vehicle following behind closely	Moderate	False detection by range sensor
			Automated controlled stops	No collision	No vehicle behind closely	Negligible	False detection by range sensor
			Driver braking due to warning	Rear end collision	Vehicle following behind closely	Moderate	False detection by range sensor
			Driver braking due	No collision	No vehicle behind	Negligible	

			to warning		closely		
Range Rate Sensing	Relative speed to obstacle in front	Over-estimating range rate	Automated controlled braking	Rear end collision	Vehicle following behind closely	Moderate	Over-estimating range rate
			Automated controlled stops	No collision	No vehicle behind closely	Negligible	Over-estimating range rate
			Driver braking due to warning	Rear end collision	Vehicle following behind closely	Moderate	Over-estimating range rate
			Driver braking due to warning	No collision	No vehicle behind closely	Negligible	
		Under-estimating range rate	No automated control	Moderate frontal collision	Obstacle ahead and driver action not in time	Critical	Over-measuring range
			No automated control	Minor frontal collision	Obstacle very small	Marginal	Over-measuring range
			No automated control	Near-miss frontal collision	Obstacle ahead and driver action in time	Marginal	Over-measuring range
			No automated control	No collision	Obstacle moves away	Negligible	
Speed Sensing	Vehicle speed	No measured speed	Vehicle disabled	Collision when vehicle stops	Other vehicles can not avoid	Critical	No measured speed
			Vehicle disabled	No collision when vehicle stops	No traffic	Marginal	No measured speed
			Vehicle disabled	Driver takeovers	Driver alert and react timely	Marginal	No measured speed
		Over-estimating speed	Automated controlled braking	Rear end collision	Vehicle following behind closely	Moderate	Over-estimating speed
			Automated controlled stops	No collision	No vehicle behind closely	Negligible	Over-estimating speed
			Driver braking due to warning	Rear end collision	Vehicle following behind closely	Moderate	Over-estimating speed
			Driver braking due to warning	No collision	No vehicle behind closely	Negligible	
		Under-	No	Moderate	Obstacle	Critical	Under-

		estimating speed	automated control	frontal collision	ahead and driver action not in time		estimating speed
			No automated control	Minor frontal collision	Obstacle very small	Marginal	Under-estimating speed
			No automated control	Near-miss frontal collision	Obstacle ahead and driver action in time	Marginal	Under-estimating speed
			No automated control	No collision	Obstacle moves away	Negligible	
Accelerati on sensing	Vehicle acceleratio n	No measured accel.	Vehicle disabled	Collision when vehicle stops	Other vehicles can not avoid	Critical	No measured accel.
			Vehicle disabled	No collision when vehicle stops	No traffic	Marginal	No measured accel.
			Vehicle disabled	Driver takeovers	Driver alert and react timely	Marginal	No measured accel.
		Over-estimating Accel.	Automated controlled braking	Rear end collision	Vehicle following behind closely	Moderate	Over-estimating Accel.
			Automated controlled stops	No collision	No vehicle behind closely	Negligible	Over-estimating Accel.
			Driver braking due to warning	Rear end collision	Vehicle following behind closely	Moderate	Over-estimating Accel.
			Driver braking due to warning	No collision	No vehicle behind closely	Negligible	
		Under-estimating Accel.	No automated control	Moderate frontal collision	Obstacle ahead and driver action not in time	Critical	Under-estimating Accel.
			No automated control	Minor frontal collision	Obstacle very small	Marginal	Under-estimating Accel.
			No automated control	Near-miss frontal collision	Obstacle ahead and driver action in time	Marginal	Under-estimating Accel.
			No automated control	No collision	Obstacle moves away	Negligible	
Throttle Angle Sensing	Throttle position	Under-estimating throttle	Excessive acceleration	Minor frontal collision	Obstacle ahead and no driver	Critical	Under-estimating throttle

		opening			action		opening
			Excessive acceleration	No collision, passenger discomfort	No obstacle	Marginal	Under-estimating throttle opening
		Over-estimating throttle opening	Insufficient acceleration	Minor rear-end collision	Vehicle behind closely	Critical	Over-estimating throttle opening
			Insufficient acceleration	Slow movement	No traffic	Marginal	Over-estimating throttle opening
Brake Line Pressure Sensing	Bake Hydraulic Pressure	No measured pressure	Vehicle disabled	Collision when vehicle stops	Other vehicles can not avoid	Critical	No measured pressure
			Vehicle disabled	No collision when vehicle stops	No traffic	Marginal	No measured pressure
			Vehicle disabled	Driver takeovers	Driver alert and react timely	Marginal	No measured pressure
		Under-estimating pressure	Excessive command on braking	Rear-end collision	Vehicle close behind	Critical	Under-measuring pressure
			Excessive command of braking	No collision, passenger discomfort	No traffic behind	Marginal	Under-measuring pressure
		Over-estimating pressure	Insufficient deceleration	Moderate front collision	Vehicle ahead and no driver action	Critical	Over-estimating pressure
			Insufficient deceleration	Near-miss collision	Vehicle ahead, but driver action in time	Marginal	Over-estimating pressure
			Insufficient deceleration	No collision	No traffic	Negligible	Over-estimating pressure
Wheel-Torque Sensing	Wheel torque	No measured Wheel torque	Excessive command on braking	Rear-end collision	Vehicle close behind	Critical	No measured torque
			Excessive command of braking	No collision, passenger discomfort	No traffic behind	Marginal	No measured torque
			Insufficient deceleration	Moderate front collision	Vehicle ahead and no driver action	Critical	No measured torque
			Insufficient deceleration	Near-miss collision	Vehicle ahead, but driver action	Marginal	No measured torque

					in time		
			Insufficient deceleration	No collision	No traffic	Negligible	
		Under-estimating wheel torque	Excessive command on braking	Rear-end collision	Vehicle close behind	Critical	Under-measuring wheel torque
			Excessive command of braking	No collision, passenger discomfort	No traffic behind	Marginal	Under-measuring wheel torque
		Over-estimating wheel torque	Insufficient deceleration	Moderate front collision	Vehicle ahead and no driver action	Critical	Over-estimating wheel torque
			Insufficient deceleration	Near-miss collision	Vehicle ahead, but driver action in time	Marginal	Over-estimating wheel torque
			Insufficient deceleration	No collision	No traffic	Negligible	

Processing

Function	Output	Failure	Effects	Hazard (potential danger)	Necessary Condition	Severity	Dangerous Situation
Obstacle detection processing	Obstacle position	Missed detection	No deceleration	Severe Collision with obstacle	Obstacle ahead and no driver action	Critical	Missed obstacle detection
			Delayed deceleration	Minor collision	Obstacle ahead and driver takes action	Critical	Missed obstacle detection
			Delayed deceleration	Near-miss	Obstacle ahead and driver takes action	Marginal	Missed obstacle detection
			Delayed deceleration	No collision	Obstacle moves away in time	Negligible	
		Over-estimating distance	Insufficient deceleration	Collision with obstacle	Obstacle ahead and no driver action	Critical	Over-estimating distance
			Insufficient deceleration	Minor collision	Obstacle ahead and driver takes action	Critical	Over-estimating distance
			Insufficient deceleration	Near-miss	Obstacle ahead and driver takes action	Marginal	Over-estimating distance
			Insufficient	No collision	Obstacle	Negligible	

			deceleration		moves away in time		
		Under-estimating distance	Excessive command on braking	Rear-end collision	Vehicle close behind	Critical	Under-estimating distance
			Excessive command of braking	No collision, passenger discomfort	No traffic behind	Marginal	Under-estimating distance
	Obstacle speed	Missed Speed detection	No deceleration	Severe Collision with obstacle	Obstacle ahead and no driver action	Critical	Missed Speed detection
			Delayed deceleration	Minor collision	Obstacle ahead and driver takes action	Critical	Missed Speed detection
			Delayed deceleration	Near-miss	Obstacle ahead and driver takes action	Marginal	Missed speed detection
			Delayed deceleration	No collision	Obstacle moves away in time	Negligible	
		Over-estimating distance	Excessive command on braking	Rear-end collision	Vehicle close behind	Critical	Over-estimating distance
			Excessive command of braking	No collision, passenger discomfort	No traffic behind	Marginal	Over-estimating distance
		Under-estimating speed	Insufficient deceleration	Collision with obstacle	Obstacle ahead and no driver action	Critical	Under-estimating speed
			Insufficient deceleration	Minor collision	Obstacle ahead and driver takes action	Critical	Under-estimating speed
			Insufficient deceleration	Near-miss	Obstacle ahead and driver takes action	Marginal	Under-estimating speed
			Insufficient deceleration	No collision	Obstacle moves away in time	Negligible	
Vehicle state and fault processing	Vehicle state variables	No processed values	Vehicle disabled	Collision when vehicle stops	Other vehicles can not avoid	Critical	No measured variables
			Vehicle disabled	No collision when vehicle stops	No traffic	Marginal	No measured variables
			Vehicle disabled	Driver takeovers	Driver alert and react timely	Marginal	No measured variables

		Under-estimating vehicle speed	Insufficient deceleration	Moderate front collision	Vehicle ahead and no driver action	Critical	Under-estimating vehicle speed
			Insufficient deceleration	Near-miss collision	Vehicle ahead, but driver action in time	Marginal	Under-estimating vehicle speed
			Insufficient deceleration	Moderate front collision	Vehicle ahead and no driver action	Critical	Under-estimating vehicle speed
		Over-estimating vehicle speed	Excessive command on braking	Rear-end collision	Vehicle close behind	Critical	Over-estimating vehicle speed
			Excessive command of braking	No collision, passenger discomfort	No traffic behind	Marginal	Over-estimating pressure
Warning & display signal processing	Warning signals	No warning signal when needed	No action taken	Severe front-end Collision	Obstacle ahead	Catastrophic	Missing warning signal
			No action taken	Moderate front-end collision	Obstacle ahead	Critical	Missing warning signal
			Driver reacts in time despite no warning	No collision	Obstacle ahead, but driver reacts in time	Marginal	Missing warning signal
		Signal present when not needed	Driver panics and brakes hard	Rear-end collision	Traffic following close behind	Critical	False warning signal
			Driver panics and brakes hard	No collision	No traffic close behind	Marginal	False warning signal
			Driver ignores signal	No collision	No alert situations	Marginal	False warning signal
	Display (monitor) signals	No monitor signal	Driver stops vehicle	Vehicle disabled	No alert situation	Critical	Missing monitoring signal
			Driver ignores situation	Vehicle problems undetected	Problems emerge later	Negligible to Critical	Missing monitoring signal
		Monitor signal always on	Driver stops vehicle	Vehicle disabled	No alert situation	Critical	False monitoring signal
			Driver ignores situation	Vehicle problems undetected	Problems emerge later	Negligible to Critical	Missing monitoring signal
Accel. command	Accel. command	No Accel. command	Vehicle disabled	Collision when	Other vehicles can	Critical	No Accel. command

processing				vehicle stops	not avoid		
			Vehicle disabled	No collision when vehicle stops	No traffic	Marginal	No Accel. command
			Vehicle disabled	Driver takeovers	Driver alert and react timely	Marginal	No Accel. command
		Accel. command too high	Vehicle accelerates forward	Front end collision	Traffic close ahead	Critical	Accel. Command too high
			Vehicle accelerates forward	No collision	No traffic ahead	Marginal	Accel. Command too high
			Vehicle accelerates forward but driver reacts to brake	No collision	Traffic ahead	Marginal	Accel. Command too high
		Accel. command too low	Vehicle slows down to stop	Collision when vehicle stops	Vehicle speed lagging traffic	Critical	Accel. command too low
			Vehicle slows down	No collision	Vehicle late to destination	Marginal	Accel. command too low
			Vehicle slows down and disabled	No collision	Driver moves vehicle to roadside	Marginal	Accel. Command too low
Braking command processing	Braking command	No Braking command	Vehicle disabled	Collision when vehicle stops	Other vehicles can not avoid	Critical	No braking command
			Vehicle disabled	No collision when vehicle stops	No traffic	Marginal	No braking command
			Vehicle disabled	Driver takeovers	Driver alert and react timely	Marginal	No braking command
		Braking command too high	Brakes too hard	Rear end collision	Vehicle following behind closely	Moderate	Braking command too high
			Brakes too hard	No collision	No vehicle behind closely	Negligible	Braking command too high
		Braking command too low	Insufficient braking	Moderate frontal collision	Obstacle ahead and driver action not in time	Critical	Braking command too low
			Insufficient braking	Minor frontal	Obstacle very small	Marginal	Braking command

				collision			too low
			Insufficient braking	Near-miss frontal collision	Obstacle ahead and driver action in time	Marginal	Braking Command too low
			Insufficient braking	No collision	Obstacle moves away	Negligible	

Warning

Function	Output	Failure	Effects	Hazard (potential danger)	Necessary Condition	Severity	Dangerous Situation
Monitor status warning	Warning signals for status being monitored	Warning missing when warranted	Driver stops vehicle	Vehicle disabled	No alert situation	Critical	Missing monitoring signal
			Driver ignores situation	Vehicle problems undetected	Problems emerge later	Negligible to Critical	Missing monitoring signal
		Warning present when not needed	Driver stops vehicle	Vehicle disabled	No problematic situation	Critical	Missing monitoring signal
			Driver ignores situation	Vehicle problems undetected	Problems emerge later	Negligible to Critical	Missing monitoring signal
Control action warning	Warning signals for control actions	Warning missing when warranted	Drivers reacts without realizing system actions	Drivers causing additional hazards	Traffic situation varies	Negligible to Critical	Missing control action warning
			Drivers ignore absence of warning	No consequence	No problematic situation	Negligible	
		Warning present when not needed	Drivers reacts without realizing system actions	Drivers causing additional hazards	Traffic situation varies	Negligible to Critical	Missing control action warning
			Drivers ignore absence of warning	No consequence	No problematic situation	Negligible	
Warning for Driver action	Warnings signal for requesting driver actions	Warning missing when needed	No action taken	Severe front-end Collision	Obstacle ahead	Catastrophic	Missing warning signal
			No action taken	Moderate front-end	Obstacle ahead	Critical	Missing warning

				collision			signal
			Driver reacts in time despite no warning	No collision	Obstacle ahead, but driver reacts in time	Marginal	Missing warning signal
		Warning present when not needed	Driver panics and brakes hard	Rear-end collision	Traffic following close behind	Critical	False warning signal
			Driver panics and brakes hard	No collision	No traffic close behind	Marginal	False warning signal
			Driver ignores signal	No collision	No alert situations	Marginal	False warning signal

Actuation

Function	Output	Failure	Effects	Hazard (potential danger)	Necessary Condition	Severity	Dangerous Situation
Activate Accel. control system	Vehicle accel. At desired level	No Accel. command	Vehicle disabled	Collision when vehicle stops	Other vehicles can not avoid	Critical	No Accel. command
			Vehicle disabled	No collision when vehicle stops	No traffic	Marginal	No Accel. command
			Vehicle disabled	Driver takeovers	Driver alert and react timely	Marginal	No Accel. command
		Accel. command too high	Vehicle accelerates forward	Front end collision	Traffic close ahead	Critical	Accel. Command too high
			Vehicle accelerates forward	No collision	No traffic ahead	Marginal	Accel. Command too high
			Vehicle accelerates forward but driver reacts to brake	No collision	Traffic ahead	Marginal	Accel. Command too high
		Accel. command too low	Vehicle slows down to stop	Collision when vehicle stops	Vehicle speed lagging traffic	Critical	Accel. command too low
			Vehicle slows down	No collision	Vehicle late to destination	Marginal	Accel. command too low
			Vehicle slows down and disabled	No collision	Driver moves vehicle to roadside	Marginal	Accel. Command too low
Activate	Vehicle	No	Vehicle	Collision	Other	Critical	No braking

braking control system	braking at desired levels	Braking command	disabled	when vehicle stops	vehicles can not avoid		command
			Vehicle disabled	No collision when vehicle stops	No traffic	Marginal	No braking command
			Vehicle disabled	Driver takeovers	Driver alert and react timely	Marginal	No braking command
		Braking command too high	Brakes too hard	Rear end collision	Vehicle following behind closely	Moderate	Braking command too high
			Brakes too hard	No collision	No vehicle behind closely	Negligible	Braking command too high
		Braking command too low	Insufficient braking	Moderate frontal collision	Obstacle ahead and driver action not in time	Critical	Braking command too low
			Insufficient braking	Minor frontal collision	Obstacle very small	Marginal	Braking command too low
			Insufficient braking	Near-miss frontal collision	Obstacle ahead and driver action in time	Marginal	Braking Command too low
			Insufficient braking	No collision	Obstacle moves away	Negligible	

Networking

Function	Output	Failure	Effects	Hazard (potential danger)	Necessary Condition	Severity	Dangerous Situation
Comm. Between processor and sensors	Sensing signals and data for processing	No Sensing signal	(SEE Sensing Section)				
		Signal too high	(SEE Sensing Section)				
		Signal too low	(SEE Sensing Section)				
Comm. Between processor and display	Signals and data for display	No display signal	(SEE warning section)				
		Signal missing when	(SEE warning section)				

		needed					
		Signal present when not needed	(SEE warning section)				
Comm. Between processor and actuators	Signals to activate control	No Actuation signal	(SEE actuation section)				
		Actuation signal too high	(SEE actuation section)				
		Actuation signal too low	(SEE actuation section)				
Comm. backbone	Signals to and from units	Network shutdown	Vehicles disabled	(SEE similar sections)		Critical	Comm. Network shutdown