

DESIGN METHODS OF
SAFETY-CRITICAL SYSTEMS
AND THEIR APPLICATION IN
ELECTRONIC BRAKE SYSTEMS

PH. D. THESIS
by
Tímea Fülep

Supervisor
László Palkovics, D.Sc.

Kandó Kálmán Doctoral School for Multidisciplinary Sciences
Science of Vehicles and Mobile Machines

Budapest University of Technology and Economics
2007

CONTENTS

1.	ABSTRACT	4
2.	DECLARATION.....	6
3.	ACKNOWLEDGEMENTS	7
4.	INTRODUCTION.....	8
5.	MOTIVATION	10
5.1	Reliability history	10
5.2	Reliability measurement.....	12
5.3	Design reliability	17
6.	STATE-OF-THE-ART IN SAFETY-CRITICAL SYSTEMS	23
6.1	Legislation	23
6.1.1	<i>Safety-related systems</i>	24
6.2	Safety-critical system in avionics.....	28
6.2.1	<i>Requirements in avionics</i>	30
6.3	Railway regulation and standardization	32
6.4	Application of qualitative risk assessment in electronic brake system	34
6.5	Legislation status of the electronic stability control.....	37
6.5.1	<i>Overview of the world-wide status of the ESC systems</i>	38
6.5.2	<i>Regulation of ESC in the UN-ECE legislation framework</i>	39
7.	STATE-OF-THE-ART ARCHITECTURES IN ROAD VEHICLES.....	45
7.1	Analogy between road vehicles and avionics systems	47
7.2	Brake system architectures of heavy commercial vehicle.....	51
7.2.1	<i>Safety considerations of specific brake-by-wire architectures</i>	53
8.	SPECIAL APPLICATION OF A DESIGN METHOD FOR REDUNDANT ELECTRONIC BRAKE SYSTEM.....	57
8.1	Overview of design techniques	57
8.2	Qualitative reliability Analysis in the concept design phase.....	59
8.2.1	<i>Ranking considerations</i>	65
8.2.2	<i>Applicability for software failures</i>	66
8.2.3	<i>Systematic set up of system structure and function</i>	68

8.3	Analysis of redundant electronic semi-trailer brake system	70
	8.3.1 <i>Reliability considerations</i>	70
	8.3.2 <i>Safety in design</i>	71
	8.3.3 <i>System and function structure</i>	74
	8.3.4 <i>Evaluation phase</i>	78
	8.3.5 <i>Results</i>	79
8.4	Complex approach to qualitative and quantitative design techniques.....	81
	8.4.1 <i>Considerations of complex methodology based on structure and</i> <i>function matrix foundation</i>	85
9.	CONCLUSIONS	87
9.1	Theses	87
10.	PUBLICATIONS.....	91
11.	REFERENCES.....	93

1. ABSTRACT

The traffic volume even it is already dense will increase further in the next years. As a result also the number of accidents will increase, and traffic efficiency and traffic flow will suffer. Trucks are involved over proportionally in the accident numbers.

Stand alone safety systems – ABS (Anti-lock Braking System), airbag, ESP (Electronic Stability Program) – are distributed functions inside a vehicle, which communicate with each other, but not strongly integrated at the moment. Furthermore functions like steering and braking are not yet fully electronically controlled. There is still conventional mechanical [124, 125] actuator control in use, resulting in a lack of safety potential.

It is important to substantially improve overall traffic safety and traffic efficiency for heavy goods vehicles by the integration of intelligent technologies into an intelligent, a fully electronically controlled power train. As part of the power train a brake-by-wire architecture has been being developed with predetermined redundancy level.

The development of these safety-critical systems is mainly driven by that social demand, that the societies wants to see safer, more reliable vehicles on the roads, which can also handle more complex situations than the human driver can.

The evolution of the heavy goods vehicle braking systems tends towards that the pneumatic and mechanic back-up systems are fading away and both the customer and the related safety requirements are fulfilled by electronic and electro-mechanic systems not just because of lower component and installation cost but increased availability.

Parallel to the fact that the expected lifetime of commercial vehicles has significantly increased in the last few years, reliability theory has become one of the important areas in Systems Engineering. Besides the system safety requirements the customers put more emphasis on the availability of the vehicle. In order to fulfil this customer request the reliability of vehicle components is a primary issue for the manufacturers.

However, the component reliability must be a well-determined term, since a ‘too reliable’ component will harm the aftermarket business of the manufacturer. Because of this reason the reliability engineering has been put into the focus of the component and system manufacturers.

Any system analysis, in order to be complete, must give due consideration to system reliability and availability. A system designer is often faced with the problems of evaluation and improvement of system reliability and determination of optimum preventive maintenance schedule. In the solution of these problems, he is largely aided by mathematical models [93, 94].

Reliability is a feature incorporated into a heavy goods vehicle in the course of the design process that is realized in the course of production by a high degree of technological discipline, and maintained in exploitation by continual and stipulated maintenance and orderly usage. In designing reliability, it is necessary to predict or estimate the reliability of each vehicle system element, as far as technically accomplishable. Reliability is mainly determined accord-

ing to the ability of the given part or assembly or system to withstand the non-foreseen overloading without catastrophic failures. Reliability of vehicle elements (system, sub-system, assemblies, sub-assemblies, parts), especially of those critical in respect of reliability, is increasingly becoming the subject of special attention by vehicle designers and automotive industry in general [1].

Active safety systems address known safety problems but also introduce new classes of potentially hazardous failure modes. In a traditional design, in which the driver's input defines the energy level, for example, a commission failure such as the inadvertent application of brakes on a single wheel of the car is impossible. This condition becomes possible, however, in a design that enables independent by-wire control of wheel brakes. Active safety functions that control such brakes are of course carefully designed to fail-silent in case of detected malfunctions. But although the likelihood of commission failures can be reduced via good design, the potential still remains. The severity and probability of occurrence of these and other failure modes likely to arise from the introduction of new technologies in vehicles, therefore, need to be carefully considered to ensure safe deployment of such technologies.

Qualitative reliability analysis of a state-of-the-art electronic semi-trailer brake system will be presented in order to show the applicability of today's reliability design techniques for redundant architectures. Conclusions are drawn in consideration of a complex analysis approach.

Understandably, such radical design changes raise serious safety concerns [98] and demand the thorough safety evaluation of any new design concepts. Potential failure modes must be identified and the effects of these failure modes in the provision of sensitive active safety functions must be established.

2. DECLARATION

The undersigned, Tímea Fülep declares that this Ph.D. Thesis has been prepared by herself and the indicated sources have been used only. All parts taken over literally or by content are cited unambiguously.

Alulírott, Fülep Tímea kijelentem, hogy ezt a doktori értekezést magam készítettem és abban csak a megadott forrásokat használtam fel. Minden olyan részt, amelyet szó szerint, vagy azonos tartalomban, de átfogalmazva más forrásból átvettem, egyértelműen, a forrás megadásával megjelöltem.

December 2007, Budapest

Tímea Fülep

3. ACKNOWLEDGEMENTS

First of all, I would like to express many thanks to Prof. László Palkovics, my supervisor, for his support in several fields to be successful in my scientific work. I also wish to thank to Prof. Péter Várlaki for his patronage, suggestions and constant encouragement during this research. I am really grateful to Dr. László Nádai for giving me guidance to the labyrinth of the doctoral environment and for the elegant representation of my research work.

However, I am a Ph.D. candidate at the Department of Automobiles of the Budapest University of Technology and Economics, a great part of my work has been accomplished at the Knorr-Bremse Research and Development Centre Budapest. I have especially benefited from many discussions with colleagues, Péter Széll, Tibor Kandár, József Neményi, János György, Michael Herges during many meetings. Of course, I express my gratitude to the fellowship of my university department for the helpful and comprehensive atmosphere.

Last, but not least, I really wish to thank my family, especially my parents for their patience, helpfulness and encouragement. Without them it would have been much more difficult.

4. INTRODUCTION

The importance of the road traffic has been grown during the last decades, and stills growth. Although this development is demanded and promoted by the society needs, slowly it becomes unsustainable. As the traffic density increases, the traffic situations become more complex, difficult to handle by the human driver, which leads to accidents. All the communities around the world are looking for solutions, which would increase the road safety, but not really willing to pay for that. The term ‘accident free’ vehicle appears more and more in research projects and some of these technologies slowly go into serial production as well.

The traffic accident analyses show that in over 90% of the cases the driver is the primary cause of the accident. Taking a deeper insight into the analyses (Figure 4.1) results, most of the failure what the driver makes is in the sensing part of the control loop (71%), followed by the decision (20%) and the action (9%). This suggests the application of intelligent vehicle systems, which compensates for the driver’s deficiency in these phases.

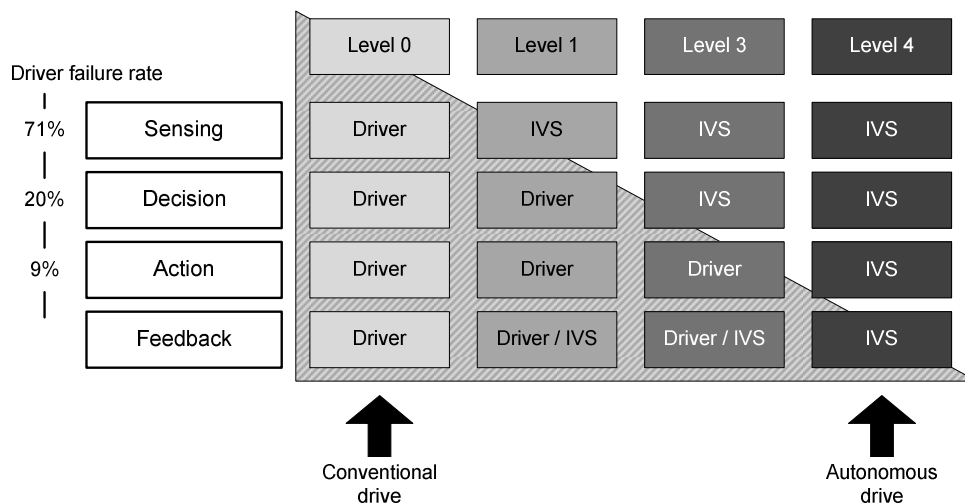


Figure 4.1 Classification of the intelligent vehicle systems

The figure above shows also the classification of the intelligent vehicle systems according to their role in the already mentioned sensing–decision–action–feedback loop. Depending on the level of the system different control scheme, different system platform system will be required. In case of level 1 systems where the Intelligent Vehicle Systems (IVS) only senses and informs the driver there is no need for fault-tolerant, it is enough if the system is fail-silent, i.e. switches out safely if critical error has been detected. Level 3 systems (if it really drives autonomously), however, will require a fully fault-tolerant system which provides the complete functionality even one critical failure has been detected. Of course, this can be the driver as well, provided that he is able to take over the control safely and the actuators are still intact. The above described problem, however, is only new in the road vehicle industry, but represents state-of-the-art solutions in the airplane industry, or even some of the high-speed trains have similar technologies.

To increase system reliability, the system designer may consider component redundancy because under certain conditions, it may be the quickest or the easiest solution or the solution with the least cost or the only solution. On the other hand, redundancy has the following disadvantages: it might be too expensive or it may exceed limitations on size, weight or power or it may require sensing and switching devices so complex as to offset the advantages.

Component replication is often essential to achieve required levels of safety or reliability. However, the options for replication in a non-trivial design are typically too many to consider in detail, so designers often rely on experience and evaluation of a few different design options to arrive at decisions about the location and level of component redundancies.

Reliability design in the concept design phase (see 5.3) is primarily oriented towards defining of reliability specification and selecting of the most acceptable solution from the point of view of reliability meeting requirements, which means that reliability of systems and their elements is analyzed. The process of system designing is started by translating the users' requirements and needs into the specification for designing, i.e. into the design assignment within creating of the pre-design. The concept design phase also defines the design goals from the point of view of meeting of the standards and regulations.

Conducting the analysis of failure mode and effects enables identifying of all potential and known modes of failure occurrences in system assemblies/parts, their causes, evaluation of consequences. Individual system elements can have several failure modes, since each stipulated function can have several failure modes. Failure modes are allocated, according to the required function, into three groups: complete function loss, partial function loss and wrong function, and this is important for conducting the analysis. For each failure mode, the possible effect (consequence) is analyzed at a higher level, i.e. at the whole system level.

It is stated that the mentioned method is appropriate mainly for non-redundant systems; however, analyses of partly redundant systems will be shown using this technique. This contradiction must be resolved by proper considerations, which are going to be presented. It should be noted that this systematic approach is only one possible solution and handles only one failure at a time. Multiple failures can be handled by quantitative reliability analysis, which creates a fault model and contains the analysis of the model deductively. Fault trees provide a convenient symbolic representation of the combination of the events resulting in the occurrence of the top event and provide statement on the total failure risk.

It should be remarked that this analysis does not necessarily depend upon credible component failure rates to produce useful results. In the case of software modules or components with no sufficient history of use, such failure rates would be impossible or very difficult to obtain anyway. However, the logical reduction of fault trees into minimal cut-sets can still indicate single points of failure in the system and point out potential design weaknesses that may lead to useful design iterations.

Results show that even handling only one failure at a time is legally prescribed, hidden failures or failure combinations can cause unintended effects in systems operation despite of redundancy. That is why qualitative reliability analysis and its structural appearance can be systematic input for further needed quantitative reliability analysis.

5. MOTIVATION

As long as mankind exists besides protecting life, ensuring life safety without harm, reliability became one of the most important fields – since unreliability and unavailability always accompany life, e. g. wrong shoes, failed machines – in any kind of tool application from the simplest instruments, devices till today’s most complex electronic systems. As inventing automated machines (also using electricity) it became therefore important to know, deriving from reliability its availability, whether man can reckon on the machine operability at any time. To ensure appropriate operation planned maintainability is essential, which establishes and increases useful lifetime of the required device. These notions are bound in RAMS (Reliability, Availability, Maintainability and Safety). During decades also under its coverage many requirements and standards were created avoiding inadvertent system operability harming life but ensuring required and prescribed safe ‘lifelong’ operation.

5.1 RELIABILITY HISTORY

If the required power of most electronic devices invented in the 1920s and 1930s failed, the device failed to operate and thus the system reliability depended on the electric power. Some reliability-aware USA cities put the electric power distribution lines underground in order to improve reliability. Electric power line unreliability is most often caused by something on those lines that cause them to break. Triode was invented in the 1920s and radios came into use. They were popular, but the major reliability difficulties with them were the electron tubes [25].

In the 1950s the great majority of designers used point characteristics of piece parts as stated by parts vendors. A few designers recognized that most piece part characteristics were distributed rather than point [20], developed error analysis and calculated performance in terms of an expected value and its variation. In organizations with strong manufacturing management, pressure was exerted on the designers to develop alternate methodologies. One result was worst case design, in which worst case characteristics were assumed for all parts. These years were also marked the beginning of efforts to approach the area of reliability from a quantitative standpoint [21] and early efforts at measurement were aimed primarily at electronic parts.

The importance of quantitative measurement to scientific progress was perhaps best stated by Lord Kelvin: ‘I often say that when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely in your thoughts advanced to the state of Science, whatever the matter may be.’

During World War II, electronic tubes were by far the most unreliable component [23, 25] used in electronic systems. This observation led to various studies and ad hoc groups whose

purpose was to identify ways that their reliability and the reliability of the systems in which they operated, could be improved [24]. One group in the early 1950s concluded that:

- There needs to be better reliability data collected from the field.
- Better components need to be developed.
- Quantitative reliability requirements need to be established.
- Reliability needs to be verified by test before full scale production.
- A permanent committee needs to be established to guide the reliability discipline.

Item 5 was implemented in the form of the Advisory Group of Reliability of Electronic Equipment (AGREE), whose charter was to identify actions that could be taken to provide more reliable electronic equipment.

In the 1960s the drive for higher reliability forced most design organizations to initiate reliability analysis and prediction as a part of the design process. Organizations using distributed-part characteristics in performance design adapted easily to reliability prediction based on failure rate distributions. Analysis of field failure data, environmental tests and material behaviour suggested the great influence of the operational environment on field failures. In the 1960s and 1970s many design organizations and project managements prepared design guidelines and mandated their use to improve reliability which was also dominated by electronic device improvements and their application. The emphasis placed on reliability demonstration in the AGREE [23] report led by the early 1960s to numerous military specifications and standards requiring factory ‘reliability acceptance tests’ for both equipment and parts. This was an era of intense missile and spacecraft development activity with many new problems and urgencies. It began with failures, in many cases more numerous than successes and ended with the triumphs of the Apollo program [21]. The judicious application of Fault Tree and Failure Modes, Effects and Criticality Analysis (FMECA) helped to pinpoint the source of failure when detailed data was missing. Chapter 9 deals with these analysis techniques in detail.

Starting early and continuing through the 1980s computer programs have played an increasing role in reliability. Widespread availability of personal computers has resulted in ever increasing use of reliability programs in design. The most evident factor was the increasing importance of quality in the commercial marketplace. One negative note in the picture of reliability progress in the 1980s was in the space program where an epidemic of launch failures, in the last half of the decade, included the tragic loss of the space shuttle Challenger (Figure 5.1). One might ask whether the early vigilance of the space effort was gradually eroded by overconfidence endangered by past success.



Figure 5.1. Challenger lifts off then explodes [121]

Attempts to delineate an independent set of tasks for mission assurance engineering resulted in the development of applied statistics for mission assurance [22]. Mission failures in a well-developed system come from necessary risks that remain in the system for the mission. Risk management is the key to mission assurance. The traditional tasks of applied statistics, reliability, maintainability, system safety, quality assurance, logistics support, human factors, software assurance and system effectiveness for a project are still important and should still be performed. The trends of the 1980s with regard to electronic equipment are continuing. The reliability is increasing; the maintainability decreasing and field data are still usually useless [25].

5.2 RELIABILITY MEASUREMENT

To increase reliability of a given system more features and parameters of reliability can be determined in order make it measurable. The following notions give an insight into these system features:

Reliability (function $R(t)$) has several kinds of definitions and all of them give a general operation statement about system functioning: ‘the probability that...’ ‘a unit will function normally when used according to specified conditions for at least a stated period of time’ [77] or ‘a component (or system) can perform a required function under stated conditions for a given period of time’ [33]. Then failure ($F(t)$) (5.1) (Figure 5.2) and failure density function ($f(t)$) (5.2) against time can be easily derived:

$$F(t) = 1 - R(t) \quad (5.1)$$

$$f(t) = \frac{dF(t)}{dt} \quad (5.2)$$

Failure rate ($\lambda(t)$) expresses the number of failures in a given time period, which is presented in the most general form as a function of time called ‘bathtub’ curve because of its shape Figure 5.3.

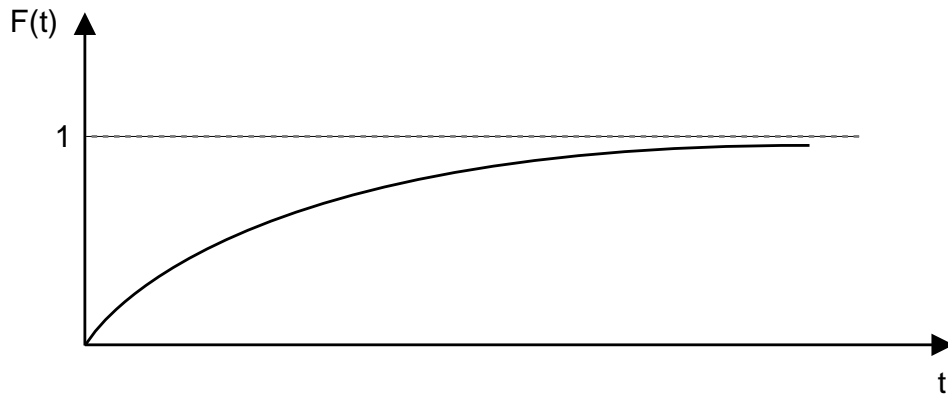


Figure 5.2. Failure function of non-repairable component with constant failure rate

$$\lambda(t) = \frac{\frac{dF(t)}{dt}}{1-F(t)} = \frac{f(t)}{R(t)} \quad (5.3)$$

Failure rate has the dimension of 1/time and it is often quoted in units of 10^{-9} per hour. This Failure-In-Time (FIT) rate is widely used to quantify the reliability of electronic components. For many electronic components it is possible to consider the failure rate to be constant and their reliability can be approximated by Poisson distribution, which is a very useful concept.

$$R = e^{-\lambda t} \quad (5.4)$$

It may roughly be divided into three portions and the reasons below can give explanation to its shape (focusing on electrical components without the detailed division of the curve according to Weibull [128]).

Reasons for burn-in (also called as early, infant) failures where the failure rate starts at a high value and falls rapidly [77]:

- inadequate quality control,
- inadequate manufacturing methods,
- substandard materials and workmanship,
- wrong start-up and installation,
- difficulties because of assembly,
- inadequate debugging,
- inadequate processes and human error,
- inadequate handling methods and wrong packaging.

Reasons for useful life failures when the failure rate is approximately constant:

- causes which cannot be explained,
- human errors, abuse and natural failures,
- unavoidable failures: these cannot be avoided by even the most effective preventive maintenance practices,
- undetectable defect,

- low safety factors,
- higher random stress than expected.

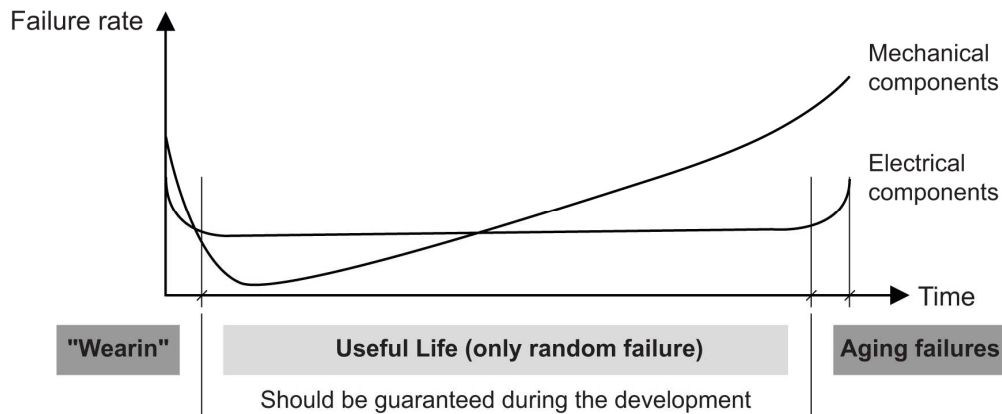


Figure 5.3. Bathtub curves comparison

Reasons for wear-out failures when the failure rate rises rapidly again:

- inadequate maintenance,
- wear due to friction,
- wear due to aging,
- wrong overhaul practices,
- corrosion and creep,
- designed-in life of the product is short.

There is a quite wide range of calculation with time concerning failure from different aspects. The following determinations are also used in evaluation, e.g. Mean Time Between Critical Failures (MTBCF) [36], Time Between Failure (TBF) [37]. Determining the Mean Time Between Failures (MTBF) for highly redundant systems is an extremely tedious, if not mathematically difficult process [35, 42, 46]. These systems are typically characterized by hierarchical application of nonidentical component (k of n) reliability calculations. Multiple levels in the hierarchy and large values of k and n make this calculation nearly intractable.

The following figure (Figure 5.4) illustrates the measures like MTTF (Mean Time To First Failure), MTT (Mean Time To Failure), MTBF, MTTR (Mean Time Between Repair).

System availability is mostly expressed by the following equation (5.5), which is also called utilization [37]:

$$A = \frac{MTBF}{MTBF + MTTR} \quad (5.5)$$

or coefficient of availability A is defined (5.6):

$$A = \frac{MUT}{MUT + MDT}, \quad (5.6)$$

where MUT is mean up time and MDT is mean down time [84, 33], which refers to maintainability meaning probability, that a failed unit is put back to satisfactory, operable condition in a given down time

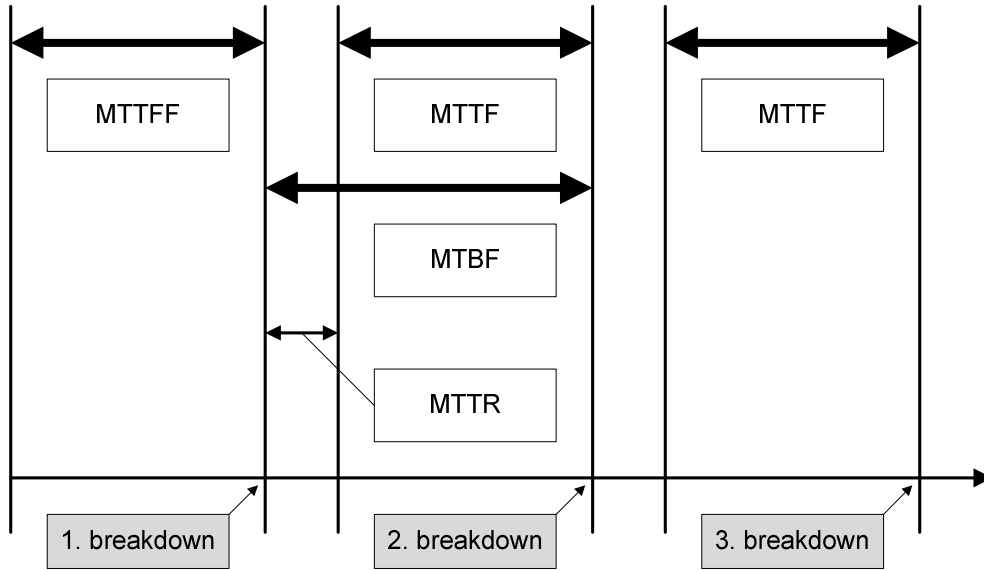


Figure 5.4. Illustration of failure – mean time intervals

It is not generally acknowledged that the resulting availability measure is actually an expected value with respect to frequency. At any point in time and with associated value for availability, the number of copies of a device that is functioning is a random variable [43].

Serial coupling between parts. In this case the failure of every individual element forces the whole system into ‘down’ state. The availability coefficient (probability of operation at time t) can be approximately calculated (5.7) as [101]:

$$A_{serial} = \frac{1}{1 + \sum_{k=1}^n \frac{T_{k2}}{T_{k1}}}, \quad (5.7)$$

where

- n is the number of parts in the system,
- T_{k1} is the mean time of operation for part k and
- T_{k2} is the mean time of repair for part k .

The reliability (probability of operation during interval τ) can be expressed (5.8) as:

$$R_{serial(\tau)} = A_{serial} e^{\frac{-\tau}{T_1}}, \quad (5.8)$$

where

$$T_1 = \frac{1}{\sum_{k=1}^n \frac{1}{T_{k1}}}. \quad (5.9)$$

If the exponentially holds for operation and maintenance/repair times, then the above expressions are accurate.

Parallel coupling between parts. In this case the failure of individual elements does not affect the reliability of the others: the failure of elements are independent, moreover, they can be repaired independently of each other. Now, in stationary case the availability (5.10) of the whole system (that is the probability that every individual element is operating at time t) is [101]:

$$A_{parallel} = \frac{T_{11}}{T_{11} + T_{12}} \cdot \frac{T_{21}}{T_{21} + T_{22}} \cdots \frac{T_{n1}}{T_{n1} + T_{n2}} = \prod_{i=1}^n \frac{T_{i1}}{T_{i1} + T_{i2}}, \quad (5.10)$$

where

- n is the number of parts in the system,
- T_{i1} is the mean time of operation for part i and
- T_{i2} is the mean time of repair for part i.

If the architecture of the system is redundant in the sense that there are homogenous (i.e. similarly reliable) parts coupled parallel, one can calculate the probability of operation (5.11) of k parts among the total number of n at a given time t:

$$A_k = \binom{n}{k} A_e^k (1 - A_e)^{n-k}, \quad (5.11)$$

where

- A_e is the availability coefficient (in stationary case).

Furthermore, the probability of operation (5.12) of k parts among the total number of n during a given period τ (in stationary case):

$$R_k(\tau) = \binom{n}{k} R_e(\tau)^k (1 - R_e(\tau))^{n-k}. \quad (5.12)$$

Mixed coupling between parts. In reality, brake systems are composed of serially coupled sub systems that have different reliability characteristics. These sub systems in some cases can be subdivided into similarly reliable parts (having the same functionality) that are coupled parallel therefore realizing fault-tolerance. Thus the structure of the whole system is mixed, and the

derivation of availability or reliability coefficients for the whole system requires the application of difficult analytic calculations and (in several cases) numerical simulations.

The accuracy of any mean time calculations depends on the proper data used. Detailed data collection, failure rate list can be found in MIL-HDBK 217 (Military Handbook) with the applied influence factors. These data can be formed upon company expectations [49].

5.3 DESIGN RELIABILITY

Figure 5.5 shows the process to system failure from failure in design [5] with the related failure notions.

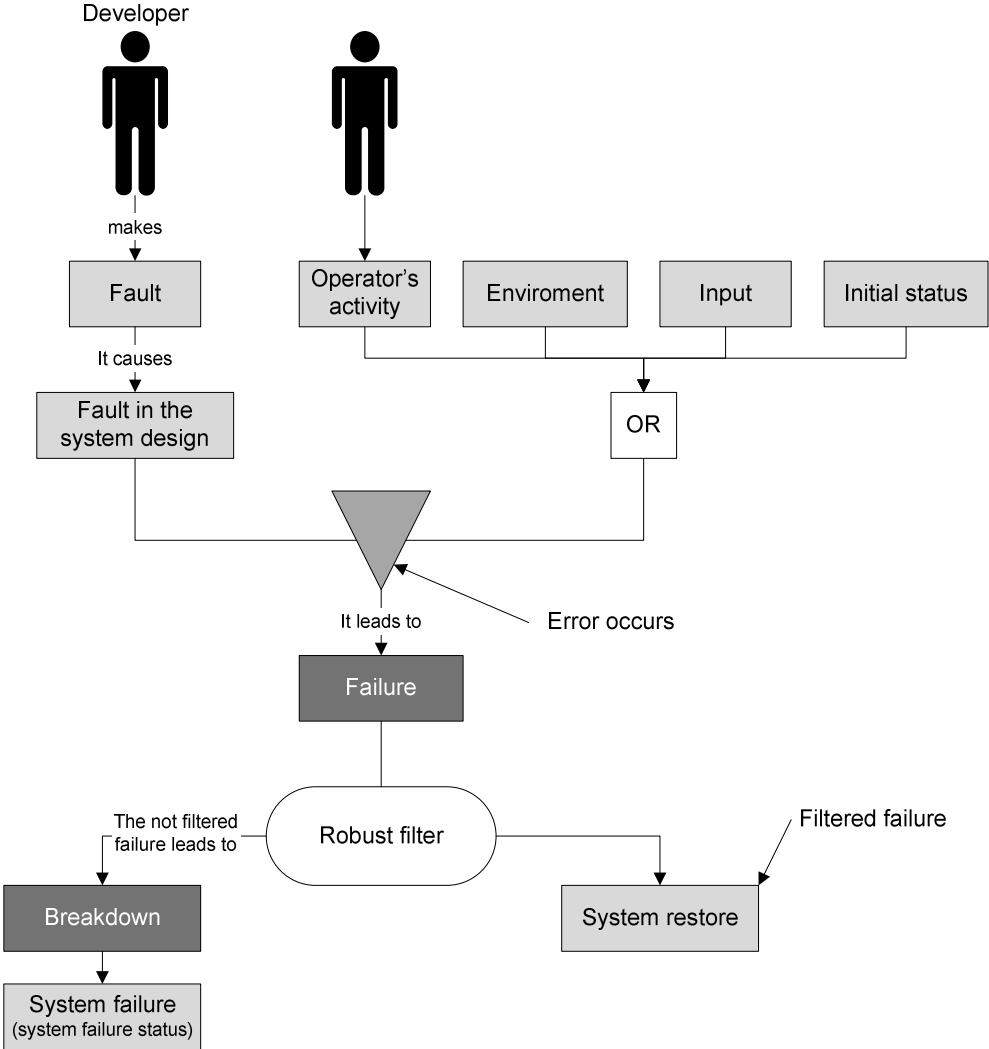


Figure 5.5. Fault – system failure concept

In general it can be stated that these notions are more or less clearly defined, but their usage is not always in the right context. An undesirable event that could result in death or damage to or loss of property called a mishap [27]. A hazard is interpreted as an undesired condition that

has the potential to cause or contribute to a mishap and the situation that results from the occurrence of a mishap is called a failure mode. Hazards and mishaps are classified in various severity levels known as Safety Integrity Levels (SIL, see 6.1.1), ranging from negligible (0) to catastrophic (4). There are different sources of hazard, e.g. human errors, unforeseen events, component failures, system complexity, fault and error propagation.

Safety is intimately connected to the notion of risk (in safety assessment: $\text{Safety} = 1 / \text{Risk}$ [79]) and popularly means a relatively high degree of freedom of harm [29]. The first step in a safety analysis process is to determine and identify the hazards of the system and to evaluate their severity and probability/likelihood [29, 105], which expresses risk (5.13):

$$\text{Risk} = \text{hazard}_{\text{severity}} \cdot \text{hazard}_{\text{probability}} \quad (5.13)$$

Both definition of system safety requirements and the subsequent safety evaluation of the safety-related system must result from risk analysis. Generally, risk R can be expressed as a combination of intensity of hazard occurrence h and its consequences S: $R = h \cdot S$ [84] or $R = F \cdot C$, F: risk frequency, C: consequence of the hazardous events [92]. If the total hazard resulting from system operation consists of n disjunctive hazards then total risk of the system can be calculated (5.14):

$$R = \sum_{i=1}^n h_i S_i \quad (5.14)$$

A system is generally considered to be safe if the level of risk is reasonable [30, see 6.1.1] and this risk must be evaluated according to societal, legal, and corporate concerns [31]. One can conceive of an acceptance criterion (5.15) for assessing the risk of an event that is a function (Figure 5.6) of the frequency of an event and consequence, such as the linear equation:

$$\frac{\text{frequency}}{a} + \frac{\text{consequence}}{b} \leq 1, \quad (5.15)$$

where

- a: the maximum frequency that can be tolerated even if the consequence is negligible,
- b: the maximum consequence that can be tolerated even if the frequency is negligible.

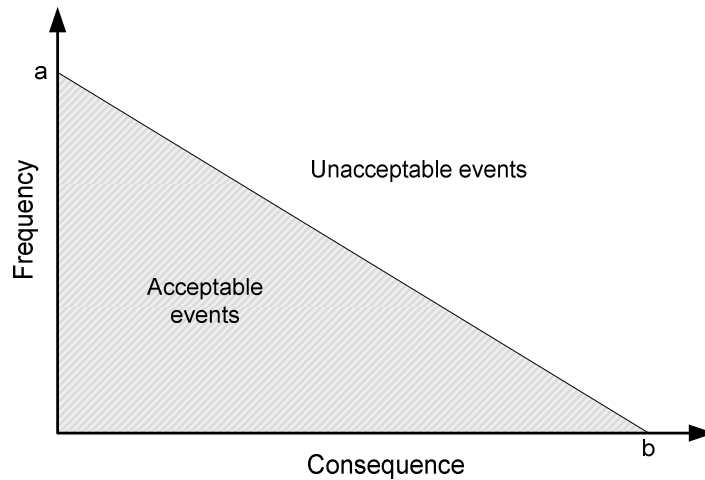


Figure 5.6. Frequency-consequence acceptance criterion

Engineering design for reliability is a systematic multidisciplinary approach utilized in the early design stages with the sole objective of significantly reducing the number of failures in the field and increasing a product's useful life. This is accomplished by the extensive implementation of design analyses, evaluations, testing and simulation techniques that can optimize and verify reliability. When utilized, this design approach significantly reduces the technical risk involved with product development and results in a higher quality product with reduced design, production and support costs. Inadequate design analysis and evaluation is often cited as a program problem, but there seems to be a distinct lack of understanding of what additional analyses are required, recommended and even the definition of criteria such as what is worst case analysis.

The level of design analysis has historically been a management option and for which the designer may have inadequate analysis tools, support or training. Unfortunately, when they are done, these analyses are often not done by the designer, but by a 'support function'. Design analysis is responsibility that must be clearly defined and include the detail designer. A design which has not successfully completed all analyses and testing should not be considered as a completed design and should not be released. Although certain analysis, such as thermal, failure modes and effects, logistics and producibility analyses will require involvement of additional engineering personnel, the lower life cycle cost of the final design will pay for these costs many times over.

The classical quality cost model is subdivided in terms of appraisal, prevention and failure costs. Figure 5.7 illustrates this model. The appraisal costs include the costs of inspection, tests such as testing media, receiving and final inspections. Prevention costs are caused by measures taken to avoid possible failures, such as the cost of quality planning or control, audits and training. Failure costs are caused if the quality demands are not fulfilled. Rejects, remachining, fair settlement and retake examination belong to the failure costs in this model.

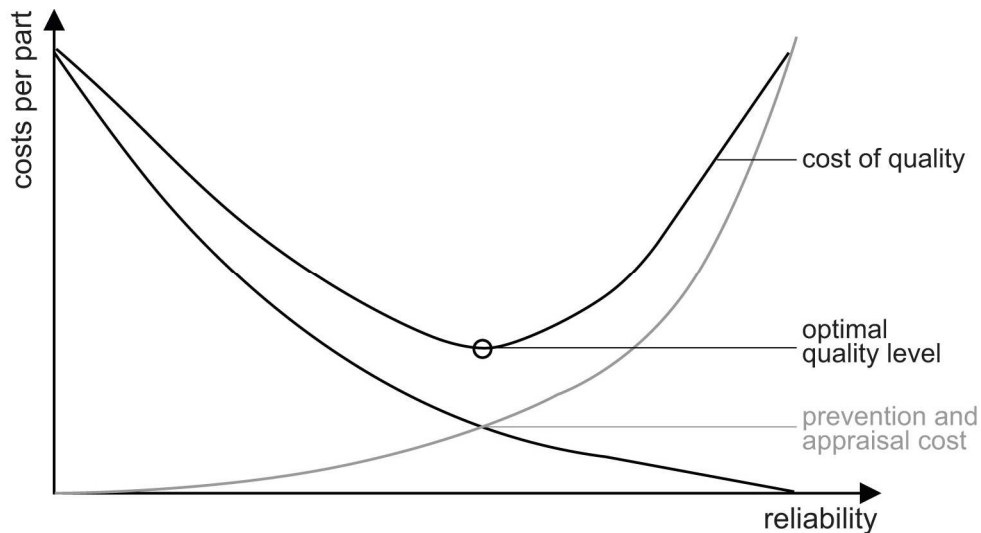


Figure 5.7. Connection of reliability and costs

Initially, the Cost of Quality procedure concentrated on the production phase. In the last ten years, the complete lifecycle of a system in the Quality Management process has been taken into consideration, to include the development phase [32].

A system with high reliability may not necessarily be highly fault-tolerant [38]. It is desirable to have a redundant system reconfigured so that it can tolerate a large number of faults [39]. In many critical applications, fault-tolerance has been essential architectural attribute for achieving high reliability. Redundancy is provided on a massive scale in critical systems requiring ultra-high reliability. The massively redundant schemes are of two types: fault masking and standby redundancy. Interestingly, in these schemes, the number of faults that are tolerated is very small compared to the number of redundant modules employed. This implies a large cost to reliability ratio.

Design redundancy requires that a failure in one function does not impair the system's ability to reconfigure to an equivalent back-up function. Redundancy can be used at hardware level, software level or in time, but it is now well-accepted that computer systems cannot achieve the required reliability and fault-tolerance without employing redundancy in their structures. Differences can be made between active ('hot') and passive ('cold') operation implementations. While the former means simultaneously functioning in the 'background', the latter interprets inactive functionality, which is switched on when the primary means of performing the function fails.

Because electronics can fail suddenly and without warning [104], redundant and fault-tolerant systems are traditionally used for safety-critical functions, such as in aerospace. The obvious benefit of redundancy is that it provides a back-up to a failed component. In avionics safe-life systems are required since there should not be possibility of error due to faults (Figure 5.8). As it is well-known, no aircraft has ever remained in the sky, so it should continue flight until it can land.

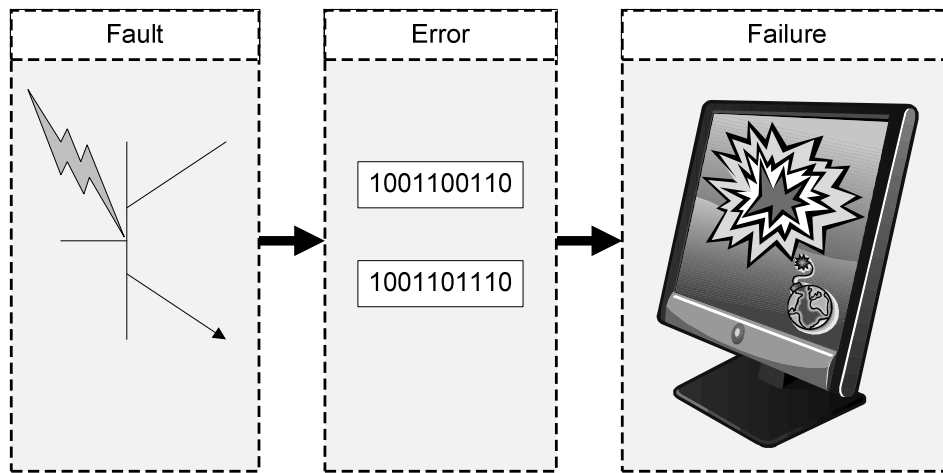


Figure 5.8. Fault – error – failure chain

It is necessary to decide what qualities of safety mechanisms are important to analyze. A list of possible safety goals includes recoverability [48], fault-tolerance and fail-safety [105]. A process is recoverable if, after the occurrence of a failure, the control of the process is not lost, and will return to normal execution in an acceptable amount of time. A process is fault-tolerant if a mechanism exists so that when there are failures the system can continue to operate, perhaps in a degraded level of performance or functionality. A system is fail-safe if no matter what combinations of failures occur, they do not lead to an unsafe state, stops functioning if minimal energy state is reached, e.g. land vehicles are stopped. In case of single-failure criterion a system should be constructed so, that one fault should not cause error. Individual faults should be detected:

- the fault is detectable
- finite number of fault possibilities
- detecting first fault before next is probable to happen
- if first failure is not detectable, number of detectable fault should be tolerated

By-wire systems, e.g. steer-, brake-, shift-, power-by-wire, offer many advantages during driving therefore a comprehensive system-safety process should be followed [29]. The objectives of a system safety program include:

- Identify potential hazards and associated avoidance requirements
- Translate safety requirements into engineering requirements
- Provide design assessment and trade-off support to the ongoing design
- Assess relative compliance of design to requirements and document findings
- Direct and monitor specialized safety testing
- Monitor and review test and field issues for safety trends

To improve the reliability of critical systems with the N-Modular Redundancy (NMR) scheme (Figure 5.9) is a popular technique [39]. High reliability in spacecraft design requires provisions for redundancy, thus complete redundancy in a spacecraft system may be achieved

through the practice of providing two or more identical assemblies and electronically cross-strapping them [64].

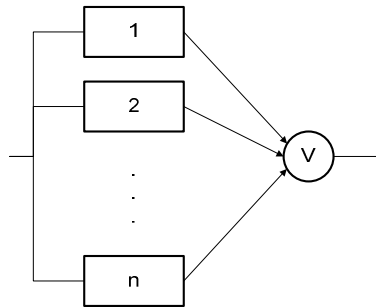


Figure 5.9. An NMR system

The value of R&M thinking is crucial to the success of any complex product or system. The best way to ensure that the discipline remains vital and needed is to treat the subject in a balanced way. The key is to achieve a balance between ultimate reliability and competitiveness. The need to insure reliability and producibility, quality and supportability in the engineering design process is increasingly important as electronic systems become more and more complex. This need in Department of Defense (DoD) procurement has resulted in ‘Transition from Development to Production’, DoD Directive [19].

Figure 5.10 indicates the possibility of iteration [79] between activities in the early stages of design but not from the latter stages back to concept design. It is worth considering briefly the possibility of iteration back to the concept stage from detail design because it will be seen that the importance of good concept design is highlighted.

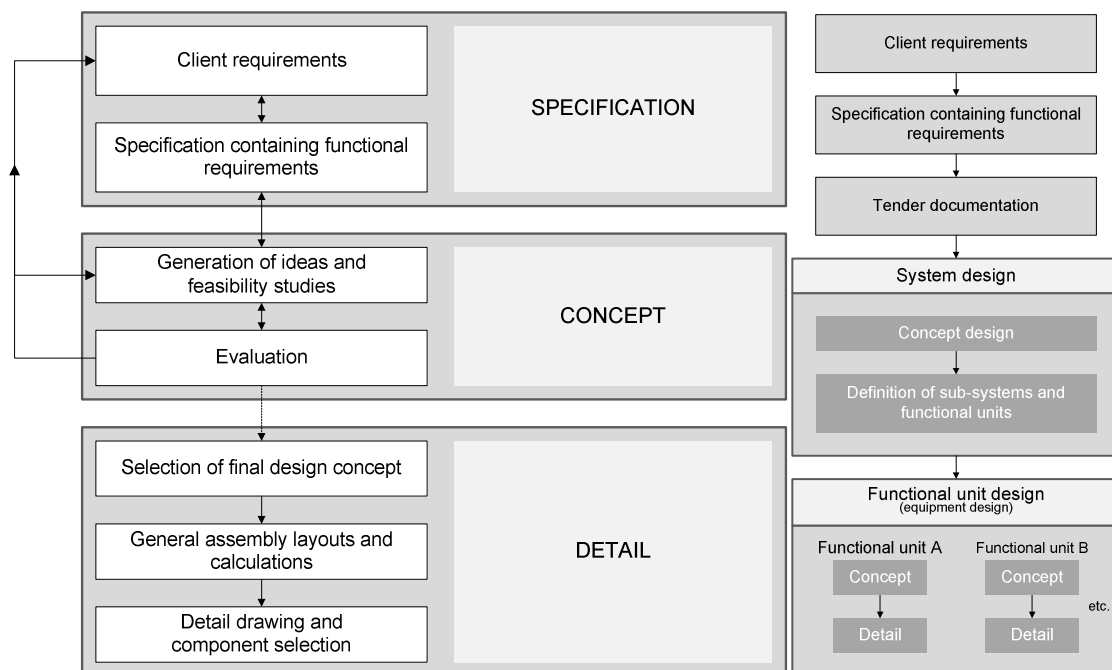


Figure 5.10. Iteration in design – Design models: equipment; systems and equipment

6. STATE-OF-THE-ART IN SAFETY-CRITICAL SYSTEMS

First of all, it should be made clear, what kind of systems can have safety-critical nature. A system is critical, if it has a feature towards the requirements are higher than usual while safety is a system feature not risking human life and environment. They are also mentioned specifically safety-related, relevant or safety instrumented systems. Deriving approaches, methods, techniques designing safety-critical architectures in all case it can be stated that they come from such primary technical fields, which concern high-level precision, safety and reliability, e.g. avionics, military, nuclear technology.

6.1 LEGISLATION

The most influential [82] system safety standard in the United States is MIL-STD-882C (Military Standard). This standard specifies detailed requirements covering all aspects of a system safety process for all DoD (Department of Defense) systems and facilities. It applies to every activity of the system life cycle including research, technology development, design, test and evaluation, manufacturing, verification, calibration, operations, maintenance and support, modification and disposal activities. Ministry of Defence Defence standard 00-56 (MOD DEF STAN 00-56) is a UK standard that was developed by the ministry of defence for contractors of defence system. This standard provides uniform requirements for implementing a system safety program in order to identify potential hazards and to impose design techniques and management controls to identify, evaluate and reduce their associated risks to a tolerable level. The standard uses the concept of Safety Integrity Levels (SILs) to determine the level of effort required for analysis and reliability requirements.

While today the risk-based approach towards safety seems to have become widely accepted and several standards have been established, the concepts of ‘risk’ and ‘target safety measures’ as they appear in many standards are very unstructured and unsystematic, giving rise to much confusion [83]:

- An expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence (MIL-STD-882-D).
- A combination of the probability of an event and its consequence (ISO/IEC Guide 73).
- A combination of the probability of occurrence of harm and the severity of that harm (ISO/IEC Guide 51/IEC 61508 [126]).
- The probable rate of occurrence of a hazard causing harm and the degree of severity of that harm (EN 50126/IEC 62278).
- The combination of the frequency, or probability, and the consequence of a specified hazardous event (IEC 60300-3-9, EN 50128/50129).
- The frequency (probability) of an occurrence and the associated level of hazard (SAE ARP 4754).

At first glance, the discrepancies may merely seem to be annoying. Within the same standardization body different definitions of risk are used. The definitions are all quite fuzzy and vague, e.g. it is not clear what ‘combination’ means or why sometimes probabilities, sometimes frequencies and sometimes rates are included. In some definitions, even mathematically incorrect concepts are introduced, e.g. ‘probable rate’. Matters get worse when it is realized that standards usually do not prescribe a particular method of risk analysis. In the end, it is up to the user to derive a quantitative target safety measure.

Usually, only the frequency of accidents can be influenced and not the severity. Often an assessment of the average risk is sufficient. Thus, risk can be regarded as being a product of the expected severity and frequency of an accident: $R = E(S) \cdot E(F)$ (see 5.3).

All standards related to safety-related computer systems in different application sectors should use the same definition of risk. A concise definition of terminology and a clear relationship between the definition of risk and the target safety measures is necessary. Otherwise, it is very likely that incorrect safety requirements will be derived or false conclusions drawn from safety analyses. A definition of risk in terms of frequency seems more natural than one based on probability as the latter requires the consideration of additional parameters (e.g. the time T) and assumptions.

6.1.1 Safety-related systems

IEC 61508 was developed by the International Electrotechnical Commission (IEC) Industrial Committee. IEC 61508 was not intended to be used as a safety standard but to act as a generic standard to encourage and facilitate the development of application sector standards. It is applicable to safety-related systems of electrical/electronic/programmable electronic systems, both integrated with the Equipment Under control (EUC) control system and separate from the EUC control system. ISO/IEC 61508 is a standard to set requirements for design, development, operation and maintenance of safety-related control and protection systems which are based on electrical, electronics and software technologies. A system is called safety-related if any failure to function correctly can present a hazard to people. Examples: railway signalling, vehicle control (braking), aircraft control, fire detection, process plant emergency control, etc. Figure 6.1 shows a comparison [92] of safety relevant products from the mentioned industries.

In the field of railway signalling and safety systems, probabilistic methods are increasing in significance. They are used for the purpose of evidencing adherence to a given quantitative safety objective. Hence, this probabilistic evidence is required as standard practice in developments in line with CENELEC (Comité Européen de Normalisation Électrotechnique).

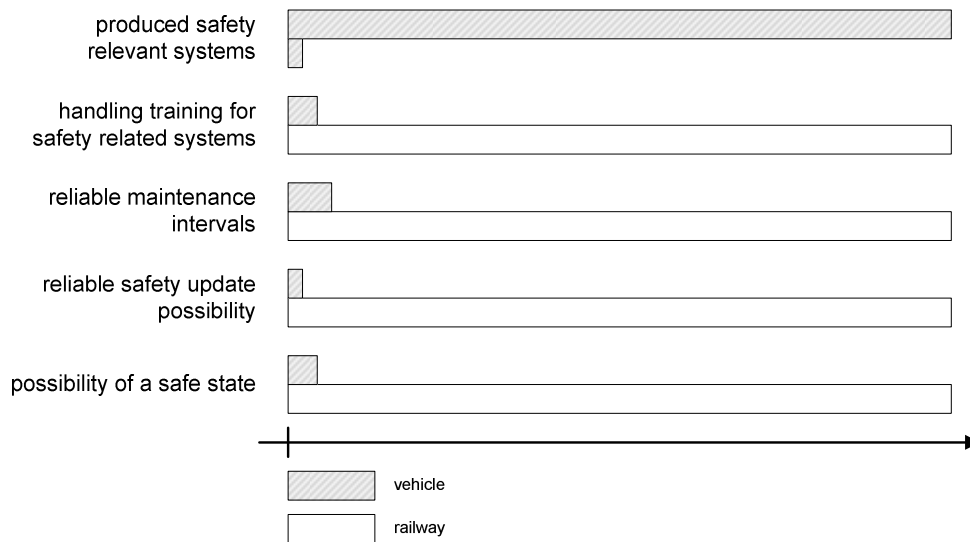


Figure 6.1. Vehicle and railway comparison

The standard covers the complete safety life cycle, and may need interpretation to develop sector specific standards. It has its origins in the process control industry sector. The safety life cycle has 16 phases which roughly can be divided into three groups as follows: phases 1-5 address analysis, phases 6-13 address realization and phases 14-16 address operation. All phases are concerned with the safety function of the system. The standard has seven parts (Figure 6.2). Parts 1-3 contain the requirements of the standard (normative), while 4-7 are guidelines and examples for development and thus informative:

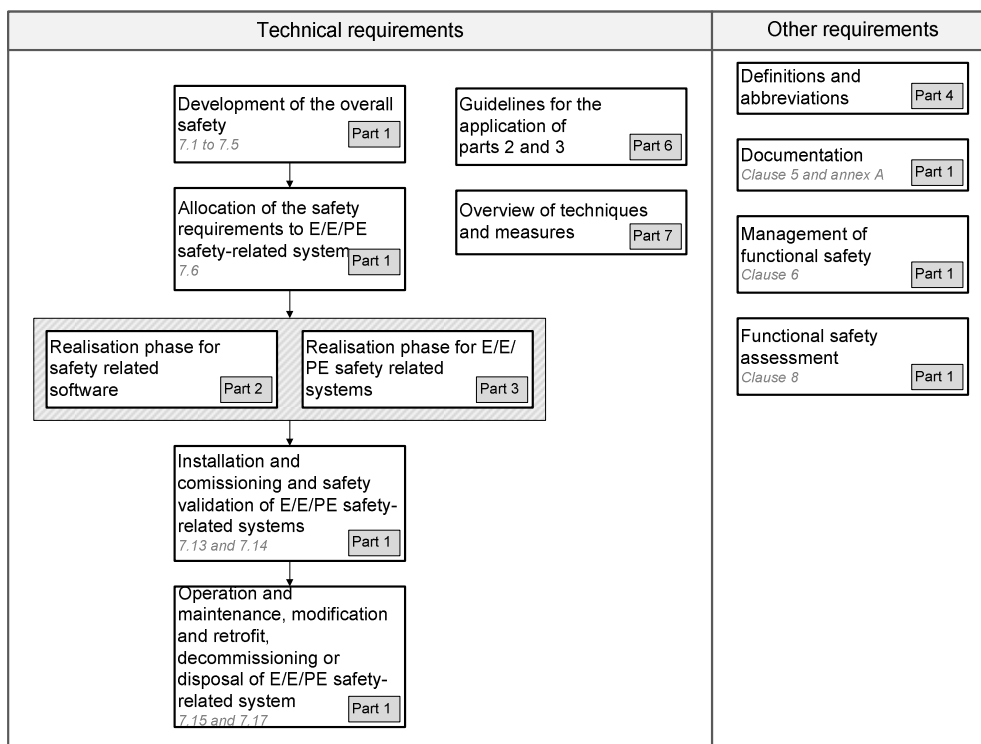


Figure 6.2 Structure overview of IEC 61508

- Part 1: General requirements
- Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
- Part 3: Software requirements
- Part 4: Definitions and abbreviations
- Part 5: Examples of methods for the determination of safety integrity levels
- Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
- Part 7: Overview of techniques and measures

The IEC 61508 is provided as a generic approach for all safety lifecycle activities. However, only the careful selection of certain methods and procedures of the IEC 61508 can ensure the achievement of the proposed goal for the respective area of application. An example for risk assessment will be shown in 6.4.

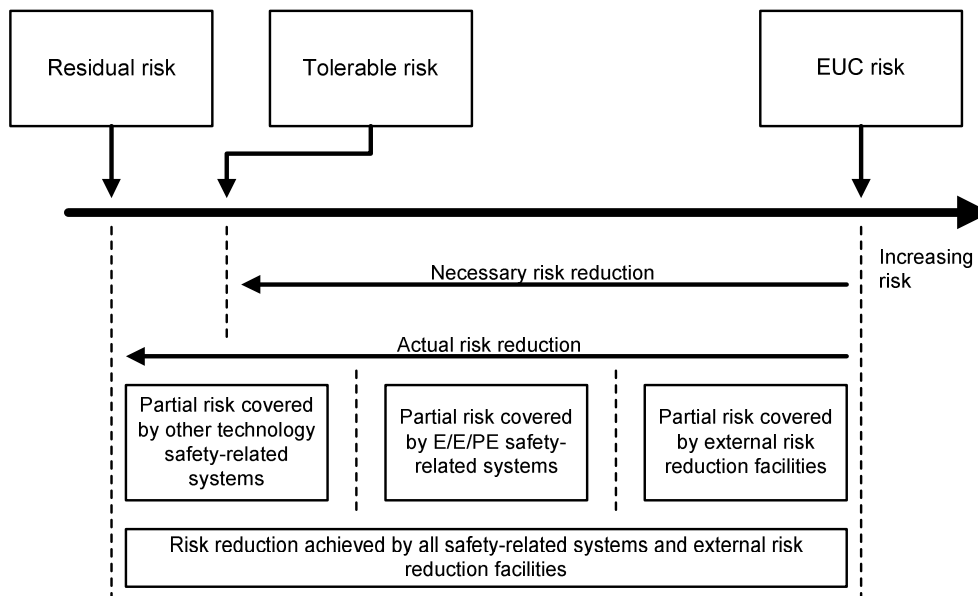


Figure 6.3. General concepts of risk reduction, IEC 1 661/98

The risk is reduced to a tolerable level (Figure 6.3) by applying safety functions which may consist of E/E/PES and/or other technologies. While other technologies may be employed in reducing the risk, only those safety functions relying on E/E/PES are covered by the detailed requirements of IEC 61508. IEC 61508 has the following views on risks:

- zero risk can never be reached,
- safety must be considered from the beginning,
- non-tolerable risks must be reduced.

One should avoid a black and white decision of categorizing systems as ‘safety-critical’ or ‘non-safety-critical’, instead it is better to use levels of safety integrity. These SILs are based on Tolerable Hazard Rate (THR) determinations (Table 6.1). The standard also provides different methods to derive tolerable hazard rates using different principles:

- Globalement Au Moins Aussi Bon (GAMAB): ‘All new guided transport systems must offer a level of risk globally at least as good as the one offered by any equivalent existing system.’
- As low as reasonably practicable (ALARP): ‘Societal risk has to be examined when there is a possibility of a catastrophe involving a large number of casualties.’
- Minimum endogenous mortality (MEM): ‘Hazard due to a new system of transport would not significantly augment the figure of the minimum endogenous mortality for an individual.’

Table 6.1. Risk classes

Risk classes	Consequence			
	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

The related risk classes are the following (Table 6.2):

Table 6.2. Risk classes

Class I	Intolerable risk
Class II	Undesirable risk, and tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained
Class III	Tolerable risk if the cost of risk reduction would exceed the improvement gained
Class IV	Negligible risk

The quantitative safety objective of an application is derived from the risk accepted by society. Operators of safety-critical applications impose this safety objective on manufacturers in the form of a THR. The THR results in an appropriate safety integrity level as indicated in Table 6.3 [102].

Table 6.3. Classification of SILs concerning THRs

SIL	Low demand mode of operation (Average probability of failure to perform its designed function on demand)	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

A SIL is usually associated with a system function or a subsystem and it is used for two purposes [103]: First, a certain SIL is used to give an interval for a rate of safety-critical failures. This characteristic applies to so called ‘random faults’, i.e. failures that occur in an unpredictable manner. Mostly, these faults are caused and accompanied by intrinsic physical processes such as ageing. Second, a SIL defines measures to be applied in the design and during the manufacturing process to keep the frequency of occurrence of so called ‘systematic faults’ small in comparison with random faults.

The reason for systematic faults is mainly a design error or a manufacturing process error that causes failures of identical replications of the same type of component or equipment under similar circumstances. These faults might reveal themselves also in the form of common cause failures. Usually, the higher the SIL, the harder the requirements for the system function. In many cases, SIL4 is the highest SIL, whereas SIL1 is the SIL with the lowest requirements. In addition, there can be system functions that do not even fall into the lowest SIL (SIL1). Sometimes, this is denoted as ‘SIL0’. Design of SIL 3 or 4 systems (that one finds in many fields related for example to transport, energy production, as in many sectors of industrial production) is subjected to the respect of technical reference frames [118]. In determining a SIL, parts 1 and 5 of IEC 61508 take a hazard and risk based approach with progressive refinement [100].

6.2 SAFETY-CRITICAL SYSTEM IN AVIONICS

Avionics equipment systems are historically expected to fail during operational usage while other aircraft systems such as structures, engines, hydraulics, etc. are expected to be failure free during operational usage. This difference in expectation is borne out of the philosophical base and the relative maturity of the technologies involved. System designers for structures, engines, hydraulics, etc. consider that a failure is a caused event while avionics designers con-

consider a failure as a random event. Viewing failures as a random rather than a caused event reflects the state of technology rather than a fundamental difference in the failure process.

Reliability of avionics is traditionally expressed in terms such as Mean Time Between Failure (MTBF) or mean failure rate [2]. Expressing equipment reliability in these terms implies that as long as on the average, the specified MTBF is achieved it is acceptable to have equipment in use that displays level of reliability less than and greater than the specified mean value. Unfortunately this approach yields no insight as to which specific copies are on the low side of the MTBF value, the unreliable units. Such an approach is reasonable if the failure of the equipment during usage does not significantly impact flight safety and/or cost and the concern is to have sufficient spare parts to maintain operational availability. But the trend in avionics is to put avionics into safety of flight, flight critical, systems such as flight control, fire control, etc. In these applications the failure of even one equipment item is not acceptable since the entire aircraft could be lost.

Table 6.4 shows the classification of the different failures, and their accepted occurrence rate in case of different levels of redundancy of the given subsystem. These values are used in the development process as target, which must be reached either by the appropriate design of the system, or increase the level of redundancy. This leads to a trade-off among several factors: safety, cost of operation, price, place, weight and will be examined very thoroughly by the designers.

Generally, the aviation safety is characterized by flight risk. Risk is the probability of appearing unwanted events with hard consequence (loosing the aircraft and/or human life). The prescribed risk level can be characterized by so called elementary risk (ER), which is the 10^{-6} . It means one catastrophic situation (hard accident) can be appeared during 1 million flying hours. In reality the flight risk depends on the types of aircraft, operational conditions and operators and it is higher (means better, therefore less) then prescribed level. Real flight risk is 10^{-7} - 10^{-9} . (Smoking one cigarette or drinking one cocktail equal to 1,5 ER, travelling from Budapest to Paris by air means about 1,5 ER, however travelling from Budapest centre to the Airport equal to 40-70 ER depending on the traffic situation [6].)

The aircraft elements should have the different failure rates depending on the applied redundancy as it shown in table. In practice, for critical elements 3-5 redundancy is applied including the emergency systems.

Table 6.4. Dependence of the failure rate of a system on the degree of redundancy

	Degree of redundancy		
	0	1	2
	Single	Double	Triple
Catastrophic	A = 10^{-9}	B	C
Hazardous	B = 10^{-7}	C	D
Major	C = 10^{-5}	D	D
Minor	D = 10^{-3}	D	D
No safety effect	E = na	E	E

A maximum target failure rate of 10^{-6} catastrophic failures per hour is often budgeted for the entire flight control system. For the ground facilities a maximum of 0.25 catastrophic control failures over the 40-year life of the system is specified, corresponding to a mean failure rate also on the order of 10^{-6} catastrophic failures per hour. These figures correspond to all elements of the system, not just software, and constitute an upper bound on the allowable catastrophic errors [7].

6.2.1 Requirements in avionics

The legacy policy of aviation and aeronautical industries is based on the international advisory (ICAO – International Civil Aviation Organization) [16] and international, country and provincial legacy (JAA – Joint Aviation Authority, National CAA Civil Aviation Authority, other laws, etc.) All the aspects of the aircraft design, manufacturing, operation, maintenance, repairing, including the applied methods of design, stress or safety analyses, education, training and examination of staff, their licensing, certification of elements, aggregates, subsystems, aircrafts, production plants, aviation companies, etc. are described in airworthiness and requirements, and related documents. The most important airworthiness materials are published by ICAO in its Annexes and manuals. Because the ICAO can give recommendation [15], only, these requirements must be published by national governments as codes, or directives.

All the aeronautical products should have the certificates. There are two different: type and airworthiness certificates. Airworthiness requirements define the physical and legal requirements. The airplane or its sub systems, parts have airworthiness if they are in physically good conditions and they have (type and airworthiness) certifications defining their fulfilling the requirements and possible safe operations. A type certification certificate is an aviation authority document which grants authorization to produce and operate a given type of aircraft. The airworthiness certificate is an aviation authority document that grants authorization to operate a given aircraft safe in flight. The certification technology is the detailed description how the type and airworthiness certification can be realized. This process including methods applied during design and fabrication as well as the series of laboratory, ground and flight tests. The certification procedures are not really described by airworthiness requirements, those must be defined and designed by producer and authority will accept and observe of the given procedures. Of course authority has rights to change the procedures and add some more tests. The cost of certification must be covered by producers. This cost can be even 2-3 times greater than the cost of preliminary investigation, design and fabrication.

The airframe manufacturers have developed on quality management systems which contain requirements for suppliers, too. The aircraft brake suppliers are using the known regulation and standards, like:

- ISO 9001:2000
- engineering standards like SAE Standards

- AIR 1934 (Use of Structural Carbon Heat Sink Brakes on Aircraft)
- AIR1064 (Brake Dynamics)
- ARP1907 (Automatic Braking Systems Requirements)
- IEC 61508 (Safety Standard for Safety Instrumented Systems)
- aviation standards AMJ 25-1309 (equipment systems and installation)
- SAE ARP 4754 (Certification considerations for highly integrated or complex aircraft systems)
- RTCA DO 254 (Design Assurance guidance for airborne electronic hardware), etc.

However, they must apply the special aviation requirements described by FAR (Federal Airworthiness Requirements) and/or JAR (Joint Airworthiness requirements) and they have to harmonize their programs with the provincial regulations and airframe producer.

The ever increasing requirement for space system products has caused increased attention to be focused on the identification and elimination of potential failure modes from both highly complex devices as well as the more mundane passive devices. Failure analysis technology is a significant factor in attaining this required satellite longevity. General Electric Space Division uses a five phase information and control program [9]:

- Identification and list of potential failure source
- Elimination of potential failures by design improvement action
- Application of assurance programs to maintain product quality through the assembly and test flow
- Utilization of inspection and test programs to find defects
- Residuals

The aim is to identify and eliminate or neutralize potential major failure mode conditions from the design, manufacture, assembly or test of its products.

From a study [10] of over 300 spacecrafts for which approximately 2500 malfunctions were reported, it is concluded that a decreasing hazard exists for overall spacecraft malfunctions and particularly for those due to design and environmental failures (which compromise approximately one-half of all reports). Malfunctions due to parts and quality problems show a closer adherence to the constant hazard model. For a spacecraft component population the reliability parameters can be expressed in many ways and good definitions are essential to the right understanding:

- Failure rate: the number of components of failing during a specified time interval. Because spacecraft components are not repaired or replaced and because entire spacecraft may cease to operate, the failure rate is expected to decrease with time on orbit.
- Hazard: the number of components failing during a specified time interval normalized to the number of components that were operational at the beginning of the interval. The time interval must be sufficiently short so that the number of operational components does not

decrease significantly. Because of the normalization, the hazard is expected to remain constant with time on orbit if the exponential failure law is valid.

- Failure ratio: the number of components that fail during a specified time interval divided by the number of spacecraft that were operational at the beginning of the interval.

To cover the main fields of the safety-critical vehicle systems the next chapter summarizes the railway systems in accordance with the related legislation, while chapter 7.1 presents design relations between aircraft and commercial vehicle systems focusing on control and brake systems with unambiguous similarities [FT11].

6.3 RAILWAY REGULATION AND STANDARDIZATION

The safety level of rail transport in the European Union (EU) is generally very good [118], particularly in comparison with road transport, which is its main competitor, especially for freight transport. In order to be authorized to use the railway infrastructure, a railway company must hold a safety certificate delivered by independent organisms accredited to public authorities. This safety certificate may cover the whole railway network of a European country or only a limited region of this network.

Safety rules and standards, such as operating rules, signalling rules, operating requirements and technical requirements applicable to rolling-stock have been designed mainly nationally at each European country level. Under the regulations currently in force, a variety of bodies deal with safety. These national safety rules, which are often based on national technical standards, should gradually be replaced by rules based on common standards, established by Technical Specifications for Interoperability (TSIs). These topics are of particular importance for signalling devices onboard rolling-stocks, which could travel in different countries throughout Europe. These devices being more and more computer based, the assessment of safety software is a question of increasing importance.

The safety requirements have always been taken into account in the railway transport system development. Nowadays, contractual obligations on performances, led industrials to a total control of parameters acting on Reliability, Availability, Maintainability and Safety (RAMS) in the field of railways. The choice of standards to be used is the designer's and the manufacturer's responsibility. But to have this done in openness and in a non-discriminatory manner, it is necessary that each State prescribes safety requirements (e.g. safety target) and that national railway networks recommend standards reference systems. Moreover, interoperability of railway equipments within European Union is a major concern which leads to increasing needs of standardizations.

The safety of railway projects is usually governed by laws and standards aiming to define and achieve a certain level of RAMS requirements. On one hand, the legislation is, at the present time, most often national: for example in France depending of the type of railway activity (urban guided transit, or intercity transit), the relevant regulations are:

- Decree 2006-1279 relating to safety of railway traffic and to interoperability of railway system (19 October 2006).
- Decree 2003-425 relating to safety of public guided transit (9 May 2003).

For high-speed railway traffic however, the existence of the European Council Directive 96/48/EC on the interoperability of the trans-European high-speed rail system (23 July 1996), is noticeable. The Technical Specification for Interoperability of the rolling-stock subsystem 2002/735/EC (30 May 2002) can also be mentioned.

On the other hand the reference standard are most often European (CENELEC reference system: EN 50126, EN 50129 and EN 50128), indeed International (IEC 61508). The latter one (applicable to all type of electrical/electronic/programmable electronic safety-related systems) is furthermore the founding one: many aspects of EN 50126, EN 50128 and EN 50129 are railway applications of IEC 61508 prescriptions. The purpose of the CENELEC reference system is to:

- Provide a common reference frame in Europe to support the widening of railway components markets, the interoperability, the interchangeability and the ‘cross acceptance’ of railway components.
- Meet the specificities in the railway domain. Facing the complexity of new systems, the RAMS requirements are an essential point in the project development of railway transportation systems.

Railway systems integrate more and more programmable numerical equipment including consequently software. Some of these systems are subjected to RAMS requirements (especially safety requirements). It is in particular the case of onboard control/command systems known as safety-critical, whose failures can cause serious damage to people or to goods, as well as systems with very high availability targets (telecommunications networks in particular). The software integrated in such systems consequently also undergoes RAMS constraints. There are several techniques making it possible, on one hand, to avoid or eliminate the development faults and, on the other hand, to make the execution of the software applications safe in case of occurrence of physical or environmental faults. These techniques include in particular tests, simulation, proofs, and design of safe and reliable architectures including the RAMS analyses (Failure Modes Effects and Criticality Analysis/Software Error Effects Analyses, Fault trees, etc.).

The standard EN 50128 is particularly dedicated to the software development for the railway field. SIL becomes SSIL (Software SIL) with levels from 0 (not critical) to 4 (critical), and for each SSIL, the specific development activities (including verification and validation: V&V) are prescribed. For of a component of a given SSIL, EN 50128 describes the processes, methods and tools to be implemented during the development. It is about an obligation of means, which is added to the obligations of quantitative and/or qualitative results.

Software certification demonstrates the reliability, or safety of software systems in such a way that an independent authority can check it with sufficient trust in the techniques and tools used in the certification process itself. It can be built on existing validation and verification

techniques but introduces the notion of explicit software certificates, which contain all the information necessary for an independent assessment of the demonstrated properties. Software certificates support a product-oriented assurance approach, combining different techniques and forms of evidence (e.g., fault trees, safety cases, formal proofs, etc.) and linking them to the details of the underlying software.

Within the framework of critical systems (SIL 3 and 4) the design principles to ensure safety generally go in opposition to system availability. This is the consequence of a ‘fail stop’ design principle aiming to stop the system in case of failure and therefore ensuring a ‘fail-safe’ behaviour. As example, in the railway field the plausible failures will generally have the effect of ‘stopping the train(s)’ which has a strong impact on the system availability. This feature, characteristic of applications (like ground transportation and energy production) having a ‘rest state’ identified as safe and reachable by (relatively) simple means and (relatively: 3 km and 1 mn 30s to stop a high-speed train at 300 km/h) fast, is not shared in other fields (like aeronautic) where some vital functions must remain available in all circumstances.

Concerning software, only subject to design faults because of its immaterial nature, the need to prevent and eliminate these faults by the various methods prescribed for high SSIL levels (SSIL 3 or SSIL 4), causes moreover to also improve the reliability level of the software by a better control of its complexity and quality. For the non-critical (SSIL 0) and not much critical (SSIL 1 and SSIL 2) applications, the design process of software is on the other hand less constrained (as well for the programming language and tools as for Verification and Validation process) inducing a less quality of software, often causing unavailability scenarios. For such applications, the use of ‘Commercial Off The Shelf’ (COTS) components is allowed and therefore frequent. The control of the quality of these COTS components, which has consequently a direct impact on system availability, remains consequently a crucial question, in a context of increasing search for profitability.

6.4 APPLICATION OF QUALITATIVE RISK ASSESSMENT IN ELECTRONIC BRAKE SYSTEM

The risk graph method (Figure 6.4) is a qualitative method that enables safety integrity level of a safety-related system to be determined from knowledge of the factors associated with the Equipment Under Control (EUC) and the EUC control system.

The qualitative approach is adopted, in order to simplify matters a number of parameters are introduced which together describe the nature of the hazardous situation when safety-related systems fail or are not available. One parameter is chosen from each of four sets, and then the selected parameters are combined to decide the safety integrity level allocated to the safety-related systems. These parameters allow a meaningful graduation of the risks to be made and contain the key risk assessment factors.

The following simplified procedure is based on the following equation: $R = f \cdot C$, where

– R is the risk with no safely-related systems in place,

- f is the frequency of the hazardous event with no safety-related systems in place,
- C is the consequence of the hazardous event (the consequences could be related to harm associated with health and safety or harm from environmental damage).

The frequency of the hazardous event f is, in this case, considered to be made up of three influencing factors:

- frequency of, and exposure time in, the hazardous zone,
- the possibility of avoiding the hazardous event,
- the probability of the hazardous event taking place without the addition of any safety-related systems (but having in place external risk reduction facilities) – this is termed by the probability of the unwanted occurrence.

This produces the following four risk parameters:

- consequence of the hazardous event (C)
- frequency of and exposure time in, the hazardous zone (F)
- possibility of failing to avoid the hazardous event (P)
- probability of the unwanted occurrence (W)

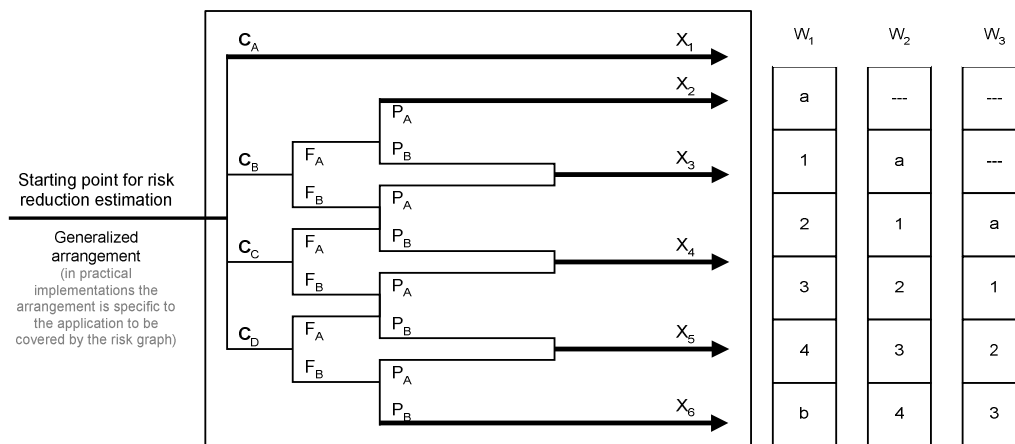


Figure 6.4. Established Risk Graph (IEC 1 666/98)

- : No safety requirements; a: No special safety requirements;
- b: A single E/E/PES is not sufficient; 1, 2, 3, 4: Safety integrity level

Table 6.5 lists the result of a cooperative work [122] with The Computer and Automation Research Institute, Hungarian Academy of Sciences (MTA SZTAKI) and Knorr-Bremse Fékrendszerek Kft. in evaluating by risk graph the most important state-of-the-art functions of an EBS used in commercial vehicles in all heavy trucks in Europe since 1996. The basis for the analysis is the Regulation UN-ECE 13 [127], which defines that an appropriate deceleration must be provided under all conditions even if there is a single failure in the service braking system. The redundancy must be assured on the way which provides controllable deceleration on prescribed level. This means if the control and the actuation of the foundation brakes need different kind of energy the redundancy must be ensured in case of both one.

Table 6.5. Assessment of electronic brake functions

Functions	SIL level	4	3	2	1	0
Deceleration (braking)	SIL 3		♦			
ISC	SIL 1				♦	
CFC	SIL 1				♦	
Brake assistant	SIL 2			♦		
Tilt prevention	SIL 0					♦
ABS	SIL 1				♦	
ATC / DTC	SIL 0					♦
ESP	SIL 1				♦	
Differential control	SIL 0					♦
Hill brake	SIL 0					♦
Trailer brake	SIL 0					♦

As a consequence, deceleration (i.e. the braking ability) as a function is only ranked as SIL 3. ‘Surprisingly’ the brake assistant function obtained ranking SIL 2, and the other important functions, such as ABS and ESP only SIL level 1. Even if these two latter functionalities have very high impact on the accident probability and their severity, their availability is not essential from the deceleration viewpoint (this is the reason that they have ‘fail-silent’ nature, i.e. in case of a failure they will be securely disabled). All the other functions (tilt prevention, ATC, DTC, hill brake) are SIL level 0, which is understandable in the light of the above analyses. The Level 0 ranking of the trailer brake function, however, requires a short explanation. The engineering feeling says that the trailer brake is a significant component in providing the required deceleration for the combination. This is true, however, the regulation does not consider the combination, but only individual vehicles, and thus the motor vehicle brake performance does not depend on the existence of the trailer brake system. This last example shows that the results of such qualitative analyses have to be carefully analyzed and the right conclusion has to be drawn.

Explanation of the examined brake functions:

- ABS: prevents wheel lock by brake, maintains vehicle stability
- ATC (Automatic Traction Control): prevents wheel spin, maintains traction behaviour
- DTC (Drag Torque Control): prevents wheel lock by driveline, maintains vehicle stability
- ISC (Intelligent Slip Control): brake force distribution between axles, includes adhesion (slip) and wear control without using direct load sensing and controlled deceleration
- CFC (Coupling Force Control): brake force distribution between vehicle tags, maintains stability of the complete combination
- ESP: includes yaw control and roll control, maintains stability of the vehicle combination

6.5 LEGISLATION STATUS OF THE ELECTRONIC STABILITY CONTROL

One of the specific function of the electronic braking system in commercial vehicles is the electronic stability control function. Earlier this function was realized in a separate add-on system (own electronic control unit, sensors), in the actual generation is integrated into the EBS system with some additional, partially already integrated sensors. The electronic stability control system has a fail-silent nature, since if the system detects a failure, which would result in malfunction, it will be disabled in a safe way and the driver receives a warning that the system is not functional. This chapter deals with some special issues of the electronic stability control systems, namely introduces the work has been made in the legislative process targeting on the generation of a new regulation in the UN-ECE framework.

The electronic stability control systems (ESC) have been installed in vehicles for more than 10 years, and their impact on the traffic safety is obviously proved. Several studies from all around the world report around 30% decrease in different accident classes, even in some cases, especially the single vehicle accidents for SUVs and mini vans reach the level of reduction over 60% [85]. The equipment rate of the ESC has been increasing continuously, in Europe it exceeded 40%, in some countries (such as Germany) even higher. There are some countries, where ESC has been made mandatory for some vehicle classes (in Denmark for buses, US is close to mandate it for SUVs), and as foreseen, it goes further. In Germany the coach manufacturers made a voluntary commitment and install all vehicles with ESC. All these activities clearly show the demand of the society for improved road safety, which cannot be neglected by the law makers either. These activities forced the UN-ECE WP29 to establish a special working group in the frame of the GRRF, which is ought to investigate the legislative issues of the ESC systems, and make a proposal for that. The committee has been established at the end of 2004 with expected results at the end of 2006.

This chapter reports about the actual status of regulatory work, explaining all relevant and still open issues. Although the work has been started as a general regulation, the scope of the ad-hoc group has been changed, and primarily concentrates on commercial vehicles in a first approach, but limits neither the definitions nor the requirements for those only.

The brake systems based Electronic Stability Control systems – although they have been invented much earlier [88, 89, 90, 91] – have become typical in commercial vehicles only few years ago, and also their equipment rate is not too high (in Europe below 5%, on the other market segments does not really exists yet). The passenger cars own a lead position, since in some markets the equipment rate goes as high as 60% of the total registered car population (details see later in this chapter). The positive impact of the ESC systems on the traffic safety has been proven; many accident statistics show very impressive improvement figures in certain accident categories.

These mentioned facts (extremely different values for markets and vehicle categories, the improvement in accident statistics) together with the increasing society demand for improved

road safety raised the question towards the legislation: if it is so, why this very important field is not referred in the regulations? This is the reason why the WP29 of the UN-ECE asked GRRF to investigate this issue, and make a proposal for the future regulation framework.

- Although the ESC systems – at least technically – are easy to understand, their regulation is not so obvious, and many questions have to be answered:
- Why these systems should be regulated at all? Obviously the market recognizes their benefits without any regulation.
- Where should it be regulated? Since all state-of-the-art systems use the brake as actuator, it seems somehow logical to amend the UN-ECE Regulation 13, but what about the other future solutions?
- What should be regulated? The system itself cannot be really defined, so the stability function should be described.
- How shall it be regulated? A minimum specific design should be required or are we in a position to prescribe a test which will produce clear, measurable and assessable performance measures?

Although it is not a technical, but rather political decision, but the question of mandating the ESC for certain vehicle types, cannot be avoided.

6.5.1 Overview of the world-wide status of the ESC systems

Equipment rate. As mentioned before, the equipment rate of the ESC systems is increasing world-wide. The most significant increase can be observed in Europe, as shown in Table 6.6. From 2003 to 2004 the average rate in the countries of the European Union has grown from 29% to 36%. The highest rate has been achieved in Germany, where 64% of the total newly registered car population is already equipped with ESC system (all major German car manufacturers, such as DaimlerChrysler, BMW, Audi, Volkswagen have the ESC as standard).

Table 6.6. ESC equipment rate in Europe, 2003-2004

	2003	2004
United Kingdom	0%	30%
Germany	55%	64%
France	35%	39%
Spain	25%	30%
Italy	14%	20%
European Union	29%	36%

Looking at the other countries, USA is catching up; the equipment rate in 2004 exceeded the 11%. This dynamics however is mostly driven by passenger cars, the trucks do not participate in this growth yet, although ESC systems have been available from more manufacturers since 2003, at least in Europe for vehicles with electro-pneumatic brake systems. It is in-

interesting to observe that demand for truck ESC systems in USA seems to be much higher than in Europe, and when the system is available, the equipment rate can rapidly exceed the European values. The difference in the two markets can be found in the different fleet insurance policies.

Impact on the accident statistics. Because of the increasing equipment rate described in the previous part of this chapter, the impact of the ESC systems on the traffic accidents became measurable. Several studies have been made all around the world, out of those a good summary [86, 87] is given. The figures reported from several sources all come up with very similar figures: since ESC has been introduced the single vehicle accidents have been reduced by 30-40%, while in case of the “loss of control” type of accident this reduction goes up to 60% in case of fatal accidents. A special attention was paid to the high cg vehicles, such as minivans, SUVs, where these figures are even more impressive.

Local legislation activities. As the equipment rate is increasing, also the impact of the ESC systems seems to be proved, several countries and technical associations started to generate terms of references for the ESC. A big effort is being currently put (or even by this time these activities might be closed) into defining the requirements for ESC systems in the United States. The target of the US government is to mandate the ESC system for some vehicle classes. Denmark has recently mandated the ESC system for touring coaches, for that reason they generated an own definition what ESC is. Technical associations, such SAE are defining also the stability control systems; there are on-going activities even in New Zealand.

6.5.2 Regulation of ESC in the UN-ECE legislation framework

As it was discussed the electronic stability control systems attract quite a high attention because of their increasing equipment rate and also their very positive impact on the traffic safety (some people say that since the safety belt was invented the ESC is the second most significant system leading to dramatic improvement in the severity and frequency of vehicle accidents). Nevertheless, the situation is not very typical: the industry provides a system with the described impact, the society demand is given, but there is no regulation, which would describe what to call an ESC system, what are the design or performance requirements, and last, but not least, which are the relevant vehicle categories, where the system should be mandated. The work of the UN-ECE initiated ad-hoc expert group intends to close this gap by means providing world-wide unified terms of references for the ESC function.

Technical issues around the ESC function. Although the principal operation of the electronic stability control function is well known, there are some basic issues, which must be mentioned here. Figure 6.5 shows the control principle of the ESC function based on the so-called reference model following control.

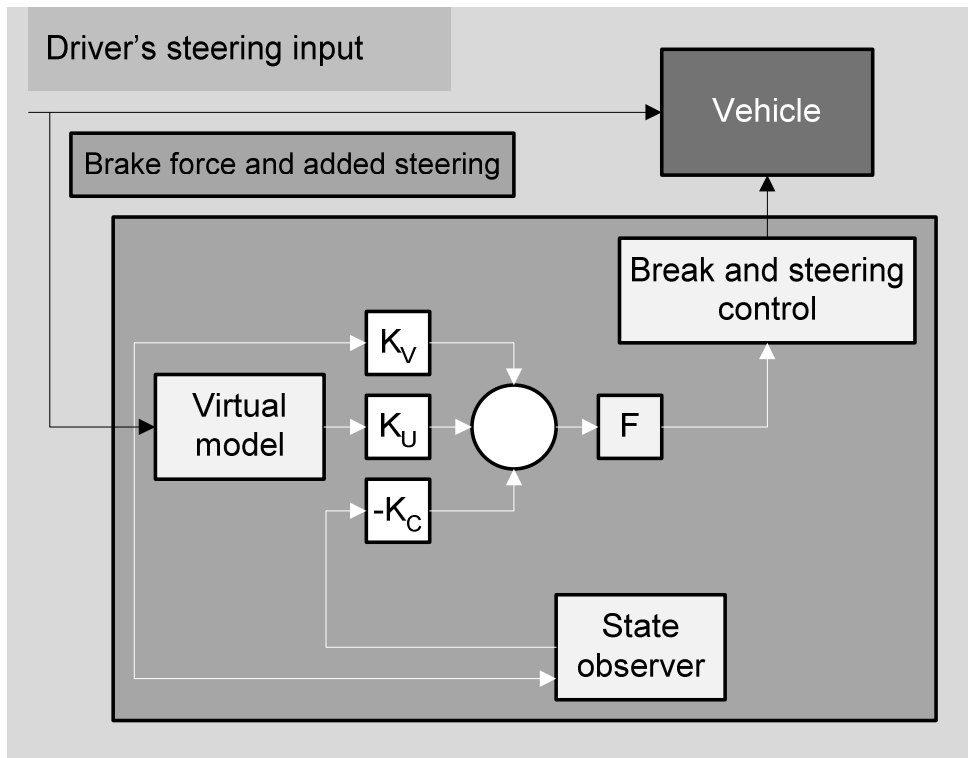


Figure 6.5. Basic control principle of the ESC function

The basic requirement for the ESC function is that the driver's intention must be followed in every situation, which means:

- The system intervenes if the driver cannot control the situation,
- The optimal vehicle behaviour is calculated from a reference model based on the measured driver's intention,
- The intervention should minimize the error between the measured and the calculated (optimal) variables.

This requirement means that although the ESC function intervenes into the vehicle dynamic behaviour, but always supports the driver, and does not make any decision against the driver's intention. In addition, similar to ABS the ESC function should have fail-silent characteristics, meaning a safe termination of its operation in case of a system failure.

When talking about ESC function one has to distinguish between the in-plane and out-of-plane functionalities, since in different vehicle types these can be separated from each other, and some vehicle might have only one of them (for example semi-trailer does not require yaw control, but roll-control).

It is important to note here that the regulation consequently talks about stability control function and not a system. The reason is that the ESC functionality – even they are functionally the same – will be realized on different platforms in passenger cars (hydraulic brake system with electric components, electro-hydraulic or electro-mechanical brake system), and in trucks (where the electro-pneumatic brake provides the platform) or in trailers.

Another problem with the unified regulation is the variety of the vehicle types: the legislation should cover a wide range starting with a simple 2-axle vehicle, up-to a 8x8 heavy truck or pusher type of articulated bus. In order to cover all these types, the regulation requires a certain level of flexibility, which, however, does not endanger the objective type approval process conducted by 3rd party institutions in the UN-ECE regulatory framework.

Definition of the function. Regardless of the system platform, sensors and actuators used, the stability control functions can be categorized into one of the two major classes: either controlling the vehicle yaw behavior or influencing the roll dynamics. The previous one covers the directional control, the latter one targets on the avoidance of roll-over. There are solutions available for both, the yaw control is the basic function of all electronic stability control systems, the roll control is used mostly in trailers as a standalone function, but also as a part of the ESC for trucks.

These two functions are defined in the text as follows:

- ‘Directional control’ means a function within a vehicle stability function that assists the driver within the physical limits of the vehicle in maintaining the direction intended by the driver in the case of a power-driven vehicle, and assists in maintaining the direction of the trailer with that of the towing vehicle in the case of a trailer.
- ‘Roll-over control’ means a function within a vehicle stability function that reacts to the potential of roll-over to stabilize the power-driven vehicle or towing vehicle and trailer combination or the trailer during dynamic manoeuvres within the physical limits of the vehicle

As seen, the definitions are giving only the basic description of the function, and not specifying anything how they should be realized, while this will be given in a special Annex to the regulation. The definition of the functions will be a part of the main text of the future regulation.

Since the above given description is only a definition, it might raise a problem: if a simple roll-over control system will be installed in the vehicle, it can also be called as vehicle stability function, meaning competitive disadvantage for those manufacturers who have the yaw control in the vehicle as well. This problem should be overcome even in the cases when the function is not mandatory to use.

Where to regulate the vehicle stability function? One of the very first questions, what the group had to answer was: where the regulation of the vehicle stability functions should be embedded? Since currently there is no vehicle level (not subsystem) regulation in the UN-ECE framework, there are four options left: to amend the ECE 13 (brake) or ECE 79 (steering) regulations as those who are dealing with the potential actuators for vehicle stability functions, or include this in the Regulation 111, or create a completely new regulation. The latter one had to be dropped rather soon, since creating a new regulation might take several years to formulate, and than until it comes into an effect can be close to 5-10 years. Regulation 111 deals with special topics of dangerous good vehicles, where the stability functions definitely

play important role, but that regulation is rather specific. The first two regulations (brake and steering) are definitely good candidates, since they exist, and have all other components necessary for the regulation of such a complicated issue as the stability function. The reason that the ECE 13 has been chosen is that all the state-of-the-art stability control systems use the brake as a primary actuator for influencing the vehicle dynamical behaviour in the most efficient way. In addition, the ECE 13 provides the frame for such an amendment. Of course, this does not exclude any other potential future actuator (for example the steering system with angle or torque superimposing possibilities will appear in the vehicle stability arena shortly), a reference to those regulations (if any, ECE 79 for the steering) can be made.

How to regulate? One of the most critical questions is how to regulate the vehicle stability function? There are two competing concepts can be followed:

- A design based requirement set, meaning that only the system can qualify for stability function, which fulfils a number of design criteria (number and type of sensors, actuators, intelligence, layout etc.). In this case is the assumption is that if all the components in the prescribed hierarchy are installed in the vehicle, the system will provide the legislation required performance (if any).
- A clearly defined performance requirement, where only the expected performance limits and the related test methodology is defined, all the rest is up-to the system and vehicle manufacturers how they achieve these goals.

Design vs. performance requirements. Both concepts have advantages and disadvantages, but sometimes certain compromise has to be found. At the beginning of the ABS introduction, the ECE 13 specified design requirements, since there was no clearly defined test and performance criteria developed (lack of experience with a new system), which has been modified over the years and now it is more performance requirement what we have today.

The ad-hoc group faces this challenge as well, since on one hand it would be much easier to define clear, easy measurable, objective performance requirement, but on the other hand the large variety of vehicles, the lacking experience how to make such investigations by third party (technical services) raise several problems.

The vehicle and system manufacturers make a wide variety of function test during the product development however, most of these are not standardized tests due to the specialties of the stability functions. Also these tests require conditions, which are normally not available everywhere (reproducible surface conditions for low adhesion investigations normally available for bigger manufacturers close to the arctic circle, large vehicle dynamic surfaces). Also the vehicle installation required for such tests (safety cage, anti-jackknifing device, outrigger, etc.) in a wide variety is not easy and cheap to be solved. If the 3rd party investigations must be conducted at these conditions, will result in additional burden on the vehicle manufacturers, what they are unwilling to pay, since they already made it all. In addition, there is no unified test and evaluation procedure for the earlier mentioned variety of vehicle and systems today.

Current proposal – a mixture of performance and design based requirements. The challenging task of the working group was (in fact, still is) to find a solution, which is somewhere in between the design and performance requirements. The short content of the current proposal can be summarized as follows:

- In case of the applied actuators a certain minimum level of design is prescribed: the autonomous (i.e. driver independent) engine control and individual wheel brake application (either automatically commanded or wheel/axle selective) must be possible. The justification for these design requirements is clear: the brake system is able to control the tire in-plane forces in the entire slip range (unlike steering does), and the engine throttle control, which is an effective means of reducing the kinetic energy of the vehicle. Other actuators (i.e. steering, controlled torsion bar, etc.) not excluded either, but only in combination with the brake and engine control systems. These design constraints are not questioned by the technical community, everybody seems to accept that an efficient stability control cannot function without them. In addition, both systems are state-of-the-art both in passenger cars and commercial vehicles as well, unlike the others, which will come in the future and will require longer time to become state-of-the-art.
- Although in the very first version of the proposal similar design constraints have been defined for the sensors, it was replaced by more performance like requirements. In the current version of the text the yaw rate as a variable which must be controlled is defined for the in-plane stabilization, and the vertical tire load for the roll control, no sensor is specified how to obtain these values. Any sensor could be used to generate these variables, provided that the calculated signal is available under any conditions, generated by a on-board sensor and shows a good alignment with a reference signal proved by the technical service. This was necessary in order to recognize the rapid technological development of vehicle on-board sensors.
- In order to temporarily overcome the difficulties with the third party testing and the lacking performance criteria, the group proposes a solution, which goes towards the unified testing and performance measurement. It means the following:
 - The technical service should make a dynamic demonstrative test on one vehicle configuration, which shall include the critical conditions of directional control and roll-over as appropriate to the vehicle stability function installed on the vehicle with the method of demonstration and results being appended to the type approval report. This test may be carried-out other than at the time of type approval, opening the opportunity for the technical service to use the facilities and installation of the vehicle manufacturer thus reducing the costs. The type of the test should be agreed between the technical service and vehicle manufacturer,
 - For the other vehicle configurations (but equipped with the same stability function) it is enough to submit measurement data made earlier by the manufacturer, or
 - Computer simulation data can also be used, provided that the simulator is validated and verified on measured data. This is a new element in the UN-ECE regulation framework,

a special appendix to the annex is being created in order to specify the conditions of the simulation.

Following the above logic, the ad-hoc working group believes that this amendment to the Regulation 13 can be introduced short termed, and can effectively regulate the vehicle stability function related issues. Of course, and there is an agreement in the group in this matter, this regulation will be re-worked in a certain time. The stability control systems still in their infancy, the rapid technology development in the actuator and sensor field will bring new and new solutions, which must be considered, but this very important field should not be left un-addressed in the legislation already today.

Effect of the amendment – why it is important to generate terms of references? The mandate of the group was limited to technical investigations, but some “political” questions cannot be separated entirely. There are several fields, where the clear definition and requirements of the stability function is needed: when the function is mandated, when incentive is given to the vehicles (road toll and tax reduction), or in general, if a vehicle is fitted with the function, it must comply with the regulations (like in case of ABS).

This is the question of mandating the stability function, which is purely a political decision. The group has been asked, where does the mandating bring the highest impact on traffic safety? Based on the attempts have been made so far, and the availability of the function for the vehicle categories, the group proposes to start with touring coaches, where the directional stabilization will be required, and in case of dangerous good vehicles the semi-trailer tractors must have at least directional, semi-trailers at least roll-over control function

The chapter described the current status and the main directions of the electronic stability control function-related UN-ECE regulatory activities [FT13, FT18]. Because of the complexity of the system, it is not obvious how to structure the regulation, and many questions have been asked. The current version of the proposal attempts to find an acceptable compromise among the different expectations in order to submit a consolidated amendment to the Regulation 13 as soon as possible. Due to the infancy of the stability control systems it will be modified based on the experiences on the other legislative solutions (such as the one will be introduced in the US), investigations of public institutions, technical services and also the manufacturers.

7. STATE-OF-THE-ART ARCHITECTURES IN ROAD VEHICLES

The issue of safety is of increasing importance also in the automotive industries. This includes making driving and the components, their architecture safer. This latter, system safety, depends strongly on the failure probability of individual components and how the handles different faults, errors and failures [27]. In wide interpretation, under the notion of dependability, system safety expresses operation without catastrophic events harming users and the environment [28], while reliability and availability presents the continuity in system readiness. Regarding reliability is more precised concerning its time dependence from which availability can be derived (see 5.2).

In today's automotive industry, companies are organized into simultaneous engineering teams to develop their new products. The new way of doing business enables some companies to develop their new products quicker, cheaper with higher quality and reliability. In the past few years there has been the tendency to increase the safety of vehicles by introducing intelligent assistance systems (e.g. ABS, Brake Assistant (BA), ESP, etc.) that help the driver to cope with critical driving situations. These functions are characterized by the active control of the driving dynamics by distributed assistance systems, which therefore need a reliable communication network.

The faults in the electronic components, which control these functions, are safety-critical. However, the assistance functions deliver only an add-on service in accordance with a fail-safe strategy for the electronic components. If there is any doubt about the correct behaviour of the assistance system, it will be switched off. For by-wire systems without a mechanical back-up a new dimension of safety requirements for automotive electronics is reached. After a fault the system has to be fail-operational until a safe state is reached [17].

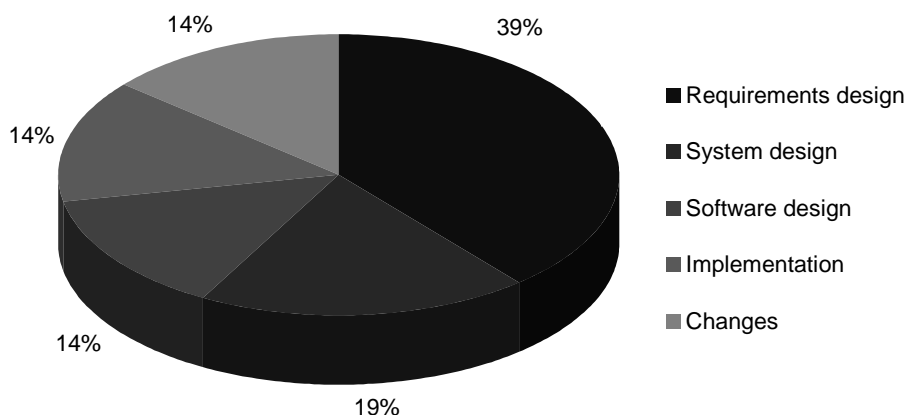


Figure 7.1. Main accident cause for all road users

Currently, only limited statistics are available regarding accidents involving trucks and even less is known about the cause of these accidents. To fill in this lack of knowledge, the European Commission (EC) and the International Road Transport Union (IRU) launched a unique scientific study, the European Truck Accident Causation (ETAC) study [119]. Knowing that there are many factors which contribute to an accident and knowing that those factors are interlinked, the aim of the study is to identify the main causes of accidents involving trucks. From a research point of view, the main cause is the cause which has made the greatest contribution to the fact that the accident happened (Figure 7.1).

In the architectures of currently designed vehicle systems will be included a significant percentage of electronics, communications and software in safety-critical systems, thus making these systems very complex [27, 29]. Today 30% of the cost of a car is in electronics and 4 % of the production costs are Software. Until 2010 this will increase to 13% and 90% of all the new innovations will be based on electronic systems. Currently, the average number of micro-controllers per automobile vehicle is about 25 [27] and this number is expected to increase in the following decade. It has been estimated that the number of in-vehicle networks currently is about 5 and will reach 15 in the year 2015. System complexity raises also safety questions concerning their impact of the vehicle and its occupants. Safety-critical systems need to be carefully and properly designed (Figure 7.2) and certified by appropriate certification body.

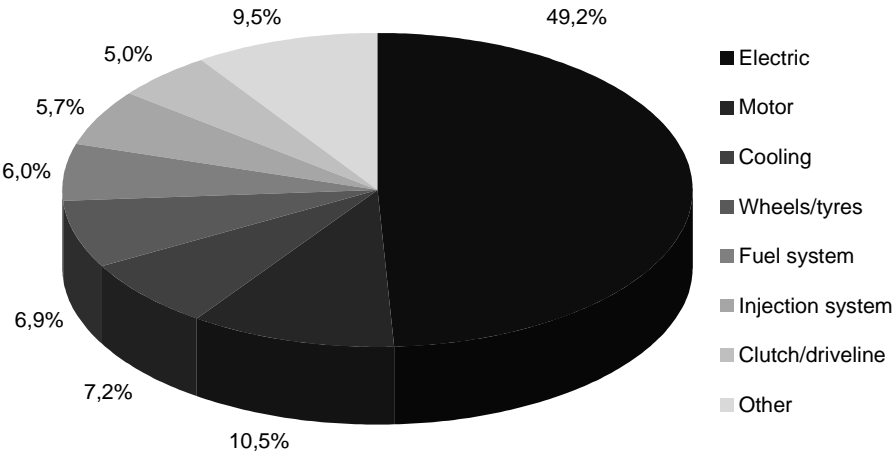


Figure 7.2. Main problems occurring in cars

For automotive, the certification standards (Figure 7.3) most likely to be used will be similar to e.g. IEC 61508 (see 6.1.1), which is a European generic safety standard for industrial systems. A UK consortium of automotive companies published the MISRA guidelines specifically for vehicle-based systems. MISRA is a consortium of UK motor manufacturers and electronics suppliers, which was responsible for the production, in 1994, of the ‘Development guidelines for vehicle based software’ (also known as the ‘MISRA Guidelines’). These have received widespread use throughout the international automotive electronics industry. The MISRA Guidelines provide important advice to the automotive industry for the creation and

application of safe, reliable software within vehicles. The Guidelines are intended to use by all those involved in the creation, procurement and support of vehicle based software. Users may be within vehicle design and manufacturing companies, component suppliers, development tool suppliers and diagnostic equipment suppliers. The Guidelines encapsulate many principles and concepts, such as:

- Safety, like justice and democracy, must be seen to be present.
- Software robustness, reliability and safety, like quality should be built rather than added on the requirements for human safety and security of property can be in conflict. Safety must take precedence.
- System design should consider both random and systematic faults.
- It is necessary to demonstrate robustness, not rely on the absence of failures.
- Safety considerations should apply across the design, manufacture, operation, servicing and disposal of products.

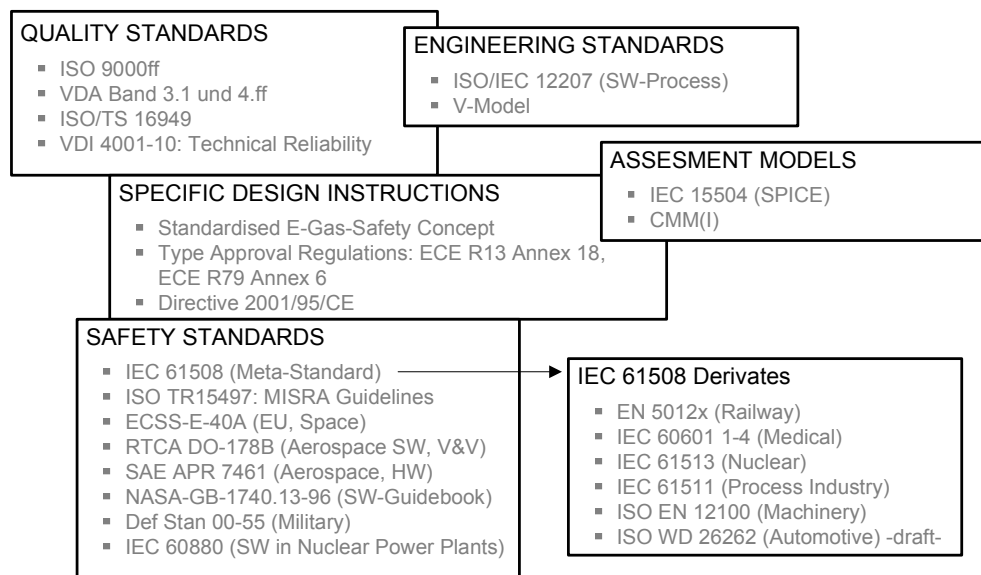


Figure 7.3. Standards and regulations: overview

7.1 ANALOGY BETWEEN ROAD VEHICLES AND AVIONICS SYSTEMS

The safety-criticality of commercial vehicle accidents – although it does not attract so high attention – is as high as those of the aircraft crashes, since its frequency is much higher. Therefore the legislation started to put more pressure on the manufacturers to increase the safety level of their products. The requirements for the safety-critical electronic systems are clearly defined in the IEC 61508 (European standard (EN 61508)), whose application has been started in the type approval process in some countries (e.g. Germany, FAKRA – Fachnormenausschuss Kraftfahrzeuge). ISO has recently started a new work item to develop an automotive functional safety standard (ISO TC22/SC3/WG16) based on a more direct interpreta-

tion of IEC 61508, although this standard is not expected to be published until 2008 (Figure 7.4).

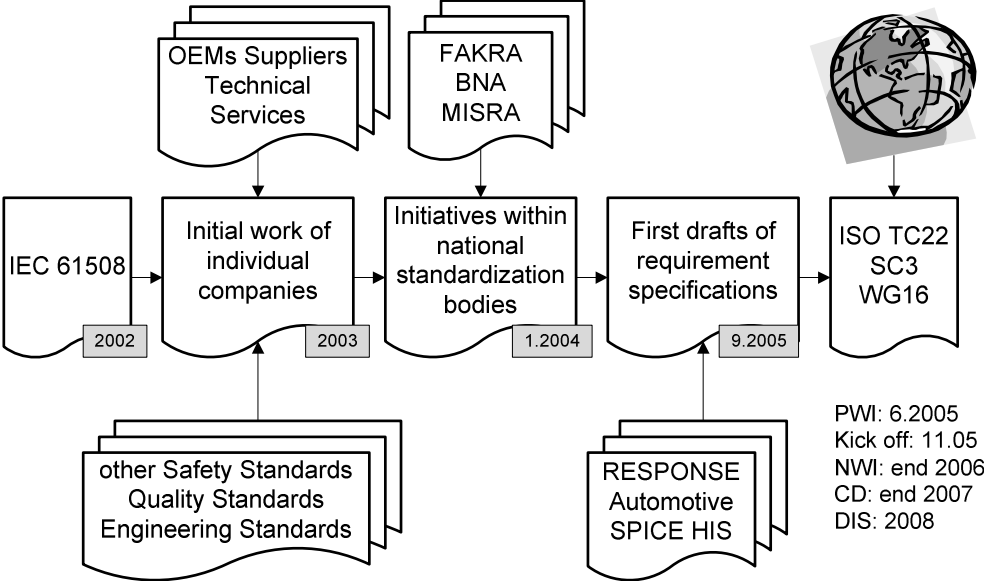


Figure 7.4. Automotive application of IEC 61508: roll out of ISO WD 26262

By-wire systems have been established for several years in the area of aircraft construction (fly-by-wire) and there are now approaches to utilize this technology in vehicles (Figure 7.5). The required electronic systems must evidently be available and safe. In the same time the requirements of mass production have to be reached (long life time, long maintainability intervals, low costs [26, 67], fulfilment of standards). In the last few years there is an endeavour in the automotive industry to realize by-wire applications without mechanical, pneumatic or hydraulic back-up systems in vehicles [81]. The required electronic systems must be highly reliable and cost-effective due to the constraints of mass production [17].

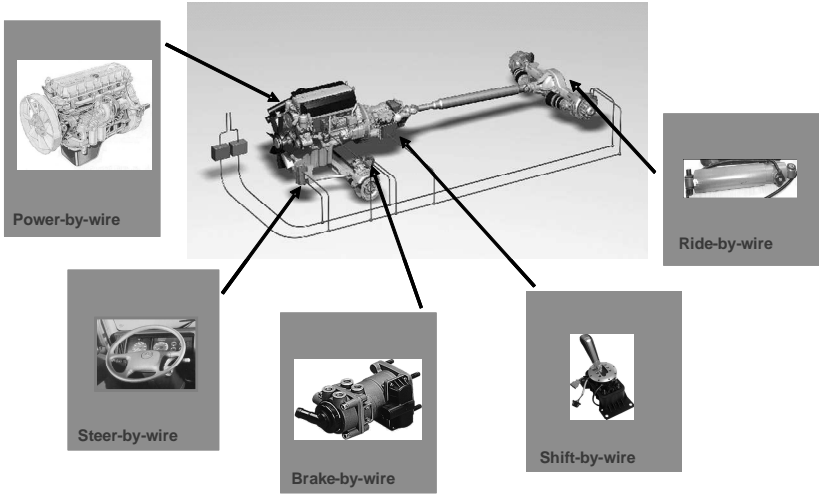


Figure 7.5. By-wire vehicle systems

Further examinations deals with and focuses on one of the safety-critical by-wire systems. Brake-by-wire systems are investigated according to their functionality and advanced feature in commercial vehicle safety. In comparison to systems in avionics similar operability consequences can be drawn. Chapter 9 presents a qualitative reliability analysis of a fully electronically controlled semi-trailer brake system.

The brake system of an aircraft is considered to be a highly critical while the plane is taking-off (in case of rejected take-off it has to decelerate the fully loaded plane) and at landing (when its not proper might lead to uncontrollability, blown-up tire or deceleration disability), since can lead to severe accident endangering the life of the passengers and high economical losses. This explains the layout of a typical airplane brake system.

Both the control and the energy supply are redundant, at least all deterministic components are double, in some of the cases there is a third hydraulic circuit used in case of the failure of the primary systems. In case of a single failure the system remains fully functional, and if a second failure occurs, brake force still available to provide a limited function in this degraded mode. What is important to note is that in addition to the physical system redundancy the human (subjective) controller, the pilot is also redundant. In case of one of them is functionally impaired, or makes an improper decision, the other can completely overrule it, since has all necessary systems at hand, which work independently of the other control/energy circuit.

The braking systems of aircraft and cars have not the principal different except the big different in energy must be absorbed and no time for cooling the aircraft brakes. Therefore the brakes for aircraft are made from several rotated and fixed disks. The disks are pressed by pistons during braking. Material of the brake linings is made from steel or composite. The composite materials have much more heat resistance. The operational conditions of brakes applied on small aircrafts of general aviation are close to the condition of car brake operation. The market of these small aircrafts is increasing more rapidly than commercial and military aviation.

Table 7.1. A comparison of the mentioned industries

Aircraft	Automobile
Long life cycles	Short life cycle
Long time to market	Short time to market
Low number of products and parts	High number of products and parts
Strict safety reliability requirements given and proofed by authorities	
Direct impact on human beings	
Highly complex	
About 1/3 of equipment is E/E/EP	
High pressure for innovations	
High operational reliability required by customer	

Difference can be evaluated in comparison to design purposes, operational condition and innovation process applied. This can be characterized with cooperative development of the new products, long life cycle and long time to market. Comparison of automation and aeronautical industry can be defined as it demonstrated by table 7.1. May be the most important different is included into the quality management (see 6.2.1).

If one wants to establish a direct analogy to the safety-critical systems of an airplane, a very similar system architecture will be defined. In the EU project 5th Frame Program supported PEIT (see 7.2.1) project (Powertrain Equipped with Intelligent Technologies) system architecture has been specified, designed and realized in a prototype truck.

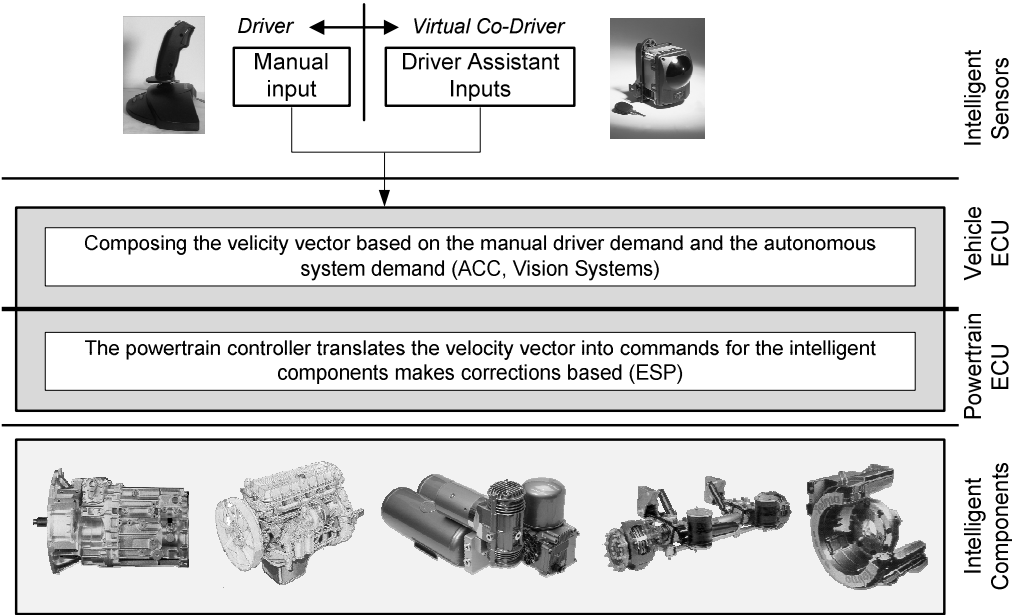


Figure 7.6. Analogue vehicle control structure to the airplane systems

As shown in figure 7.6, the architecture has 2 layers, which are separated logically as well as physically:

- The command layer (which physically represents the truck cabin with the driver interfaces and intelligent sensors) collects all the information about the vehicle direction and the surrounding and composes the so called targeted motion vector
- The execution layer (which is the power train with all the actuators and sensors) commands the individual actuators and realizes the motion vector.

When analyzing the system shown in the figure, one can note the composition of the motion vector is very similar to the way as the 2 pilots control their airplane. If one makes a failure in the sensing, or misjudges the situation and takes an improper action, the other can still modify it. It is the same here, but instead of a second human driver, the sensors collecting information about the environment (radar and video sensor, external information about the road conditions, whether, etc.) and also the physical driver (whether he is really able to control his

vehicle) play the role of a ‘virtual co-driver’. In order to make the autonomous vehicle control safely possible (in case of level 2 for the judgment, and level 3), the information from the command layer must be transmitted to the execution layer in a redundant way, and also the execution layer must have redundant communication and energy supply architecture.

In this chapter the iso- and homomorphic system relations were demonstrated according to reliability design and analysis between the future commercial vehicle and today’s aircraft electronic control and brake systems.

7.2 BRAKE SYSTEM ARCHITECTURES OF HEAVY COMMERCIAL VEHICLE

The following picture (Figure 7.7) shows the system architecture of the since 1996 in heavy commercial vehicle classes typical (in Europe) brake system architecture.

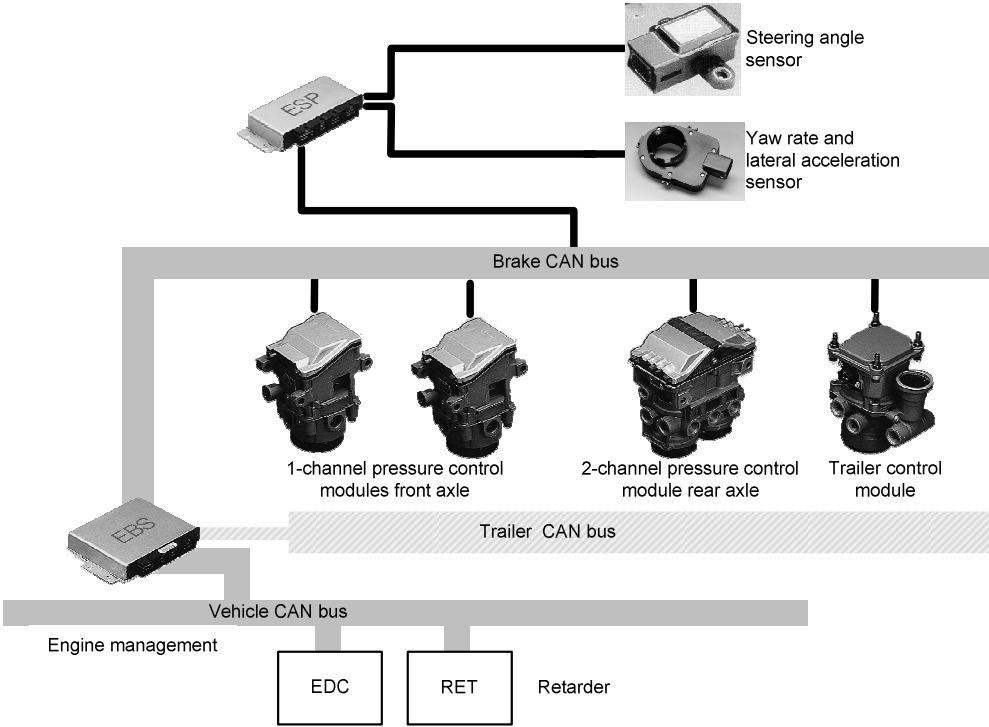


Figure 7.7. ‘Typical’ brake system architecture

The main components of the system are the central Electronic Control Unit of the Electronic Brake System (EBS ECU) maintaining communication on several Controller Area Network (CAN) interfaces to the vehicle, to the trailer control and also a defined proprietary brake CAN. The wheel/axle brake control modules are connected to the brake CAN bus; their control will be executed via this bus. Depending on the system, the control software modules are distributed between the central and the module ECUs. The ESP can have a separate ECU connected to the brake CAN bus (see the figure above) or can also be integrated into the central ECU, and a separate CAN bus is defined for the sensors.

Concerning the level of redundancy, these systems have a single electronic circuit (which controls all modulators) and – as a definite customer requirement – also double pneumatic circuit as a back-up system. In case of a single failure in the electronic circuit, depending on the severity of the occurred failure the system switches back into a partial or a full back-up mode, in which concerning the basic brake function, there is a full redundancy. This layout fulfils the related legislative requirements, but in the full pneumatic back-up mode several functions are not available. Such a system is called as 1E+2P (one electronic circuit, two pneumatic circuits).

Because of cost and design constraints, there is a continuous discussion about leaving one of the pneumatic circuits from the system, since the related standards can also be fulfilled with a 1E+1P layout, meaning that the pneumatic back-up circuit either from the trailer control valve or from the rear axle can be cancelled or from both. The table below shows most of the possible layouts for 1E+2P (but no back-up on the rear axle or in the trailer control valve) with 2 circuit pneumatic foot brake valve, and also the 1E+1P layouts, where the Foot Brake Module (FBM) has only single circuit.

In order to understand the evolution of the brake-by-wire system, it is necessary to get an insight into the state-of-the-art electronic braking system and their redundancy levels. Table 7.2 shows most of the possible layouts for 1E+2P (but no back-up on the rear axle or in the trailer control valve) with 2 circuit pneumatic foot brake valve, and also the 1E+1P layouts, where the FBM has only single circuit.

Table 7.2. Possible layouts for brake systems in terms of their back-up

	Rear axle with back-up		Rear axle without back-up	
	TCM with 2P	TCM with 1P	TCM with 2P	TCM with 1P
FBM with 2P+1E				
FBM with 1P+1E				

The two 1E+1P layouts fulfil the legislative requirements keeping the fail-safe nature of the basic brake system of the vehicle (means that the system will provide the legislation required reduced brake performance in case of a single failure). However, if the electronic circuit is not intact, no functions like ABS, brake force distribution, etc. are available.

The 1E+1P architecture, however, would not suit the purposes of the automatic driving, since external brake actuation is not possible in the pneumatic back-up mode. This means that from this perspective the system neither is fault-tolerant nor fail-safe.

7.2.1 Safety considerations of specific brake-by-wire architectures

Although (as described in the previous part) the 2E brake system architecture of the PEIT is not fully fault-tolerant (at least in the classical sense: all functions are provided without any performance reduction in case of a failure), but this architecture provides several features, which result in enhanced system performance even if – as a consequence of a single failure – one of circuits is not intact, and as such, provides enhanced safety in comparison to the 2P, 1E+2P and 1E+1P systems [97].

In case of the 1E+2P or 1E+1P system a single failure potentially leads to a non-functioning electronic circuit, which from the system performance viewpoint means the loss of all functions, since the typical brake functions (load sensing, CFC, ABS, ESP, slip control, etc.) are realized only electronically, no mechanic/pneumatic back-up is available. The 2E architecture – where all functions are being computed in both ECUs – however can provide several functions even on the partially disabled hardware.

If the front axle control circuit fails, the rear axle can realize functions like ABS, ATC, DTC, load proportioning, etc. Some part of the ESP functionality would also be possible (understeer compensation). Similarly, in case of a rear axle control circuit failure the front axle brake control can realize functions, which are in pneumatic mode not available, such as tilt prevention, ABS on the front axle, some ESP functionality (compensation of the oversteered behaviour); brake assistant functions can be provided. In both cases the trailer control (CFC, roll-over prevention function), the engine and retarder control (non-friction brake integration) functions are fully available, thus reducing the load on the friction brake and providing the trailer stability.

The 2 1E+1P layouts fulfil the legislative requirements keeping the fail-safe nature of the basic brake system of the vehicle (means that the system will provide the legislation required reduced brake performance in case of a single failure). However, if the electronic circuit is not intact, no functions like ABS, brake force distribution, etc. available.

The 1E+1P architecture, however, would not suit the purposes of the automatic driving, since external brake actuation is not possible in the pneumatic back-up mode. This means that from this perspective the system neither is fault-tolerant nor fail-safe. In order to handle the problem of the automatic drive (or so called platooning) problem, a fully fault-tolerant, redundant brake system has been developed in the framework of the EU supported Chauffeur 2 project. Although the system is fully fault-tolerant, its realization in the practical life is difficult, primarily because of the very high costs. Nevertheless, it was a very useful exercise in order to understand the requirements for such a system, and many other, lower safety requirement applications can be deduced from that.

The Chauffeur 2 project sets the requirement for a fully fault-tolerant system providing the full system performance in case of a single failure. This requirement, however, results in a system architecture (2E), which is highly complex, all components, communication and power interfaces are doubled (Figure 7.8), and as such, in this form, is not marketable.

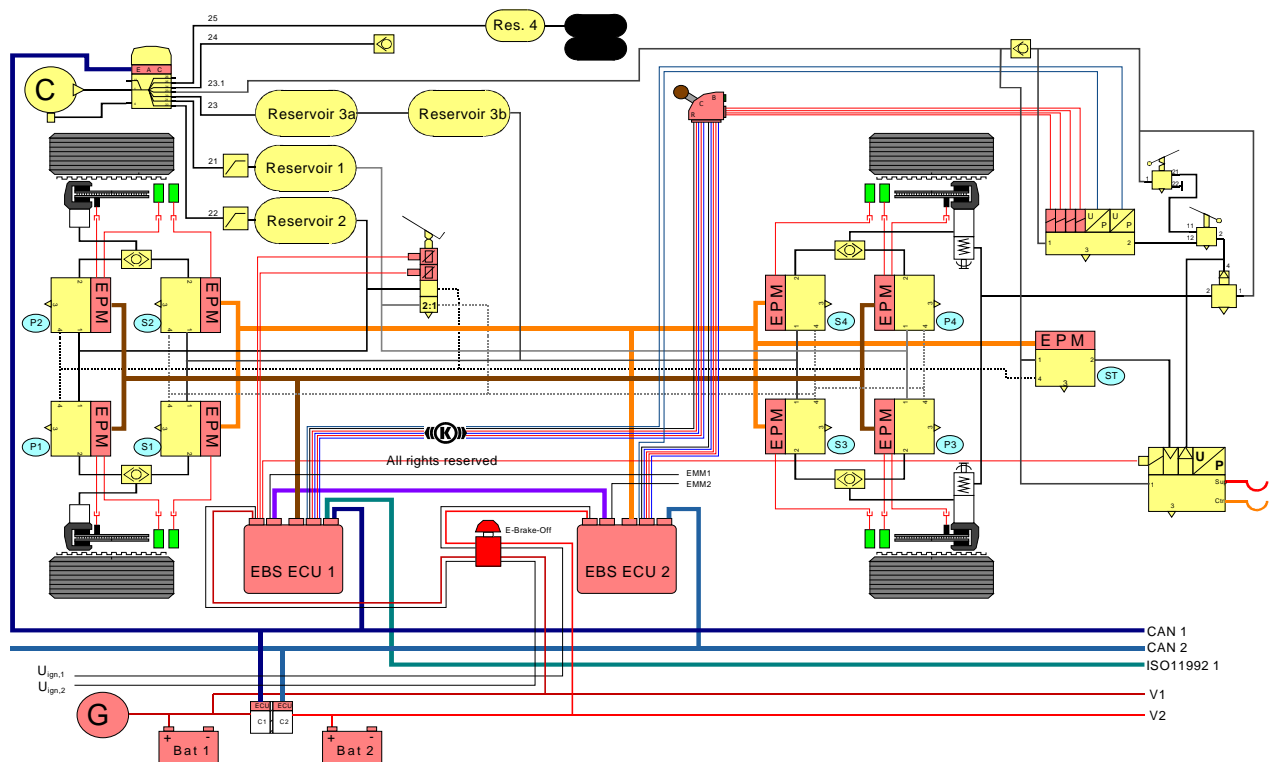


Figure 7.8. Chauffeur 2 system architecture

The PEIT system architecture is a compromise, which can be found between the 1E+1P ‘conventional’ electronic braking systems and the Chauffeur 2 solution, but provides an ultimate solution for fulfilling the requirements of the automated driving and the related standards, and also the cost/installation requirements of the customer (Figure 7.9).

The brake system is totally controlled by means of electronic circuits and electronic/electric commands/signals. Actuation however remained pneumatic, as compressed air is necessary on board anyway and pneumatic actuators are very economical and effective.

The production of compressed air remains similar to the conventional vehicles, there is no redundancy foreseen (unlike in airplanes, where the energy generation is also redundant). The compressed air of the brake system is then stored in three independent reservoirs. Separation is solved by a four circuit protection valve. Reservoir 1 supplies the front axle’s electro-pneumatic modulators (EPM), reservoir 2 supplies the rear axle’s EPMs, while reservoir 3 supplies the parking and trailer brake systems. This layout fully corresponds with the legal requirements. The electric energy supply also has to be redundant, but it is enough to have one ultimate source like alternator and then store energy in redundant storages (batteries), which are galvanically separated. However, the availability of the other energy storage device (either the pneumatic reservoir, or the battery) must be guaranteed in case of a failure in the other circuit by an appropriate management system, as shown in the figure.

From the control aspect, important is that the brake system is supplied by a dual electric supply. These are EBS ECU1 and EBS ECU2. All other components are supplied through the ECUs. The intelligent components like EPMs are organised into two groups. Group one (EPM A and EPM B) is supplied by ECU1, while group two (EPM C, EPM D and EPM E)

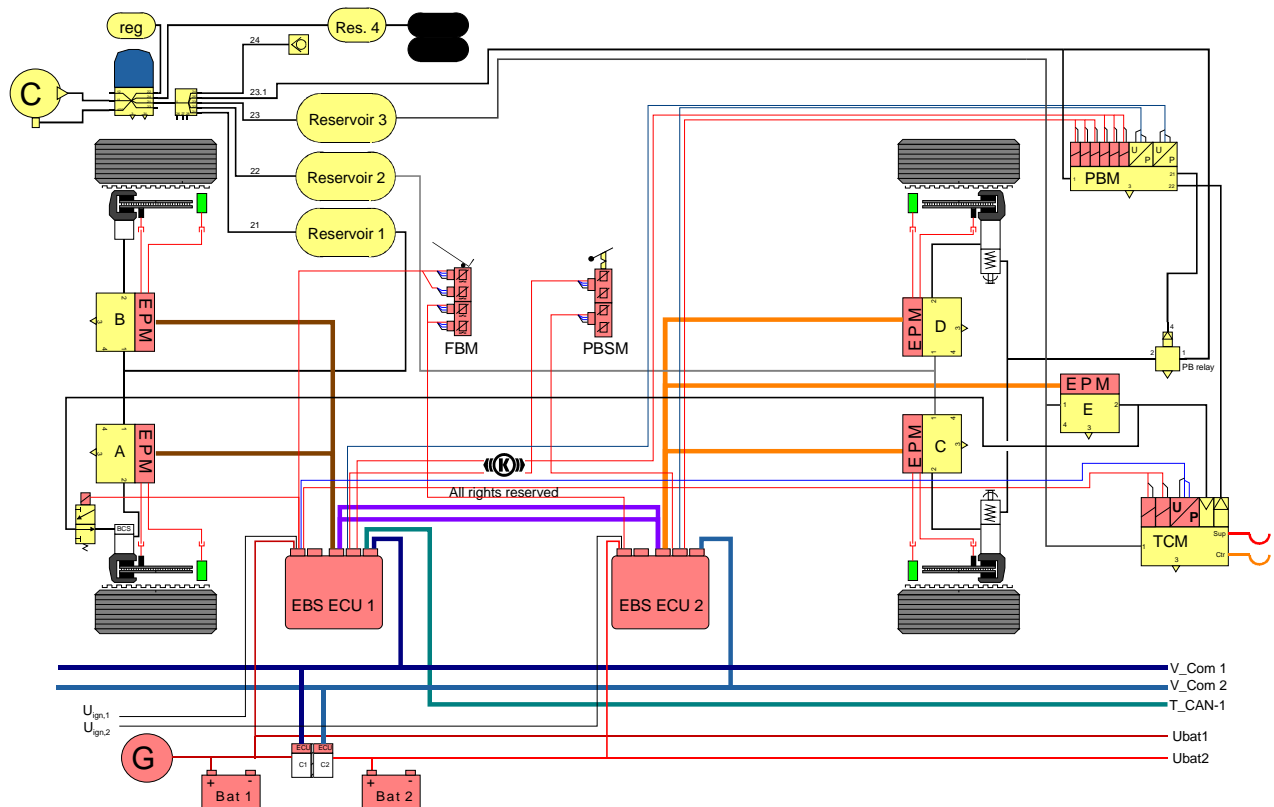


Figure 7.9. PEIT system architecture

are supplied by ECU2. Controls, like foot brake module (FBM) and parking brake stick module (PBSM) are themselves one-piece duo-duplex units, so these are supplied by both ECUs so, that galvanic isolation is solved. The parking brake module is a one-piece duo-duplex unit, but it has only electric coils in it, which are driven by either ECU1 or ECU2 so that galvanic isolation is guaranteed. The trailer control module (TCM) is a series product of a today simplex EBS, so its duo-duplex electronic control required that its electrically controllable interface is connected to ECU1, while its pneumatically controllable interface (control pressure input) is connected to EPM E, which is controlled by ECU2.

There is no mixing of electric power supplies, not even through semiconductors. Control of the brake system will be done by the driver as before, or by the superior electronic control called Power Train Controller (PTC). Complex modes are possible too, where the PTC modifies the driver's input in case of e.g. ESP situations, which increases the reactive active safety of the vehicle. This dual behaviour is achieved by a simple logic. EBS controls the brakes in a closed control loop, based on the driver's demands. In such a case EBS will control the brakes based on the values received from the superior ECU (PTC). If the brake system is controlled by the driver, then the usual brake controls can be used: the pedal (FBM) and the lever of the parking brake. These are exclusive electronic ones.

There are two 'central' EBS ECUs, but there is one vehicle to be controlled, so an appropriate control strategy had to be established. In the case of this architecture of the service brake, one has to distinguish between physical and logical control. Physically there are two groups of electro-pneumatic modulators, each subordinated to exclusively one of the main

ECUs. ECU1 controls the front and ECU2 the rear axle physically. Logical control means, where the current control parameters of a given axle come from. There are two communication paths between ECU1 and ECU2. Using these, it is possible that ECU1 builds a command, sends it to ECU2 and ECU2 transmits to their EPMS bind to it.

Concerning the above described and realized different kinds of solution for fulfilling legal and customer requirements without mentioning all of them; the process of designing a conceived, predetermined redundant electronic brake system is an iterative method applying various reliability analysis techniques. The realization of the system described previously, however, is rather complex. Technically its realization is in the pipeline, but the cost, legal and moral aspects should also be considered. The commercial vehicle industry is driven mostly by cost objectives, which cannot be neglected in the design process. In addition, the legislation does not require full redundancy for the brake-by-wire system, only a single failure must be tolerated with a defined performance decay (50%). Of course, this is different for the steer-by-wire systems, where a 100% fault-tolerance is required.

As mentioned above the brake system related regulation (UN-ECE Reg. 13) does not require a completely fault-tolerant architecture, a single failure should be tolerated with permissible function decay. However, the autonomous drive systems in some of the cases (for example the so called platooning, when vehicles follow each other in a certain distance, and only the lead vehicle is controlled by a driver, the rest of the platoon drives autonomously) would require a full tolerance of a single failure. This leads to a system architecture, where all the components are duplicated, and a safe switch from the faulty system to the one, which is intact guaranteed. This can be realized, but with all the consequences: increased complexity, price, weight, etc. In order to at least partially fulfil the conditions of the autonomous drive, a different system architecture has been designed as shown in Figure PEIT.

Summarizing this chapter the iso- and homomorphic relation of electronic brake systems (2E) were analysed and the connections with the relative systems of legislation were demonstrated, in so far as these architectures meet the legislative requirements without providing pneumatic back-up mode [FT9].

8. SPECIAL APPLICATION OF A DESIGN METHOD FOR REDUNDANT ELECTRONIC BRAKE SYSTEM

The vast majority of available safety tools and methods [27, 29] support severity analysis also combining other system features from different aspects. The overall goal in designing a safety-critical system is eliminate hazards from the design or to minimize risk by modifying the design so there is a very low probability of the hazard occurring. Safety in design means that the examined specification is correctly implemented, no failure occurs, the system operation will not result in a catastrophic event. Safety of a system can be expressed by the strategy of design, which means that the risk of faults or failure leading to an undesired event must be eliminated or minimized by using fail-safe or fault-tolerant procedures. The length of time of hazard occurrence must be maximally reduced if the hazard can not be completely eliminated.

8.1 OVERVIEW OF DESIGN TECHNIQUES

The used techniques to enhance reliability can also call tools to their aid, e.g. fuzzy logic, neural networks [44, 75] and Pascal programs [45] or combination of methods, e.g. functional block diagrams [68], BDD (Binary Decision Diagram) [70, 71, 73], RBD (reliability block diagram) with a simplified Markov model and conditional probabilities that reflect the dependence among system elements [47], Markov chains [116] or confidence level (PVCL – Probabilistic Varied Confidence Level) [66]. Reliability prediction can be conducted by pattern recognition (statistic classification), which is called a certain mathematical-statistical method of concluding from a number n of known variables on another – unknown – variable [34]. Classification of analysis techniques (Figure 8.1) according to [18]:

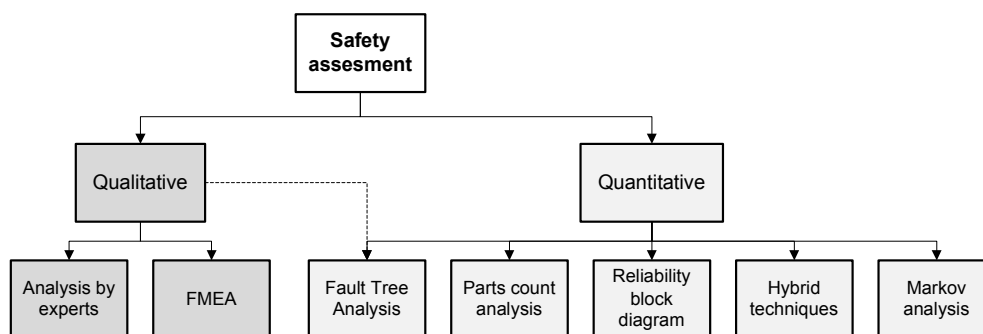


Figure 8.1. Classification of qualitative-quantitative techniques

The most wide-spread and legally prescribed (UN-ECE Reg. 13, Annex 18, 3.4.4.) two techniques are the Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA), which are usually combined before their use with systematic, functional techniques, e.g. RBD [11, 33, 35, 36, 40, 41]. It can be ambivalent how to classify these techniques, be-

cause on the one hand it is stated and visible that FTA has proper quantitative nature, but on the other hand it has also qualitative nature, because of e.g. sensitivity analysis. For FMEA there are solutions about integrating failure costs [60] into these forms and to order according their highness. According to this aspect we can call FMEA a quantitative technique as well, however not from the reliability point of view, but the possible integrated expenditure for it. Combination of different techniques with FMEA is often used, e.g. combining with sneak circuit analysis (SCA) [54], fault tree analysis [61], event sequence analysis [53]. SCA and FMEA focus on a different, but vital, aspect of the system functioning. Both analyses should be performed to validate and produce a robust design. A variation and efficient combination of a special kind of FMEA and FTA will be presented.

The table below (Table 8.1) shows an overview and classification of different analyses according to their usefulness [3] in each development phase.

Table 8.1. Reliability tool matrix (1: Primary Usage, 2: Secondary Usage)

	Planning	Product design & development	Process design & development	Product & process validation	Production
Accelerated Testing		1		1	2
Benchmarking	1	1	2		1
Degradation Analysis	2	1	1	1	1
Design For Manufacturing And Assembly (DFMA)		1	1	1	2
Design Of Experiments (DOE)		1	1	2	1
Design Reviews	1	1	1	1	
Design Selection And Optimization		1	1	2	
Early Warning Problem Identification					1
Environmental Stress Screening				2	1
Error Proofing/Fail Safing/Poka Yoke		1	1		
Failure Modes And Effects Analysis (FMEA)	2	1	1	1	2
Failure Reporting, Analysis And Corrective Action System (FRACAS)	2	2	1	1	1
Fault Tree Analysis	2	1		2	2
Finite Element Analysis		1		2	
Functional Block Diagrams	1	2			
Highly Accelerated Life Test (HALT)/ Stress Screening (HASS)		1			2
Life Cycle Cost Analysis	2	1		1	2
Life Data Analysis		1	1	1	1
Measurement Systems Analysis	1			1	
Multi-Vari Analysis			1	1	1
Parameter Diagrams	1	1			

	Planning	Product design & development	Process design & development	Product & process validation	Production
Part Derating	2	1		2	
Problem-Solving - Root Cause Analysis	2	1	1	1	1
Process Capability Studies			1	1	2
Process Flow Chart / Map			1	2	1
Product Performance Specifications	1	1			
Product Reliability Plan	1	2	2	2	2
Product Scorecard	2	1	1	1	2
Production Part Approval Process (PPAP)				1	
Quality Function Deployment (QFD)	1	1	1	1	
Reliability Allocation Model	1	2	2	2	
Reliability Block Diagrams	2	1			
Reliability Centered Maintenance		1	1	2	2
Reliability Growth Modelling (Crow/AMSAA)	2	1	2	1	2
Reliability Prediction	1	1			
Safety Hazard Analysis	2	1	1	1	1
Sneak Circuit Analysis	2	1	1	1	
Software Analysis	2	1	1	1	
Special Characteristics	2	1	1	1	1
Statistical Tolerancing		1			
Taguchi – Robust Design		1	1	1	
Test Plan And Report	1	1	1	1	
Warranty Databases	2				1
Weibull Analysis		1	1	1	1
Worst Case Analysis	1	1		1	

8.2 QUALITATIVE RELIABILITY ANALYSIS IN THE CONCEPT DESIGN PHASE

Solutions for FMEA automation are presented in several articles. Flame [50, 51, 62] is a knowledge based system which is able to automate the failure mode and effects analysis for electrical systems, spans the entire design cycle for electrical/electronic circuits. A software supported knowledge based solution for building up an analysis will be presented in this chapter, which also contains proposals for better measures.

The literary work of FMEA is quite extensive and in terms of interpretation and explanation the understood is extremely flexible. It can be stated facetiously that ‘So many houses, so many customs’. It refers also to the used terminology of types, the forms, the ranking. There are FMEAs mentioned at a specified functional level (Functional FMEA) and at the compo-

ment level (Detailed FMEA) [54]. These kinds of differences can give rise to misunderstanding, because it can be comprehended like similarities and compared to the fundamentally accepted types: system, design, process. In these cases negotiations should be accepted; obviously it makes the comprehension impede.

FMEA is a Six Sigma tool (Juran, Deming and others developed statistical tools and methods after World War II. These ideas became part of today's body of knowledge for manufacturing quality. One of the offshoots of their effort is a business quality doctrine called Six Sigma.) for identifying, analyzing and prioritizing failures and recommended actions [106]. FMEA provides a detailed framework for a cause and effect analysis [107]. FMEA requires the analysis and quantification of the relationships among failure modes, causes, effects and controls. It is especially prevalent in the automotive and aerospace industries [108]. FMEA is neither easy to learn nor easy to use. A tool is difficult to learn when its conceptual model is inadequate, wrong or non-existent [109]. The meanings and relationships for the FMEA concepts of cause, failure mode and effect are ambiguous and weakly defined [110]. Entries in a FMEA worksheet are voluminous and consequently very brief [51]. These copious brief entries make the FMEA hard to produce, hard to understand and hard to maintain. FMEA does not group items with like effects together [112]. FMEA, as implemented in Excel, is unwieldy, with much scrolling required. Scrolling detracts from a user's mental representation of a document as a whole [113]. The use of expected costs was suggested in prioritizing failures. An expected cost is the cost of an event multiplied by its probability. Expected costs can be summed to show the impact of all failure modes for a root cause. For hundreds of years, it has been generally agreed that the way to express severity has been in financial terms [115].

There are many benefits of performing FMEA, including a systematic approach to classify hardware failures, reduces development time and cost, reduces engineering changes, easy to understand, serves as a tool for more efficient test planning, highlights safety concerns to be focused on, improves customer satisfaction. It is an effective tool to analyze small, large, and complex systems, useful in the development of cost-effective preventive maintenance systems, provides safeguard against repeating the same mistakes in the future, useful to compare designs, a visibility tool for manager, a useful approach that starts from the detailed level and works upward improving communication among design interface personnel [4, 99].

FMEA is an analytical method of the preventive quality assurance. It serves to find the potential failure of a product/process, to recognize and evaluate its importance and to identify appropriate actions to prevent the potential failure or to discover it in time. The systematic analysis and removal of weak points leads to the minimization of risks, to the reduction of failure costs and to an improved reliability. In the mid 1960s, this method was developed within the Apollo project in the USA. It has first been used by the aerospace industry and the nuclear technology and later by the automobile industry and also in other sections.

A FMEA is a good means to analyze risks caused by individual failures. The individual risks are weight against each other to recognize priorities. FMEA does not provide a statement on the total failure risk. For the analysis of failure combinations, the fault-tree analysis is more appropriate.

The advantages of a FMEA prove that the efforts to prevent failures from the beginning of the development process of a product are justified because the very much higher resulting costs are eliminated later. Advantages are, e.g.:

- prevention of failures in design and development,
- prevention of repeated failures through systematic consideration of expert/failure knowledge on the product or process,
- less subsequent product changes and thus reduction of costs.

An argument which is often used against FMEA is its high expenditure. The following topics play an important role (especially the two last topics offer big saving potentials):

- complexity of the product,
- level of analysis/type of FMEA,
- methodological experience of moderator/team,
- quality of preparations,
- terms of reference/scope of analysis.

The scope of analyses can be reduced in co-ordination with the client and the team. Approaches for savings are:

- priority system and selection of analyses,
- decision analysis that shows the critical component groups,
- use of existing products/processes with similar FMEA,
- use of a ‘Basis-FMEA‘ [120] with parts/products processes which are repeatedly analysed.

The implementation of a FMEA is necessary when products are newly developed, when there are changes on the product or procedures, products with safety regulations or customer requirements. Besides all that, the FMEA implementation shows the following positive aspects, for example:

- all project participants are ready for team work at an early stage,
- better understanding of the system for all participants,
- early detection of problem areas,
- consequent taking of actions up to implementation.

The biggest benefit is gained when the FMEA is made at an early stage simultaneous to the development and planning of the production. It is important that the results can be used in the product development process and so unnecessary recurrences are avoided.

To improve efficiency, the FMEA is performed by a team of experts (Table 8.2) from all responsible and affected areas.

Table 8.2. FMEA team members (example)

	System FMEA	Design FMEA	Process FMEA
Core team	System development (responsible) Application Moderator	Design (responsible) Testing Plant (production engineering department or quality assurance) Moderator	Production engineering Department (responsible) Quality assurance Manufacturing operations Department Moderator
Supplemental members	Component development Sales Department Purchase department	Application/System development Endurance testings Departments Sales department Plant Purchase department	Development (design and/or testings) Departments Purchase department

The main objective of FMEA is to assist and support the design process (it does not only refers to the Design FMEA) by identifying the effects of component or module failures on system operation [52], moreover eliminating causes of the potential failures, thus serving a positive influence on the failure chain. It can be stated that the focus is on preventing the occurrence of failure causes and the intervention must happen as early as possible.

Figure 8.2 shows a typical product development cycle beginning with conceptual design and progressing to deployment in the field. During the conceptual design and preliminary design phases the FMECA serves primarily to verify the adequacy of the system requirements; during the detailed design phase it is used to verify design compliance with the requirements [63].

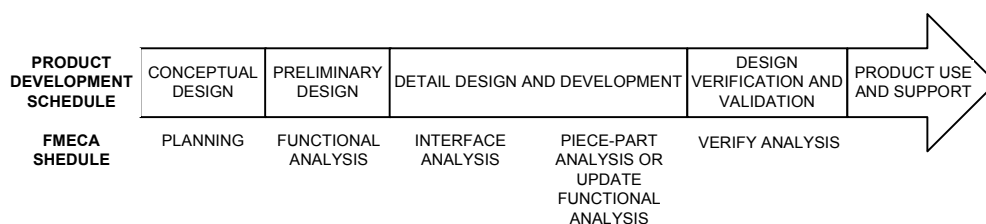


Figure 8.2. Typical product development cycle and FMECA schedule

FMEA types and forms. There are different types of FMEA depending on the time [120], the depth and the object of the analysis (Figure 8.3):

- FMEA: Failure Mode and Effects Analysis – qualitative analysis of failure modes and effect.
- FMECA: Failure Modes Effects and Criticality Analysis – quantitative analysis of failure mode criticality, an extension of FMEA. It includes a criticality analysis, which is used to chart the probability of failure modes against the severity of their consequences.

- SFMEA: System FMEA (sometimes this is called a Conception FMEA or CFMEA) is used to analyze systems and subsystems in the early concept and design stage. It focuses on potential failure modes between the functions of the system caused by system deficiencies. It includes the interactions between systems and elements of the system. It includes the interaction of element within the system and failure modes that may occur at the vehicle level as experienced by the customer. It considers failure modes at the functional level of components or due to errors in the architectural arrangement of the system.
- DFMEA: Design Failure Mode and Effects Analysis is used to analyze products before they are released to manufacturing. It focuses on failure modes caused by design deficiencies. The primary purpose is to rate the risk of design errors so that a development and test plan can be devised which reduces risk until acceptable risk level according to the market, and to identify areas for redesign to reduce risk (improve reliability and robustness of product). It is to cover analysis of the assembly as well as each component.
- PFMEA: Process FMEA is used to analyze manufacturing and assembly processes. It focuses on failure modes caused by process or assembly deficiencies. For purchased safety parts the PFMEA should contain also references to the supplier processes.

Further FMEA types are also known like:

- FMEDA: Failure Mode Effects and Diagnostic Analysis – for the electrical/electronic equipment have been used to provide failure rates, failure mode distributions and diagnostic self-test capability measures for products based on extensive component failure rate and failure mode databases.
- Service FMEA (also SFMEA) [59] is used to analyze the product serviceability, i.e. it is focused on the potential problems associated with both maintenance issues and field failures of the manufactured products.
- Interface FMEA: The interfaces between different systems, subsystems or components are analyzed in this type of FMEA. The interface FMEA can be part of a system or design FMEA and is methodically a system or design FMEA.
- Logistics FMEA: The methodology of the logistics FMEA is comparable to that of the process FMEA. The logistics FMEA analyzes the logistical flow of products from receiving until delivery to the customer. Customer complaints are analyzed and evaluated with logistics FMEA.
- In-Service (System) FMEA is to highlight high risk failures so that the brake systems and components may be developed to minimize the effect of the potential failure. Assume all parts are to print and function as designed /intended. Only single failures are considered. In general, the vehicle is being driven when the failure occurs, unless specifically noted otherwise. The In-Service System FMEA is conducted from the perspective of the customer, where the customer is the vehicle user, driver, owner or maintenance person. This type of FMEA exists in the USA.

One classification according to [78] the FMEA variations are differentiated to Functions and Component FMEAs then the further two kinds (Construction and Process FMEA) belongs to Component FMEA.

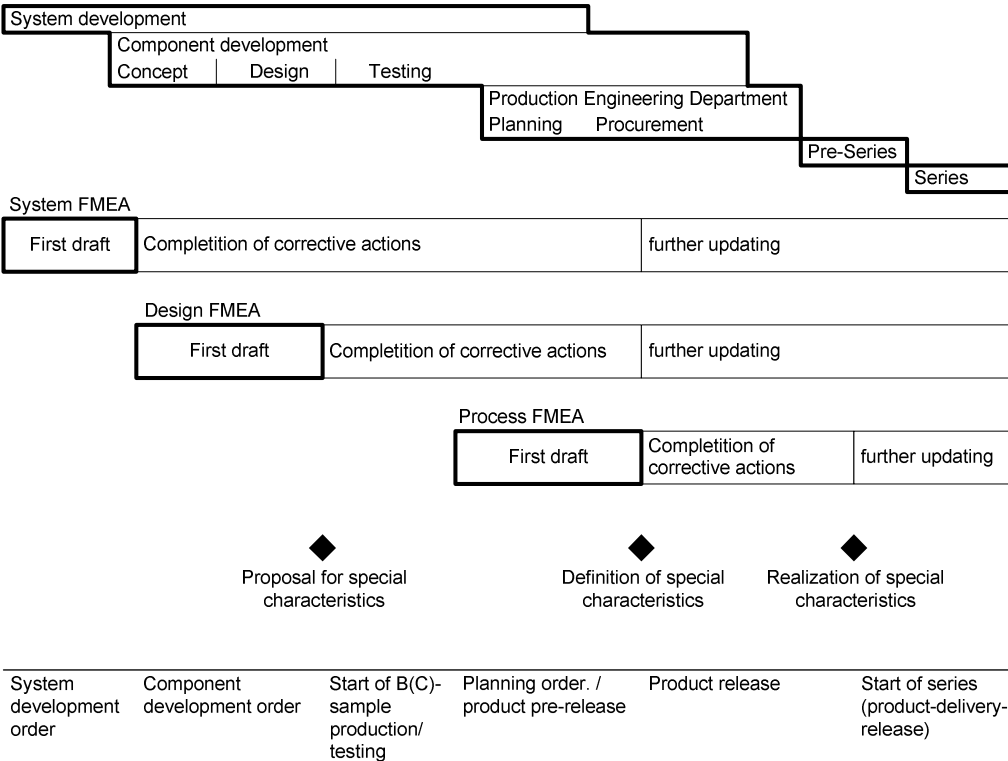


Figure 8.3. Chronological integration of the FMEA (example)

MIL-STD-1629 tells us in its foreword: ‘The usefulness of an FMECA as a design tool, and in the design process is dependent upon the effectiveness with which the problem information is communicated for early design attention’ [55]. Two of the best-known FMECA practices are outlined in MIL-STD-1629 and the SAE FMEA documents. The third, IEC document on FMECA is very similar to the MIL-STD-1629 [61].

Columns are given like: Function, Failure mode and causes, Mission phase/operational mode, Failure effects: local effects, next higher level, end effects. IEC Standard 812 form uses Equipment name, Function, Failure mode, Failure causes, Failure effects: local effects, end effects, Failure detection, Failure probability, Criticality level, Remarks (Counter-measures) [65].

FMEA improvements. Improving FMEA is not a newly presented claim. Through decades several conceptions, well-tried solutions were published. Many of them are based on automation ideas in connection with (failure) matrix, building up data- or knowledgebase [50, 51, 52, 57, 58, 60]. The Advanced Matrix Technique has been design to minimize several problems which are inherent in traditional, tabular, MIL-STD-1629A FMEA. Specific objectives in the development of the technique were:

- accelerate the timing of the analysis, wherever possible, to integrate the FMEA process with the hardware design,
- reduce the analysis cost to the extent possible,
- provide a data structure which was inherently usable by all specialty engineering groups,
- design the technique to allow automation to be accomplished.

Primarily matrix can sound like a tabular implementation of the analysis and in many cases it is true, but it is possible to handle the threefold failure chain like three hierarchical levels of a system.

8.2.1 Ranking considerations

It is often confusing to relate the FMEA's severity, detection and occurrence ratings to failure modes, causes and effects [56]. Problems with the definitions of probabilities and severities in spreadsheet FMEA make FMEA difficult to use [111].

The FMEA Risk Priority Number method is intrinsically subjective because guidelines for rating severity, occurrence and detection vary from one institution to another. The same risk priority number can be obtained using a number of different combinations of severity, occurrence and detection factors. The risk priority number does not distinguish among the linguistic variations possible for a risk priority number [114]. The FMEA scales for severity and detection are only qualitative. For instance, a rank 8 severity is not twice as severe as a rank 4. When the severity, detection and occurrence are multiplied together to form the risk priority number, the ratings are treated as if they represent numeric quantities. The calculation erroneously implies that a two-fold increase in one factor (e.g. severity) can be offset by a corresponding decrease of half in another factor [63].

The idea of expressing an RPN as a likelihood value lends itself to perhaps redefining an RPN as a probability value. However, a modification needs to be introduced to ensure that any RPN lies in the range of values between 0 and 1. No confusion is anticipated here, as the analyst can still use values in the range 1 to 10 for the rankings and the software will simply divide the calculated product by 1000. Summing the three rankings together has its advantages in that the calculated sum in terms of a percentage give a better understanding of the importance of the RPN. This can be demonstrated by the following special example where the severity rating is very high compared with the occurrence and detection ratings [56]. Suppose that:

- Occurrence rating = 1 (1 out of 10)
- Severity rating = 9 (9 out of 10)
- Detection rating = 1 (1 out of 10)

Multiplying the rating together gives: $O \times S \times D = 1 \times 9 \times 1 = 9$ (9 out of 1000), 0.9%, summing the ratings together gives: $O + S + D = 1 + 9 + 1 = 11$ (11 out of 30), 37%.

According to the first calculation the accepted intervention limit is at 10% (RPN = 100), but this value can also be different per ranking catalogues.

A particular failure mode can be considered with two associated causes. The failure mode occurs if cause 1 OR cause 2 occurs, expressed (8.1) in probabilistic terms:

$$RPN_{OR} = RPN_1 + RPN_2 - RPN_1 \cdot RPN_2 \quad (8.1)$$

In expanded FMEA (EFMEA) a special evaluation of RPNs were conducted using a feasibility rank, which divided the differences (8.2) between the RPN values before and after [59]:

$$\frac{(RPN_{iBefore} - RPN_{iAfter})}{F_i} = \frac{\Delta RPN}{F_i} \quad (8.2)$$

This feasibility rank [59] is established by criteria in connection with the implementation classification of corrective actions ranging from 1 to 10, where 1 means a corrective action with fully available resources, very low cost and time consumption, near 100% chance of success and near zero probability of undesirable impact and 10 means safety problem and/or non-compliance to government regulation and/or unavailable necessary resources and/or unacceptable cost and/or time consumption and/or zero chance of success and /or 100% probability of undesirable impact. As a result the priority of corrective actions is given.

MIL-STD-1629 provides for calculation of criticality of individual failure modes by applying multipliers to failure rate of individual parts such as Failure Mode Ratio, α , probability that the failure mode will affect the assembly, β , duration of operational state of the part, t, in a mission. SAE FMECA provides a means for prioritization of failure modes calculation of a RPN, but in large number of cases, these numbers were obtained by subjective estimation. This practice can result into improper prioritization [61].

8.2.2 Applicability for software failures

Software reliability is the probability that a software program functions without an external error for a time period on the system it is to be used under the actual working conditions [76].

- | | |
|--|---|
| <ul style="list-style-type: none"> – Software reliability <ul style="list-style-type: none"> ▪ No bathtub hazard rate curve ▪ SW will not wear out ▪ SW field is relatively new ▪ Useful data collection is a problem ▪ Basically the SW reliability is design oriented | <ul style="list-style-type: none"> – Hardware reliability <ul style="list-style-type: none"> ▪ Has the bathtub hazard rate curve ▪ HW will wear out ▪ HW is well-established (especially in the area of electronic components) ▪ Same as for software |
|--|---|

- Has the potential for monetary savings
- Redundancy in the SW may not be effective
- Classical reliability analysis tools can be applied difficulty
- HW reliability is affected by design, production and operation
- Same as for software
- Generally, item redundancy is effective
- Classical reliability analysis tools can be applied

There is a continuing need throughout development to assess the reliability of our products, including software. It should be emphasized that software has become the dominant failure contributor in complex systems. The MTBF of the software improves as the faults are found and removed. This is where software reliability traditionally measured [72].

FMEA has not been widely used on software and is best used for systems with minimal hardware protection and few authors reported successes in using FMEA in software development [60].

- The most failures will be done during the requirement management phase and the system design phase
- Requirement management failures are not detected with test cases (Test is checking if the implementation forward to the requirements)
- Specification shall be clear, precise and unambiguous

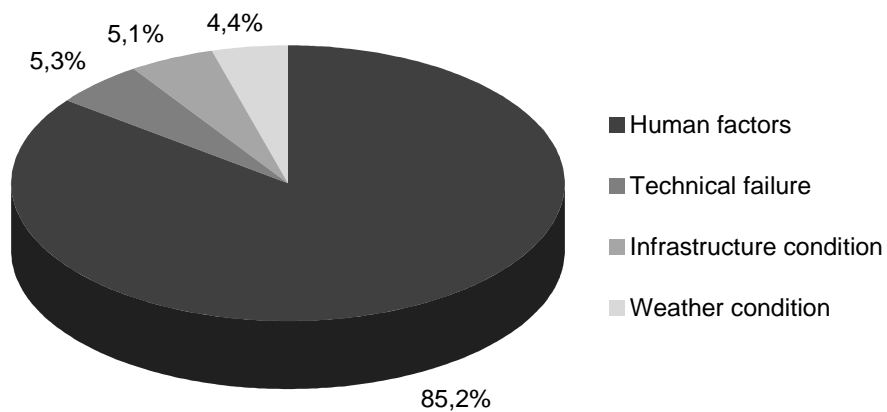


Figure 8.4. Frequency of failure arts for software

Most of the failures (Figure 8.4) are done during the requirement management and the system design phase. Requirement management failures are not detected with test cases. Test is checking if the implementation forward to the requirements, thus specification shall be clear, precise and unambiguous.

Traditional FMEA techniques have been adapted and extended [53] to include assessment of software failures. Hughes has been using the resulting technique to assess the safety of embedded real-time control systems designed for use in automotive applications. The use of FMEA techniques in assessing the software safety of these controllers has allowed analysis of the effects of a more comprehensive set of potential failures, including data corruption, than is practical using other software safety analysis techniques.

Analytical verification methods for assessing the hardware failures are well-known within the reliability discipline. FMEA and FTA are proven methods and have been used to assess many safety-critical hardware systems. Analytical verification methods for software exist, but are not as well-known within the reliability discipline, e.g. software fault tree analysis, Petri nets.

Embedded control systems for safety-critical applications require designs which protect against hardware failures, software failures and failures which cross the hardware/software boundary; the system must never be allowed to enter an unsafe state. FMEA applied to software allows assessment of the impact of single point software failures and of those failures in hardware whose effects are determined by the software. For systems where undetected data hardware integrity failures are possible, software FMEAs being inductive have significant advantages over software fault tree analysis.

8.2.3 Systematic set up of system structure and function

Before starting the FMEA it is worth deploying the related requirements to design specification level. For that purpose, several tools are available; one of them is the Matrix Analysis (MX FMEA) from Plato AG, which seems to be very powerful in safety-critical applications. The advantages of using matrix analysis over representing the system in a structure tree lie in the fact that the function, failure and system structures are set up almost simultaneously and that functional relationships are indicated within the matrix.

The system-level structure of each matrix is based on the answers to three questions:

- What is the system or product to be analyzed?
- What customer needs/expectations, regulatory requirements, standards, etc. are associated with such a system or product (functions and/or requirements)?
- What subsystems make up the system or product? And which functions correspond to these subsystems (directly or indirectly)?

The requirements that the relevant components must meet in order to fulfil a function are mapped at interfaces (Figure 8.5). An interface is both a means of separating system from design and a means of linking the two. Interfaces make it possible for the teams to work independently at different locations. Design and System FMEAs can run parallel to each other up to a certain stage of the development process and then the conception FMEA (how the whole complex system is influenced by each component) can be executed [4].

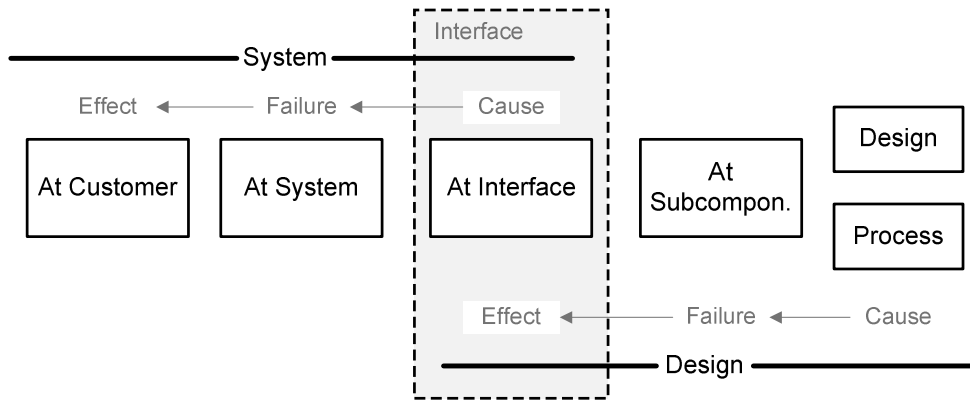


Figure 8.5. Representation of involved levels in System and Design FMEAs with defined interface

Question guideline concerning building up the matrix structure (Figure 8.6):

1. What is the overall system?
2. What do customers, laws, standards, etc. expect from such a system (functions/requirements)?
3. Of which sub systems the system should consist of? Which functions do they support?
4. Which functions should each sub system have? Which (external) functions/requirements do they support?
5. Of which interfaces each sub system should consist of? Which functions do they support?

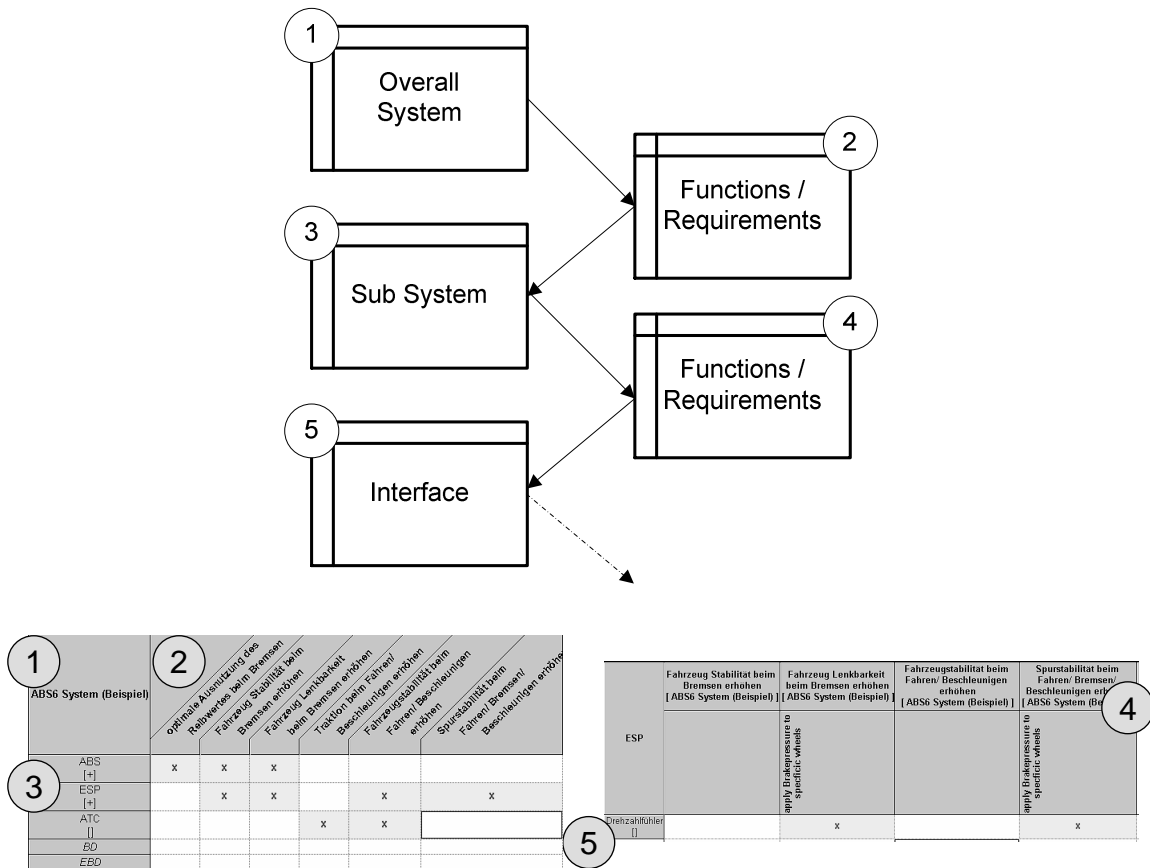


Figure 8.6. Matrix structure

8.3 ANALYSIS OF REDUNDANT ELECTRONIC SEMI-TRAILER BRAKE SYSTEM

The goal of SPARC (Secure Propulsion using Advanced Redundant Control, EU 6th framework) is to substantially improve traffic safety and efficiency for heavy goods vehicles using intelligent x-by-wire technologies in the power train. To provide this standardized concept, an automotive Software/Hardware platform is currently being developed. It is scalable and usable from heavy-goods vehicles down to small passenger cars and can be integrated therein. SPARC is the continuation of the EU 5th framework project PEIT extended to the vehicle combination (tractor – semi-trailer).

The towing vehicle's brake system has to be built up by the power train controller, axle modulators (responsible for braking and levelling) and additional modules of parking brake. The trailer's brake system has to be built up by using axle modules (AM) responsible for braking and levelling, controlled by a Central Trailer Controller (CTC) being able to be controlled by a towing vehicle with conventional (pneumatic) or fully electronically controlled brake system in terms of interchangeability.

The goal is to demonstrate a qualitative reliability analysis using (Matrix) FMEA approach applying to a partly redundant semi-trailer electronic brake system paying attention to all the experience was known during the analysis.

The scope is focuses on the steps of a correct procedure of handling redundant systems with classical reliability approach starting from the system definition through function deployment finishing with assessment.

In this case a partly redundant system is available and the FMEA method, which is appropriate mostly for non-redundant systems. This contradiction must be resolved by proper considerations, which are going to be presented in this document. It should be noted that this systematic approach is only one possible solution.

8.3.1 Reliability considerations

On the one hand central control of chassis systems gives the possibility to improve the vehicle safety and reliability. On the other hand the new control strategy (only electric connection between truck and trailer) requires some new considerations:

- In case of losing both communication channels, the CTC brings the trailer to a safe status. After loosing the communication, the CTC waits for a certain time if the communication will be restored. If not, CTC will brake the trailer smoothly (with a ramp) until stop and activates the parking brakes. During the braking, both ABS and Roll-over Stability Program (RSP) are available to assure the safe stop. If the communication is restored during the braking, the CTC will follow the command from the truck.
- In case of failure in any axle modules, CTC can distribute the braking request among the available modules to achieve the demanded retardation. It means that retardation, which is

expected by the truck, will be always executed. If the brake force of the remaining axle is not enough longer, CTC can activate the parking brake, and provide the remaining retardation portion with parking brake.

- If CTC detects unordinary action at any axle module, CTC can replace the brake force with the parking brake at this given axle. If the axle module is not broken anyway, it will detect the activation of parking brake and in case of unintended locking of the wheels it can provide ABS functionality on one wheel of the axle.
- If CTC Master is broken, Slave can provide the brake force with the parking brake modules. If the axle modules are not broken, they can provide ABS function on one wheel per axle.
- If CTC Slave is broken, the possibility of continuous parking brake pressure control is lost. But CTC Master can keep the parking brake open with the back-up valve and engage it any time.

Interconnectivity. Because of high amount of the different tractors and trailers on the traffic, very important task is to assure interconnectivity between vehicles from different age. The SPARC semi-trailer structure is built up on the way, which fulfils this requirement. The design makes it possible, beside the control by wire architecture the control by air-pressure system was implemented on the semi-trailer, as well.

The table below (Table 8.3) shows the used connections in case of different kind of tractors. GF (Georg Fischer) coupling (combined connection of pneumatically and electronically controlled brake systems for semi-trailers) is an automatic coupling method, which provides transfer not only the lines defined in ISO7638 (Road vehicles – Brake anti-lock device connector (ISO 7638-1985)) and ISO12098 (EBS functions (ISO 12098:1994)) but the high load power line as well. The control information is superposed to every supply line as well so the redundancy is assured.

Table 8.3. Possible connections between tractor and semi-trailer

Tractor	Connection on SPARC semi-trailer				
	Electrical			Pneumatic	
	ISO12098	ISO7638	GF coupling	RED	YELLOW
Old	X			X	X
EBS	X	X		X	X
SPARC			X		

8.3.2 Safety in design

Advanced automotive truck-trailer architecture require higher reliability than achieved by single channel of CAN whose nodes are interconnected via twisted pair cables. The power line was used in the SPARC project to add redundant CAN channel over the power line providing a relatively fail-safe communication channel between the truck and its trailer: communicating

over the power line as a redundant channel for CAN messages, maintains the required communication performance and transmission delays while increasing the network reliability. The reliability level achieved by using this redundant architecture is indeed sufficient for safety applications

Adding redundant channel to increase the reliability of truck-trailer communication is an obvious solution, since the connecting cable is already defined in ISO 12098 or ISO 1185 standard. The only possibility is to use the defined pins dedicated for power or the different lights activation also to transfer data over its power line.

Power Line Communication (PLC) can be employed for redundant CAN communication over DC power lines. Transmitting CAN messages over the power line avoids complex cabling, thus reducing weight and greatly simplifying installation, while maintaining the CAN user format.

The CAN protocol over twisted pair physical medium is widely used in automotive applications. Fault-tolerant CAN transceivers allow network operation even if one of the twisted pair lines is not functioning. However, for safety applications, communication must be robust enough to withstand potential mechanical and electrical failures not usually tended by the CAN transceiver. These include: one-wire interruption, one-wire short-circuit either to power or ground, two-wire short-circuit, termination failure and various noises.

Communicating over the power line as a redundant channel for CAN messages, maintains the required communication performance and transmission delays while increasing the network reliability. The reliability level achieved by using this redundant architecture is indeed sufficient for safety applications.

The fault-tolerant requirements for drive-by-wire systems (Table 8.4):

- the system should tolerate a transient fault
- the system should tolerate one permanent fault
- the system should tolerate a transient fault after a permanent fault has occurred.

Table 8.4. Requirements for drive-by-wire systems

Term	Definition
Fail-silent	The system/subsystem/device switches off automatically when a fault is detected internally and no longer actively participates in communication.
Fail-safe	The system/subsystem/device switches the outputs (state) into a safe specified state when a fault is detected.
(Fail-operational) Fault-tolerant	The system/subsystem/device continues to operate with a full or limited functionality even after a fault. The system is designed to be tolerant of faults. The time and value thresholds are selected so that the system remains active even when faults of this kind occur (short-term or with a modified functionality if necessary, but even with modified functionality, the system (vehicle) continues to be reliably controllable by the driver.).

Modularity in design. Considering the design a modular structure was implemented since the three axle modules are mounted with no difference of their construction but in classification since only the AM1 has connection to SCV and SLS. As advantage, this construction makes the so called road train function possible for semi-trailers with no matter how many axles.

The implementation of road train function for the TEBSs realizing the point-to-point connection can be a weak point in communication between the AMs hence the function ‘setting with initialization’, related only to TEBS1, arises functional questions: In case of a failure occurred at the input side of TEBS1 the other connected TEBS2 and TEBS3 do not get data through ISO11992? Before answering this question two objects should be taken in account:

- The unique feature of ISO 11992 communication line being redundant in itself handling seven kinds of single failures (see 8.3.4) except the eighth, double failure, when CANL and CANH are broken, which is contradictory with
- FMEA handling only one failure at a time.

The TEPBs’ communication is a star point design, which ensures no loss of whole communication and provides the additional functions in case of one failure in one of the TEPBs.

The system structure defines the appropriate function structure, which can be linked together considering the related legal requirements (UN-ECE 13). This structure follows level-by-level and is developed parallel to the previously built-up system structure.

The vehicle combination’s brake system has to feature all functions of a today one-circuit (non-redundant) EBS (electronic brake system) with the addition that the control is electronically redundant and there is no pneumatic back-up. The trailers will have no external pneumatic supply and control. Supply has to be solved by electric compressors, while brake control will be solved by two independent communication links between towing and towed vehicle.

Service and parking brake operation. Concerning the above introduced modularity a safety function will be presented satisfying the prescribed deceleration value in case of failure combination. At this architecture three modes can be differentiated:

- Disadvantage of this road train design, which means if there is a failure combination at the root of the information flow, communication between CTCM and AM1 (TEBS1), then only the safety ramp function is available provided by the EPBs since the road train implementation prevents the dataflow between the AMs, till the whole combination stops, the redundant functionality of ISO11992 is not ensured.
- Facing the next case when a communication interruption is realized between AM1 and AM2, then there is neither communication between AM2 and AM3. In this status the appropriate EPBs (EPB2 and EPB3) on the axles, which lost the communication, are providing together with the intact TEBS (TEBS1) the prescribed deceleration value as the calculation shows below.
- In the third situation when the communication failure occurs between AM2 and AM3 the intact TEBS1 and TEBS providing the deceleration function with EPB3.

The following table (Table 8.5) shows the necessity of minimal number and combination (9.3, 9.4) of intact communication elements to participate in realizing any braking function on the trailer.

Table 8.5. Service and parking brake operability

Brake type	Service	Parking	Parking	Service
ISO 11992	0	1	0	1
PLC	1	0	0	0
5V	-	1	1	0
OPTO Interface	-	0	-	1

The following equations (8.3, 8.4) express the reliability of the service and parking brake functions:

$$R_{Service} = R_{ISO11992} \cdot R_{OPTO} + R_{PLC} \quad (8.3)$$

$$R_{Parking} = R_{ISO11992} \cdot R_{5V} + R_{PLC} \cdot R_{OPTO} \cdot R_{5V} + R_{5V} \quad (8.4)$$

8.3.3 System and function structure

Taking the lay-out (Figure 8.7) into consideration seven main groups were created at the main, analyzed level.

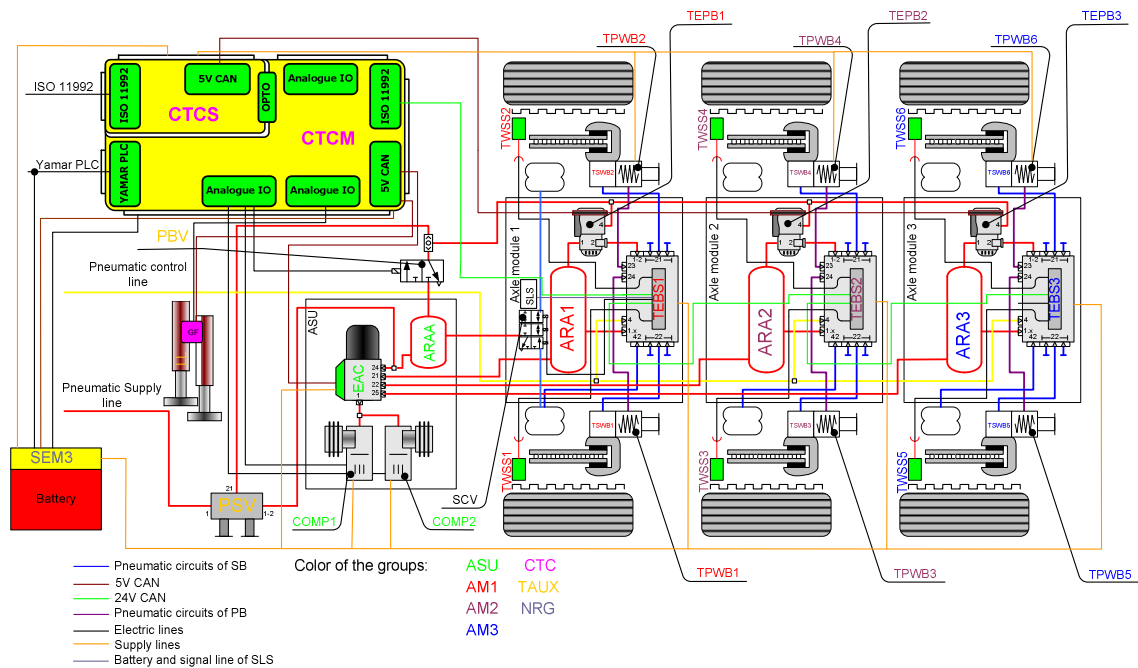


Figure 8.7. SPARC semi-trailer lay-out

According to the system lay-out the system structure is the following (Figure 8.8):

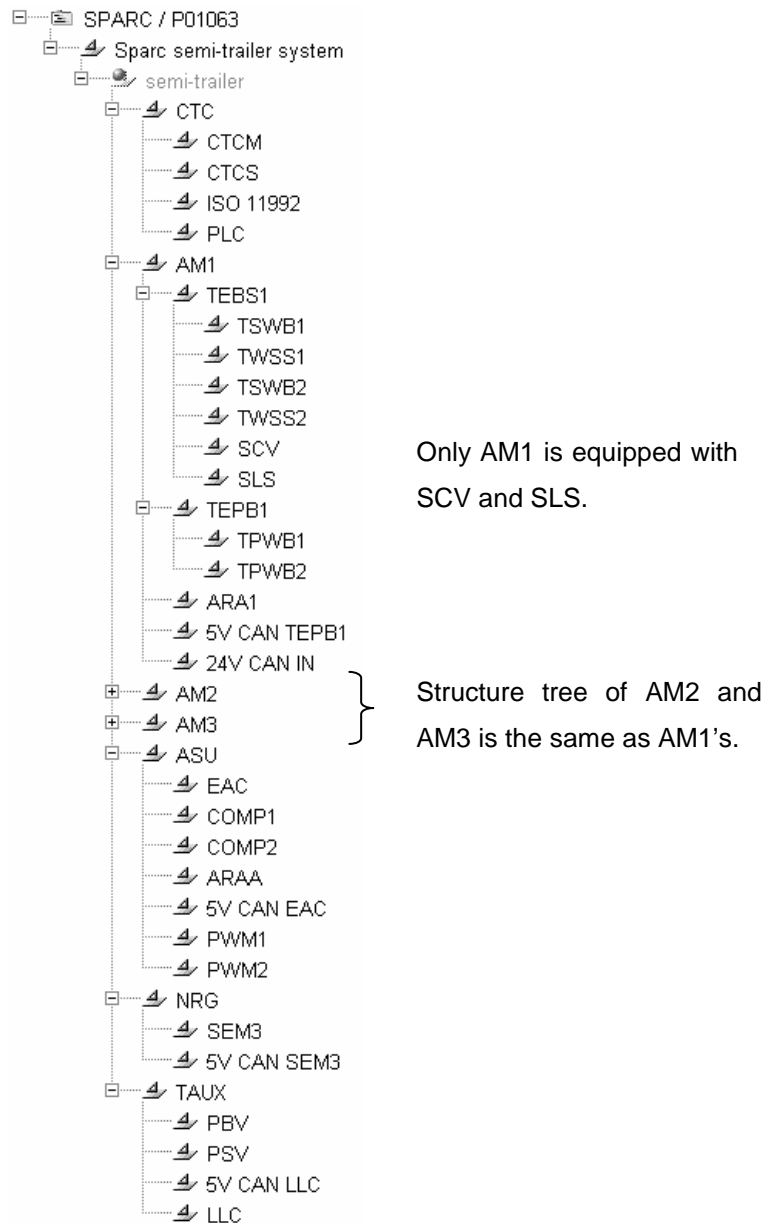


Figure 8.8. SPARC Structure tree

Function structure link to system structure. Concerning an accurate description of communication links it was considered solving redundant input problems with defining only the input side of the information flow. This approach made it easier not to miss any links, but also supported creating the systematic description. In order to comply with the system structure a new dilemma was outlined concerning the function deployment. It is obvious that a system contains subsystems and the subsystems contain components, which is shown by the structure tree. What is not so obvious: How can be made difference between subsystem and component functions? As it was mentioned above the theory of handling the communication links was the input side definition. In order to make difference between function and sub function the basis was the same. Table 8.6 shows the classification of each sub function linked to upper-level functions considering their assigned tasks and controlled unit.

Table 8.6. AM1 TEBS1 function links

TEBS1	Controls the service brake	Wheel speeds of axle 1	Communicates to the previous equipment	Controls the suspension with external valve
Signal processing of wheel speed sensors		✓	✓	
Signal processing of SLS				✓
Setting with initialization				✓
Controls the pressure on the service brake chambers	✓		✓	
Controls the SCV				✓

At the system level (Table 8.7), only customer needs or regulatory requirements and the functions by which they are met are mapped to subsystems. No components are mapped or analyzed at the system level.

Table 8.7. Top level function and sub function links

SPARC semi-trailer	Legal requirements	Customer/Consortium requirements	Internal requirements
Utilization of adhesion (ABS efficiency)	✓		
Provide requested retardation	✓		
Hold laden vehicle stationary at prescribed up or down-gradient	✓		
Direct controlled wheels not allowed to lock	✓		
Deceleration on μ -split (laden vehicle)	✓		
Air consumption regulations	✓		
Lessen probability of trailer rolling-over		✓	
Provide trailer speed value	✓		
Supply pressure status info	✓		
ABS status info	✓		
RSP status info	✓		
Yellow warning signal required	✓		
Red warning signal required	✓		
Automatic landing leg control		✓	
Keep target level of chassis height		✓	

SPARC semi-trailer	Legal requirements	Customer/Consortium requirements	Internal requirements
Assure manual handling (LL)		✓	
Compressor control			✓
μ-jump recognition	✓		
Signal of continuous failure in electrical control transmission	✓		
Difference in transverse braking pressures on any axles	✓		
Individual compensating value on any axle	✓		
Assure manual handling (ELC)		✓	
Communication (CAN) tractor – s.-trailer assured	✓		
Communication (PLC) tractor – s.-trailer assured		✓	
Load proportional brake force distribution	✓		

Primary functions that are developed using software are mapped to subsystems of the semi-trailer electronic brake system and then linked to their influence on the requirements for the overall system with an ‘X’ in the matrix (Table 8.8). These links indicate direct relationships (via ‘function’) and indirect relationships (via ‘failure’ only).

Table 8.8. Links of sub functions and sub systems

semi-trailer	Utilization of adhesion (ABS efficiency)	Provide requested retardation	Hold laden vehicle stationary at prescribed up or down-gradient	Direct controlled wheels not allowed to lock	Deceleration on mu-split (laden vehicle)	Air consumption regulations	Lessen probability of trailer rolling-over	Provide trailer speed value	Supply pressure status info	ABS status info	RSP status info	Yellow warning signal required	Red warning signal required	Automatic landing leg control	Keep target level of chassis height	Assure manual handling (LL)	Compressor control	μ-jump recognition	Signal of continuous failure in electrical control transmission	Difference in transverse braking pressures on any axles	Individual compensating value on any axle	Assure manual handling (ELC)	Communication (CAN) tractor-s.trailer assured	Communication (PLC) tractor-s.trailer assured	Load proportional brakeforce distribution
CTC	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AM1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AM2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AM3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ASU	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
NRG	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
TAUX	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Since the matrix structure is finished with the added failures the FMEA form is automatically generated for the specific level, including the levels above (failure effect) and below (failure cause), to be analyzed.

8.3.4 Evaluation phase

During the optimization procedure of the FMEA evaluative considerations were implemented to handle the given redundant electronic brake system.

Guidelines of the evaluation. The basis for the Severity, Occurrence and Detection Probability evaluation is the SAE J1739 from June 2000, which is similar to the former QS9000 evaluation criteria.

In handling redundancy the following rules were applied during the evaluation and optimization phase regarding specific causes like no communication between tractor and semi-trailer. In this case there is a triple redundancy if ISO 11992 is handled like a solution for masking seven kinds of single failures (CANL is broken, CANH is broken, short circuit between CANL and CANH, CANH short circuit to 24V, CANH short circuit to GND, CANL short circuit to 24V, CANL short circuit to GND). Hence being more experienced in using ISO 11992, an evaluation method was found out in the optimization phase because of the mutual redundancy.

The non-redundant PLC in itself was evaluated like a stand alone electric line with relatively high single values of detection and occurrence regarding the less experienced usage of that. During the optimization phase at the evaluation the following methods were applied:

– Standard evaluation

Standard evaluation has its own rules how to apply. Evaluation begins after creating the FMEA form derived from the matrix. Two different aspects will be taken into account concerning the evaluation: whether the value refers to the failure effect or to the failure cause. The final value (RPN – Risk Priority Number) contains three factors:

- Severity (S), which always refers to the failure effect (FE)
- Occurrence (O) and Detection (D) for the failure cause (FC)

Multiplying these factors we get the RPN, which will be analyzed whether the corrective action is needed or not. The range for each value is 1 to 10 (including only integers).

– Severity evaluation

The severity value is strictly not changeable not even in the optimization phase because the effect of the failure does not change during the analysis and this value refers only to the failure effect. It is classified once based on the evaluation catalogue to a specific value.

– Occurrence evaluation

In case of occurrence evaluation if a preventive action can be implemented the originally determined value can be reduced the way as follows:

$$O = O(\text{FC}) - P \text{ (evaluation of the preventive action - value of 'goodness')}$$

These operations are applied during the automatic evaluation process.

Solving the optimization problem for the redundancy of the communication lines the following mathematical operation (8.5) was applied, which is analogue to the calculation of resistors connected in parallel:

$$O_2 = \frac{O_{1_preventive_action} \cdot O_{1_redundant_preventive_action}}{O_{1_preventive_action} + O_{1_redundant_preventive_action}} \quad (8.5)$$

– Detection evaluation

In case of detection evaluation if a detective action can be implemented the originally determined value can be reduced the way as follows:

$$D = 10 - C \text{ (evaluation of control action - value of 'goodness')}$$

These operations are applied during the automatic evaluation process.

Since a better detectable (lower value) solution (8.6) provides the connection between the combination parts the basis for the detection value after optimization was its detection probability number.

$$D_2 = \min[D_{1_corrective_action}; D_{1_redundant_corrective_action}] \quad (8.6)$$

RPN = S×O×D. The RPN value was marked as critical at 100; corrective actions were carried out in all cases the value was above 100.

8.3.5 Results

The diagram below (Figure 8.9) demonstrates the distribution of the RPNs before and after the corrective actions. It can be seen that no RPN2 can be found above 100, but more at lower products. In this case the used operations during the second phase of the evaluation ensure right conclusions concerning the analysed system architecture.

In this chapter it was shown that the presented qualitative reliability analysis technique in itself is not applicable for redundant systems in order to draw the proper design consequences. It was proposed that suitable calculations make the qualitative reliability analysis method adaptable to redundant systems [FT1, FT2, FT16].

Abbreviations used during the analysis:

AM	Axle Module
ARA	Air Reservoir in the Axle
ARAA	Auxiliary Air Reservoir
ASU	Air Supply Unit

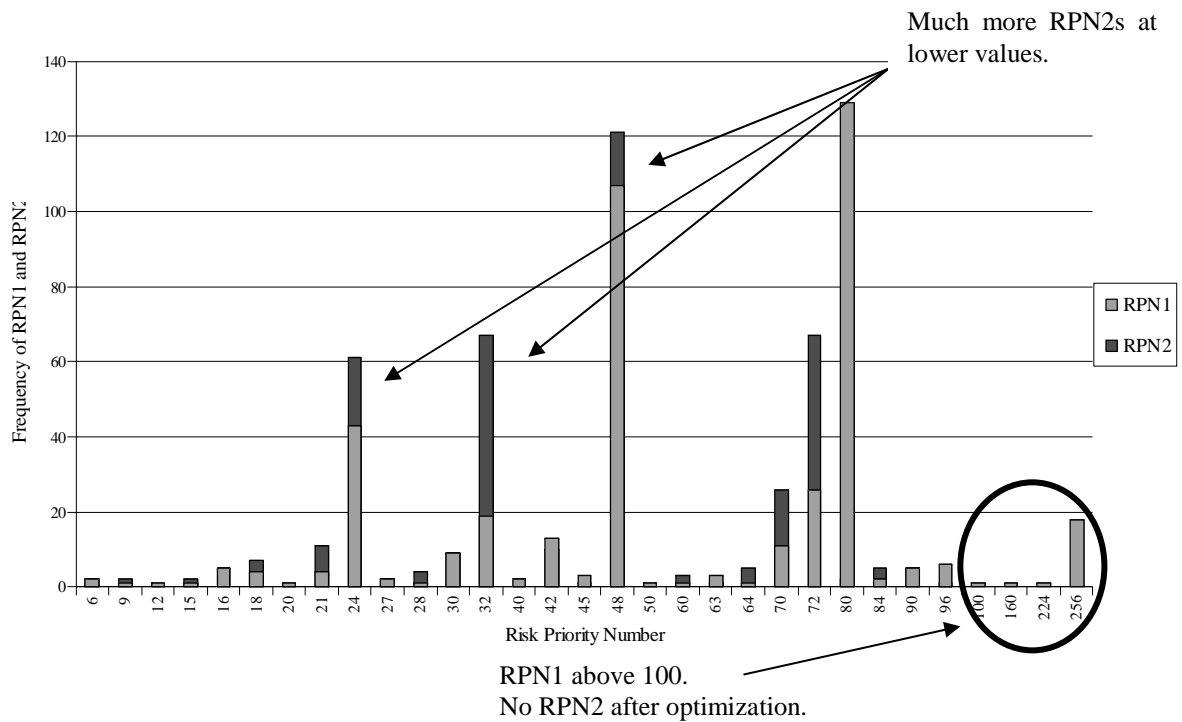


Figure 8.9. Distribution of RPN1 and RPN2

CAN	Controller Area Network
COMP	Compressor
CTC	Central Trailer Controller
CTCM	CTC Master
CTCS	CTC Slave
EAC	Electronic Air Supply Control unit
LLC	Landing Leg Control
NRG	Energy Unit
PBV	Parking Brake Valve (back-up valve)
PLC	Power Line Communication from truck to trailer
PSV	Park and Shunt Valve
PWM	Pulse-Width Modulation (compressors control)
SCV	Suspension Control Valve
SEM	Smart Energy Management
SLS	Suspension Levelling Sensor
TAUX	Trailer Auxiliary
TEBS	Trailer EBS
TEPB	Trailer Electro-Pneumatic Parking Brake module
TPWB	Trailer Parking Wheel Brake Module
TSWB	Trailer Service Wheel Brake Module
TWSS	Trailer Wheel Speed Sensor

8.4 COMPLEX APPROACH TO QUALITATIVE AND QUANTITATIVE DESIGN TECHNIQUES

One of the most widely employed general safety techniques is fault-tree analysis [123]. Fault-tree analysis was developed by H. R. Watson of Bell Telephone Laboratories in 1962. The technique was initially used for safety and reliability studies of a missile system. Engineers at Boeing further developed and redefined the procedures and became the method's foremost proponents as a method of performing safety analysis of complex electro-mechanical systems. Fault-tree analysis has become a standard technique for safety and reliability of such systems [45]. It is also widely used in nuclear industries [8].

While FMEA is applied as a bottom-up analytical technique, FTA is applied to the product as a top down in view of its functionality, failure definition, architecture and stress and operational profiles provides a methodical way of following products functional flow down to the low level assemblies, components, failure modes and respective causes and their combination. FTA was used primarily to model reliability of a system regarding its potential failure modes associated with hardware, software or their interactions [61].

Event Tree Analysis (ETA) is an inductive (forward logic) technique, which examines all possible responses, failure effects [80] to the initiating event, progressing left to right across the page. The branch points on the tree structure usually represent the success, failure or partial failure of systems and subsystems, which can respond to initiating event. ETA can be used in conjunction with FTA to identify the causes of the subsystem failures or branch events. Quantification of the fault tree provides the probability of passing along each of the event-tree branches [73].

In commercial aviation fault trees have become the accepted means to show compliance with various FAA safety regulations [69].

Comparison of the above mentioned techniques can be seen in Figure 8.10.

The FTA creates a fault model, and contains the analysis of the model. The fault tree is built from top to down, it is a deductive procedure. Fault trees provide a convenient symbolic representation of the combination of the events resulting in the occurrence of the top event. The FTA provides a statement on the total failure risk. For the analysis of failure combinations FTA is more appropriate than FMEA.

The starting-point is always a system-level problem, the top event (Figure 8.11). The goal of the modelling is to find the basic cause(s) of the predetermined problem. These causes are called basic events. The relations between the basic events must be accurately specified. This influences fundamentally the final result of calculation. On easy fault tree construction behalf we could define intermediate events. This type of events is composed of basic events. During the analysis the occurrence of the intermediate events is counted from the failure rates of the basic events.

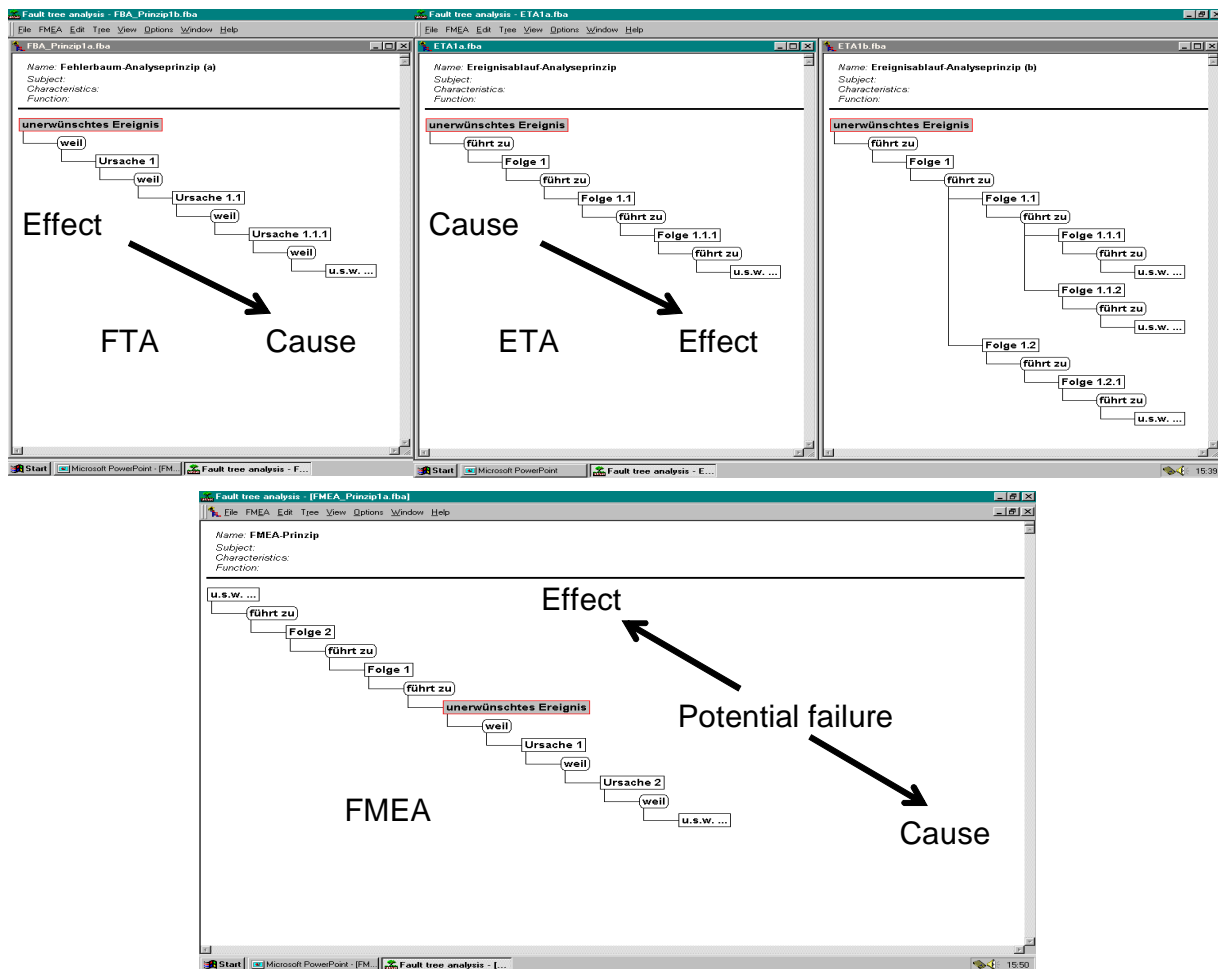


Figure 8.10. Direction and focus of analyses

The functional failures or malfunctions at the outputs of the system are caused by logical combinations of the failure rates of the events. Some possible relations are enumerated below:

AND: It indicates that the output occurs if and only if all of the input events occur. The output of an AND gate can be the top event or any intermediate event. The input events can be basic events, intermediate events (outputs of other gates), or a combination of both. There should be at least two input events to an AND gate.

OR: It indicates that the output occurs if and only if at least one of the input events occurs. The output of an OR gate can be the top event or any intermediate event. The input events can be basic events, intermediate events, or a combination of both. There should be at least two inputs to an OR gate.

K/N: The Voting gate indicates that the output occurs if and only if K out of the N input events occurs [117]. The N input events need not occur simultaneously. The output occurs when at least K input events occur. When $K=1$, the Voting gate behaves like an OR gate. The output of a Voting gate can be a top event or an intermediate event. The input events can be basic events, intermediate events, or combinations of both.

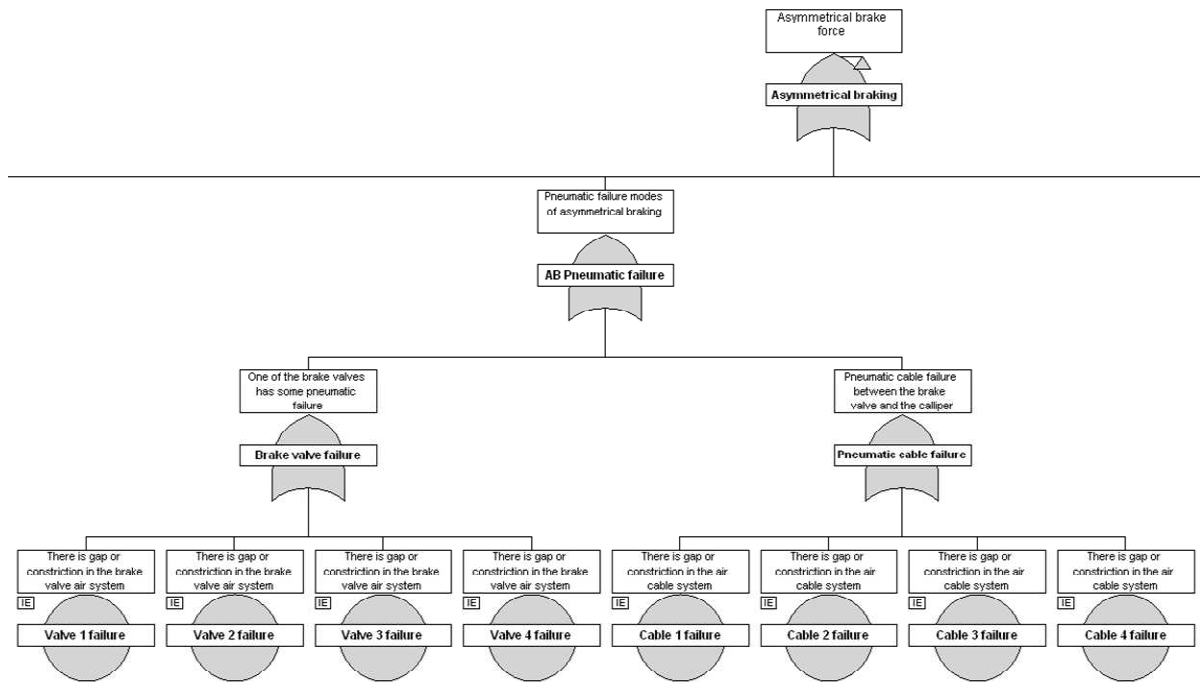


Figure 8.11. FTA extract of a redundant electronic brake system with OR gates and basic events

It should be remarked that this analysis does not necessarily depend upon credible component failure rates to produce useful results. In the case of software modules, or components with no sufficient history of use, such failure rates would be impossible or very difficult to obtain anyway. However, the logical reduction of fault trees into minimal cut-sets can still indicate single points of failure in the system and point out potential design weaknesses that may lead to useful design iterations. In the terminology of fault trees, a cut-set (Figure 8.12) is a set of basic events (i.e. leaf nodes of the tree or component failures) that if they occur cause the top event of the tree (system failure). A cut-set is called ‘minimal’ if there is no subset of events in that set that is also a cut-set, i.e. if there are no redundant events in the set.

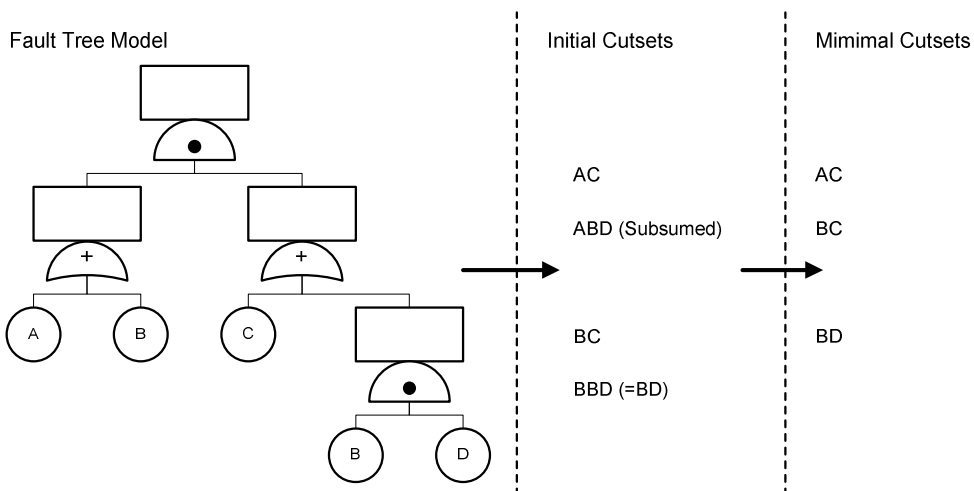

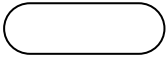
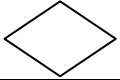
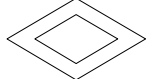
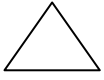


Figure 8.12. Illustration of cut sets

OR is associated with redundancy and an AND gate means that both of the lower level faults must occur for the next level fault to occur. When a system operation calls for dormant states (Table 8.9) interchanging with operational states, it may be difficult to decide how to assign appropriate failure rates or failure probabilities to the basic events. One possible solution could be to prepare two separate trees, one for dormant and the other for active system state and then append these to one top OR gate that would compile the results. Undeveloped event indicates that the failure state is treated as a basic event, even though further development is possible [69].

Table 8.9. Specifically used gates and their description

	Symbol name	Description	Reliability model
	Basic event	Basic event for which reliability information is available	Component failure mode or a failure mode cause
	Conditional event	Event that is a condition of occurrence of another event when both must occur for the output to occur	Occurrence of event that must occur for another event to occur
	Dormant event	A basic event that represents a dormant failure	Dormant component failure mode or dormant failure cause
	Undeveloped event	A part of the system that yet has to be developed – defined	A contributor to the probability of failure. Structure of that system part is not yet defined
	Transfer gate	Gate indicating that this part of the system is developed in another part or page of the diagram	A partial reliability block diagram that is shown in other location of the overall system block diagram

Dynamic fault-tree gates refer to a major disadvantage of traditional FTA, which is the inability of standard fault tree models to capture sequence dependencies in the system and still allow an analytic solution. As an example of a sequence dependent failure, consider a system with one active component and one standby spare connected with a switch controller [74]. If the switch controller fails after the active unit fails (and thus the standby is already in use), then the system can continue operation. However, if the switch controller fails before the active unit fails, then the standby unit can not be switched into active operation and the system fails when the active unit fails. Thus, the failure criteria depend not only on the combination of events, but also on the sequence in which events occur. Systems with various sequence dependencies are usually modelled with Markov models. If, instead of using standard Markov fault tree solution methods, the fault tree is converted to a Markov chain for solution, the expressive power of a fault tree can be expanded by allowing certain kinds of sequence dependencies to be modelled. A tool is described [45] that largely automates the process of constructing a software fault-tree of a Pascal program.

8.4.1 Considerations of complex methodology based on structure and function matrix foundation

The relations between the two techniques can be summarized in narrow interpretation that FMEA behaves like an ‘OR’ FTA, in which the previously systematically collected failure causes can (even automatically) build up a tree and the failure effects represent the different top events. The point of this combination is the proper redundancy handling, which cannot be guaranteed during FMEA. There were presented guidelines and conclusion drawn in this Chapter resolving this statement. The combination with FTA technique, the implementation of FMETA (Failure Mode and Effects Tree Analysis) can solve this problem. Aiming prompt a quantitative analysis from a system block diagram (Figure 8.12) or layout through the presented systematic implementation of Matrix FMEA with FMETA brings the analyser faster to the result.

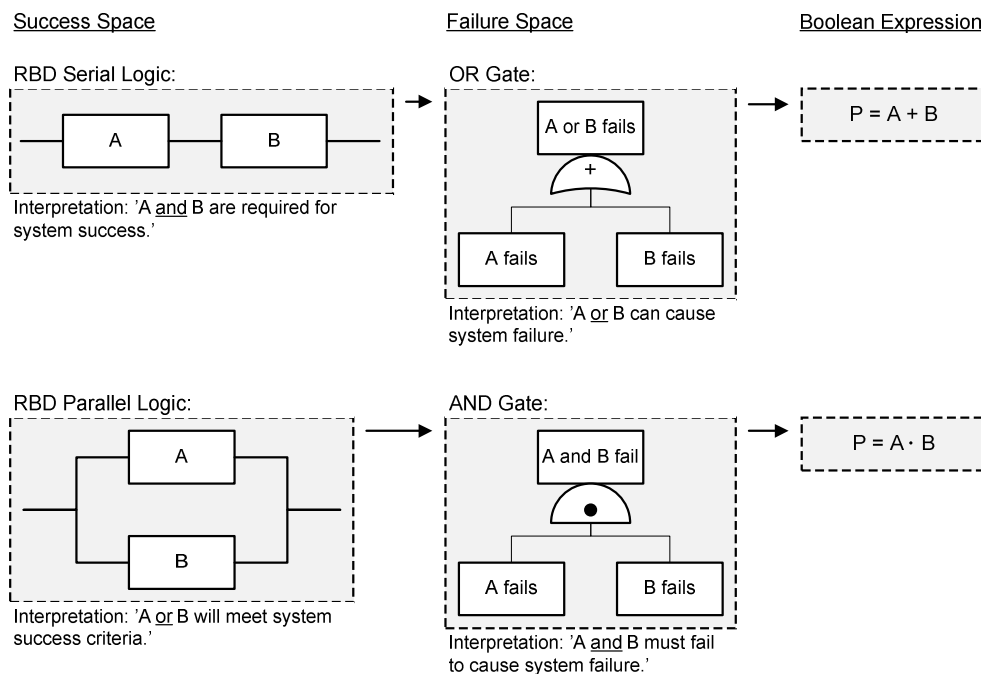


Figure 8.12. Boolean expression of system structure

The whole procedure can be summarized by an MFMETA (Matrix Failure Mode and Effects Tree Analysis) process. The MFMETA schema is the following:

- According to the design concept and system layout deployment of the system hierarchically (system – subsystem – component) marking redundancy
 - Any other form of redundancy (e.g. NMR) should be given as attributes of function failure (in connection to the component responsible for the given function)
- Determination of functions according to system specification per levels (requirements – functions – sub functions) in parallel to

- Fault integration per functions per (system) levels (with possible failure rates, if can be applied)
- Decision about the aim of the analysis:
 - Continuing the analysis as a ‘classic’ FMEA in a qualitative manner
 - Continuing the a analysis as a FTA
 - Conducting also qualitative and quantitative analysis

Failure causes of FMEA which come automatically from Matrix analysis can be converted to FTA inputs with the OR gates. In case of marking redundancy these failure causes should be handled like inputs to AND gates.

9. CONCLUSIONS

Summarizing the thesis it can be stated that the integration of modern electronic technologies and a well-implemented chassis control [95, 96] into an intelligent, a fully electronically controlled power train the overall traffic safety and traffic efficiency [FT3, FT4, FT5, FT19] for heavy goods vehicles can be improved [97]. The by-wire technologies offer functional as well as design benefits, but their application in safety-critical systems, such as the brake and steering [FT14] requires special care during the design and release process.

The proposed theses concerning this work are summarized in the following chapter including publications related to each thesis and the dissertation.

9.1 THESES

THESIS 1. *Based on comparative analyses and critical evaluations the efficiency and deficiency of legislation were presented concerning the electronic stability control function of heavy commercial vehicles (Chapter 6.5). [FT13, FT18]*

The international legislation systems (neither the UN-ECE nor the FMVSS frame) have not had any explicit chapter which describes the operation of the electronic stability control systems until quite recently. The availability of such systems and the strong pressure from the society to reduce the severity, primarily the traffic accident fatalities forced the law makers to address this issue both in Europe and North-America. The difficulties of regulating a system which efficiently intervenes to the vehicle dynamics does not requiring a direct action from the driver is high, many issues have to be addressed: where the regulation is to be placed (existing regulation or new one), what to regulate (system or function), how to regulate (clear performance or pure design criteria should be fulfilled)? In my work I analyzed some these aspects of the highly safety-critical electronic stability control system and elaborated proposals to some of the technical aspect.

- a) The regulation should specify a function and not its/their technical realization.

The SIL (safety integrity level) can be clearly determined for the electronic stability control function and its sub-functions (in-plane, or yaw control and out-of plane or roll-control), and depending on the actual application, the appropriate sub function can be mandated for the given vehicle type. In case of commercial vehicles both sub-functions are applicable either in combination (for motor vehicle, which is controlling the towed vehicle's roll behaviour as well) or as independent functions (only roll-stability control for trailer application). The regulation should not hinder the application of one or another of these sub-functions, this should be regulated on political and technical level.

b) Accepting that the definition of pure performance criteria is the long term optimal solution, actually some design requirement type of elements should be embedded into the regulation in order to promote its short termed acceptance and introduction.

For the control design the yaw rate (for yaw control) and vertical wheel load (for roll control) information, which should not be directly measured, but these variables should be observable. The authorities should check the goodness of these two signal used as state variables, thus it becomes a performance-like criteria. For the sake of the efficient intervention into the vehicle dynamics the electronic throttle control and the individual wheel brake control as actuators should be used. Any additional actuator can be used in the future (electronic steering, suspension, etc.), but in order to ensure the controllability of the vehicle, the engine and brake control is necessary. This criterion can be envisaged as design-like requirement.

The two components above have been integrated into the 11th amendment of the UN-ECE 13 regulation, Annex 21 dealing with electronic stability control systems, and this amendment has been accepted by WP29 in November, 2007. In addition, using this amendment as terms of reference, the WP29 accepted the proposal of the European Union to mandate the ESC system for vehicles above 3.5 tonnes from 2012 (according to a defined roadmap).

THESIS 2. According to reliability design and analysis the iso- and homomorphic system relations were demonstrated between the future commercial vehicle and today's aircraft electronic control and brake systems (Chapter 7.1). [FT11]

a) Relations between aircraft and commercial vehicle control systems

The equivalence relations were deduced between the control systems mentioned above based on principles and guidelines developed in R&D projects supported by 5th EU Frame Programs. The experienced usage of by-wire (fly-by-wire) systems becomes more and more integrated into heavy commercial vehicles regarding the x-by-wire systems providing additional stability and safety functions. In control the command layer collects all the information about the vehicle direction and the surrounding and composes the so called targeted motion vector, the execution layer commands the individual actuators and realizes the motion vector. One can note the composition of the motion vector is very similar to way as the 2 pilots control their airplane. In order to make the autonomous vehicle control safely possible, the information from the command layer must be transmitted to the execution layer in a redundant way, and also the execution layer must have redundant communication and energy supply architecture.

The demonstrated relative isomorphic systems between the aircraft and commercial vehicle control processes provide efficient reliability design and analysis for the improvement of road

vehicle brake systems. (It is widely known that – primarily because of the prescribed reliability and availability requirements – the aircraft control systems represent more advanced level of technology.)

b) Relations between aircraft and heavy commercial vehicle brake system.

The brake system of an aircraft is considered to be highly critical while the plane is taking-off (in case of rejected take-off it has to decelerate the fully loaded plane) and at landing (when its not proper might lead to uncontrollability, blown-up tire or deceleration disability). This explains the layout of a typical airplane brake system. Both the control and the energy supply are redundant, at least all deterministic components are double, in some of the cases there is a third hydraulic circuit used in case of the failure of the primary systems.

THESIS 3. The iso- and homomorphic relation of electronic brake systems (2E) were analysed and the connections with the relative systems of legislation were demonstrated, in so far as these architectures meet the legislative requirements without providing pneumatic back-up mode (Chapter 7.2). [FT9]

According to the relevant legislation today's commercial vehicle brake systems should be designed with two-circuit pneumatic (back-up) systems (2P). Despite the fact that the two-circuit electronic brake system (2E) provides such electronic functions that are available in case of electronic (back-up) system only, these advantages cannot be taken with the prescribed pneumatic back-up systems. Although the 2E meets the legislation requirements, 1E+2P integration is accepted, not the 1E+1P structure even permitted yet.

THESIS 4. It was shown that the presented qualitative reliability analysis technique is not applicable in itself for redundant systems, in order to draw the proper design consequences It was proposed that suitable calculations make the qualitative reliability analysis method adaptable to redundant systems (Chapter 8.2, 8.3). [FT1, FT2, FT16]

The presented qualitative reliability method, the failure modes and effects analysis, is an accepted and widely used technique in concept design phase of system architectures. It can be derived, from its feature handling one failure at a time, that in case of redundant (sub) systems this method is not the most suitable technique. In the final phase of the analysis, at optimization, excluding severity the RPN depends on the new occurrence and detection values. The aim of FMEA is the intervention at failure cause, that is why severity, which refers to failure effect, must remain the same. In this case if a redundant system is the preventive or detection action no adequate information can be derived from system architecture, since fault-tree analysis can give useful values counting with failure rates of failure combinations. The evaluation phase of failure mode and effects analysis based on appropriate ranking catalogues concerning the analysed system and the type of the FMEA. There are given guidelines to the

ranks of each factor (severity, occurrence, detection), for instance, experience in usage, degree of known component features. RPN1 includes factors before optimization which if is above 100 recommendations for corrective actions must be done that is why in the optimization phase with proper considerations must be used to evaluate the whole design. In order to resolve the optimization problem of the redundant system the following operations were introduced during the analysis expressing the weights of each factor. For occurrence (O):

$$O_2 = \frac{O_{1_preventive_action} \cdot O_{1_redundant_preventive_action}}{O_{1_preventive_action} + O_{1_redundant_preventive_action}} \quad (1)$$

For detection (D):

$$D_2 = \min[D_{1_corrective_action}; D_{1_redundant_corrective_action}] \quad (2)$$

Results show the success of optimization, there is no critical risk priority number after these operations.

10. PUBLICATIONS

Refereed journal papers in English

- [FT1] Fülep, T., Palkovics, L., Nádai, L.: On qualitative and operational reliability of electronic brake systems for heavy duty vehicles, *Periodica Polytechnica Transportation Engineering*, 2007. (Accepted for publication)
- [FT2] Fülep, T., Palkovics, L.: On functional and quantitative reliability of electronic brake systems for heavy duty vehicles, *Periodica Polytechnica Transportation Engineering*, 2007. (Accepted for publication)

Refereed journal papers in Hungarian

- [FT3] Fülep, T., Lengyel, D.: Intelligens vezetőtámogató-rendszerek szükségessége a közlekedési balesetek figyelembe vételével, *GÉP*, LVII. évfolyam, 2006/7, 15-18. o.
- [FT4] Fülep, T.: Intelligens vezetőtámogató-rendszerek fontossága a közlekedésben, *Tavaszi Szél 2006*, Kaposvár, Doktoranduszok Országos Szövetségének kiadványa, ISBN 963 229 773 3, 359-362. o.
- [FT5] Fülep, T., Palkovics, L.: Elektronikus jármű és infrastruktúra rendszerek a közlekedésbiztonság növelésének szolgálatában, *Magyar Tudomány*, 2007. (Accepted for publication)
- [FT6] Fülep, T., Nádai, L.: Biztonságkritikus járműrendszerek kvalitatív megbízhatósági elemzése, *A jövő járműve – Járműipari innováció*, 2007/1-2, 35-37. o.

Publications in conference proceedings

- [FT7] Fülep, T., Palkovics, L.: Reliability analysis of redundant electronic brake system for heavy goods vehicle, *Proceedings of the 9th Mini Conference on Vehicle System Dynamics, Identification and Anomalies* (Ed. by Prof. I. Zobory), BUTE Budapest, 8-10 November, 2004, ISBN 963 420 875 4, pp. 303-310.
- [FT8] Fülep, T., Lengyel, D.: Development of electronic dynamic system for road vehicle using data of accident analysis, *Proceedings of the 9th Mini Conference on Vehicle System Dynamics, Identification and Anomalies* (Ed. by Prof. I. Zobory), BUTE Budapest, 8-10 November, 2004, ISBN 963 420 875 4, pp. 311-316.
- [FT9] Fülep, T., Palkovics, L.: Reliability analysis of electronic brake system for heavy duty vehicle, *European Automotive Congress (EAEC 2005)*, Beograd, Serbia, Serbia & Montenegro, 30 May-1st June, 2005, ISBN 86-80941-30-1.
- [FT10] Fülep, T., Óberling, J.: Reliability analysis of an electronic brake system for heavy duty vehicles applying qualitative methodology, *Proceedings of the International Conference on Vehicle Braking Technology* (Ed. by Prof. D. Barton and Dr. J. Fieldhouse), St William's College, York, United Kingdom, 7-9 May 2006, ISBN No. 0 85316 245X, pp. 83-94.

- [FT11] Fülep, T., Óberling, J., Palkovics, L.: Design of redundant brake-by-wire architecture for commercial vehicles based on qualitative reliability approach, Journal of KONES Powertrain and Transport (Ed. by Prof. A. Jankowski), 2006, Vol. 13, No. 1, ISSN 1231 – 4005, pp. 7-16.
- [FT12] Gerum, E., Palkovics, L., Fülep, T.: Brake-by-Wire System in Nutzfahrzeugen – Treiber und Probleme, 2. Grazer Nutzfahrzeug Workshop Handout, Österreich, 12. Mai 2006
- [FT13] Palkovics, L., Straub, L., Koleszár, P., Fülep, T.: Electronic stability control - status of the international legislation with commercial vehicle focus, 9th International Symposium on Heavy Vehicle Weights and Dimensions, June 18-22, 2006, The Pennsylvania State University, State College, Pennsylvania, United States of America. (Available on CD)
- [FT14] Koleszár, P., Voith, A., Palkovics, L., Kandár, T., Fülep, T.: Integrated commercial vehicle chassis control, World Automotive Congress, FISITA 2006, 22-27 October, Yokohama, Japan. (Available on CD)
- [FT15] Fülep T., Óberling J.: Design of x-by-wire architectures based on reliability analyses of electronically non-redundant systems, Proceedings of the 10th Mini Conference on Vehicle System Dynamics, Identification and Anomalies (Ed. by Prof. I. Zobory), BUTE Budapest, 2006. (Accepted for publication)
- [FT16] Fülep T., Óberling J.: Qualitative reliability approach of redundant brake-by-wire design for commercial vehicles, 11th European Automotive Congress (EAEC 2007) ‘Automobile for the Future’, 30 May - 1 June 2007. (Available on CD)
- [FT17] Fülep T., Michelberger P., Nádai L.: Applicability of qualitative reliability analysis for redundant systems, Proceedings of the 3rd International Symposium on Computational Intelligence and Intelligent Informatics (ISCIII '07), IEEE Catalog Number: 07EX1756C, ISBN: 1-4244-1158-0, Library of Congress: 2007923135, Agadir, Morocco, March 28-30, 2007.

Publications in Hungarian

- [FT18] Palkovics, L., Koleszár, P., Fülep, T.: Az elektronikus menetstabilizáló rendszerek - a nemzetközi jogalkotás jelenlegi állása (Electronic stabilization programs – The present situation of international law-making), Magyar Autóipar (Hungarian Automotive Industry), 2006. március, 12-20. o.
- [FT19] Fülep, T., Palkovics, L.: Elektronikus jármű és infrastruktúra rendszerek a közlekedésbiztonság növelésének szolgálatában, 6. Európai Közlekedési Kongresszus, Budapest, 2007. április 25-27., 59-61. o.

11. REFERENCES

- [1] Popović, P., Ivanović, G.: Design for reliability of vehicles in the concept phase, EAEC Congress 2005, Belgrade, Serbia and Montenegro.
- [2] Burkhard, A. H.: Deterministic Failure Prediction, Proc. of Annual Reliability and Maintainability Symposium, Philadelphia, USA, 1987, pp. 21-24.
- [3] Reliability Methods Guideline, Truck and Heavy Equipment Reliability Methods Work Group, Automotive Industry Action Group (AIAG), 2004.
- [4] Dobry, A.: Global denken, lokal handeln, Carl Hanser Verlag, München, 2003, Vol. 48, No. 11, pp. 1096-1097.
- [5] Balogh Dr., A.: A rendszer-megbízhatóság műszaki tervezése, Híradástechnika, LIX. évfolyam, 2004/9, pp. 2-8.
- [6] Rohács, J.: Quick market analysis and foresight on aircraft brake system, 2005.
- [7] W. R. Dunn, L. D. Corliss: Software safety: A User's Practical Perspective, Proc. of Annual Reliability and Maintainability Symposium, Los Angeles, USA, 1990, pp. 430-435.
- [8] Bokor, J., Szabó, G., Gáspár, P., Hetthéssy, J.: Reliability Analysis of Protection Systems in NPPs Using Fault-Tree Analysis Method, Proceedings of the IAEA Symposium on Computerized Reactor Protection and Safety Related Systems in Nuclear Power Plants, pp. 91-104., Budapest, 1997.
- [9] Dick, P.: Feedback of failure and non-conformance information for long-life space systems, Proc. of Advance Techniques in Failure Analysis, 1977, pp. 12-16.
- [10] Hecht, H., Fiorentino, E.: Reliability assessment of spacecraft electronics, Proc. of Annual Reliability and Maintainability Symposium, Philadelphia, USA, 1987, pp. 341-346.
- [11] Harma, T. C., Zilberman, B.: Reliability analysis of redundant aircraft systems with possible latent failures, Proc. of Annual Reliability and Maintainability Symposium, Los Angeles, USA, 1990, pp. 303-308.
- [12] Ulrey, M. L., Palumbo, D. L., Nicol, D. M.: Case study: Safety analysis of the NASA/Boeing Fly-by-light airplane using a new reliability tool, Proc. of Annual Reliability and Maintainability Symposium, Las Vegas, USA, 1996, pp. 318-325.
- [13] Casetta, O. P., Surace, G., Post, W.: Human factors data and accident reporting systems for aviation safety, Safety and Reliability, Lydersen, Hansen & Sandtorv (eds), 1998, Balkema, Rotterdam, pp. 825-831.
- [14] Putney, Jr., B. F., Fragola, J. R.: Application of risk assessment for the NASA vision for space exploration, Risk, Reliability and Societal Safety, Aven & Vinnem (eds), 2007, Taylor & Francis Group, London, pp. 2129-2134.
- [15] Skorupski J., Malarski M., Stelmach A.: Methods for determining air traffic safety, Risk, Reliability and Societal Safety, Aven & Vinnem (eds), 2007, Taylor & Francis Group, London, pp. 2135-2142.
- [16] Travascio L., Compare M., Anna G. D., Gigante G., Vozella A.: About the aerospace and aeronautics domains overlapping in safety issues, Risk, Reliability and Societal Safety, Aven & Vinnem (eds), 2007, Taylor & Francis Group, London, pp. 2151-2156.
- [17] Hedenetz, B., Schedl, A. V.: Fault Injection and Fault Modeling for a Safety-critical Automotive Communication System, Safety and Reliability, Lydersen, Hansen & Sandtorv (eds), 1998, Balkema, Rotterdam, pp. 417-423.

- [18] Rouvroye, J. L., Brombacher, A. C.: New quantitative safety standards: Different techniques, different results?, *Safety and Reliability*, Lydersen, Hansen & Sandtorv (eds), 1998, Balkema, Rotterdam, pp. 305-309.
- [19] Priest, J. W.: Insuring reliability in the design process: Proc. of Annual Reliability and Maintainability Symposium, Las Vegas, USA, 1986, pp. 44-45.
- [20] Kuehn, R. E.: Four decades of reliability experience, Proc. of Annual Reliability and Maintainability Symposium, Orlando, USA, 1991, pp. 76-81.
- [21] Knight, C. R.: Four decades of reliability progress annual reliability and maintainability symposium, Proc. of Annual Reliability and Maintainability Symposium, Orlando, USA, 1991, pp. 156-160.
- [22] Lalli, V.R.: Space-system reliability: a historical perspective, *IEEE Transactions on Reliability*, 1998, Vol. 47, No. 3, pp. 355-360.
- [23] Denson, W.: The history of reliability prediction, *IEEE Transactions on Reliability*, 1998, Vol. 47, No. 3, pp. 321-328.
- [24] Coppola, A.: Reliability engineering of electronic equipment: A historical perspective, *IEEE Transactions on Reliability*, 1984 April, Vol. R-33, pp. 29-35.
- [25] Evans, R.A.: Electronics reliability: a personal view, *IEEE Transactions on Reliability*, 1998, Vol. 47, Issue: 3, Part 2, pp. 329-332.
- [26] Feiler, A. M.: Incorporating risk analysis into life cycle costing, Proc. of Annual Reliability and Maintainability Symposium, Las Vegas, USA, 1986, pp. 469-476.
- [27] Pimentel, J. R.: Verification, validation and certification issues of safety-critical communication systems, *Safety-critical automotive systems*, Ed. by J. R. Pimentel, Society of Automotive Engineers, Inc., 2006, pp. 3-12.
- [28] Leveson, N. G.: *Safeware: System safety and computers*, Addison-Wesley, 1995.
- [29] Amberkar, S., D'Ambrosio, J. G., Murray, B.T., Wysocki, J., Czerny, B. J.: A system-safety process for by-wire automotive systems, *Safety-critical automotive systems*, Ed. by J. R. Pimentel, Society of Automotive Engineers, Inc., 2006, pp. 13-18.
- [30] Bahr, N. J.: *System safety engineering and risk assessment: A practical approach*, Taylor and Francis, Washington DC, 1997.
- [31] Goddard, P. L.: Automotive embedded computing: The current non-fault-tolerant baseline for embedded systems, Proc. of Workshop on Embedded Fault-Tolerant Systems, 1998.
- [32] Rzepka, B., Bertsche, B.: Design of a reliability conception with implementation of costs by a semantic network, Annual Reliability and Maintainability Symposium, Newport Beach, California, USA, 2006.
- [33] Beasley, M.: *Reliability for engineers: An introduction*, Macmillan Press Ltd., 1991.
- [34] Michelberger, P., Barta, Gy., Farkas, T.: Reliability prediction of vehicles by pattern recognition, *Periodica Polytechnica (Transportation Engineering)* 10., 1982, No. 1., pp. 41-52.
- [35] LaPointe, J. T.: SYSREL: Reliability of complex redundant systems, Proc. of Annual Reliability and Maintainability Symposium, Philadelphia, USA, 1985, pp. 63-68.
- [36] Willingham, D. G., Forster, J. D.: Availability tradeoffs for today's complex systems, Proc. of Annual Reliability and Maintainability Symposium, Los Angeles, USA, 1990, pp. 242-249.
- [37] Reid, J. M.: Predicting failure modes to improve reliability, Proc. of Annual Reliability and Maintainability Symposium, Los Angeles, USA, 1990, pp. 497-500.
- [38] Johnson, B. W.: *Design and analysis of fault tolerant digital systems*, Addison-Wesley, 1989.

- [39] Upadhyaya, S. J., Pham, H., Saluja, K. K.: Reliability enhancement by submodule redundancy, Proc. of Annual Reliability and Maintainability Symposium, Los Angeles, USA, 1990, pp. 127-132.
- [40] Forché, R. F.: Analysis of reliability block diagrams with multiple blocks per component, Proc. of Annual Reliability and Maintainability Symposium, Los Angeles, USA, 1990, pp. 145-148.
- [41] Gough, W. S., Riley, J. R., Koren, J. M.: A new approach to the analysis of reliability block diagrams, Proc. of Annual Reliability and Maintainability Symposium, Los Angeles, USA, 1990, pp. 456-464.
- [42] Wood, A. P., Elerath, J. G.: A comparison of predicted MTBFs to field and test data, Proc. of Annual Reliability and Maintainability Symposium, Anaheim, California, USA, 1994, pp. 153-156.
- [43] Cassady, C. R., Hachlas, J. A.: The frequency distribution of availability, Proc. of Annual Reliability and Maintainability Symposium, Anaheim, California, USA, 1994, pp. 278-282.
- [44] Bazovsky Sr., I., Benz, G. E.: An application of fuzzy logic to reliability, Proc. of Annual Reliability and Maintainability Symposium, Atlanta, Georgia, USA, 1993, pp. 372-374.
- [45] Friedman, M. A.: Automated software fault-tree analysis of Pascal programs, Proc. of Annual Reliability and Maintainability Symposium, Atlanta, Georgia, USA, 1993, pp. 458-461.
- [46] Demko, E.: True reliability growth measurement, Proc. of Annual Reliability and Maintainability Symposium, Las Vegas, USA, 1986, pp. 92-96.
- [47] Collas, G.: Reliability & availability estimation for complex systems: a simple concept and tool, Proc. of Annual Reliability and Maintainability Symposium, Anaheim, California, USA, 1994, pp. 110-113.
- [48] Karyagina, M.: Designing for fault-tolerance in the commercial environment, Proc. of Annual Reliability and Maintainability Symposium, Las Vegas, USA, 1996, pp. 258-262.
- [49] Löffelbein, S.: Qualität und Zuverlässigkeit hochintegrierter mechatronischer Systeme, Master-Thesis, Berlin, 2003.
- [50] Pugh, D. R., Snooke, N.: Dynamic analysis of qualitative circuits for failure mode and effects analysis, Proc. of Annual Reliability and Maintainability Symposium, Las Vegas, USA, 1996, pp. 37-42.
- [51] Montgomery, T. A., Pugh, D. R., Leedham, S. T., Twitchett, S. R.: FMEA automation for the complete design process, Proc. of Annual Reliability and Maintainability Symposium, Las Vegas, USA, 1996, pp. 30-36.
- [52] Kukkal, P., Bowles, J. B., Bonnell, R. D.: Database design for failure modes and effects analysis, Proc. of Annual Reliability and Maintainability Symposium, Atlanta, Georgia, USA, 1993, pp. 231-239.
- [53] Goddard, P. L.: Validating the safety of embedded real-time control systems using FMEA, Proc. of Annual Reliability and Maintainability Symposium, Atlanta, Georgia, USA, 1993, pp. 227-230.
- [54] Savakoor, D. S., Bowles, J. B., Bonnell, R. D.: Combining sneak circuit analysis and failure modes and effects analysis, Proc. of Annual Reliability and Maintainability Symposium, Atlanta, Georgia, USA, 1993, pp. 199-205.
- [55] Sexton, R. D.: An alternative method for preparing FMECA's, Proc. of Annual Reliability and Maintainability Symposium, Orlando, USA, 1991, pp. 222-225.
- [56] Kara-Zaitri, C., Keller, A. Z., Barody, I., Fleming, P. V.: An improved FMEA methodology, Proc. of Annual Reliability and Maintainability Symposium, Orlando, USA, 1991, pp. 248-252.

- [57] Dussault, H. B.: Automated FMEA – Status and future, Proc. of Annual Reliability and Maintainability Symposium, San Francisco, USA, 1984, pp. 1-5.
- [58] Goddard, P. L., Daviy, R. W.: The automated, advanced matrix FMEA technique, Proc. of Annual Reliability and Maintainability Symposium, Philadelphia, USA, 1985, pp. 77-81.
- [59] Bluvband, Z., Grabov, P., Nakar, O.: Expanded FMEA, Proc. of Annual Reliability and Maintainability Symposium, Los Angeles, USA, 2004, pp. 31-36.
- [60] Signor, M.: The failure-analysis matrix: A Kinder, gentler alternative to FMEA for information systems, Proc. of Annual Reliability and Maintainability Symposium, Seattle, USA, 2002, pp. 173-177.
- [61] Krasich, M.: Use of fault tree analysis for evaluation of system-reliability improvements in design phase, Proc. of Annual Reliability and Maintainability Symposium, Los Angeles, USA, 2000, pp. 1-7.
- [62] Price, C. J., Taylor, N. S.: FMEA for multiple failures, Proc. of Annual Reliability and Maintainability Symposium, Anaheim, California, USA, 1998, pp. 43-47.
- [63] Bowles, J. B.: The new SAE FMECA standard, Proc. of Annual Reliability and Maintainability Symposium, Anaheim, California, USA, 1998, pp. 48-53.
- [64] Sincell, J., Perez, R. J., Noone, P., Oberhettinger, D.: Redundancy verification analysis – An alternative to FMEA for low cost missions, Proc. of Annual Reliability and Maintainability Symposium, Anaheim, California, USA, 1998, pp. 54-59.
- [65] Onodera, K.: Effective techniques of FMEA at each life-cycle stage, Proc. of Annual Reliability and Maintainability Symposium, Philadelphia, USA, 1997, pp. 50-56.
- [66] Pickard, K., Leopold, T., Dieter, A., Bertsche, B.: Validation of similar based on FMEA assessment, Risk, Reliability and Societal Safety, Aven & Vinnem (eds), 2007, Taylor & Francis Group, London, pp. 1859-1863.
- [67] Marx, G.: The use of the failure mode and effect analysis in automotive product design, Proc. of Advance Techniques in Failure Analysis, 1977, pp. 135-139.
- [68] Cox, T. D., Bohan, E. M.: High reliability by automation and design quality, Proc. of Annual Reliability and Maintainability Symposium, Philadelphia, USA, 1987, pp. 108-114.
- [69] Burkett, M. A.: Facilitating fault tree preparation and review by applying complementary event logic, Proc. of Annual Reliability and Maintainability Symposium, Las Vegas, USA, 1996, pp. 223-228.
- [70] Bouissou, M.: An ordering heuristic for building binary decision diagrams from fault-trees, Proc. of Annual Reliability and Maintainability Symposium, Las Vegas, USA, 1996, pp. 208-214.
- [71] Andrews, J. D., Bartlett, L. M.: Efficient basic event orderings for binary decision diagrams, Proc. of Annual Reliability and Maintainability Symposium, Anaheim, California, USA, 1998, pp. 61-67.
- [72] Bell, D. D., Keene, S. J.: Software reliability: A continuing dilemma, Proc. of Annual Reliability and Maintainability Symposium, Anaheim, California, USA, 1998, p. 215.
- [73] Andrews, J. D., Dunnett, S. J.: Event-tree analysis using binary decision diagrams, IEEE Transactions on Reliability, Vol. 49, No. 2, June 2000, pp. 230-238.
- [74] Dugan, J. B.: Fault-tree analysis of computer-based systems, Proc. of Annual Reliability and Maintainability Symposium, Washington, USA, 1999, pp. Dugan-1-24.
- [75] Rawicz, A. H., Girling, D. R.: Neural-network enhancement for a reliability expert-system, Proc. of Annual Reliability and Maintainability Symposium, Anaheim, California, USA, 1994, pp. 468-474.

- [76] Dhillon, B. S.: Reliability engineering in systems design and operation, Van Nostrand Reinhold Company Inc., 1983.
- [77] Dhillon, B. S., Reiche, H.: Reliability and maintainability management, Van Nostrand Reinhold Company Inc., 1985.
- [78] Bertsche, B., Lechner, G.: Zuverlässigkeit im Maschinenbau, Ermittlung von Bauteil- und System-Zuverlässigkeiten, Springer-Verlag Berlin, Heidelberg, 1990.
- [79] Thompson, G.: Improving maintainability and reliability through design, Professional Engineering Publishing, London, 1999.
- [80] Bertsche, B., Lechner, G.: Zuverlässigkeit im Fahrzeug- und Maschinenbau, Ermittlung von Bauteil- und System-Zuverlässigkeiten, 3., überarbeitete und erweiterte Auflage, Springer-Verlag Berlin Heidelberg New York, 2004.
- [81] Reichel, H.-R.: Elektronische Bremssysteme, Vom ABS zum Brake-by-Wire, 2. Auflage, Expert Verlag, 2003.
- [82] Czerny, B., D'Ambrosio, J. G., Jacob, P. O., Murray, B. T.: Identifying and understanding relevant system safety standards for use in the automotive industry, Safety-critical automotive systems, Ed. by J. R. Pimentel, Society of Automotive Engineers, Inc., 2006, pp. 101-111.
- [83] Braband, J.: On a formal definition of risk in standards for safety-related computer systems, Forms/Format 2004, Formal Methods for Automation and Safety in Railway and Automotive Systems, Schnieder, E. & Tarnai, G. (eds), Braunschweig, Germany pp. 19-23.
- [84] Rástocny, K., Janota, A., Zahradník, J., Franeková, M.: How to negate risk resulting from implementation of new functions into the existing safety-related system, Forms/Format 2004, Formal Methods for Automation and Safety in Railway and Automotive Systems, Schnieder, E. & Tarnai, G. (eds), Braunschweig, Germany pp. 24-29.
- [85] Current Analysis of the Accident Statistics: Mercedes Passenger Cars Get Into Fewer Accidents, www.media.daimlerchrysler.com
- [86] Dang, J. N.: Preliminary results analyzing the effectiveness of electronic stability control (ESC) systems, DOT HS 809 790, Evaluation Note, September 2004.
- [87] Garrot, R.: The Status of the NHTSA's ESC Research, US-DOT NHTSA, 329244_web, 2005.
- [88] Kimbrough, S.: Coordinated Braking and Steering Control for Emergency Stops and Acceleration, ASME WAM 1991, Proc. of Advanced Automotive Technologies, DE-Vol. 40, pp. 243.
- [89] Kimbrough, S., and VanMoorhem: A Control Strategy for Stabilizing Trailers via Selective Actuation of Brakes, ASME 1992, Transportation Systems, DSC.-Vol. 44, pp. 413-428.
- [90] Palkovics, L., El-Gindy, M.: Examination of different control strategies of heavy-vehicle performance, Int.J. of Dynamic Systems, Measurement and Control, 1996, Vol. 118, pp. 489-498.
- [91] Palkovics, L., El-Gindy, M.: Design of an active unilateral brake control system for five-axle tractor-semitrailer based on sensitivity analysis, Vehicle System Dynamics, 1995, Vol. 24, pp. 725-758.
- [92] Kübler Dr., Klaus: Development and safety evaluation of driving-critical systems in the context of the IEC 61508, Forms/Format 2004, Formal Methods for Automation and Safety in Railway and Automotive Systems, Schnieder, E. & Tarnai, G. (eds), Braunschweig, Germany pp. 24-29.
- [93] Srinivasan, S. K., Subramanian R.: Probabilistic Analysis of Redundant Systems, Springer-Verlag, Berlin, 1980.
- [94] Ebeling, C. E.: An Introduction to Reliability and Maintainability Engineering, Mcgraw-Hill Companies, Inc., 1997.
- [95] Péter, T.: Gépjármű lengőrendszerek felfüggesztésparamétereinek optimalása, MTA, Budapest, Kandidátusi értekezés, 1997.

- [96] Péter, T.: Mathematical Transformations of Road Profile Excitation for Variable Vehicle Speeds. Studies in Vehicle Engineering and Transportation Science – A Festschrift in Honor of Professor Pál Michelberger on Occasion of his 70th Birthday. Hungarian Academy of Sciences; Budapest Univ. of Technology and Economics, 2000, pp. 51-69.
- [97] Armbruster, M., Bäuerle, K., Reichel, R., Maisch, A., Spiegelberg, G.: X-By-Wire systems of the next generation, AVEC International Symposium, 2004, Arnhem, The Netherlands.
- [98] Papadopoulos, Y., Grante, C., Wedlin, J.: Automating aspects of safety design in contemporary automotive system engineering, FISITA Conference, 2004, Barcelona, Spain.
- [99] Dhillon, B. S.: Design reliability: Fundamentals and Applications, CRC Press LLC, 1999.
- [100] Robinson, R. M., Anderson, K. J.: SIL Rating Fire Protection Equipment, 8th Australian Workshop on Safety-critical Systems and Software (SCS'03), Canberra. Conferences in Research and Practice in Information Technology, P. Lindsay & T. Cant, Eds., Vol. 33.
- [101] Prezenszki, J., Várlaki, P.: A raktári anyagmozgatási géprendszerek megbízhatósági és kapacitásvizsgálata, GÉP, XXX. évfolyam, 3. szám, március.
- [102] Filippidis Dr., A. B. L.: Acceptable failure detection and negation times based on hazard rates and probabilities, Forms/Format 2004, Formal Methods for Automation and Safety in Railway and Automotive Systems, Schnieder, E. & Tarnai, G. (eds), Braunschweig, Germany pp. 44-51.
- [103] Schäbe Dr., H.: Different approaches for determination of tolerable hazard rates, Proc. of European Safety and Reliability Conference (ESREL) 2001, Torino, Vol. 1, pp. 435-442.
- [104] Hammett, R. C., Babcock, P. S.: Achieving 10^{-9} Dependability with drive-by-wire systems, Safety-critical automotive systems, Ed. by J. R. Pimentel, Society of Automotive Engineers, Inc., 2006, pp. 149-162.
- [105] Pimentel, J. R.: An architecture for a safety-critical steer-by-wire system, Safety-critical automotive systems, Ed. by J. R. Pimentel, Society of Automotive Engineers, Inc., 2006, pp. 199-207.
- [106] Breyfogle, F. W. III.: Implementing Six Sigma: Smarter solutions using statistical methods, John Wiley & Sons, 1999.
- [107] Russomanno, D. J., Bonnell, R. D., Bowles, J. B.: Viewing computer-aided failure modes and effects analysis from an artificial intelligence perspective, Integrated Computer-Aided Engineering, Vol. 1, 1994, pp. 209-228.
- [108] Huang, G. Q., Nie, M., Mak, K. L.: Web-based failure mode and effect analysis, Computer & Industrial Engineering, Vol. 37, 1999 Oct, pp. 177-180.
- [109] Norman, D. A.: The design of everyday things, 1990, Doubleday.
- [110] Lee, B. H.: Encoding design FMEA casual models as Bayesian network structures, Int. Conf. on Engineering Design, 1999 Aug, pp. 165-170.
- [111] Lee, B. H.: Using Bayes belief networks in industrial FMEA modelling and analysis, Proc. of Annual Reliability and Maintainability Symposium, Philadelphia, USA, 2001, pp. 7-15.
- [112] Passey, R. D. C.: Foresight begins with FMEA, Medical Device Technology, Vol. 10, 1999, pp. 88-92.
- [113] Piolat, A., Roussey, J., Thunin, O.: Effects of screen presentation on text reading and revising, Int. Journal of Human-Computer Studies, Vol. 47, 1997, pp. 565-589.
- [114] Kara-Zaitri, C., Fleming, P. V.: Application of fuzzy inference methods to failure modes effects and criticality analysis (FMECA), Int. conf. on Safety and Reliability, 1997, pp. 2403-2414.
- [115] Gilchrist, W.: Modelling failure modes and effects analysis, Int. Journal of Quality and Reliability Management, Vol. 10, 1993, pp. 16-23.

- [116] Szabó, G., Gáspár, P.: Practical treatment methods for adaptive components in the fault-tree analysis, Proc. of Annual Reliability and Maintainability Symposium, Washington, USA, 1999, pp. 97-104.
- [117] http://www.relexsoftware.com/resources/art/art_fta2.asp
- [118] Boulanger, J. L., Schön, W.: Reference systems and standards for safety assessment of railway applications, Risk, Reliability and Societal Safety, Aven & Vinnem (eds), 2007, Taylor & Francis Group, London, pp. 2609-2613.
- [119] A Scientific Study 'ETAC' European Truck Accident Causation, Executive Summary and Recommendations, International Road Transport Union (IRU), 2007.
- [120] Failure Mode and Effects Analysis, FMEA, Robert Bosch GmbH, 1998.
- [121] http://en.wikipedia.org/wiki/Space_Shuttle_Challenger_disaster
- [122] Bartha, T., Náday, L., Szabó, G.: Dependable architectures and techniques for electronic brake systems, MTA-SZTAKI study for Knorr-Bremse R&D Center Budapest August, 2005.
- [123] Szabó, G., Gáspár, P.: Probabilistic dependability analysis of adaptive functions: a fault-tree based approach and its applications in transportation, Periodica Polytechnica, 1998, Vol. 26, pp. 187-200.
- [124] Posfalvi, Ö.: Haszonjárművek stabilitásának mechanikai elméleti vizsgálata, Járművek, Mezőgazdasági Gépek, Vol. 35., 12/1988, 471. o.
- [125] Posfalvi, Ö.: Mechanical Test of the Stability of Tractor-Semitrailer System., Periodica Polytechnica, Vol. 18., 1990, 1-2., p. 173.
- [126] IEC 61508 - International standard for electrical, electronic and programmable electronic safety related systems, 1998.
- [127] United Nations, ECE Regulation No. 13, 2004.
- [128] Weibull, W.: A statistical distribution function of wide applicability, J. Appl. Mech.-Trans. ASME 18(3), 1951, pp. 293-297.